ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Аналіз та порівняння протоколів маршрутизації для побудови надійних та швидких комп'ютерних мереж»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерна інженерія
(назва)

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

_____ *Олег ГАЛЕНКО*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КІД-42
Олег ГАЛЕНКО
Ім'я, ПРІЗВИЩЕ
Керівник: Ярослав ТОРОШАНКО
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Рецензент: _____
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерної інженерії

Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерної інженерії
_____ Наталія ЛАЩЕВСЬКА
_____
«_____» _____ 2025р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Галенко Олег Олегович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Аналіз та порівняння протоколів маршрутизації для побудови надійних та швидких комп'ютерних мереж
_____
керівник кваліфікаційної роботи Ярослав ТОРОШАНКО
_____,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «24» лютого 2025р. № 56
2. Строк подання кваліфікаційної роботи «3» червня 2024р.
3. Вихідні дані до кваліфікаційної роботи: науково-технічна література; Фундаментальні принципи функціонування комп'ютерних мереж та технологій маршрутизації. Стандарти та рекомендації міжнародних організацій (IETF RFC), Наукові публікації, монографії та технічна документація провідних виробників мережевого обладнання
_____
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. _____
2. _____
3. _____
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання «24» лютого 2025р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	25.02-24.03.2025	
2	Обробка матеріалу	23.03-05.04.2025	
3	Розробка теоретичної частини	06.04-10.04.2025	
4	Преддипломна практика	21.04-16.05.2025	
5	Висновки за результатами аналізу	17.05-19.05.2025	
6	Розробка презентації	20.05-26.05.2025	
7	Передзахист	27.05-29.05.2025	
8	Здача в деканат	03.06-03.06.2025	

Здобувач вищої освіти _____ Олег ГАЛЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ярослав ТОРОШАНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 46 стор., 2 рис., 9 джерел.

Мета роботи – Проаналізувати різні протоколи маршрутизації для визначення їх ефективності та надійності для побудови сучасних комп'ютерних мереж.

Об'єкт дослідження – Дослідження протоколів маршрутизації, їх характеристики, переваги та недоліки з метою вибору найбільш відповідного протоколу для побудови надійних та швидких комп'ютерних мереж.

Предмет дослідження – Різні протоколи маршрутизації, їх функціональні особливості та показники.

Короткий зміст роботи: У роботі розглянуто фундаментальні принципи маршрутизації, класифікацію протоколів та ключові критерії їх оцінки. Детально проаналізовано алгоритмічні основи основних класів протоколів внутрішньої маршрутизації (IGP): дистанційно-векторних (на прикладі RIP), протоколів на основі стану каналу (на прикладі OSPF) та гібридних протоколів (на прикладі EIGRP). Також розглянуто принципи функціонування протоколу зовнішньої маршрутизації BGP.

Проведено порівняльний аналіз зазначених протоколів за такими ключовими показниками, як швидкість конвергенції, ефективність використання мережевих та обчислювальних ресурсів, масштабованість, стійкість до утворення петель маршрутизації та механізми забезпечення відмовостійкості. Особливу увагу приділено аспектам, що безпосередньо впливають на надійність та швидкодію мережевої інфраструктури. На основі проведеного дослідження сформульовано практичні рекомендації щодо вибору оптимального протоколу маршрутизації залежно від розміру мережі, вимог до продуктивності, надійності, наявного обладнання та специфіки завдань, що вирішуються.

КЛЮЧОВІ СЛОВА: ПРОТОКОЛИ МАРШРУТИЗАЦІЇ, RIP, OSPF, EIGRP, BGP, НАДІЙНІСТЬ МЕРЕЖІ, ШВИДКОДІЯ МЕРЕЖІ, АНАЛІЗ ПРОТОКОЛІВ, ПОРІВНЯННЯ ПРОТОКОЛІВ, КОМП’ЮТЕРНІ МЕРЕЖІ.

ЗМІСТ

ВСТУП…… 8
1. ПОНЯТТЯ МАРШРУТИЗАЦІЇ…… 10
1.1 Базова маршрутизація……..... 10
1.2 Класифікація протоколів маршрутизації …… 11
1.3 Критерії вибору та порівняння протоколів маршрутизації …….. 13
2 СТРУКТУРА ТА АЛГОРИТМИ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ.. 15
2.1 Фундаментальні механізми функціонування протоколів маршрутизації …… 16 16
2.2 Алгоритмічні основи дистанційно-векторних протоколів маршрутизації…… 19
2.3 Алгоритмічні основи протоколів маршрутизації на основі стану каналу …….. 23
2.4 Алгоритмічні основи гібридних (збалансованих) протоколів маршрутизації …… 28
АНАЛІЗ ЗАСТОСУВАННЯ ДИНАМІЧНИХ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ В СИСТЕМАХ ДЛЯ ПІДВИЩЕННЯ ТА ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ МЕРЕЖІ…… 31
3.1 Аналіз використання дистанційно-векторних протоколів маршрутизації ……..... 31
3.2 Протокол RIP ……. 32
3.3 Протокол IGRP …… 36
3.4 Протокол EIGRP ……... 39
3.5 Протокол BGP ……..43
3.6 Протокол OSPF…….47
ВИСНОВКИ…… 52
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ…….. 54

ВСТУП

У сучасному світі, де цифрова трансформація охоплює всі сфери життя, стабільність та ефективність комп’ютерних мереж стають критично важливими. Від безперебійної роботи корпоративних систем до швидкості передачі даних у глобальному інтернеті — основу цих процесів закладають протоколи маршрутизації, які визначають оптимальні шляхи для інформації. Вибір правильного протоколу впливає не лише на продуктивність мережі, а й на її здатність адаптуватися до змін, протистояти збоям та забезпечувати безпеку даних. Проте різноманітність існуючих рішень, таких як RIP, OSPF, EIGRP чи BGP, ускладнює завдання інженерів, які стикаються з необхідністю балансувати між швидкодією, надійністю та масштабованістю.

Метою даної роботи є комплексний аналіз сучасних протоколів маршрутизації, спрямований на визначення їх переваг, недоліків та оптимальних сфер застосування. Дослідження охоплює як теоретичні аспекти функціонування алгоритмів (від Distance-Vector до Link-State), так і практичні експерименти, проведені за допомогою симуляторів мереж. У роботі порівнюються ключові параметри: час збіжності після збоїв, витрати ресурсів, підтримка IPv6, рівень захисту від кіберзагроз, а також придатність для різних типів інфраструктур — від локальних мереж малих підприємств до розподілених систем дата-центрів.

Важливим результатом дослідження стають рекомендації щодо вибору протоколів відповідно до конкретних вимог: наприклад, OSPF для динамічних середовищ із високою доступністю, BGP для глобальних мереж із складною топологією або EIGRP для гібридних рішень у корпоративних сегментах. Окрема увага приділена тенденціям майбутнього, таким як інтеграція SDN (програмно-визначених мереж) та вплив технологій 5G/IoT на розвиток маршрутизації.

1. Поняття маршрутизації

1.1 Базова Маршрутизація

Маршрутизація є ключовим процесом у комп'ютерних мережах, основним завданням якого є визначення оптимальних шляхів для передачі даних між вузлами. Вона ґрунтується на використанні **таблиць маршрутизації** — спеціалізованих структур даних, що зберігаються на маршрутизаторах та містять інформацію про доступні мережеві маршрути, включаючи адреси призначення, інтерфейси виходу та метрики. Саме метрики виступають критеріями для вибору найефективнішого шляху. Серед них найчастіше використовуються **затримка** (час передачі пакета від джерела до одержувача) та **пропускна здатність** (максимальний обсяг даних, який може бути переданий через канал за одиницю часу). Наприклад, протоколи, орієнтовані на мінімізацію затримки, забезпечують ефективність для потокового відео, тоді як високі значення пропускної здатності критичні для передачі великих масивів даних.

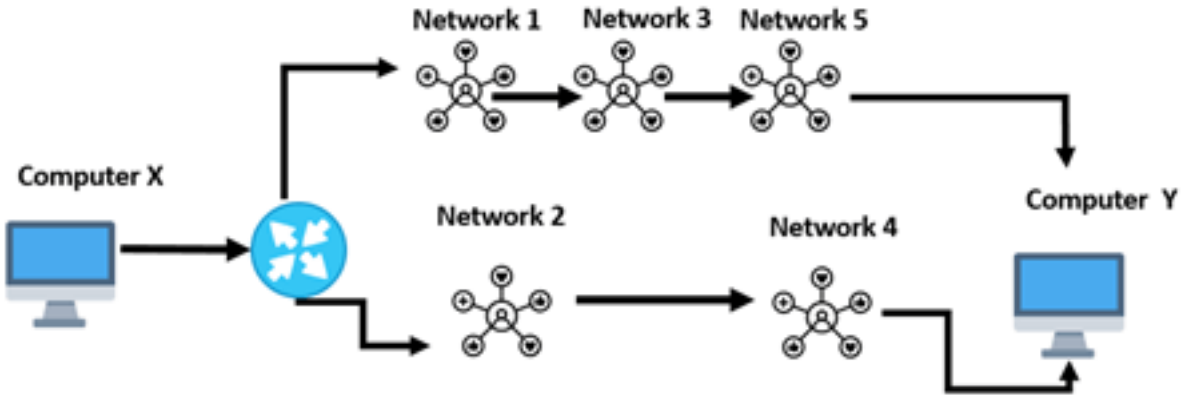


Рисунок 1.1 – Приклад роботи маршрутизації мережі

1.2 Класифікація протоколів маршрутизації

Маршрутизаційні протоколи поділяються на категорії за механізмами роботи та методами обміну інформацією між вузлами. Перший рівень класифікації базується на способі визначення маршрутів: **статичні** та **динамічні** (рис 1.2). Статичні протоколи передбачають ручне задавання шляхів адміністратором, що забезпечує повний контроль над топологією, але вимагає постійного втручання при змінах мережі. Динамічні протоколи автоматично адаптуються до змін, обмінюючись даними про доступні шляхи між маршрутизаторами, що робить їх придатними для складних і масштабних інфраструктур.

Серед динамічних протоколів виділяють дві основні групи: **Distance-Vector** (вектор відстані) та **Link-State** (стан зв'язків). Протоколи типу Distance-Vector, такі як RIP або IGRP, працюють на основі періодичного обміну повними таблицями маршрутизації між сусідніми вузлами. Вибір оптимального шляху здійснюється через метрики, такі як кількість переходів (хопів). Навпаки, протоколи Link-State (наприклад, OSPF, IS-IS) передають інформацію лише про стан безпосередніх зв'язків, після чого кожен маршрутизатор самостійно будує повну карту мережі за допомогою алгоритмів (наприклад, Дейкстри) і обчислює найкоротші шляхи.

Окрім класичних дистанційно-векторних та протоколів стану каналу, виділяють так звані гібридні або вдосконалені дистанційно-векторні протоколи. Прикладом такого підходу є EIGRP, який, використовуючи алгоритм DUAL, забезпечує швидке визначення оптимальних та резервних шляхів. Він підтримує топологічну базу даних, що є характерною рисою Link-State протоколів, однак механізм розповсюдження оновлень в EIGRP є більш вибірковим та ефективним, знижуючи навантаження. Завдяки цьому досягається висока швидкість реакції на зміни в мережі та стабільність її роботи при оптимальному використанні ресурсів маршрутизаторів.

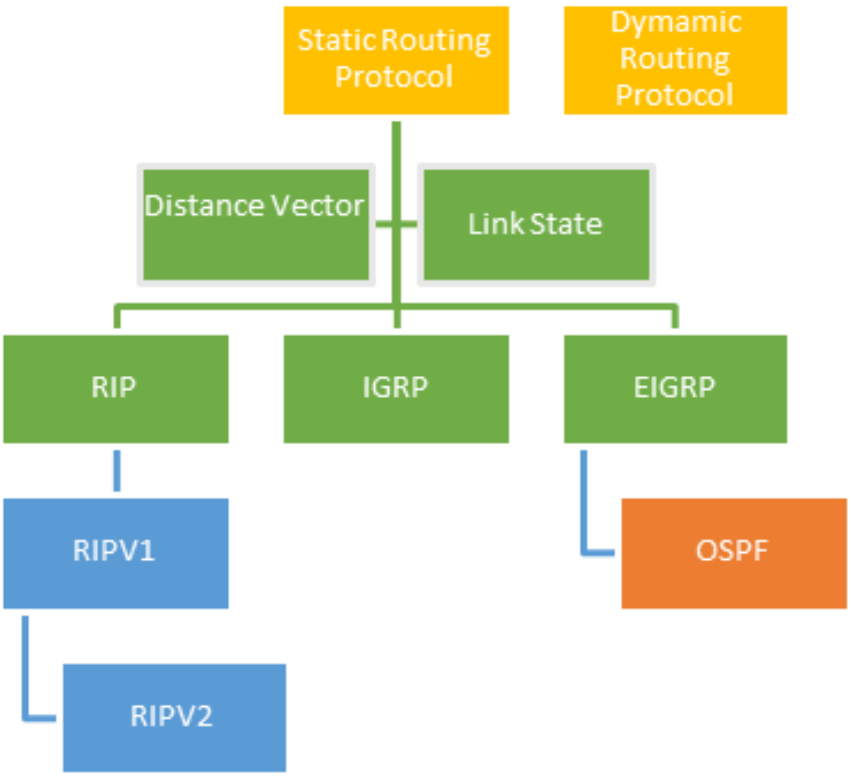


Рисунок 1.2 – Типи протоколів маршрутизації

Центральним елементом EIGRP, що забезпечує його ефективність, є алгоритм **Diffusing Update Algorithm (DUAL)**. DUAL не лише обирає найкращий безпетлевий шлях до мережі призначення, відомий як **Successor**, але й проактивно ідентифікує **Feasible Successor(s)** – резервні безпетлеві шляхи. Ключовим для цього є дотримання "умови здійсненності" (Feasibility Condition): шлях через сусіда вважається Feasible Successor, якщо метрика цього сусіда до кінцевого пункту (Advertised Distance, AD) є строго меншою, ніж поточна найкраща метрика локального маршрутизатора до того ж пункту (Feasible Distance, FD). Якщо основний шлях (Successor) стає недоступним, але існує Feasible Successor, EIGRP майже миттєво перемикається на нього без необхідності запуску складних обчислень чи надсилання запитів (Query) іншим маршрутизаторам, що кардинально прискорює збіжність мережі. Вся інформація про відомі шляхи, їх метрики, а також про Successors та Feasible Successors зберігається у **топологічній таблиці (Topology Table)**, тоді як таблиця сусідів (Neighbor Table) формується за допомогою обміну Hello-пакетами та підтримує актуальний стан зв'язків..

1.3 Критерії вибору та порівняння протоколів маршрутизації

Обґрунтований вибір оптимального протоколу маршрутизації є фундаментальним інженерним завданням при проєктуванні комп'ютерних мереж, оскільки універсального рішення не існує, і вибір завжди є компромісом, що ґрунтується на аналізі специфічних вимог мережі та її операційних цілей. До ключових факторів, що впливають на цей процес, належить **масштаб мережі та її потенціал до розширення**: для невеликих мереж можуть підійти простіші протоколи (наприклад, RIP), тоді як для середніх та великих корпоративних мереж перевага надається OSPF або EIGRP, а для глобальних – BGP. Важливими є також **вимоги до швидкості збіжності**, критичної для сервісів реального часу, та **топологічна конфігурація мережі**, оскільки різні структури впливають на ефективність протоколів. Протоколи OSPF, IS-IS та EIGRP зазвичай забезпечують вищу швидкість збіжності порівняно з класичними дистанційно-векторними аналогами.

Поряд із фундаментальними факторами, вибір протоколу детермінується практичними та ресурсними аспектами. До таких належать **апаратні ресурси маршрутизаторів** (CPU, пам'ять), оскільки протоколи стану каналу є більш вимогливими. **Рівень складності конфігурування та адміністрування** також є суттєвим, особливо для організацій з обмеженими IT-ресурсами; протоколи OSPF та EIGRP вимагають глибшого розуміння порівняно з RIP. З позицій забезпечення інформаційної **безпеки**, сучасні протоколи (OSPF, EIGRP, BGP) підтримують механізми автентифікації маршрутних оновлень. Нарешті, **правовий статус протоколу** – його належність до відкритих стандартів чи пропрієтарних розробок – впливає на сумісність обладнання та гнучкість вибору вендорів.

Порівняльний аналіз протоколів маршрутизації базується на їхніх іманентних техніко-експлуатаційних характеристиках. Фундаментальною відмінністю є імплементований **алгоритм роботи** (дистанційно-векторний, стану каналу чи гібридний), що визначає механізми збору інформації, розрахунку шляхів та реакції на зміни. Кожен протокол використовує власну **метрику** для визначення оптимального шляху (наприклад, кількість переходів для RIP, "вартість" для OSPF, композитна метрика для EIGRP). У випадках отримання інформації про маршрут від декількох джерел, маршрутизатор застосовує **адміністративну відстань (AD)** – числовий індикатор довіри до джерела, де менше значення означає вищий пріоритет.

Важливою експлуатаційною характеристикою є ефективність **механізмів запобігання петлям маршрутизації**, критичних для стабільності мережі. Дистанційно-векторні протоколи використовують для цього Split Horizon та інші техніки, тоді як протоколи стану каналу та EIGRP забезпечують безпетлевість за своєю природою. Сучасні протоколи повинні підтримувати технології **безкласової адресації (VLSM та CIDR)**. **Тип, частота та обсяг оновлень маршрутної інформації** також різняться, впливаючи на завантаження мережі: від періодичного розсилання повних таблиць у RIP до тригерних, часткових оновлень в OSPF та EIGRP. Можливість **балансування навантаження** є важливою функцією для оптимізації ресурсів. Розуміння цих критеріїв та характеристик формує методологічну базу для подальшого детального аналізу та порівняння протоколів RIP, OSPF та EIGRP, що є метою наступних розділів даної роботи.

2. Структура та алгоритми протоколів маршрутизації

2.1 Фундаментальні механізми функціонування протоколів маршрутизації

Протоколи маршрутизації, що є невід'ємною складовою сучасних комп'ютерних мереж, забезпечують інтелектуальну основу для передачі даних, дозволяючи маршрутизаторам колективно визначати та підтримувати оптимальні шляхи через складні, динамічно змінювані топології. Незважаючи на значне розмаїття існуючих протоколів, кожен з яких адаптований під конкретні завдання та умови, в їхній основі лежить набір універсальних функціональних принципів та компонентів. Глибоке розуміння цієї спільної архітектурної бази є критично важливим для подальшого аналізу їхніх класифікаційних відмінностей, алгоритмічних особливостей та, зрештою, для формування обґрунтованих рішень при проектуванні мережевих інфраструктур, орієнтованих на високу надійність та швидкодію. Цей підрозділ присвячений детальному розгляду таких ключових елементів, що формують єдину функціональну структуру протоколів маршрутизації

Процес взаємодії маршрутизаторів, керованих динамічними протоколами, незмінно починається з етапу **виявлення та встановлення відносин сусідства**. Сусідами, або, в термінології деяких протоколів, суміжними маршрутизаторами (**adjacencies**), вважаються пристрої, що підключені до одного фізичного чи логічного сегмента мережі та здатні безпосередньо обмінюватися маршрутною інформацією. Цей процес зазвичай ініціюється за допомогою спеціалізованих службових повідомлень, часто відомих як "Hello-пакети", які періодично розсилаються на зарезервовані для протоколу групові або широкомовні адреси. Отримання такого пакета сигналізує маршрутизатору про присутність потенційного партнера для обміну даними. Важливо, що ці Hello-пакети часто несуть не лише ідентифікаційну інформацію відправника, як-от унікальний ідентифікатор маршрутизатора (**Router ID**), але й набір критичних параметрів конфігурації. До таких параметрів можуть належати ідентифікатор мережевої області (наприклад**, Area ID** в **OSPF**), маска підмережі, часові інтервали роботи протоколу (**Hello Interval, Dead Interval**), а також прапори та дані автентифікації. Успішне встановлення сусідства можливе лише за умови повного збігу цих параметрів між потенційними сусідами, що слугує важливим механізмом запобігання обміну потенційно некоректною або конфліктною маршрутною інформацією. Наприклад, у протоколі **OSPF** маршрутизатори, що знаходяться в різних областях (за винятком спеціальних типів сусідств, як-от з **ABR**) або мають неузгоджені таймери Hello/Dead, не зможуть сформувати відносини суміжності. Після успішного встановлення, ці відносини потребують постійної підтримки, яка також реалізується через періодичний обмін Hello-пакетами або аналогічними механізмами, як-от **Keepalive**-повідомлення в протоколі **BGP**. Якщо маршрутизатор перестає отримувати такі підтверджуючі сигнали від сусіда протягом визначеного часового інтервалу (зазвичай **Dead Interval**, що у кілька разів перевищує **Hello Interval**), він розцінює це як втрату зв'язку, розриває відносини сусідства та ініціює процес перерахунку маршрутів, видаляючи всі шляхи, що були отримані від цього, тепер вже недоступного, сусіда. Цей механізм є фундаментальним для забезпечення швидкої реакції мережі на зміни топології, такі як відмова каналу зв'язку або вихід з ладу маршрутизатора, що безпосередньо впливає на загальну надійність та відмовостійкість мережевої інфраструктури. Варто зазначити, що протоколи зовнішньої маршрутизації, такі як BGP, мають свою специфіку: встановлення сусідства (пірінгу) тут не відбувається автоматично на основі широкомовних Hello-пакетів, а вимагає явного адміністративного конфігурування та часто покладається на протокол **TCP** для забезпечення надійного транспортного з'єднання між піринговими маршрутизаторами, які можуть бути географічно віддалені та не мати прямого фізичного з'єднання.

Після того, як відносини сусідства встановлені та підтверджені, починається ключовий етап – **обмін маршрутною інформацією**. Саме цей процес є серцевиною будь-якого динамічного протоколу маршрутизації. Маршрутизатори інформують один одного про мережі, до яких вони мають доступ, та про характеристики шляхів до цих мереж. Форми, зміст та періодичність цього обміну суттєво варіюються залежно від типу протоколу. Історично, ранні дистанційно-векторні протоколи, як-от RIP, вдавалися до періодичної передачі всієї своєї таблиці маршрутизації всім сусідам, наприклад, кожні 30 секунд. Такий підхід, хоч і простий в реалізації, призводив до значного навантаження на мережу службовим трафіком, особливо у великих та стабільних мережах. Сучасніші реалізації дистанційно-векторних протоколів та більш просунуті протоколи, такі як **EIGRP**, застосовують значно ефективніші стратегії. Вони можуть використовувати так звані "спровоковані оновлення" **(triggered updates**), коли інформація про зміни розсилається негайно, а не за розкладом, а також передавати лише часткові оновлення, що стосуються лише змінених маршрутів, після початкового повного обміну таблицями. На противагу цьому, канально-станні протоколи, такі як **OSPF** та **IS-IS**, оперують інакше. Кожен маршрутизатор у мережі генерує детальну інформацію про стан своїх безпосередньо підключених каналів зв'язку та про встановлені відносини сусідства. Ця інформація оформлюється у вигляді спеціальних повідомлень (**Link-State Advertisements - LSAs** в **OSPF**, або **Link State PDUs - LSPs** в **IS-IS**) і потім розповсюджується методом "затоплення" (**flooding**) по всій мережевій області або домену маршрутизації. В результаті, кожен маршрутизатор в межах області отримує ідентичну копію бази даних станів каналів **(Link-State Database - LSDB**), що представляє собою повну карту топології цієї області. Оновлення розсилаються лише тоді, коли відбуваються реальні зміни у стані каналу (наприклад, його активація чи деактивація, зміна вартості), що робить канально-станні протоколи більш ефективними з точки зору використання пропускної здатності у стабільних мережевих середовищах.

Протоколи вектора шляху, до яких належить **BGP**, обмінюються інформацією про повні шляхи до мереж призначення, представлені у вигляді послідовності номерів автономних систем (атрибут AS_PATH), що дозволяє ефективно виявляти та запобігати петлям маршрутизації на міждоменному рівні. Крім того, **BGP** передає велику кількість різноманітних атрибутів шляху, які використовуються для реалізації складних політик маршрутизації, що є його ключовою особливістю. Оновлення в **BGP** також передаються лише при змінах у доступності маршрутів або їхніх атрибутах. Забезпечення надійності передачі цієї критично важливої маршрутної інформації є першочерговим завданням. Деякі протоколи, як-от **RIP** та частково **EIGRP**, використовують **UDP** для транспортування своїх повідомлень, покладаючись на власні вбудовані механізми для підтвердження доставки та повторної передачі втрачених пакетів. Інші, такі як **OSPF** та **IS-IS**, функціонують безпосередньо поверх протоколу IP, реалізуючи власні складні та надійні механізми розповсюдження інформації (**flooding**) та підтвердження отримання **LSA/LSP** кожним маршрутизатором. **BGP**, як вже зазначалося, для встановлення та підтримки сесій між пірами використовує протокол **TCP**, який за своєю природою забезпечує гарантовану доставку та збереження послідовності переданих повідомлень.

2.2. Алгоритмічні основи дистанційно-векторних протоколів маршрутизації

Дистанційно-векторні протоколи є одним з фундаментальних типів протоколів, що використовуються для визначення шляхів у комп'ютерних мережах. Їхня назва відображає ключовий принцип роботи: кожен маршрутизатор приймає рішення на основі "відстані" (метрики, наприклад, кількості переходів) до цільової мережі та "напрямку" або "вектора" (через якого сусіда або який інтерфейс ця мережа досяжна). Уявіть собі систему дорожніх знаків, де кожен знак показує відстань до певного міста і напрямок до наступного перехрестя на шляху до нього. Головна ідея дистанційно-векторних протоколів полягає в тому, що маршрутизатори не мають повної карти всієї мережі. Натомість, кожен маршрутизатор знає лише про своїх безпосередньо підключених сусідів. Він обмінюється з ними інформацією про те, які мережі він може досягти і яка "вартість" цього досягнення. Цей процес часто порівнюють із поширенням чуток: маршрутизатор А каже маршрутизатору Б, що він знає шлях до мережі Х. Маршрутизатор Б, довіряючи А, додає до вартості шляху від А до Х вартість шляху від себе до А, і повідомляє цю інформацію своєму сусідові В, і так далі.

Маршрутизатори, що працюють за дистанційно-векторним принципом, періодично (наприклад, кожні 30 секунд) надсилають своїм сусідам копії своїх таблиць маршрутизації або, принаймні, інформацію про відомі їм шляхи. Ця інформація включає список мереж та метрику (вартість) для досягнення кожної з них. Коли маршрутизатор отримує таку інформацію від сусіда, він аналізує її: якщо сусід повідомляє про мережу, якої ще немає в таблиці поточного маршрутизатора, цей новий маршрут додається; якщо сусід повідомляє про шлях до вже відомої мережі, але з кращою (меншою) метрикою, ніж поточний шлях, то маршрутизатор оновлює свою таблицю, обираючи новий, ефективніший шлях; якщо інформація надходить від сусіда, який вже є "наступним кроком" для певного маршруту, це просто підтверджує актуальність цього маршруту. Таким чином, поступово, шляхом обміну інформацією між сусідами, кожен маршрутизатор будує свою власну картину доступних мереж та найкращих шляхів до них.

Основною складністю дистанційно-векторних протоколів є забезпечення того, щоб усі маршрутизатори в мережі мали узгоджену та актуальну інформацію, особливо коли в мережі відбуваються зміни, такі як вихід з ладу каналу зв'язку або маршрутизатора. Процес, за допомогою якого всі маршрутизатори досягають узгодженого розуміння топології, називається конвергенцією. У дистанційно-векторних протоколах конвергенція може бути відносно повільною, особливо при поширенні "поганих новин" (інформації про недоступність мережі). Однією з найвідоміших проблем є "рахунок до нескінченності". Це класична проблема, коли через неправильне поширення інформації маршрутизатори можуть утворити петлю. Наприклад, маршрутизатор А втрачає зв'язок з мережею Х, але маршрутизатор Б, який раніше дізнався про Х від А, ще не знає про проблему. Якщо Б, в свою чергу, повідомить А, що він має шлях до Х (хоча насправді цей шлях йшов через А), А може помилково подумати, що знайшовся альтернативний шлях через Б. В результаті вони почнуть вказувати один на одного як на шлях до Х, а метрика буде безкінечно зростати, поки не досягне максимального встановленого значення.

Для вирішення цієї та інших проблем, пов'язаних з конвергенцією та утворенням петель, було розроблено спеціальні алгоритмічні механізми. Перший з них – обмеження максимальної метрики, також відоме як "визначення нескінченності". Протокол встановлює максимальне значення метрики (наприклад, 15 переходів для RIP). Якщо метрика до мережі досягає цього значення (або 16, що у випадку RIP означає недосяжність), маршрут вважається недійсним. Це допомагає розірвати петлі "рахунку до нескінченності", хоча й не миттєво, та обмежує максимальний розмір мережі, яку може обслуговувати протокол.

Другий важливий механізм – розщеплення горизонту (**Split Horizon**). Його суть полягає в тому, що маршрутизатор не повинен надсилати інформацію про маршрут назад на той інтерфейс, з якого він цю інформацію отримав. Якщо маршрутизатор Б дізнався про мережу Х від маршрутизатора А, то Б не буде повідомляти А, що він знає шлях до Х. Це ефективно запобігає утворенню петель між двома сусідніми маршрутизаторами, які є найпростішим типом петель.

Третій механізм – отруєння маршруту (**Route Poisoning**). Коли маршрут стає недоступним, маршрутизатор не просто перестає його анонсувати, а починає активно повідомляти сусідам, що цей маршрут недосяжний, встановлюючи для нього метрику "нескінченність". Це явно і швидко інформує сусідні маршрутизатори про непрацездатність маршруту, прискорюючи процес вилучення недійсних шляхів з таблиць маршрутизації по всій мережі. Існує також отруєння у відповідь (Poison Reverse), яке є більш агресивною формою розщеплення горизонту. Маршрутизатор не просто не надсилає інформацію про маршрут назад, а надсилає її з метрикою "нескінченність", що ще рішучіше бореться з можливими петлями, хоча й може збільшити обсяг службового трафіку.

Четвертим механізмом є тригерні оновлення (**Triggered Updates**), іноді звані миттєвими оновленнями (flash updates). Замість того, щоб чекати на чергове періодичне оновлення (наприклад, кожні 30 секунд), маршрутизатор надсилає спеціальне оновлення негайно, як тільки виявляє зміну в топології мережі, наприклад, обрив зв'язку або появу нового маршруту. Такі оновлення часто містять інформацію лише про змінені маршрути, що зменшує їх розмір. Це значно прискорює конвергенцію мережі, оскільки інформація про зміни поширюється швидше.

П'ятий механізм – таймери утримання (**Hold-down Timers**). Після отримання інформації про те, що раніше доступний маршрут став недоступним або його метрика значно погіршилася, маршрутизатор може на певний час "заморозити" цей маршрут і не приймати нових, потенційно суперечливих, оновлень щодо нього, особливо якщо ці оновлення пропонують шлях з гіршою або такою ж метрикою. Це дає час "поганим новинам" про недоступність маршруту поширитися по всій мережі, перш ніж буде прийнято рішення про альтернативний шлях. Такий підхід допомагає уникнути повернення до нестабільних маршрутів та коливань у таблицях маршрутизації, хоча в деяких випадках може незначно уповільнити встановлення нового, дійсного шляху.

Підсумовуючи, дистанційно-векторні протоколи базуються на простому принципі обміну інформацією про відстані та напрямки між безпосередніми сусідами. Хоча цей підхід інтуїтивно зрозумілий і не вимагає значних обчислювальних ресурсів від маршрутизаторів, він має свої вроджені недоліки, пов'язані з швидкістю конвергенції, особливо при виявленні несправностей, та ризиком утворення тимчасових петель маршрутизації. Для подолання цих недоліків використовуються спеціальні алгоритмічні вдосконалення, такі як розщеплення горизонту, отруєння маршруту та тригерні оновлення. Розуміння цих механізмів є важливим для оцінки придатності таких протоколів для конкретних мережевих завдань, особливо в порівнянні з більш сучасними та складними протоколами, такими як протоколи стану каналу. Для невеликих, стабільних мереж простота налаштування та низькі вимоги до ресурсів можуть все ще робити дистанційно-векторні протоколи прийнятним вибором.

2.3. Алгоритмічні основи протоколів маршрутизації на основі стану каналу

Протоколи маршрутизації на основі стану каналу (**Link-State Routing Protocols**) представляють фундаментально інший підхід до визначення оптимальних шляхів у мережі порівняно з дистанційно-векторними протоколами. Ключова відмінність полягає в тому, що кожен маршрутизатор, який використовує протокол стану каналу, прагне побудувати повну та ідентичну карту топології мережі (або її визначеної області). Маючи таку всеосяжну "карту", кожен маршрутизатор самостійно обчислює найкоротші шляхи до всіх інших вузлів, використовуючи стандартизований алгоритм. Цей підхід забезпечує швидшу конвергенцію та вищу стійкість до утворення петель маршрутизації, що робить його кращим вибором для великих та складних мережевих інфраструктур.

Теоретична база: Алгоритм Дейкстри (Dijkstra's Shortest Path First - SPF)

В основі обчислення шляхів у протоколах стану каналу лежить алгоритм Дейкстри, також відомий як алгоритм найкоротшого шляху (Shortest Path First - SPF). Цей алгоритм є класичним методом теорії графів для знаходження найкоротших шляхів від однієї стартової вершини до всіх інших вершин у зваженому орієнтованому або неорієнтованому графі з невід'ємними вагами ребер. У контексті мережевої маршрутизації:

- **Вершини графу** представляють маршрутизатори та, в деяких випадках, транзитні мережі.
- **Ребра графу** відповідають каналам зв'язку між маршрутизаторами або між маршрутизатором та мережею.
- **Ваги ребер** – це метрики (або "вартості"), асоційовані з кожним каналом. Ці метрики можуть базуватися на пропускній здатності, затримці або інших адміністративно визначених параметрах. Протоколи, такі як OSPF, зазвичай використовують вартість, обернено пропорційну пропускній здатності каналу.

Алгоритм Дейкстри ітеративно будує дерево найкоротших шляхів, починаючи з поточного маршрутизатора (кореня дерева). На кожному кроці алгоритм вибирає ще не оброблений вузол з найменшою сукупною вартістю шляху від кореня та додає його до дерева. Потім він оновлює вартості шляхів до сусідів новододаного вузла. Процес триває, поки всі доступні вузли не будуть включені до дерева SPF. Результатом роботи алгоритму є повний набір найкоротших шляхів від поточного

маршрутизатора до всіх інших вузлів у топології, на основі якого формується таблиця маршрутизації.

Фундаментальні процеси функціонування протоколів стану каналу

Робота протоколів стану каналу складається з декількох взаємопов'язаних процесів:

1. **Виявлення сусідів (Neighbor Discovery and Adjacency Formation):** Кожен маршрутизатор використовує спеціалізований механізм, такий як **Hello-протокол**, для виявлення безпосередньо підключених сусідів, на інтерфейсах яких активовано той самий протокол маршрутизації. Hello-пакети періодично розсилаються на відповідні інтерфейси. Для успішного встановлення сусідських відносин (adjacency) певні параметри в Hello-пакетах повинні збігатися між маршрутизаторами. Наприклад, для OSPF це включає ідентифікатор зони (Area ID), таймери інтервалів Hello та Dead, тип автентифікації та параметри автентифікації, а також, для деяких типів мереж, маску підмережі. Процес встановлення сусідства проходить через кілька станів (наприклад, в OSPF: Down, Init, 2-Way, ExStart, Exchange, Loading, Full), що забезпечує впорядкований обмін інформацією.

2. **Розповсюдження інформації про стан каналів (Link-State Advertisement Flooding):**
   Після встановлення сусідства маршрутизатори починають обмінюватися інформацією про стан своїх каналів. Ця інформація інкапсулюється в спеціальні пакети, відомі як **Link-State Advertisements (LSAs)** в OSPF або **Link-State Packets (LSPs)** в IS-IS. Кожен маршрутизатор генерує LSA/LSP, що описують його власні підключені інтерфейси, стан цих інтерфейсів (активний/неактивний), метрики відповідних каналів та ідентифікатори відомих сусідів на цих каналах. Розповсюдження LSA/LSP по всій мережі (або зоні) відбувається за допомогою механізму **надійного флудингу (reliable flooding)**. Коли маршрутизатор отримує нову або оновлену LSA/LSP, він зберігає її копію, надсилає підтвердження (LSAck) відправнику та пересилає цю LSA/LSP на всі свої інші інтерфейси (окрім того, з якого вона була отримана), забезпечуючи таким чином її поширення. Для запобігання нескінченному циркулюванню та розповсюдженню застарілої інформації використовуються:

   Порядкові номери (Sequence Numbers): Кожна LSA/LSP має порядковий номер, який збільшується при кожному оновленні. Маршрутизатори приймають лише LSA/LSP з більшим (новішим) порядковим номером.

   Контрольні суми (Checksums): Для перевірки цілісності LSA/LSP.

Механізм старіння (Aging): Кожна LSA/LSP має максимальний час життя (MaxAge). Якщо LSA/LSP не оновлюється протягом цього часу, вона вважається недійсною та видаляється. Також існує періодичне оновлення (LSRefreshTime) для підтримки активних LSA/LSP в базі даних.

3. **Побудова бази даних стану каналів (Link-State Database - LSDB)**: Кожен маршрутизатор збирає всі отримані та власно згенеровані LSA/LSP в локальну базу даних, яка називається Link-State Database (LSDB). Завдяки механізму флудингу, в ідеалі, всі маршрутизатори в межах однієї зони або рівня ієрархії мають абсолютно ідентичні копії LSDB. Ця база даних є репрезентацією поточної топології мережі. На етапі встановлення повного сусідства (adjacency), особливо після стану 2-Way, маршрутизатори обмінюються пакетами опису бази даних (Database Descriptor - DBD або DDP packets), які містять стислі заголовки LSA/LSP з їхніх LSDB. Це дозволяє їм ефективно синхронізувати свої бази даних, запитуючи лише ті LSA/LSP, яких не вистачає або які є новішими (Link State Request - LSR, Link State Update - LSU).
4. **Обчислення дерева найкоротших шляхів (SPF Tree Calculation)**: Маючи повну та синхронізовану LSDB, кожен маршрутизатор незалежно запускає алгоритм SPF (Дейкстри), використовуючи себе як кореневу вершину дерева. Результатом виконання алгоритму є дерево найкоротших шляхів до всіх інших маршрутизаторів та мереж, описаних в LSDB. На основі цього дерева найкоротших шляхів безпосередньо формується таблиця маршрутизації (Routing Information Base - RIB), де для кожної досяжної мережі вказується метрика та наступний перехід (next-hop). Оскільки всі маршрутизатори в зоні працюють з ідентичними LSDB та використовують однаковий алгоритм SPF, обчислені шляхи є узгодженими, що виключає можливість утворення петель маршрутизації на рівні протоколу в межах однієї зони. Алгоритм SPF запускається щоразу, коли відбувається зміна в топології, що відображається в отриманні нової або зміненої LSA/LSP, яка модифікує LSDB.

Ієрархічна маршрутизація та масштабованість

Для забезпечення масштабованості у великих мережах протоколи стану каналу, такі як OSPF, підтримують концепцію ієрархічної маршрутизації шляхом поділу автономної системи на менші логічні одиниці, що називаються зонами (Areas).

- **Зменшення LSDB**: Кожен маршрутизатор підтримує повну LSDB лише для своєї зони. Інформація про маршрути до інших зон передається в агрегованому (резюмованому) вигляді спеціальними граничними маршрутизаторами (Area Border Routers - ABRs).
- **Обмеження флудингу LSA**: Більшість типів LSA (наприклад, Router LSA та Network LSA в OSPF) не поширюються за межі своєї зони.
- **Зменшення частоти SPF-обчислень**: Зміни топології в одній зоні не завжди вимагають перерахунку SPF в інших зонах. OSPF визначає спеціальну **магістральну зону (Backbone Area / Area 0)**, до якої повинні бути підключені всі інші зони (безпосередньо або через віртуальні канали). Маршрутизатори класифікуються за їх роллю: внутрішні маршрутизатори зони, ABR, магістральні маршрутизатори, ASBR (Autonomous System Boundary Router – для зв'язку з іншими автономними системами). Різні типи LSA (наприклад, Type 1-5, 7 в OSPF) слугують для передачі різної топологічної інформації всередині зон, між зонами та від зовнішніх систем.

Вибори DR/BDR в мережах з множинним доступом

У сегментах мережі з множинним доступом (наприклад, Ethernet), де багато маршрутизаторів підключені до спільного середовища, встановлення повного сусідства між усіма парами маршрутизаторів (full mesh adjacency) призвело б до надмірної кількості LSA та неефективного використання ресурсів. Для оптимізації цього процесу обираються **Designated Router (DR)** та **Backup Designated Router (BDR)**. Всі інші маршрутизатори в сегменті (DROther) встановлюють повне сусідство лише з DR та BDR. DR відповідає за генерацію Network LSA (Type 2 LSA в OSPF), яка представляє цей сегмент мережі та всі підключені до нього маршрутизатори. Вибори DR/BDR відбуваються на основі адміністративно налаштованого пріоритету маршрутизатора (Router Priority) та, у випадку рівних пріоритетів, за найбільшим Router ID.

Переваги та недоліки алгоритмічного підходу стану каналу

Переваги:

1. **Швидка конвергенція**: Завдяки тому, що зміни топології швидко розповсюджуються через флудинг LSA/LSP, і кожен маршрутизатор самостійно перераховує шляхи.

2. **Стійкість до петель маршрутизації**: Оскільки кожен маршрутизатор має повну та узгоджену карту топології (в межах зони/рівня), ймовірність утворення петель мінімальна.
3. **Масштабованість**: Ієрархічна структура дозволяє ефективно використовувати протокол у великих мережах.
4. **Підтримка VLSM та CIDR**: Сучасні протоколи стану каналу повністю підтримують безкласову адресацію.

Недоліки:

1. **Вищі вимоги до ресурсів**: Зберігання LSDB вимагає більше пам'яті, а часті обчислення SPF – більше ресурсів CPU порівняно з дистанційно-векторними протоколами, особливо у великих, "плоских" (неієрархічних) топологіях.
2. **Складність**: Концептуально та в налаштуванні протоколи стану каналу є складнішими, ніж дистанційно-векторні.

На завершення, алгоритмічні основи протоколів маршрутизації на основі стану каналу забезпечують надійний та ефективний механізм для побудови конвергентних та безпетлевих мережевих топологій. Розуміння процесів виявлення сусідів, розповсюдження LSA/LSP, побудови LSDB та роботи алгоритму SPF є критично важливим для проектування, впровадження та адміністрування сучасних комп'ютерних мереж.

2.4. Алгоритмічні основи гібридних (збалансованих) протоколів маршрутизації

Гібридні протоколи маршрутизації, також відомі як вдосконалені або збалансовані дистанційно-векторні протоколи, були розроблені з метою поєднати найкращі риси двох основних класів протоколів: простоту та ефективність використання ресурсів дистанційно-векторних підходів із швидкістю конвергенції та стійкістю до петель, характерними для протоколів на основі стану каналу. Вони прагнуть уникнути основних недоліків традиційних дистанційно-векторних алгоритмів, таких як повільна конвергенція та проблема "рахунку до нескінченності", шляхом впровадження більш складних алгоритмів обчислення шляхів та механізмів обміну інформацією.

Ключові алгоритмічні концепції гібридного підходу:

1. **Обмін інформацією з сусідами та підтримка топологічних даних:** Як і дистанційно-векторні протоколи, гібридні протоколи встановлюють сусідські відносини та обмінюються маршрутною інформацією безпосередньо з підключеними сусідами. Однак, на відміну від класичного підходу, де передається вся таблиця маршрутизації, гібридні протоколи часто передають лише зміни в топології (часткові оновлення) і лише тим сусідам, яких ці зміни стосуються (обмежені оновлення). Це значно зменшує обсяг службового трафіку. Маршрутизатори можуть підтримувати локальну базу даних топології, яка містить інформацію, отриману від сусідів, що виходить за рамки простої таблиці маршрутизації.
2. **Гарантоване уникнення петель через координацію:** Центральним елементом багатьох гібридних протоколів є алгоритми, що забезпечують гарантоване уникнення петель маршрутизації без необхідності побудови повної карти мережі кожним маршрутизатором. Це досягається шляхом синхронізованих обчислень та використання спеціальних умов при виборі шляхів. Наприклад, алгоритм може вимагати, щоб альтернативний шлях, запропонований сусідом, задовольняв певній умові, яка гарантує, що цей сусід знаходиться "ближче" до цільової мережі, ніж поточний маршрутизатор через його основний шлях. Це запобігає вибору шляхів, які могли б призвести до повернення трафіку назад.
3. **Використання резервних шляхів для швидкої конвергенції:** Гібридні протоколи часто передбачають проактивне обчислення та зберігання інформації про потенційні резервні шляхи. Якщо основний шлях до цільової мережі стає недоступним, маршрутизатор може миттєво

переключитися на заздалегідь визначений резервний шлях, що задовольняє умовам безпетлевості, без необхідності запускати тривалий процес пошуку нового шляху через запити до всіх сусідів. Ця можливість забезпечує надзвичайно швидку конвергенцію.

4. **Механізм запитів у разі відсутності очевидних резервних шляхів:** У ситуаціях, коли після відмови основного шляху немає негайно доступного та гарантовано безпетлевого резервного шляху, гібридні протоколи можуть ініціювати процес активного пошуку нового шляху. Це може включати розсилку спеціальних запитів (queries) сусідам. Однак, на відміну від простого "рахунку до нескінченності", цей процес є більш контрольованим і координованим, часто обмежуючи область поширення запитів, щоб мінімізувати вплив на мережу.
5. **Використання складних (композитних) метрик:** На відміну від простої метрики "кількість хопів", яку використовують деякі дистанційно-векторні протоколи, гібридні протоколи часто дозволяють використовувати більш складні, композитні метрики. Такі метрики можуть враховувати різноманітні характеристики каналів, такі як пропускна здатність, затримка, надійність та завантаження. Це дозволяє більш точно оцінювати якість шляхів та обирати маршрути, що краще відповідають вимогам додатків.
6. **Надійний механізм транспортування оновлень:** Для критично важливої маршрутної інформації (оновлення, запити, відповіді) гібридні протоколи можуть використовувати власні надійні транспортні механізми, що забезпечують гарантовану доставку та правильний порядок пакетів між сусідами.

Загальні переваги та потенційні складності гібридного підходу:

- **Переваги:**
    - Значно швидша конвергенція порівняно з традиційними дистанційно-векторними протоколами.
    - Ефективне використання мережевих ресурсів завдяки частковим та обмеженим оновленням.
    - Висока стійкість до утворення петель маршрутизації.
    - Можливість використання більш гнучких та інформативних метрик.
- **Потенційні складності:**
    - Алгоритми, що лежать в основі гібридних протоколів, можуть бути досить складними для розуміння та аналізу.

- У деяких сценаріях, особливо у великих та нестабільних мережах, координація між маршрутизаторами під час пошуку нових шляхів може вимагати значних обчислювальних ресурсів або призводити до затримок, якщо мережа спроектована неоптимально.
- Історично, деякі реалізації гібридних протоколів були пропрієтарними, що обмежувало їх використання в мультивендорних середовищах.

Підсумовуючи, алгоритмічні основи гібридних протоколів маршрутизації являють собою значний крок вперед порівняно з класичними дистанційно-векторними підходами. Вони пропонують збалансоване рішення, яке прагне забезпечити високу продуктивність та надійність, характерні для протоколів стану каналу, при цьому зберігаючи деякі переваги ефективності, властиві дистанційно-векторним методам. Розуміння цих фундаментальних концепцій є важливим для оцінки їхньої ролі в побудові сучасних комп'ютерних мереж.

3. Аналіз застосування динамічних протоколів маршрутизації в системах для підвищення та забезпечення надійності мережі

3.1 Аналіз використання дистанційно-векторних протоколів маршрутизації

Дистанційно-векторний підхід до маршрутизації базується на принципі, згідно з яким кожен маршрутизатор визначає найкращий шлях до кожної досяжної в мережі цілі (мережі призначення) на основі двох ключових параметрів: напрямку (вектора), що вказує на наступний маршрутизатор на шляху, та відстані (метрики), що кількісно характеризує "вартість" цього шляху. Фундаментальним механізмом функціонування таких протоколів є періодичний обмін маршрутною інформацією між безпосередньо підключеними маршрутизаторами (сусідами). Як правило, кожні 30 секунд (цей інтервал може варіюватися залежно від конкретного протоколу) маршрутизатор надсилає всю або частину своєї таблиці маршрутизації своїм сусідам. Важливою особливістю є те, що ці періодичні оновлення розсилаються навіть за відсутності будь-яких змін у топології мережі, що, хоча й забезпечує певну підтримку актуальності шляхів, є неефективним з точки зору використання мережевих ресурсів.

Отримавши таблицю маршрутизації від сусіда, маршрутизатор аналізує її зміст. Він порівнює запропоновані сусідом шляхи з тими, що вже наявні у власній таблиці маршрутизації. Якщо для певної цільової мережі отриманий шлях має кращу (меншу) метрику, або якщо це шлях до нової, раніше невідомої мережі, маршрутизатор оновлює свою таблицю відповідним чином. Цей ітеративний процес поширення інформації часто характеризують як "маршрутизацію за чутками" (routing by rumor), оскільки знання кожного маршрутизатора про загальну топологію мережі обмежені й формуються виключно на основі інформації, наданої його безпосередніми сусідами, які, в свою чергу, покладаються на своїх сусідів.

Математичною основою для більшості дистанційно-векторних протоколів слугує алгоритм Беллмана-Форда або його модифікації. Цей алгоритм дозволяє обчислювати найкоротші шляхи в графі з можливими від'ємними вагами ребер (хоча в контексті маршрутизації метрики зазвичай невід'ємні), що робить його придатним для розподілених обчислень, де кожен вузол має лише локальну інформацію.

3.2 Протокол RIP

Протокол маршрутної інформації (RIP) є одним із найстаріших і найпростіших дистанційно-векторних протоколів внутрішньої маршрутизації (IGP), визначених у стандартах Інтернету. Він був розроблений на основі алгоритмів, що використовувалися в Xerox Network Systems (**XNS**). Незважаючи на появу більш досконалих протоколів, RIP все ще іноді використовується в невеликих, простих мережах завдяки своїй легкості налаштування та невибагливості до ресурсів.

Принцип роботи та ключові характеристики:

RIP використовує класичний дистанційно-векторний алгоритм, заснований на алгоритмі Беллмана-Форда. Його основні характеристики такі:

1. Метрика – кількість переходів (**Hop Count**): RIP використовує кількість маршрутизаторів (хопів), які необхідно пройти для досягнення цільової мережі, як єдину метрику для вибору найкращого шляху. Шлях з меншою кількістю хопів вважається кращим. Максимально допустима кількість хопів – 15. Значення 16 означає, що мережа недосяжна (нескінченність). Це обмежує максимальний діаметр мережі, в якій може використовуватися RIP.
2. Періодичні оновлення: Маршрутизатори, що використовують RIP, розсилають повні копії своїх таблиць маршрутизації своїм безпосередньо підключеним сусідам кожні 30 секунд (за замовчуванням). Ці оновлення надсилаються незалежно від того, чи відбулися зміни в топології мережі.
3. Механізми запобігання петлям та прискорення конвергенції: Для боротьби з проблемами, властивими дистанційно-векторним алгоритмам (зокрема, "рахунком до нескінченності" та повільною конвергенцією), RIP використовує кілька механізмів:
    - Обмеження максимальної кількості хопів: Як зазначено, 15 хопів.
    - Розщеплення горизонту: Маршрутизатор не надсилає інформацію про маршрут назад на той інтерфейс, з якого ця інформація була отримана.
    - Отруєння маршруту: Коли маршрут стає недосяжним, маршрутизатор починає анонсувати його з метрикою 16 (нескінченність), щоб швидко повідомити сусідів про недійсність шляху.
    - Отруєння у відповідь (Poison Reverse): Посилена версія розщеплення горизонту, де маршрутизатор анонсує маршрути назад на інтерфейс, з якого вони були отримані, але з метрикою 16.

- Тригерні оновлення): При виявленні зміни в топології (наприклад, відмова каналу або зміна метрики), маршрутизатор негайно надсилає оновлення, не чекаючи закінчення 30-секундного таймера. Це допомагає прискорити поширення інформації про зміни.
- Таймери утримання: Після отримання інформації про те, що маршрут став недосяжним або його метрика погіршилася, маршрутизатор може активувати таймер утримання (зазвичай 180 секунд). Протягом цього часу маршрутизатор не прийматиме нових оновлень для цього маршруту з такою ж або гіршою метрикою, щоб дати час інформації про проблему поширитися.

4. Таймери: RIP використовує кілька таймерів для своєї роботи:
   - Update Timer (Таймер оновлень): 30 секунд – інтервал між розсиланням регулярних оновлень.
   - Invalid Timer (Таймер недійсності): 180 секунд – якщо протягом цього часу не надходить оновлення для певного маршруту, він позначається як недійсний (метрика встановлюється в 16).
   - Flush Timer (Таймер очищення): 240 секунд – якщо протягом цього часу не надходить оновлення для недійсного маршруту, він видаляється з таблиці маршрутизації.
   - Hold-down Timer (Таймер утримання): Зазвичай 180 секунд (не завжди ввімкнений за замовчуванням у всіх реалізаціях).

Версії протоколу RIP:

Існує три основні версії протоколу RIP:

- **RIPv1** (**Routing Information Protocol version 1**):
  - Визначений у RFC 1058.
  - Класовий протокол: Не підтримує маски підмереж змінної довжини (**VLSM**) та безкласову міждоменну маршрутизацію (**CIDR**). Він передбачає, що всі пристрої в одній мережі використовують однакову маску підмережі.
  - Широкомовні оновлення: Надсилає маршрутні оновлення на широкомовну IP-адресу 255.255.255.255.
  - Відсутність автентифікації: Не підтримує жодних механізмів автентифікації, що робить його вразливим до підробки маршрутів.
- **RIPv2** (Routing Information Protocol version 2):
  - Визначений у RFC 2453.

- Безкласовий протокол: Підтримує VLSM та CIDR, оскільки передає інформацію про маску підмережі разом з адресою мережі в маршрутних оновленнях.
- Багатоадресні (мультикаст) оновлення: Надсилає маршрутні оновлення на багатоадресну IP-адресу 224.0.0.9, що зменшує навантаження на хости, які не є маршрутизаторами.
- Підтримка автентифікації: Підтримує автентифікацію маршрутних оновлень, використовуючи простий текстовий пароль або MD5-хешування, що підвищує безпеку.
- Використовує поле "Next Hop" для вказівки кращого наступного маршрутизатора, якщо він знаходиться в тій же підмережі, що й отримувач оновлення.

- **RIPng** (RIP next generation):
  - Визначений у RFC 2080.
  - Призначений для використання в мережах IPv6.
  - Зберігає більшість характеристик RIPv2, включаючи використання кількості хопів як метрики, обмеження в 15 хопів та механізми запобігання петлям.
  - Використовує багатоадресну IPv6-адресу FF02::9 для розсилання оновлень.
  - Використовує розширення заголовків IPv6 для автентифікації (IPsec).

Переваги (Плюси) RIP:

1. Простота налаштування та адміністрування: RIP є одним з найпростіших протоколів маршрутизації для конфігурації та розуміння, що робить його привабливим для невеликих мереж або для навчальних цілей.
2. Низькі вимоги до ресурсів: Не потребує значних обчислювальних потужностей CPU або великих обсягів пам'яті на маршрутизаторах порівняно з більш складними протоколами, такими як OSPF або EIGRP.
3. Широка підтримка: Як один з найстаріших стандартів, RIP підтримується практично всіма виробниками мережевого обладнання.
4. Швидке початкове розгортання: Завдяки простоті, мережу з RIP можна швидко запустити в роботу.

Недоліки (Мінуси) RIP:

1. Повільна конвергенція: Час, необхідний для того, щоб всі маршрутизатори в мережі узгодили зміни в топології, може бути значним (хвилини), особливо у великих мережах. Це пов'язано з періодичними оновленнями та механізмами таймерів (зокрема, Hold-down).
2. Обмежена масштабованість: Максимальна кількість хопів у 15 обмежує розмір мережі, де може ефективно використовуватися RIP. Він не підходить для великих корпоративних або провайдерських мереж.
3. Використання кількості хопів як єдиної метрики: Ця метрика не враховує важливі характеристики каналів, такі як пропускна здатність, затримка або надійність. В результаті RIP може обрати шлях з меншою кількістю хопів, але з низькою пропускною здатністю, замість шляху з більшою кількістю хопів, але значно вищою пропускною здатністю.
4. Великий обсяг службового трафіку: Періодичне розсилання повних таблиць маршрутизації кожні 30 секунд створює значне навантаження на мережу, особливо на низькошвидкісних каналах, навіть якщо змін у топології не було.
5. Проблема "рахунку до нескінченності": Хоча існують механізми для боротьби з цією проблемою, вони не завжди запобігають їй повністю або можуть уповільнювати конвергенцію.
6. Відсутність підтримки VLSM/CIDR у RIPv1: Це робить RIPv1 непридатним для сучасних мереж, де ефективне використання адресного простору є критичним.
7. Обмежені можливості безпеки (особливо в RIPv1): RIPv1 не має автентифікації, що робить його вразливим. RIPv2 пропонує автентифікацію, але вона не завжди є достатньо надійною порівняно з механізмами безпеки в новіших протоколах.

Незважаючи на свої недоліки, RIP (особливо RIPv2 та RIPng) все ще може знайти застосування в дуже специфічних сценаріях: невеликі, статичні мережі, де простота та мінімальні вимоги до ресурсів є пріоритетом, а швидкість конвергенції та масштабованість не є критичними факторами. Однак для більшості сучасних мережевих інфраструктур, що вимагають високої надійності, швидкодії та масштабованості, перевага надається більш досконалим протоколам, таким як OSPF або EIGRP. Розуміння принципів роботи та обмежень RIP є важливим для мережевих фахівців, оскільки це допомагає оцінити його придатність для конкретних завдань та зрозуміти еволюцію протоколів маршрутизації.

3.3 Протокол IGRP

Протокол маршрутизації внутрішнього шлюзу (IGRP) – це дистанційно-векторний протокол внутрішньої маршрутизації (IGP), розроблений компанією Cisco Systems в середині 1980-х років. Він був створений як відповідь на обмеження протоколу RIP, зокрема, його обмеження на 15 хопів та використання кількості переходів як єдиної метрики, що робило RIP непридатним для великих та складних мереж. IGRP був пропрієтарним протоколом Cisco і мав на меті забезпечити більш надійну та гнучку маршрутизацію в корпоративних мережах. Зараз IGRP вважається застарілим і був витіснений своїм наступником – EIGRP, а також відкритими стандартами, такими як OSPF.

Принцип роботи та ключові характеристики:

IGRP, як і RIP, базується на дистанційно-векторному алгоритмі, але впроваджує кілька значних вдосконалень:

1. Композитна метрика: Однією з ключових відмінностей IGRP є використання складної (композитної) метрики для оцінки шляхів. За замовчуванням метрика IGRP розраховується на основі:
    - **Пропускна здатність**: Найменша пропускна здатність каналу на всьому шляху до цільової мережі (в кілобітах на секунду).
    - **Затримка**: Сумарна затримка на всіх каналах шляху до цільової мережі (в десятках мікросекунд). Додатково, хоча й не використовуються за замовчуванням у формулі, метрика може враховувати:
    - **Надійність**: Оцінка надійності каналу (від 1 до 255, де 255 – найнадійніший).
    - **Завантаження**: Поточне завантаження каналу (від 1 до 255, де 1 – найменш завантажений).
    - **MTU (Maximum Transmission Unit)**: Найменший MTU на шляху (не використовується безпосередньо в обчисленні метрики, але передається в оновленнях).
2. Періодичні оновлення: IGRP надсилає повні таблиці маршрутизації своїм сусідам кожні 90 секунд (за замовчуванням), що є довшим інтервалом порівняно з 30 секундами у RIP.

3. Максимальна кількість хопів: За замовчуванням максимальна кількість хопів для IGRP становить 100, але може бути налаштована до 255. Це значно більше, ніж 15 хопів у RIP, що дозволяє будувати більші мережі.
4. Механізми запобігання петлям та стабілізації: IGRP використовує ті ж самі базові механізми, що й RIP, для боротьби з проблемами дистанційно-векторних алгоритмів:
    - Розщеплення горизонту (Split Horizon).
    - Отруєння маршруту (Route Poisoning).
    - Отруєння у відповідь (Poison Reverse).
    - Тригерні оновлення (Triggered Updates): Надсилаються при зміні метрики маршруту, щоб прискорити конвергенцію.
    - Таймери утримання (Hold-down Timers): Запобігають прийняттю потенційно некоректної інформації про маршрут протягом певного часу після того, як він став недоступним.
5. Таймери: IGRP використовує набір таймерів, схожих на RIP, але з іншими значеннями за замовчуванням:
    - Update Timer: 90 секунд.
    - Invalid Timer: 270 секунд (3 * Update Timer). Маршрут позначається як недійсний, якщо оновлення не надходить протягом цього часу.
    - Hold-down Timer: 280 секунд (Invalid Timer + 10 секунд).
    - Flush Timer: 630 секунд (7 * Update Timer). Маршрут видаляється з таблиці, якщо оновлення не надходить протягом цього часу.
6. Нерівномірне балансування навантаження (Unequal Cost Load Balancing): IGRP підтримує можливість балансування навантаження між декількома шляхами до однієї цільової мережі, навіть якщо ці шляхи мають різну метрику (нерівну вартість). Це досягається за допомогою команди variance. Маршрутизатор може використовувати до 4 шляхів за замовчуванням (максимум до 6) для балансування, якщо їхня метрика не перевищує метрику найкращого шляху, помножену на коефіцієнт variance.

Переваги IGRP:

1. Використання композитної метрики: Дозволяло приймати більш обґрунтовані рішення щодо вибору шляху, враховуючи пропускну здатність та затримку, на відміну від простої кількості хопів у RIP.
2. Більша максимальна кількість хопів: Дозволяло будувати значно більші мережі порівняно з RIP.

3. Підтримка нерівномірного балансування навантаження: Надавало гнучкість у використанні доступних каналів зв'язку, навіть якщо вони мали різні характеристики.
4. Відносна простота налаштування: Хоча складніший за RIP, IGRP все ж був простішим у конфігурації порівняно з протоколами стану каналу, такими як OSPF, на той час.

Недоліки IGRP:

1. Пропрієтарність Cisco: Будучи власністю Cisco, IGRP міг використовуватися лише на обладнанні цієї компанії, що обмежувало його застосування в мультивендорних середовищах.
2. Класовий протокол: IGRP не підтримував маски підмереж змінної довжини (VLSM) та безкласову міждоменну маршрутизацію (CIDR). Це призводило до неефективного використання адресного простору IP та обмежувало гнучкість проектування мережі, особливо з огляду на зростаючий дефіцит IPv4-адрес.
3. Повільна конвергенція: Незважаючи на вдосконалення порівняно з RIP, IGRP все ще залишався дистанційно-векторним протоколом і страждав від відносно повільної конвергенції, особливо у великих та складних топологіях. Час оновлення у 90 секунд та тривалі таймери утримання сприяли цьому.
4. Великий обсяг періодичних оновлень: Як і RIP, IGRP розсилав повні таблиці маршрутизації, що створювало значне навантаження на мережу, особливо на повільних каналах.
5. Відсутність автентифікації: IGRP не мав вбудованих механізмів автентифікації маршрутних оновлень, що робило його вразливим до атак, пов'язаних з підробкою маршрутної інформації.
6. Застарілість: IGRP був повністю витіснений своїм значно досконалішим наступником EIGRP (який є безкласовим, має швидшу конвергенцію та інші переваги), а також відкритими стандартними протоколами. Cisco офіційно припинила підтримку IGRP в IOS версії 12.2(8)T та пізніших.

IGRP відіграв важливу роль у свій час, надавши мережевим адміністраторам більш потужний інструмент для маршрутизації у великих мережах, ніж RIP. Його композитна метрика та підтримка більшої кількості хопів були значними перевагами. Однак його класова природа, пропрієтарність та відносно повільна конвергенція призвели до того, що він став застарілим з появою більш ефективних та гнучких протоколів. Вивчення IGRP сьогодні має переважно історичний інтерес,

допомагаючи зрозуміти еволюцію технологій маршрутизації та передумови для розробки EIGRP.

3.4 Протокол EIGRP

Розширений протокол маршрутизації внутрішнього шлюзу (EIGRP) – це вдосконалений дистанційно-векторний (часто класифікований як гібридний) протокол внутрішньої маршрутизації (IGP), розроблений компанією Cisco Systems. Він є наступником IGRP і був створений для усунення багатьох його недоліків, таких як класова природа, повільна конвергенція та обмежені можливості масштабування. EIGRP поєднує переваги дистанційно-векторних протоколів (простота адміністрування, ефективність використання ресурсів у стабільних мережах) з перевагами протоколів стану каналу (швидка конвергенція, стійкість до петель). Хоча спочатку EIGRP був повністю пропрієтарним протоколом Cisco, у 2013 році Cisco відкрила частину його функціональності як стандарт RFC (RFC 7868), що дозволило іншим виробникам реалізовувати його.

Принцип роботи та ключові характеристики:

EIGRP використовує **алгоритм DUAL (Diffusing Update Algorithm)**, який є серцем протоколу і забезпечує гарантоване уникнення петель та швидку конвергенцію.

1. **Алгоритм DUAL:**
    - **Successor:** Найкращий шлях до цільової мережі, який встановлюється в таблицю маршрутизації. Він визначається на основі найменшої **Feasible Distance (FD)** – обчисленої метрики від поточного маршрутизатора до цілі.
    - **Feasible Successor (FS):** Резервний шлях, що гарантовано не утворює петлю. FS визначається за допомогою **Feasibility Condition**: сусідній маршрутизатор може бути FS, якщо його **Reported Distance (RD)** (метрика, анонсована сусідом до цілі) є строго меншою, ніж FD поточного маршрутизатора до цієї ж цілі. Наявність FS дозволяє миттєво переключитися на резервний шлях у разі відмови основного Successor'a.
    - **Таблиця топології:** EIGRP підтримує таблицю топології, де зберігається інформація про всі шляхи (Successors та Feasible Successors) до всіх відомих цільових мереж.

- **Активний та пасивний стан:** Маршрут вважається в пасивному стані, коли є дійсний Successor. Якщо Successor втрачається і немає FS, маршрут переходить в активний стан, і DUAL ініціює процес запитів (Queries) до сусідів для пошуку нового шляху.

2. **Композитна метрика:** Як і IGRP, EIGRP використовує композитну метрику, яка за замовчуванням враховує:
   - **Пропускна здатність (Bandwidth):** Найменша пропускна здатність на шляху.
   - **Затримка (Delay):** Сумарна затримка на шляху. Опціонально можуть враховуватися **надійність (Reliability)** та **завантаження (Load)**. MTU також передається, але не використовується в розрахунку метрики. K-значення дозволяють адміністратору впливати на компоненти метрики. Формула схожа на IGRP, але значення метрики в EIGRP множаться на 256 порівняно з IGRP, що забезпечує більшу точність.
3. **Типи пакетів EIGRP:**
   - **Hello:** Використовуються для виявлення та підтримки сусідських відносин. Надсилаються як мультикаст-пакети на адресу 224.0.0.10.
   - **Update:** Містять маршрутну інформацію. Надсилаються як юнікаст або мультикаст при необхідності (наприклад, при встановленні нового сусідства або при зміні топології).
   - **Query:** Надсилаються, коли маршрутизатор втрачає шлях до цілі і не має Feasible Successor'a, запитуючи сусідів про альтернативні шляхи.
   - **Reply:** Надсилаються у відповідь на Query, повідомляючи про наявність (або відсутність) шляху.
   - **Acknowledgement (ACK):** Використовуються для підтвердження отримання пакетів Update, Query та Reply (надсилаються як юнікаст Hello-пакети).
4. **Надійний транспортний протокол (Reliable Transport Protocol, RTP):** EIGRP використовує власний протокол RTP для забезпечення гарантованої та впорядкованої доставки пакетів Update, Query та Reply. Hello та ACK пакети надсилаються негарантовано.
5. **Часткові та обмежені оновлення:** На відміну від RIP та IGRP, EIGRP не надсилає періодично повні таблиці маршрутизації. Оновлення надсилаються лише тоді, коли відбуваються зміни в топології (тригерні оновлення). Ці

оновлення є частковими (містять інформацію лише про змінені маршрути) та обмеженими (надсилаються лише тим сусідам, яких стосуються ці зміни).

6. **Безкласовий протокол:** EIGRP підтримує маски підмереж змінної довжини (VLSM) та безкласову міждоменну маршрутизацію (CIDR), що дозволяє ефективно використовувати адресний простір.
7. **Підтримка декількох мережевих протоколів:** EIGRP може маршрутизувати не тільки IPv4, але й IPX та AppleTalk (хоча підтримка останніх двох зараз є менш актуальною) за допомогою модулів, залежних від протоколу (Protocol-Dependent Modules, PDM). Для IPv6 існує окрема конфігурація EIGRP (EIGRP for IPv6).
8. **Автентифікація:** EIGRP підтримує MD5-автентифікацію маршрутних оновлень для підвищення безпеки.
9. **Резюмування маршрутів (Summarization):** EIGRP дозволяє агрегувати (резюмувати) маршрути на будь-якому інтерфейсі маршрутизатора, що допомагає зменшити розмір таблиць маршрутизації та обмежити поширення запитів (Query domain).
10. **Нерівномірне балансування навантаження (Unequal Cost Load Balancing):** Як і IGRP, EIGRP підтримує балансування навантаження по шляхах з різною вартістю за допомогою команди variance.

Переваги EIGRP:

1. **Дуже швидка конвергенція:** Завдяки алгоритму DUAL та наявності Feasible Successors, EIGRP може відновлювати зв'язок після відмови основного шляху практично миттєво, якщо є FS.
2. **Ефективне використання пропускної здатності:** Часткові та обмежені оновлення значно зменшують обсяг службового трафіку порівняно з протоколами, що надсилають повні періодичні оновлення.
3. **Гарантоване уникнення петель:** Алгоритм DUAL з його Feasibility Condition забезпечує побудову безпетлевих шляхів.
4. **Простота налаштування:** Для багатьох типових сценаріїв EIGRP налаштовується простіше, ніж OSPF, особливо в мережах Cisco.
5. **Гнучка метрика:** Композитна метрика дозволяє враховувати різні характеристики каналів, забезпечуючи більш оптимальний вибір шляху.
6. **Підтримка VLSM та CIDR:** Забезпечує ефективне використання адресного простору.

7. **Масштабованість:** Добре масштабується для середніх та великих мереж, особливо завдяки можливостям резюмування.
8. **Нерівномірне балансування навантаження:** Дозволяє ефективніше використовувати доступні канали.

Недоліки EIGRP:

1. **Історична пропрієтарність Cisco:** Хоча частина специфікацій EIGRP була відкрита, він все ще переважно асоціюється з обладнанням Cisco. Повна функціональність та оптимізації можуть бути доступні лише на пристроях Cisco, що може ускладнювати інтеграцію в мультивендорні середовища.
2. **Складність алгоритму DUAL:** Хоча DUAL ефективний, його внутрішня робота, особливо процес дифузійного обчислення (Query/Reply) при відсутності FS, може бути складною для розуміння та діагностики.
3. **Проблема "Stuck In Active" (SIA):** У великих, погано спроектованих або нестабільних мережах маршрутизатор може занадто довго перебувати в активному стані, чекаючи на відповіді (Reply) на свої запити (Query). Це може призвести до тимчасової втрати зв'язку. Хоча існують механізми для боротьби з SIA (Active timer, SIA-Query/SIA-Reply), проблема може виникати.
4. **Обмежене поширення за межі автономної системи:** EIGRP є протоколом IGP і не призначений для використання як EGP (Exterior Gateway Protocol) для маршрутизації між різними автономними системами в Інтернеті (для цього використовується BGP).

EIGRP є потужним та ефективним протоколом маршрутизації, який пропонує чудове поєднання швидкості конвергенції, ефективності використання ресурсів та відносної простоти адміністрування, особливо в мережах, побудованих переважно на обладнанні Cisco. Його здатність швидко реагувати на зміни в топології та гарантовано уникати петель робить його привабливим вибором для багатьох корпоративних мереж. Незважаючи на деякі складності, пов'язані з алгоритмом DUAL та історичною пропрієтарністю, EIGRP залишається популярним та широко використовуваним протоколом.

3.5 Протокол BGP

Протокол граничного шлюзу (BGP) є стандартизованим протоколом зовнішньої маршрутизації (Exterior Gateway Protocol, EGP), розробленим для обміну маршрутною інформацією та інформацією про досяжність мереж між різними автономними системами (AS) в Інтернеті. Автономна система – це сукупність IP-мереж та маршрутизаторів, що знаходяться під єдиним адміністративним керуванням та використовують спільну політику маршрутизації. BGP є ключовим протоколом, що забезпечує функціонування глобального Інтернету, дозволяючи різним інтернет-провайдерам (ISP), великим підприємствам та іншим організаціям обмінюватися інформацією про те, як досягти певних IP-префіксів. Поточна версія протоколу – BGP-4, визначена в RFC 4271**.**

Принцип роботи та ключові характеристики:

BGP є протоколом векторів шляху (Path Vector Protocol). Це означає, що при анонсуванні маршруту до цільового префіксу, BGP передає не тільки сам префікс, але й послідовність номерів автономних систем (AS_PATH), через які пройшов цей анонс. Це дозволяє виявляти та запобігати петлям маршрутизації на рівні AS.

1. **Типи BGP-сусідства (Peering)**:
    - **External BGP** (eBGP): Встановлюється між маршрутизаторами, що належать різним автономним системам. Зазвичай це граничні маршрутизатори ISP або великих організацій. TTL для eBGP-сесій за замовчуванням дорівнює 1 (вимагає прямого підключення або налаштування ebgp-multihop).
    - **Internal BGP** (iBGP): Встановлюється між маршрутизаторами всередині однієї автономної системи. iBGP використовується для розповсюдження зовнішніх маршрутів (отриманих через eBGP) всередині AS. Маршрутизатори iBGP-сусіди не обов'язково повинні бути безпосередньо підключені, і для запобігання петлям всередині AS iBGP має правило "не анонсувати маршрут, отриманий від одного iBGP-сусіда, іншому iBGP-сусідові" (вимагає повнозв'язної топології iBGP-сусідів або використання механізмів, таких як Route Reflectors або Confederations).
2. Атрибути шляху (Path Attributes): BGP використовує велику кількість атрибутів для опису маршрутів та прийняття рішень щодо вибору найкращого шляху. Атрибути діляться на кілька категорій:

- **Well-known mandatory** (Добре відомі обов'язкові): Повинні бути присутні у всіх BGP-оновленнях та розпізнаватися всіма BGP-реалізаціями (наприклад, AS_PATH, ORIGIN, NEXT_HOP).
- **Well-known discretionary** (Добре відомі необов'язкові): Повинні розпізнаватися всіма реалізаціями, але можуть бути відсутні в оновленнях (наприклад, LOCAL_PREF).
- **Optional transitive** (Опціональні транзитивні): Якщо реалізація не розпізнає цей атрибут, вона повинна передати його далі без змін (наприклад, AGGREGATOR, COMMUNITY).
- **Optional non-transitive** (Опціональні нетранзитивні): Якщо реалізація не розпізнає цей атрибут, вона повинна його видалити і не передавати далі (наприклад, MED – Multi-Exit Discriminator).

Ключові атрибути:

- **AS_PATH**: Список номерів AS, через які пройшов анонс маршруту. Використовується для запобігання петлям (маршрутизатор відкидає анонс, якщо бачить свій номер AS у списку) та як один з критеріїв вибору шляху (коротший AS_PATH зазвичай кращий).
- **NEXT_HOP**: IP-адреса наступного маршрутизатора на шляху до цільового префіксу. Для eBGP це зазвичай IP-адреса інтерфейсу сусіднього маршрутизатора. Для iBGP правила зміни NEXT_HOP складніші.
- **ORIGIN**: Вказує на джерело походження маршруту (IGP, EGP або Incomplete).
- **LOCAL_PREF** (Local Preference): Використовується всередині AS для вибору кращого вихідного шляху до зовнішньої мережі. Маршрут з більшим значенням LOCAL_PREF є кращим. Передається лише між iBGP-сусідами.
- **MED** (Multi-Exit Discriminator): Використовується для впливу на вибір вхідного шляху з боку сусідньої AS. Сусідня AS може враховувати MED для вибору точки входу у вашу AS (менше значення MED зазвичай краще).
- **COMMUNITY**: Теги, які можна присвоювати маршрутам для групування та застосування спільних політик (наприклад, NO_EXPORT, NO_ADVERTISE).

3. Процес вибору найкращого шляху (BGP Best Path Selection Algorithm): BGP використовує складний, послідовний алгоритм для вибору найкращого

шляху до цільового префіксу, коли доступно декілька шляхів. Критерії застосовуються в певному порядку, і як тільки один з критеріїв дозволяє однозначно обрати шлях, наступні критерії не розглядаються. Типовий порядок (може дещо відрізнятися залежно від виробника):

1. Найвищий **WEIGHT** (локальний для маршрутизатора атрибут Cisco).
2. Найвищий **LOCAL_PREF**.
3. Маршрут, згенерований локально (network, aggregate).
4. Найкоротший **AS_PATH**.
5. Найнижчий тип **ORIGIN** (IGP < EGP < Incomplete).
6. Найнижчий **MED** (якщо порівнюються шляхи від однієї сусідньої AS).
7. **eBGP** шляхи кращі за **iBGP** шляхи.
8. Найнижча **IGP**-метрика до **NEXT_HOP** атрибута.
9. Найстаріший (найдовше відомий) **eBGP** шлях.
10. Найнижчий **Router ID** відправника.

11. Найнижча IP-адреса сусіда **(Cluster_ID length для RR, потім Neighbor IP Address).**

4. Надійний транспорт: BGP використовує TCP (порт 179) як транспортний протокол, що забезпечує надійну доставку маршрутних оновлень.
5. Інкрементальні оновлення: BGP надсилає повну таблицю маршрутизації лише при встановленні сесії. Надалі передаються лише інкрементальні оновлення, що містять інформацію про нові, змінені або відкликані (withdrawn) маршрути.
6. Політики маршрутизації (Routing Policies): BGP надає потужні інструменти для реалізації політик маршрутизації. Адміністратори можуть контролювати, які маршрути приймаються, які анонсуються, та маніпулювати атрибутами шляху для впливу на вибір шляхів (як своїх вихідних, так і вхідних шляхів сусідів). Це робиться за допомогою route maps, prefix lists, AS-path access lists, community lists тощо.

Переваги BGP:

1. Масштабованість: BGP розроблений для роботи з величезною кількістю маршрутів, які існують в глобальному Інтернеті (сотні тисяч і мільйони префіксів).

2. Гнучкість та контроль політик: Надає широкі можливості для визначення політик маршрутизації, дозволяючи організаціям контролювати, як їхній трафік входить та виходить з їхньої автономної системи.
3. Стабільність: Завдяки використанню TCP та механізмам інкрементальних оновлень, BGP є відносно стабільним протоколом, хоча конвергенція може бути повільною.
4. Запобігання петлям на рівні AS: Атрибут AS_PATH ефективно запобігає петлям маршрутизації між автономними системами.
5. Підтримка CIDR: BGP повністю підтримує безкласову маршрутизацію, що є критичним для ефективного використання адресного простору IPv4 та для IPv6.
6. Стандартизація: BGP є відкритим стандартом, що забезпечує сумісність між обладнанням різних виробників.

Недоліки BGP:

1. Складність: BGP є одним з найскладніших протоколів маршрутизації для розуміння, налаштування та діагностики. Він вимагає глибоких знань та досвіду.
2. Повільна конвергенція: Порівняно з IGP, BGP конвергує значно повільніше. Час відновлення після збоїв може становити хвилини. Це пов'язано з таймерами (наприклад, MinRouteAdvertisementInterval) та самою природою протоколу, орієнтованого на стабільність, а не на миттєву реакцію.
3. Вимоги до ресурсів: Маршрутизатори, що обробляють повну таблицю інтернет-маршрутів (full BGP table), потребують значних обсягів пам'яті (RAM) та потужних процесорів (CPU).
4. Безпека: Хоча існують механізми для підвищення безпеки BGP (наприклад, автентифікація TCP MD5, фільтрація на основі префіксів, RPKI – Resource Public Key Infrastructure), BGP історично був вразливим до таких проблем, як витік маршрутів (route leaks) та перехоплення маршрутів (route hijacking).
5. Не призначений для внутрішньої маршрутизації: BGP не оптимізований для швидкої конвергенції всередині AS. Для цього використовуються IGP.

BGP є незамінним протоколом для функціонування глобального Інтернету, забезпечуючи зв'язність та обмін маршрутною інформацією між тисячами автономних систем. Його сила полягає в масштабованості, гнучкості політик та здатності обробляти величезні обсяги маршрутної інформації. Однак його складність, повільна конвергенція та високі вимоги до ресурсів роблять його

непридатним для використання як основного протоколу внутрішньої маршрутизації. Розуміння BGP є критично важливим для мережевих інженерів, що працюють з інтернет-провайдерами, великими корпоративними мережами, що мають підключення до кількох провайдерів, та центрами обробки даних.

3.6 Протокол OSPF

Протокол OSPF (Open Shortest Path First) є одним з найпоширеніших та найпотужніших протоколів внутрішньої маршрутизації (IGP), що належить до класу протоколів на основі стану каналу (Link-State). Він був розроблений Робочою групою інженерів Інтернету (IETF) як відкритий стандарт для заміни старіючого протоколу RIP. OSPF широко використовується в корпоративних мережах різного масштабу, а також у мережах інтернет-провайдерів як внутрішній протокол маршрутизації. Його популярність зумовлена швидкою конвергенцією, масштабованістю, підтримкою ієрархічної структури та стійкістю до утворення петель маршрутизації.

OSPF базується на алгоритмі Дейкстри (також відомому як алгоритм SPF – Shortest Path First) для обчислення найкоротших шляхів у мережі. Кожен OSPF-маршрутизатор будує повну "карту" (топологію) своєї зони (Area) і на основі цієї карти самостійно розраховує найкращі шляхи до всіх інших вузлів.

1. **Алгоритм стану каналу :**
    - **Виявлення сусідів:** Маршрутизатори використовують **Hello-протокол** для встановлення та підтримки сусідських відносин (adjacencies) з іншими OSPF-маршрутизаторами на тих самих каналах зв'язку. Hello-пакети періодично надсилаються на багатоадресні адреси 224.0.0.5 (всі OSPF-маршрутизатори) або 224.0.0.6 (всі OSPF DR-маршрутизатори).
    - **Обмін інформацією про стан каналів:** Після встановлення сусідства маршрутизатори обмінюються **повідомленнями про стан каналів (Link-State Advertisements, LSAs)**. Кожен маршрутизатор генерує LSA, що описують його власні підключені інтерфейси, стан цих інтерфейсів, метрики каналів та відомих сусідів.
    - **Побудова бази даних стану каналів (Link-State Database, LSDB):** Кожен маршрутизатор зберігає всі отримані LSA у своїй

локальній LSDB. Завдяки механізму флудингу, всі маршрутизатори в межах однієї зони мають ідентичні копії LSDB.

- **Обчислення дерева SPF:** Кожен маршрутизатор запускає алгоритм SPF на своїй LSDB, використовуючи себе як корінь дерева. Результатом є дерево найкоротших шляхів, на основі якого формується таблиця маршрутизації.

2. **Ієрархічна структура (Зони / Areas):** OSPF підтримує дворівневу ієрархічну структуру шляхом поділу автономної системи на **зони (Areas)**.
   - **Зона 0 (Backbone Area / Магістральна зона):** Є ядром OSPF-домену. Всі інші зони повинні бути підключені до зони 0 (безпосередньо або через віртуальні канали).
   - **Стандартні зони (Standard/Normal Areas):** Можуть містити LSA типів 1, 2, 3, 4, 5.
   - **Тупикові зони (Stub Areas):** Не приймають LSA типу 5 (зовнішні маршрути AS). Замість них ABR генерує маршрут за замовчуванням. Дозволяють зменшити розмір LSDB та таблиці маршрутизації.
   - **Повністю тупикові зони (Totally Stubby Areas – Cisco-proprietary extension):** Не приймають LSA типів 3, 4, 5 (крім маршруту за замовчуванням).
   - **Не такі вже й тупикові зони (Not-So-Stubby Areas, NSSA):** Дозволяють імпортувати зовнішні маршрути (LSA типу 7), які потім ABR перетворює на LSA типу 5 для поширення в магістральну зону.

     Ієрархія допомагає зменшити розмір LSDB, частоту обчислень SPF та обсяг маршрутної інформації.

3. **Типи маршрутизаторів OSPF:**
   - **Internal Router (Внутрішній маршрутизатор):** Усі інтерфейси належать одній зоні.
   - **Area Border Router (ABR / Граничний маршрутизатор зони):** Має інтерфейси в кількох зонах, включаючи обов'язково зону 0. Відповідає за резюмування та поширення маршрутної інформації між зонами.
   - **Backbone Router (Магістральний маршрутизатор):** Маршрутизатор, хоча б один інтерфейс якого належить зоні 0.
   - **Autonomous System Boundary Router (ASBR / Граничний маршрутизатор автономної системи):** Маршрутизатор, що підключений до зовнішньої автономної системи (наприклад, до іншого

домену OSPF або до мережі, що використовує інший протокол маршрутизації, як-от BGP або статичні маршрути) і впроваджує (redistributes) зовнішні маршрути в домен OSPF.

4. **Типи LSA (Link-State Advertisements):** OSPF використовує різні типи LSA для передачі різної топологічної інформації:
    - **Type 1 (Router LSA):** Генерується кожним маршрутизатором, описує його підключені канали та сусідів в межах однієї зони. Поширюється лише в межах зони.
    - **Type 2 (Network LSA):** Генерується DR в мережах з множинним доступом, описує всі маршрутизатори, підключені до цього сегменту. Поширюється лише в межах зони.
    - **Type 3 (Summary LSA):** Генерується ABR, описує маршрути до мереж в інших зонах. Поширюється між зонами.
    - **Type 4 (ASBR Summary LSA):** Генерується ABR, описує шлях до ASBR. Поширюється між зонами.
    - **Type 5 (AS External LSA):** Генерується ASBR, описує маршрути до зовнішніх мереж. Поширюється по всьому OSPF-домену (крім stub-зон).
    - **Type 7 (NSSA External LSA):** Генерується ASBR в NSSA-зоні, описує зовнішні маршрути. ABR перетворює LSA типу 7 на LSA типу 5.
5. **Вибори DR та BDR:** У мережах з множинним доступом (наприклад, Ethernet), для зменшення кількості сусідських відносин та LSA-трафіку обираються **Designated Router (DR)** та **Backup Designated Router (BDR)**. Всі інші маршрутизатори (DROther) встановлюють повне сусідство лише з DR та BDR. Вибори відбуваються на основі пріоритету маршрутизатора та Router ID.
6. **Метрика (Вартість / Cost):** OSPF використовує метрику "вартість" (cost), яка за замовчуванням обернено пропорційна пропускній здатності каналу. Формула: Cost = Reference Bandwidth / Interface Bandwidth. Адміністратор може змінювати референтну пропускну здатність або встановлювати вартість інтерфейсу вручну. Вартість шляху – це сума вартостей всіх вихідних інтерфейсів на шляху до цілі.
7. **Версії:**
    - **OSPFv2 (RFC 2328):** Для мереж IPv4.
    - **OSPFv3 (RFC 5340):** Для мереж IPv6. OSPFv3 має значні відмінності від v2, зокрема, працює на канальному рівні (не використовує IP для

транспортну), підтримує кілька екземплярів на одному каналі та може переносити маршрутну інформацію для різних адресних сімейств (Address Families).

8. **Автентифікація:** OSPF підтримує різні типи автентифікації для захисту обміну маршрутною інформацією: null (відсутня), простий текстовий пароль та MD5 (або SHA в OSPFv3 з використанням IPsec).

Переваги OSPF:

1. **Швидка конвергенція:** Завдяки тому, що зміни топології швидко розповсюджуються через флудинг LSA, і кожен маршрутизатор самостійно перераховує шляхи, OSPF забезпечує швидке відновлення після збоїв.
2. **Масштабованість:** Ієрархічна структура з зонами дозволяє ефективно використовувати OSPF у великих та дуже великих мережах, зменшуючи навантаження на маршрутизатори та обсяг LSDB.
3. **Стійкість до петель маршрутизації:** Оскільки кожен маршрутизатор в зоні має повну та узгоджену карту топології, ймовірність утворення петель маршрутизації в межах зони мінімальна.
4. **Відкритий стандарт:** Будучи відкритим стандартом, OSPF підтримується широким колом виробників мережевого обладнання, що забезпечує сумісність у мультивендорних середовищах.
5. **Підтримка VLSM та CIDR:** OSPF є безкласовим протоколом, що дозволяє ефективно використовувати адресний простір.
6. **Ефективне використання пропускної здатності:** Після початкової синхронізації LSDB, OSPF надсилає лише невеликі LSA при змінах у топології, а Hello-пакети мають малий розмір.
7. **Гнучкість:** Підтримка різних типів зон та LSA, а також можливість налаштування метрик, надає гнучкість у проектуванні мережі.

Недоліки OSPF:

1. **Складність:** OSPF є значно складнішим протоколом для розуміння, налаштування та діагностики порівняно з RIP або навіть EIGRP. Вимагає глибоких знань про його роботу, типи LSA, зони тощо.
2. **Вищі вимоги до ресурсів:** Зберігання LSDB та періодичні обчислення SPF вимагають більше пам'яті (RAM) та потужності процесора (CPU) на маршрутизаторах, особливо у великих зонах або при частих змінах топології.

3. **Чутливість до нестабільності каналів:** Часті зміни стану каналів (flapping links) можуть призводити до постійних перерахунків SPF та розповсюдження LSA, що негативно впливає на стабільність мережі та навантаження на маршрутизатори.
4. **Проектування ієрархії:** Правильне проектування зональної структури є критично важливим для ефективної роботи OSPF у великих мережах і може бути складним завданням.

OSPF є потужним, гнучким та масштабованим протоколом маршрутизації, який став де-факто стандартом для багатьох корпоративних та провайдерських мереж. Його здатність швидко адаптуватися до змін топології, забезпечувати безпетлеву маршрутизацію та підтримувати складні ієрархічні структури робить його чудовим вибором для побудови надійних та ефективних IP-мереж. Однак його складність вимагає від мережевих інженерів глибоких знань та ретельного планування при впровадженні та експлуатації.

ВИСНОВКИ

Аналіз ключових протоколів маршрутизації виявляє значну еволюцію в підходах до забезпечення зв'язності, надійності та ефективності комп'ютерних мереж. Для побудови сучасних, стійких до відмов та високопродуктивних інфраструктур вибір протоколу маршрутизації відіграє критичну роль.

Традиційні дистанційно-векторні протоколи, такі як **RIP**, незважаючи на свою історичну значущість та простоту, демонструють суттєві обмеження в контексті вимог сьогодення. Їхня повільна конвергенція, залежність від метрики на основі лише кількості переходів та значне службове навантаження через періодичні повні оновлення роблять їх малопридатними для мереж, де критична швидкість відновлення та оптимальне використання ресурсів. Навіть RIPv2, з його підтримкою безкласової адресації та автентифікації, не вирішує фундаментальних проблем цього підходу. Аналогічно, пропрієтарний протокол **IGRP** від Cisco, хоча й запропонував свого часу вдосконалення у вигляді композитної метрики та більшого ліміту хопів, також є застарілим через свою класову природу та властиві дистанційно-векторним алгоритмам недоліки.

Значно вищий рівень надійності та ефективності пропонують сучасніші протоколи. **EIGRP**, розроблений Cisco, є яскравим прикладом успішного вдосконалення дистанційно-векторного підходу, що часто класифікується як гібридний протокол. Завдяки алгоритму DUAL, EIGRP забезпечує надзвичайно швидку конвергенцію, особливо за наявності попередньо обчислених резервних шляхів (Feasible Successors), гарантоване уникнення петель та ефективне використання мережевих ресурсів через часткові та обмежені оновлення. Його гнучка композитна метрика та підтримка нерівномірного балансування навантаження роблять його потужним інструментом для корпоративних мереж, особливо в інфраструктурах, орієнтованих на обладнання Cisco.

З іншого боку, протоколи на основі стану каналу, зокрема **OSPF**, стали де-факто стандартом для багатьох складних корпоративних та провайдерських

внутрішніх мереж. OSPF забезпечує швидку конвергенцію, високу стійкість до петель завдяки тому, що кожен маршрутизатор має повне уявлення про топологію своєї зони, та чудову масштабованість через ієрархічну структуру зон. Як відкритий стандарт, він гарантує сумісність у мультивендорних середовищах. Хоча OSPF може бути складнішим у налаштуванні та вимагати більше ресурсів від маршрутизаторів порівняно з EIGRP для певних сценаріїв, його надійність, гнучкість та стандартизація роблять його незамінним для побудови великих та критично важливих мереж.

Окремо стоїть протокол **BGP**, який є фундаментальним для функціонування глобального Інтернету. Як протокол зовнішньої маршрутизації, BGP призначений для обміну маршрутною інформацією між автономними системами і вирішує завдання масштабованості та реалізації складних політик маршрутизації на глобальному рівні. Його повільна конвергенція та високі вимоги до ресурсів є прийнятною ціною за стабільність та контроль у величезних масштабах Інтернету, проте роблять його непридатним для використання як основного протоколу внутрішньої маршрутизації.

Таким чином, для побудови сучасних, надійних та ефективних комп'ютерних мереж пріоритет однозначно надається протоколам EIGRP та OSPF для внутрішньої маршрутизації, тоді як BGP залишається невід'ємною частиною міждоменної взаємодії. Вибір між EIGRP та OSPF часто залежить від специфіки мережі, існуючої інфраструктури, вимог до сумісності та рівня експертизи персоналу. Протоколи ж попередніх поколінь, такі як RIP та IGRP, хоча й важливі для розуміння еволюції технологій, не відповідають сучасним вимогам до продуктивності та відмовостійкості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Routing Protocol URL: https://en.wikipedia.org/wiki/Routing_protocol
2. Призначення та класифікація протоколів маршрутизації URL: https://web.posibnyky.vntu.edu.ua/fitki/3yarovijk_komp_merezhi/4.1.html
3. IPX/SPX. URL: https://wiki.cusu.edu.ua/index.php/IPX/SPX
4. . Реалізація сучасних технологій маршрутизації і комутації URL: https://e-tk.lntu.edu.ua/mod/page/view.php?id=3573
5. RIP URL: https://uk.wikipedia.org/wiki/Routing_Information_Protocol
6. Динамічна маршрутизація URL: https://www.vpnunlimited.com/ua/help/cybersecurity/dynamic-routing
7. What is network architecture? Everything you need to know. NordVPN. URL: https://nordvpn.com/uk/blog/network-architecture/
8. Статична та динамічна маршрутизація URL: http://inter.ptngu.com/kompyuterni-merezhi/statychna-ta-dynamichna-marshrutyzatsiya

9. IPv4 vs IPv6: What's The Difference Between the Two Protocols?. Kinsta®. URL: https://kinsta.com/blog/ipv4-vs-ipv6/

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій
Кафедра Комп'ютерної інженерії

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА

на тему: «Аналіз та порівняння протоколів маршрутизації для побудови надійних та швидких комп'ютерних мереж»

Виконав студент групи КІД-42
Галенко Олег Олегович
Керівник кваліфікаційної роботи:
Торошанко Ярослав Іванович
канд. Техн. Наук, доц., с.н.с.

Київ – 2025

Мета роботи – Проаналізувати різні протоколи маршрутизації для визначення їх ефективності та надійності для побудови сучасних комп'ютерних мереж.

Об`єкт дослідження – Дослідження протоколів маршрутизації з метою вибору найбільш відповідного протоколу для побудови надійних та швидких комп'ютерних мереж.

Предмет дослідження – Різні протоколи маршрутизації, їх функціональні особливості та показники.

Актуальність обраної теми

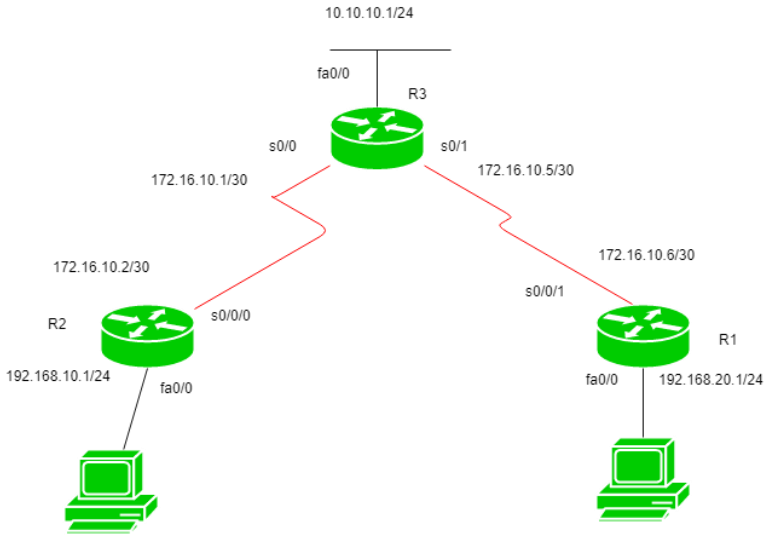
Актуальність даної роботи полягає в необхідності забезпечення високої надійності та швидкодії сучасних комп'ютерних мереж, що є критично важливим для функціонування бізнесу, державних установ та повсякденного життя. Протоколи маршрутизації відіграють центральну роль у досягненні цих цілей. Тому аналіз їхніх характеристик, переваг та недоліків, а також порівняння їхньої ефективності в різних сценаріях є важливим науково-практичним завданням.

3

- Протокол маршрутизації є стандартизованим набором правил, який керує тим, як маршрутизатори спілкуються та обмінюються маршрутною інформацією. Його ключові функції включають виявлення сусідніх маршрутизаторів, обмін даними про доступні мережі, обчислення найкращих шляхів та підтримку актуальності цієї інформації при змінах у топології мережі.

4

Приклад роботи маршрутизації



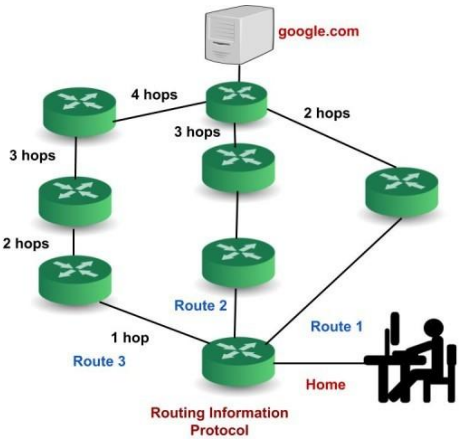
5

Характеристики та вимоги до корпоративної комп’ютерної мережі:

1. швидкість протоколу;
2. надійність протоколу;
3. масштабованість;
4. безпека протоколу;
5. складність налаштування.

6

Протокол RIP:



Протокол маршрутної інформації (RIP) є одним із найстаріших і найпростіших дистанційно-векторних протоколів внутрішньої маршрутизації (IGP), визначених у стандартах Інтернету. Він був розроблений на основі алгоритмів, що використовувалися в Xerox Network Systems (**XNS**). Незважаючи на появу більш досконалих протоколів, RIP все ще іноді використовується в невеликих, простих мережах завдяки своїй легкості налаштування та невибагливості до ресурсів.

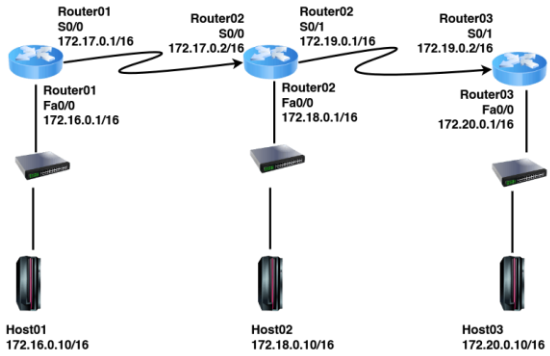
7

Швидкість протоколу	**Повільна**
Надійність протоколу	**Низька**
Масштабованість	**Низька**
Безпека протоколу	**RIPv1: Відсутня.** **RIPv2: базовий рівень захисту**
Складність налаштування	**Дуже низька**

Висновок:
Простий у налаштуванні та невибагливий до ресурсів. Однак, через повільну конвергенцію, обмежену масштабованість та неефективну метрику, не рекомендується для більшості сучасних мереж. Придатний для дуже малих, статичних мереж або навчальних цілей.

8

Протокол IGRP



Протокол маршрутизації внутрішнього шлюзу (IGRP) – це дистанційно-векторний протокол внутрішньої маршрутизації (IGP), розроблений компанією Cisco Systems в середині 1980-х років. Він був створений як відповідь на обмеження протоколу RIP, зокрема, його обмеження на 15 хопів та використання кількості переходів як єдиної метрики, що робило RIP непридатним для великих та складних мереж. IGRP був пропрієтарним протоколом Cisco і мав на меті забезпечити більш надійну та гнучку маршрутизацію в корпоративних мережах.

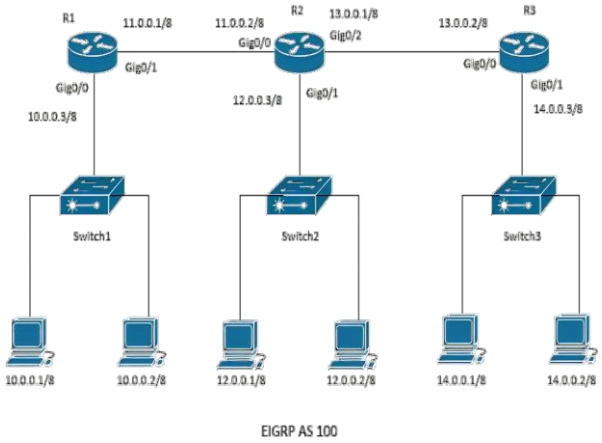
9

Швидкість протоколу	**Відносно повільна**
Надійність протоколу	**Середня (для свого часу).**
Масштабованість	**Середня**
Безпека протоколу	**Відсутня**
Складність налаштування	**Низька або середня**

Висновок:
Був значним кроком вперед порівняно з RIP, пропонуючи кращу метрику та масштабованість. Однак, через класову природу, відсутність автентифікації та пропрієтарність Cisco, повністю застарів. Витіснений EIGRP та відкритими стандартами. Має лише історичний інтерес.

10

Протокол EIGRP



Розширений протокол маршрутизації внутрішнього шлюзу (**EIGRP**) – це вдосконалений дистанційно-векторний (часто класифікований як гібридний) протокол внутрішньої маршрутизації, розроблений компанією Cisco Systems. Він є наступником **IGRP** і був створений для усунення багатьох його недоліків, таких як класова природа, повільна конвергенція та обмежені можливості масштабування. EIGRP поєднує переваги дистанційно-векторних протоколів з перевагами протоколів стану каналу.

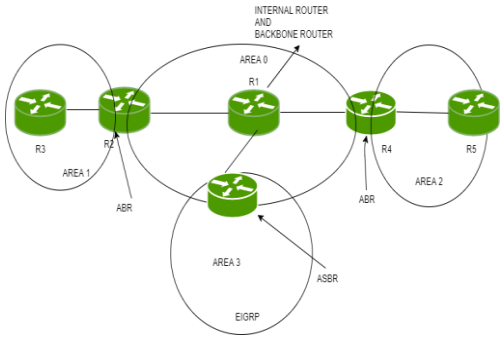
11

Швидкість протоколу	**Дуже висока**
Надійність протоколу	**Висока**
Масштабованість	**Висока**
Безпека протоколу	**Середня або висока**
Складність налаштування	**Середня**

Висновок:
Потужний та ефективний протокол, що забезпечує чудовий баланс швидкості, надійності та ефективності використання ресурсів. Відмінний вибір для мереж Cisco різного розміру. Відкриття частини специфікацій розширює можливості застосування.

12

Протокол OSPF



Протокол OSPF (Open Shortest Path First) є одним з найпоширеніших та найпотужніших протоколів внутрішньої маршрутизації (IGP), що належить до класу протоколів на основі стану каналу. Він був розроблений Робочою групою інженерів Інтернету (IETF) як відкритий стандарт для заміни старіючого протоколу RIP. OSPF широко використовується в корпоративних мережах різного масштабу, а також у мережах інтернет-провайдерів як внутрішній протокол маршрутизації.

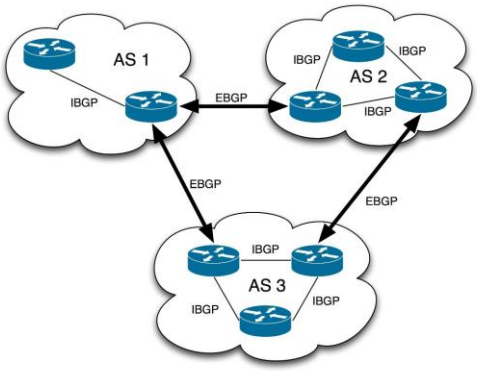
13

Швидкість протоколу	**Висока**
Надійність протоколу	**Висока**
Масштабованість	**Дуже висока**
Безпека протоколу	**Середня або висока**
Складність налаштування	**Висока**

Висновок:
Потужний, гнучкий та масштабований протокол, що є стандартом де-факто для багатьох корпоративних та провайдерських IGP. Ідеальний для складних, великих, мультивендорних мереж. Вимагає ретельного проектування та глибоких знань для ефективного впровадження.

14

Протокол BGP



Протокол граничного шлюзу (**BGP**) є стандартизованим протоколом зовнішньої маршрутизації, розробленим для обміну маршрутною інформацією та інформацією про досяжність мереж між різними автономними системами (AS) в Інтернеті. Автономна система – це сукупність IP-мереж та маршрутизаторів, що знаходяться під єдиним адміністративним керуванням та використовують спільну політику маршрутизації.

15

Швидкість протоколу	**Відносно повільна**
Надійність протоколу	**Висока (для свого завдання)**
Масштабованість	**Надзвичайно висока**
Безпека протоколу	**Середня та покращується**
Складність налаштування	**Дуже висока**

Висновок:
Незамінний для функціонування Інтернету, забезпечуючи міждоменну маршрутизацію та реалізацію складних політик. Не використовується як IGP. Його сила – в масштабованості та гнучкості політик, а не в швидкості конвергенції.

16

ВИСНОВКИ

У ході виконання бакалаворської роботи було виявлено, що для побудови сучасних, надійних та ефективних комп'ютерних мереж пріоритет однозначно надається протоколам EIGRP та OSPF для внутрішньої маршрутизації, тоді як BGP залишається невід'ємною частиною міждоменної взаємодії. Вибір між EIGRP та OSPF часто залежить від специфіки мережі, існуючої інфраструктури, вимог до сумісності та рівня експертизи персоналу. Протоколи ж попередніх поколінь, такі як RIP та IGRP, хоча й важливі для розуміння еволюції технологій, не відповідають сучасним вимогам до продуктивності та відмовостійкості.

17