Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет навчально-науковий центр заочної форми навчання
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Модель моніторингу розподілених комп'ютерних систем

(тема)

Виконав:

студент II курсу, групи КСМзм-22-1

Ладика Є.О.
(прізвище, ініціали)

Спеціальність

123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма

Комп’ютерні системи та мережі
(повна назва освітньої програми)

Керівник: доц. Голубничий.Д.Ю.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет навчально-науковий центр заочної форми навчання

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Комп'ютерні системи та мережі
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Ладиці Євгену Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Модель моніторингу розподілених комп'ютерних систем

затверджена наказом по університету від " 03 " листопада 2023 р. № 244 Стз

2. Термін подання студентом роботи до екзаменаційної комісії 15 січня 2024 р.

3. Вхідні дані до роботи

число ребер в одному графові – 14 шт.;

число вузлів в одному графові – 9 шт.;

загальне число кінцевих точок – 20 шт.;

число кінцевих точок на одному сайті – 10 шт.;

при передачі використовували один пакет розміром 20 КБ

4. Перелік питань, що потрібно опрацювати у роботі

1) Аналіз побудови віртуальних приватних мереж
2) Розробка модифікованої потокової моделі VPN при наявності обмежень на мережні ресурси
3) Дослідження властивостей моделей VPN

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів)

Слайд-презентація – 20 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Огляд способів побудови драйверів та служб	07.11.23 – 05.11.23	
	на вузлах комп'ютерної мережі		
2	Вибір та обґрунтування методики дослідження	06.11.23 – 12.11.23	
3	Вибір інструментальних засобів	13.11.23 – 19.11.23	
4	Розробка моделі мережі	20.11.23 – 03.12.23	
5	Проведення експериментів	04.12.23 – 10.12.23	
6	Оформлення матеріалів кваліфікаційної роботи	11.12.23 – 29.12.23	
7	Подання кваліфікаційної роботи керівникові та	30.12.23 – 04.01.24	
	її попередній захист		
8	Подання кваліфікаційної роботи на	05.01.24 – 10.01.24	
	рецензування		

Дата видачі завдання 06 листопада 2023 р.

Студент _____
(підпис)

Керівник роботи _____ доц. Голубничий Д.Ю.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 90 с., 34 рис., 5 табл., 1 дод., 32 джерел.

ГРАФ, ВІРТУАЛЬНА ПРИВАТНА МЕРЕЖА, РЕСУРС, СМУГА ПРОПУСКАННЯ, КОРИСТУВАЧ.

Метою кваліфікаційної роботи є підвищення ефективності використання ресурсів мереж загального користування на основі розробки елементів теорії планування VPN в умовах дистанційної роботи.

Об'єктом дослідження є процеси передачі даних з використанням технології віртуальних приватних мереж в умовах дистанційної роботи.

Предметом дослідження є моделі та методи оптимального розподілу смуги пропускання мережі загального користування для реалізації віртуальних приватних мереж відповідно до вимог користувачів послуг і можливостями провайдера послуг VPN.

У ході виконання кваліфікаційної роботи проведено аналіз характерних особливостей практичної реалізації віртуальних приватних мереж в умовах дистанційної роботи, які необхідно враховувати при розробці теоретичної основи планування VPN; обґрунтувані базові принципи побудови автоматизованої системи експлуатаційної підтримки OSS (Operations Support System) діяльності провайдера послуг VPN; розроблено метод аналізу та синтезу топології VPN на основі теорії графів з урахуванням різних аспектів практичної реалізації приватної мережі (характеру трафіку, способів маршрутування трафіку в VPN, обмежень на доступну смугу пропускання та ін.); проведені експериментальні дослідження моделей і методів планування VPN і оцінена їх ефективність.

ABSTRACT

Master’s thesis: 90 pages, 34 figures, 5 tables, 1 appendices, 32 sources.

GRAPH, VIRTUAL PRIVATE NETWORK, RESOURCE, BANDWIDTH, USER.

The major goal of this thesis is to increase the efficiency of using public network resources based on the development of elements of VPN planning theory in the conditions of remote work.

The object of the study is data transfer processes using the technology of virtual private networks in the conditions of remote work.

The subject of the study is models and methods of optimal distribution of the bandwidth of the public network for the implementation of virtual private networks in accordance with the requirements of service users and the capabilities of the VPN service provider.

In order to analysis of the characteristic features of the practical implementation of virtual private networks in the conditions of remote work, which must be taken into account when developing the theoretical basis of VPN planning, was carried out; substantiated basic principles of building an automated OSS (Operations Support System) operational support system for the activity of a VPN service provider; a method of analysis and synthesis of VPN topology based on graph theory was developed, taking into account various aspects of the practical implementation of a private network (the nature of traffic, methods of routing traffic in VPN, restrictions on available bandwidth, etc.); experimental studies of VPN planning models and methods were conducted and their effectiveness was evaluated.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

BGP – протокол прикордонного шлюзу (англ. Border Gateway Protocol)

CE – граничний клієнт (англ. Customer Edge)

CoS – клас обслуговування (англ. Class of Service)

CPVPN – клієнт – наданий VPN (англ. Customer - Provisioned VPN)

GRE – загальна інкапсуляція маршрутизації (англ. Generic Routing Encapsulation)

IETF – робоча група з розробки Інтернету (англ. The Internet Engineering Task Force)

IP – Інтернет-протокол (англ. Internet Protocol)

MIB – інформаційна база управління (англ. Management Information Base)

MPLS – багатопротокольне перемикання міток (англ. Multiprotocol Label Switching)

NGN – мережа нового покоління (англ. Next Generation Network)

OSI – взаємозв'язок відкритих систем (англ. Open systems interconnection)

OSPF – протокол маршрутизації, заснований на відстеженні стану каналу (англ. Open Shortest Path First)

PE – пограничний постачальник (англ. Provider Edge)

PPTP – протокол тунелювання точка-точка (англ. Point-to-Point Tunneling Protocol)

PPVPN – VPN, наданий постачальником (англ. Provider-Provisioned VPN)

QoS – якість обслуговування (англ. Quality of Service)

RNMON – віддалений моніторинг мережі (англ. Remote Network Monitoring)

SLA – погоджений рівень обслуговування (англ. Service Level Agree)

SNMP – простий протокол керування мережею (англ. Simple Network Management Protocol)

TE – транспортна інженерія (англ. Traffic Engineering)

VPLS – служба віртуальної приватної локальної мережі (англ. Virtual Private LAN Service)

VPN – віртуальна приватна мережа (англ. Virtual Private Network)

VPN-OSS – система підтримки операцій в віртуальній приватній мережі (англ. Operations Support System)

VPRN – віртуальна приватна маршрутизована мережа (англ. Virtual Private Routed Network)

VPWS – віртуальна приватна телеграфна служба (англ. Virtual Private Wire Service)

ВСТУП

У зв'язку з пандемією короновірусу COVID-19, дистанційна робота в навчальних закладах стала актуальною як ніколи раніше. Багато з викладачів переймаються питанням як організувати процес такої роботи. Способів кілька: від перенесення навчальних матеріалів з дисциплін на домашні комп’ютери до організації доступу ззовні до серверу, на якому зберігаються ці матеріали. В деяких випадках доступ до серверу можна налаштувати через RDP, при якому людина на своєму домашньому комп’ютері запускає підключення до віддаленого робочого столу, вводить IP-адресу і порт, який їй надає системний адміністратор, вводить логін і пароль (або той, що вводить щодня на роботі, або той, що надає IT-спеціаліст).

Однією з альтернатив є такий спосіб підключення як VPN. Для вирішення цих проблем може бути використана послуга віртуальних приватних мереж VPN (Virtual Private Network). Віртуальна приватна мережа будується на основі логічних з'єднань між певними корпоративними користувачами через мережу загального користування з пакетною комутацією, ізольованих на логічному рівні від інших користувачів тієї ж мережі. VPN забезпечує безпеку і секретність, як у традиційній приватної мережі, при збереженні вартості передачі інформації, як в мережі загального користування. Отже, така послуга затребувана багатьма корпоративними користувачами, які не мають власних мережних ресурсів, в тому числі органами державної влади та іншими бюджетними організаціями, зважаючи на її показники економічності та доступності.

Хоча послуги віртуальних приватних мереж оператори надають уже досить тривалий період, тим не менше, тільки з активним розвитком мереж на базі протоколу IP (Internet Protocol) останнім часом спостерігається зростання наукових досліджень технології VPN. Незважаючи на значну популярність тематики дослідження VPN доводиться констатувати, що до

цих пір залишається низка питань і невирішених завдань. Перелічимо основні з них:

- фактично відсутня єдина теоретична база, яка б служила методологічною основою вирішення всього комплексу завдань підтримки послуг VPN - планування, реалізації та експлуатації віртуальних мереж;

- наявні теоретичні підходи до оптимального розподілу смуги пропускання мереж загального користування для реалізації VPN не враховують багатьох особливостей функціонування сучасних віртуальних мереж;

- відсутні ефективні алгоритми та програмні системи, які дозволяють скоротити експлуатаційні витрати провайдерів послуг VPN і тим самим знизити на них тарифи.

Вирішення зазначених питань дозволить підвищити ефективність використання мережної інфраструктури в цілому, що вигідно як споживачам, так і постачальникам послуг VPN. Таким чином, актуальність теми кваліфікаційної роботи визначається необхідністю розробки теорії планування VPN, під якою розуміється сукупність математичних моделей і методів дослідження, призначених для використання провайдерами послуг VPN при вирішенні завдань оптимального розподілу наявних мережних ресурсів на різних етапах експлуатації віртуальних мереж.

Актуальність теми роботи визначається необхідністю розробки теорії планування VPN, під якою розуміється сукупність математичних моделей і методів дослідження, призначених для використання провайдерами послуг VPN при вирішенні завдань оптимального розподілу наявних мережних ресурсів на різних етапах експлуатації віртуальних мереж.

Об'єктом дослідження є процеси передачі даних з використанням технології віртуальних приватних мереж в умовах дистанційної роботи.

Предметом дослідження є моделі та методи оптимального розподілу смуги пропускання мережі загального користування для реалізації

віртуальних приватних мереж відповідно до вимог користувачів послуг і можливостями провайдера послуг VPN.

Мета роботи і задачі дослідження. Мета кваліфікаційної роботи полягає в підвищенні ефективності використання ресурсів мереж загального користування на основі розробки елементів теорії планування VPN в умовах дистанційної роботи. В результаті повинні бути побудовані моделі та методи аналізу VPN, використання яких вигідно як користувачам, так і провайдерам послуг VPN.

Для реалізації поставленої мети необхідно вирішити наступні задачі:

- провести аналіз характерних особливостей практичної реалізації віртуальних приватних мереж, які необхідно враховувати при розробці теоретичної основи планування VPN;

- обґрунтувати базові принципи побудови автоматизованої системи експлуатаційної підтримки OSS (Operations Support System) діяльності провайдера послуг VPN;

- розробити методи аналізу та синтезу топології VPN на основі теорії графів з урахуванням різних аспектів практичної реалізації приватної мережі (характеру трафіку, способів маршрутування трафіку в VPN, обмежень на доступну смугу пропускання та ін.);

- провести експериментальні дослідження моделей і методів планування VPN і оцінити їх ефективність.

Методи дослідження. Для вирішення перерахованих задач в роботі використовувалися методи теорії графів, теорії оптимізації, теорії ймовірностей і математичної статистики, чисельні методи розрахунку і аналізу. Достовірність основних результатів роботи забезпечується строгим характером використаних методів, адекватністю і коректністю застосованого математичного апарату, зіставленням з аналогічними результатами, отриманими іншим дослідниками. Достовірність положень і висновків роботи підтверджується результатами моделювання, практичної реалізації та впровадження розробок.

1 АНАЛІЗ ПОБУДОВИ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ

1.1 Перспективність послуг в мережах VPN

Перш ніж розглядати можливі моделі й методи реалізації віртуальних приватних мереж, покажемо, що послуги VPN знаходять усе більш широке застосування в існуючих мережах і, особливо перспективні в мережах наступного покоління NGN (Next Generation Network), заснованих на пакетних технологіях передачі інформації.

VPN входить у трійку найважливіших технологій, які корпоративні користувачі збираються використовувати в найближчім майбутньому. Значимість цієї технології для будь-яких компаній, а тим більше для мало бюджетних організацій, обумовлена, насамперед, тими економічним вигодами, які пов'язані з її впровадженням. По оцінці компанії Infonetics Research при використанні VPN компанія може заощадити від 20% до 40% засобів для зв'язку "мережа-мережа" і від 60% до 80% при підключенні віддалених користувачів.

Існують різноманітні способи побудови віртуальних приватних мереж. Серед усього іншого, ці способи відрізняються розподілом функцій по підтримці VPN між корпоративною мережею й мережею загального користувача провайдера послуг VPN.

В одному випадку всі функції по підтримці VPN виконує мережа провайдера, а корпоративні клієнти тільки користуються послугами VPN.

Провайдер гарантує конфіденційність і якість обслуговування клієнтського трафіка від точки входу в мережу загального користування до точки виходу. При цьому зусилля користувача по створенню віртуальної приватної мережі зводяться до підписанням контракту із провайдером на надання VPN-послуг (а, можливо, ще й до контролю над дотриманням провайдером умов контракту). Цей варіант найбільше підходить для

невеликих організацій і підприємств, у яких найчастіше відсутні кваліфіковані фахівці з реалізації й підтримці VPN власними силами.

В іншому випадку підприємство організує віртуальну приватну мережу власними силами, за рахунок застосування спеціальних VPN-продуктів у своїй мережі. У якості таких продуктів можуть використовуватися всілякі засоби: маршрутизатори й захисні екрани з додатковим програмним забезпеченням, що виконують шифрування переданих даних, а також спеціальні програмні й апаратні засоби для створення захищених каналів.

Побудувати повноцінну віртуальну приватну мережу тільки силами підприємства, без участі провайдера, неможливо. Усі наявні на ринку VPN-продукти забезпечують рішення тільки однієї із двох необхідних для імітації приватної мережі завдань, а саме, виконують захист переданих даних. Ніяких же способів підтримки заданого якості транспортного обслуговування ці продукти не надають.

Підтримувати необхідну якість обслуговування для окремих потоків даних у транспортній мережі може тільки сам провайдер послуг VPN. Технологія, яка з'явилася порівняно недавно, мультипротокольної комутації по мітках MPLS (Multiprotocol Label Switching) з її механізмом управління трафіком TE (Traffic Engineering) щонайкраще реалізує послугу віртуальних приватних мереж VPN. MPLS VPN являє собою закінчений високонадійний розв'язок по швидкіснім об'єднанню IP-мереж різних операторів зі збереженням унікальної адресації їх мереж.

Завдяки транспортуванню даних на третьому (мережному) рівні (7-ми рівневої моделі взаємодії відкритих систем (OSI)), послуга MPLS VPN має високу економічну ефективність у порівнянні із традиційно застосовуваними для цих цілей послугами VPN мереж Frame Relay і ATM. Рівень захищеності VPN-з'єднання в MPLS-мережі не уступає аналогічним показникам мереж четвертого (транспортного) рівня. Для сервісів-провайдерів технологія MPLS – це можливість економічної підтримки масштабованих послуг VPN у мережі IP. При цьому для захисту даних різних клієнтів використовується технологія

поділу трафіка. Інжиніринг трафіка, якість послуг QoS (Quality of Service) і функції протоколу MPLS, що передбачають роботу без установлення з'єднань (connectionless features), надають сервіс – провайдерам небувалі можливості для нарощування VPN у своїй інфраструктурі без шкоди для продуктивності. Якщо користувачеві потрібно забезпечити високий рівень безпеки, він може використовувати набір відповідних протоколів (наприклад, IPsec), які дозволяють захистити дані в будь-яких каналах, де може виникати погроза несанкціонованого доступу.

В Україні існує велика кількість компаній зв'язку, які надають на послуги VPN. Так компанія АТ "Укртелеком" на базі своєї мережі MPLS обслуговує вже більш 300 віртуальних IP-мереж (рисунок 1.1).

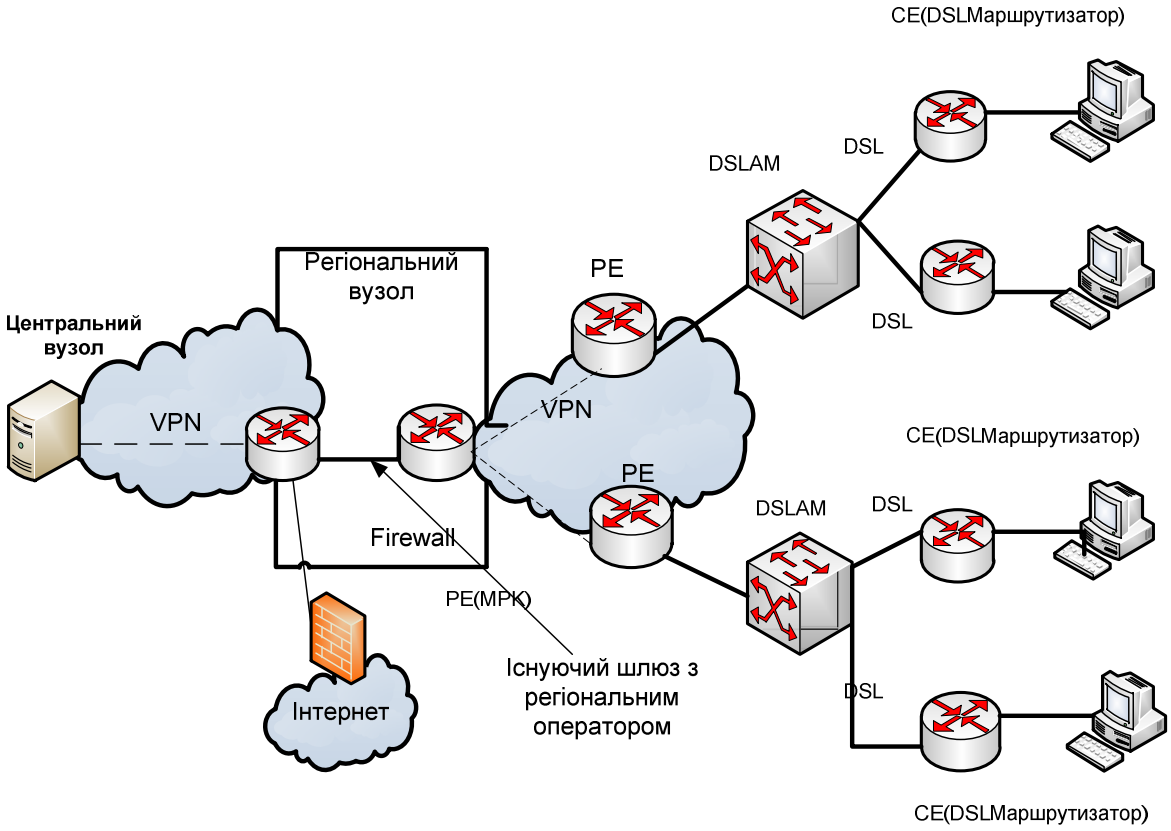

Рисунок 1.1 – Схема організації VPN від "Укртелеком"

Таким чином, спостережувані за останні роки темпи росту попиту корпоративних клієнтів на послуги віртуальних приватних мереж показує

перспективність використання технології VPN у мережах наступного покоління NGN, проекти яких останнім часом широко реалізуються за кордоном і в Україні. Зі збільшенням числа віртуальних мереж і їхніх масштабів для провайдерів послуг VPN усе гостріше встає проблема ефективного використання мережних ресурсів, успішне рішення якої дозволить не тільки збільшити доходи провайдерів, але й підвищити якість і знизити тарифи на надавані послуги користувачам.

1.2 Класифікація технологій реалізації VPN

Класифікувати VPN можна по декільком основним параметрам: по типу використовуваного середовища, по способу реалізації, по призначенню, за рівнем мережного протоколу й ін. Насамперед, усі віртуальні частки мережі діляться за наступною класифікацією (рисунок 1.2).

VPN, підтримувані обладнанням, яке встановлюється в приміщенні клієнта CE (Customer Edge) і служить для його підключення до магістралі сервісу-провайдера – так звані Customer – Provisioned VPN (CPVPN);

- VPN, підтримувані прикордонним устаткуванням провайдера PE (Provider Edge) – так звані Provider-Provisioned VPN (PPVPN).

- І ті й інші VPN у свою чергу можна розділити на два класи залежно від характеру організації зв’язки корпоративних користувачів:

- для підключення декількох філій однієї організації в одну віртуальну приватну мережу (так звані site-to-site VPN);

- для підключення вилучених користувачів до центрального офісу або філії компанії (так звані remote access VPN).

Віртуальні мережі можуть бути реалізовані на базі протоколів моделі OSI різних рівнів:

- другого (канального) – L2VPN;
- третього (мережного) – L3VPN;
- п’ятого (сеансового) – L5VPN.

Для реалізації VPN 2-го рівня (L2VPN) можуть бути використані наступні протоколи й технології.

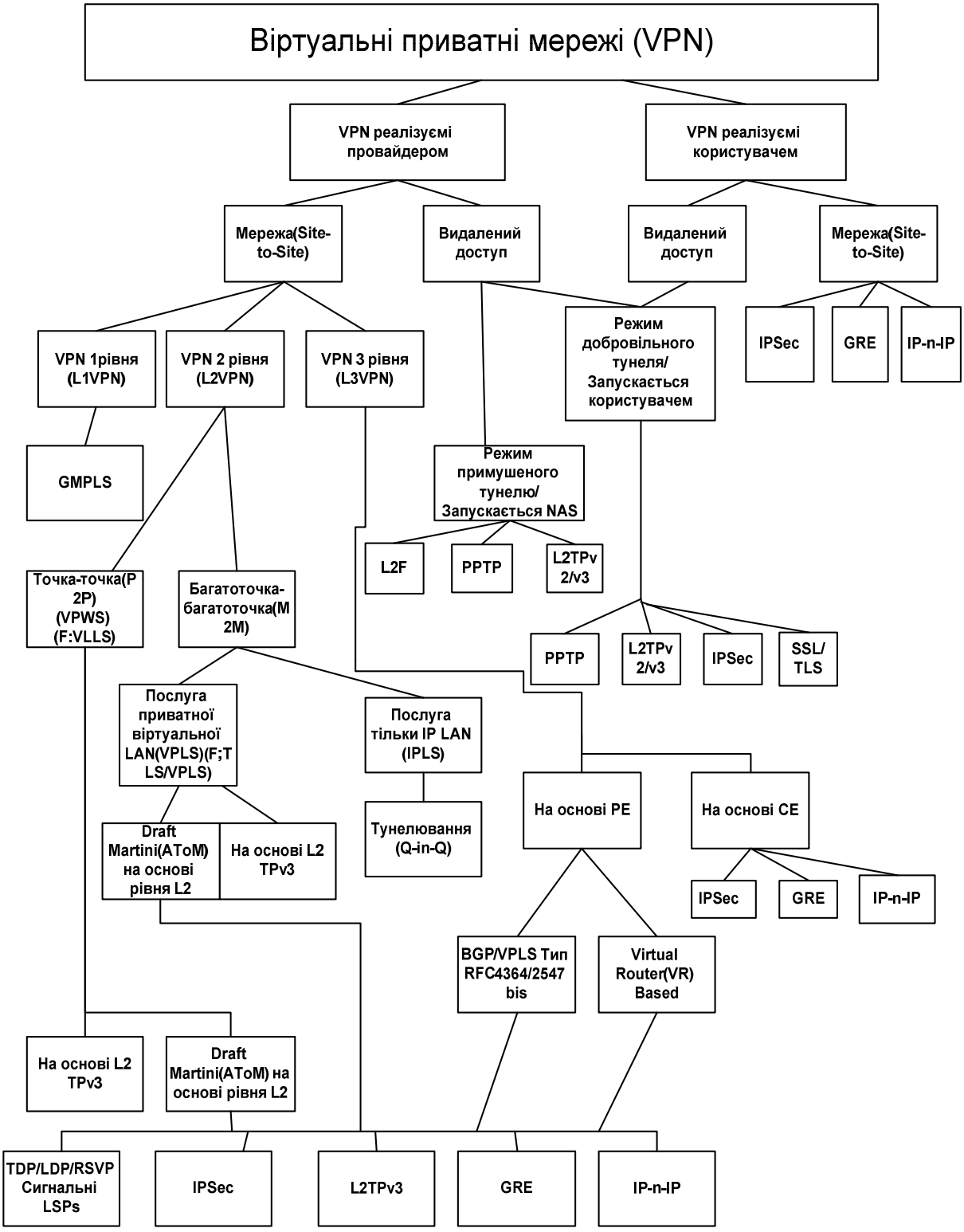

Рисунок 1.2 – Класифікація технологій реалізації VPN

1. Тунельний протокол 2-го рівня L2TP (Layer 2 Tunnelling Protocol) (стандарт IETF RFC 2661) – мережний протокол тунелювання канального рівня протокол, що поєднує в собі L2F (layer 2 Forwarding), розроблений компанією Cisco, і протокол PPTP корпорації Microsoft. Дозволяє організовувати VPN із заданими пріоритетами доступу, однак не містить у собі засобів шифрування й механізмів автентифікації.

2.Тунельний протокол “точка-точка” PPTP (Point-to-Point Tunneling Protocol) – стандарт IETF RFC 2637 – протокол типу “ точка-точка”, що дозволяє встановлювати захищене з’єднання за рахунок утворення спеціального тунелю в стандартній, незахищеній, мережі фактично PPTP поміщає (інкапсулює) кадри PPP в IP-пакети для передачі по глобальній IP-мережі.

3. Послуга віртуальної приватної локальної мережі VPLS (Virtual Private LAN Service) – пакети локальної мережі інкапсулюються з використанням технології MPLS, яка забезпечує створення тунелів у мережі оператора зв'язки, які незалежні від користувацького трафіка. VPLS використовує стандарти IEEE 802.1q і MPLS Martini-drafts для інкапсуляції пакетів і їх транспорту.

4. Послуга віртуального приватного проведення VPWS (Virtual Private Wire Service) – дозволяє організовувати прозорі з'єднання (на другому рівні OSI: 802.1q, Frame Relay, ATM і ін.) типу " точка-точка" через мережу MPLS.

5. Традиційні VPN (на базі традиційних пакетних технологій).

Для реалізації VPN 3-го рівня (L3VPN) можуть бути використані наступні протоколи й технології:

1. Набір протоколів IPsec (IP Security) – для забезпечення захисту даних, переданих по міжмережному протоколу IP, дозволяє здійснювати підтвердження справжності й/або шифрування Ip-Пакетів.

Більшість сучасних реалізацій Ipsec засноване на стандартах RFC 2401.

2. Загальна інкапсуляція маршрутів GRE (Generic Routing Encapsulation) – протокол тунелювання мережних пакетів, розроблений

фірмою Cisco, забезпечує інкапсуляцію пакетів мережного рівня моделі OSI в IP пакети, використовується в комбінації із протоколом PPTP для створення віртуальних приватних мереж.

3. Комбінована технологія BGP/MPLS – протокол прикордонного шлюзу BGP (Border Gateway Protocol) служить для прокладки маршрутів через опорну мережу MPLS. Заснована на стандарті IETF RFC 4364 (раніше RFC 2547bis).

4. Віртуальна приватна маршрутизуюча мережа VPRN (Virtual Private Routed Network) – використовуються для створення тунелів між вузлами транзитної мережі, а не між, що приєднуються мережами через транзитну мережу. При цьому маршрутизація трафіка мереж, що приєднуються, здійснюється в транзитній мережі. Заснована на стандарті IETF RFC 2764.

В роботі основна увага буде приділена дослідженню моделей віртуальних приватних мереж, які можна умовно описати як IP MPLS L3 PPVPN, тобто реалізованих в IP-мережі на базі протоколів 3 рівня й технології MPLS і підтримуваних граничним устаткуванням провайдера послуг VPN. Це обумовлене тим, що даний тип VPN найпоширеніший і має безліч переваг: масштабованість, керованість, надійність, гнучка багаторівнева підтримка якості обслуговування (QoS) і класів сервісу (CoS) тощо.

1.3 Оптимальний розподіл ресурсів мереж загального користування для реалізації VPN

Підтримка різних критичних до характеристик мережі послуг вимагає від VPN виконання певних гарантій якості, прописаних у так званім угоді про якість обслуговування SLA (Service Level Agreement). Якщо орендовані (частки) канали повністю ізолюють різні потоки даних і забезпечують повну гарантію мережних характеристик (смугу пропускання, затримки, джиттер і втрати пакетів), то в VPN повинні бути передбачені відповідні механізми для

реалізації подібних гарантій якості послуг, певних в SLA. І тут виникає проблема конфлікту вимог різних VPN до загальних поділюваних мережних ресурсів. В умовах сучасного висококонкурентного ринку провайдеру послуг VPN необхідно розв'язати цю проблему так, щоб, з одного боку, забезпечити максимальне завантаження мережі й одержати максимальний мережний дохід, а з іншого – надати послуги користувачам з гарантованою якістю й з мінімально можливою вартістю.

Трафік пакетних даних останнім часом став для телекомунікаційних операторів будь-яких рівнів і типів помітним джерелом доходу, тому мережі IP експлуатуються усе активніше. У погоні за прибутком оператори намагаються вичавити з мережі максимум можливого, а виходить, методи оптимального розподілу ресурсів мереж IP здобувають усе більшу популярність. Функціонування пакетної мережі можна вважати ефективним, коли кожний ресурс завантажений, але не перевантажений. Це значить, що коефіцієнт використання ресурсу повинен наближатися до одиниці, але не настільки, щоб черги пакетів до нього були б постійно більшими, приводячи до затримок і втратам через переповнення внутрішніх буферів у маршрутизаторах.

Проблема управління пакетною мережею полягає в досягненні двох цілей. По-перше, необхідно прагнути до поліпшення якості обслуговування переданого трафіка, тобто до зниження затримок, зменшенню втрат пакетів і збільшенню інтенсивності потоків трафіка, що дозволить залучити якнайбільше користувачів і добитися успіхів у конкурентній боротьбі. По-друге, завантаження всіх ресурсів мережі повинна бути максимально можливої для підвищення обсягів переданого трафіка.

Донедавна завдання оптимального використання ресурсів пакетних мереж на базі протоколу IP вирішувалася найчастіше за допомогою перерозподілу ресурсів окремого маршрутизатора між різними потоками, що протікають через нього. Саме це завдання вирішують методи, об'єднані під загальною назвою - якість обслуговування QoS (Quality of Service). У той же

час такий потужний засіб, як вибір шляхів проходження трафіка через мережу, традиційно застосовувалося в мережах IP у дуже обмежених масштабах. Але ж від шляхів проходження трафіка (особливо при його фіксованій інтенсивності) у першу чергу залежить завантаження маршрутизаторів і каналів, а виходить, і ефективність використання мережі. Відомо, що всі протоколи маршрутизації – як дистанційно векторні (наприклад, RIP), так і стану зв'язків (OSPF і IS-IS), визначають для трафіка, спрямованого в конкретну мережу, найкоротший маршрут відповідно до деякої метрики. Обраний шлях може бути більш раціональним, якщо в розрахунки ухвалюється номінальна пропускна здатність каналів зв'язки або внесені ними затримки, або менш раціональним, якщо враховується тільки кількість проміжних маршрутизаторів між вихідної й кінцевої мережами, але в кожному разі вибирається єдиний маршрут навіть при наявності декількох альтернативних.

Класичним прикладом неефективності такого підходу служить мережа з топологією (рисунок 1.3).

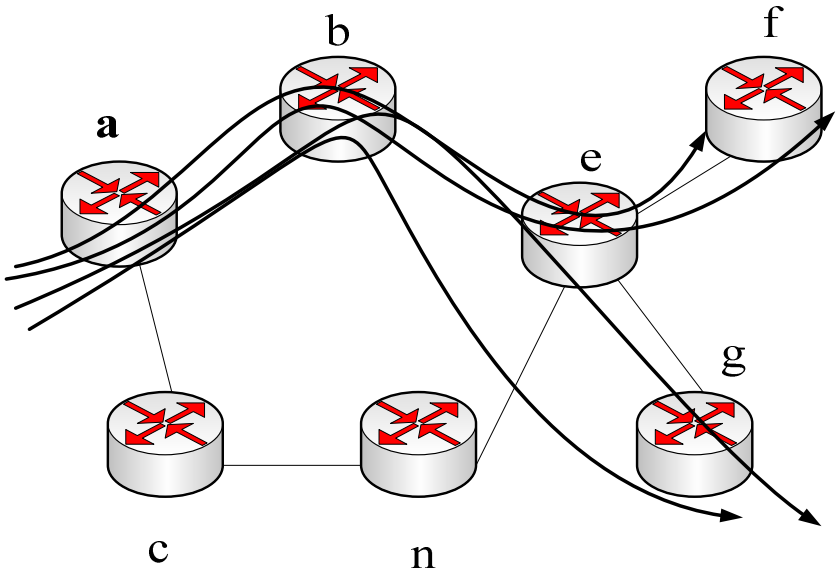

Рисунок 1.3 – Приклад топології мережі з неефективним завантаженням ресурсів шляхами, обумовленими протоколами маршрутизації

Незважаючи на те, що між маршрутизаторами A та E є два шляхи: верхній, через маршрутизатор B, і нижній, через маршрутизатори C и D – увесь трафік від A до E відповідності із принципами маршрутизації, прийнятими в мережах IP, направляється по верхньому шляхові. Тільки тому, що нижній шлях небагато довше, чим верхній (у ньому на один транзитний вузол більше), він ігнорується, хоча міг би задіятися паралельно з верхнім шляхом.

Помітимо, однак, що при наявності в мережі декількох альтернативних маршрутів рівної вартості (метрики), трафік ділиться між ними, і навантаження на маршрутизатори й канали зв'язки розподіляється більш збалансовано. По коли вартість альтернативних маршрутів навіть незначно гірше, чим у найкоротшого маршруту, цей інструмент не працює.

Ще один недолік традиційних методів маршрутизації трафіка в мережах IP полягає в тому, що шляхи вибираються без обліку поточного завантаження ресурсів мережі. Якщо найкоротший шлях уже перевантажений, то пакети однаково будуть посилати цим шляхом. Так, у мережі, зображеної на рисунку 1.3, верхній шлях задіється й у тому випадку, якщо його ресурсів постійно не вистачає для обслуговування трафіка від A до E нижній простоює, незважаючи на те, що ресурсів маршрутизаторів B та C вистачило б для якісної передачі трафіка. У наявності явний недолік методів розподілу ресурсів мережі – одні з них працюють із перевантаженням, а інші не використовуються зовсім. Ніякі методи QoS дану проблему розв'язати не можуть – потрібні якісно інші механізми. Одним з модних, але не застосовуваних раніше в мережах IP методів впливу на ефективне використання ресурсів мережі є технологія Traffic Engineering (TE), або в дослівному перекладі "інжиніринг трафіка". Під TE розуміються методи й механізми досягнення збалансованості завантаження всіх ресурсів мережі за рахунок раціонального вибору шляхів проходження трафіка через мережу. Постановку завдання відповідно до такого розуміння технології TE ілюструють рисунки 1.4 і 1.5.

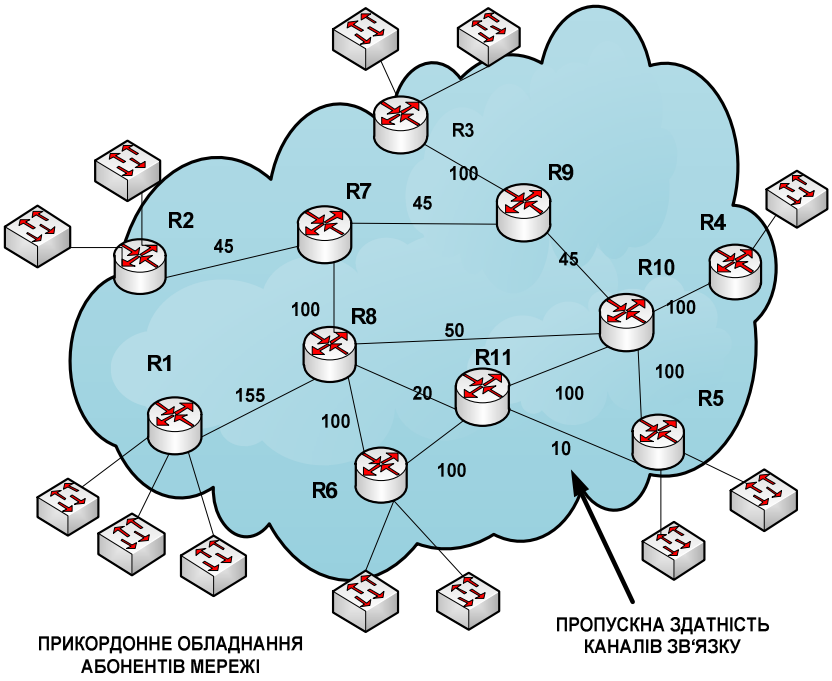

Рисунок 1.4 – Топологія мережі й продуктивність її ресурсів

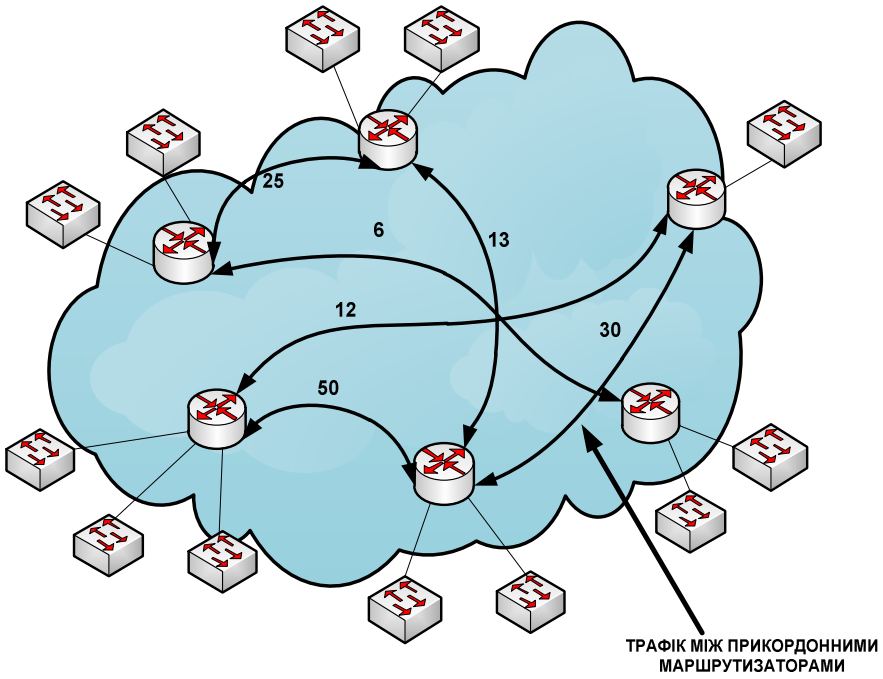

Рисунок 1.5 – Навантаження між прикордонними маршрутизаторами

Вихідними даними для вибору шляхів є, по-перше, характеристики передавальної мережі – топологія, а також продуктивність складових її

маршрутизаторів і каналів зв'язки (рисунок 1.4), а по-друге, відомості про навантаження мережі, тобто про потоки трафіка, які вона повинна передати між своїми прикордонними маршрутизаторами (рисунок 1.5).

Кожний потік характеризується точкою входу в мережу, точкою виходу з неї й деякими параметрами трафіка. Тому що при виборі шляхів прагнуть забезпечити рівномірне завантаження маршрутизаторів і каналів зв'язки, то для кожного потоку, як мінімум, потрібно враховувати його середню інтенсивність (рисунку 1.5).

Для більш тонкої оптимізації трафіка в мережі можна залучати й більш детальний опис кожного потоку: наприклад, величину можливої пульсації трафіка або вимоги до якості обслуговування - чутливість до затримок, варіації затримок і припустимий відсоток втрат пакетів. Однак, оскільки оцінити такого роду параметри трафіка більш складно, ніж середню інтенсивність, а їх вплив на функціонування мережі менш значно, звичайно при знаходженні оптимального розподіл шляхів проходження потоків через мережу враховуються тільки параметри їх середньої інтенсивності.

Завдання інжинірингу трафіка ТЕ полягає у визначенні маршрутів потоків трафіка через мережу, тобто для кожного потоку потрібно вказати точну послідовність проміжних маршрутизаторів і їх інтерфейсів на шляху між вхідною й вихідною точкою потоку. При цьому всі ресурси мережі повинні бути завантажені як можна більш збалансовано. Ця умова можна формалізувати різними способами. Наприклад, максимальний коефіцієнт використання ресурсу по всіх ресурсах мережі повинен бути мінімальний, щоб трафіку був нанесений як можна менший збиток. Саме так формулюється завдання ТЕ в RFC 2702 "Requirements for Traffic Engineering Over MPLS". У даному документі, що містить загальні рекомендації Інженерної групи підтримки Інтернет IETF (The Internet Engineering Task Force) за рішенням завдань ТЕ за допомогою технології комутації по мітках MPLS, у якості цільової функції оптимізації шляхів запропоноване вираження:

$$\min (\max Ki) \qquad (1.1)$$

де K_i – коефіцієнт використання ресурсу.

Іншим способом постановки завдання ТЕ може бути пошук такого набору шляхів, при яких усі значення коефіцієнтів використання ресурсів не будуть перевищувати деякий заданий поріг K_{ax}. Подібний підхід більш простий у реалізації, тому що пов'язаний з перебором меншої кількості варіантів, тому він частіше застосовується на практиці. Термін ТЕ має й більш широке трактування, коли під ним розуміється глобальна оптимізація мережі за рахунок зміни всіх можливих параметрів: кількості й продуктивності маршрутизаторів, топології зв'язків між ними, швидкостей каналів передачі даних, пріоритетів обслуговування потоків тощо. У набір керованих параметрів включаються також і параметри навантаження: наприклад, інтенсивності переданих мережею потоків – у випадку перевантаження мережі їх можна обмежити до деякої величини, щоб затори зменшилися до прийнятного рівня. Такий глобальний підхід прийнятий в основному документі робочої групи Traffic Engineering (TEWG) RFC 3272 "Overview and Principies of Internet Traffic Engineering". У зазначеному документі в технологію ТЕ включаються методи трьох основних тимчасових масштабів (рисунок 1.6):

1. Управління в реальному масштабі часу, коли параметри змінюються з періодом у кілька секунд і навіть мілісекунд. До цього типу ставляться методи забезпечення якості обслуговування в маршрутизаторах різні дисципліни, що використовують, обслуговування черг, що й оперують кожним окремим пакетом.

2. Оперативне управління параметрами з періодичністю в кілька хвилин або днів. Сюди входять і методи вибору шляхів проходження трафіка через мережу, у якій шляхи проходження трафіка варіюються тільки в тому випадку, коли виміру показують стійка зміна інтенсивностей потоків протягом кількох годин або днів.

3. Планування мережі, що регламентує зміни параметрів мережі один раз у кілька тижнів або місяців. У цьому випадку в якості параметрів виступають структурні характеристики мережі: кількість і типи маршрутизаторів, топологія й типи каналів зв'язки, а також інші параметри, зміна яких вимагає більших витрат часу й засобів.

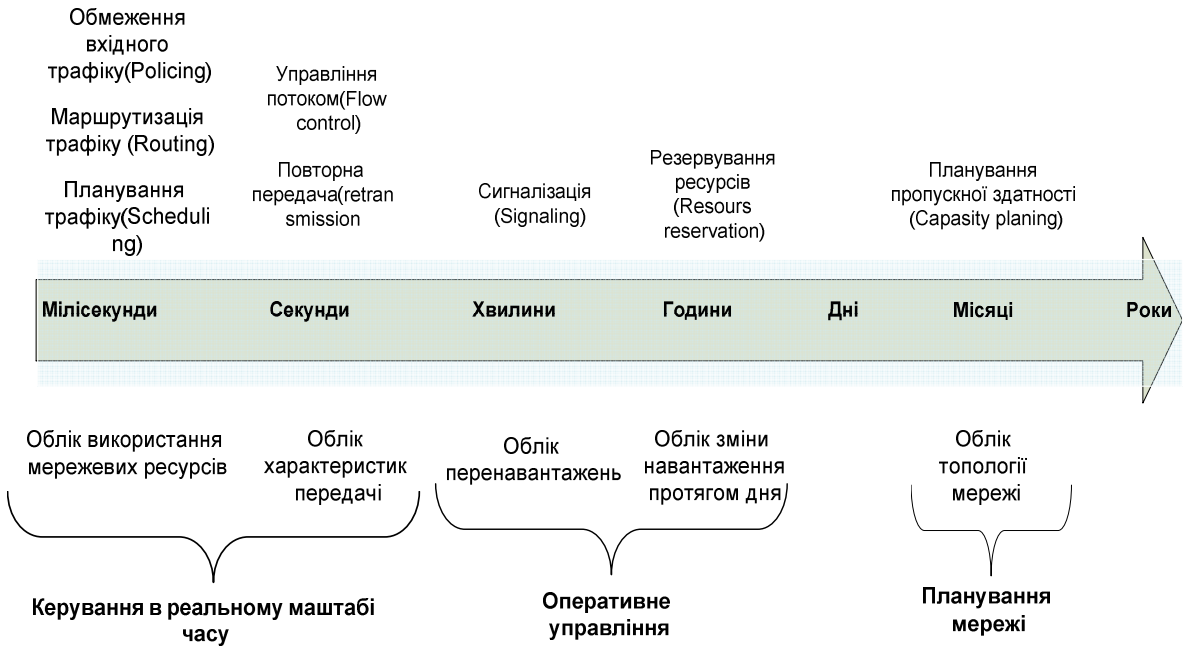

Рисунок 1.6 – Часові масштаби інжинірингу трафіка в IP-мережах

У загальному випадку при інжинірингу трафіка управління шляхами проходження потоків трафіка через мережу виступає в якості тільки одного з методів оптимізації мережі, застосовуваних поряд з іншими. Так у документі IETF "A Framework of Network Engineering" статус, що має, Internet Draft, із усіляких методів оптимізації мережі вичленовано два основні класи:

- методи мережної інженерії (Network Engineering), що виконують оперативну зміну пропускної здатності фізичних каналів між маршрутизаторами;

- методи планування мережі (Network Planning) більш довгочасні розв'язки, що реалізують, засновані на зміні кількості маршрутизаторів у мережі, їх продуктивності й топології фізичних каналів.

При цьому термін Traffic Engineering використовується в більш вузькому змісті – як вибір шляхів проходження трафіка через мережу. В роботі основна увага приділена методам планування мережі, які працюють у третьому тимчасовому масштабі, тому що при наданні послуг VPN її характеристики задаються на досить тривалий проміжок часу.

Слід зазначити, що на практиці ідеї TE застосовуються поки тільки для підтримки способів управління шляхами проходження потоків трафіка через мережу. При цьому основним інструментом вибору й установлення шляхів у мережах IP сьогодні є технологія MPLS. Вона використовує й розбудовує концепцію віртуальних каналів у мережах Frame Relay і ATM, поєднуючи її з технікою вибору шляхів на основі інформації про топологію й поточному завантаженню мережі, одержуваної за допомогою протоколів маршрутизації мереж IP.

Технологія MPLS TE вже досить добре стандартизована в ряді документів IETF і підтримується більшістю провідних виробників устаткування для мереж IP. Саме ця технологія, як найбільше далеко просунувся на шляху практичної реалізації TE, найбільшою мірою підходить для реалізації основних моделей і методів планування VPN.

Очевидно, що пошук шляхів TE по черзі знижує якість розв'язку при одночасному розгляді всіх потоків можна знайти більш раціональне завантаження ресурсів. У прикладі, показаному на рисунку 1.7, обмеженням є максимально припустиме значення коефіцієнта використання ресурсів, рівне 0,65. У варіанті 1 рішення було знайдено при черговості розгляду потоків 1 → 2 → 3. Для першого потоку був обраний шлях A – B – C, тому що в цьому випадку він, з одного боку, задовольняє обмеженню (усі ресурси уздовж шляху – канали A – B, A – C і відповідні інтерфейси маршрутизаторів виявляються завантаженими на 50/155 = 0,32), а з іншого – має мінімальну метрику (65+65 = 130). Для другого потоку також був обраний шлях A – B – C, тому що й у цьому випадку обмеження задовольняється – результуючий коефіцієнт використання виявляється рівним 50+40/155 = 0,58. Третій потік

направляється по шляху A – D – E – C і завантажує ресурси каналів A – D, D – E і E – E – C на 0,3. Варіант 1 можна назвати задовільними, тому що коефіцієнт використання будь-якого ресурсу в мережі не перевищує 0,58.

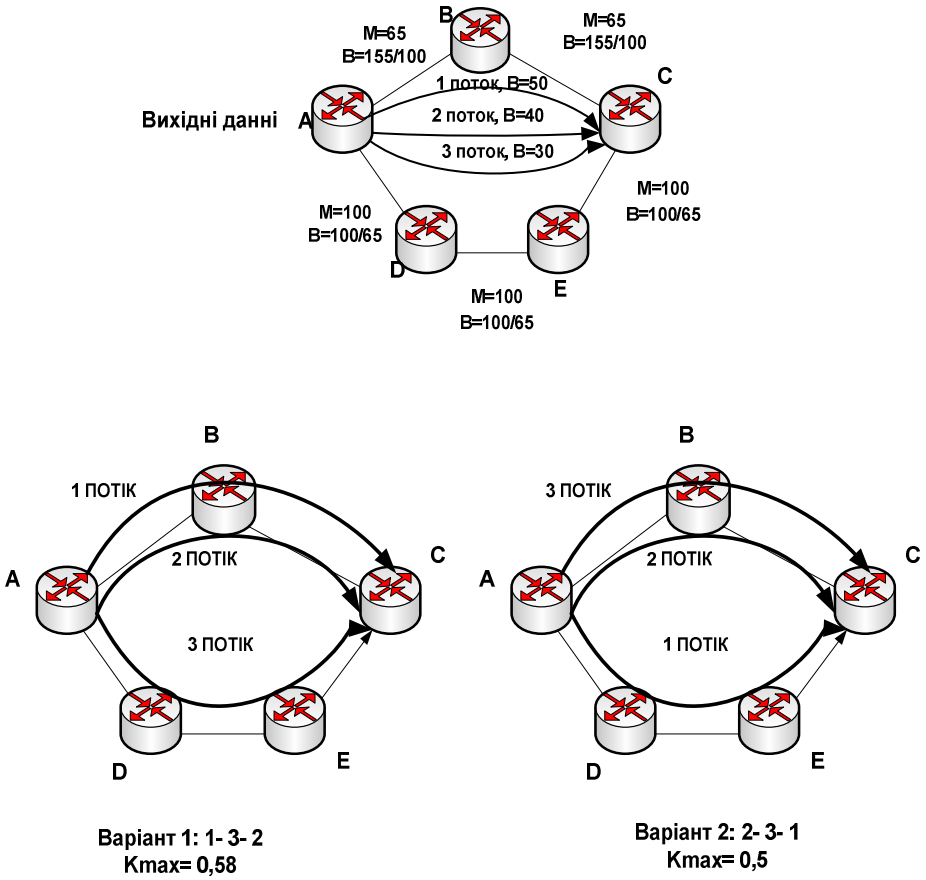

Рисунок 1.7 – Вплив порядку розгляду потоків на якість рішення

Однак існує кращий спосіб, представлений у варіанті 2. Тут по верхньому шляхові A – B – C були спрямовані потоки 2 і 3, а потік 1 – по нижньому шляху A – D – E – C. Ресурси верхнього шляху виявляються завантажено на 0,45, а нижнього – на 0,5, тобто в наявності більш рівномірне завантаження ресурсів, а максимальний коефіцієнт використання по всіх ресурсах мережі не перевищує 0,5. Цей варіант може бути отриманий при одночасному розгляді всіх трьох потоків з урахуванням обмеження min (max). До або ж при розгляді потоків по черзі в послідовності 2 → 3 → 1.

Слід зазначити, що у виробленім сьогодні встаткуванні застосовується варіант MPLS TE з послідовним розглядом потоків. Він простіше в реалізації й ближче до стандартних для протоколів OSPF і IS-IS процедурам знаходження найкоротшого шляху для однієї мережі призначення (у відсутності обмежений знайдений розв'язок для набору найкоротших шляхів не залежить від послідовності розгляду мереж, для яких проводився пошук). Крім того, при зміні ситуації – появі нових потоків або зміні інтенсивності існуючих - знайти шлях вдається тільки для одного потоку.

Однак у принципі можливий спосіб знаходження оптимального розв'язку для набору потоків зовнішньої стосовно мережі системою, в автономному режимі. Ця система повинна включати підсистему розрахунків і, можливо імітаційного моделювання, і враховувати не тільки середні інтенсивності потоків, але і їх пульсації, і оцінити не тільки завантаження ресурсів, але й результуючі параметри QoS – затримки, втрати й т.п. Після знаходження оптимального розв'язку його можна модифікувати вже в оперативному режимі пошуку шляхів " по одному". Розробці математичних моделей і алгоритмів, що є основою функціонування такої системи планування мережі й присвячена дисертація. Основна увага приділена дослідженню питань управління ресурсами мережі загального користування з метою оптимальної реалізації віртуальних приватних мереж, як з погляду постачальників, так і споживачів послуг VPN.

1.4 Розробка загальної архітектура системи експлуатаційної підтримки VPN

У процесі життєвого циклу послуг VPN провайдер повинен мати можливість реалізовувати наступні функції (рисунок 1.8):

1. Введення даних про послугу VPN – одержання вихідної інформації про необхідну послугу від замовника й уведення її в систему автоматизованої підтримки послуг VPN. Тут можливі різні варіанти реалізації даної функції -

уведення інформації через автоматизоване робоче місце системи, за допомогою імпорту даних або через інтерфейс OSS для автоматизованого обміну інформацією з додатками користувача.

2. Модифікація VPN – можливість додавання нових географічних точок, пристроїв і функцій у віртуальній мережі, зберігаючи при цьому всю існуючу функціональність VPN.

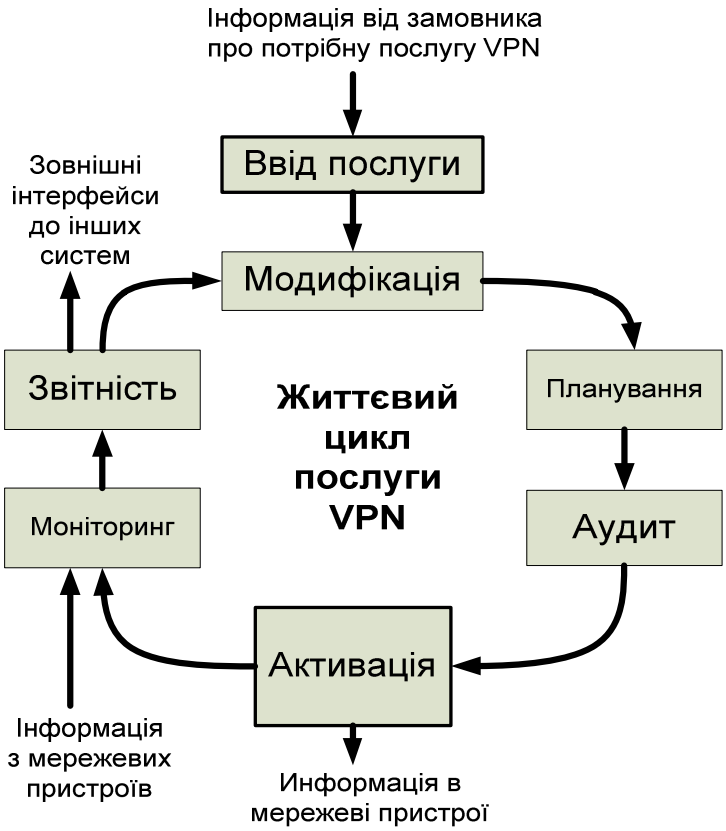

Рисунок 1.8 – Життєвий цикл послуг VPN

3. Планування VPN – розподіл доступних мережних ресурсів на стадії створення VPN для виконання специфічних вимог, при цьому створені раніше VPN не зачіпаються й безупинно функціонують у колишньому режимі.

4. Аудит VPN – перевірка доступності всіх необхідних мережних ресурсів і можливості функціонування віртуальної мережі в заданій конфігурації.

5. Активація VPN – передача конфігураційної інформації в мережні пристрої для реалізації планованої VPN.

6. Моніторинг VPN – після настроювання встаткування й запуску послуги здійснюється контроль функціонування мережних пристроїв з метою забезпечення повної працездатності віртуальної мережі.

7. Звітність по VPN – формується оперативна й статистична звітність про всі аспекти функціонування VPN, що дозволяє забезпечити високу доступність і якість надання послуги. Можливо також взаємодія з різними автоматизованими системами провайдера (білінговими, CRM, BSS і ін.) через прикладний програмний інтерфейс API.

Для автоматизації процесів адміністрування й настроювання мереж загального користування з метою ефективного надання корпоративним клієнтам послуг віртуальних приватних мереж пропонується використовувати спеціальну систему підтримки експлуатаційної діяльності провайдерів послуг VPN – VPN-OSS (Operations Support System).

Система VPN-OSS повинна підтримувати реалізацію наступних функцій:

- зберігання даних технічного обліку й топології пакетної мережі загального користування й реалізованих VPN;
- моніторинг зайнятої й доступної смуги пропускання й характеристик окремих ланок пакетної мережі загального користування затримок (затримки пакетів, джиттер, відсоток втрат пакетів, коефіцієнт готовності тощо);
- зберігання, аналіз і видача даних про характеристики трафіка пакетної мережі загального користування й реалізованих VPN;
- балансування завантаження пакетної мережі загального користування за допомогою відповідного конфігурування мережних пристроїв; – автоматизація й спрощення завдань оптимального планування й конфігурування VPN.

Система VPN-OSS складається з наступних функціональних підсистем (рисунок 1.9):

- підсистема вимірів пропускної здатності й затримок у мережі загального користування;
- підсистема даних про мережу загального користування;
- підсистема мережної топології;
- підсистема планування VPN;
- підсистема конфігурування VPN;
- підсистема прийняття замовлень.

Рисунок 1.9 – Архітектура системи VPN-OSS

Підсистема вимірів мережі забезпечує моніторинг IP-мережі й включає наступні виміри:

- наявної смуги пропускання каналів мережі загального користування;
- використаної смуги пропускання потоку VPN (кожний потік ідентифікується парою адрес вузлів джерела/одержувача);
- величини затримки від краю до краю між вузлами мережі.

У підсистемі вимірів для збору інформації в мережі можуть бути використані наступні основні механізми й протоколи:

- для виміру наявної смуги пропускання (пропускної здатності) ланки (каналу) мережі – простий протокол управління мережею SNMP (Simple Network Management Protocol);

- для виміру задіяної смуги пропускання потоку;

- технологія вилученого моніторингу мережі RNMON (Remote Network Monitoring), технологія Netflow (фірми Cisco);

- для виміру затримок – пробні пакети (маршрутизуються з використанням джерела трафіка).

При проведенні вимірів у мережі IP необхідно враховувати той факт, що використання повідомлень SNMP і Netflow може сильно вплинути на продуктивність маршрутизаторів (зменшення її до 20%), тому що переданий службовий трафік створює додаткове навантаження на мережу.

У підсистемі даних мережі зберігаються наступні дані, що збираються в мережі:

- пропускна здатність ланок (каналів) мережі;

- задіяна смуга пропускання потоків;

- затримка від краю до краю;

- підсистема мережної топології призначена для;

- автоматичного відстеження стану поточних активних мережних вузлів і їх інтерфейсів;

- автоматичного відстеження стану з'єднань мережних вузлів на 2-му рівні моделі OSI;

- підтримки мережної бази даних, що містить архівні й поточні дані про елементи мережі і їх з'єднаннях;

- пошуку й видачі інформації про зміни топології мережі загального користування.

Знання мережної топології необхідно для розв'язку багатьох завдань технічної експлуатації, і, насамперед для інжинірингу трафіка, визначення кореляцій подій у мережі, аналізу першопричин подій, управління мережною конфігурацією.

Необхідність автоматизації процесів відстеження стану мережної топології обумовлена наступними причинами:

- мережа зв'язку є динамічною системою, стан якої міняється досить часто;
- великі мережі загального користування включають сотні вузлів і тисячі ланок;
- ручне відстеження стану мережної топології є вкрай трудомісткою й приводить до частих помилок.

Основні підходи, які повинні використовуватися в підсистемі мережної топології:

- зберігання даних про всі вузли й інтерфейсах даного мережного сегмента;
- використання інформаційної бази даних MIB (Management Information Base) для одержання списків вузлів, у яких зазначені всі порти кожного вузла;
- для кожного порту кожного вузла генерація списку вузлів, з якими зв'язаний цей порт;
- використання алгоритмів генерації топології, що дозволяють одержувати карту мережі даного мережного сегмента.

Підсистема планування віртуальних приватних мереж призначена для оптимізації використання ресурсів мережі загального користування з мінімізацією резервуємої смуги пропускання для кожної реалізованої VPN з обліком раніше реалізованих віртуальних мереж. У даній підсистемі Б залежності від виставлених вимог замовника можуть використовуватися різні моделі й методи реалізації VPN. Основними відмінними рисами пропонованої підсистеми планування VPN є:

- перша система, що використовує різні моделі реалізації VPN;
- оригінальні алгоритми для оптимального резервування смуги пропускання в мережі загального користування з метою маршрутування трафіка VPN;

- стандартні протоколи для сигналізації й резервування ресурсів пакетної мережі загального користування.

Підсистема конфігурування VPN призначена для формування необхідної маршрутної інформації залежно від використовуваного протоколу або механізму маршрутизації пакетів і передачі її в устаткування мережі загального користування. У підсистемі можуть бути використані наступні механізми для реалізації віртуальних мереж:

- ваги протоколу динамічної маршрутизації OSPF (Open Shortest Path First);
- політики протоколу граничного шлюзу BGP (Border Gateway Protocol);
- тунелі MPLS.

Підсистема конфігурування безпосередньо взаємодіє з мережним устаткуванням і забезпечує автоматизацію підтримки маршрутних таблиць у вузлах мережі.

Підсистема взаємодії реалізує інтерфейс "оператор - система" і забезпечує введення необхідної інформації про, що замовляється послузі VPN (перелік кінцевих точок віртуальної мережі, необхідна зв’язність у мережі, величина й тип переданого трафіка й ін.).

В роботі основна увага приділена розробці методів реалізації підсистеми планування VPN як найбільш важливому й теоретично складному завданню при організації експлуатаційної підтримки послуг VPN.

1.5 Розробка моделей реалізації VPN

1.5.1 Канальна модель VPN

Розподіл ресурсів мережі загального користування по різних віртуальних приватних мережах може бути реалізоване за допомогою класичного підходу емуляції приватних ліній від однієї кінцевої точки VPN

до всіх інших кінцевих точок (сайтам). Такий підхід використовує так звану канальну модель (в англомовній літературі – pipe model). У деяких роботах використовується також термін "VPN точка-точка" (point-to-point VPN) для опису VPN на основі потокової моделі. Канальна модель VPN подібна послузі орендованої (приватної) лінії. Це вимагає від користувача орендувати набір приватних віртуальних каналів і запросити відповідну смугу пропускання в кожному каналі протягом усього шляхе між парою кінцевих точок "джерело-одержувач" в VPN. Рисунок 1.10 ілюструє приклад канальної моделі VPN.

Мережний провайдер повинен забезпечувати адекватну смугу пропускання уздовж усього шляху для кожного каналу, гарантуючи виконання SLA.

Головний недолік такого підходу в тому, що користувач повинен попередньо знати всю матрицю трафіка між кінцевими точками VPN.

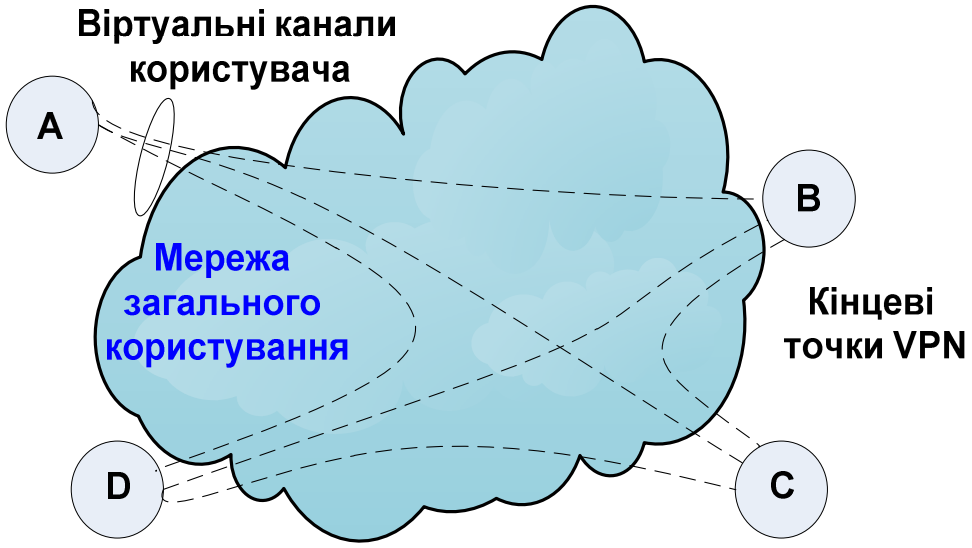

Рисунок 1.10 – VPN на основі канальної моделі

Крім того, мережні ресурси, задіяні для одного користувацького каналу, не можуть бути використані для передачі іншого трафіка. Це дуже важливо для мережного провайдера, тому що він не може одержати вигоду за

рахунок статистичного мультиплексування в одному каналі користувацький інформації від різних джерел.

Основною проблемою побудови VPN на базі канальної моделі є оптимальний розподіл мережних ресурсів по різних каналах. У випадку необмеженої смуги пропускання на кожній ділянці мережі це завдання зводиться до вирішення ізольованих завдань вибору оптимальної топології кожної VPN з урахуванням відповідного критерію оптимізації: сумарної вартості використовуваної смуги пропускання, сумарної довжини каналів або ін. При цьому вирішення такого завдання для однієї VPN не впливає на рішення завдання оптимізації для інший VPN.

1.5.2 Потокова модель VPN

В протилежність канальній моделі в потоковій моделі не потрібно знання матриці трафіку віртуальної мережі, необхідно тільки вказати сумарний трафік на вході і виході кожної кінцевої точки VPN. На рисунку 1.11 показаний приклад реалізації VPN на базі потокової моделі. Припустимо, в VPN є чотири кінцеві точки: A, B, C і D. Користувачі орендують чотири потоки для кожної кінцевої точки і визначають для них агрегований витікаючий трафік, що входить.

Переваги використання потокової моделі VPN, з точки зору користувачів, наступні:

Простота опису VPN. Для кожної кінцевої точки мають бути визначені тільки сумарні вхідна та вихідна смуги пропускання (можливо, асиметричні) в протилежність визначення смуг пропускання для кожного призначеного для користувача каналу між парами кінцевих точок в канальній моделі VPN.

Гнучкість розподілу трафіку. Трафік від/до цієї кінцевої точки VPN в потоці може бути розподілений довільно по інших кінцевих точках, забезпечуючи в цілому агреговане узгодження з резервованою смугою пропускання потоку.

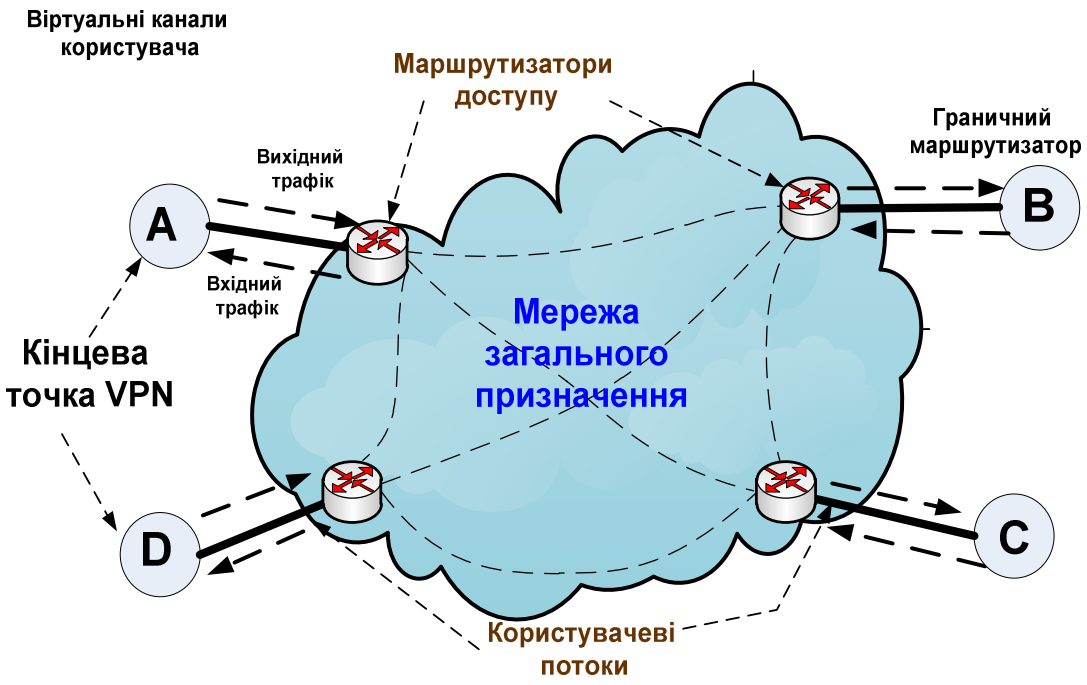

Рисунок 1.11 – VPN на основі потокової моделі

Вигода від мультиплексування навантаження в потоці. Завдяки статистичному мультиплексуванню трафіку смуга пропускання потоку може бути менше, ніж сумарна смуга пропускання, потрібна для усього набору каналів користувачів.

Простота визначення параметрів потоку. Характеристики потоку легко визначити, оскільки статистичні зміни в індивідуальному трафіку для кожної пари "джерело – одержувач" згладжуються шляхом агрегації трафіку в потоці.

З точки зору провайдерів, потокова модель VPN також являється привабливішої завдяки можливості підтримки SLA з менш жорстким описом матриці трафіку. Для управління ресурсами мережі загального користування при великій невизначеності матриці трафіку можуть бути використаний два основні механізми:

Статичне мультиплексування. Завдяки зменшенню вимог на агреговану смугу пропускання провайдер може використовувати мультиплексування

різних потоків трафіку, які мають однакові характеристики QoS. При цьому можливі три різні рівні агрегації. Перший – мультиплексується увесь трафік одного потоку, що має однакові параметри QoS. Другий – мультиплексуються окремі потоки, що мають однакові параметри QoS. Третій – мультиплексується трафік різних VPN, що має однакові параметри QoS. Ці три способи можуть бути застосовані як до каналів доступу, так і до внутрішніх каналів в мережі загального користування.

Зміна меж резервованої смуги пропускання. Для забезпечення відповідних гарантій параметрів QoS провайдер може використовувати механізм резервування агрегованих мережних ресурсів, який розподіляє смугу пропускання на використовуваних ділянках мережі загального користування для цього потоку або VPN.

Провайдер може робити розподіл смуги пропускання статично, на основі розрахунків найгіршого випадку навантаження. Крім того, провайдер може виконати деякий початковий розподіл смуги пропускання і потім змінювати цю смугу динамічно на основі цих періодичних (online) вимірів.

Слід зазначити, що ці два механізми управління ресурсами мережі можуть використовуватися окремо або спільно.

Порівняння характеристик канальної і потокової моделей VPN наведено в таблиці 1.1.

Однак на практиці окремі ділянки мережі завжди мають обмежену пропускну здатність і в цьому випадку смуга пропускання, зайнята під одну VPN, впливає на рішення завдання розподілу мережних ресурсів для інший VPN. Облік цього фактору суттєво ускладнює математичні методи дослідження потокової моделі VPN.

Таблиця 1.1 – Характеристики канальної й потокової моделі VPN

Характеристики	Канальна модель VPN	Потокова модель VPN
Поділ мережних ресурсів	Окремі канали "точка-крапка" для кожної пари кінцевих крапок VPN	Єдиний потік для доступу в мережу кожного користувача VPN
Спосіб резервування смуги пропускання в мережі загального користування	Статичне заняття смуги в каналі	Можливо динамічна зміна смуги пропускання потоку на вимогу
Сигналізація	Не потрібно	Потрібно при зміні резервуємої смуги пропускання
Матриця трафіка	Необхідна інформація про трафике між кожною парою кінцевих крапок VPN	Не потрібно
Облік змін трафіка	Використовується пікове значення трафіка	Використовується прогноз трафіка
Алгоритмічна складність	Відсутня	Складні алгоритми реалізації VPN
Управління доступом	Детерміноване, одноразове	Необхідний розрахунок розподілу потоків по ланках мережі для кожної зміни необхідної смуги пропускання
Виграш від мультиплексування	Немає	Статичний виграш через агрегування трафіка на рівні потоку

1.6 Постановка завдання дослідження

У загальному випадку завдання планування VPN полягає у визначенні мінімально необхідної смуги пропускання на окремих ділянках мережі для забезпечення передачі трафіка певної величини між заданими парами кінцевих точок VPN. Тому що при використанні смуги пропускання в мережі загального користування необхідно враховувати її вартість, то вирішення завдання планування VPN необхідно виконувати з урахуванням мінімізації витрат. Крім цього, сумарні резервуємі мережні ресурси для різних VPN не повинні перевищувати обмежень на смугу пропускання окремих ділянок мережі загального користування.

Критичне припущення в канальній моделі – що матриця трафіка Y для всіх пар кінцевих точок $(i, j) \in P$ відома заздалегідь.

Однак у сучасних мережах з декількома додатками, коли телекомунікаційні вимоги часто змінюються згодом, матрицю трафіка важко задати заздалегідь. Як вказувалося вище, для подолання цього недоліку можна використовувати потокову модель реалізації VPN, яка забезпечує більшу гнучкість у передачі трафіка. У цій моделі задаються потоки Bi^{in} і Bj^{out} як сумарні величини трафіків кожної кінцевої точки, який вона може ухвалювати й передавати, і в VPN необхідно забезпечити підтримку будь-якої припустимої матриці трафіка з урахуванням резервування відповідних смуг пропускання на окремих ланках мережі.

Вирішення завдання планування VPN при використанні потокової моделі допускає багато варіацій залежно від додаткових обмежень на реалізацію потоків у мережі й, особливо від топології VPN.

В роботі розглянуто три основні типи обмежень:

- структурні обмеження – коли VPN має спеціальну топологію, наприклад, у вигляді дерева;

- не розподільні потоки – коли для будь-якої припустимої матриці трафіка і будь-якої пари кінцевих точок із трафіком $y_{ij} > 0$ потік маршрутизується по єдиному шляхові.

- розподільні потоки – коли використовується розподіл потоків на кілька частин, тобто для будь-якої припустимої матриці трафіка Y і будь-якої пари кінцевих точок (y) із трафіком $y_{ij} > 0$ потік маршрутизується по декільком шляхам.

Таким чином, у самому загальному випадку завдання оптимального планування VPN на базі потокової моделі в термінах теорії графів можна сформулювати в таким чином.

Задано:

- граф мережі G з набором вершин V і ребер E, доступною смугою пропускання L_{uv} і питомою вартістю смуги пропускання S_{uv} для кожного ребра $(u, v) \in E$;

- для кожної кінцевої точки VPN $I \in P$ пари максимальних значень трафіка на вході й виході Bi^{in} і $Bj^{out} \in Z$.

Знайти:

- величину резервуємої смуги пропускання Cuv для кожного ребра (u,v) с сумарною мінімальною вартістю реалізації VPN S_{VPN};

- маршрут R_{ij} у графові G для передачі трафіка y_{uv} по ребру (uv), при цьому повинна підтримуватися будь-яка припустима матриця трафіка Y_{VPN}, що задовольняє потоку з кінцевої точки VPN і у кінцеву точку j, що й направляється по маршруту $R_{ij.}$

Таким чином, поставлене завдання має й безперервні й дискретні аспекти. Необхідно зарезервувати відповідну смугу пропускання на кожному ребрі, при цьому повинен бути заздалегідь визначений такий фіксований шлях R_{ij}, щоб маршрутизувати потік F(i,j) для будь-якої матриці трафіка Y_{VPN}. Вимога про те, щоб кожний потік F(i,j) маршрутизувався по фіксованому шляхові R_{ij}, обумовлена необхідністю виконання гарантій по затримці й продуктивності, наприклад при наданні послуг VoIP (голос

поверх IP) потрібна передача інформації в реальному часі. Нарешті, фундаментальною особливістю даного завдання є те, що вибір шляхів і смуги пропускання повинен відповідати сукупності можливих сценаріїв трафіка – будь-якій припустимій матриці Y_{VPN}, яка не суперечить границям трафіка B^{in} і Bi^{out} у кожної і-ої кінцевої точки VPN, а також доступним смугам пропускання на кожному ребрі L_{UV}.

Загальна схема взаємозв'язку завдань планування VPN показано на рисунку 1.12. Вона містить два основні види завдань – синтезу й аналізу.

Рисунок 1.12 – Загальна схема взаємозв'язку завдань планування VPN

Завдання синтезу покликано визначити оптимальну топологію VPN з необхідною смугою пропускання ребер на підставі вихідних даних про топологію мережі, трафікі кінцевих точок VPN і способи реалізації VPN.

Вирішення завдання аналізу забезпечує перевірку можливості реалізації заданої матриці трафіка при обраній топології VPN і заданих шляхах передачі трафіка на базі доступних ресурсів мережі загального користування. Основна відмінність пропонованого в роботі підходу до дослідження моделей VPN – це комплексний облік характеристик як самих VPN, так і мереж загального користування, на базі яких ці віртуальні мережі реалізуються. Це, насамперед облік топології VPN і мережі загального користування, обмежень на мережні ресурси, повноти відомостей про розподіли трафіка кінцевих точок VPN, змін трафіка віртуальної мережі, можливих алгоритмів маршрутизації трафіка, переліку послуг, гарантій якості надаваних послуг QoS тощо.

Слід зазначити, що способи зменшення резервуючої смуги пропускання,для VPN можуть застосовуватися навіть тоді, коли мережа не надає можливості реагувати на зміни трафіка. Наприклад, коли топологія VPN статична й задана заздалегідь. Цей випадок особливо важливий для практики, тому що первісні запити на реалізацію VPN реалізуються саме в цьому режимі. При статичній маршрутизації потоків трафіка визначення оптимальної топології VPN є в ряді випадків складним теоретичним завданням.

Завдання реалізації потокових моделей VPN ще більш ускладнюється, якщо ресурси на окремих ділянках мережі мають обмеження, що найчастіше й відповідає практиці проектування й планування VPN.

Для компаній, що мають розгалужену, територіально рознесену структуру, важливим практичним завданням є одержання оцінок доцільності й ефективності застосування технології віртуальних приватних мереж. Запропоновані експертні моделі оцінок потреб корпоративних користувачів у послугах VPN і ухвалення рішення на вибір технологій реалізації віртуальної мережі.

2 РОЗРОБКА МОДИФІКОВАНОЇ ПОТОКОВОЇ МОДЕЛІ VPN ПРИ НАЯВНОСТІ ОБМЕЖЕНЬ НА МЕРЕЖНІ РЕСУРСИ

2.1 Вплив обмежень мережних ресурсів на реалізацію VPN

Усі розглянуті раніше потокові моделі VPN ґрунтувалися на припущенні, що будь-який обсяг смуги пропускання може бути зарезервований для пропуску трафіка на кожному ребрі в графі *G,* що моделює мережа загального користування. Однак у загальному випадку ребро *e* графа *G* може мати обмежену пропускну здатність L(*e)* і необхідно забезпечити виконання умови C(e) < *L(e),* де C(e) – необхідна смуга пропускання для передачі трафіка VPN. Якщо ця умова не виконується, то відбувається відхилення запиту на реалізацію послуги VPN. У цьому випадку стає актуальною завдання визначення таких алгоритмів планування VPN, які дозволять провайдерам зменшити ймовірність відхилення вступників запитів на реалізацію послуг віртуальних мереж.

Завдання розподілу смуги пропускання VPN може здійснюватися й в оперативному режимі ("online") розподілення, смуги пропускання для раніше прийнятих запитів впливає на можливість реалізації наступної VPN.

Однак зазначені роботи розглядають установлення тунелів з гарантованою смугою пропускання в мережах MPLS у режимі online стосовно для канальної моделі реалізації VPN.

Розглянемо потокову модель VPN з обліком того, що є обмеження на доступні ресурси на кожній ділянці мережі. Дана модель із урахуванням уведених позначень для випадку симетричного трафіка, загального виду маршрутування трафіка й статичного заняття смуги пропускання має вигляд *Sym/G/Fix/Stat.* Будемо розглядати випадок маршрутування трафіка між кожною парою кінцевих точок VPN по одному шляху в мережі (відсутній розподіл трафіка по декільком шляхам). Як звичайно, мережа описується за

допомогою неорієнтованого графа $G = (V,E)$, де V і E – множина вершин (відповідають маршрутизаторам мережі) і множина ребер (відповідають ділянкам мережі, що з'єднують сусідні маршрутизатори) відповідно. Нехай n и m позначають кількість елементів множин V і E відповідно. Позначимо через L доступну (вільну) смугу пропускання ребер і її величину на певному ребрі e $(e \in E)$ позначимо як $L(e)$.

Підмножина $AR=\{ar_1,ar_2,...,ar_p\}$ множини V $(AR \in V)$ є набором точок доступу до VPN (відповідають маршрутизаторам доступу), через які підключаються користувачі віртуальної мережі. Інакше кажучи, кожній кінцевій крапці VPN pj відповідає свій маршрутизатор доступу VPN з підмножини AR.

Граф G, зображений на рисунку 2.1, відповідає мережі загального користування провайдера послуг VPN. Вершини графа G (позначені на рисунку буквами від a до g) з множини V відповідають магістральним маршрутизаторам.

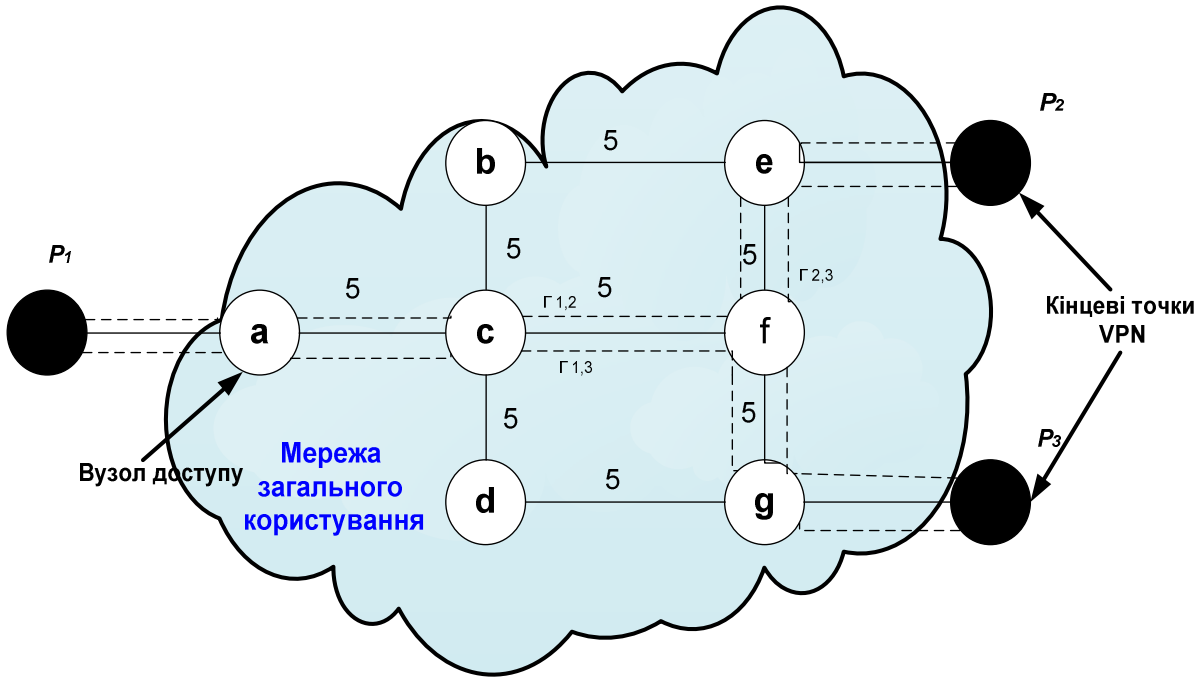

Рисунок 2.1 – Приклад графа мережі G

Суцільні лінії між двома вершинами відповідають неорієнтованим ребрам графа з множини *E*. Число, зазначене поруч із кожним ребром, відповідає величині доступної смуги пропускання в ньому (на рис.2.1 для простоти на всіх ребрах доступна смуга пропускання *L(e)* рівна 5 умовним одиницям). Підмножина вершин, через які здійснюється доступ користувачів послуг VPN до мережі загального користування $F = \{a, e, g\}$. Вершини, позначені цифрами p_1, p_2 і p_3, є кінцевими точками VPN, які одержують доступ до VPN через вузли доступу з підмножини *AR*. Пунктирні лінії на рисунок 2.1, позначені як r_y, є шляхами (маршрутами) передачі трафіка VPN між кінцевими точками p_i і p_j.

Вимоги клієнтів на надання послуги VPN будемо називати запитами на реалізацію VPN. Будемо розглядати ситуацію, коли трафік кожної кінцевої точки p_j є симетричним. Позначимо через $B(p_j)$ трафік кінцевої точки p_j і через L_{max} – максимально гарантовану смугу пропускання, забезпечувану сервісом-провайдером у мережі загального користування. Позначимо і-й запит на реалізацію VPN через z_i і він характеризує таку віртуальну приватну мережу, яку сервіс-провайдер повинен установити за заявкою клієнта. Кожний запит z_i – відображається за допомогою Р-кортежу вектора $(B_i, B_2, ..., B_p)$, де P – кількість вузлів доступу з множини *AR*. Число ненульових елементів у запиті z_i означає кількість кінцевих точок, що втримуються у відповідній віртуальній мережі. Значення j-го елемента B_j у запиті z_i, означає величину вхідного/вихідного трафіка кінцевої точки p_j.

Будемо розглядати ситуацію, коли:

- запити на реалізацію VPN надходять один за іншим незалежно;
- інформація про наступні запити на реалізацію VPN невідома.

Така інформація могла б містити в собі число майбутніх запитів на створення VPN і трафік кожної кінцевої точки. Фактично в цій ситуації сервіс-провайдер повинен обробити кожний запит на створення VPN в оперативному режимі ("online").

Ухвалюючи і-й запит на реалізацію VPN z_i сервіс-провайдер повинен перевірити, чи можлива реалізація запитуваної віртуальної мережі. Для цього необхідний відповідний алгоритм аналізу, який, по-перше, повинен визначити шлях між кожною парою кінцевих точок VPN і, по-друге, розподілити доступну смугу пропускання на кожному ребрі в обраному шляху. Якщо недостатньо наявної смуги пропускання, отриманий запит на реалізацію VPN z_i буде відхилений. У якості критерію для порівняння різних моделей VPN будемо використовувати коефіцієнт відхилення запитів на реалізацію VPN, який визначається відношенням:

$$A = Z_0 / Z, \tag{2.1}$$

де Z_0 – число відхилених запитів на реалізацію VPN;

Z – загальне число отриманих запитів на реалізацію VPN.

Таким чином, основною метою алгоритму реалізації VPN при обмежених мережних ресурсах є мінімізація коефіцієнта відхилення запитів *A*, що відповідає більшій кількості успішно реалізованих запитів у мережі.

Побудова методики реалізації VPN при обмеженій смузі пропускання окремих ділянок мережі засноване на відомім співвідношенні необхідних смуг пропускання для різних моделей VPN. Можна легко довести, що справедливо наступне співвідношення між величинами смуг пропускання *C*, зайнятими на кожному з ребер шляху, для різних моделей реалізації VPN: канальної C_k, потокової з урахуванням трафіка окремої VPN C_{VPN} і потокової з урахуванням трафіка всіх реалізованих VPN $C_{\sum VPN}$:

$$C_k > C_{VPN} / C_{\sum VPN}, \tag{2.2}$$

Слід зазначити, що дане співвідношення дійсне не тільки для займаної смуги пропускання на окремих ділянках мережі, але й для всієї сумарної резервуємої смуги пропускання для реалізації VPN.

Проілюструємо на конкретному прикладі відмінність між необхідною смугою пропускання в різних моделях реалізації VPN, для чого порівняємо канальну модель із потоковою моделлю, яка використовує деревоподібну топологію.

Допустимо, що спочатку провайдер одержує один запит на реалізацію VPN Z_1= (2, 2, 3), де цифри вказують трафік кінцевих точок в умовних одиницях. При використанні канальної моделі провайдер для кожної пари кінцевих точок відповідно до запиту z_1 організує схему реалізації VPN, показану на рисунку 2.2.

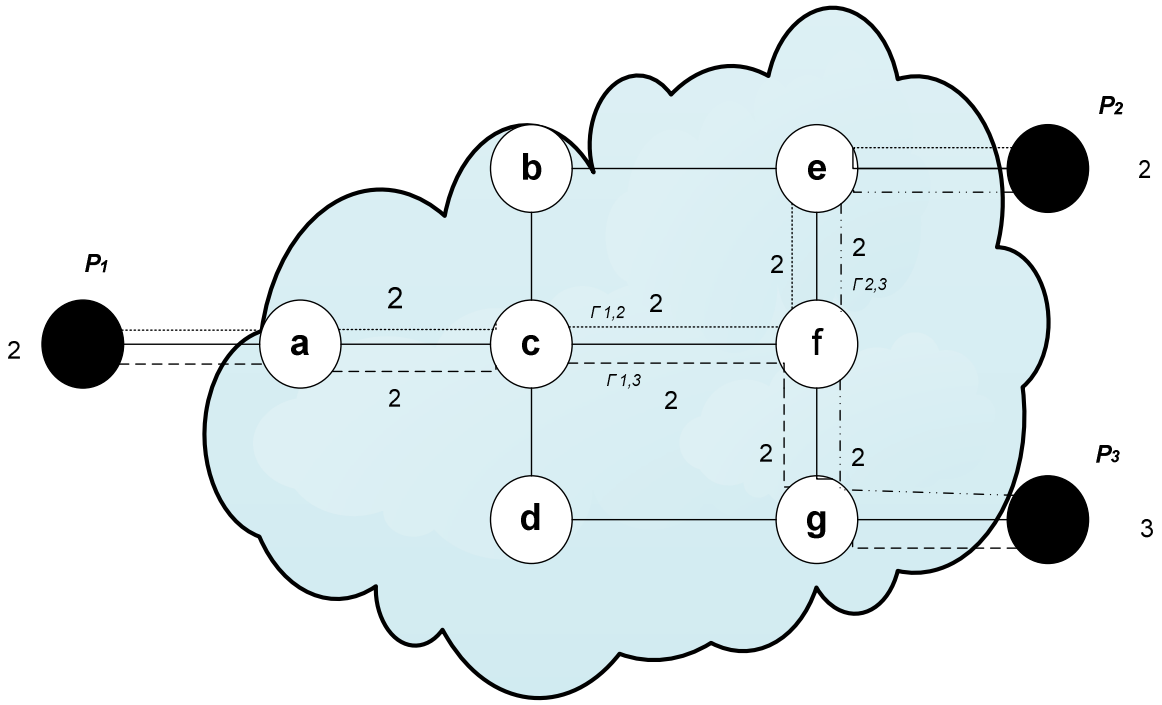

Рисунок 2.2 – Реалізація одного запиту на базі канальної моделі VPN

Числа, що перебувають поруч із трьома кінцевими точками VPN, характеризують сумарний трафік у них ($B(p_1)$, $B(p_2)$ і $B(p_3)$. Числа, що перебувають поруч із пунктирними лініями, характеризують обсяг

резервуємої смуги пропускання, необхідної для пропуску трафіка VPN на відповідних ребрах мережі. Відзначимо, що величини смуг пропускання, резервуючих на ребрах *(a,c), (c,f), (e,f)* і *(f,g),* рівняються 4-м умовним одиницям при використанні канальної моделі VPN, тоді як при використанні потокової моделі з деревоподібною топологією ці величини рівняються 2, 2, 2 і 3 відповідно. Таким чином, канальна модель VPN використовує більшу смугу пропускання на всіх ребрах. Наприклад, обсяг трафіка через ребро *(a,c)* у будь-який момент часу не перевищить min $(B(p_1),B(p_2)+B\{p_3)) = 2$. Однак у канальній моделі VPN на цьому ребрі резервується 4 одиниці смуги пропускання (подібне співвідношення характерне також для ребер *{c,f), {e,f)* і *(fgj).*

Розглянутий приклад показує відмінність між задіяними смугами пропускання в різних моделях при реалізації єдиної VPN. У випадку реалізації множини VPN відмінність резервуючих смуг пропускання в канальній моделі, потоковій моделі окремої VPN і потокової моделі для всіх VPN буде ще більш значним. Якщо пропускна здатність ребер *E* обмежена, то це приведе до збільшення коефіцієнта відхилення запитів А. Однак навіть потокова модель із деревоподібною топологією не може гарантувати необхідного значення коефіцієнта Δ.

Покажемо, що відсутність інформації про доступну смугу пропускання на ребрах мережі в рамках потокової моделі з деревоподібною топологією приводить до збільшення коефіцієнта відхилення. Допустимо, сервіс-провайдер одержує два запити на реалізацію VPN: $Z_1 = (2, 2, 3)$ $Z_2 = (3, 3, 3)$ (рис. 2.3). Нехай доступна смуга пропускання на всіх ребрах графа мережі становить 5 умовних одиниць. Вершина, позначена на рисунку 2.3 як p_{ij}, характеризує j - кінцеву точку запиту z_i. Число поруч із кожної кінцевою точкою $P_{i,j}$ відповідає трафіку й визначає вимогу до необхідної смуги пропускання.

При використанні потокової моделі з деревоподібною топологією дерева VPN, відповідні до запитів Z_1 і Z_2, зображені точкової й пунктирної

лініями відповідно. Числа поруч із цими лініями означають величини смуг пропускання, резервуючих на відповідних ребрах мережі.

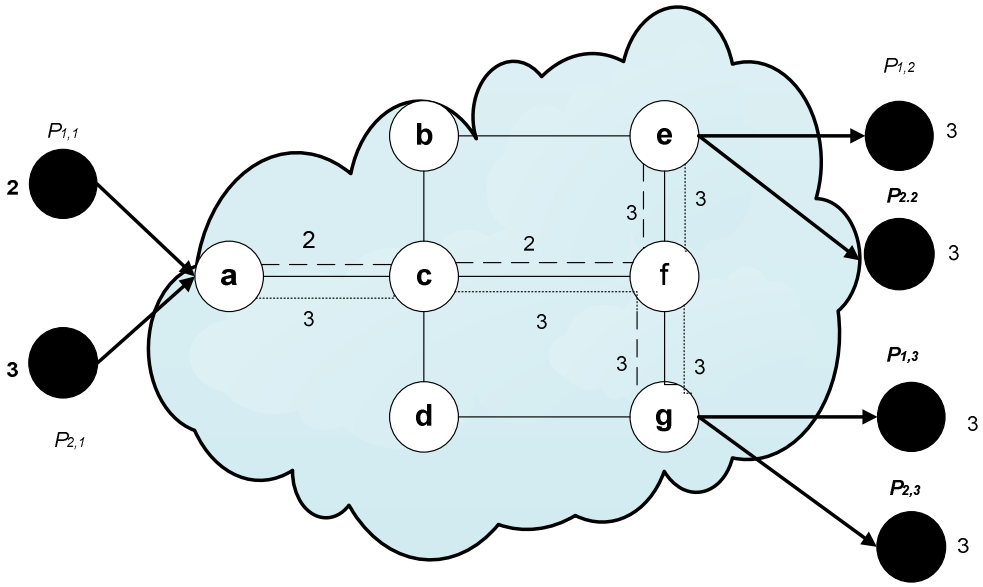

Рисунок 2.3 – Реалізація двох запитів на базі канальної моделі VPN

На рисунку 2.3 ні ребро *(e,f),* ні ребро *(f,g)* не мають необхідної смуги пропускання для другого запиту реалізації VPN після виділення ресурсу під перший запит. Коефіцієнт відхилення запитів Δ, отриманий при використанні потокової моделі з деревоподібною топологією, для розглянутого прикладу склав 50%.

Однак фактично наявних ресурсів смуги пропускання в мережі *G* досить для того, щоб обслужити обидва запити. Якщо побудувати дерево VPN для реалізації другого запиту Z_2, як це показано на рисунку 2.4 точковою лінією, то в цьому випадку обидва запити Z_1 і Z_2 можуть бути реалізовані. Коефіцієнт відхилення запитів у результаті такої зміни маршрутів передачі трафіка в VPN буде дорівнює нулю.

У потоковій моделі з деревоподібною топологією також можливе відхилення запитів на реалізацію VPN, навіть якщо наявних вільних ресурсів у мережі досить для їхньої обробки. Це відбувається через те, що алгоритм

синтезу даної моделі формує з ребер оптимальне дерево VPN без обліку наявної в наявності вільної смуги пропускання в мережі.

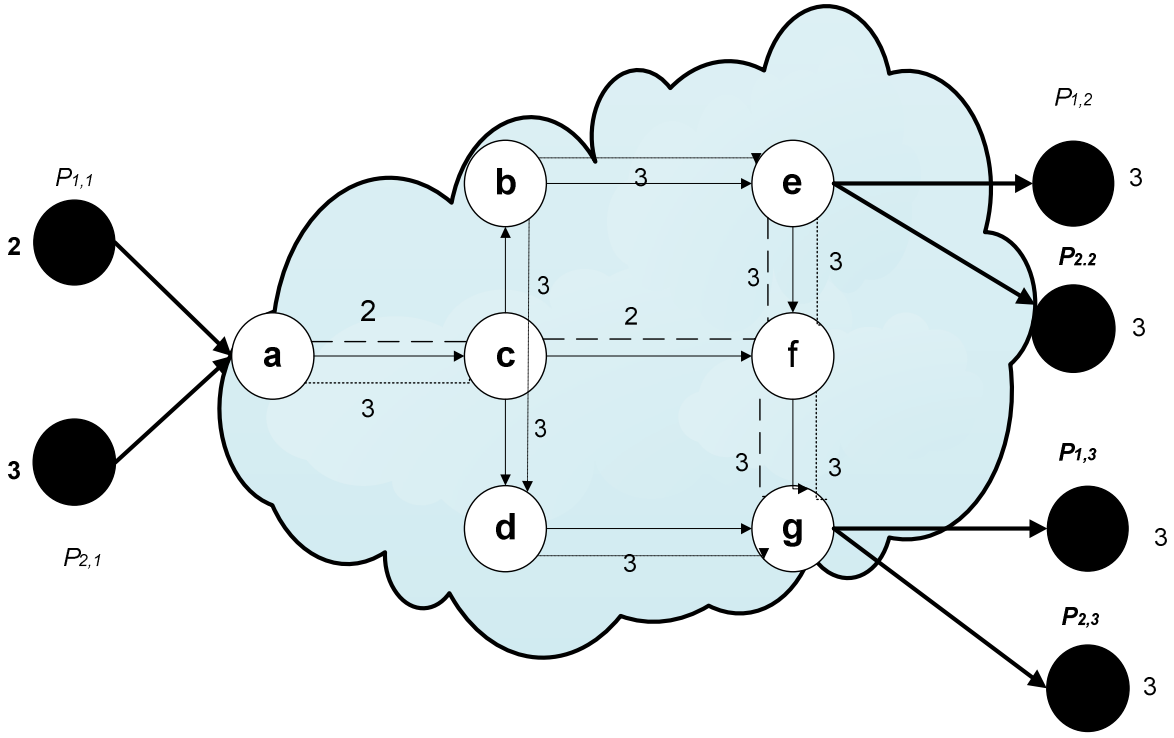

Рисунок 2.4 – Реалізація двох запитів на базі потокової моделі VPN

2.2 Потокова модель VPN із багатошляховою маршрутизацією трафіка

Перевірка можливості резервування необхідної смуги пропускання при багатошляховому маршрутуванні трафіка в потоковій моделі VPN при наявності обмежень на мережні ресурси може бути виконана аналогічно перевірці можливості одношляхового маршрутування. Як і в попередньому випадку, кожне ребро *e* в графові *G* розглядається незалежно. На рисунку 2.5 показано, як використовуються шляхи, що проходять через ребро *e,* за допомогою завдання відповідних коефіцієнтів поділу *h(u,v,e)*. Передбачається, що для ребер без зазначеного коефіцієнта він рівний 1 (відсутнє поділ доступної смуги пропускання даного ребра по декільком шляхам).

Як і для одношляхового маршрутування трафіка, двочастковий граф будується на підставі схеми маршрутизації трафіка по ребру *e*, а початкова вершина-джерело S і кінцева вершина-стік t використовуються для одержання графа G_{Bie}. Ребра з вершини S у кінцеві точки u $\in$ P мають значення трафіка B^{out}_{U}, а ребра з V $\in$ P в *t* - значення B^{in}_{V}. Усі інші ребра між початковими й кінцевими точками мають нескінченну смугу пропускання.

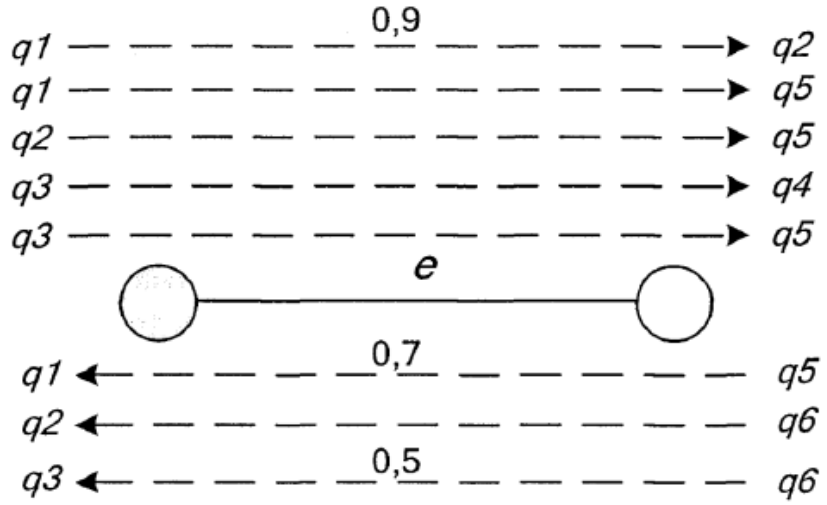

Рисунок 2.5 – Використання ребра *e* у різних шляхах при багатошляхової маршрутизації трафіка VPN

Відмінність і головна ідея перевірки можливості резервування смуги пропускання при багатошляхової маршрутизації трафіка являє собою визначення деякої умовної вартості CBie для кожного ребра в графові GBie. У той час як ребра з S і t мають вартість SBie = 0, то вартість ребер між кінцевими точками VPN і обраними шляхами ухвалює негативне значення відповідно до коефіцієнта розподілу. Це означає, що використання ребер з більш високим коефіцієнтом поділу є більш дешевим. На рисунку 2.6 показаний граф G_{Bie} з мінімальною вартістю потоку. Ті ребра, у яких коефіцієнт розподілу не зазначений у круглих дужках, він приймається рівним 1.

Як зазначено вище, алгоритм мінімальної вартості потоку дозволяє визначити максимально необхідну смугу пропускання Y_E для ребра *e.*

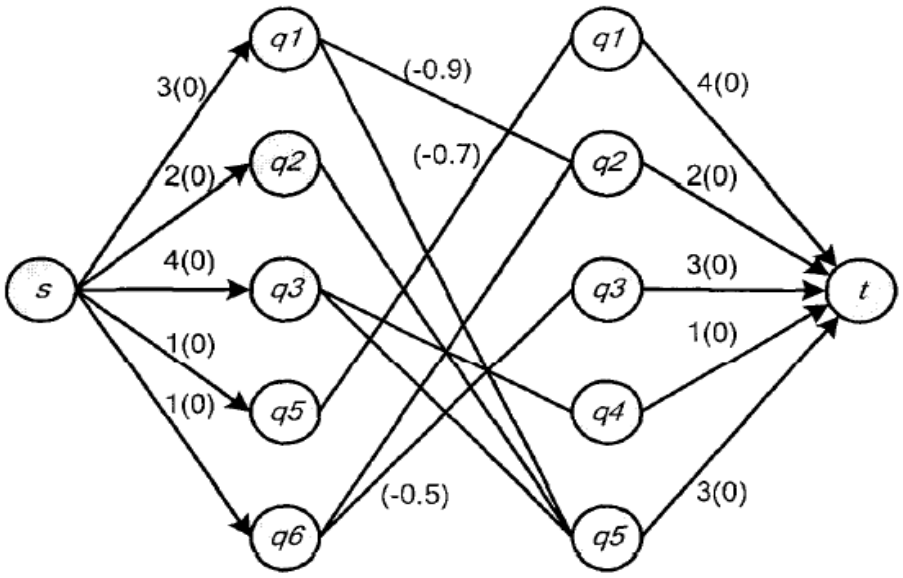

Рисунок 2.6 – Двочастковий граф з мінімальною вартістю потоку

Тому що невідомо, який потік буде мати мінімальну вартість, повинні бути розглянуті всі можливості, починаючи від мінімального потоку 1 до максимального потоку, виданого алгоритмом максимального потоку. Однак повного перебору варіантів можна уникнути шляхом простого способу, показаного на рисунку 2.7. Додавання ребра *e* прямо від вершини *s* до вершини *t* з вартістю О и нескінченною смугою пропускання дозволяє знайти оптимальне рішення мінімальної вартості потоку для нескінченного потоку від *S* і *t.* Через нульову вартість ребра *e* воно не впливає на вартість усього рішення, у той час можливо створення будь-якого потоку від *s* і *t.* Схема алгоритму модифікованої потокової моделі зображена на рисуноку 2.8.

Оцінимо тимчасові витрати алгоритму перевірки багаторівневої маршрутизації. У найгіршому разі поточний час виконання алгоритму залежить від того, як ефективний побудований граф G_{Bie} для кожного ребра *e* в графові *G.* Нехай *m* – це число ребер, а *n* – число вершин графа G_{Bie}. Тоді

буде потрібно $O(n^3)$ операцій, щоб здійснити перевірку для всіх пар кінцевих точок VPN (u,v). І для кожного значення смуги резервування.

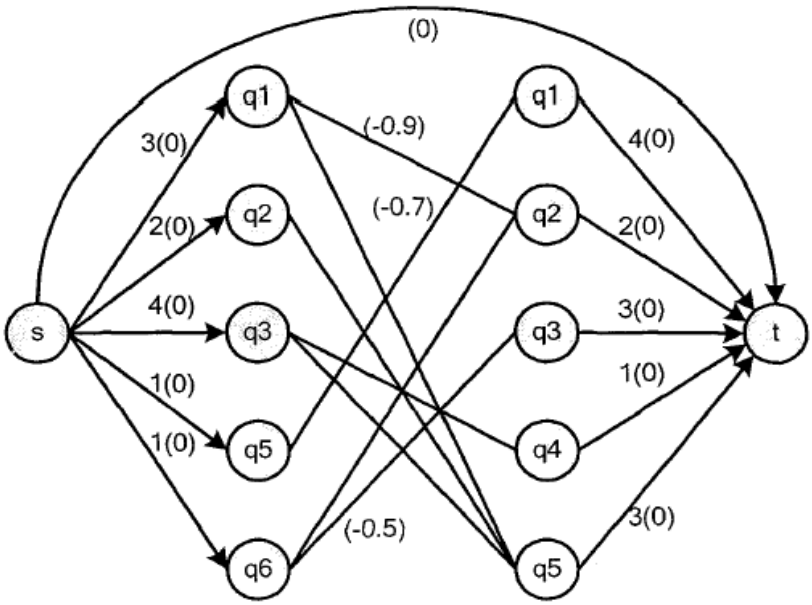

Рисунок 2.7 – Модифікація двочасткового графа

Тому, для кожного випадку вибору маршруту передачі трафіка кінцевих точок VPN існує якнайбільше *m* шляхів від m до v, то складність алгоритму можна оцінити величиною ($O(n^3)$).

Таким чином, виконання даного завдання більш складне, чому при одношляхової маршрутизації, яка використовує додатковий алгоритм мінімальної вартості, і має в самому гіршому випадку складність *O(mlogU[m + nlogn]),* де *U* – це найбільше абсолютне значення доступної смуги пропускання на будь-якому ребрі графа мережі.

Усі розглянуті раніше потокові моделі VPN ґрунтувалися на припущенні, що будь-який обсяг смуги пропускання може бути зарезервований для пропуску трафіка на кожнім ребрі в графі *G,* що моделює мережа загального користування.

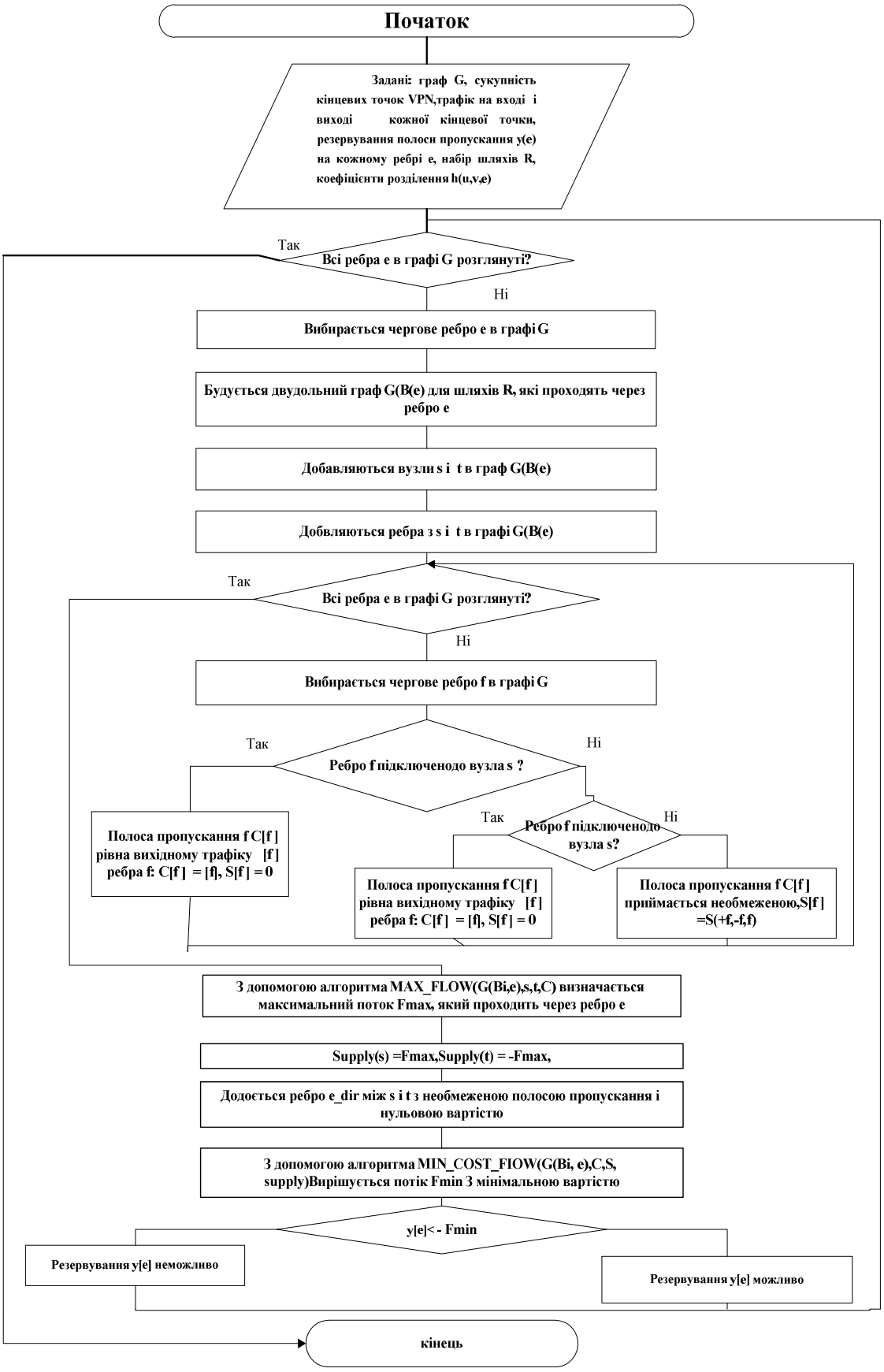

Рисунок 2.8 – Схема алгоритму модифікованої потокової моделі

3 ДОСЛІДЖЕННЯ ВЛАСТИВОСТЕЙ МОДЕЛЕЙ VPN

3.1 Обґрунтування вимог щодо вибору програмного пакету дослідження моделей VPN

Для дослідження розроблених моделей і оцінки практичної ефективності застосування пропонованих алгоритмів планування VPN були розроблені вимоги до програмного комплексу ViPNet. Даний пакет являє собою програмний інструментальний засіб, який призначений для створення й редагування моделей віртуальних приватних мереж і дослідження їх характеристик.

ViPNet – це програмний комплекс, який виконує на робочому місці користувача або сервері з прикладним програмним забезпеченням функції VPN-клієнта, персонального екрану, клієнта захищеної поштової системи.

ViPNet має сучасний графічний інтерфейсом і широкі функціональні можливості. Загальна структура пакета ViPNet представлено на рисунку 3.1.

Основними вимогами до використання комплексу ViPNet були:

- зручний для фахівців різного рівня інтерфейс;
- можливість інтерактивного введення даних;
- підтримка збереження й завантаження створених моделей мереж;
- розв'язок завдань планування VPN при різних моделях;
- інтерактивний перегляд результатів розв'язку завдань;
- невисокі системні вимоги;
- високі ємнісні характеристики пакета;
- можливість стикування із зовнішнім програмним генератором топологій графа, наприклад пакетом BRITE, широко використовуваним при дослідженні графових моделей.

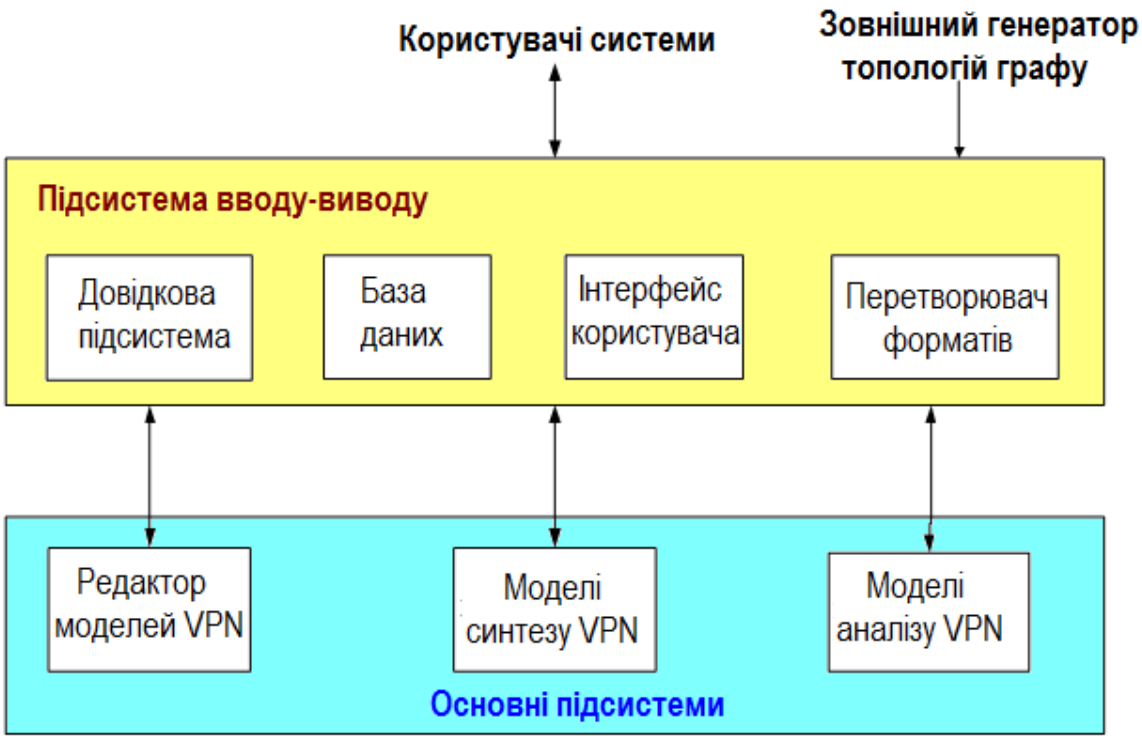

Рисунок 3.1 – Структура програмного пакета ViPNet

Спектр завдань, розв'язуваних розробленим програмним продуктом, містить у собі завдання аналізу й синтезу оптимальної топології VPN із симетричним і асиметричним трафіком кінцевих точок, з різною топологією одержуваних результатів: дерево, набір дерев або підграф, з урахуванням вартості використання смуги пропускання каналів або без нього, з обмеженим максимальним трафіком через канал або без обліку тощо.

Задачі синтезу оптимальної топології, побудованої на канальній і потокової моделях VPN містять часткові задачі:

- синтезу оптимальної топології VPN з урахуванням мінімізації вартості або смуги пропускання при симетричному трафіку кінцевих точок без обліку обмежень на пропускну здатність каналів мережі загального користування;

- аналізу можливості побудови заданої топології VPN при симетричному трафіку з урахуванням обмежень на пропускну здатність каналів мережі загального користування;

- синтезу оптимальної топології VPN з урахуванням мінімізації вартості або смуги пропускання при асиметричному трафіку кінцевих точок без обліку обмежень на пропускну здатність каналів мережі загального користування;

- синтезу оптимальної топології VPN з урахуванням мінімізації вартості або смуги пропускання при симетричному трафіку кінцевих точок з урахуванням обмежень на пропускну здатність каналів мережі загального користування;

- синтезу оптимальної топології VPN з урахуванням мінімізації вартості або смуги пропускання при асиметричному трафіку кінцевих точок з урахуванням обмежень на пропускну здатність каналів мережі загального користування;

- синтезу оптимальної топології VPN з урахуванням мінімізації вартості або смуги пропускання при одношляховому маршрутуванні симетричного трафіка кінцевих точок без обліку обмежень на пропускну здатність каналів мережі загального користування;

- синтезу оптимальної топології VPN з обліком мінімізації вартості або смуги пропускання при багато шляховому маршрутуванні симетричного трафіка кінцевих точок без обліку обмежень на пропускну здатність каналів мережі загального користування;

- синтезу топології канальної моделі VPN;

- синтезу оптимальних деревоподібних топологій відмова стійкого VPN із симетричним і асиметричним трафіком кінцевих точок при одиночних відмовах ребер дерева VPN для стратегій захисту ланки й захисту шляхи.

Комплекс ViPNet функціонує під управлінням операційних систем Windows (32/64-розрядна) і забезпечує роботу додатків в наступних основних режимах:

- створення нових і редагування вже існуючих моделей VPN;
- виконання експериментів з моделями VPN.

Розроблена система виконана у вигляді додатка із багатодокументним графічним інтерфейсом і дозволяє одночасно працювати з декількома моделями, кожна з яких представлена у своєму власнім вікні (рисунок 3.2). Модель VPN представляється користувачеві у вигляді її графа, що відображає. Система здатна "розпізнавати" усі зміни в графові й автоматично вносити відповідні зміни в саму модель.

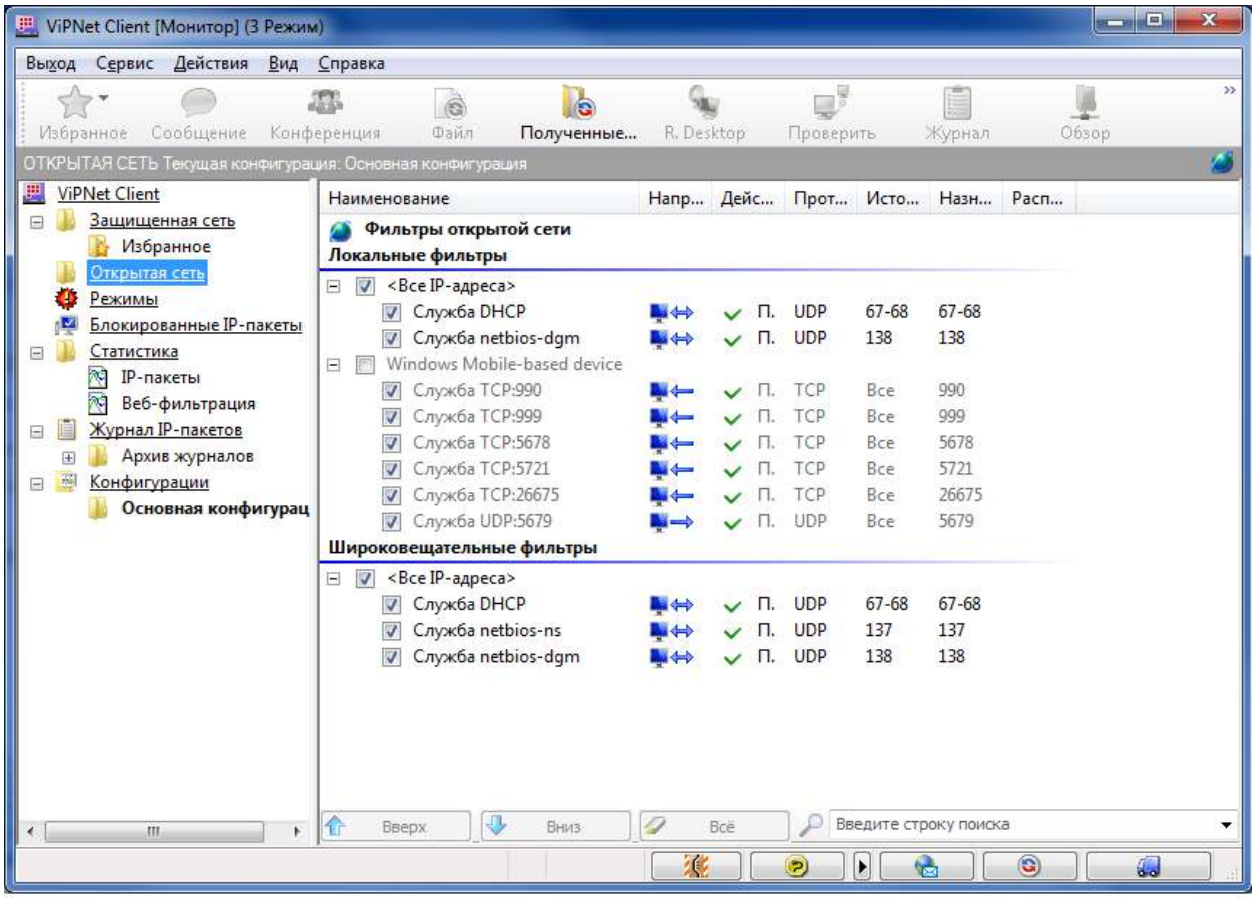

Рисунок 3.2 – Користувальницький інтерфейс програмного комплексу ViPNet

Відмінність внутрішньої вистави моделі VPN від її графа, що відображає, полягає тільки у відсутності в ній інформації, необхідної для візуального зображення графа. Система дозволяє користувачеві працювати з моделлю й через її відображення у вигляді матриці. Управління взаємодією моделі з різними формами її графічного відображення здійснюється редактором моделі. Крім цього, редактор забезпечує взаємодію з базою даних

і здійснює оперативний контроль і відповідає за відновлення моделі в процесі редагування її візуального відображення у вигляді графа. Для проектування алгоритмів обрана наступна інтуїтивно зрозуміла модель мережі загального користування й модель VPN:

- мережа загального користування – граф, де вершини відповідають вузлам мережі, а ребра відповідають каналам між вузлами. Граф орієнтований, зважений, вага ребра означає вартість використання каналу, можуть уводитися обмеження на пропускну здатність ребра;
- кінцеві точки VPN задаються додатковими вершинами графа, мають одне вихідне й одне вхідне навантажене ребро в ту саму вершину графа мережі загального користування. Навантаженням даного ребра є трафік кінцевої точки VPN.

Наведене порівняння канальної й потокової моделей VPN нічого не говорить про те, наскільки гарна кожна з них при інших умовах. У зв'язку із цим було проведене порівняння моделей по абсолютній величині, тобто по сумарній резервуючій смузі пропускання в мережі загального користування для реалізації віртуальних мереж з однаковою матрицею трафіка *Y.*

Для порівняння моделей використовувалися різні матриці трафіка *Y* із усіх можливих, які були отримані на основі величин потоків кінцевих точок VPN B^{in}_i та B^{out}_i, тобто $Y = (y_{ij})$, де

$$\sum_{i \in P} \left(y_{ij}\right) \le B_i^{in} \quad \text{та} \quad \sum_{i \in P} \left(y_{ij}\right) \le B_i^{out} \tag{3.1}$$

Задача визначення матриці *Y,* обмежена умовами (3.1), може бути вирішена як завдання знаходження 5-ти паросполучень або як завдання максимального потоку між усіма парами вершин і та j. Приклад такого відображення показано на рисунку 3.3.

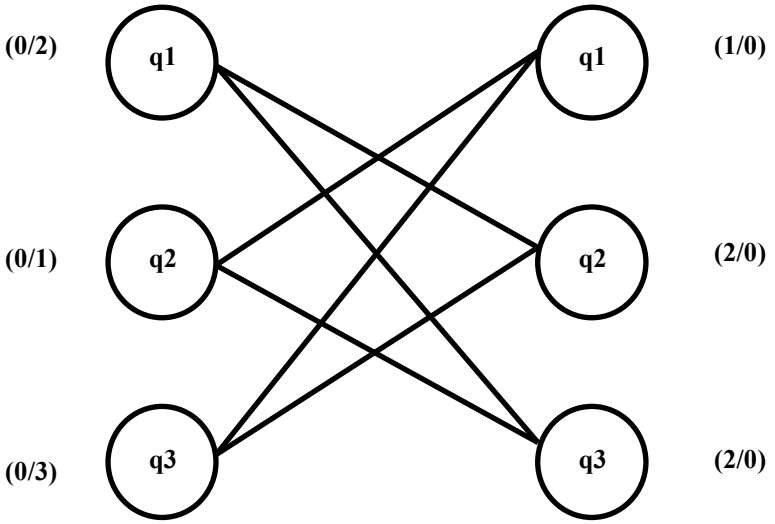

Рисунок 3.3 – Приклад формування матриці трафіка по значенням вихідного й вхідного трафіка *B* для VPN із трьома кінцевими точками

Враховуючи той факт, що відсутній трафік з вершини *I* до самої себе, те відповідно не буде з'єднання однойменних вершин, розташованих ліворуч і праворуч у двочастковому графові. Наприклад, одна з можливих матриць трафіка для графа, має вигляд :

$$Y = \begin{matrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \end{matrix} \qquad (3.2)$$

Проведені розрахунки канальної й потокової моделей VPN з деревоподібним маршрутуванням трафіка. Порівняння моделей здійснювалося по мінімальній резервуючій смузі пропускання при заданій матриці трафіка *Y* для випадків симетричного трафіка $Bi^{in} = Bi^{out}$ і асиметричного трафіка $Bi^{in} \neq Bi^{out}$ для всіх i ∈ P. Результати отримані на основі згенерованих графів G, для яких:

- число вершин у графові $n = |V| \in \{3, 4, ..., 10\}$;
- число ребер у графові $m = |E| \in \{n-1, n ...., (n(n-1)/2)\}$;

- число кінцевих точок VPN $q = |P| \in \{3, 4, .., .n\}$;
- трафік кінцевих точок VPN Bi^{in}, $Bi^{out} \in \{1, 2, ..., 5\}$.

Для кожної можливої комбінації параметрів *n, m и q* вибиралося 100 довільних графів з різними значеннями трафіка кінцевих точок. Таким чином, було згенеровано 100 графів з параметрами $n = 3$, $m = 3$ і $q = 3$, 100 графів – з параметрами $n = 10$, $m = 45$ і $q = 10$ тощо.

На рисунках 3.4 – 3.6 показані результати розрахунків для випадку симетричного трафіка кінцевих точок VPN $Bi^{in} = Bi^{out} = 1$ (умовні одиниці) з використанням потокової й канальної моделей, причому для потокової моделі показані мінімальні, середні й максимальні значення резервуючої смуги пропускання.

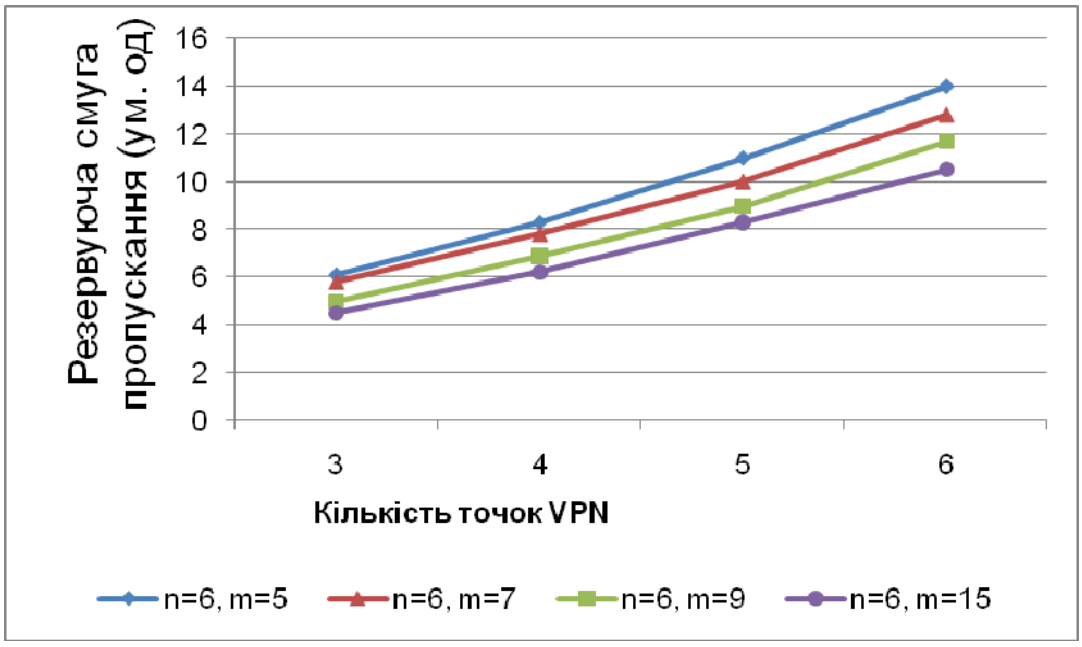

Рисунок 3.4 – Число кінцевих точок VPN для канальної моделі

На рисунку 3.4 і 3.5 показані залежності величини резервуючої смуги пропускання від числа кінцевих точок VPN у потоковій моделі при різних топологіях мережі, а на рисунку 3.6 при $n = 9$, $m=10$.

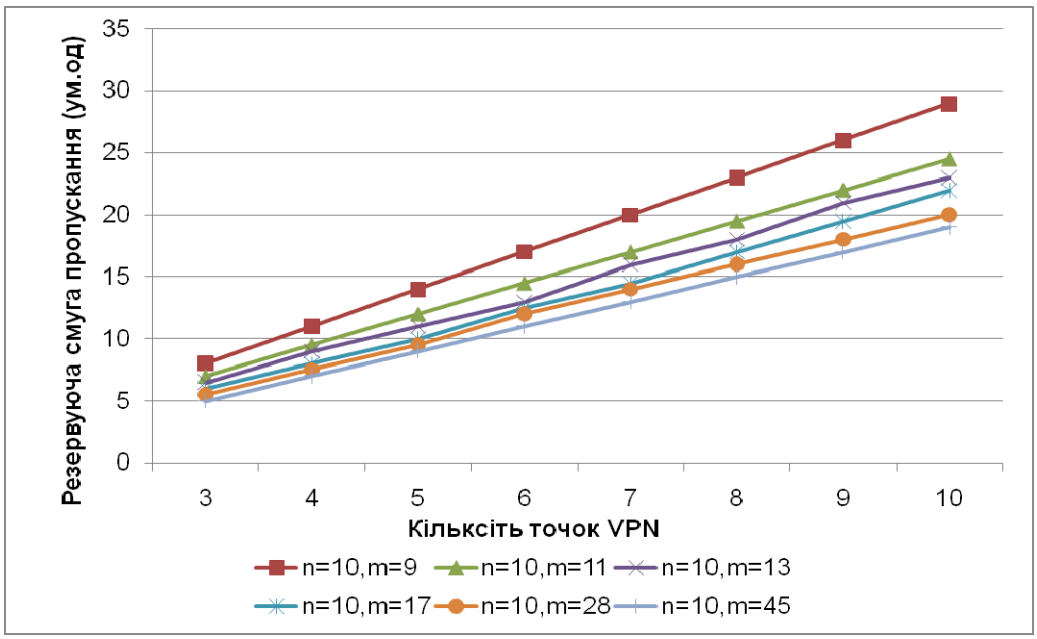

Рисунок 3.5 – Число кінцевих точок VPN для потокової моделі

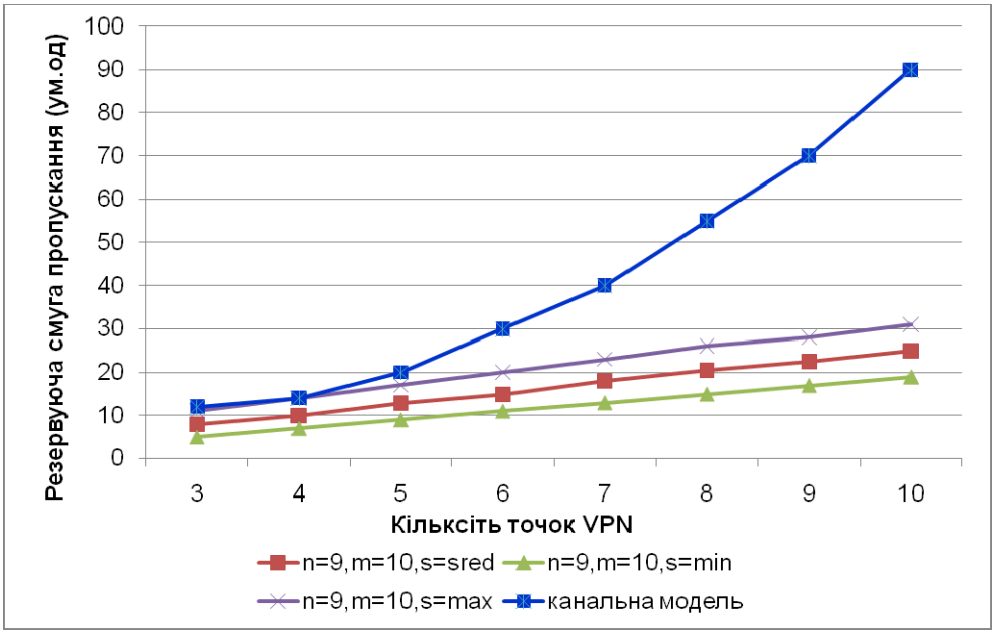

Рисунок 3.6 – Залежності величини резервуючої смуги пропускання від числа кінцевих точок VPN для канальної й потокової моделей

Проведене дослідження дозволяє зробити наступні висновки.

1. Характеристики мережі загального користування (число вузлів *n,* число ребер *m,* зв'язність мережі) суттєво впливають на резервируемую смугу

пропускання для реалізації VPN. Наприклад, при кількості кінцевих точок віртуальної мережі $P = 6$ для реалізації VPN у мережі загального користування із числом вузлів $n = 6$ і ребер $m = 5$ на базі потокової моделі необхідно зарезервувати смугу пропускання в 14 умовних одиниць (рис. 3.4), у той час як для такої ж VPN при $n = 10$ і $m = 45$ потрібна смуга 11 умовних одиниць (рис. 3.5), тобто різниця становить більш 22%.

2. Зі збільшенням розміру віртуальної мережі збільшується розкид можливих значень резервованої смуги пропускання залежно від топології мережі загального користування. Наприклад, при реалізації VPN з 9-ю кінцевими точками в мережі з 10 вузлами й 45 ребрами розкид від мінімального до максимального значення становить 40% (рис. 3.6).

3. При використанні канальної моделі VPN залежність резервованої смуги пропускання від числа кінцевих точок P підкоряється практично квадратичному закону, що випливає з формули числа необхідних каналів для реалізації повнозв'язної схеми $P * (P - 1)/2$.

У потоковій моделі VPN характерно лінійне наростання величини резервованої смуги пропускання з коефіцієнтом 0,15 при збільшенні числа кінцевих точок VPN, тому потокова модель є особливо ефективною для великих мереж з більшою кількістю вузлів і кінцевих точок.

Було проведено також дослідження потокової моделі при асиметричному трафіку кінцевих точок VPN. Введений коефіцієнт асиметрії г, під яким розуміється відношення трафіку на вході до трафіку на виході для кожної кінцевої точки VPN-мережі. Для всієї VPN подібний коефіцієнт дорівнює відношенню величин, які позначають сумарний трафік на вході і виході всіх кінцевих точок VPN відповідно. Результати розрахунків сумарної смуги пропускання при різних коефіцієнтах асиметрії трафіка для мережі з 50 вузлів і VPN з 20 кінцевими точками показані на рисунку 3.7.

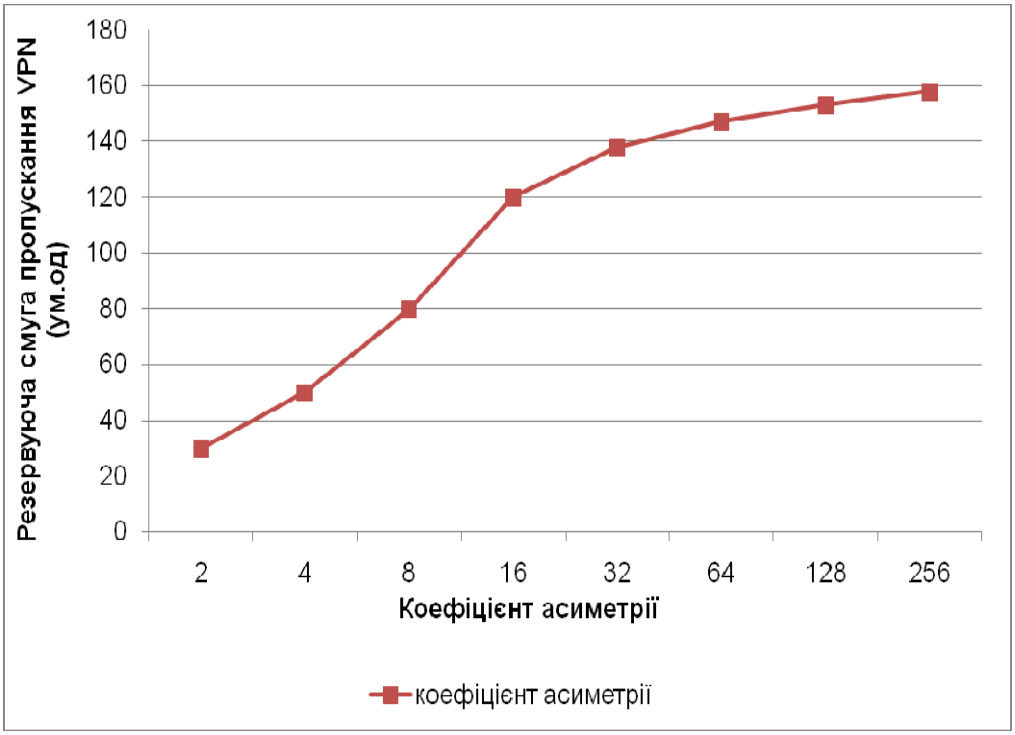

Рисунок 3.7 – Залежність резервованій смуги пропускання VPN від величини коефіцієнта симетрії трафіку

Із графіка видно, що при невеликих значеннях коефіцієнта асиметрії його зміна сильна впливає на характеристики VPN, а при більших коефіцієнтах асиметрії резервуюча смуга пропускання для VPN практично залишається постійною. Це можна пояснити тим, що при великій асиметрії основна частка резервуючої смуги пропускання в мережі припадає на напрямки з більшою величиною переданого трафіка, а вплив напрямків з малим навантаженням незначно.

Експериментальні дослідження показали, що в канальній моделі VPN залежність резервованої смуги пропускання від числа кінцевих точок підкоряється практично квадратичному закону, тоді як для потокової моделі VPN характерна лінійна залежність. Тому, потокова модель особливо ефективна для великих мереж з більшою кількістю кінцевих крапок.

У результаті проведених досліджень виявлено, що характеристики мережі загального користування (число вузлів і ребер графа мережі, його

зв'язність) істотно впливають на резервовану смугу пропускання для реалізації віртуальної приватної мережі на базі потокової моделі й різниця може становити кілька десятків відсотків.

Зі збільшенням розмірів віртуальної мережі збільшується також розкид можливих значень резервованої смуги пропускання для VPN залежно від характеристик мережі загального користування й він може становити 40% і більше.

3.2 Експериментальне дослідження модифікованої потокової моделі VPN

Розглянемо визначені в роботі дві моделі для забезпечення якості обслуговування QoS в контексті VPN-мереж: канальну (pipe) та потокову (hose) модель.

Зазначимо, що в канальній моделі клієнт VPN-мережі визначає вимоги до QoS між кожною парою кінцевих точок VPN-мережі. Інакше, канальна модель вимагає знати підсумкову матрицю трафіку, яка є навантаженням між кожною парою кінцевих точок VPN. Проте число кінцевих точок в VPN-мережі постійно збільшується і з'єднання між кінцевими точками стає все більш і більш скрутним. В результаті майже неможливо передбачити параметри трафіку між парою кінцевих точок, що вимагаються для канальної моделі. Звідси недовикористання мережних ресурсів, що резервуються для VPN.

Для моделювання виберемо наступні початкові дані (рисунок 3.8):

- число ребер в одному графові – 14 шт.;
- число вузлів в одному графові – 9 шт.;
- загальне число кінцевих точок – 20 шт.;
- число кінцевих точок на одному сайті – 10 шт.;
- при передачі використовували один пакет розміром 20 КБ.

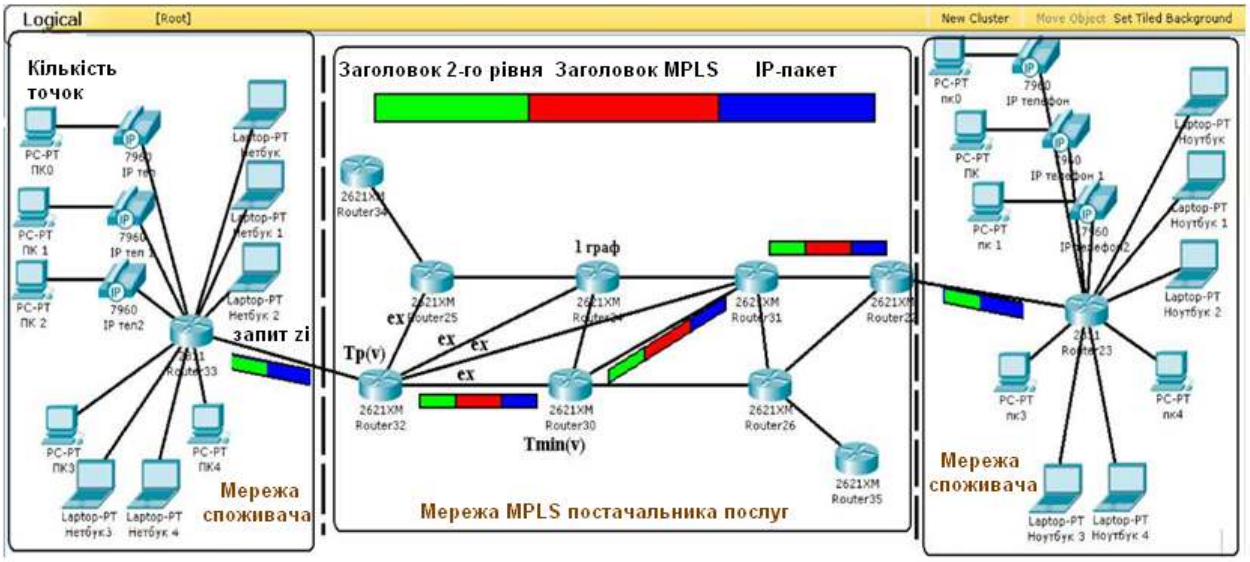

Рисунок 3.8 – Мережа загального користування, побудована в програмі Cisco Packet Tracer

В якості показника для порівняння різних моделей в роботі використаний коефіцієнт відхилення запитів на реалізацію VPN:

$$\Delta = Z_0 / Z \tag{3.1}$$

де Z_0 – число відхилених запитів на реалізацію VPN;

Z – загальне число отриманих запитів.

Показник використання смуги пропускання для графа VPN визначаються як:

$$C(T) = \sum_{x}^{E(T)} C(e_x), \tag{3.2}$$

де $C(e_x)$ – необхідна смуга пропускання на ребрі e_x;

$L(e_x)$ – доступна смуга пропускання.

В канальній моделі VPN залежність резервованої смуги пропускання від числа кінцевих точок підкоряється практично квадратичному закону, тоді

як для потокової моделі VPN характерна лінійна залежність (таблиця 3.1, рисунок 3.9). Це дозволяє рекомендувати потокову модель для великих мереж з великою кількістю вузлів і кінцевих точок VPN.

Таблиця 3.1 Резервируемая смуга пропускання від числа кінцевих

Число кінцевих точок VPN	Потокова модель	Канальна модель
3	0,1032	0,1143
4	0,1234	0,1554
5	0,1436	0,2764
6	0,1676	0,3134
7	0,1827	0,4086
8	0,2098	0,6439
9	0,2256	0,8987
10	0,2446	1,000

В роботі запропонована модифікована модель для потокової моделі, що враховує одночасно два чинники: ефективність розподілу смуги пропускання в мережі для кожного запиту VPN і механізм балансування навантаження в мережі з урахуванням вільної смуги пропускання.

Показники використання смуги пропускання в модифікованій моделі визначали по формулі 3.3:

$$C_M(T) = \sum_{x=1}^{E(T)} \frac{C(e_x)}{D(e_x)}, \qquad (3.3)$$

де $C(e_x)$ – необхідна смуга пропускання на ребрі e_x;

$D(e_x) = L(e_x) – C(e_x)$ – вільна смуга пропускання;

$L(e_x)$ – доступна смуга пропускання.

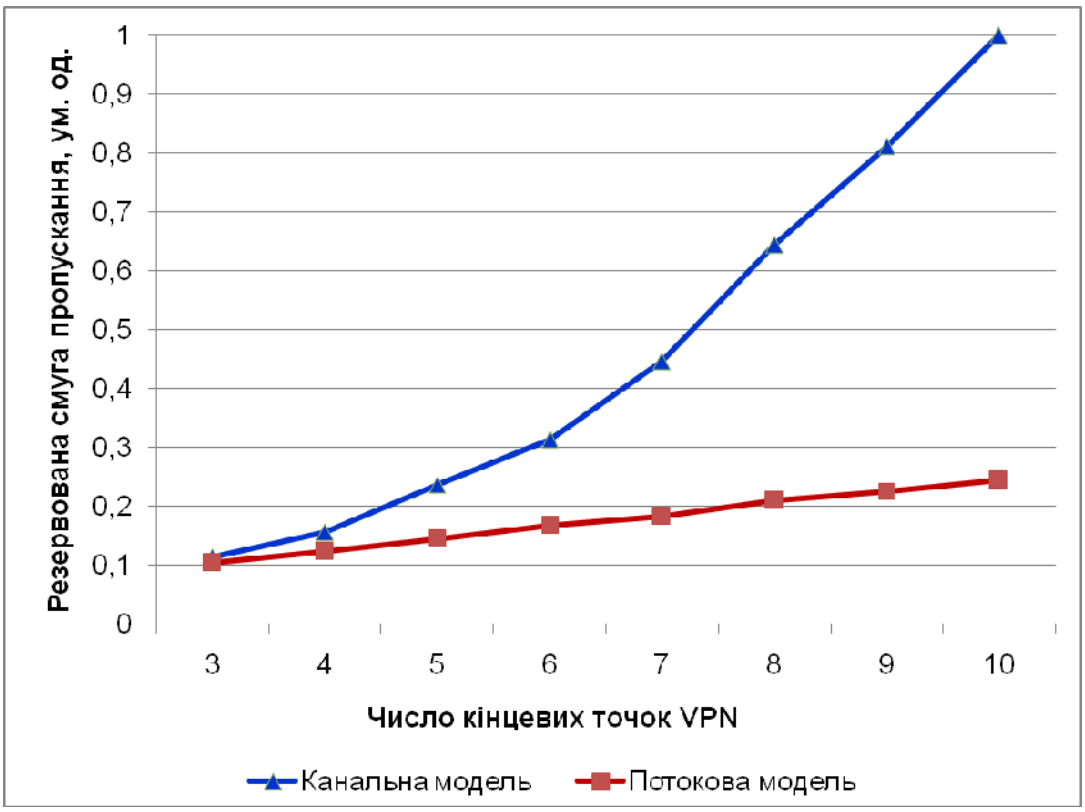

Рисунок 3.9 – Залежність величини резервованій смуги пропускання від числа кінцевих точок VPN для канальної і потокової моделей

Модифікована модель виконується з використанням n – ітерацій, по одній ітерації для кожної вершини (V) графа VPN-мережі:

- знаходиться дерево-кандидат $T_p(v)$ для запиту z_i з коренем у вершині v;

- визначається величина смуги пропускання, необхідна для розподілу на кожному ребрі e_x в знайденому дереві;

- обчислюється сумарна резервована смуга пропускання для усього дерева $T_p(v)$. Якщо після розгляду усіх дерев $T_p(v \in V)$ не існує якого-небудь дерева, в якому усі ребра мають достатню вільну смугу пропускання для розподілу, то запит z_i відхиляється;

- у разі прийняття запиту z_i, визначається дерево VPN з мінімальною резервованою смугою пропускання Tmin(v) серед усіх дерев $T_p(v)$. Далі виконується розрахунок вільної смуги пропускання, що залишилася, на

кожному ребрі e_x дерева Tmin(v), яка може використовуватися для реалізації наступного запиту.

На рисунку 3.10 представлена залежність коефіцієнта відхилення від числа запитів (таблиця 3.2).

З нього видно, що значення верхньої межі коефіцієнта відхилення для модифікованої моделі в ~2,5 разу нижче, ніж для канальної і потокової моделей. Усі розрахунки були вироблені в програмі GPSS World (рисунок 3.11 – 3.12).

Таблиця 3.2 – Коефіцієнт відхилення від числа запитів

Моделі	Канальна модель		Потокова модель		Модифікована модель	
Z число запитів	N_k число відмов	Коеф. відхилення N_k	N_p число відмов	Коеф. відхилення N_p	N_m число відмов	Коеф. відхилення N_m
100	92	0,92	33	0,33	0	0
200	194	0,97	116	0,58	0	0
300	294	0,98	222	0,74	0	0
400	396	0,99	328	0,82	0	0
500	495	0,99	430	0,86	0	0
600	600	1	528	0,88	0	0
700	700	1	637	0,91	189	0,27
800	800	1	736	0.92	336	0,42
900	900	1	846	0,94	414	0,46
1000	1000	1	950	0,95	490	0,49

Дослідження впливу щільності графа мережі, рівного відношенню числа ребер до вершин в графі, на середнє значення коефіцієнта відхилення показало, що запропонована модифікована модель має значно кращі характеристики в порівнянні з іншими моделями, особливо при малій щільності графа мережі.

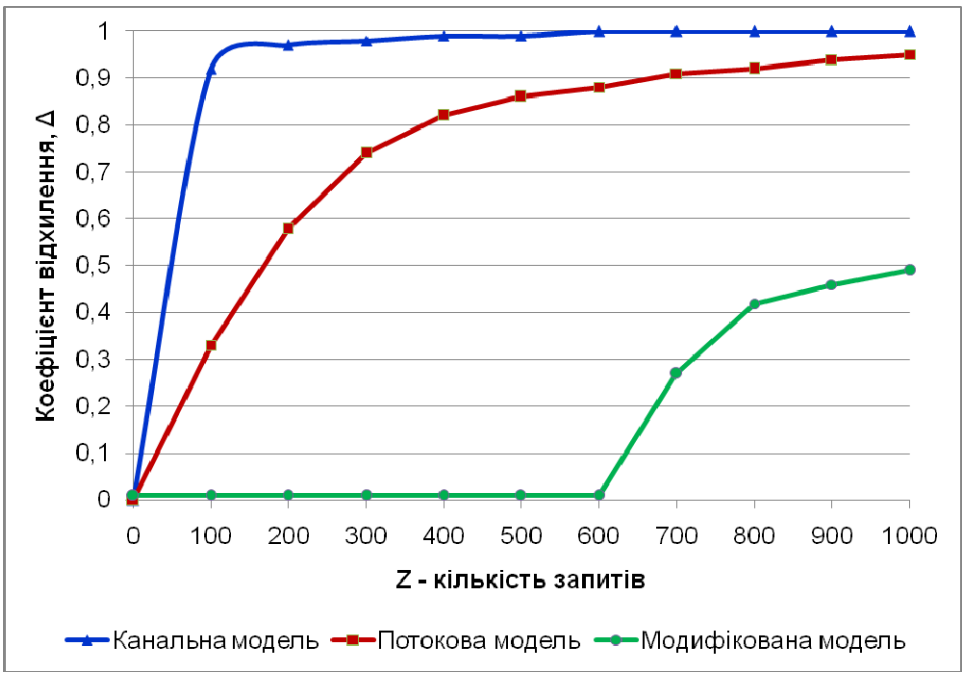

Рисунок 3.10 – Залежність коефіцієнта відхилення Δ від числа запитів z для різних моделей VPN

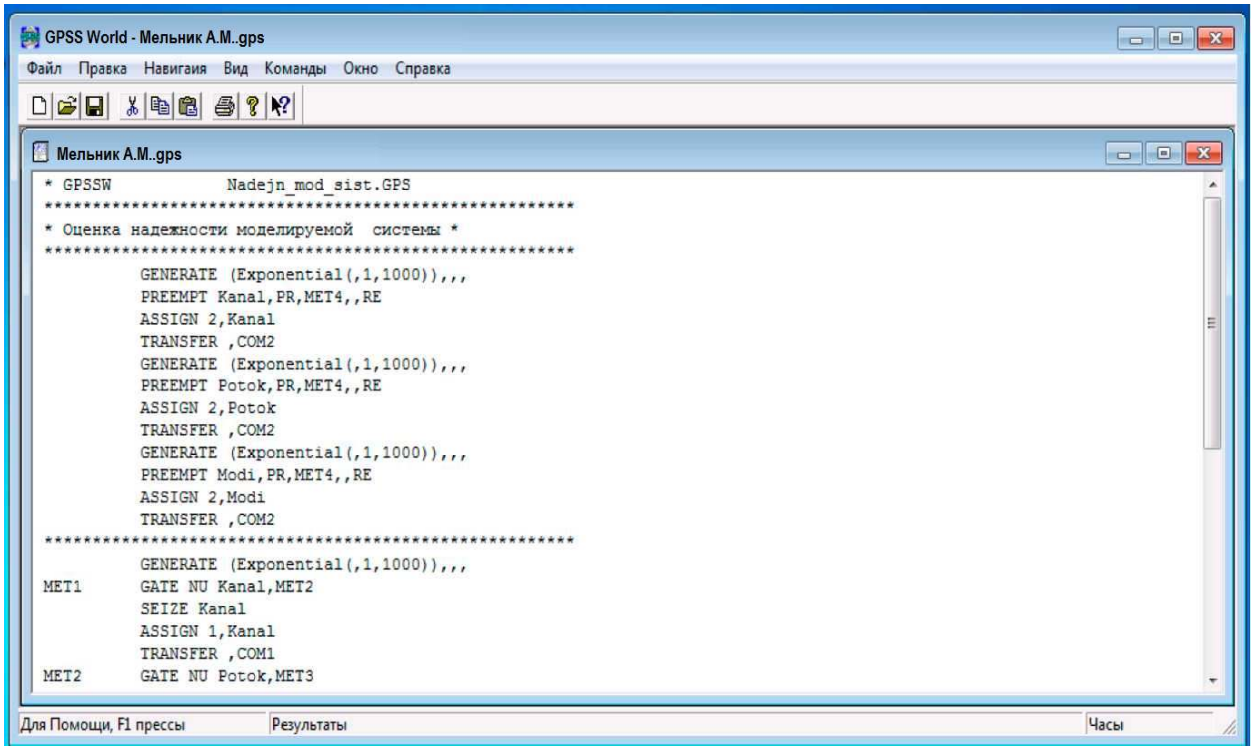

Рисунок 3.11 – Вікно програми імітаційного моделювання в GPSS World

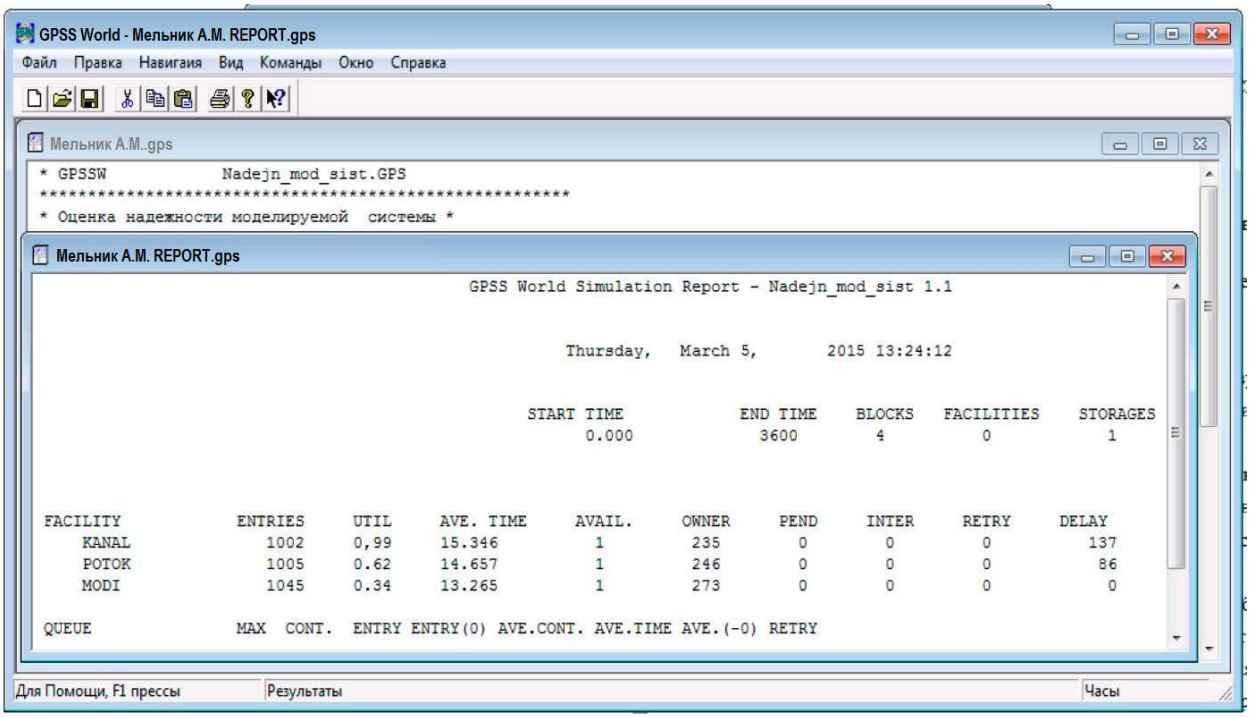

Рисунок 3.12 – Вікно програми імітаційного моделювання, REPORT з результатами моделювання імітаційної моделі

На рисунку 3.13 та в таблиці 3.3 представлена залежність середнього коефіцієнта відхилення від щільності графа для модифікованої моделі порівняно з існуючими моделями.

Таблиця 3.3 – Щільність графів всіх трьох моделей від середнього значення коефіцієнта відхилення Δ

Щільність графів	Канальна модель, %	Потокова модель, %	Модифікована модель, %
2	40,45	38,78	8,35
3	25,64	19,46	7,21
4	17,34	6,43	4,54
5	13,76	5,52	3,32
6	5,41	4,67	3,12

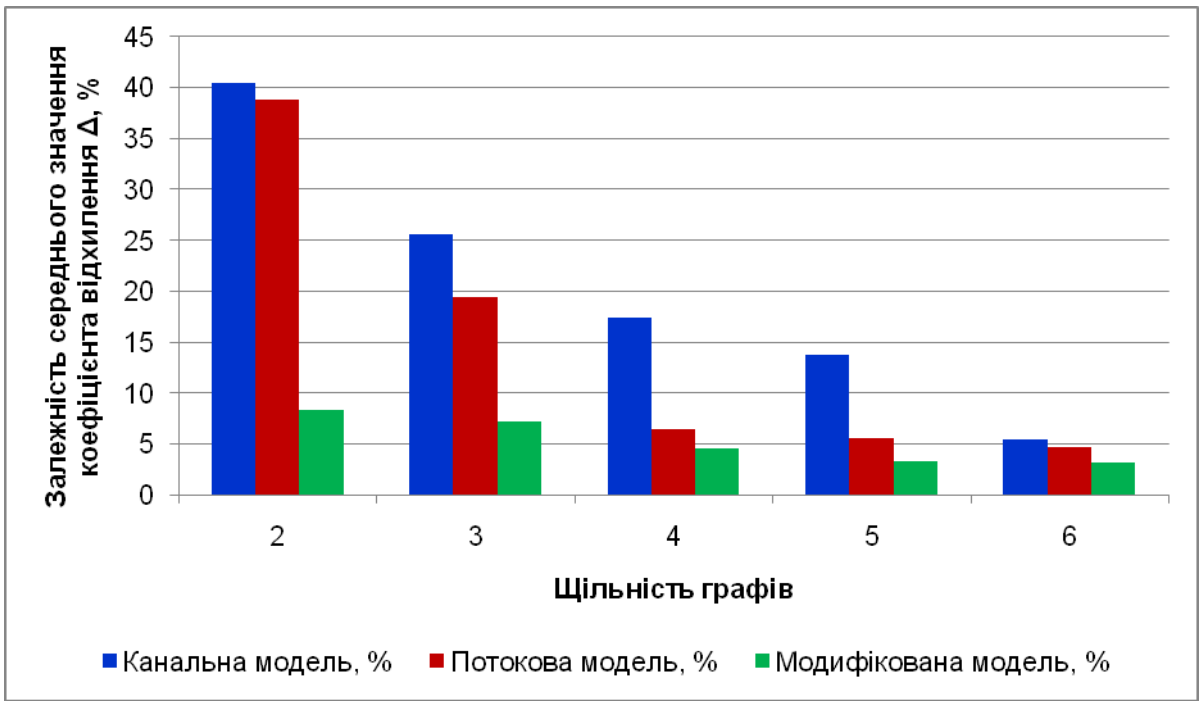

Рисунок 3.13 – Залежність середнього значення коефіцієнта відхилення від щільності графа при різних моделях реалізації VPN

На рисунку 3.14 та в таблиці 3.4 представлена залежність економії смуги пропускання від числа сайтів мережі.

Таблиця 3.4 – Економія смуги пропускання для модифікованої моделі в порівнянні її з іншими моделями

Число сайтів мережі	Порівняно з канальної моделлю, %	Порівняно з потоковою моделлю, %
1	2	3
2	5,43	5,21
5	12,34	9,34
10	20,54	16,23
15	24,32	19,76
20	27,24	23,45
25	30,12	26,36

Продовження таблиці 3.4

1	2	3
30	35,31	32,28
35	36,43	35,17
40	36,32	35,39
45	37,51	35,62

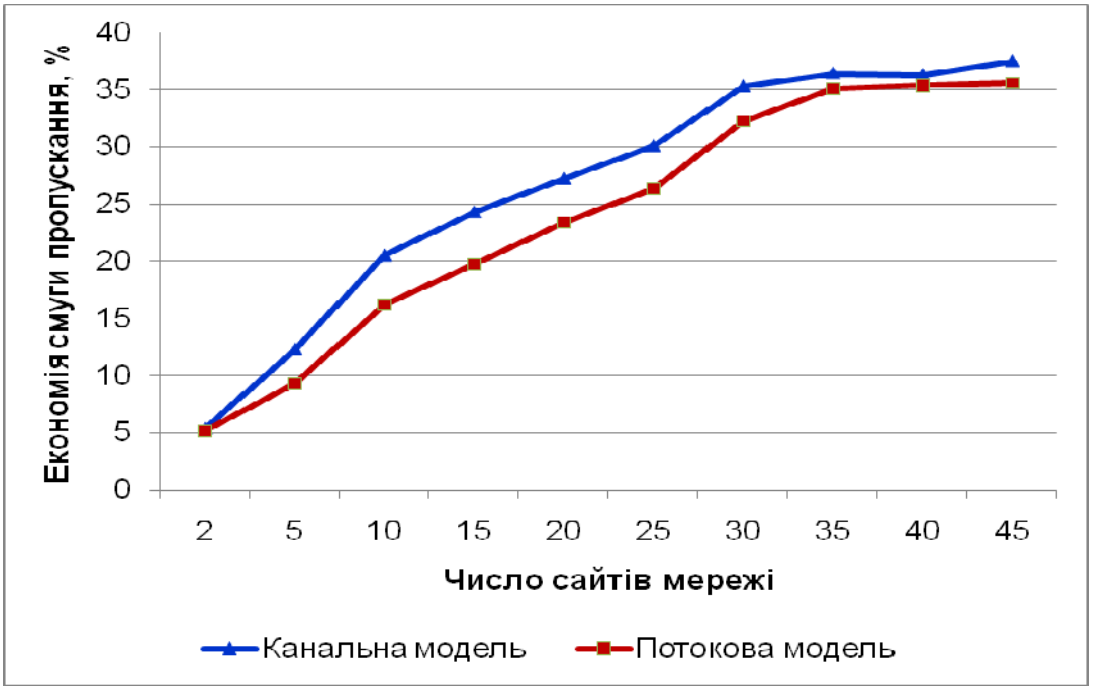

Рисунок 3.14 – Економія смуги пропускання в модифікованої моделі VPN залежно від числа сайтів мережі

З рисунку 3.14 видно, що розроблена модифікована модель забезпечує резервування значно меншої смуги пропускання, чим наявні моделі. Перевага модифікованої моделі VPN, виражається в економії мережних ресурсів до 35% залежно від числа сайтів мережі.

ВИСНОВКИ

В ході роботи були отриманні наступні результати:

1. Розроблений підхід до планування віртуальних приватних мереж, який враховує в сукупності інтереси споживачів і постачальників послуг VPN та дозволяє отримати закінчене системно-технічне рішення – від аналізу потреб у послугах VPN до планування, створення і подальшого обслуговування корпоративних мереж зв'язку.

2. Розроблені елементи теорії планування VPN з використанням апарату теорії графів у вигляді комплексу моделей і методів аналізу і синтезу топології віртуальної мережі з урахуванням повноти інформації про трафік кінцевих точок VPN і його характері, способів його маршрутування, обмежень на доступні мережні ресурси.

3. Запропоновано модифікована потокова модель VPN, яка базується на використанні більш повної інформації про розподіл трафіку, що дає суттєвий виграш в необхідній смузі пропускання мережі загального користування в порівнянні як з потокової моделлю, так і з канальною.

4. Надані практичні рекомендації використання модифікованої потокової моделі, що дозволить провайдерам послуг VPN підвищити ефективність планування, адміністрування та функціонування віртуальних мереж, автоматизувати процеси експлуатаційної підтримки діяльності провайдера послуг VPN, знизити тарифи на послуги, які надаються, забезпечити підтримку угод про заданій рівень якості обслуговування користувачів SLA.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Мережі наступного покоління NGN/А. В. Росляков, С. В. Ваняшин, М.Ю. Самсонов, І. А. Чечнєва, І. В. Шибаєва; під. ред. А. В. Рослякова. – Алмати: Еко-Трендз, 2018. - 436 с.

2. Росляков А. В. Віртуальні приватні мережі. Теорія і практика застосування / А. В. Росляков. – Алмати: Еко-Трендз, 2017. - 304 с.

3. Lewis M. Comparing, Designing, and Deploying VPNs / M . Lewis. – Cisco Press, 2016. – 1080 p.

4. Yuan R. Virtual Private Networks: Technologies and Solutions / R.Yuan, W. T. Strayer. – Addison-Wesley, 2014. – 317 p.

5. Scott C. Virtual Private Networks / C. Scott, M . Erwin, P. Wolfe. – O'Reilly Nutshell, 2019. – 225 p.

6. Brown S. Virtual private networks / S. Brown. – Lori, 2018. – 508 p.

7. Запечніков С. В. Основи побудови віртуальних приватних мереж. Навч. посібник для ВНЗ / С. В. Запечніков, Н. Г. Милославська, А. І. Толстой. - Тернопіль: УкрТелеком, 2023. – 249 с.

8. Загальна архітектура системи експлуатаційної підтримки VPN // Голубничий Д.Ю., Агаджанян Н.Г., Гєрко А.В., Мельник А.М. / Тези доповіді V міжнародної НТК "Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління" 23 – 24 квітня 2015 року. Полтава – Баку – Кіровоград – Харків, 2015. – С. 23.

9. Моделі розподілу ресурсів мереж загального користування для реалізації VPN // Голубничий Д.Ю., Агаджанян Н.Г., Гєрко А.В., Мельник А.М. / Матеріали XI наукової конференції ХНУПС. – Харків: ХНУПС ім..І.Кожедуба, 2015. – С.173.

10. Duffield N.G. A flexible model for resource management in virtual private networks / N.G. Duffield, P. Goyalm, A. Greenberg, P. Mishra, K.K. Ramakrishnan, J. E. van der Merwe // A C M SIGCOMM Computer

Communication Review. – 2019. – V.29. – № 4. – Pp. 95 – 108.

11. Gary M. Computing machines and intractable problems / M. Gary, D. Johnson; per. from English – New York, 2022 . – 416 p.

12. Кучерявий А. Є. Мережі зв'язку нового покоління / А. Є. Кучерявий, А. Л. Цупріков. - Тернопіль: ТУПЦНДІВ, 2016. – 280 с.

13. Virtual Private Networks. A partnership between service providers and network managers [Електронний документ]. – Режим доступа: http://www.infonetics.com/services/whitepapersA/'PNet.VPNs.l 0.97.pdf.

14. Захватов М. А. Питання безпеки в MPLS мережах / М. А. Захватов // Документальний електрозв'язок. – 2004. – №13. – С.76 – 78.

15. Корпоративні територіальні мережі. Випуск 3. / За ред. М.Б. Купермана. - Київ: Інформзв'язок, 2017. – 348 с.

16. IP VPNs for Service Providers: The Foundation for Profitable [Електронний ресурс] // Режим доступа: http://www.cisco.com/en/US/netsol/ns341.

17. Побудова віртуальних приватних мереж (VPN) з урахуванням технології MPLS. - Cisco Systems, 2011. - 48 с.

18. Розробка загальних вимог до архітектури мультисервісних мереж зв'язку. – Київ: ЗАТ "РТК-Консалтинг", 2012. – 112 с.

19. Пятаєв В. О. Технологічні платформи для мультисервісних мереж / В. О. Пятаєв, А. А. Філіппов, Є. А. Захарова / Інформкур'єрзв'язок. – 2022. – № 22. – С. 36 – 38.

20. RFC 1058 "Routing Information Protocol)). [Електронний документ]. – Режим доступа: http://www.faqs.org/rfcs/rfcl058.htmL

21. STD 56. RIP Version 2. [Електронний ресурс] // Режим доступа: http://rfc.net/std0056.html.

22. RFC 1247. OSPF Version 2. [Електронний ресурс] // Режим доступа: http://www.faqs.org/rfcs/rfc 1247.html.

23. RFC 1142. OSI IS-IS Intra-domain Routing Protocol. [Електронний ресурс] //Режим доступа: http://www.faqs.org/rfcs/rfcll42.html.

24. Оліфер В.Г. Мистецтво оптимізації трафіку /В. Оліфер, Н. Оліфер [Електронний ресурс] // Режим доступу: http://www.olifer.co.uk/ articles/ip_l/ip_l.html.

25. Оліфер В. Г. Нові технології та обладнання IP-мереж / В. Г. Оліфер, Н. А. Оліфер. – Київ: БХВ-Петербург, 2001. – 512 с.

26. RFC 2702. Requirements for Traffic Engineering Over MPLS. [Електронний ресурс] // Режим доступу: http://www.faqs.org/rfcs/rfc2702.html.

27. RFC 3272. Overview and Principles of Internet Traffic Engineering. [Електронний ресурс] // Режим доступу: http://www.faqs.org/rfcs/rfc3272.html.

28. Awduche D. A Framework for Internet Traffic Engineering / D. Awduche, A.Chiu, A. Elwalid, I. Widjaja, X . Xiao [Електронний ресурс] // Режим доступу: http://cvs.gnus.org/intemet-drafts/draft-cheng-network-engineering-framework-OO.txt.

29. Тропченко О.Ю. Методи VPN. Навч. посібник / А.Ю. Тропченко, О.О. Тропченко. – Львів: ІТМО, 2022. – 156 с.

30. Colbourn C.J. Some open problems on reliability polynomials // Congr. № 165, 2023. – Pp. 187 – 202.

31. Росляков, А. В. Оптимальний розподіл мережевих ресурсів для реалізації віртуальних приватних мереж / А. В. Росляков // Праці навчальних закладів зв'язку. - Вип. №170, 2024. - С. 65 – 74.

32. Росляков, А.В. Оптимальний розподіл ресурсів мережі MPLS для реалізації VPN/А. В. Росляков// X міжнародна науково-технічна конференція "Радіолокація, навігація, зв'язок" (RLNC-2004): Праці. - Київ, 2024. – С. 35 – 40.