ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем

Кафедра телекомунікацій, медійних та інтелектуальних технологій

ДИПЛОМНА РОБОТА

Другий (Магістерський)

Освітній рівень

Галузь знань 17 Електроніка та телекомунікації

Шифр і назва спеціальності

Спеціальність 172 Телекомунікації та радіотехніка

Шифр і назва спеціальності

на тему: «Метод визначення пропускної здатності мереж з пакетною комутацією»

ДРТР.15013.01.09.ПЗ

Виконав: студент 2 курсу, група $ТР_м$-19-1 _____ Н.О. Кубатий

підпис Ініціали, прізвище

Керівник: канд. техн. наук, доц. _____ А.А. Таранчук

підпис Ініціали, прізвище

До захисту допускаю:

Зав. кафедри: д-р техн. наук, доц. _____ С.К. Підченко

підпис Ініціали, прізвище

09.12.2020 р.

Хмельницький, 2020

Хмельницький національний університет

Факультет *програмування та комп'ютерних і телекомунікаційних систем*
Кафедра *телекомунікацій, медійних та інтелектуальних технологій*
Освітній рівень *другий (магістерський)*
Галузь знань *17 – Електроніка та телекомунікації*
Спеціальність 172 – *Телекомунікації та радіотехніка*
Освітня-професійна програма *Телекомунікації та радіотехніка*

ЗАТВЕРДЖУЮ
Зав. кафедрою ТМІТ
«3» 09 2020 р.

ЗАВДАННЯ
НА ДИПЛОМНУ РОБОТУ

Кубатому Назару Олексійовичу

1 **Тема роботи:** «Метод визначення пропускної здатності мереж з пакетною комутацією»
керівник роботи Таранчук Алла Анатоліївна, к.т.н, доцент
Затверджено наказом по університету від «1» вересня 2020 р. № 118
2 Строк подання студентом роботи на кафедру: 02.12.2020 р.
3 Вихідні дані (характеристика об'єкта, умов дослідження та ін.)

Мета роботи полягає в удосконаленні методу визначення пропускної здатності мереж з пакетною комутацією.

Об'єктом досліджень є процеси передачі трафіку в мережах з пакетною комутацією.

Предметом досліджень є метод визначення пропускної здатності мереж з пакетною комутацією.

4. Зміст пояснювальної записки (перелік питань, що їх належить розробити)

1. Розглянути принципи організації та використання мереж з пакетною комутацією.
2. Дослідити протоколи передачі даних та визначити основні характеристики мереж з комутацією пакетів.
3. Розрахувати пропускну здатність мережі голосової IP – телефонії.
4. Провести моніторинг трафіку мереж з пакетною комутацією.

Завдання отримав

Науковий керівник

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів (розділів) дипломної роботи	Строк виконання етапів дипломної роботи	Примітка
1	Аналіз літературних джерел	10.09.2020 р.	*виконано*
2	Написання 1 розділу. Принципи організації та використання мереж з пакетною комутацією	15.09.2020 р.	*виконано*
3	Написання 2 розділу. Протоколи передачі даних та основні характеристики мереж з комутацією пакетів	25.09.2020 р.	*виконано*
4	Написання 3 розділу. Пропускна здатність мережі голосової IP - телефонії	27.10.2020 р.	*виконано*
4	Теоретичне та практичне моделювання	7.11.2020 р.	*виконано*
5	Написання 4 розділу. Моніторинг трафіку мереж з пакетною комутацією	24.11.2020 р.	*виконано*
6	Оформлення пояснювальної записки	26.11.2020 р.	*виконано*
7	Оформлення презентаційних матеріалів	2.12.2020 р.	*виконано*

Студент _____ Кубатий Н.О.
Підпис Ініціали, прізвище

Керівник роботи _____ Таранчук А.А.
Підпис Ініціали, прізвище

ЗМІСТ

ВСТУП

Розвиток глобальних мереж (англ. Wide Area Network, WAN) привів до різкого зростання кількості користувачів Інтернет – мереж у всьому світі [1].

На сучасному етапі глобальні мережі об'єднують користувачів, розташованих по всьому світі, використовуючи при цьому найрізноманітніші канали зв'язку.

Сучасний Інтернет - це складна і високотехнологічна система, що дозволяє користувачеві спілкуватися з людьми, які знаходяться в будь-якій точці земної кулі, швидко і комфортно відшукувати будь-яку необхідну інформацію, публікувати свої дані, які він хотів би повідомити всьому світу. Інтернет це не просто мережа, а структура, що об'єднує звичайні телекомунікаційні мережі. Тобто, мережу Інтернет іншими словами можна назвати «мережею мереж», яка складається з багатьох мереж, які працюють відповідно до протоколів сімейства TCP/IP. Всі мережі Інтернет об'єднані через телекомунікаційні шлюзи і використовують єдиний адресний простір і простір доменних імен [2]. Для організації телефонного зв’язку IP – телефонії по IP-мережах використовуються шлюзи IP-телефонії.

За даними аналітичного прогнозу [1] середня глобальна швидкість широкосмугового зв'язку зросте до 2023 року майже на 110,4 Мбіт/с. Швидкість широкосмугового зв’язку є вирішальним фактором, що сприяє IP - трафіку (об'єм інформації, переданий мережею за визначений період часу), яка, в свою чергу, залежить від пропускної здатності телекомунікаційної мережі.

При проектуванні мереж та їх адмініструванні, мережеві інженери та адміністратори потребують методів правильного визначення пропускної здатності проектованої мережі, або мережі, яка розширюється. Теорія масового обслуговування (МО) дає можливість проектувальникам мереж робити припущення про їх роботу на основі минулого досвіду та існуючих статистичних моделей [3]. Тому дана дипломна робота, яка полягає в удосконаленні методу визначення пропускної здатності мереж пакетної комутації є актуальною.

Використання методу визначення пропускної здатності мережі надає можливість проектувати трафік інтернет мереж, вирішувати проблеми якості зв'язку, визначити рівень обслуговування та коефіцієнт блокування мереж. Мережа, спроектована належним чином, має низький коефіцієнт блокування і високий рівень використання каналу. При підвищенні якості обслуговування зменшуються також і мережеві витрати.

Мета роботи полягає в удосконаленні методу визначення пропускної здатності мереж пакетної комутації.

Об'єкт дослідження: процеси передачі трафіку в мережах з пакетною комутацією.

Предмет дослідження: метод визначення пропускної здатності мереж з пакетною комутацією.

Для досягнення поставленої мети в роботі вирішуються наступні задачі:

1. Розглянути принципи організації та використання мереж з пакетною комутацією.
2. Дослідити протоколи передачі даних та визначити основні характеристики мереж з комутацією пакетів.
3. Розрахувати пропускну здатність мережі голосової IP – телефонії.
4. Провести моніторинг трафіку мереж з пакетною комутацією.

Наукова новизна отриманих результатів:

1. Набув подальшого розвитку метод визначення здатності мережі VoIP телефонії з використанням моделей трафіку систем масового обслуговування (СМО), зокрема:

– СМО з утриманням заблокованих викликів на основі розподілу Пуассона;

– СМО з заблокованими викликами, що перенапрямлені на основі моделі Ерланга B;

– СМО з затриманими заблокованими викликами, що побудовані на основі моделі Ерланга C.

Використання запропонованого методу дозволяє підвищити ефективність використання мережі за рахунок збільшення рівня використання каналу передачі даних та зменшення коефіцієнту блокування мережі.

Практична значимість отриманих результатів:

1. Розраховані типові затримки, що виникають при комутації пакетів VoIP мережі. Надані рекомендації для використання високошвидкісних комутаторів, які використовують буферизацію на вході з чергами віртуальних виходів для збільшення пропускної здатності мережі.

2. За допомогою активних засобів моніторингу трафіку виконано оцінку часу на прийом–передачу пакетів мережею Інтернет за допомогою спеціальних утиліт ping та tracert та програмного забезпечення, що призначене для діагностики мереж Інтернет. Виконано трасування маршруту до віддалених серверів розташованих в різних частинах світу, визначений максимальний та мінімальний час передачі пакетів – RTT, при різній кількості стрибків. Експериментально підтверджено результати аналітичних розрахунків.

Апробація результатів дослідження: Результати досліджень представлені у вигляді доповіді на науково-практичній інтернет - конференції молодих науковців і студентів «Інтелектуальний потенціал-2020.

Дипломна робота складається із вступу, чотирьох розділів, висновків до кожного розділу, висновків, списку використаних джерел, 2 додатків. Загальний обсяг роботи складає 80 сторінок комп’ютерного тексту, у тому числі: 38 рисунків, список використаних джерел вміщує 26 найменувань.

1. ПРИНЦИПИ ОРГАНІЗАЦІЇ ТА ВИКОРИСТАННЯ МЕРЕЖ З ПАКЕТНОЮ КОМУТАЦІЄЮ

1.1. Принцип організації глобальної мережі

Глобальна мережа Інтернет утворена сукупністю мереж операторів і провайдерів фіксованого та мобільного зв'язку (рисунок 1.1) [2]. Провайдери надають доступ в Інтернет (і пов'язані з цим послуги) окремим користувачам (абонентам), а також користувачам, об'єднаним в локальні мережі, прикладом яких є домашні мережі, а також мережі малих підприємств, комп'ютерні класи.

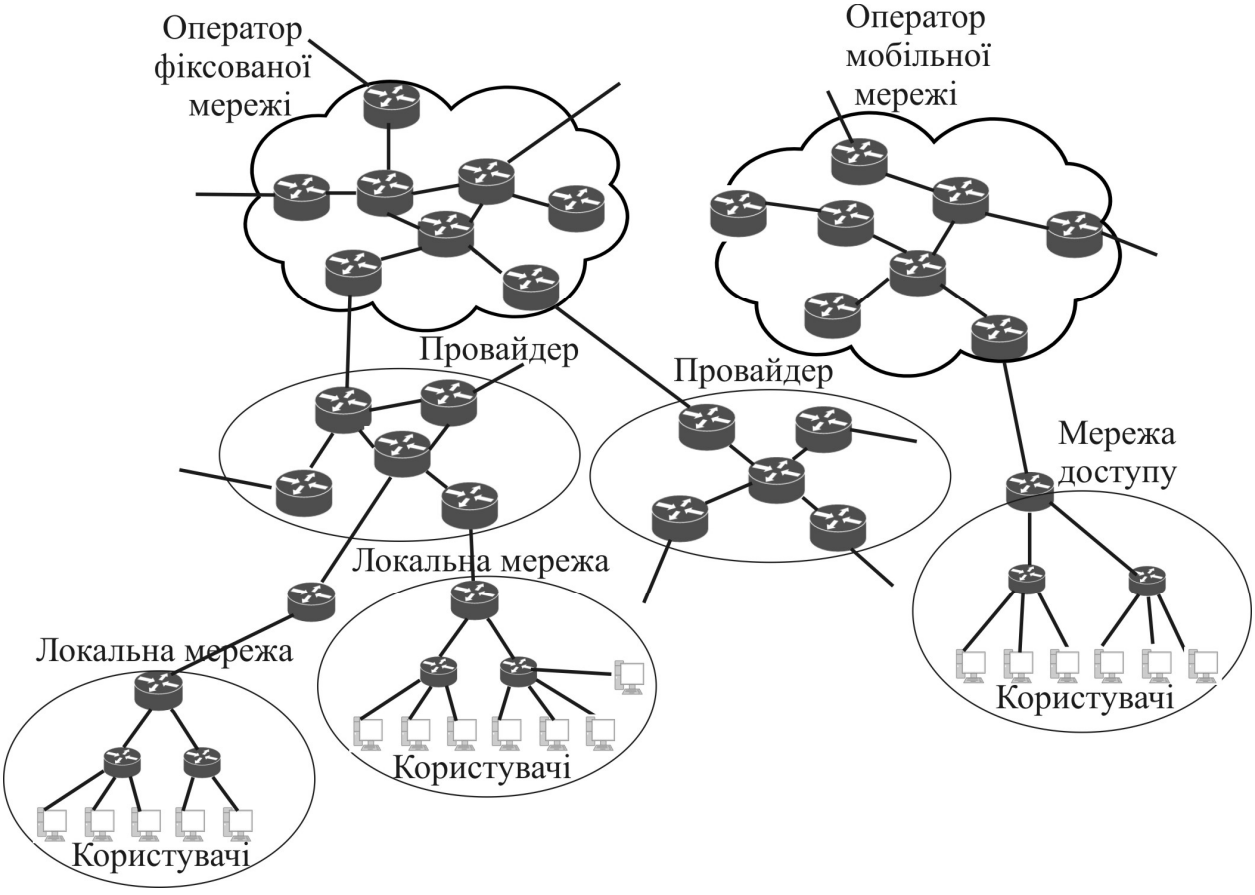


Рисунок 1.1 – Структура глобальної мережі Інтернет

В Інтернет немає єдиного пункту передплати або реєстрації, а користувачі напряму контактують з постачальником послуг, який надає їм

доступ до мережі через комп’ютер – хост провайдера. Наслідки такої децентралізації з точки зору доступності мережевих ресурсів також дуже значні. Середовище передачі даних в Інтернет не можна розглядати тільки як павутину ліній зв’язку. Дані після їх оброблення пересилаються через маршрутизатори за допомогою складних алгоритмів маршрутизації.

На відміну від локальних мереж, в складі яких є свої високошвидкісні канали передачі інформації, глобальна (а також регіональна або корпоративна) мережа включає підмережу зв’язку (інакше: територіальну мережу зв’язку, систему передачі інформації), до якої підключаються локальні мережі, окремі компоненти і кінцеві термінали користувачів (рисунок 1.1) [4,5].

Маршрутизатори об'єднують окремі мережі в загальну складову мережу. При передачі пакетної інформації маршрутизатори вибирають найкоротші маршрути для інформаційних потоків.

Внутрішня структура кожної мережі на рисунку 1.1. не відображено, так як вона не має значення при розгляді мережевого протоколу. До кожного маршрутизатора можуть бути приєднані кілька мереж.

Мережі з комутацією пакетів були розроблені урядом США в 70-і роки для забезпечення надійної цифрової передачі даних телефонними лініями.

У мережі з пакетною комутацією повідомлення поділяються на пакети [6]. Кожен пакет містить власний заголовок з керуючим і адресним полями, а також власну перевірочну послідовність знаків. Максимальна довжина пакета лежить в межах від 10000 до 20000 біт.

Пакети можуть передаватися в місце призначення за різними маршрутами мережі комутації пакетів. Різні пакети повідомлення можуть мати різні маршрути. В маршрутизації трафіку важливо досягти найкращого маршруту і якнайшвидшої їх доставки, причому для комутаційного вузла навантаження від кожного пакета можна приблизно прирівняти навантаженню від одного виклику в мережі з комутацією каналів.

Безліч джерел і приймачів повідомлень, з’єднаних між собою телекомунікаційними засобами і середовищем передачі сигналів (лініями

зв’язку), утворюють мережу передачі інформації (телекомунікаційну мережу). Абоненти, які отримують послуги телекомунікаційних мереж з обміну повідомленнями (комп’ютерними даними, аудіо-та відео), є користувачами мережевих послуг.

Апаратура абонентів (рисунок 1.2) представлена кінцевими вузлами (КВ) мереж, або кінцевим обладнанням DTE1 – DTE6 (англ. Data Terminal Equipment– DTE), які називаються хостами. З’єднання численних вузлів, що знаходяться на великій відстані між собою, зазвичай проводиться через транзитні (проміжні) мережеві з’єднувальні вузли (ЗВ1-ЗВ3) або пункти зв’язку [7].

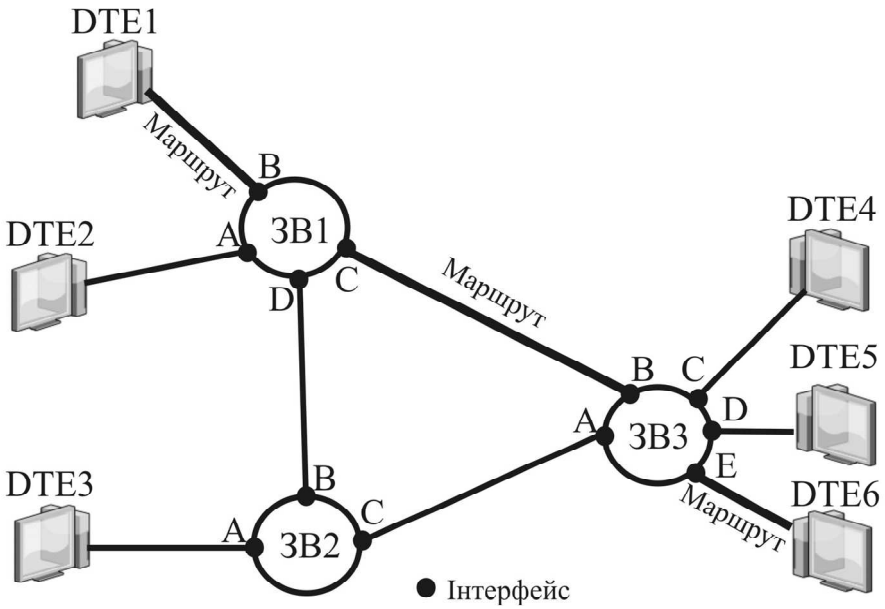


Рисунок 1.2 – Мережа передачі повідомлень

У комутаційному вузлі приймача кожен пакет перевіряється на відсутність помилок. На пакети, прийняті без помилок, у відповідь направляється підтвердження їх прийому. Якщо ж в будь-якому пакеті виявлено помилки, то надсилається запит на його повторну передачу. Мережа комутації пакетів, а саме глобальна мережа Інтернет, зазвичай має багато вузлів і забезпечує альтернативні і резервні маршрути. Ефективність

використання каналів в таких мережах вище, ніж в мережах з комутацією каналів.

1.2 Протоколи мереж з пакетною комутацією

Мережами з пакетною комутацією, працюючих за IP – протоколом передаються різні види інформації, до яких належать голос, відео, мультимедіа.

Таке об'єднання називається конвергенцією мереж і призводить до значної економії витрат на обладнання при розширення існуючих та проектування нових мереж.

Використання протоколу IP в якості транспорту інтегрованої мережі пред'являє певні вимоги до пропускної здатності мережі, часу доставки пакетів і деяким іншим параметрам. Існує декілька технологій мереж, що забезпечують задану якість сервісу та надають конвергентні послуги мережі. Розглянемо деякі з них.

1.2.1. Протокол X.25

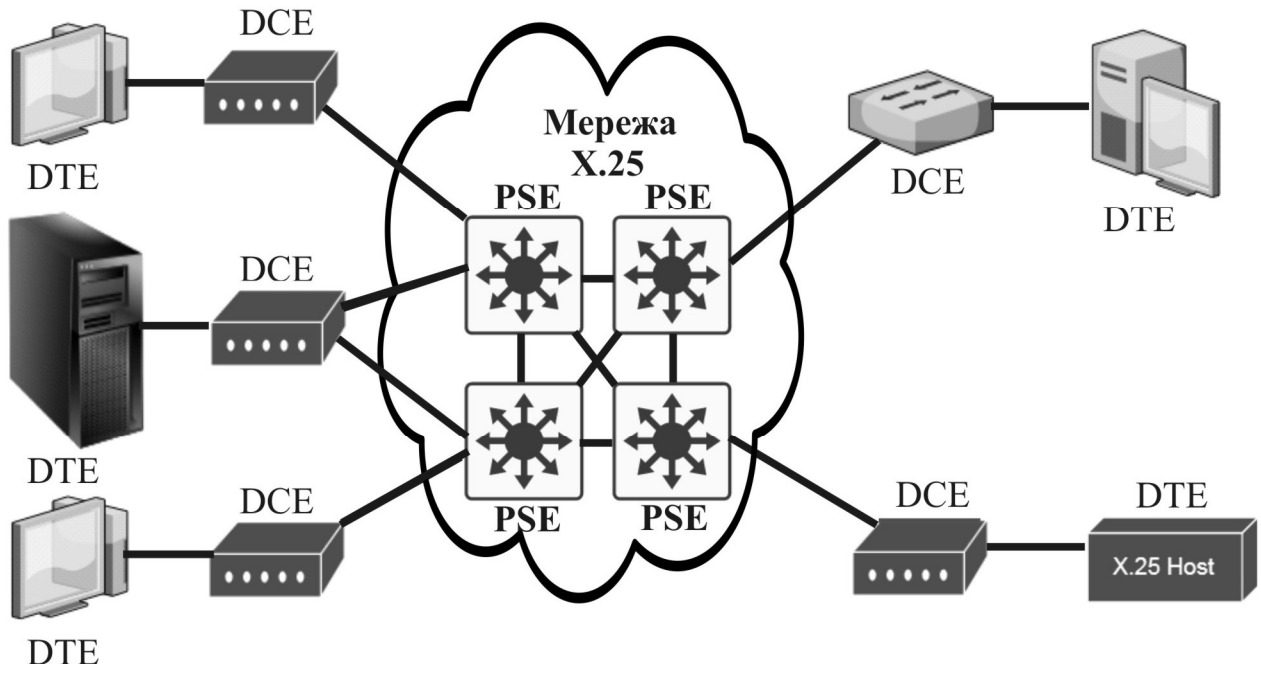
X.25 – це протокол пакетної передачі даних (прийнятий в 1976 році), який призначався для організації WAN (абр. WAN – Wide Area Networks,) на основі телефонних мереж з лініями з досить високою частотою помилок. Протокол орієнтований на роботу з встановлення з'єднань і містить розвинені механізми корекції помилок [5,7].

Даний протокол є попередником протоколу Frame Relay, який розроблено Study Group VII Міжнародним союзом телекомунікацій - ITU (абр. International Telecommunication Union) в якості пакетного протоколу передачі даних в телефонних мережах. Істотні доповнення до протоколу були прийняті у 1984 р, в даний час діє стандарт ISO 8208 протоколу X.25, стандартизований також під застосування X.25 в локальних мережах (стандарт ISO 8881). X.25 називають протоколом канального рівня за рахунок застосування інкапсуляції протоколу

IP в X.25, але протокол має всі ознаки мережевого рівня, тому що здійснює маршрутизацію між мережами і забезпечує контроль передачі між кінцевими абонентами, виконуючи функції транспортного рівня [9].

Максимальний розмір корисного блоку даних одного пакету для X.25 дорівнює 576 байт. Також це число вважається мінімальним розміром дейтаграми, яку повинен вміти прийняти і обробити будь-який хост в мережі Інтернет.

Обладнання X.25 може забезпечувати «гарячу» заміну окремих блоків. Основу мережі складають пакетні комутатори (англ. Packet switching exchange - PSE), які з'єднуються між собою синхронними каналами зв'язку через інтерфейси X.21 або синхронні модеми по каналах тональної частоти або радіоканалах (рисунок 1.3).



PSE – Packet switching exchange – Пакетний комутатор обміну
DCE – Data Circuit-terminating Equipment – Обладнання перетворення даних
DTE – Data Terminal Equipment – Термінальне обладнання даних

Рисунок 1.3 – Структура мережі, що побудована за протоколом X.25

Всі абоненти мережі X.25 діляться на синхронних і асинхронних. Синхронні мають вбудовані інтерфейси X.25 і підключаються безпосередньо до PSE, а асинхронні для передачі даних використовують вбудовані або віддалені

пакетні адаптери даних (англ. Packet Assembler-Disassembler – PAD) згідно рекомендацій X.3, X.28 і X.29.

До головного недоліку роботи мережі за протоколом X.25 можна віднести великі затримки відгуку при передачі даних, для яких типовим значенням є 0,6 секунд.

Завдяки надійності протоколу і його роботі поверх телефонних мереж загального користування X.25 широко використовувався (і місцями ще використовується) як в корпоративних мережах, так і у всесвітніх спеціалізованих мережах надання послуг, таких як SWIFT (банківська платіжна система, припинили використання у 2005 році) і SITA-система інформаційного обслуговування повітряного транспорту). В даний час X.25 практично витіснений іншими технологіями канального рівня (Ethernet, Frame Relay, ISDN і т. інші.) і протоколом IP, залишаючись, проте, досить поширеним в країнах і територіях з нерозвиненою телекомунікаційною інфраструктурою. Також протокол продовжує використовуватися в банківських мережах, там, де потрібна висока надійність.

1.2.2. Протокол Frame Relay

Протокол Frame Relay забезпечує комутацію пакетів між призначеними для користувача інтерфейсами - кінцевим обладнанням користувачів DTE і мережевими інтерфейсами (інтерфейсами комутаторів) - кінцевим обладнанням каналів передачі даних (DCE) (рисунок 1.4).

Як протокол канального рівня, Frame Relay багато в чому подібний до відповідних елементів сімейства X.25, проте відрізняється за своєю функціональністю і формату пакетів, які передаються. Зокрема, Frame Relay краще структурований і забезпечує більш високу продуктивність і ефективність використання мереж.

Frame Relay підтримує статистичне мультиплексування численних логічних з'єднань по єдиному фізичному каналу. Такий підхід суттєво відрізняється від систем з мультиплексуванням і поділом у часі (англ. Time

Division Multiplexing – TDM). Статистичне мультиплексування Frame Relay забезпечує більш ефективне і гнучке використання пропускної здатності мережі і може застосовуватися самостійно або в каналах на базі TDM [10].

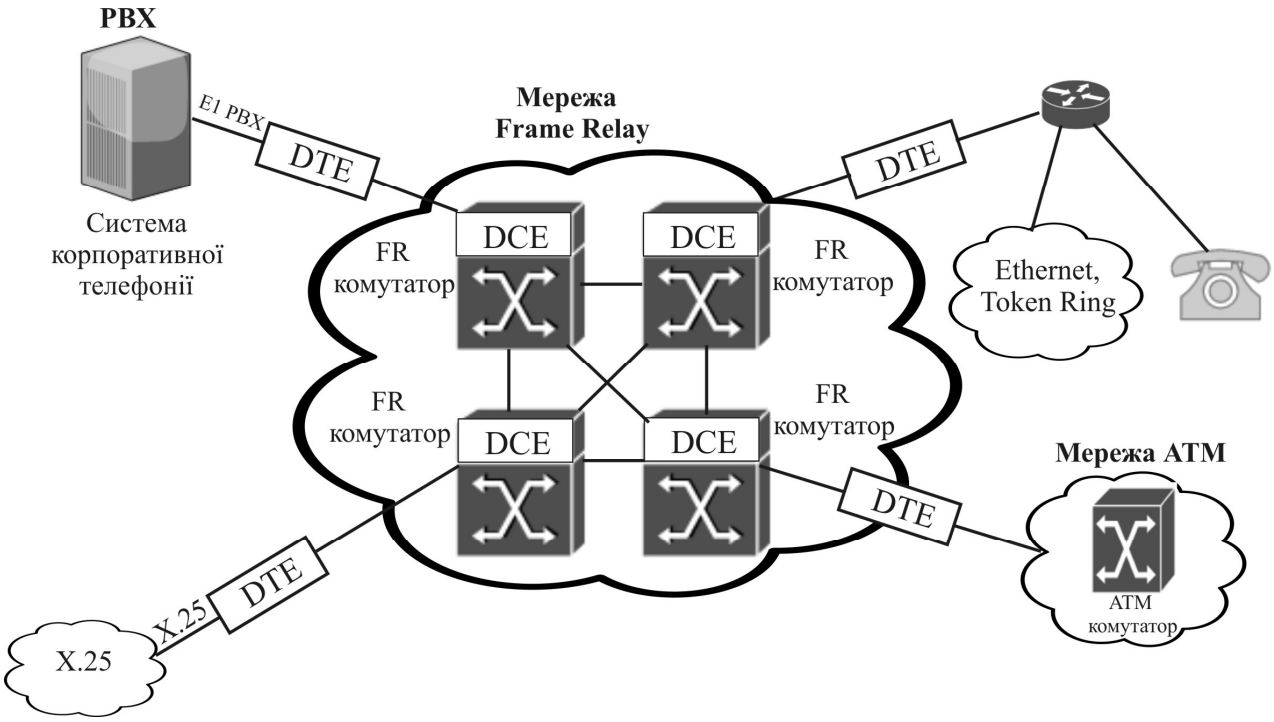


Рисунок 1.4 – Структура мережі побудована за протоколом Frame Relay

Іншою важливою перевагою Frame Relay є використання сучасних технологій передачі для глобальних мереж (WAN). Застосування надійних і практично безпомилкових оптичних ліній дозволяє позбавити протоколи канального рівня від виправлення помилок, передавши ці функції протоколів більш високих рівнів. Frame Relay просто відкидає помилкові (з невірною контрольною сумою) пакети, не намагаючись виправити помилки (наприклад, за рахунок повторної передачі).

Ще однією істотною відмінністю Frame Relay від X.25 є відсутність явного управління потоком даних, оскільки в наш час подібні функції управління ефективно реалізуються протоколами більш високих рівнів. Замість цього використовується механізм повідомлень про наближення до стану насичення, які передаються на вище розташовані рівні, де і реалізуються функції управління потоком даних.

Сучасний стандарт Frame Relay підтримує постійні віртуальні з'єднання (англ. Permanent Virtual Circuits, PVC), які настроюються і керовані в масштабах мережі. Іншим типом є комутовані віртуальні з'єднання (англ. Switched Virtual Circuits, SVC).

Основні особливості протоколу Frame Relay [10]:

– підтримка декількох віртуальних з'єднань на один фізичний порт;

– управління швидкістю передачі: гарантована швидкість передачі (Committed Information Rate, CIR) та форсована швидкість передачі (Excess Information Rate, EIR);

– підтримка повідомлень про насичення мережі.

1.2.3 Протокол ATM

ATM (англ. Asynchronous Transfer Mode) є комутованою технологією, призначеною для одночасної передачі голосу і даних у вигляді комірок (англ. cell) фіксованої довжини, що зменшує час на обробку і дозволяє забезпечити більш рівномірне завантаження процесора [10,11].

ATM вирішує проблему затримок в мережі за рахунок розподілу інформації будь-якого типу на невеликі комірки фіксованої довжини. Комірка ATM має розмір 53 байти, п'ять з яких складають заголовок, а інші, що залишилися 48 - власне інформацію. У мережах ATM дані повинні вводитися в формі комірок або перетворюватися в комірки за допомогою функцій адаптації. Мережі ATM складаються з комутаторів, з'єднаних транковими каналами ATM. Кінцеві комутатори, до яких підключаються призначені для користувача пристрої, забезпечують функції адаптації, а якщо ATM не використовується тоді до призначених для користувача станцій. Інші комутатори, розташовані в центрі мережі, забезпечують перенесення комірок, поділ транків і розподіл потоків даних. У телефоні функції адаптації відновлюють з комірок вихідний потік даних і передають його на пристрій-одержувач, як показано на рисунку 1.5.

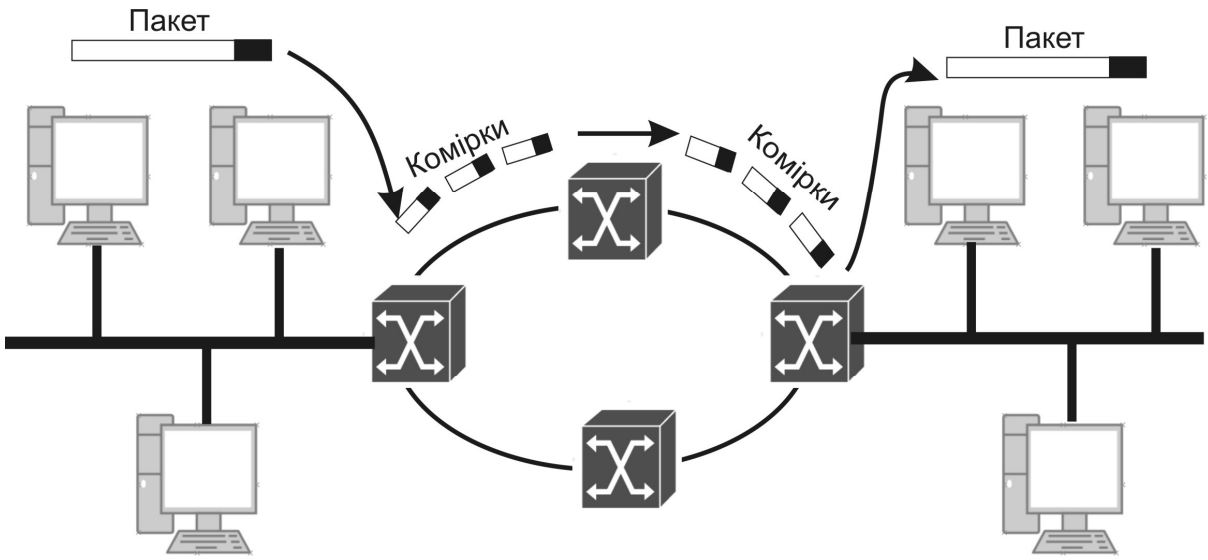


Рисунок 1.5 – Адаптація АТМ

Передача даних в коротких комірках дозволяє АТМ ефективно управляти потоками різної інформації і забезпечує можливість пріоритезації трафіку. Передбачуваний час процесорної обробки комірок дозволяє забезпечити ефективне, високошвидкісне управління змішаним трафіком голос / дані, оскільки в АТМ для комутації використовуються спеціалізовані мікросхеми.

У технології АТМ передбачений механізм встановлення з'єднання між точками, які будуть вести передачу. Недоліки такого методу, пов'язані з накладними витратами на початковому етапі взаємодії, що компенсуються можливістю установки з'єднання з гарантованою смугою пропускання.

В мережі АТМ з встановленням з'єднань може здійснюватися одночасна передача різних видів трафіку, що залежить від якості сервісу, наприклад, звуку, відео і даних (рисунок 1.6).

На рисунках 1.6-1.8 показані типові користувацькі пристрої, що породжують різнотипний трафік (голос, відео, дані). Ці три типи трафіку можуть передаватися з використанням сервісу АТМ трьома показаними на рисунках способами.

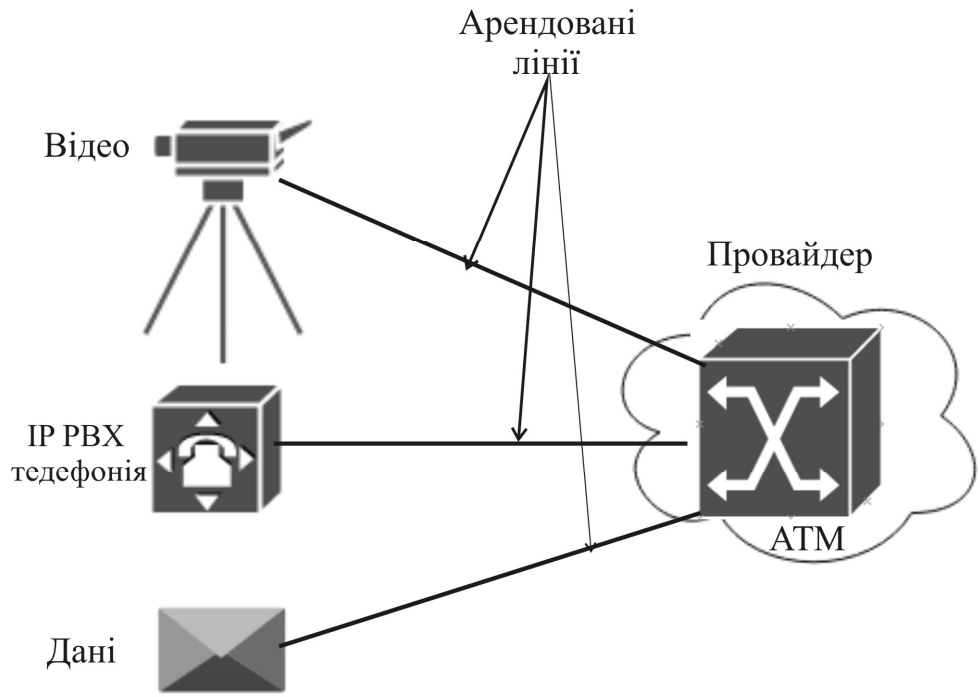


Рисунок 1.6 – Перетворення в ATM здійснюється оператором мережі

На рисунку 1.7 наведена інше рішення для побудови мереж ATM, де локальні обчислювальні мережі (ЛОМ), голосові і відео-пристрої підключаються до локального комутатора ATM для перетворення трафіку в комірці. Для доступу в мережу оператора використовується одна лінія, що передає всі потоки трафіку одночасно (як віртуальні пристрої). Мережа оператора забезпечує маршрутизацію трафіку. Таке рішення більш економічне і може використовуватися для організації "приватних мереж ATM" для користувачів, які мають доступ до ATM-сервісу або хочуть створити свою розподілену мережу на базі ATM. При цьому, комутатор ATM може знаходиться в мережі користувача або належати оператору (провайдеру) і перебувати у нього на обслуговуванні.

На рисунку 1.8 наведений приклад побудови мережі ATM, де пристрої обладнуються власними інтерфейсами ATM. Один пристрій доступу дозволяє об'єднати весь призначений для користувача трафік в одному транку, пов'язаному з мережею оператора. У цьому випадку на стороні користувача встановлюється належне йому обладнання ATM, яке можна використовувати для організації магістралей ЛОМ або підключення настільних станцій.

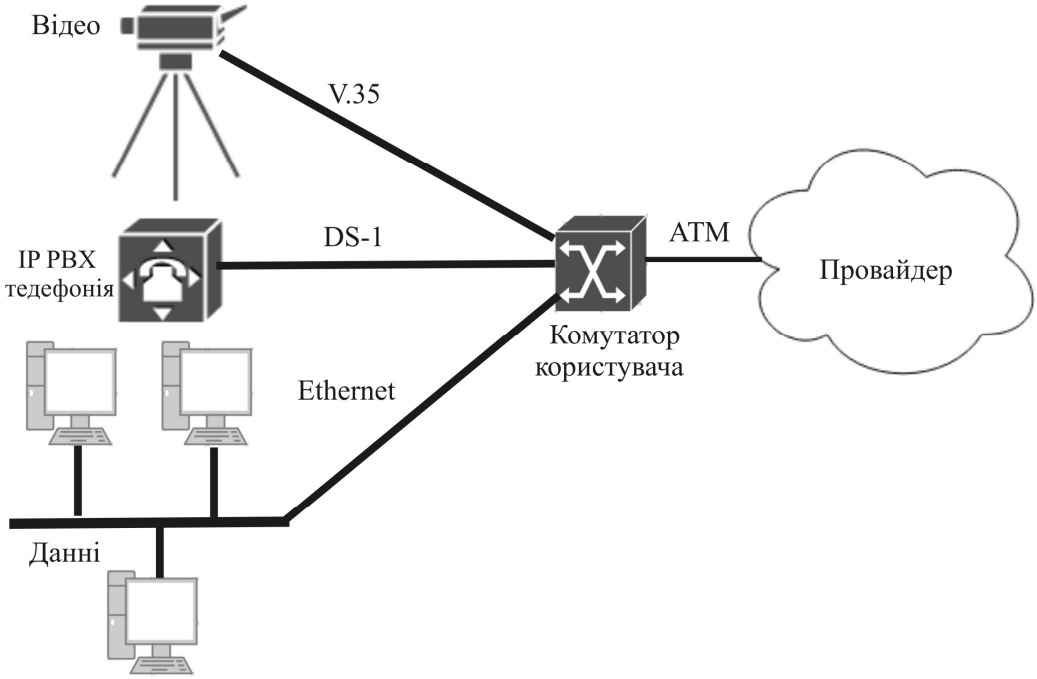


Рисунок 1.7 – Перетворення в ATM здійснюється у користувача

Швидкої появи інтерфейсів ATM в телефонному та відео-обладнанні не представляється можливим, тому реалізація третього варіанту з'єднання з мережею не зможе в найближчі роки стати домінуючим. Фактично, швидкість поширення кожного з наведених варіантів буде визначатися темпами зниження цін на обладнання та послугами операторів мереж ATM. Відсутність ефективного управління цими процесами породжує певний хаос і не дозволяє надійно передбачити перспективи того чи іншого сервісу ATM.

Стандарт, який визначає інтерфейс між операторами і користувачами ATM називається Public User Network Interface або Public UNI. Цей інтерфейс визначається для різних значень швидкості. Перші послуги ATM пропонувалися в основному зі швидкістю T3 (45 Мбіт / с). Зараз багато операторів пропонують швидкість 155 Мбіт / с і вище, але така смуга звичайно не потрібна користувачам, також і вартість подібних послуг досить висока. Для більшості користувачів, які планують організувати доступ до ATM або створити приватну мережу ATM основною проблемою є вартість обладнання.

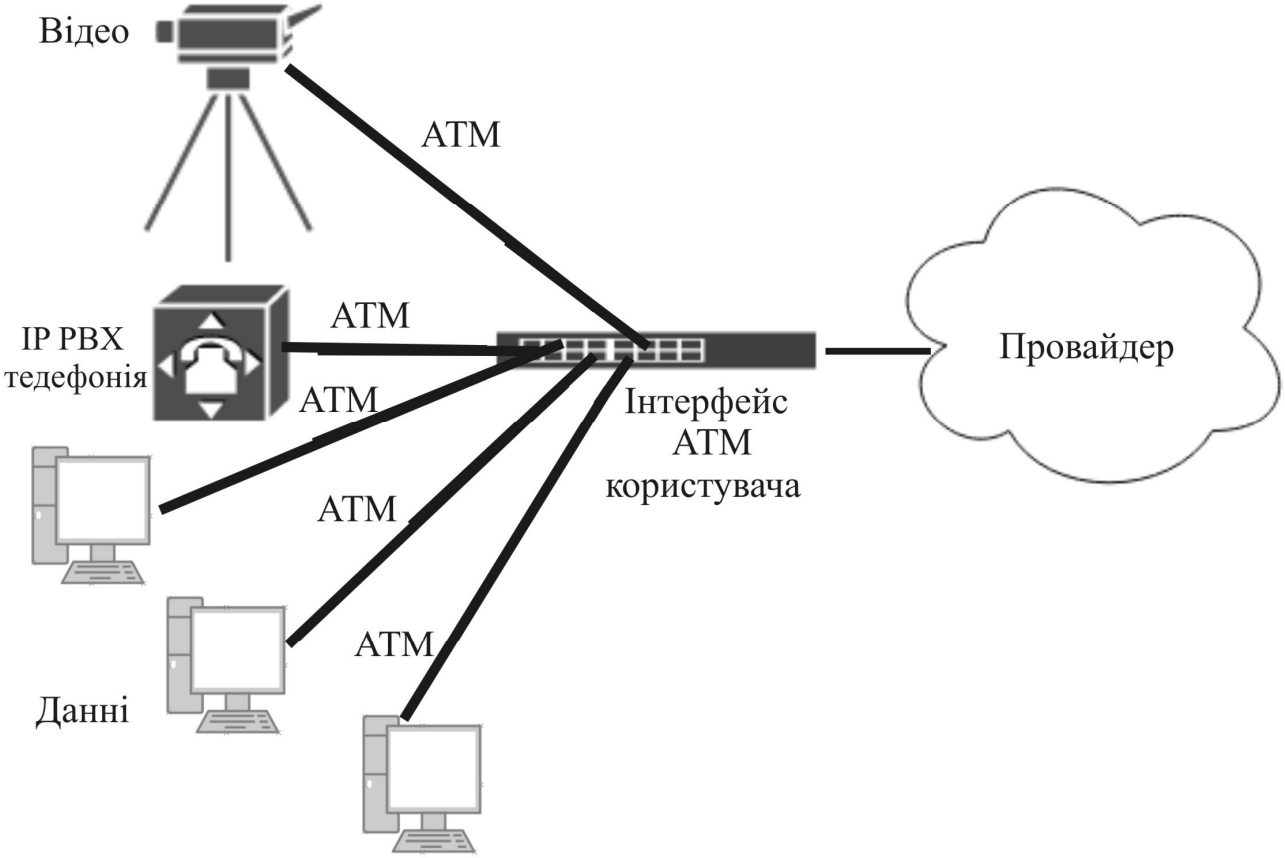


Рисунок 1.8 – Мережа на базі ATM

1.3 Комутовані мережі Ethernet

За останні кілька років Ethernet стала найпопулярнішою технологією для локальних мереж (LAN). У всьому світі нараховується мільйони користувачів Ethernet. У 1998 році був випущений стандарт для 1-гігабітної мережі Ethernet. Це викликало велику увагу з боку користувачів, особливо багатьох з тих, хто не хотів застосовувати дорогу технологію ATM для своїх локальних мереж. Протягом кількох років 1-гігабітний Ethernet домінував на ринках локальної мережі. Але оскільки попит на високошвидкісні мережі продовжував зростати то очевидно, що виникла потреба у швидшій технології Ethernet [5,13].

З моменту свого створення Ethernet розвивався, щоб задовольнити зростаючий попит на високошвидкісні локальні мережі. Коли був представлений оптичний волоконний носій, Ethernet адаптувався до цієї нової

технології, щоб скористатися перевагою пропускної здатності та низьким рівнем помилок, які пропонує волокно. Сьогодні той самий протокол, який передавав дані зі швидкістю 3 Мбіт / с, може передавати дані зі швидкістю 10 Гбіт / с та вище.

Перші версії Ethernet використовували коаксіальний кабель для підключення комп'ютерів у топології шини. Кожен комп'ютер був безпосередньо підключений до магістралі. Ці ранні версії Ethernet були відомі як 10BASE5 і 10BASE2. 10BASE5 використовував «товстий» коаксіальний кабель, який дозволяв проводити кабельні відстані до 500 метрів, перш ніж сигнал вимагав повторювача. 10BASE2 використовував «тонкий» коаксіальний кабель, який був меншим у діаметрі та більш гнучким, ніж «товстий» і дозволяв проводити кабельні відстані 185 метрів.

Ранні реалізації Ethernet були розгорнуті в середовищі з низькою пропускною здатністю локальної мережі. На додаток до топології логічної шини на рівні ліній передачі даних, Ethernet також використовував фізичну топологію шини. Ця топологія стала більш проблематичною, оскільки локальні мережі зростали, а послуги локальних мереж вимагали змін до їхньої інфраструктури. Оригінальні товсті коаксіальні та тонкі коаксіальні фізичні середовища були замінені ранніми категоріями кабелів UTP. У порівнянні з коаксіальними кабелями UTP-кабелі були простішими в роботі, легкими та менш дорогими. Фізична топологія «шина» також була змінена на топологію «зірка» та будувалась на допомогою концентраторів, які були центрами концентрації з'єднань. Використання концентратора в цій топології підвищило надійність мережі, дозволивши будь-якому одному кабелю вийти з ладу, не порушуючи всю мережу. Однак повторення кадру на всіх інших портах концентраторів при передачі даних, не вирішило проблеми виникнення колізій.

У періоди низької комунікаційної активності нечисленні колізії, що трапляються, управляються методом доступу до середовища з прослуховуванням носійної та контролем колізій (англ. Carrier Sense Multiple Access with Collision Detection, CSMA / CD), що не дуже впливало на

продуктивність. Однак із збільшенням кількості пристроїв та подальшого трафіку даних зростання кількості зіткнень може мати значний вплив на мережеву продуктивність [13].

Значним розвитком, який покращив продуктивність локальної мережі, стало введення комутаторів взамін концентраторів у мережах на базі Ethernet. Ця розробка тісно відповідала розробці Ethernet 100BASE-TX. Комутатори можуть керувати потоком даних, ізолюючи кожен порт і надсилаючи кадр лише до відповідного місця призначення (якщо пункт призначення відомий), а не надсилаючи кожен кадр на кожен пристрій. Комутатор зменшує кількість пристроїв, які отримують кожен кадр, що в свою чергу зменшує або мінімізує можливість зіткнень. Це, а пізніше впровадження повнодуплексного зв'язку дозволило розвивати 1 Гбіт / с Ethernet, а також і подальші стандарти.

Однією з головних переваг 10-гігабітного стандарту Ethernet є те, що він пропонує недороге рішення для вирішення вимог до пропускної здатності. Не тільки вартість установки низька, але й вартість обслуговування та управління мережею також мінімальна. Управління та обслуговування 10-гігабітної мережі Ethernet можуть здійснювати адміністратори локальної мережі.

На додаток до переваг зниження витрат, 10-гігабітний Ethernet може дозволити швидше перемикання. Оскільки 10-гігабітний Ethernet використовує той самий формат Ethernet, це дозволяє безперешкодно інтегрувати LAN, MAN та WAN. Немає необхідності в фрагментації пакетів, повторному складанні або перекладі адрес, усуваючи необхідність у маршрутизаторах, які набагато повільніші за комутатори. 10-гігабітний Ethernet також пропонує пряму масштабованість (10/100/1000/10000 Мбіт / с). Оновлення до 10-гігабітної мережі Ethernet повинно бути простим, оскільки шляхи оновлення подібні до шляхів 1-гігабітної мережі, яка добре знайома до моменту випуску стандарту 10-гігабітної мережі. Основні проблеми полягають у тому, що 10-гігабітний Ethernet оптимізований для передачі даних і що він не забезпечує вбудовану якість послуг. Однак якість послуг може надаватися на вищих рівнях [13].

Існує широкий попит на 10-гігабітну мережу Ethernet на ринках локальної мережі (LAN), мережі мегаполісів (MAN) та мережі глобальної мережі (WAN). Кожен ринок, як правило, має різні вимоги.

На розробку та ратифікацію шести стандартів Ethernet (10 Мбіт / с до 100 Гбіт / с) IEEE знадобилося 35 років. В даний час додаткові шість стандартів Ethernet або нещодавно завершили розробку, або перебувають на завершальній стадії (рисунок 1.9). Ці нові стандартизовані швидкості портів варіюються від оптичного Ethernet 400 / 200G для високошвидкісного маршрутизатора та комутаторів між з'єднаннями до швидкості 5G / 2,5G для збільшення пропускної здатності при повторному використанні існуючих мідних кабелів Cat 5e /6. Хоча, ймовірно, пройде деякий час, перш ніж деякі з цих стандартів побачать широке розгортання, дизайнерам центрів обробки даних потрібно підготуватися зараз, щоб не відставати від попиту на пропускну здатність та модернізації технологій, які дозволять їм залишатися конкурентоспроможними.

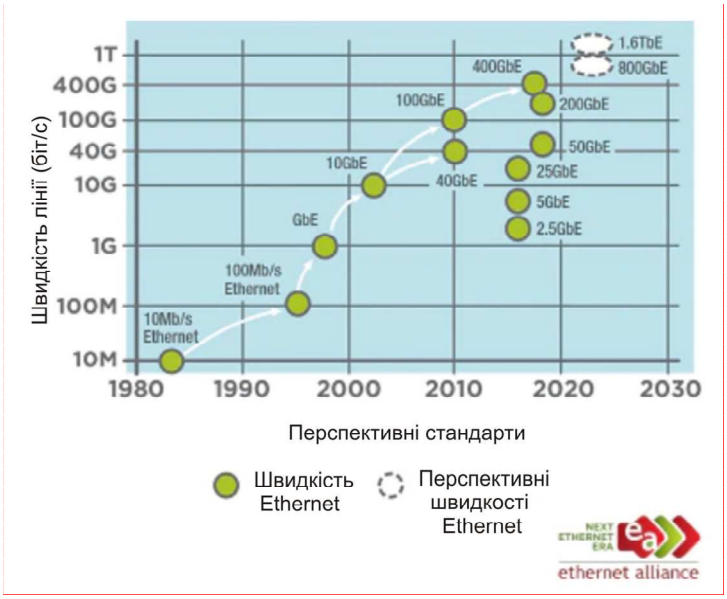


Рисунок 1.9 – Перспективні швидкості Ethernet,
що заплановані Ethernet Alliance до 2030 року

Висновки до першого розділу

1. Розглянуто принципи організації глобальної мережі, описана структура та протоколи мережі з пакетною комутацією повідомлень. Показано, що використання протоколу IP в якості транспорту інтегрованої мережі пред'являє високі вимоги до пропускної здатності мережі та часу доставки пакетів.

2. Проведений аналіз комутованих технологій показав, що існує декілька технологій мереж - X.25, Frame Relay, ATM, Ethernet, що забезпечують задану якість сервісу та надають конвергентні послуги мережі. Показано, що найбільш перспективною технологією є Ethernet, який пропонує масштабованість 10/100/1000/10000 Мбіт/с, завдяки використання одного формату Ethernet кадру у всіх його модифікаціях, це дозволяє безперешкодно інтегрувати LAN, MAN та WAN та будувати високошвидкісні мережі з високою пропускною здатністю.

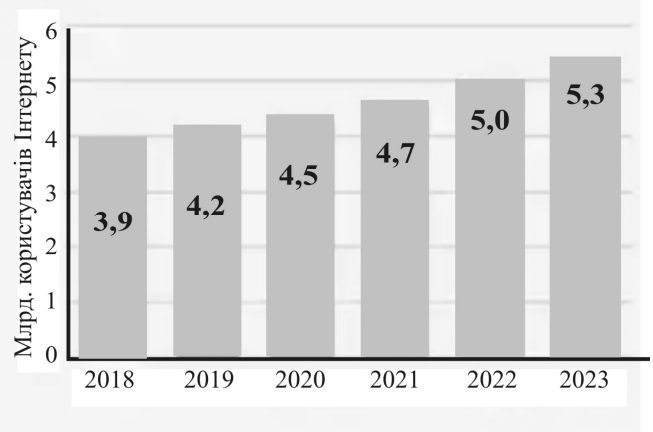
3. Виявлено, що швидкість широкосмугового зв’язку є вирішальним фактором, що сприяє IP - трафіку, яка, в свою чергу, залежить від пропускної здатності телекомунікаційної мережі. Тому, при проектуванні мереж та їх адмініструванні, мережеві інженери та адміністратори потребують методів правильного визначення пропускної здатності проектованої мережі, або мережі, яка розширюється.

2 ПРОТОКОЛИ ПЕРЕДАЧІ ДАНИХ ТА ОСНОВНІ ХАРАКТЕРИСТИКИ МЕРЕЖ З КОМУТАЦІЄЮ ПАКЕТІВ

2.1 Аналіз сучасного трафіку глобальної мережі

Активний розвиток мережевих технологій та розширення об’єму інфо-телекомунікаційних послуг обумовлює постійний приріст нових користувачів. При цьому також спостерігається збільшення об’ємів мережевого трафіку.

За даними глобального прогнозу та річного звіту Cisco, близько двох третин світового населення матимуть доступ до Інтернету вже у 2023 році (рисунок 2.1). Згідно проведених досліджень [1] кількість пристроїв, підключених до IP-мереж, буде втричі перевищувати загальносвітове населення. На кожного користувача мережі інтернет буде припадати біля 3,6 мережевих пристроїв, а всього мережевих пристроїв збільшиться до 29,3 млрд. (рисунок 2.2). При цьому, кількість користувачів Інтернету сягне 5,3 мільярди, що складе 66 відсотків світового населення [1].

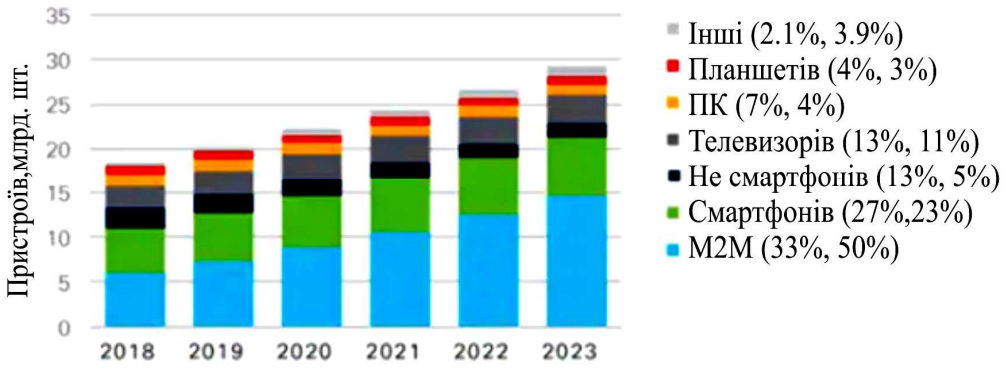


(Джерело: Річний звіт Cisco в Інтернеті, 2018-2023)

Рисунок 2.1 – Глобальний ріст користувачів Інтернету

Мережі, що призначені для передачі голосу або даних створюються з урахуванням безлічі різних факторів. Серед них два фактори: пропускна здатність мережі, і витрати є найбільш важливими при проектуванні, або розширенні мережі. При цьому, пропускна здатність і отже, якість зв'язку

важлива для задоволення клієнта, а витрати завжди впливають на отриманий прибуток.



(Джерело: Річний звіт Cisco в Інтернеті, 2018-2023)

Рисунок 2.2 – Глобальний ріст пристроїв та з'єднань

В сучасних IP-мережах з появою безлічі нових мережевих пристроїв (рисунок 2.2) оцінити необхідну пропускну здатність стає все важче: як правило, необхідно знати, які програми планується застосовувати, які протоколи передачі даних вони використовують і яким чином будуть здійснювати обмін даними.

2.2 Стек протоколів TCP / IP

Функціонування Інтернету базується на технологіях мереж з комутацією пакетів, основу яких складає розроблений стек протоколів TCP / IP (абр. Transmission Control Protocol / Internet Protocol - протокол управління передачею / міжмережний протокол). Стек протоколів TCP / IP представляє собою сукупність правил, що дозволяють абонентам спільно використовувати мережеві ресурси [5,12,13].

На рисунку 2.3 представлено співвідношення чотирирівневої архітектури протоколів TCP / IP і семирівневої архітектури OSI [14].

Об'єднання канального і фізичного рівнів моделі OSI в єдиний мережевий рівень TCP / IP було обумовлене вимогою незалежності від використовуваного середовища передачі даних. Справа в тому, що функції протоколів канального і

фізичного рівнів реалізуються в даний час, як правило, єдиними технічними засобами (мережевими контролерами).

Відповідно до термінології TCP / IP елементи мережевого рівня називаються підмережами. Ідеологія TCP / IP допускає, щоб в якості "підмереж" виступали реальні мережі з їх власними стеками протоколів, вузлами, шлюзами і т.п.

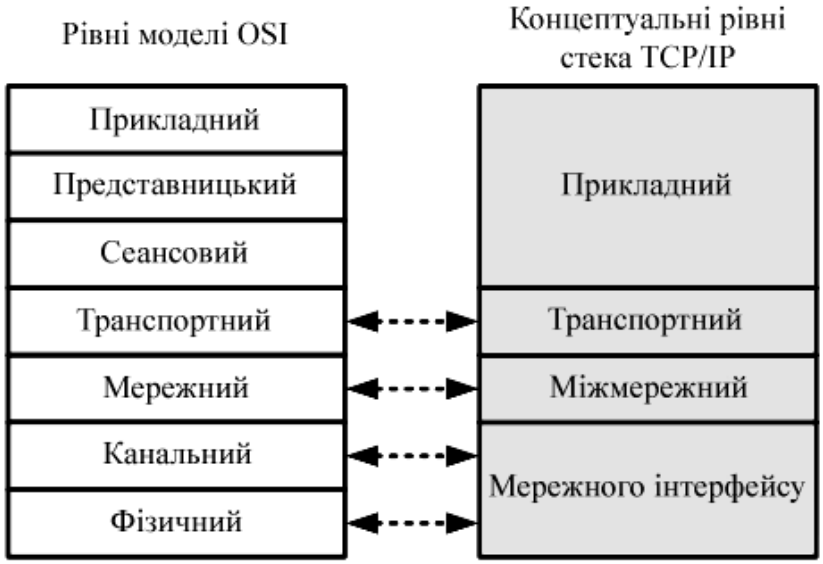


Рисунок 2.3 - Співвідношення чотирирівневої архітектури протоколів TCP / IP і семирівневої архітектури OSI

На рисунку 2.4 представлена архітектура основних протоколів TCP / IP, які використовуються на трьох нижніх рівнях стеку.

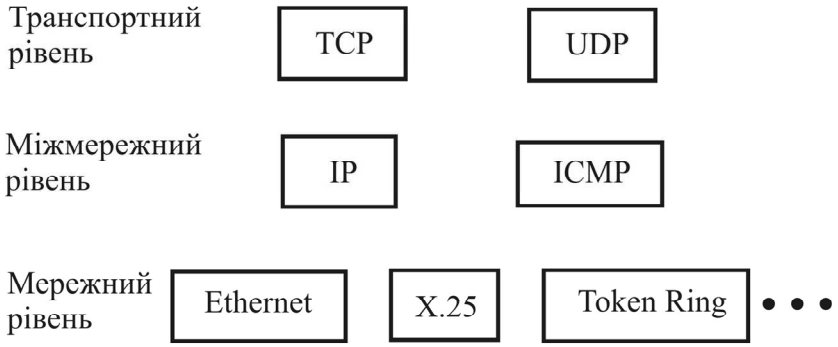


Рисунок 2.4 - Архітектура основних протоколів TCP / IP, які використовуються на трьох нижніх рівнях стеку

Основою усієї архітектури є міжмережний протокол IP (англ. Internet Protocol). З його допомогою реалізується адресація вузлів мережі і доставка даних. Міжмережний протокол керуючих повідомлень ICMP (англ. Internet Control Message Protocol) призначений для передачі діагностичної інформації та повідомлень про помилки в роботі мережі.

Протокол ICMP віднесений до міжмережного рівня умовно, тому що, з одного боку, він користується можливостями протоколу IP для транспортування власних даних, але, з іншого боку, сам для транспортування даних користувача не застосовується.

Двома основними протоколами транспортного рівня є надійний протокол управління передачею даних TCP (англ. Transmission Control Protocol) і швидкий протокол дейтаграм користувача UDP (англ. User Datagram Protocol). TCP реалізує мережну взаємодію в режимі з встановленням логічного (віртуального) з'єднання, а UDP – його не використовує.

Функції кожного протоколу реалізуються компонентою програмного забезпечення - модулем. Взаємодія модулів сусідніх рівнів здійснюється через стандартизований інтерфейс.

На кожному рівні стека протоколів TCP / IP обмін даними ведеться блоками даних кінцевої довжини. Однак, до сих пір, відсутня усталена термінологія в позначенні цих блоків.

2.3 Міжмережний протокол

Міжмережний протокол IP специфікований в RFC 791. Його основні характеристики перераховані нижче:

– реалізує обмін інформації IP- сегментами (максимальний розмір IP-сегмента - 65535 байт);

– є протоколом взаємодії без встановлення логічного з'єднання;

– для адресації вузлів мережі використовується адреса довжиною 4 байта;

– забезпечує в разі потреби фрагментацію IP-сегментів;

– IP-сегменти мають кінцевий час життя в мережі;

– не гарантує надійність доставки IP- сегментів адресату;

– не має засобів управління інтенсивністю передачі IP-сегментів, що надсилає (flow control);

– не гарантує правильну послідовність IP-сегментів на приймаючій стороні.

На рисунку 2.5 наведений формат заголовка IP-сегмента [15].

Рисунок 2.5 - Формат заголовка IP-сегмента

Розглянемо призначення полів IP –сегмента [15]:

1. Версія. 4-х бітове поле, що містить номер версії протоколу IP (номер поточної версії IPv4);

2. Довжина заголовка - 4-х бітове поле, що містить довжину заголовка IP-сегмента в 32-бітових словах. Мінімальна (і типова) довжина заголовка - п'ять слів.

3. Тип обслуговування - байт, що містить набір критеріїв, що визначають тип обслуговування IP-сегментів. Детальний опис окремих бітів дано нижче:

– біти 0 ... 2 - пріоритет (англ. precedence - перевага) даного IP-сегмента;

– біт 3 - вимога до часу затримки (англ. delay) передачі IP-сегмента (0 - нормальна, 1 - низька затримка);

– біт 4 - вимога до пропускної здатності (англ. throughput) маршруту, по якому повинен відправлятися IP-сегмент (0 - низька, 1 - висока пропускна здатність);

– біт 5 - вимога до надійності (англ. reliability) передачі IP-сегмента (0-нормальна, 1 - висока надійність);

– біти 6 ... 7 - зарезервовані.

4. Довжина сегмента - двобайтове поле, що містить довжину (в байтах) усього IP-сегмента, включаючи довжину заголовка. Максимальна довжина IP-сегмента (включаючи заголовок) - 65535 байт. Специфікація IP протоколу встановлює, що будь-який вузол мережі повинен бути здатний обробляти IP-сегменти довжиною не менш 576 байт (що відповідає 512 байтам даних при можливій довжині заголовка до 64 байт). На практиці ж, вузли мережі можуть обробляти IP-сегменти багато довше, ніж 576 байт (як правило, допустима довжина IP-сегмента пов'язана з максимальною довжиною кадру нижчого мережного рівня).

5. Ідентифікатор - двобайтове поле, що містить унікальний ідентифікатор IP-сегмента, який присвоюється йому вузлом, який відповів. Це поле використовується для розпізнавання фрагментів одного IP-сегмента (в ситуаціях, коли в ході переміщення по глобальній мережі єдиний IP-сегмент був розбитий на кілька фрагментів з причини його неприпустимо великої довжини).

6. Прапорці (DF, MF) - біти, що використовуються при обробці фрагментованих IP-сегментів. Якщо біт DF (Do not Fragment) встановлено в 1, то це означає, що IP-сегмент не може бути розбитий на фрагменти ні за яких умов (навіть, якщо він не може бути переданий без цього далі до адресата і повинен бути знищений). Біт MF (More Fragments) вказує, є (MF - 0) чи ні (MF - 1) даний IP- "підсегмент" останнім в ланцюжку IP- "підсегменту", в яку був перетворений (фрагментований) вихідний IP-сегмент.

7. Зміщення фрагмента - 13-бітове поле, що є фрагментом іншого (вихідного) IP-сегмента. Це поле містить зміщення даних, що містяться в IP-

фрагменті, по відношенню до початку даних вихідного IP-сегмента. Зсув вимірюється в восьмибайтових одиницях, тому 13 бітів достатньо для подання зміщення в IP-сегменті максимальної можливої довжини $8 \cdot 2^{13} - 1 = 65535$.

8. Час життя - однобайтовое поле, що заповнюється вузлом мережі, який створює IP-сегмент кількістю одиниць часу життя IP-сегмента в мережі. На практиці, час життя (англ. TTL - Time To Live) - це максимальна кількість вузлів, пройшовши через які буде знищенний IP-сегмент. Кожен IP-модуль на будь-якому вузлі мережі зобов'язаний знищувати IP-сегменти, для яких поле "час життя" стало рівним нулю. Цим запобігається поява в мережі IP-сегментів, які не будуть передаватись нескінченний час. При цьому вузлу-джерелу знищеного IP-сегмента посилається ICMP-сегмент, що сповіщає про цю подію.

9. Протокол - поле розміром в байт, що містить ідентифікатор протоколу більш високого (зазвичай, транспортного) рівня, для якого призначені дані IP-сегмента.

10. Контрольна сума заголовка - двобайтове поле, що містить контрольну суму заголовка IP-сегмента (для даних IP-сегмента контрольна сума не підраховується; контролювати дані - задача протоколів транспортного рівня). Для обчислення контрольної суми повинен використовуватися ефективний і простий алгоритм. У всіх протоколах, що входять в архітектуру TCP / IP, використовується так звана Internet-контрольна сума, яка є доповненням 16-бітної суми всіх 16-бітних слів контрольованої інформації.

11. Адреса джерела і адреса приймача - чотирибайтові IP-адреси вузлів мережі.

12. Додаткові дані заголовка - послідовність полів довільної довжини, що описують необов'язкові дані заголовка. Такі дані використовуються для спеціальних цілей (управління мережею, таємність і т.п.).

13. Дані вирівнювання - дані, що не мають сенсу і включаються в заголовок тільки для вирівнювання його довжини до розміру чотирибайтового слова.

2.4 Протокол управління передачею

Протокол управління передачею TCP є протоколом транспортного рівня і базується на можливостях, що надаються міжмережним протоколом IP. Основне завдання TCP - забезпечення надійної передачі даних в мережі. Протокол TCP описаний в RFC 793. Його основні характеристики перераховані нижче [5,16]:

– реалізує взаємодію в режимі з встановленням логічного (віртуального) з'єднання;

– забезпечує двосторонній дуплексний зв'язок;

– організовує потоковий тип передачі даних;

– дає можливість пересилки частини даних, як "екстрених";

– для ідентифікації партнерів по взаємодії на транспортному рівні використовує 16-бітові "номери портів";

– реалізує принцип «ковзного вікна» для підвищення швидкості передачі;

– підтримує ряд механізмів для забезпечення надійної передачі даних.

Незважаючи на те, що для користувача передача даних з використанням протоколу TCP виглядає як потокова, насправді ж обмін між партнерами здійснюється за допомогою пакетів даних, які називають "TCP-пакетами".

Порт джерела (*Source port*)											Порт призначення (*Destination port*)
Номер послідовності (*Sequence number*)											
Номер підтвердження (*Acknowledgment number*)											
Зміщення даних (*Data offset*)	Зарезервовано (*Reserved*) 0 0 0	NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Розмір вікна (*Window Size*)
Контрольна сума (*Checksum*)											Покажчик важливості (*Urgent pointer*)
Опції (*Options*) *необов'язкове, розмір залежно від значення поля «Зміщення даних»*											
Дані (*Data*)											

Рисунок 2.5 – Формат TCP - пакета

Опишемо основні поля TCP-пакету (рисунок 2.5):

1. Порт джерела і порт призначення –16-бітові поля, що містять номери портів, відповідно, джерела і адресата TCP-пакета.

2. Номер в послідовності (англ. sequence number) – 32-бітове поле, вміст якого визначає (опосередковано) положення даних TCP-пакета всередині вихідного потоку даних, що існує в рамках поточного логічного з'єднання. У момент встановлення такого з'єднання кожен з партнерів генерує ідентифікаційний "номер в послідовності", основна вимога до якого - не повторюватися в проміжку часу, протягом якого TCP-пакет може знаходитися в мережі. Клієнти - партнери обмінюються цими початковими номерами і підтверджують їх отримання. Під час відправлення TCP-пакетів з даними поле "номер в послідовності" містить суму початкового номера і кількість байт даних, що передані раніше.

3. Номер підтвердження (англ. acknowledgement number) – 32-бітове поле, вміст якого визначає кількість прийнятих даних з вхідного потоку до TCP-модулю, що формує TCP-пакет.

4. Змішення даних – чотирибітове поле, що містить довжину заголовка TCP-пакета в 32-бітових словах і використовується для визначення початку розташування даних в TCP-пакеті.

5. Прапор URG – біт, встановлений в 1 значення якого означає, що TCP-пакет містить важливі (англ. urgent) дані.

6. Прапор ACK – біт, встановлений в 1 значення якого означає, що TCP-пакет містить в поле "номер підтвердження" вірні дані.

7. Прапор PSH – біт, встановлений в 1 значення якого означає, що дані містяться в TCP-пакеті повинні бути негайно передані прикладній програмі, для якої вони адресовані. Підтвердження для TCP-пакета, що містить середнє арифметичне значення у прапорі PSH, означає, що і всі попередні TCP-пакети досягли адресата.

8. Прапор SYN – біт, встановлений в 1 значення якого означає, що TCP-пакет являє собою запит на встановлення логічного з'єднання. Отримання

пакета з встановленим прапором SYN має бути підтверджено приймаючою стороною.

9. Прапор FIN – біт, встановлений в 1 значення якого означає, що TCP-пакет являє собою запит на закриття логічного з'єднання і є ознакою кінця потоку даних, переданих в цьому напрямку. Отримання пакета з встановленим прапором FIN має бути підтверджено приймаючою стороною.

10. Прапор RST – біт, встановлений на 1 в TCP-пакеті, відправляється у відповідь на отримання невірного TCP-пакета. Також може означати запит на переустановлення логічного з'єднання.

11. Розмір вікна – 16-бітове поле, що містить кількість байт інформації, яка може прийняти в свої внутрішні буфера TCP-модуль, що відправляє партнеру даний TCP-пакет. Дане поле використовується TCP-модулем, який приймає потік даних для керування інтенсивністю цього потоку: так, встановивши значення поля в 0, можна повністю зупинити передачу даних, до наявності вікна з великим значенням. Максимальний розмір вікна залежить від реалізації, в деяких реалізаціях цей розмір встановлюється системним адміністратором (типове значення максимального розміру вікна - 4096 байт). Визначення оптимального розміру вікна - одна з найбільш складних завдань реалізації протоколу TCP.

12. Контрольна сума – 16-бітове поле, що містить Internet-контрольну суму, розраховану для TCP-заголовка, даних пакета і псевдозаголовка.

13. Покажчик важливості – 16-бітове поле, що містить покажчик (у вигляді зсуву) на перший байт в тілі TCP-пакета, що починає послідовність важливих (urgent) даних.

14. Додаткові дані заголовка – поля довільної довжини, що описують необов'язкові дані заголовка. Протокол TCP визначає тільки три типи додаткових даних заголовка:

– кінець списку полів додаткових даних;

– порожньо (No Operation);

– максимальний розмір пакету.

Додаткові дані останнього типу посилаються в TCP-заголовку в момент встановлення логічного з'єднання для виразу готовності TCP-модулем приймати пакети, які завдовжки більше 536 байтів.

2.5 Комутація пакетів та типи затримок в IP мережі

Комутація пакетів (КП) - це метод передачі даних в мережі у формі пакетів. Для швидкої та ефективної передачі файлу мережею та мінімізації затримки передачі, дані розбиваються на невеликі фрагменти змінної довжини, які називаються пакетами . У пункті призначення всі ці дрібні частини (пакети) мають бути зібрані заново, що належать одному файлу. Пакет складається з корисного навантаження та різної контрольної інформації. Попереднє налаштування або резервування ресурсів не потрібно [13,15].

Комутація пакетів використовує техніку збереження та пересилання при перемиканні пакетів; під час пересилання пакету кожен стрибок спочатку зберігає цей пакет, а потім пересилає. Цей прийом є дуже корисним, оскільки пакети можуть з якоїсь причини викидатися в будь-якому стрибку. Між парою джерела та пункту призначення можливо кілька шляхів. Кожен пакет містить адресу джерела та адреси, за допомогою якої вони самостійно передаються мережею. Іншими словами, пакети, що належать одному файлу, можуть і не рухатися одним шляхом. Якщо на якомусь шляху є затори, пакетам дозволено вибрати інший шлях, можливий у існуючій мережі.

Мережі з КП розроблені для подолання слабких сторін мереж із комутацією каналів, оскільки мережі з комутацією каналів були не дуже ефективними для невеликих повідомлень.

Перевагами пакетної комутації в порівнянні з комутацією каналів є [6]:

– краща пропускна здатність, оскільки концепція схеми резервування відсутня;

– мінімальна затримка передачі;

– більш надійна, оскільки пункт призначення може виявити відсутній пакет;

– більш стійка до несправностей, оскільки пакети можуть йти іншим шляхом, якщо якесь посилання не працює, на відміну від комутації каналів;

– економічна та ефективна і порівняно дешевша у впровадженні.

Недоліками пакетної комутації в порівнянні з комутацією каналів є:

– комутація пакетів не приводить пакети в порядок, тоді як комутація каналів забезпечує упорядковану доставку пакетів, оскільки всі пакети йдуть за однаковим шляхом;

– оскільки пакети впорядковані, нам потрібно вказати порядкові номери для кожного пакета;

– складність на кожному вузлі більша завдяки можливості проходження декількох шляхів;

– затримка передачі більше через перенапрямлення маршруту;

– комутація пакетів вигідна лише для невеликих повідомлень, але для швидких даних (великих повідомлень) комутація каналів краще.

2.6 Режими комутації пакетів

Розглянемо режими комутації пакетів. До них відносяться [17]:

1. Режими віртуальних з’єднань. Комутація пакетів, що орієнтована на підключення у віртуальну схему: перед початком передачі встановлюється логічний шлях або віртуальне з'єднання, використовуючи протокол сигналізації, між відправником і одержувачем і всіма пакетами, що належать до цього потоку, пакети будуть прямувати цим заздалегідь визначеним маршрутом. Ідентифікатор віртуального кола надається комутаторами / маршрутизаторами для унікальної ідентифікації цього віртуального з'єднання. Дані діляться на невеликі одиничні сегменти, і всі ці малі сегменти додаються за допомогою порядкового номера. Загалом, при такій комутації проходить три фази - налаштування, передача даних та фаза зриву (рисунок 2.6).

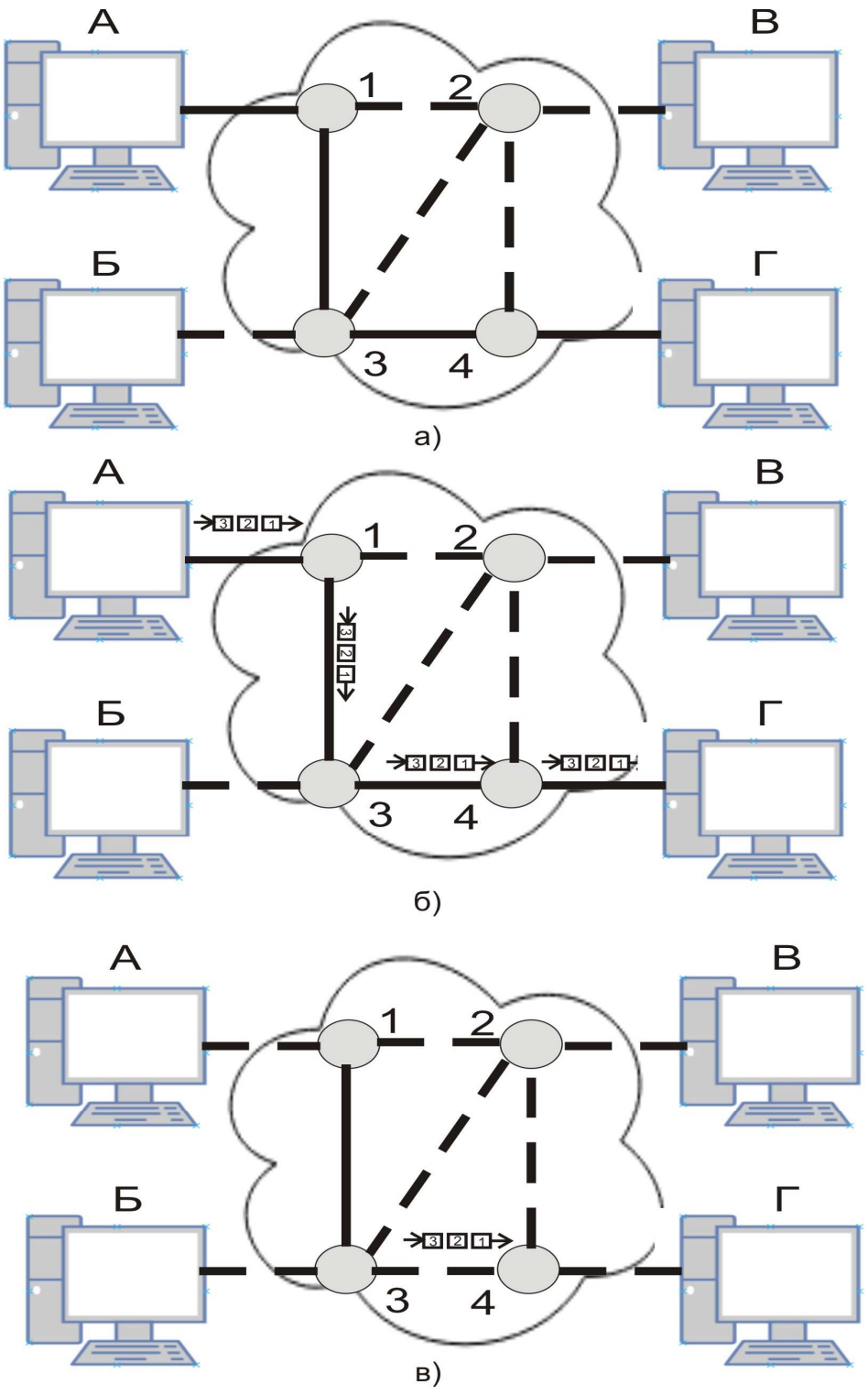


Рисунок 2.6 – Три фази комутації: налаштування (а), передача даних (б) та фаза зриву (в)

Вся інформація про адресу передається лише на етапі налаштування. Після виявлення маршруту до пункту призначення запис додається до таблиці перемикань кожного проміжного вузла. Під час передачі даних заголовок

пакета (локальний заголовок) може містити таку інформацію, як довжина, позначка часу, порядковий номер тощо.

Деякі популярні протоколи, що використовують підхід до комутації віртуальних з'єднань – це X.25, Frame-Relay, ATM та MPLS (Multi-Protocol Label Switching).

2. Дейтаграмний режим (рисунок 2.6). Комутація пакетів без підключення (дейтаграма). На відміну від перемикання пакетів, орієнтованих на підключення, в цьому режимі кожен пакет містить всю необхідну адресну інформацію, таку як адреса джерела, адреса призначення та номери портів тощо. Пакети, що належать одному потоку, можуть використовувати різні маршрути, оскільки рішення про маршрутизацію приймаються динамічно, тому пакети, що надійшли до пункту призначення, можуть бути прийняті не по порядку. Він не має налаштування підключення та фази відключення, як віртуальні схеми.

Доставка пакетів не гарантується при комутації пакетів без з'єднання, тому надійну доставку повинні забезпечувати кінцеві системи, що використовують додаткові протоколи.

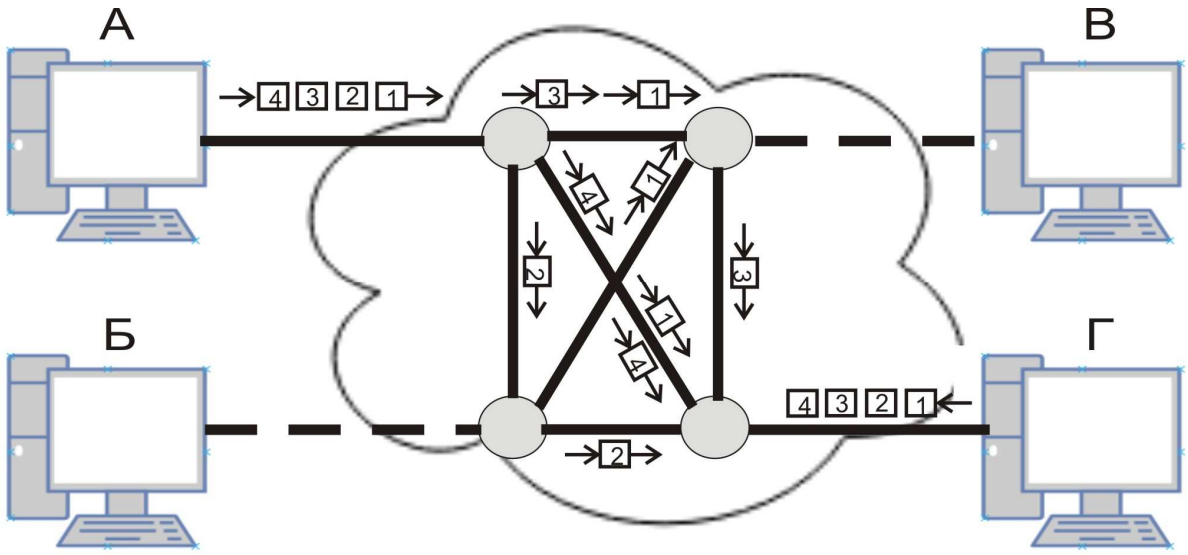


Рисунок 2.6 – Комутація пакетів без підключення (дейтаграма)

За рисунком 2.6 клієнт А - відправник пакету пересилає повідомлення через два маршрутизатори М1, М2, які зберігають і пересилають дані в пункт

призначення Б – приймач. При відправлення пакетів з вузла А в вузол Б, виникають затримки, оскільки це мережа «Зберігання» та «Пересилання».

2.7 Розрахунок затримок при комутації пакетів

Існують чотири типи затримок при комутації пакетів: затримка передачі; затримка поширення; затримка черги та затримка обробки [17,18].

1. Затримка передачі – це час, необхідний для розміщення пакета на пересилання. Іншими словами, просто потрібен час, щоб розмістити біти даних на проводовому / комунікаційному носії. Це залежить від довжини пакету та пропускної здатності мережі, а саме:

$$t_{затр.пер.} = L / C_п, \text{ с}, \quad (2.1)$$

де $t_{затр.пер.}$ – затримка передачі; L – розмір даних; $C_п$ – пропускна здатність, с.

2. Затримка поширення – час, необхідний першому біту, щоб пройти шлях від відправника до кінця лінії отримання. Іншими словами, це просто час, необхідний бітам, щоб дістатися до пункту призначення з початкової точки. Факторами, від яких залежить затримка поширення, є відстань та швидкість поширення:

$$t_{затр.пош.} = d / c, \text{ с}. \quad (2.2)$$

d – відстань, с– швидкість передачі.

3. Затримка черги – це час, коли завдання чекає в черзі, поки воно не може бути виконане. Це залежить від заторів, і розраховується як різниця в часі між тим, коли пакет прибув у пункт призначення, і коли пакетні дані були оброблені або виконані. Це може бути спричинено головним чином трьома причинами, тобто вихідними комутаторами, проміжними комутаторами або комутаторами обслуговування приймача дзвінків.

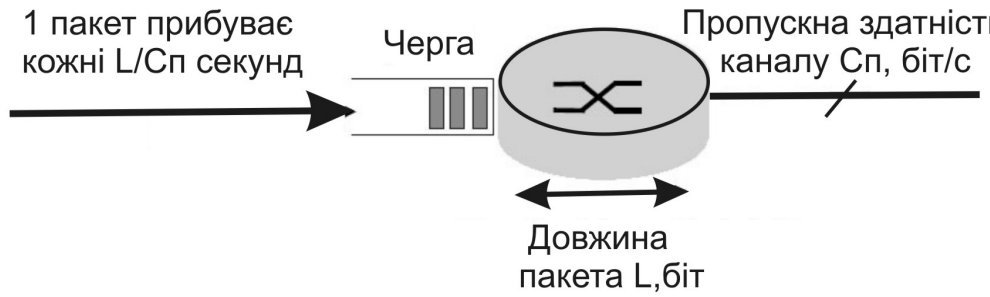


Рисунок 2.7 – Затримка черги на комутаторі

Швидкість прибування пакетів розраховується, як

$$c_{пр.пак.}=1/(L/C_п)= C_п/ L, \text{ пакетів/секунду.} \quad (2.3)$$

Інтенсивність трафіку, при цьому, дорівнює:

$$I_{тр}= c_{пр.пак.} \cdot L/C_п= C_п/ L \cdot (L/C_п)=1. \quad (2.4)$$

Середня затримка черги розраховується, як:

$$t_{сер.зч} = (N-1)\ L / (2 \cdot C_п), \quad (2.5)$$

де N – кількість пакетів; L – розмір пакета; $C_п$ – пропускна здатність.

4. Затримка обробки – це час, який потрібен маршрутизаторам для обробки заголовка пакета. Обробка пакетів допомагає виявити помилки на рівні бітів, які виникають під час передачі пакета до місця призначення. Затримки обробки у високошвидкісних маршрутизаторах зазвичай становлять мікросекунди або менше. Простими словами, це просто час, необхідний для обробки пакетів.

Загальний час або час від кінця до кінця:

$$t_{заг.}= t_{затр.пер.} + t_{затр.пош.} + t_{сер.зч} + t_{затр.обр.}, \quad (2.6)$$

де $t_{затр.пер}$ – затримка передачі; $t_{затр.пош}$ – затримка поширення; $t_{сер.зч}$ – середня затримка черги; $t_{затр.обр.}$– затримка на обробку.

Для M стрибків і N пакетів –

Загальна затримка:

$$t_{заг.} = M_{стр.} \cdot (t_{затр.пер} + t_{затр.пош}) + (M_{стр.}-1) \cdot (t_{затр.обр.} + t_{сер.зч} + (N-1) \cdot (t_{затр.пер}) \quad (2.7)$$

Для N сполучної ланки в каналі: затримка передачі – $t_{затр.пер} = N \cdot L / C_п$: $t_{затр.пош} = N \cdot (d / c)$ – затримка поширення.

Розглянемо приклад. Необхідно передати 10 пакетів від вузла А до вузла Б із заданим розміром пакета L, біт. Мережа складається з 3-х пакетних комутаторів, та має кількість стрибків $M_{стр.}=4$. Пропускна здатність для передачі даних - $C_п$, Мбіт / с, а швидкість поширення – с, м/с. Припустимо, що затримка обробки дорівнює $t_{затр.обр} = p$ секунд, а відстань між двома точками (вузлами) - d метрів. Знайдемо загальний час, необхідний 10 пакетам, щоб дістатися до Б з точки А.

Тут ми відправляємо 10 пакетів, також оскільки немає підтвердження прийнятого пакету, ми виконуємо паралельну обробку. Коли 1-й пакет досягає М2, другий пакет досягає М1.

Отже, за формулою 2.6, отримуємо загальну затримку:

$t_{заг.} = = 4 \cdot (L / C_п \cdot 10^6 + d / c) + (4-1) \cdot (P + 0) + (10-1) \cdot L / C_п \cdot 10^6$.

Для відстань L =d метрів знаходимо:

– затримка передачі $t_{затр.пер} = (N \cdot L) / C_п = (3 \cdot L) / C_п$, с;

– затримка поширення $t_{затр.пош} = N \cdot (d / t) = (3 \cdot d) / t$, с;

– загальний час $t_{заг.} = 3 \cdot (L / C_п + d / t)$, с.

1. Для випадку 1 та для розміру даних L = 1000 байт, де пропускна здатність $C_п$ = 1 Мбіт/с, розмір заголовка З= 100 байт, кількості стрибків $M_{стр.}$= 3 і затримки поширення $t_{затр.пош}$ = 0 с та кількості пакетів N = 1 шт, отримуємо:

– розмір пакету даних дорівнює доданку розміру даних та розміру заголовка: L = 1000 + 100 = 1100 байт;

– затримка передачі: $t_{затр.пер} = L / C_п = 1100/10^6 = 1{,}1$ мс;

– загальний витрачений час: $t_{заг.} = 3 \cdot 1{,}1 = 3{,}3$ мс.

2. Для випадку, при кількості пакетів N = 5 шт., розмірі кожного пакета даних L= (1000/5) + 100 = 300 байт, отримуємо:

– затримка передачі для кожного пакета – $t_{затр.пер} = 300/10^6 = 0,3$ мс;

– час, зайнятий 1-м пакетом дорівнює кількість стрибків помноженому на затримку передачі – $t_{з1}=3 \cdot 0,3 = 0,9$ мс;

– час, який займають решта 4 пакети $t_{з4}= 4 \cdot 0,3 = 1,2$ мс;

– загальний витрачений час $t_{заг.}= 0,9 + 1,2 = 2,1$ мс.

3. Для випадку 3: при кількості пакетів N = 10 шт., розмірі кожного пакета даних L= (1000/10) + 100 = 200 байт, отримуємо:

– затримка передачі для кожного пакета $t_{затр.пер} = 200/10^6 = 0,2$ мс;

– час, зайнятий першим пакетом $t_{з1}= 3 \cdot 0,2 = 0,6$ мс;

– час, що забирається рештою 9-ю пакетами $t_{з9}= 9 \cdot 0,2 = 1,8$ мс;

– загальний витрачений час $t_{заг.} = 0,6 + 1,8 = 2,4$ мс.

4. Для випадку 4: при кількості пакетів N = 20 шт., розмірі кожного пакета даних L= (1000/20) + 100 = 150 байт, отримуємо:

– затримка передачі для кожного пакета $t_{затр.пер}= 150/10^6 = 0,15$ мс;

– час, зайнятий 1-м пакетом $t_{з1}= 3 \cdot 0,15 = 0,45$ мс;

– час, залишений 19-ти пакетам $t_{з19}= 19 \cdot 0,15 = 2,85$ мс;

– загальний витрачений час $t_{заг.}= 0,45 + 2,85 = 3,3$ мс.

Як можна побачити:

1. Затримка передачі для кожного пакета зменшується при збільшенні кількості пакетів (з 1,1 мс при N = 1 шт. до 0,45 мс при N = 20 шт.).

2. Існує граничне значення, при якому загальний витрачений час на початку зменшується (N = 1 шт., $t_{заг.}=3,3$ мс; N = 5 шт. $t_{заг.}=2,1$ мс). При збільшенні кількості пакетів після цього обмеження, загальний час починає збільшуватися (N = 10 шт., $t_{заг.}= 2,4$ мс; N = 20 шт., $t_{заг.}= 3,3$ мс). Якщо кількість пакетів дуже велика, то це займає набагато більше часу, ніж час, необхідний для передачі одного пакета.

Висновки до другого розділу

1. Проведений аналіз сучасного трафіку глобальної мережі, який показав, що до 2023 року на кожного користувача мережі інтернет буде припадати біля 3,6 мережевих пристроїв, а всього мережевих пристроїв збільшиться до 29,3 млрд. При цьому, кількість користувачів Інтернету сягне 5,3 мільярди, що складе 66 відсотків світового населення. Це вимагає удосконалення методів проведення оцінки необхідної пропускної здатності IP мережі.

2. Розглянуто стек протоколів TCP / IP. Представлена архітектура основних протоколів TCP / IP, які використовуються на трьох нижніх рівнях стеку. Показано, що основою усієї архітектури є міжмережний протокол IP за допомогою якого реалізується адресація вузлів мережі і доставка даних і який працює разом з міжмережним протоколом керуючих повідомлень ICMP, що призначений для передачі діагностичної інформації та повідомлень про помилки в роботі мережі та протоколом управління передачею TCP – протоколом транспортного рівня.

3. Розглянуто принципи комутації пакетів, описані основні режими комутації пакетів: віртуальних з'єднань та дейтаграмний режим. Наведені переваги використання дейтаграмного режиму за рахунок можливості використання динамічної маршрутизації при передачі пакетів між абонентськими вузлами.

4. Розраховані чотири типи затримок при комутації пакетів: затримка передачі; затримка поширення; затримка черги та затримка обробки. Розрахунки показали, що затримка передачі для кожного пакета зменшується при збільшенні кількості пакетів (з 1,1 мс при N = 1 шт. до 0,45 мс при N = 20 шт.). Існує граничне значення, при якому загальний витрачений час на початку зменшується (N = 1 шт., $t_{заг.}$=3,3 мс; N = 5 шт. $t_{заг.}$=2,1 мс). При збільшенні кількості пакетів після цього обмеження, загальний час починає збільшуватися (N = 10 шт., $t_{заг.}$= 2,4 мс; N = 20 шт., $t_{заг.}$= 3,3 мс). Якщо кількість пакетів дуже велика, то це займає набагато більше часу, ніж час, необхідний для передачі одного пакета.

3 ПРОПУСКНА ЗДАТНІСТЬ МЕРЕЖІ ГОЛОСОВОЇ IP- ТЕЛЕФОНІЇ

3.1. Основні положення теорії масового обслуговування

Трафік - це обсяг даних або кількість повідомлень, переданих через канал за певний проміжок часу та включає відношення між спробами виклику обладнання, чутливого до трафіку, і швидкістю виконання цих викликів. Аналіз трафіку дає можливість визначити необхідну ширину смуги пропускання каналів передачі даних і голосових викликів [18,19].

У теорії масового обслуговування вимірюється інтенсивність трафіку. Інтенсівность трафіку - це відношення кількості викликів за певний період часу до середнього часу, що витрачається на обслуговування кожного виклику протягом цього періоду. Ці одиниці виміру засновані на середньому часу утримання (англ. Average Hold Time, AHT). AHT – це сумарна тривалість всіх викликів за вказаний період (загальних секунд дзвінка), поділена на кількість викликів за цей період (кількість дзвінків).

Навантаження трафіку вимірюється в одиницях – Ерланг та ста викликів-секунд (англ. Centum Call Seconds, CCS). При цьому, один Ерланг – це 3600 секунд викликів в одному каналі або інтенсивність трафіку, достатня для завантаження каналу протягом однієї години. Трафік в Ерланг – це добуток кількості викликів (дзвінків) на середній час утримання виклику (AHT), поділене на 3600 секунд [8]. 100 викликів-секунд (CCS) – це 100 секунд викликів в одному каналі. Голосові комутатори зазвичай вимірюють обсяг трафіку в сотнях викликів - секунд.

Вибір одиниці виміру залежить багато в чому від використовуваного обладнання та одиниць вимірювання, в яких ведеться запис. CCS застосовуються в багатьох комутаторах з тієї причини, що число 100 є більш практичною базовою одиницею періоду, ніж 3600. Обидві одиниці виміру вважаються стандартними в цій сфері. Вони співвідносяться наступним чином: 1 Ерланг = 3600 викликів-секунд.

Навантаження мережі зазвичай вимірюється в час найбільшого навантаження (ЧНН), тому що цей період характеризується максимальною інтенсивністю трафіку, яку повинна витримувати мережа. Результатом є величина інтенсивності трафіку, яка зазвичай називається трафіком в час найбільшого навантаження (ТЧН). Бувають ситуації, коли неможливо провести точне вимірювання, і є тільки приблизна оцінка числа викликів, оброблюваних за день. У таких випадках доречно виходити в своїх оцінках зі специфіки конкретного оточення, наприклад, з середньої кількості викликів за день або середнього часу утримання (АНТ). ITU-T прийнято, що час найбільшого навантаження даного дня займає приблизно від 15 до 20% трафіку за день. У розрахунках зазвичай використовується значення в 17% загального трафіку за день для характеристики трафіку в піковий період. Для багатьох бізнес-організацій прийнятною оцінкою середнього часу утримання (АНТ) буде інтервал від 180 до 210 секунд. Ці оцінки можна використовувати, якщо необхідно визначити вимоги до магістральних каналів.

Для вимірювання пропускної здатності мережі (ПЗМ) необхідно знати такі 2 показники: кількість спроб викликів на годину найбільшого навантаження (КСВЧН) та кількість викликів в секунду (КВС). Але ці данні не дають точного опису трафіку мережі. Для більш точного визначення, ці вимірювання необхідно використовувати разом зі значенням середнього часу утримання та показником ймовірності блокування викликів під час спроби зайняти канал (коефіцієнт блокування), щоб обчислити трафік під ЧНН і використовувати отримані значення для аналізу трафіку.

Існує поняття двох типів трафіку [18]:

– фактичний трафік $Y_{факт.}$ - це трафік, який фактично оброблений телекомунікаційним обладнанням;

– запропонований трафік $Y_{запр.}$ – це фактична кількість спроб обміну даними в системі.

Необхідно враховувати той факт, що чим більше параметр блокування, тим більша різниця між фактичним і запропонованим навантаженням. Для

розрахунку запропонованого навантаження з фактичного навантаження можна використовувати таку формулу:

$$Y_{запр.} = Y_{факт.} / 1 - K_{б}, \quad (3.1)$$

де $Y_{факт.}$ – фактичний трафік; $Y_{запр.}$ – запропонований трафік; $K_{б}$ – коефіцієнт блокування.

Вираз (3.1) не враховує повторні виклики, які можуть відбуватися при блокуванні абонента. Для розрахунку частки повторних викликів можна використовувати таку формулу [18]:

$$Y_{запр.} = Y_{факт.} \cdot (1{,}0 - E_{v} \cdot K_{б}) / 1 - K_{б}, \quad (3.2)$$

де $Y_{факт.}$ – фактичний трафік; $Y_{запр.}$ – запропонований трафік; E_{v} – відсоток ймовірності повторного виклику; $K_{б}$ – коефіцієнт блокування.

Теорія ймовірності стверджує, що для точної оцінки трафіку мережі передачі голосу період вимірювання повинен включати принаймні 30 годин найбільшого навантаження мережі голосового зв'язку. При цьому, для отримання найбільш точних результатів, необхідно виконати якомога більше вимірів запропонованого навантаження. Данні виміри проводяться на протязі року, результати можуть спотворюватися, тому що навантаження трафіку протягом року збільшується і зменшується. За рекомендаціями Відділу стандартизації телекомунікацій Міжнародного союзу телекомунікацій (ITU-T) для отримання точних результатів пікового навантаження необхідно проводити вимірювання в мережі ТМЗК по 60 хвилин і / або з 15-хвилинним інтервалом протягом дня і виявляти пікове навантаження трафіку в будь-який день. Або ITU-T рекомендовано здійснювати фіксований інтервал вимірювань за день тільки протягом заздалегідь визначених пікових періодів. Цей метод використовується, коли моделі трафіку в певній мірі передбачувані, і пікові періоди наступають з регулярними інтервалами. Наприклад, бізнес- трафік

зазвичай досягає свого піку приблизно з 10:00 до 11:00 і з 14:00 до 15:00. За даними (ITU-T) час найбільшої загальної інтенсивності трафіку - 10:00, причому загальна інтенсивність трафіку дорівнює 60,6 Ерл.

Також необхідно розділити вимірювання за день по групах з однаковою статистичною поведінкою. Згідно зі специфікацією ITU-T, такими групами є: робочі дні, вихідні дні та святкові дні в році. Групування вимірювань з однаковим статистичною поведінкою є важливим, так як дні з виключно високою кількістю викликів (наприклад, святкові дні)) можуть спотворити результати.

Рекомендація відділу стандартизації телекомунікацій E.492 включають рекомендації щодо визначення звичайної і високої інтенсивності трафіку протягом місяця. Відповідно до рекомендації відділу стандартизації комунікацій E.492 звичайна інтенсивність трафіку протягом місяця визначається як четвертий зверху найвищий піковий трафік за день. Якщо вибирається другий зверху найвищий результат вимірювань за місяць, це призводить до завищення інтенсивності трафіку за місяць. Цей результат дозволяє визначити прогнозовану інтенсивність трафіку за місяць.

3.2 Механізми керування обслуговуванням черг

Для роботи в часи найбільшого навантаження виникають проблеми з обслуговуванням трафіку, що надходить на певний мережевий пристрій, який може не справлятися з викликами, що надходять з заданим інтервалом надходження. Тому існують певні механізми до яких відносяться [17]:

1. Механізм керування FIFO (англ. first in, first out) (рисунок 3.1). У черзі FIFO у разі перевантаження мережевого пристрою, всі пакети розміщуються в одній загальній черзі й вибираються з неї у тому порядку, у якому надійшли. Саме в пристроях з КП цей механізм керування використовується за замовчуванням Такий механізм керування дуже просто реалізувати. Але в такій реалізації, коли усі пакети, і чутливі до затримок трафіку (голосова телефонія), і не чутливі до них, а також пакети дуже інтенсивного трафіку знаходяться у

буфері пристрою, в черзі на рівних підставах, їх не має можливості передавати з заданою якістю [17].

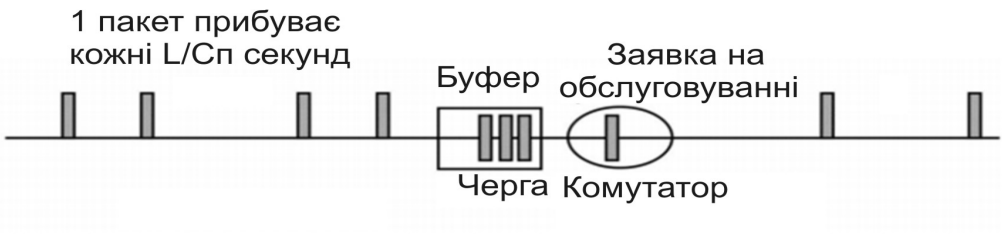


Рисунок 3.1 – Механізм керування FIFO

2. Механізм пріоритетного обслуговування. Цей механізм обслуговування заснований на поділі мережного трафіку, що передається через пристрої телекомунікаційної мережі, на певні класи, кожному з яких призначається деяка ознака пріоритетності. Дані пріоритети виставляються як за допомогою в полях заголовку пакетів (протокол Ethernet), або призначатися використовуваним мережним пристроєм, який забезпечує передачу трафіку.

При такому механізмі керування створюються декілька черг в буферах пристроїв для кожного окремого пріоритетного класу. Заявки на обслуговування вибираються з черги відповідно до їх пріоритетів.

На рисунку 3.2 наведено приклад реалізації описаного FIFO обслуговування чотирьох черг, різного класу пріоритетності.

За рисунком 3.2 усім чергам пакетів призначений певний клас пріоритету від високого до низького. У такому випадку, в першу чергу, обслуговуються пакетний трафік з вищою пріоритетністю і, в останню – пакетний трафік з самим низьким класом пріоритетності. Причому, існують ситуації, які обумовлені розміром буфера обслуговуючого пристрою, коли буфер стає заповненим і наступний пакет, що надходить до нього просто відкидається.

На сьогодні в більшості телекомунікаційних пристроїв можна настроїти кожній черзі буфер індивідуального розміру, який залежить від мережевого навантаження. Саме в таких випадках і необхідні регулярні спостереження за роботою мережі. Даний алгоритм зазвичай застосовується для чутливого до

затримок класу трафіку, що має невелику інтенсивність, до якого відноситься, наприклад, голосовий трафік з інтенсивністю 8–16 Кбіт/с, тому, коли йому призначений вищий пріоритет, то цей трафік не значно впливає на нижчі класи трафіку, що передається [18].

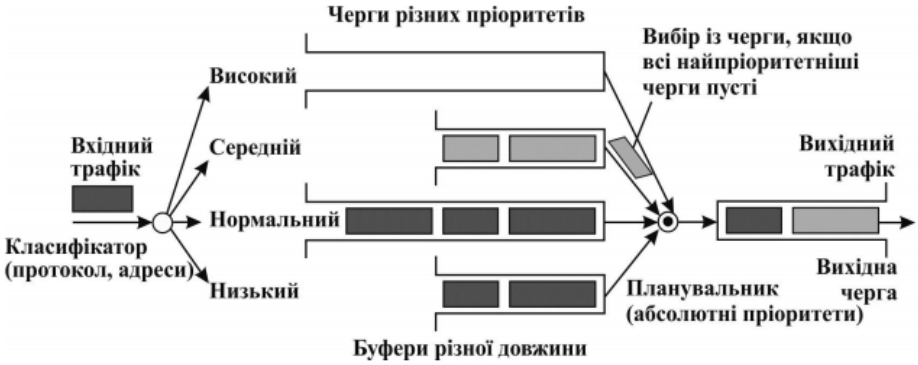


Рисунок 3.2 – Механізм обслуговування черг за пріоритетами [17]

3.3. Типи пакетних комутаторів

Усі пакетні комутатори виконують дві базові операції [17]:

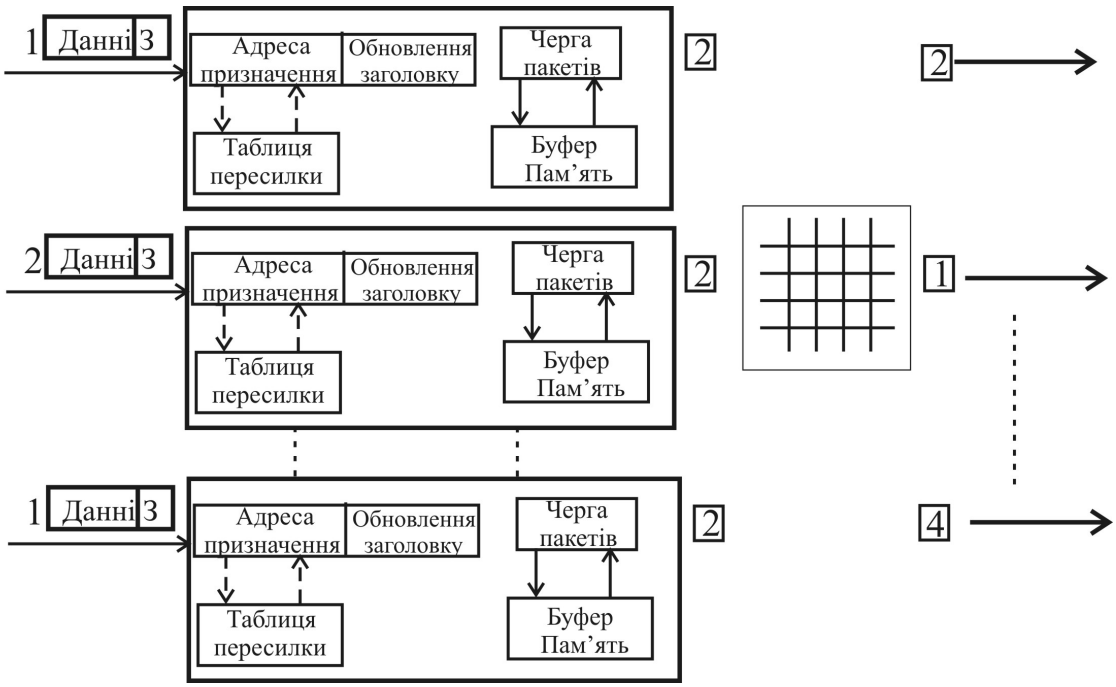
- пошук відповідності в таблиці комутації;
- передачу пакетів даних на призначений вихідний порт.

У відповідності до механізмів обслуговування черг обслуговуючі пристрої (комутатори) поділяються на:

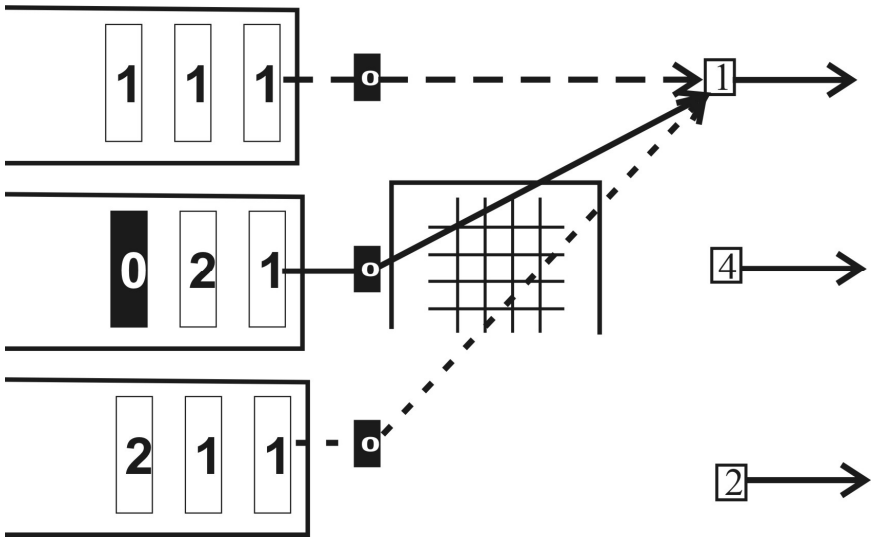
1. Комутатори з буферизацією на вході (рисунок 3.3,а,б).

2. Комутатори з буферизацією на виході та поділюваною пам’яттю для зберігання черг пакетів кожного потоку трафіку (рисунок 3.4). Такий тип комутаторів працює з мінімальними втратами пакетів, максимальною пропускною здатністю та з мінімальними затримками на очікування обслуговування. Але такі схеми буферизації вимагають високих швидкостей роботи та ємностей буфера.

3. Високошвидкісні комутатори, які використовують буферизацію на вході з чергами віртуальних виходів (рисунок 3.5).



а)



б)

Рисунок 3.3 – Комутатори з буферизацією на вході: пакетний комутатор (а); схема блокувань (б)

Комутатори з буферизацією на вході (рисунок 3.3,а,б) мають низьку пропускну здатність завдяки блокування на входах (рисунок 3.3,б). При цьому, такі схеми комутаторів не вимагають високих швидкостей роботи та обсягу черги.

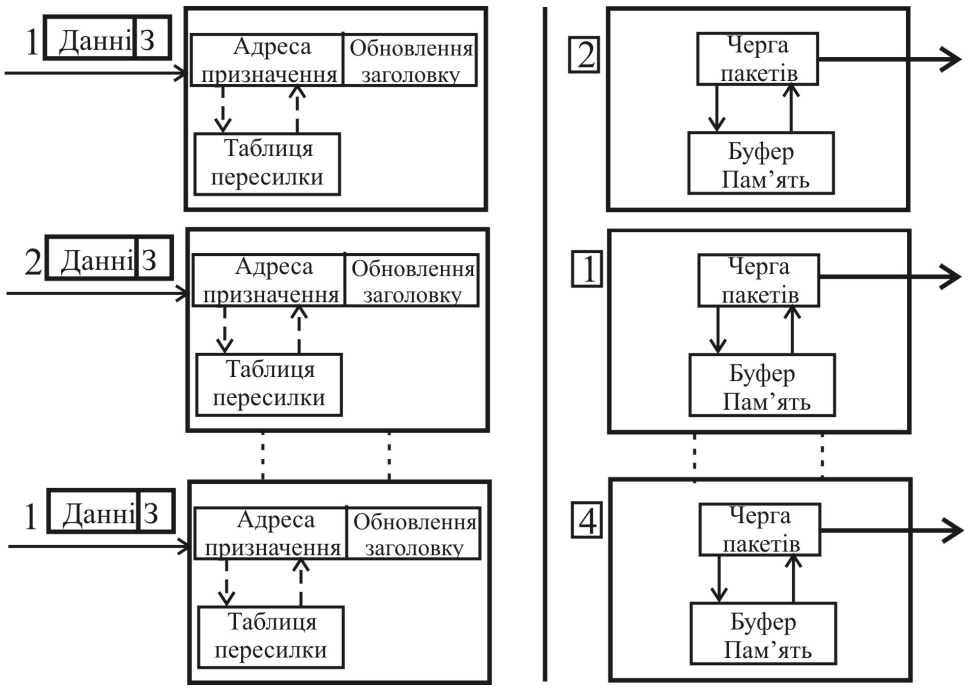


Рисунок 3.4 – Комутатори з буферизацією на виході

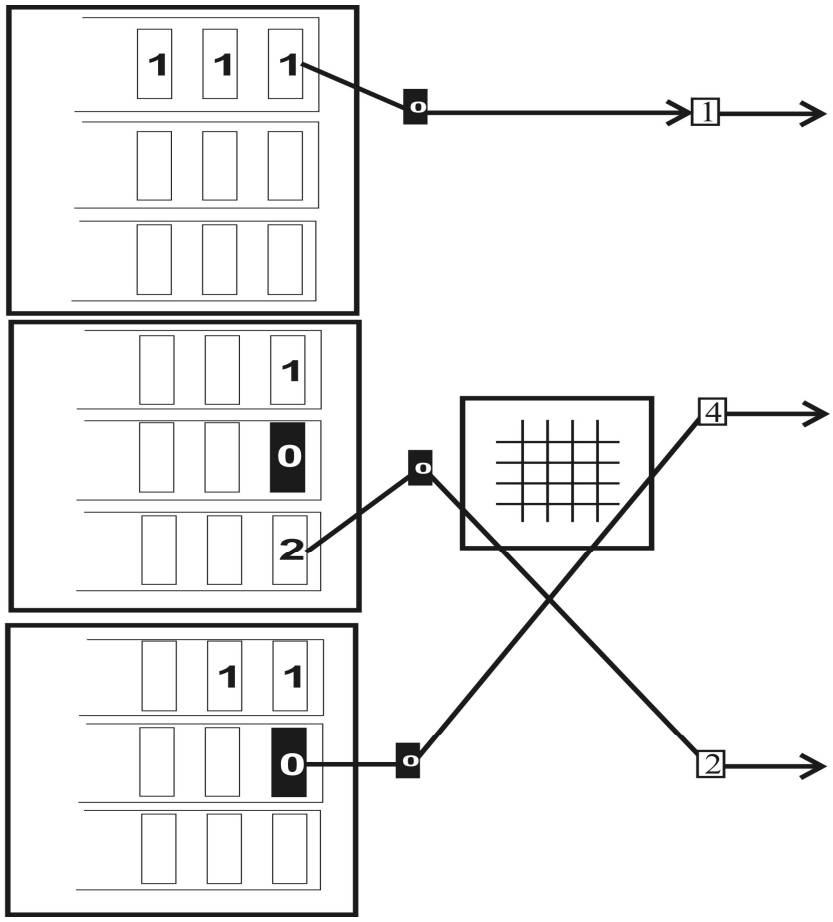


Рисунок 3.5 – Комутатори з буферизацією на вході з чергами віртуальних виходів

Високошвидкісні комутатори використовують буферизацію на вході з чергами віртуальних виходів, це дозволяє значно збільшити пропускну здатність пристрою.

3.4 Метод розрахунку пропускної здатності мережі VoIP телефонії

При проектуванні і налагодженні мереж VoIP телефонії, які є чутливими до трафіку використовують кілька різних моделей трафіку, які необхідно правильно обирати та використовувати. Існуючи моделі теорії масового обслуговування дозволяють проектувальникам мереж робити припущення про роботу мереж на основі минулого досвіду [19,20].

Аналіз трафіку VoIP мереж дає можливість визначити необхідну пропускну здатність (продуктивність) мережі. Поняття трафіку включає відношення між спробами виклику обладнання, чутливого до трафіку, і швидкістю виконання цих викликів. Проектування трафіку направлено на вирішення проблем зв’язаними з визначенням таких параметрів якості зв'язку, як рівень обслуговування та коефіцієнт блокування. Зазвичай, для визначення навантаження, обирається період часу найбільшого навантаження на мережу, який характеризується максимальною інтенсивністю трафіку, який здатна витримати мережа. Результатом є величина інтенсивності трафіку, або трафік в час найбільшого навантаження [20].

Для аналізу трафіку систем масового обслуговування (СМО) [3,20], які використовують необмежену кількість джерел, випадкове надходження трафіку на вхід комутаційної системи та утримання заблокованих викликів за експоненціальним розподіленим часом утримання, застосовують так звану модель Пуассона. В такій моделі заблоковані виклики утримуються, поки канал не стане доступним. За моделлю Пуассона абонент може зробити тільки одну спробу здійснити виклик, а заблоковані виклики втрачаються. Модель Пуассона зазвичай використовується для розрахунку окремих груп магістральних каналів груп з запасом.

Розрахуємо середню інтенсивність навантаження від одного абонента в напрямку за формулою $\bar{c} = 3{,}4$ – середня кількість заявок від абонента за одиницю часу ($\bar{t} = 286/3600 \approx 0{,}08$ год.) (за умовами завдання до ДР):

$$y = \bar{c} \cdot \bar{t} = 3{,}4 \cdot 0{,}08 = 0{,}272 \text{ Ерл.}$$

Інтенсивність заявленого навантаження розраховується за формулою [20]:

$$Y = N \cdot \bar{c} \cdot \bar{t}. \tag{3.3}$$

Інтенсивність трафіку в напрямку розрахуємо як [20]:

$$Y = N \cdot \bar{c} \cdot \bar{t} = 749 \cdot\ 3{,}4 \cdot\ 0{,}08 = 203{,}7 \text{ Ерл.}$$

Для обчислення моделі трафіку Пуассона використовується наступний вираз [20]:

$$p_k(Y) = \frac{(Y)^k}{k!} e^{-Y}, \tag{3.4}$$

де, $p_k(Y)$ – імовірність надходження k викликів, Y=203,6 Ерл. – інтенсивність трафіку (розрахована для наступних змінних: кількість абонентів VoIP – телефонії в офісі провайдера –749 чол.; середня кількість викликів, які ініціює один абонент офісу – 3,4 викликів за годину).

Модель трафіку, що розрахована за розподілом Пуассона (3.4), наведена на рисунку 3.6.

Згідно розподілу Пуассона (рисунок 3.6) для обробки навантаження 203,6 Ерл. з ймовірністю блокування 2,4% СМО проектованої мережі може обслужити 216 викликів.

Розрахунки здійснімо в пакеті математичного моделювання MATLAB [21].

Лістинг програми для розрахунку розподілу Пуассона наведений нижче:

```
function mass = PoissonV(Y, N_Abon)
CurP = exp(-Y);
mass = [];
for k=1:N_Abon
   CurP = CurP*Y/k;
   mass(k) = CurP;
end
return
```

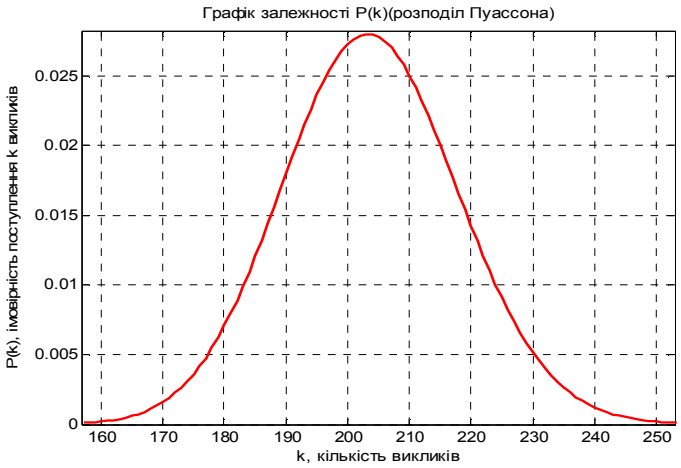


Рисунок 3.6 – Графік залежності $p_k(Y)$ від кількості викликів

Модель трафіку Ерланг В використовується, при заблокованих викликах та перенапрямлених без повернення до вихідної групи магістральних каналів. Ця модель передбачає випадкове надходження викликів. Абонент робить тільки одну спробу виклику. У випадку блокування цього виклику, він перенаправляється. Модель Ерланг В зазвичай використовується для розрахунку необхідних каналів з низьким коефіцієнт блокування, обслужених з першої спроби, без потреби врахування відсотку повторних викликів, тому що абоненти перенаправляються.

Для обчислення моделі трафіку Ерланг В використовується наступний вираз [3,19,20]:

$$E_v(Y) = \frac{Y^v / v!}{\sum_{i=1}^{v} Y^i / i!}, \tag{3.5}$$

де $E\nu(Y)$ – ймовірність блокування викликів; ν – кількість каналів; Y – інтенсивність трафіку.

Використаємо модель трафіку Ерланг В для перепроектування вихідних груп магістральних каналів для міжміських викликів, які зараз блокуються під час години найбільшого навантаження. Врахуємо, що під час найбільшого навантаження на групу магістральних каналів надходить 203,6 Ерл. трафіку (рисунок 3.7). При розрахунках кількості каналів скористуємось методом підбору (3.5) та графічним методом [20].

При підборі повинна виконуватися умова:

$$E_v(Y) \le p_b, \tag{3.6}$$

де p_b – задані допустимі втрати.

За допомогою методу підбору – задаємо інтенсивність трафіку та допустиму імовірність очікування (ДІО) $p_b = 0{,}07$, а далі підбираємо кількість ліній за якої обчислена імовірність очікування буде ближче до значення ДІО.

Представимо формулу Ерланга як:

$$E_v(Y) = \frac{\prod_{k=1}^{v} \frac{Y}{k}}{\sum_{i=1}^{v} \prod_{j=1}^{i} \frac{Y}{j}},$$

Позначимо:

$$F_v(Y) = \frac{Y^v}{v!},$$

$$S_v(Y) = \sum_{i=1}^{v} \frac{Y^i}{i!} = \sum_{i=1}^{v} F_i(Y).$$

Звідси, буде справедливо наступне:

$$F_{v+1}(Y) = F_v(Y)\ \frac{Y}{v+1};$$
$$S_{v+1}(Y) = S_v(Y) + F_{v+1}(Y);$$

$$E_{v+1}(Y)=\frac{F_{v+1}(Y)}{S_{v+1}(Y)}=\frac{F_{v+1}(Y)}{S_v(Y)+F_{v+1}(Y)}=\frac{F_v(Y)\ \dfrac{Y}{v+1}}{S_v(Y)+F_v(Y)\ \dfrac{Y}{v+1}};$$

$$F_1(Y)=\frac{Y^1}{1!}=Y;$$

$$S_1(Y)=\sum_{i=1}^{1}F_i(Y)=F_1(Y)=Y;$$

$$E_1(Y)=\frac{F_1(Y)}{S_1(Y)}=\frac{Y}{Y}=1.$$

Розрахунки здійснімо в пакеті математичного моделювання MATLAB [21].

Лістинг програми наведений нижче:

```
function Ev_Y = ErlangV( Y, N_Abon )
% Розрахунок Ev(Y)
% N_Abon - максимальна кількість каналів
Fv_Y = 1;
Sv_Y = 1;
Ev_Y(1) = 1;
for v = 2:N_Abon
   Fv_Y = Fv_Y * Y / v;
   Sv_Y = Sv_Y + Fv_Y;
   Ev_Y(v) = Fv_Y / Sv_Y;
end
return
end
```

Використовуючи графічний метод [20], будуємо графіки залежності імовірності очікування від кількості каналів при сталій інтенсивності трафіку.

За результатами моделювання (рисунок 3.7) видно, що з ймовірністю блокування 0,024, необхідна кількість магістральних каналів для оброблення заданого навантаження трафіку дорівнює – 216 каналам.

Отже, програмна реалізація методу підбору в системі математичного моделювання MATLAB працює коректно.

При використанні такої кількості магістральних каналів та за умови використання голосового кодеку G.711 (загальна пропускна здатність кодеку

G.711 - 107,2 Кбіт/с [18, табл.4]), максимальна пропускна здатність мережі сягає 23,155 Мбіт/с.

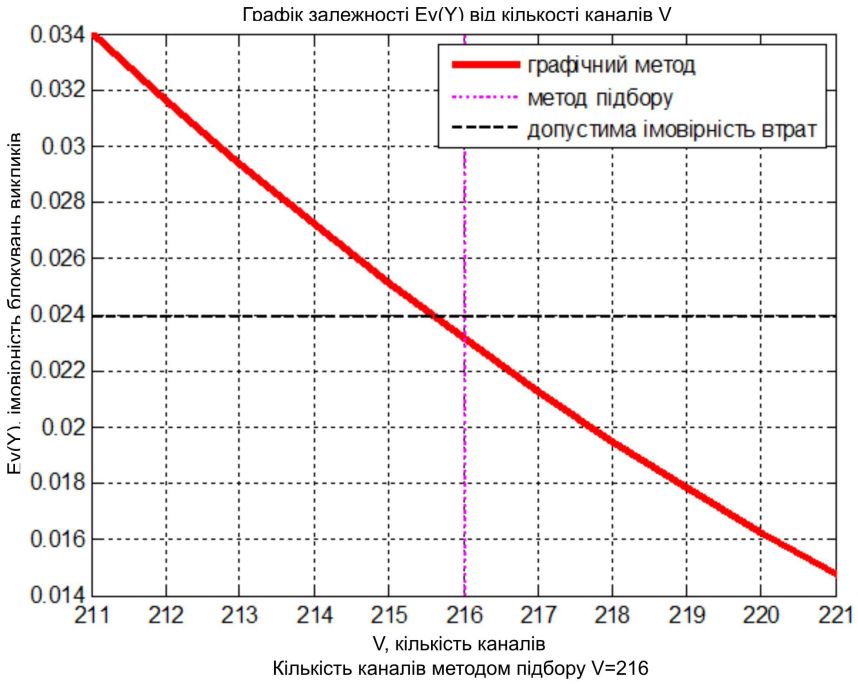


Рисунок 3.7 - Графік залежності Ev(Y) від кількості каналів

Розрахунки показали, що магістральна мережа спроектована якісно, має високу продуктивність та низький коефіцієнт блокування. За таких даних, якість обслуговування значно підвищується, а витрати зменшуються.

Модель випадкового надходження трафіку Ерланг С застосовується при наявності необмеженої кількості джерел і затриманих заблокованих викликів та побудована на теорії черг. Ця модель передбачає випадкове надходження викликів, при цьому, абонент здійснює один виклик і утримується в черзі до відповіді на виклик. Модель Ерланг С частіше використовується при проектуванні сталого пристрою автоматичного розподілу викликів (ACD), щоб визначити необхідну кількість агентів.

Для обчислення моделі трафіку Ерланг С використовується наступна формула [19,20]:

$$D_v(Y) = \frac{E_v(Y)}{1 - \frac{Y}{v}(1 - E_v(Y))}, \qquad (2.5)$$

де $E_v(Y)$ – кількість каналів, що визначаються за формулою Ерланг B (3.5).

Для розрахунків використовується формулою Ерланг B та Ерланг C.

Розрахунки здійснимо за допомогою пакета математичного моделювання MATLAB [21]. Лістинг програми наведений нижче:

```
function Dv_Y = Erlang2V(Y, N_Abon)
% Розрахунок Dv(Y)
% N_Abon - максимальна кількість каналів
Fv_Y = 1;
Sv_Y = 1;
Dv_Y(1) = 1;
for v = 2:N_Abon
   Fv_Y = Fv_Y * Y / v;
   Sv_Y = Sv_Y + Fv_Y;
   Ev_Y = Fv_Y / Sv_Y;
   Dv_Y(v) = Ev_Y/(1-Y*(1-Ev_Y)/v);
end
return
end
```

Отримана графічна залежність імовірності очікування $D_v(Y)$ від кількості каналів v для заданої інтенсивності трафіку Y (рисунок 3.8).

З рисунку 3.8 видно, що для забезпечення необхідних параметрів моделі трафіку з очікуванням обслуговування потрібно 234 канали.

При використанні такої кількості магістральних каналів та за умови використання голосового кодеку G.711 (загальна пропускна здатність кодеку G.711 - 107,2 Кбіт/с [18, табл.4]), максимальна пропускна здатність мережі сягає 25,084 Мбіт/с, що значно вище чим при використанні моделі з блокуванням (модель B).

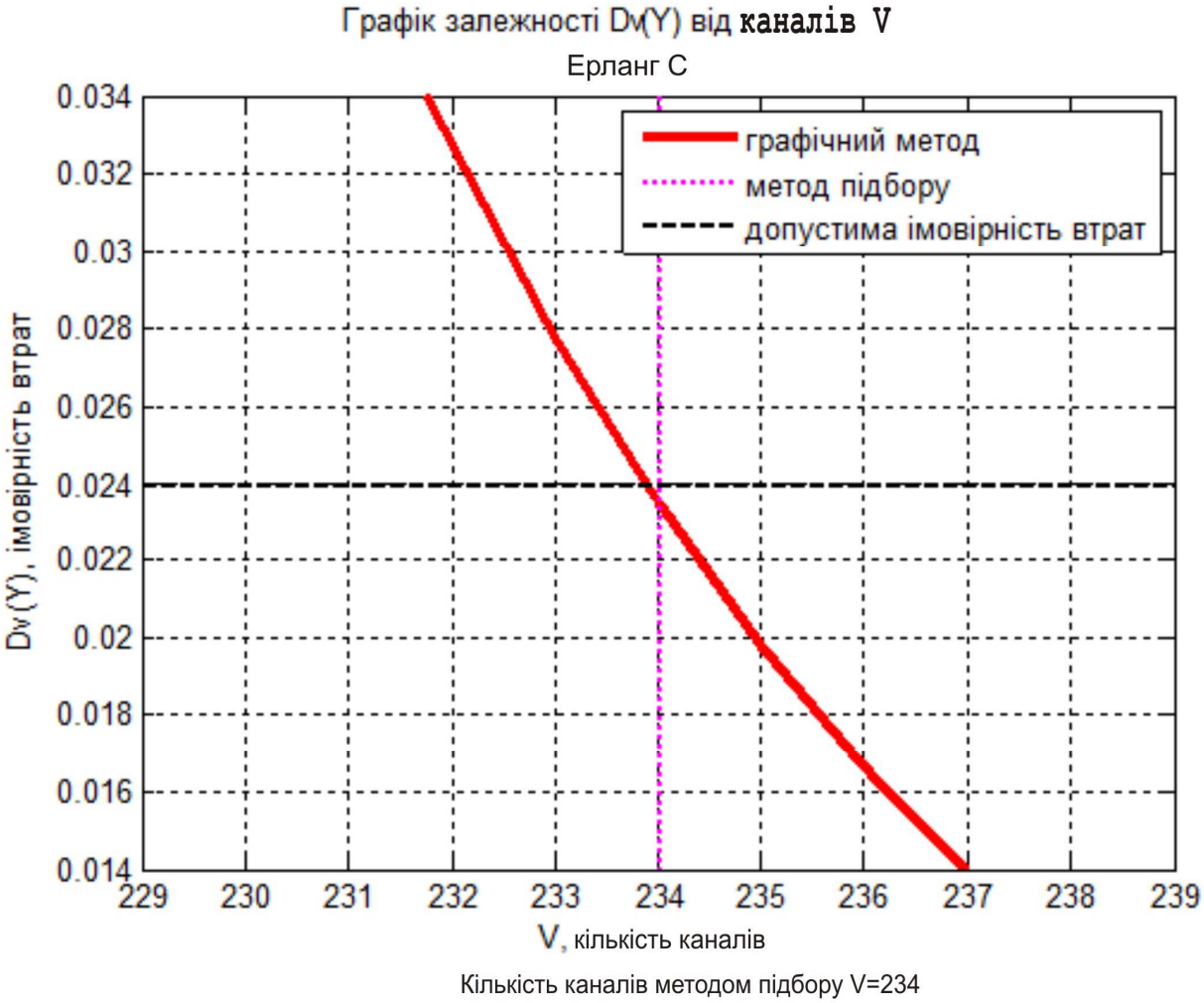


Рисунок 3. 8 - Графік залежності $D_v(Y)$ від кількості каналів

Висновки до третього розділу

1. Розглянуті основні положення теорії масового обслуговування, наведені основні вирази для розрахунку фактичного і запропонованого трафіку на основі рекомендацій ITU-T та відділу стандартизації комунікацій E.492. Показано, що при визначені пропускної здатності мережі окрім таких вимірюваних показників, як кількість спроб викликів на годину найбільшого навантаження та кількість викликів в секунду, необхідно додатково враховувати значення середнього часу очікування та показник ймовірності блокування викликів під час спроби зайняття каналу (коефіцієнт блокування). Це дозволить отримати більш точні параметри трафіку під час найбільшого навантаження.

2. Описані механізми керування обслуговуванням черг. Показано, що механізм керування черг FIFO не в змозі забезпечити передачу різного типу трафіку з заданою якістю, хоча його дуже просто реалізувати. При використанні механізму пріоритетного обслуговування черг, що зазвичай застосовується для чутливого до затримок класу трафіку, невеликої інтенсивності (8–16 Кбіт/с) і ставиться до вищого класу пріоритетності, забезпечується мінімізація впливу VoIP трафіку на інші, нижчі класи різного трафіку, що передається.

3. У відповідності до механізмів обслуговування черг обслуговуючі пристрої поділяються на комутатори: з буферизацією на вході, що мають низьку пропускну здатність завдяки блокування на входах та не вимагають високих швидкостей роботи та обсягу черги; з буферизацією на виході та поділюваною пам’яттю, які працюють з мінімальними втратами пакетів, максимальною пропускною здатністю та з мінімальними затримками на очікування обслуговування, але вимагають високих швидкостей роботи та ємностей буфера та високошвидкісні комутатори, які використовують буферизацію на вході з чергами віртуальних виходів (модель з очікуванням – Ерланг С), схеми яких дозволяють значно збільшити пропускну здатність

пристрою. Показано, що такі комутатори рекомендовано використовувати для обслуговування екстрених служб масового обслуговування і т. інш.

4. Наведений метод розрахунку пропускної здатності мережі VoIP телефонії з використанням моделей трафіку систем масового обслуговування (СМО) таких як: СМО з утриманням заблокованих викликів; СМО з заблокованими викликами, що перенапрямлені; СМО з затриманими заблокованими викликами, що побудовані на теорії черг. Показано, що системи з блокуванням доцільно використовувати на міжміських комутаційних центрах з великою інтенсивністю трафіку, де для її зменшення можна використовувати пакетні комутатори з блокуванням на вході (модель з блокуванням – Ерланг В).

5. Проведені розрахунки моделі трафіку згідно розподілу Пуассона показали, що для обробки навантаження 203,6 Ерл. з ймовірністю блокування 2,4% СМО проектованої мережі може обслужити 216 викликів.

6. Проведені розрахунки за моделлю трафіку Ерланг В для перепроектування вихідних груп магістральних каналів для міжміських викликів, показали що з ймовірністю блокування 0,024, необхідна кількість магістральних каналів для оброблення навантаження трафіку 203,6 Ерл. дорівнює – 216 каналам. При використанні такої кількості магістральних каналів та за умови використання голосового кодеку G.711 (загальна пропускна здатність кодеку G.711 - 107,2 Кбіт/с, максимальна пропускна здатність мережі сягає 23,155 Мбіт/с.

7. Проведені розрахунки за моделлю трафіку Ерланг С показали, що для забезпечення необхідних параметрів моделі трафіку Ерланг С очікуванням обслуговування потрібно 234 канали. Максимальна пропускна здатність мережі (за умови використання голосового кодеку G.711) сягає 25,084 Мбіт/с, що значно вище чим при використанні моделі з блокуванням (модель В).

4 МОНІТОРИНГ ТРАФІКУ МЕРЕЖ З ПАКЕТНОЮ КОМУТАЦІЄЮ

4.1 Оцінка часу прийомо – передачі пакетів мережею Інтернет

За допомогою утілити ping перевіримо мережне підключення до віддаленого сервера шляхом пересилання ехо –запиту на хост з вимогою відповіді. При цьому, відповідь для кожного пакета будемо отримувати на локальному персональному комп'ютері (ПК). За допомогою утілити ping можна оцінити, скільки часу витрачено на прийом- передачу трафіку мережею [22].

За замовчуванням передаються чотири ехо-пакета довжиною 32 байта, що представляють собою послідовність символів алфавіту в верхньому регістрі. Ping дозволяє змінити розмір і кількість пакетів, вказати, чи слід записувати маршрут, який вони використовують, яку величину часу життя встановлювати, чи можна фрагментувати пакет і т.д. При отриманні відповіді в поле визначається, за який час (у мілісекундах) посланий пакет доходить до віддаленого хосту і повертається назад. Так як значення за замовчуванням для очікування відгуку дорівнює 1 с, то всі значення даного поля будуть менше 1000 мс [23].

На персональному комп'ютері виконаємо пошук "cmd" та відправимо ехо – запит на хост з доменною адресою: ping www.cisco.com в командному рядку.

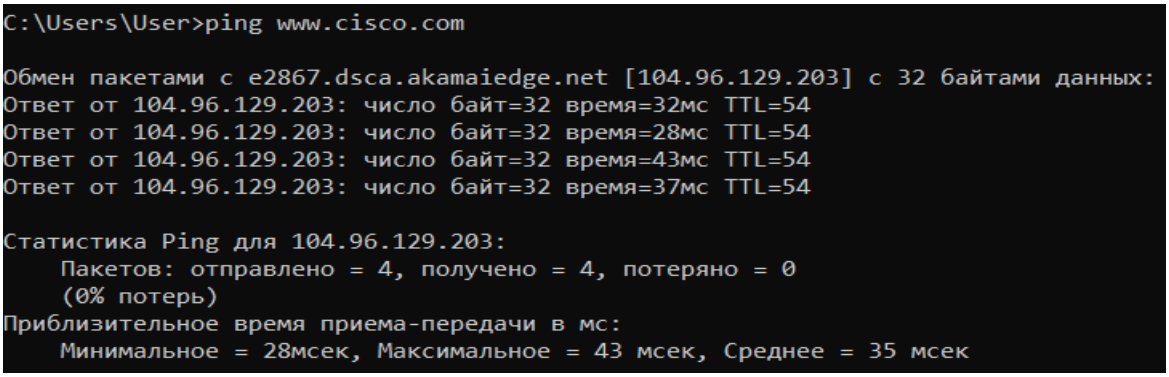


Рисунок 4.1 – Виконання команди ping www.cisco.com (копія екрану)

У першому рядку отриманих даних (рисунок 4.1) відображено повне доменне ім'я (Fully Qualified Domain Name, FQDN): e2867.dsca.akamaiedge.net та IP-адреса: 104.96.129.203.

За отриманими статистичними даними (нижня частина рисунку 4.1) видно (рисунок 4.2), що було відправлено чотири ехо –запити на хост з IP адресою 104.96.129.203, і на кожен з них була отримана відповідь. Отже, втрата пакетів склала 0%. В середньому, для прийомо- передачі пакетів по мережі потрібно 35 мс (рисунок 4.2).

```
Статистика Ping для 104.96.129.203:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 28мсек, Максимальное = 43 мсек, Среднее = 35 мсек
```

Рисунок 4.2 – Статистика при 4-х ехо –запитів (копія екрану)

При збільшенні ехо –запитів до 100 втрата пакетів склала 1%. В середньому, для прийомо- передачі пакетів мережею потрібно 39 мс (рисунок 4.3). Отже, при збільшенні запитів до хосту втрачаються передані дані. Така ситуація може скластися при передачі мережею, наприклад, потокового відео.

```
C:\Users\User>ping -n 100 www.cisco.com

Статистика Ping для 104.96.129.203:
    Пакетов: отправлено = 100, получено = 99, потеряно = 1
    (1% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 24мсек, Максимальное = 1138 мсек, Среднее = 39 мсек
```

Рисунок 4.3 – Статистика при 100 ехо –запитів (копія екрану)

Для обчислення втрат пакетів в мережі Інтернет скористаємось також утилітою ping [23], для чого відправимо ехо - запити на веб-сайти регіональних інтернет - реєстраторів (англ. Regional Internet Registry, RIR), розташованих в різних частинах світу, якими є: Африка (рисунок 4.4); Австралія (рисунок 4.5); Європа (рисунок 4.6) та Південна Америка (рисунок 4.7).

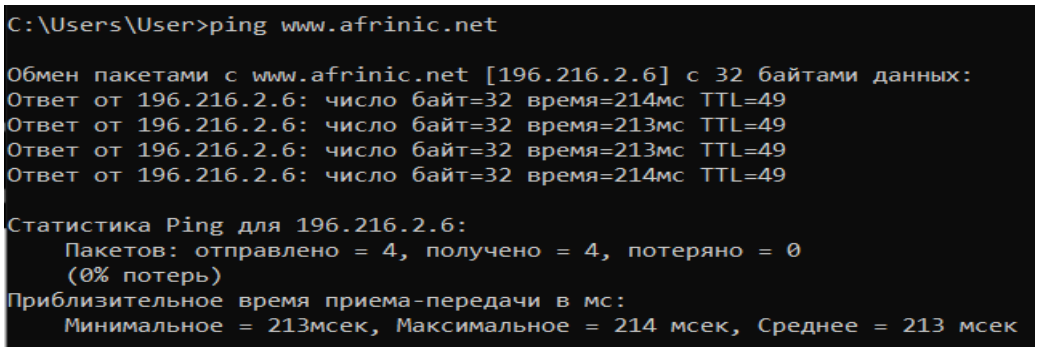


Рисунок 4.4 – Виконання команди ping на хост RIR з IP адресою 196.216.2.6 розташованого в Африці (копія екрану)

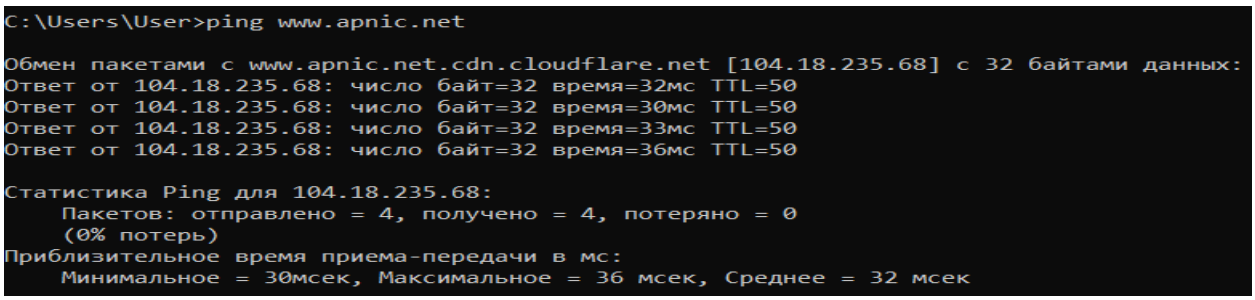


Рисунок 4.5 – Виконання команди ping на хост RIR з IP адресою 104.18.255.68 розташованого в Австралії (копія екрану)

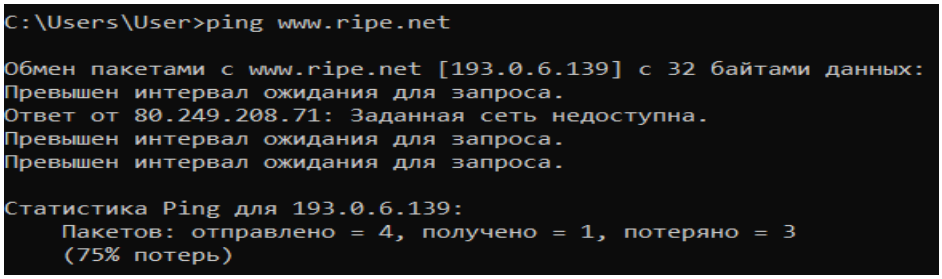


Рисунок 4.6 – Виконання команди ping на хост RIR з IP адресою 193.0.6.139 розташованого в Європі (копія екрану)

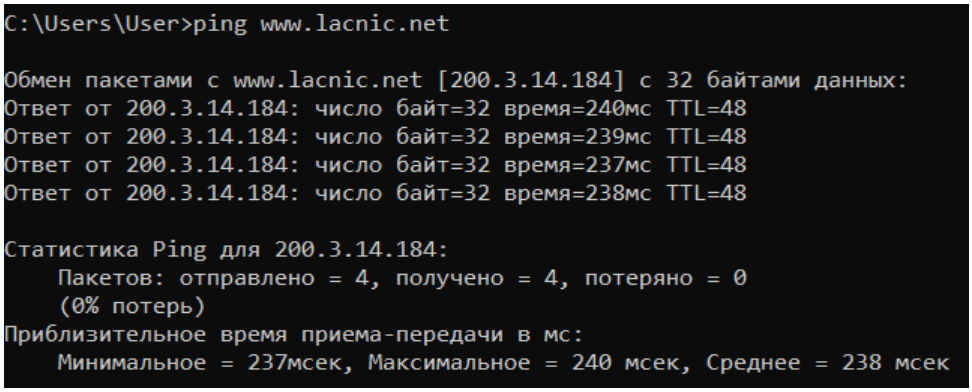


Рисунок 4.7 – Виконання команди ping на хост RIR з IP адресою 200.3.14.184 розташованого в Південній Америці (копія екрану)

Результати моніторингу показали, що найбільший час потрачено на прийом - передачу пакетів на хост RIR (238 мс), що розташований в Південній Америці (рисунок 4.7) – найменший на хост RIR (32 мс), що розташований в Австралії (рисунок 4.5). Затримка, визначена утилітою, викликана не тільки пропускною здатністю каналу передачі даних до певного хосту, але й завантаженістю цієї машини.

При цьому, при відправленні ехо –запитів на хост RIR з IP адресою 193.0.6.139, що розташований в Європі було перевищений інтервал часу очікування для запиту та як результат, втрачено 75% пакетів (рисунок 4.6), це може означати, що даний хост не доступний, або швидкість Інтернету дуже повільна.

4.2 Визначення затримок в мережі Інтернет за допомогою утиліти tracert

Для отримання значень затримок в мережі розглянемо кожен її сегмент, через який проходили дані. Для цього використаємо утиліту tracert [24].

Засіб діагностики tracert визначає маршрут до місця призначення, надіславши протокол керівних повідомлень Інтернету (ICMP) ехо- пакетів до місця призначення. У цих пакетів tracert, використовує різні IP час TTL, значення. На кожному маршрутизаторі на маршруті tracert надсилає перший пакет, TTL якого дорівнює 1 і далі, збільшує TTL на 1 на кожному наступному кроці передачі, доки не достанеться місця призначення або не досягне максимального TTL. При цьому, в обидві сторони передаються ICMP, "Перевищення часу" – повідомлення від проміжних маршрутизаторів. Tracert, також, виводе замовлений список проміжних маршрутизаторів, які завершуються ICMP- "Перевищення часу" повідомлення та повідомляє про IP-адресу інтерфейсу кожного маршрутизатора.

Введемо команду tracert www.cisco.com в командному рядку (рисунок 4.8) [23]:

```
C:\Users\User>tracert www.cisco.com

Трассировка маршрута к e2867.dsca.akamaiedge.net [104.96.129.203]
с максимальным числом прыжков 30:

  1     2 ms     2 ms    11 ms  192.168.0.1
  2     4 ms     5 ms     6 ms  93-77-12-1.khm.volia.net [93.77.12.1]
  3     3 ms     4 ms     4 ms  km-5.cr-1.tvservice.km.ua [77.121.26.145]
  4     7 ms     4 ms     5 ms  v3325.cs-1.khm.volia.net [77.121.26.161]
  5     *       12 ms    13 ms  be7.966.cr-2.g50.kiev.volia.net [77.120.0.69]
  6    10 ms     9 ms     8 ms  be3.180.cr-1.g50.kiev.volia.net [77.120.1.41]
  7    13 ms    13 ms    12 ms  be6172.ccr22.kbp01.atlas.cogentco.com [149.6.190.25]
  8    28 ms    25 ms    24 ms  be2047.ccr22.bts01.atlas.cogentco.com [154.54.60.205]
  9    30 ms    25 ms    26 ms  be3463.ccr52.vie01.atlas.cogentco.com [154.54.59.185]
 10    28 ms    27 ms    30 ms  ae-14.r00.vienat02.at.bb.gin.ntt.net [129.250.9.129]
 11    27 ms    29 ms    31 ms  185.84.16.3
 12    28 ms    27 ms    27 ms  a104-96-129-203.deploy.static.akamaitechnologies.com [104.96.129.203]

Трассировка завершена.
```

Рисунок 4.8 – Виконання команди tracert www.cisco.com (копія з екрану)

Залежно від зони охоплення інтернет-провайдера і розташування вузлів джерела і призначення маршрути перетинали безліч переходів і мереж. Кожен «Перехід» - це один маршрутизатор (рисунок 4.8).

Оскільки комп'ютери спілкувались на мові цифр, а не слів, маршрутизаторам присвоювались унікальні IP-адреси (числа в форматі x.x.x.x для адрес IPv4). З рисунку 4.8 видно, яким шляхом проходить пакет даних до кінцевого пункту призначення. Крім того, за допомогою утиліти tracert можна визначити, з якою швидкістю проходив трафік через кожен сегмент мережі. Кожному маршрутизатору на шляху проходження даних відправлялись три пакети, час відповіді на які вимірювались в мілі секундах. Використовуючи дану інформацію, можна проаналізувати результати, отримані за допомогою утиліти tracert при відправці пакетів до www.cisco.com. Нижче представлений весь маршрут трасування.

У наведеному вище прикладі (рисунок 4.8) пакети, відправлені за допомогою утиліти tracert, пересилаються з ПК джерела на шлюз локального маршрутизатора (перехід 1: 192.168.0.1), а потім на маршрутизатор в точці присутності (POP) до інтернет-провайдера (перехід 2: 93.77.12.1). У кожного провайдера є безліч маршрутизаторів POP. Вони відзначали границі мережі інтернет-провайдера і служили точками підключення до Інтернету клієнтів

мережі. Пакети проходили через два переходи в мережі Volia і потрапляли в маршрутизатор, який належить хосту ntt.net та хосту atlas.cogentco.com. Це означає, що пакети досягли іншого інтернет-провайдера. Цей момент дуже важливий, оскільки при пересиланні пакетів від одного до іншого провайдера можливі втрати, а також важливо пам'ятати, що не всі інтернет-провайдери здатні забезпечити однакову швидкість передачі даних.

Отже, інтернет-трафік починався на ПК користувача і проходив через домашній маршрутизатор (перехід 1). Потім дані надходили до інтернет-провайдера і передавались його мережею (переходи 2-11), поки не досягнули віддаленого сервера (перехід 12). Це досить нетиповий приклад, так як від початку до кінця маршруту задіяний тільки один провайдер. Як правило, буває два або кілька Інтернет-провайдерів, як показано на рисунках 4.8, 4.9.

Розглянемо приклад з пересилкою інтернет-трафіку через кілька інтернет-провайдерів. На рисунку 4.9 показані результати виконання команди tracert для трасування маршруту за доменною адресою: www.afrinic.net.

```
C:\Users\User>tracert www.afrinic.net

Трассировка маршрута к www.afrinic.net [196.216.2.6]
с максимальным числом прыжков 30:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     6 ms     4 ms     5 ms  93-77-12-1.khm.volia.net [93.77.12.1]
  3     6 ms     6 ms     4 ms  km-5.cr-1.tvservice.km.ua [77.121.26.145]
  4     6 ms     7 ms     5 ms  v3325.cs-1.khm.volia.net [77.121.26.161]
  5    12 ms    12 ms    14 ms  be7.966.cr-2.g50.kiev.volia.net [77.120.0.69]
  6    13 ms    12 ms    12 ms  ae20.RT.NTL.KIV.UA.retn.net [87.245.237.56]
  7    39 ms    40 ms    38 ms  ae4-2.RT.EQX.FKT.DE.retn.net [87.245.233.164]
  8    41 ms    37 ms    38 ms  ipv4.de-cix.fra.de.as37271.workonline.africa [80.81.195.27]
  9   211 ms   212 ms   212 ms  cr1-fxn-agr1-te0-2.wolcomm.net [197.157.77.48]
 10     *        *        *     Превышен интервал ожидания для запроса.
 11     *        *        *     Превышен интервал ожидания для запроса.
 12   215 ms   215 ms   218 ms  esr1-isd-cr2-te0-0-27.wolcomm.net [197.157.77.101]
 13   210 ms   209 ms   215 ms  197.157.64.195
 14   214 ms   214 ms   211 ms  www.afrinic.net [196.216.2.6]

Трассировка завершена.
```

Рисунок 4.9 – Виконання команди tracert на хост www.afrinic.net (копія екрану)

На рисунку 4.10 наведені результати, які отримані в ході трасування маршруту до хосту RIR www.lacnic.net, що розташований в Південній Америці, за якими можна побачити, що максимальне число скачків дорівнює –30 та 18

переходів між різними провайдерами, на відміну від попереднього трасування, де було 14 переходів, причому 2 хости, з них, не відповіли на запити. Загальна затримка для першого випадку (рисунок 4.9) склала – 214 мс, тоді як у другому випадку вона дорівнювала вже 235 мс.

```
C:\Users\User>tracert www.lacnic.net

Трассировка маршрута к www.lacnic.net [200.3.14.184]
с максимальным числом прыжков 30:

  1     2 ms     1 ms     1 ms  192.168.0.1
  2    12 ms     4 ms     5 ms  93-77-12-1.khm.volia.net [93.77.12.1]
  3     3 ms     6 ms     3 ms  km-5.cr-1.tvservice.km.ua [77.121.26.145]
  4     5 ms     4 ms     8 ms  v3325.cs-1.khm.volia.net [77.121.26.161]
  5    14 ms    13 ms    11 ms  be7.966.cr-2.g50.kiev.volia.net [77.120.0.69]
  6    16 ms    10 ms    14 ms  ae20.RT.NTL.KIV.UA.retn.net [87.245.237.56]
  7     *       43 ms    43 ms  ae8-10.RT.IRX.FKT.DE.retn.net [87.245.232.139]
  8    45 ms    44 ms    43 ms  ae17.cr6-fra2.ip4.gtt.net [154.14.40.233]
  9   150 ms   188 ms   149 ms  et-0-0-17.cr6-mia1.ip4.gtt.net [213.200.113.142]
 10   157 ms   150 ms   151 ms  ip4.gtt.net [98.124.189.122]
 11   259 ms   254 ms   254 ms  et-14-0-4-0.monet.ptx-b.spo-piaf.algartelecom.com.br [168.197.23.146]
 12   254 ms   253 ms   254 ms  100.127.5.114
 13   255 ms   255 ms   259 ms  201-048-035-089.static.ctbctelecom.com.br [201.48.35.89]
 14   238 ms   237 ms   244 ms  xe-4-2-1-0.core1.nu.registro.br [200.160.0.180]
 15   239 ms   237 ms   238 ms  xe-0-0-0.ar3.nu.registro.br [200.160.0.249]
 16   244 ms   241 ms   240 ms  ae0-0.gw1.jd.lacnic.net [200.160.0.212]
 17   238 ms   241 ms   239 ms  200.3.12.34
 18   239 ms   235 ms   241 ms  www.lacnic.net [200.3.14.184]

Трассировка завершена.
```

Рисунок 4.10 – Виконання команди tracert на хост www.lacnic.net (копія екрану)

Виконати трасування маршруту до віддаленого сервера можливо також і за допомогою програмного інструменту Visual Route Lite Edition – це програма, що дозволяє наочно відобразити результати трасування маршруту та визначити час RTT (час пересилання сигналу від передавача до отримувача та у зворотному напрямку – підтвердження отримання сигналу) (рисунок 4.11) [25].

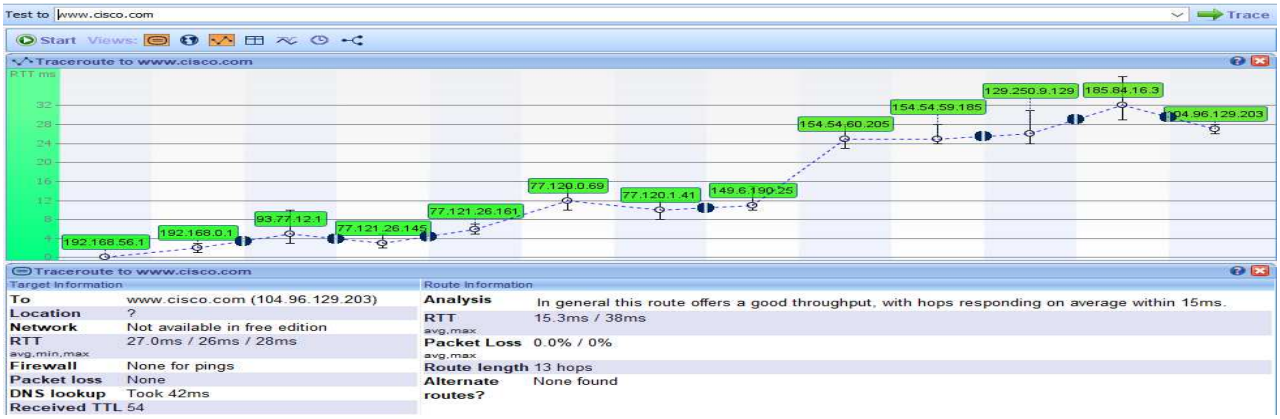


Рисунок 4.11– Трасування маршрутів за адресом www.cisco.com за допомогою програмного забезпечення Visual Route

З рисунку 4.11 видно, що отриманий час RTT (передачі пакетів) від передавача з IP адресою 192.168.56.1 до отримувача (приймача) з IP адресою 104.96.129.203 становив 38 мс (максимальне значення) та 15,3 мс (середнє значення).

4.3 Аналіз параметрів трафіку за допомогою програмного забезпечення Wireshark

Для аналізу параметрів трафіку та визначення його характеристик скористуємось програмним забезпеченням Wireshark – це програма для аналізу мережевих протоколів з відкритим кодом, заснована Джеральдом Комбсом у 1998 році. Глобальна організація мережевих спеціалістів та розробників програмного забезпечення підтримує Wireshark і продовжує оновлювати нові мережеві технології та методи шифрування [26].

Wireshark абсолютно безпечний у використанні. Державні установи, корпорації, некомерційні організації та навчальні заклади використовують Wireshark для пошуку та усунення несправностей. Немає кращого способу навчитися роботі з мережею, ніж розглянути трафік за допомогою Wireshark.
Wireshark - це інструмент аналізу пакетів (одне повідомлення від будь-якого мережевого протоколу – TCP, DNS тощо). Він фіксує мережевий трафік у локальній мережі та зберігає ці дані для автономного аналізу. Wireshark фіксує мережевий трафік з Ethernet, Bluetooth, Wireless (IEEE.802.11), Token Ring, Frame Relay і багато іншого.

При цьому, трафік локальної мережі повинен знаходиться в режимі трансляції, тобто один комп’ютер з Wireshark може бачити трафік між двома іншими комп’ютерами. Якщо необхідно проаналізувати трафік на зовнішньому сайті, то потрібно здійснити захоплення пакетів на локальному комп’ютері користувача.

Окрім того, Wireshark дозволяє фільтрувати журнал перед початком захоплення або під час аналізу, завдяки чому можна звузити і обнулити те, що є шуканим в мережевій трасі. Наприклад, можна встановити фільтр для

перегляду тільки TCP- трафіку між двома IP-адресами. Також можна встановити його лише для показу пакетів, надісланих з одного комп'ютера. Фільтри Wireshark - одна з основних причин, через яку він став стандартним інструментом для аналізу пакетів [23,26].

Скористаємося можливостями даного програмного продукту, для чого запустимо в браузері онлайн відео трансляцію фільму.

Відкриємо Wireshark та запустимо режим захоплення пакетів. Режим захоплення зупинимо, коли число захоплених пакетів на обраному інтерфейсі Ethernet досягне – 20 000 штук (рисунок 4.12).

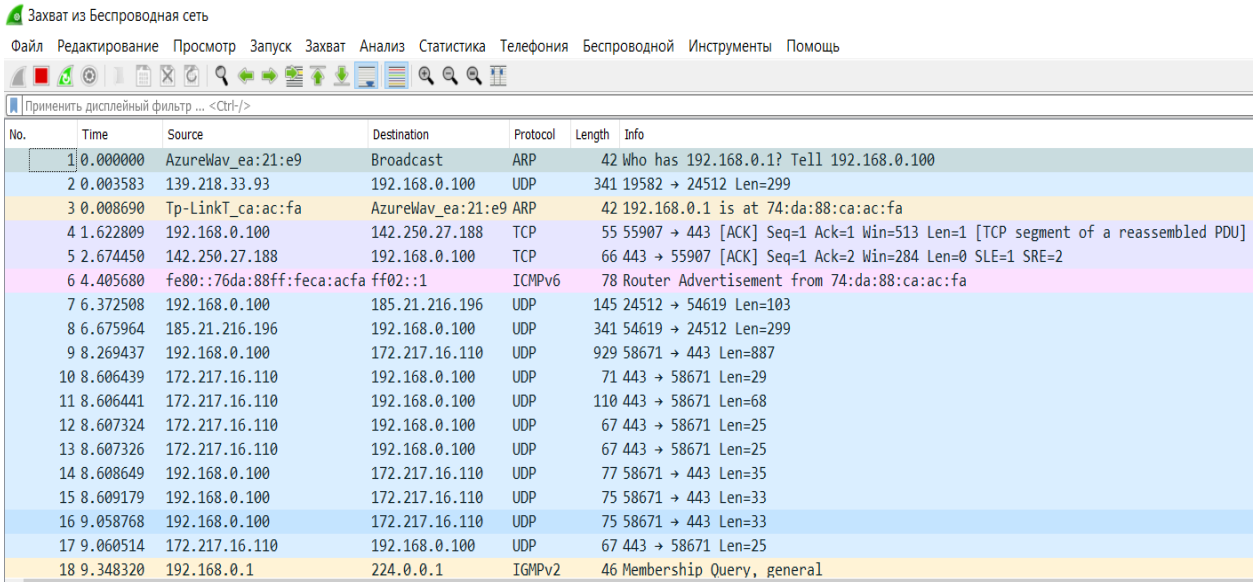


Рисунок 4.12 – Результат реєстрації потоку пакетів на інтерфейсі Ethernet

Подальшим кроком є виділення пакетів потоку відео серед захоплених пакетів. Для цього у вікні (рисунок 4.12) знайдемо IP адресу джерела пакетів 192.168.0.100 - IP адреса джерела, і ввівши в поле «Filter» рядок ip.src ==192.168.0.100 відфільтруємо тільки пакети, що надійшли від обраного джерела (рисунок 4.13).

Для визначення інтенсивності трафіку мережі Інтернет в меню Wireshark оберемо меню «Статистика» підменю «Загалом». У вікні (рисунок 4.14) знайдемо наступні параметри: інтенсивність пакетів; середній розмір пакета та інтенсивність трафіку (Кбіт / с).

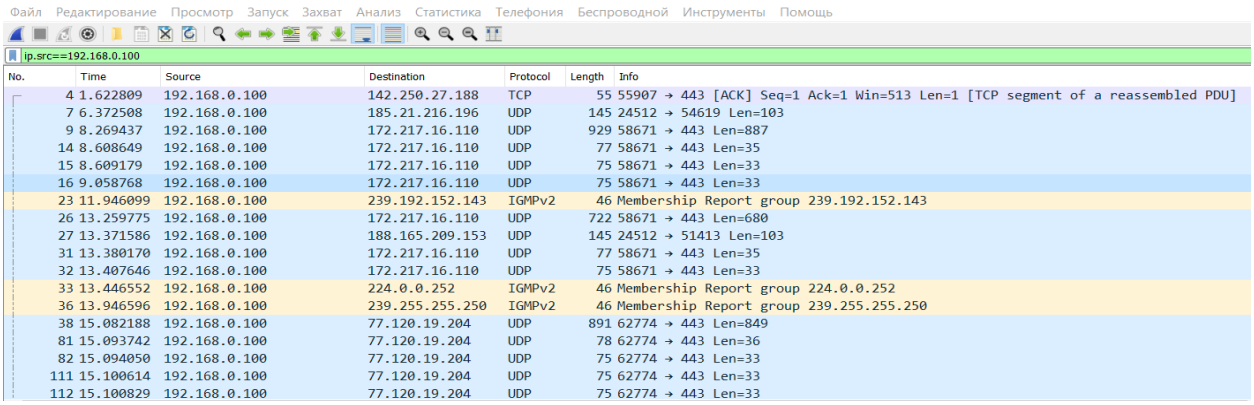


Рисунок 4.13 - Фільтрація потоку відеотрафіку

Згідно з отриманими статистичними даними (рисунок 4.14) визначаємо наступні характеристики відеотрафіку: λ = 8,7 пакета / с – інтенсивність пакетів; L=171 байти – середній розмір пакета, a=11 Кбіт/ с – інтенсивність відеотрафіку / с.

Статистика

Измерение	Захвачено	Показано	Помеченный
Пакеты	20316	3855 (19.0%)	–
Временной промежуток, с	445.671	444.004	–
В среднем, пакетов/с	45.6	8.7	–
Средний размер пакета, Байт	1062	171	–
Байты	21567809	658452 (3.1%)	0
В среднем байт/с	48 k	1482	–
В среднем бит/с	387 k	11 k	–

Рисунок 4.14 – Статистичні параметри відеотрафіку

Графіки введення/виведення переданих відеопакетів за секундні інтервали наведені на рисунку 4.15, а результати оцінки параметрів трафіку зведено до таблиці 4.1.

Таблиця 4.1– Результати оцінки параметрів трафіку, отриманих експериментальним шляхом

№	Параметр	Од. виміру	Значення
1	Інтенсивність пакетів	пакетів / с	8,7
2	Розмір пакету	байт	171
3	Часовий проміжок	с	444,004
4	Число пакетів	шт.	3855
5	Інтенсивність трафіку	Кбіт / с	11

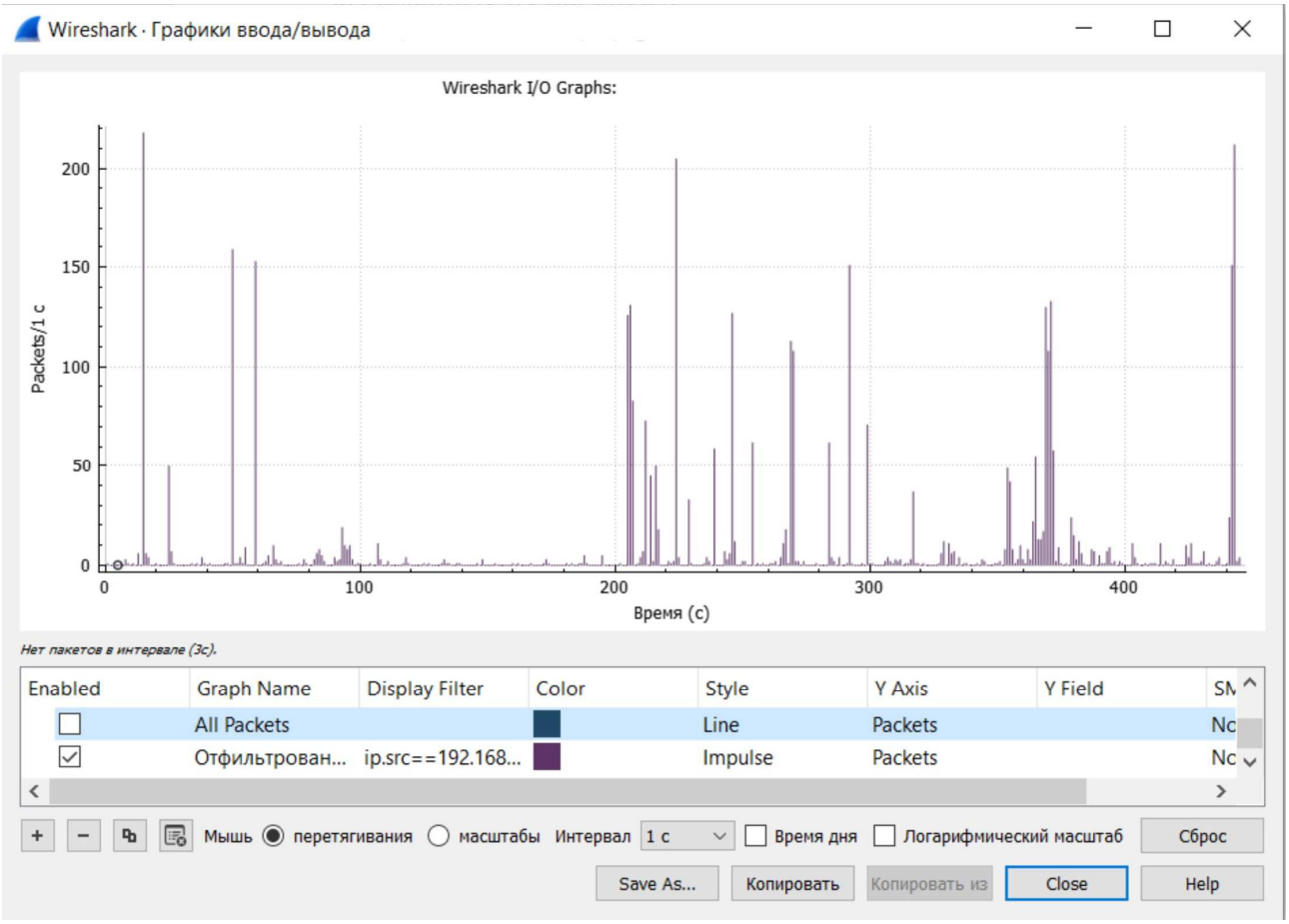


Рисунок 4.15 – Графіки введення/виведення переданих відеопакетів

Висновки до четвертого розділу

За допомогою активних засобів моніторингу трафіку зроблено оцінку часу на прийом–передачу пакетів мережею Інтернет:

1. Показано, що утиліта ping дозволяє змінити розмір і кількість пакетів, вказати, чи слід записувати маршрут, який він використовує, яку величину часу життя встановлювати, чи можна фрагментувати пакет і т.д. Отримані статистичні значенні показали, що при збільшенні запитів до хосту втрачаються передані дані. Виявлено, що при 4-х ехо –запитів на хост з IP адресою 104.96.129.203 для прийомо- передачі пакетів мережею, в середньому, потрібно 35 мс при 0% втрат. При збільшенні ехо –запитів до 100 втрата пакетів склала 1%, а час прийомо- передачі пакетів збільшився до 39 мс. Так як значення за замовчуванням для очікування відгуку дорівнює 1 с, то всі отримані значення часу склали менше 1000 мс, що цілком прийнятно. Результати моніторингу на хости регіональних інтернет - реєстраторів RIR, розташованих в різних частинах світу показали, що найбільший час потрачено на прийом - передачу пакетів на хост RIR (238 мс), що розташований в Південній Америці – найменший на хост RIR (32 мс), що розташований в Австралії. Затримка, визначена утилітою, викликана не тільки пропускною здатністю каналу передачі даних до певного хосту, але й завантаженістю цієї машини. При цьому, при відправленні ехо –запитів на хост RIR з IP адресою 193.0.6.139, що розташований в Європі було перевищений інтервал часу очікування для запиту та як результат, втрачено 75% пакетів, це може означати, що даний хост не доступний, або швидкість Інтернету дуже повільна.

2. Отримані значення за допомогою засобу діагностики tracert. Побудований маршрут до місця призначення. Показано, що у кожного провайдера є безліч маршрутизаторів POP. Вони відзначають границі мережі інтернет-провайдера і служать точками підключення до Інтернету клієнтів мережі. Для наведених прикладів отримано максимальне число скачків від 14

до 30 при 12 та 18 переходах між різними провайдерами, відповідно. Загальна затримка на трасі маршруту склала – 214 мс та 235 мс, відповідно.

3. Виконано трасування маршруту до віддаленого сервера за допомогою програмного інструменту Visual Route Lite Edition та визначений час RTT (передачі пакетів) від передавача з IP адресою 192.168.56.1 до отримувача (приймача) з IP адресою 104.96.129.203, що становив 38 мс (максимальне значення) та 15,3 мс (середнє значення).

4. Проведений аналіз параметрів трафіку потокового відео та визначенні його характеристики за допомогою програмного забезпечення Wireshark. Експериментальним шляхом отримані оцінки параметрів трафіку. Розрахований параметр інтенсивності трафіку потокового відео на хості ютуб-каналу дорівнював 11 Кбіт/с. Рекомендовано для більш точних вимірювань параметрів трафіку за допомогою Wireshark використовувати проводові підключення до мережі Інтернет, а також до початку проведення діагностики, закрити всі інші відкриті веб – сторінки та завершити всі зайві задачі ОС на локальному комп’ютері.

Висновки

1. Розглянуто принципи організації глобальної мережі, описана структура та протоколи мережі з пакетною комутацією повідомлень. Проведений аналіз комутованих технологій показав, що існує декілька технологій мереж - X.25, Frame Relay, ATM, Ethernet, що забезпечують задану якість сервісу та надають конвергентні послуги мережі. Показано, що найбільш перспективною технологією є Ethernet, який пропонує масштабованість 10/100/1000/10000 Мбіт/с, завдяки використання одного формату Ethernet кадру у всіх його модифікаціях, це дозволяє безперешкодно інтегрувати LAN, MAN та WAN та будувати високошвидкісні мережі з високою пропускною здатністю.

2. Виявлено, що швидкість широкосмугового зв'язку є вирішальним фактором, що сприяє IP - трафіку, яка, в свою чергу, залежить від пропускної здатності телекомунікаційної мережі.

3. Проведений аналіз сучасного трафіку глобальної мережі, який показав, що за прогнозами, кількість користувачів Інтернету до 2023 року сягне 5,3 мільярди, що складе 66 відсотків світового населення. Це вимагає удосконалення методів проведення оцінки необхідної пропускної здатності IP мережі.

4. Розглянуто стек протоколів TCP / IP. Представлена архітектура основних протоколів стеку TCP / IP. Показано, що основою усієї архітектури є міжмережний протокол IP за допомогою якого реалізується адресація вузлів мережі і доставка даних та транспортний протокол управління передачею TCP.

5. Розглянуто принципи комутації пакетів, описані основні режими комутації пакетів: віртуальних з'єднань та дейтаграмний режим, перевагою якого є можливість використання динамічної маршрутизації при передачі пакетів між абонентськими вузлами.

6. Розраховані типові затримки, що виникають при комутації пакетів. Розрахунки показали, що затримка передачі для кожного пакета зменшується при збільшенні кількості пакетів (з 1,1 мс при N = 1 шт. до 0,45 мс при N = 20 шт.). Існує граничне значення, при якому загальний витрачений час на початку

зменшується (N = 1 шт., $t_{заг.}$=3,3 мс; N = 5 шт. $t_{заг.}$=2,1 мс). При збільшенні кількості пакетів після цього обмеження, загальний час починає збільшуватися (N = 10 шт., $t_{заг.}$= 2,4 мс; N = 20 шт., $t_{заг.}$= 3,3 мс). Якщо кількість пакетів дуже велика, то це займає набагато більше часу, ніж час, необхідний для передачі одного пакета.

7. Розглянуті основні положення теорії масового обслуговування, Показано, що при визначені пропускної здатності мережі необхідно враховувати параметри трафіку під час найбільшого навантаження. Описані механізми керування обслуговуванням черг. Показано, що при використанні механізму пріоритетного обслуговування черг в мережах голосової телефонії, забезпечується мінімізація впливу VoIP трафіку на інші, нижчі класи різного трафіку, що передається. Надані рекомендації для використання високошвидкісних комутаторів, які використовують буферизацію на вході з чергами віртуальних виходів для збільшення пропускної здатності мережі.

8. Наведений метод розрахунку пропускної здатності мережі VoIP телефонії з використанням моделей трафіку систем масового обслуговування (СМО) таких як: СМО з утриманням заблокованих викликів (розподіл Пуассона); СМО з заблокованими викликами, що перенапрямлені (модель трафіку Ерланг В); СМО з затриманими заблокованими викликами, що побудовані на теорії черг (модель трафіку Ерланг С), використання якого надає можливість проектувати трафік інтернет мереж, вирішувати проблеми якості зв'язку, визначити рівень обслуговування та коефіцієнт блокування мереж. Мережа, спроектована з використанням даного методу, має низький коефіцієнт блокування і високий рівень використання каналу.

9. За допомогою активних засобів моніторингу трафіку зроблено оцінку часу на прийом–передачу пакетів мережею Інтернет за допомогою спеціальних утиліт ping та tracert та програмного забезпечення, що призначене для діагностики мереж Інтернет: Visual Route Lite Edition та Wireshark. Побудований маршрут до місця призначення. Показано, що у кожного провайдера є безліч маршрутизаторів POP. Виконано трасування маршруту до

віддалених серверів розташованих в різних частинах світу, визначений максимальний та мінімальний час передачі пакетів – RTT, при різній кількості скачків. Проведений аналіз параметрів трафіку потокового відео та визначенні його характеристики. Експериментальним шляхом отримані оцінки параметрів трафіку, що співпали з аналітичними розрахунками.

Перелік посилань

1. Cisco Annual Internet Report (2018–2023) White Paper. – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://u.to/4bxgGg

2. Брейман А.Д. Сети ЭВМ и телекоммуникации. Глобальные сети. – М.: МГУПИ, 2006. – 117 с.

3. Ложковський А.Г. Теорія масового обслуговування в телекомунікація / А.Г. Ложковський. – Одеса: ОНАЗ ім. О.С. Попова, 2010. – 112 с.: іл.

4. Комп'ютерні мережі: навч. посібник / [О.Д. Азаров, С.М. Захарченко, О.В. Кадук та ін.] – Вінниця: ВНТУ, 2013. – 371 с.

5. В. Г. Олифер, Н.А. Олифер. Компьютерные сети. Принципы, технологии, протоколы: Ученик для вузов. 5-е узд.– СПб. : Питер, 2016. – 992 с.

6. Глобальные сети с коммутацией пакетов – Назва з екрану. – [Електронний ресурс]. – Режим доступу: http://rz6hpi.narod.ru/net/cisco/cisco/cv_34A.html

7. Телекомунікаційні системи та мережі : навчальний посібник для студентів спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології» / Укладачі : Микитишин А.Г., Митник М.М., Стухляк П.Д. – Тернопіль : ТНТУ ім. Івана Пулюя, 2017 – 384 с.

8. Протоколы информационно-вычислительных сетей. Под. ред. Мизина И.А. и Кулешова А.П. М.: Радио и связь, 1990, 504 с.

9. Configuring X.25 PVCs – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/wan/x25-protocols/12498-config-x25-pvcs.html

10. Комп'ютерні мережі: [навчальний посібник] / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник.– Львів: «Магнолія 2006», 2013. – 256 с.

11. Технология АТМ – Назва з екрану. – [Електронний ресурс]. – Режим доступу: http://network.xsp.ru/5_9.php

12. Буров Є.В. Комп'ютерні мережі: підручник /Є.В. Буров. – Львів: «Магнолія 2006», 2010. – 262 с.

13. Організація комп'ютерних мереж [Електронний ресурс] : підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Електронні текстові дані (1 файл: 45,7 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2018. – 259 с.

14. Halsall F. Data communications, computer networks and open systems. Addison-Wesley publishing company, 1992, 772 pp.

15. Internet protocol – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https:|//tools.ietf.org/html/RFC791.

16. Сетевые модели TCP/IP и OSI – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://ciscolearning.ru/basics/tcpip-osi/

17. Конспект лекцій з дисципліни «Інформаційно-комунікаційні системи», Ч. II, для студентів усіх форм навчання спеціальності 125 «Кібербезпека» за освітньою програмою «Безпека інформаційних комунікаційних систем» [Електронний ресурс] / Упоряд. Г.З. Халімов. – Електронне видання. – Харків: ХНУРЕ, 2019. – 207 с. – pdf 6,19 Mb.

18. Характеристики голосового трафика. – Назва з екрану. – [Електроний ресурс]. – Режим доступу: http://surl.li/gqpv.

19. Еременко, В.Т. Методы и модели теории телетрафика: учебное пособие / В.Т. Еременко [и др.]. – Орёл: ОГУ им. И.С. Тургенева, 2019. –244 с.

20. Системи комутації – Назва з екрану. – [Електроний ресурс]. – Режим доступу: http://vnstele.com/system-komut.html.

21. Math. Graphics. Programming. – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://www.mathworks.com/products/matlab.html

22. Команда ping – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://www.new-line.net/podderzhka/diagnostika-seti/proverka-trafika/komanda-ping/

23. Empowering all people with career possibilities – [Електронний ресурс]. – Режим доступу: https://www.netacad.com/

24. Использование команды TRACERT для устранения неполадок TCP/IP в Windows – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://u.to/LeJgGg

25. VisualRoute Lite – Назва з екрану. – [Електронний ресурс]. – Режим доступу: http://www.visualroute.com/lite.html

26. Wireshark – Назва з екрану. – [Електронний ресурс]. – Режим доступу: https://www.wireshark.org/

Додаток А

Презентація

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет програмування та комп'ютерних і телекомунікаційних систем

Кафедра телекомунікацій, медійних та інтелектуальних технологій

ДИПЛОМНА РОБОТА
«МЕТОД ВИЗНАЧЕННЯ ПРОПУСКНОЇ ЗДАТНОСТІ МЕРЕЖ З ПАКЕТНОЮ КОМУТАЦІЄЮ»

Спеціальність 172 – «Телекомунікації та радіотехніка»

Виконав: студент 2 курсу, група $ТР_м$-19-1 Н. О. Кубатий

Керівник: канд. техн. наук, доц. А. А. Таранчук

Хмельницький, 2020

Мета роботи – удосконалення методу визначення пропускної здатності мереж пакетної комутації.

Завдання, які вирішуються в роботі

1. Розглянути принципи організації та використання мереж з пакетною комутацією.
2. Дослідити протоколи передачі даних та визначити основні характеристики мереж з комутацією пакетів.
3. Розрахувати пропускну здатність мережі голосової IP – телефонії.
4. Провести моніторинг трафіку мереж з пакетною комутацією.

Об'єкт дослідження: процеси передачі трафіку в мережах з пакетною комутацією.

Предмет дослідження: метод визначення пропускної здатності мереж з пакетною комутацією.

Наукова новизна отриманих результатів:

1. Набув подальшого розвитку метод визначення здатності мережі VoIP телефонії з використанням моделей трафіку систем масового обслуговування (СМО), зокрема:

– СМО з утриманням заблокованих викликів на основі розподілу Пуассона;

– СМО з заблокованими викликами, що перенапрямлені на основі моделі Ерланга B;

– СМО з затриманими заблокованими викликами, що побудовані на основі моделі Ерланга C.

Використання запропонованого методу дозволяє підвищити ефективність використання мережі за рахунок збільшення рівня використання каналу передачі даних та зменшення коефіцієнту блокування мережі.

Практична значимість отриманих результатів:

1. Розраховані типові затримки, що виникають при комутації пакетів VoIP мережі. Надані рекомендації для використання високошвидкісних комутаторів, які використовують буферизацію на вході з чергами віртуальних виходів для збільшення пропускної здатності мережі.

2. За допомогою активних засобів моніторингу трафіку виконано оцінку часу на прийом–передачу пакетів мережею Інтернет за допомогою спеціальних утиліт ping та tracert та програмного забезпечення, що призначене для діагностики мереж Інтернет. Виконано трасування маршруту до віддалених серверів розташованих в різних частинах світу, визначений максимальний та мінімальний час передачі пакетів – RTT, при різній кількості стрибків. Експериментально підтверджено результати аналітичних розрахунків.

Структура і обсяг дипломної роботи. Дипломна робота складається із вступу, чотирьох розділів, висновків до кожного розділу, висновків, списку посилань, додатку. Загальний обсяг роботи складає 82 сторінки комп'ютерного тексту, у тому числі: 38 рисунків, список використаних джерел вміщує 26 найменувань.

1. ПРИНЦИПИ ОРГАНІЗАЦІЇ ТА ВИКОРИСТАННЯ МЕРЕЖ З ПАКЕТНОЮ КОМУТАЦІЄЮ

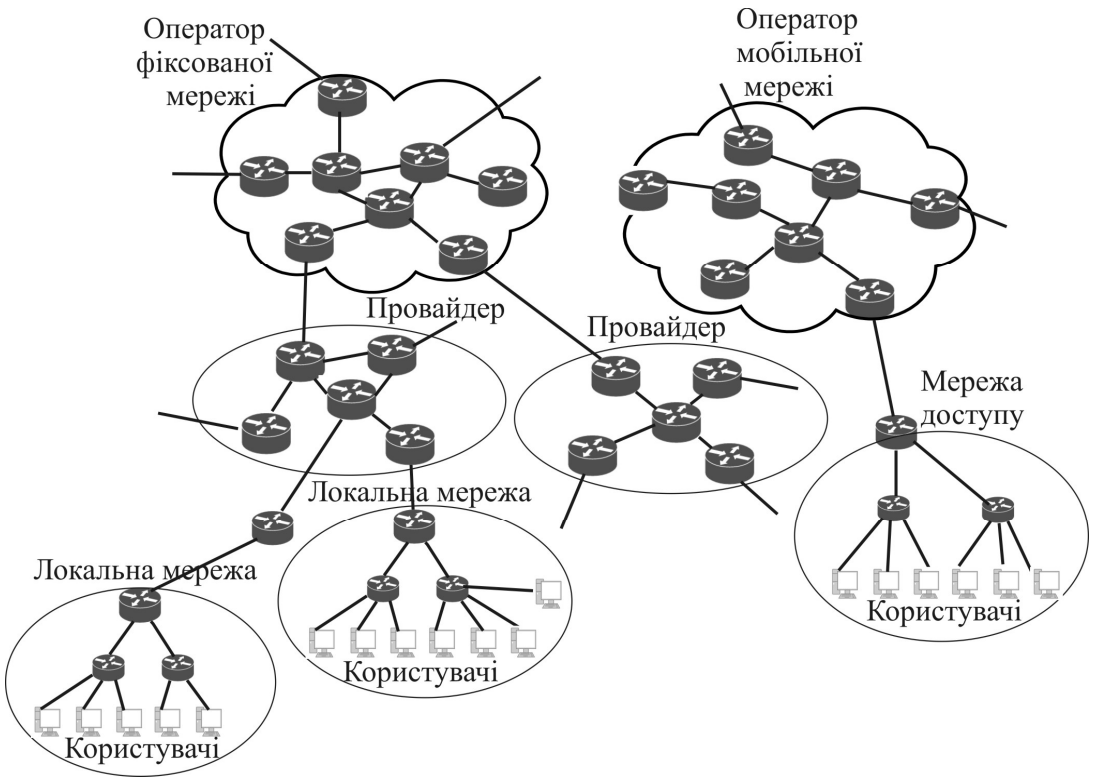


Рисунок 4.1 – Структура глобальної мережі Інтернет

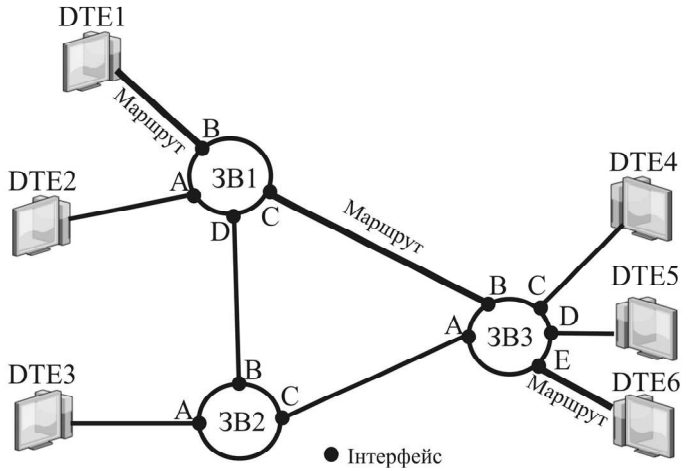


Рисунок 4.2 – Мережа передачі повідомлень

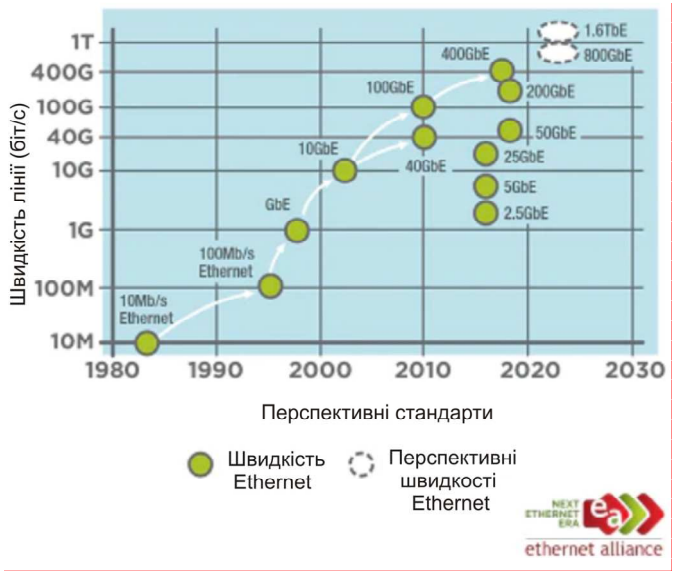
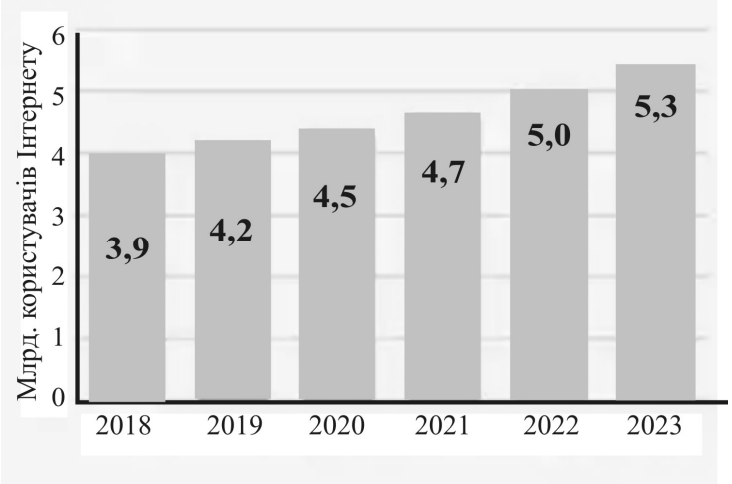


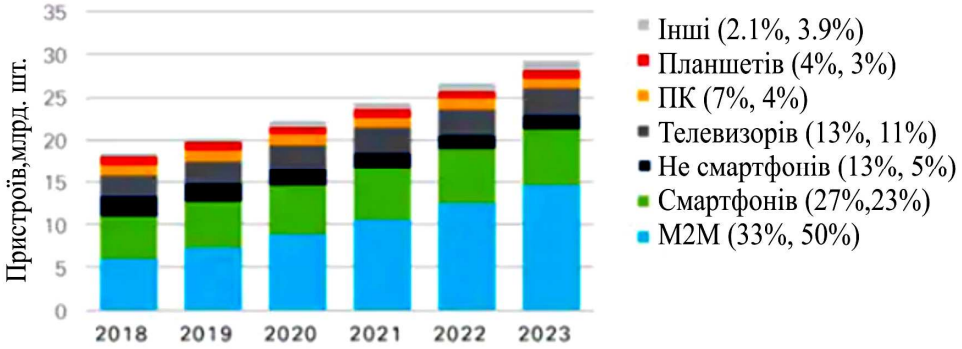
Рисунок 4.3 – Перспективні швидкості Ethernet, що заплановані Ethernet Alliance до 2030 року

2 АНАЛІЗ СУЧАСНОГО ТРАФІКУ ГЛОБАЛЬНОЇ МЕРЕЖІ



(Джерело: Річний звіт Cisco в Інтернеті, 2018-2023)

Рисунок 5.1 – Глобальний ріст користувачів Інтернету



(Джерело: Річний звіт Cisco в Інтернеті, 2018-2023)

Рисунок 5.2 – Глобальний ріст пристроїв та з'єднань

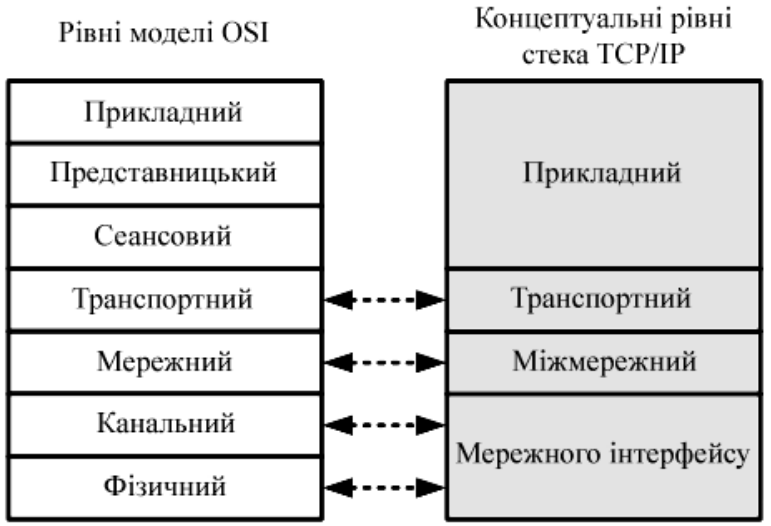


Рисунок 5.3 - Співвідношення чотирирівневої архітектури протоколів TCP / IP і семирівневої архітектури OSI

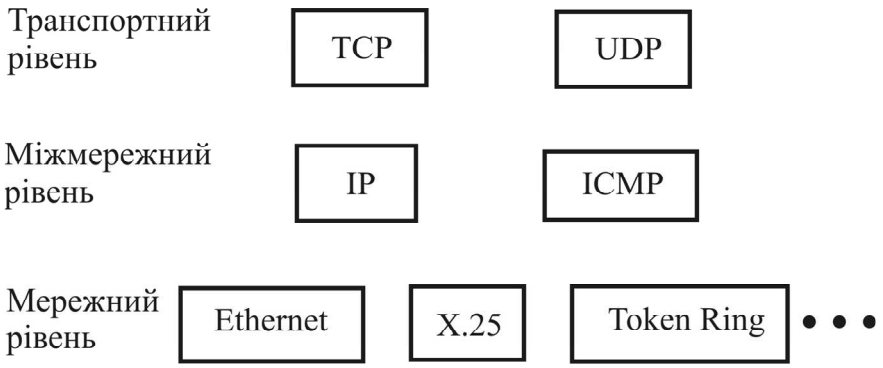


Рисунок 5.4 - Архітектура основних протоколів TCP / IP, які використовуються на трьох нижніх рівнях стеку

3 РЕЖИМИ КОМУТАЦІЇ ПАКЕТІВ

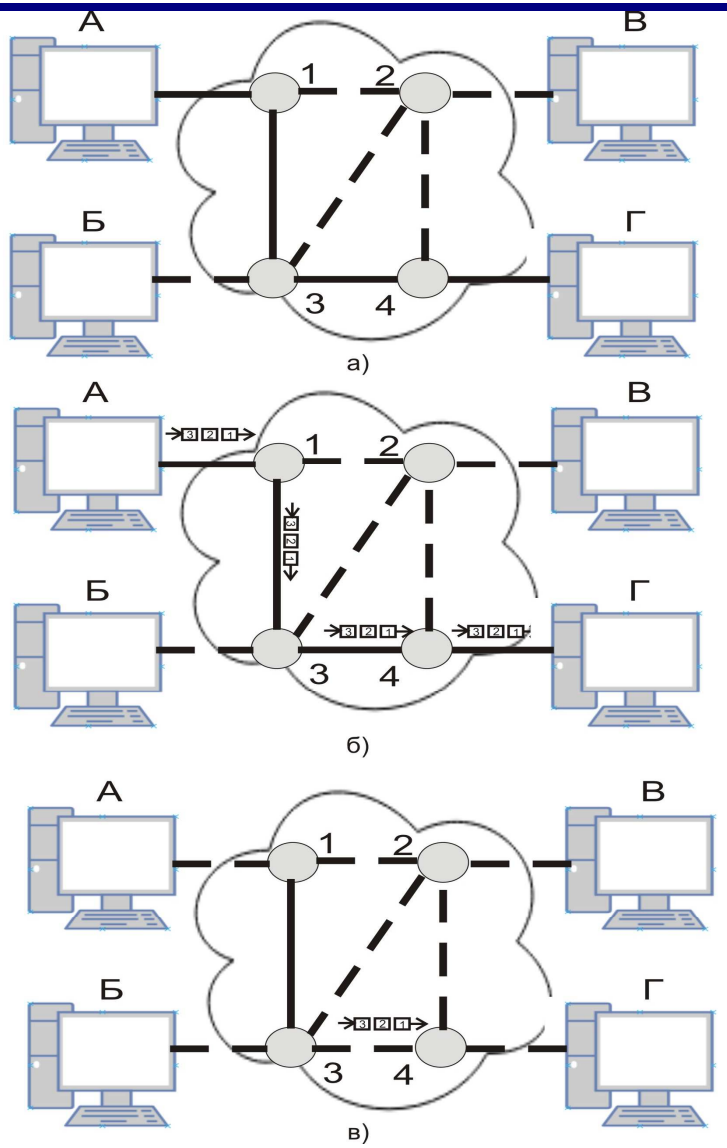


Рисунок 6.1 – Три фази комутації: налаштування (а), передача даних (б) та фаза зриву (в)

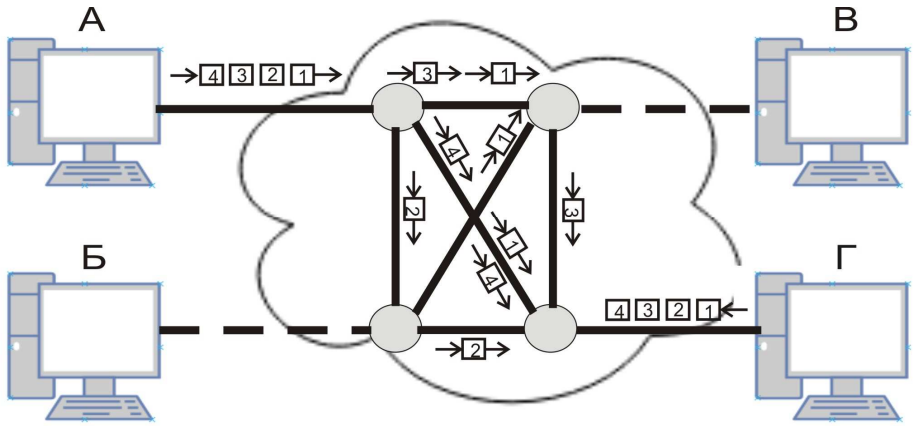


Рисунок 6.2 – Комутація пакетів без підключення (дейтаграма)

Існують чотири типи затримок при комутації пакетів: затримка передачі; затримка поширення; затримка черги та затримка обробки

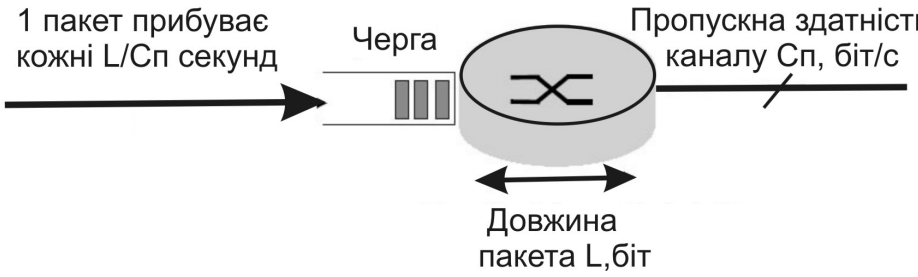
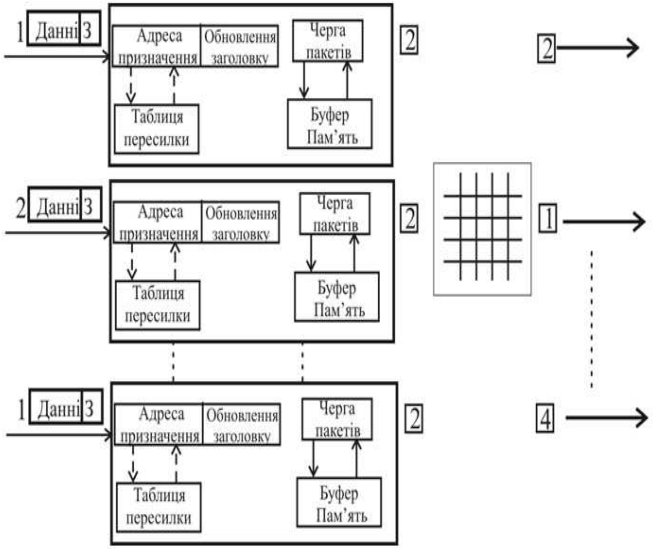
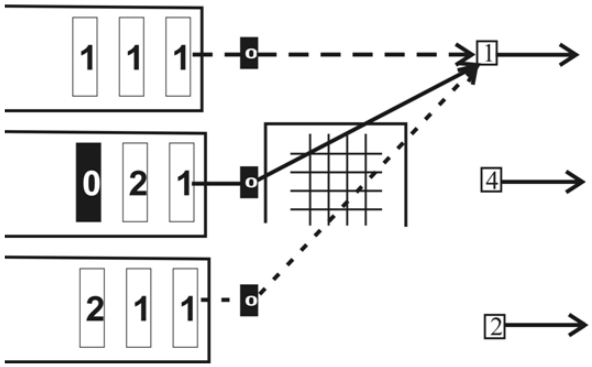


Рисунок 6.3 – Затримка черги на комутаторі

4 Типи пакетних комутаторів



а)



б)

Рисунок 7.1 – Комутатори з буферизацією на вході: пакетний комутатор (а); схема блокувань (б)

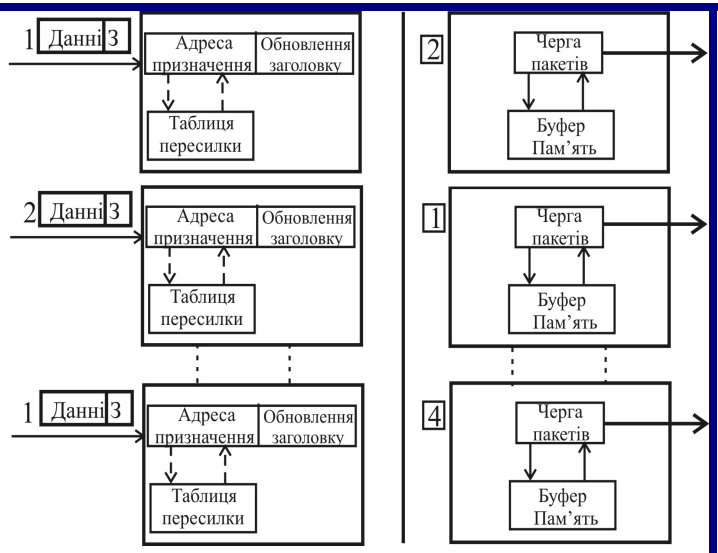


Рисунок 7.2 – КМ з буферизацією на виході та поділюваною пам'яттю

Висновок: комутатори (КМ) поділяються на: 1. **КМ з буферизацією на вході**, що мають низьку пропускну здатність завдяки блокування на входах та не вимагають високих швидкостей роботи та обсягу черги; 2. **КМ з буферизацією на виході та поділюваною пам'яттю**, які працюють з мінімальними втратами пакетів, максимальною пропускною здатністю та з мінімальними затримками на очікування обслуговування, але вимагають високих швидкостей роботи та ємностей.

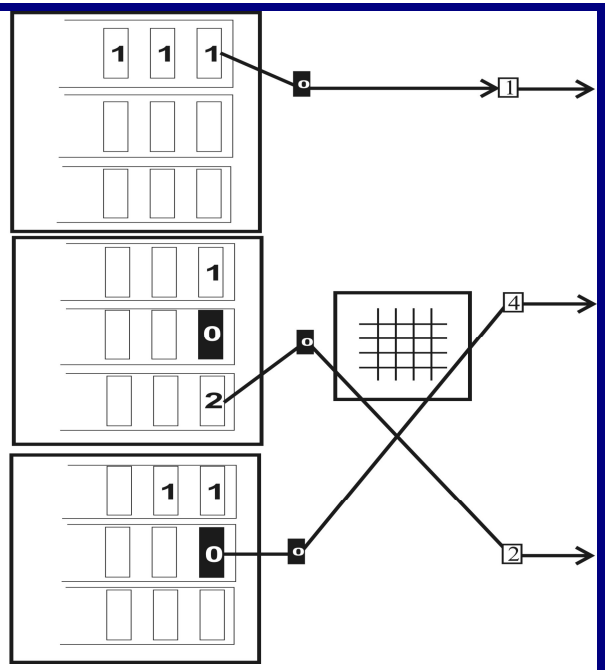


Рисунок 7.3 – Комутатори з буферизацією на вході з чергами віртуальних виходів

3. **Високошвидкісні комутатори використовують буферизацію на вході з чергами віртуальних виходів**, це дозволяє значно збільшити пропускну здатність пристрою.

Такі комутатори рекомендовано використовувати для обслуговування екстрених служб масового обслуговування і т. інш.

5.1 МЕТОД РОЗРАХУНКУ ПРОПУСКНОЇ ЗДАТНОСТІ МЕРЕЖІ VOIP ТЕЛЕФОНІЇ

МОДЕЛЬ ПУАССОНА

Середня інтенсивність навантаження від одного абонента:

$$y = \bar{c} \cdot \bar{t} \text{ Ерл.} \qquad (8.1)$$

Інтенсивність заявленого навантаження розраховується за формулою:

$$Y = N \cdot \bar{c} \cdot \bar{t}. \qquad (8.2)$$

Для обчислення моделі трафіку Пуассона використовується наступний вираз:

$$p_k(Y) = \frac{(Y)^k}{k!} e^{-Y}, \qquad (8.3)$$

де, $p_k(Y)$ – імовірність надходження k викликів, Y=203,6 Ерл. – інтенсивність трафіку (розрахована для наступних змінних: кількість абонентів VoIP – телефонії в офісі провайдера –749 чол.; середня кількість викликів, які ініціює один абонент офісу – 3,4 викликів за годину).

Лістинг програми для розрахунку розподілу Пуассона наведений нижче:

```
function mass = PoissonV(Y, N_Abon)
CurP = exp(-Y);
mass = [];
for k=1:N_Abon
   CurP = CurP*Y/k;
   mass(k) = CurP;
end
return
```

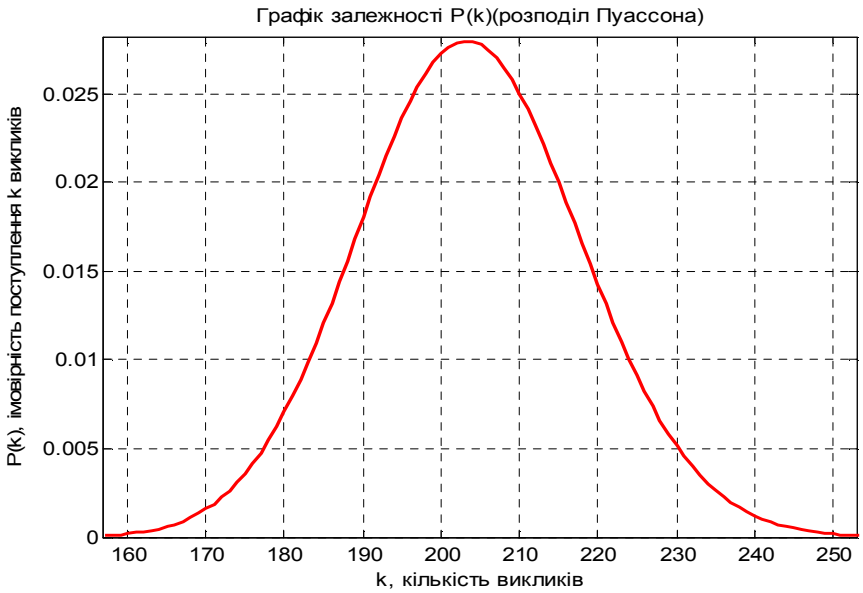


Рисунок 8.1 – Графік залежності $p_k(Y)$ від кількості викликів

5.2 МОДЕЛЬ ТРАФІКУ ЕРЛАНГ В

Модель трафіку Ерланг В використовується, при заблокованих викликах та перенапрямлених без повернення до вихідної групи магістральних каналів. Ця модель передбачає випадкове надходження викликів.

$$E_v(Y) = \frac{Y^v / v!}{\sum_{i=1}^{v} Y^i / i!}, \qquad (9.1)$$

де $E\nu(Y)$ – ймовірність блокування викликів; ν – кількість каналів; Y – інтенсивність трафіку.

Представимо формулу Ерланга як:

$$E_1(Y) = \frac{F_1(Y)}{S_1(Y)} = \frac{Y}{Y} = 1 \qquad (9.2)$$

Висновок. За результатами моделювання (рисунок 9.1) видно, що з ймовірністю блокування 0,024, необхідна кількість магістральних каналів для оброблення заданого навантаження трафіку дорівнює – 216 каналам.

При використанні такої кількості магістральних каналів та за умови використання голосового кодеку G.711 (загальна пропускна здатність кодеку G.711 - 107,2 Кбіт/с, максимальна пропускна здатність мережі сягає 23,155 Мбіт/с.

Розрахунки показали, що магістральна мережа спроектована якісно, має високу продуктивність та низький коефіцієнт блокування. За таких даних, якість обслуговування значно підвищується, а витрати зменшуються.

Лістинг програми наведений нижче:

```
function Ev_Y = ErlangV( Y, N_Abon )
% Розрахунок Ev(Y)
% N_Abon - максимальна кількість каналів
Fv_Y = 1;
Sv_Y = 1;
Ev_Y(1) = 1;
for v = 2:N_Abon
   Fv_Y = Fv_Y * Y / v;
   Sv_Y = Sv_Y + Fv_Y;
   Ev_Y(v) = Fv_Y / Sv_Y;
end
return
end
```

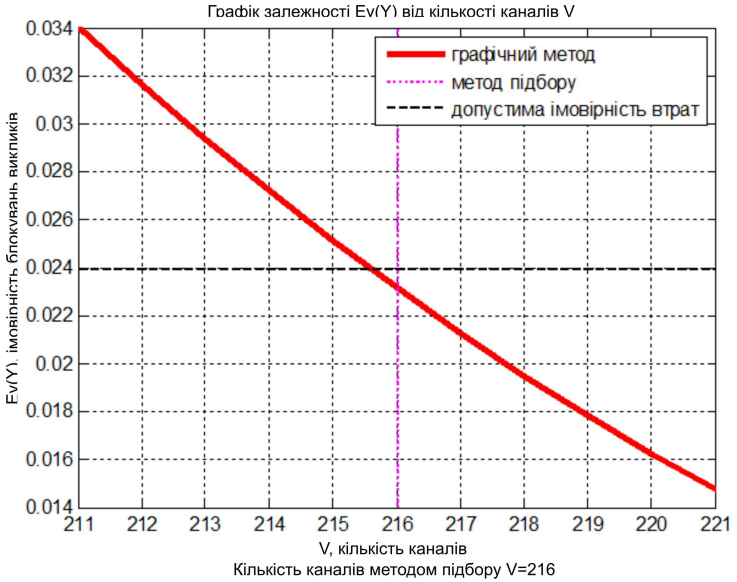


Рисунок 9.1 – Графік залежності Ev(Y) від кількості каналів

5.3 МОДЕЛЬ ВИПАДКОВОГО НАДХОДЖЕННЯ ТРАФІКУ ЕРЛАНГ С

Модель Ерланг С застосовується при наявності необмеженої кількості джерел і затриманих заблокованих викликів та побудована на теорії черг.

Передбачає випадкове надходження викликів, при цьому, абонент здійснює один виклик і утримується в черзі до відповіді на виклик.

Використовується при проектуванні сталого пристрою автоматичного розподілу викликів (ACD), щоб визначити необхідну кількість агентів.

Для обчислення моделі трафіку Ерланг С використовується наступна формула:

$$D_v(Y) = \frac{E_v(Y)}{1 - \frac{Y}{v}(1 - E_v(Y))}, \qquad (10.1)$$

де $E_v(Y)$ – кількість каналів, що визначаються за формулою Ерланг В.

Висновок: З рисунку 10.1 видно, що для забезпечення необхідних параметрів моделі трафіку з очікуванням обслуговування потрібно 234 канали. При використанні такої кількості магістральних каналів та за умови використання голосового кодеку G.711 (загальна пропускна здатність кодеку G.711 - 107,2 Кбіт/с), максимальна пропускна здатність мережі сягає 25,084 Мбіт/с, що значно вище чим при використанні моделі з блокуванням (модель Ерланг В).

```
function Dv_Y = Erlang2V(Y, N_Abon)
% Розрахунок Dv(Y)
% N_Abon - максимальна кількість каналів
Fv_Y = 1;
Sv_Y = 1;
Dv_Y(1) = 1;
for v = 2:N_Abon
   Fv_Y = Fv_Y * Y / v;
   Sv_Y = Sv_Y + Fv_Y;
   Ev_Y = Fv_Y / Sv_Y;
   Dv_Y(v) = Ev_Y/(1-Y*(1-Ev_Y)/v);
end
return
end
```

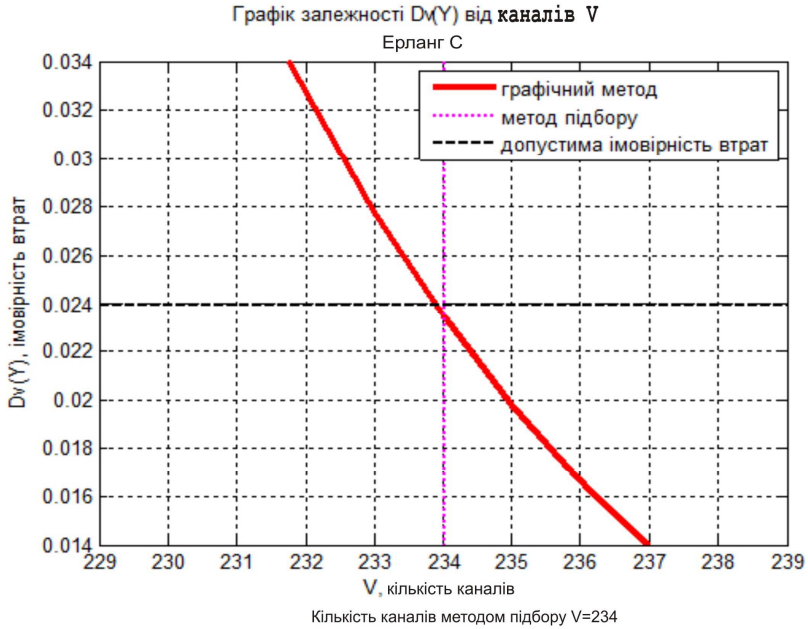


Рисунок 10.1 – Графік залежності $D_v(Y)$ від кількості каналів

7.1 МОНІТОРИНГ ТРАФІКУ МЕРЕЖ З ПАКЕТНОЮ КОМУТАЦІЄЮ З ВИКОРИСТАННЯМ УТИЛІТИ PING

```
C:\Users\User>ping www.afrinic.net

Обмен пакетами с www.afrinic.net [196.216.2.6] с 32 байтами данных:
Ответ от 196.216.2.6: число байт=32 время=214мс TTL=49
Ответ от 196.216.2.6: число байт=32 время=213мс TTL=49
Ответ от 196.216.2.6: число байт=32 время=213мс TTL=49
Ответ от 196.216.2.6: число байт=32 время=214мс TTL=49

Статистика Ping для 196.216.2.6:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 213мсек, Максимальное = 214 мсек, Среднее = 213 мсек
```

Рисунок 11.1 – Виконання команди ping на хост RIR з IP адресою 196.216.2.6 розташованого в Африці (копія екрану)

```
C:\Users\User>ping www.apnic.net

Обмен пакетами с www.apnic.net.cdn.cloudflare.net [104.18.235.68] с 32 байтами данных:
Ответ от 104.18.235.68: число байт=32 время=32мс TTL=50
Ответ от 104.18.235.68: число байт=32 время=30мс TTL=50
Ответ от 104.18.235.68: число байт=32 время=33мс TTL=50
Ответ от 104.18.235.68: число байт=32 время=36мс TTL=50

Статистика Ping для 104.18.235.68:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 30мсек, Максимальное = 36 мсек, Среднее = 32 мсек
```

Рисунок 11.2 – Виконання команди ping на хост RIR з IP адресою 104.18.255.68 розташованого в Австралії (копія екрану)

```
C:\Users\User>ping www.ripe.net

Обмен пакетами с www.ripe.net [193.0.6.139] с 32 байтами данных:
Превышен интервал ожидания для запроса.
Ответ от 80.249.208.71: Заданная сеть недоступна.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.

Статистика Ping для 193.0.6.139:
    Пакетов: отправлено = 4, получено = 1, потеряно = 3
    (75% потерь)
```

Рисунок 11.3 – Виконання команди ping на хост RIR з IP адресою 193.0.6.139 розташованого в Європі (копія екрану)

```
C:\Users\User>ping www.lacnic.net

Обмен пакетами с www.lacnic.net [200.3.14.184] с 32 байтами данных:
Ответ от 200.3.14.184: число байт=32 время=240мс TTL=48
Ответ от 200.3.14.184: число байт=32 время=239мс TTL=48
Ответ от 200.3.14.184: число байт=32 время=237мс TTL=48
Ответ от 200.3.14.184: число байт=32 время=238мс TTL=48

Статистика Ping для 200.3.14.184:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 237мсек, Максимальное = 240 мсек, Среднее = 238 мсек
```

Рисунок 11.4 – Виконання команди ping на хост RIR з IP адресою 200.3.14.184 розташованого в Південній Америці (копія екрану)

7.2 МОНІТОРИНГ ТРАФІКУ МЕРЕЖ З ПАКЕТНОЮ КОМУТАЦІЄЮ ВИКОРИСТАННЯ УТИЛІТИ “TRACERT”

```
C:\Users\User>tracert www.cisco.com

Трассировка маршрута к e2867.dsca.akamaiedge.net [104.96.129.203]
с максимальным числом прыжков 30:

  1     2 ms     2 ms    11 ms  192.168.0.1
  2     4 ms     5 ms     6 ms  93-77-12-1.khm.volia.net [93.77.12.1]
  3     3 ms     4 ms     4 ms  km-5.cr-1.tvservice.km.ua [77.121.26.145]
  4     7 ms     4 ms     5 ms  v3325.cs-1.khm.volia.net [77.121.26.161]
  5     *       12 ms    13 ms  be7.966.cr-2.g50.kiev.volia.net [77.120.0.69]
  6    10 ms     9 ms     8 ms  be3.180.cr-1.g50.kiev.volia.net [77.120.1.41]
  7    13 ms    13 ms    12 ms  be6172.ccr22.kbp01.atlas.cogentco.com [149.6.190.25]
  8    28 ms    25 ms    24 ms  be2047.ccr22.bts01.atlas.cogentco.com [154.54.60.205]
  9    30 ms    25 ms    26 ms  be3463.ccr52.vie01.atlas.cogentco.com [154.54.59.185]
 10    28 ms    27 ms    30 ms  ae-14.r00.vienat02.at.bb.gin.ntt.net [129.250.9.129]
 11    27 ms    29 ms    31 ms  185.84.16.3
 12    28 ms    27 ms    27 ms  a104-96-129-203.deploy.static.akamaitechnologies.com [104.96.129.203]

Трассировка завершена.
```

Рисунок 12.1 – Виконання команди tracert www.cisco.com (копія з екрану)

```
C:\Users\User>tracert www.afrinic.net

Трассировка маршрута к www.afrinic.net [196.216.2.6]
с максимальным числом прыжков 30:

  1     1 ms     1 ms     1 ms  192.168.0.1
  2     6 ms     4 ms     5 ms  93-77-12-1.khm.volia.net [93.77.12.1]
  3     6 ms     6 ms     4 ms  km-5.cr-1.tvservice.km.ua [77.121.26.145]
  4     6 ms     7 ms     5 ms  v3325.cs-1.khm.volia.net [77.121.26.161]
  5    12 ms    12 ms    14 ms  be7.966.cr-2.g50.kiev.volia.net [77.120.0.69]
  6    13 ms    12 ms    12 ms  ae20.RT.NTL.KIV.UA.retn.net [87.245.237.56]
  7    39 ms    40 ms    38 ms  ae4-2.RT.EQX.FKT.DE.retn.net [87.245.233.164]
  8    41 ms    37 ms    38 ms  ipv4.de-cix.fra.de.as37271.workonline.africa [80.81.195.27]
  9   211 ms   212 ms   212 ms  cr1-fxn-agr1-te0-2.wolcomm.net [197.157.77.48]
 10     *        *        *     Превышен интервал ожидания для запроса.
 11     *        *        *     Превышен интервал ожидания для запроса.
 12   215 ms   215 ms   218 ms  esr1-isd-cr2-te0-0-27.wolcomm.net [197.157.77.101]
 13   210 ms   209 ms   215 ms  197.157.64.195
 14   214 ms   214 ms   211 ms  www.afrinic.net [196.216.2.6]

Трассировка завершена.
```

Рисунок 12.2 – Виконання команди tracert на хост www.afrinic.net (копія екрану)

```
C:\Users\User>tracert www.lacnic.net

Трассировка маршрута к www.lacnic.net [200.3.14.184]
с максимальным числом прыжков 30:

  1     2 ms     1 ms     1 ms  192.168.0.1
  2    12 ms     4 ms     5 ms  93-77-12-1.khm.volia.net [93.77.12.1]
  3     3 ms     6 ms     3 ms  km-5.cr-1.tvservice.km.ua [77.121.26.145]
  4     5 ms     4 ms     8 ms  v3325.cs-1.khm.volia.net [77.121.26.161]
  5    14 ms    13 ms    11 ms  be7.966.cr-2.g50.kiev.volia.net [77.120.0.69]
  6    16 ms    10 ms    14 ms  ae20.RT.NTL.KIV.UA.retn.net [87.245.237.56]
  7     *       43 ms    43 ms  ae8-10.RT.IRX.FKT.DE.retn.net [87.245.232.139]
  8    45 ms    44 ms    43 ms  ae17.cr6-fra2.ip4.gtt.net [154.14.40.233]
  9   150 ms   188 ms   149 ms  et-0-0-17.cr6-mia1.ip4.gtt.net [213.200.113.142]
 10   157 ms   150 ms   151 ms  ip4.gtt.net [98.124.189.122]
 11   259 ms   254 ms   254 ms  et-14-0-4-0.monet.ptx-b.spo-piaf.algartelecom.com.br [168.197.23.14
 12   254 ms   253 ms   254 ms  100.127.5.114
 13   255 ms   255 ms   259 ms  201-048-035-089.static.ctbctelecom.com.br [201.48.35.89]
 14   238 ms   237 ms   244 ms  xe-4-2-1-0.core1.nu.registro.br [200.160.0.180]
 15   239 ms   237 ms   238 ms  xe-0-0-0.ar3.nu.registro.br [200.160.0.249]
 16   244 ms   241 ms   240 ms  ae0-0.gw1.jd.lacnic.net [200.160.0.212]
 17   238 ms   241 ms   239 ms  200.3.12.34
 18   239 ms   235 ms   241 ms  www.lacnic.net [200.3.14.184]

Трассировка завершена.
```

Рисунок 12.3 – Виконання команди tracert на хост www.lacnic.net (копія екрану)

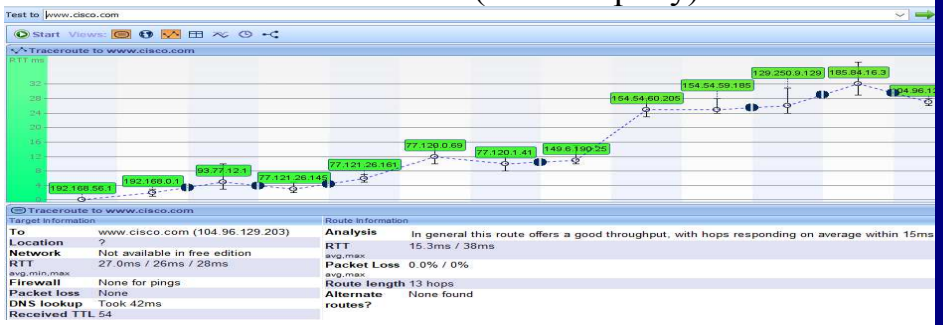


Рисунок 12.4 – Трасування маршрутів за адресом www.cisco.com за допомогою програмного забезпечення Visual Route

Висновок: З рисунку 12.4 видно, що отриманий час RTT (передачі пакетів) від передавача з IP адресою 192.168.56.1 до отримувача (приймача) з IP адресою 104.96.129.203 становив 38 мс (максимальне значення) та 15,3 мс (середнє значення).

АНАЛІЗ ПАРАМЕТРІВ ТРАФІКУ ЗА ДОПОМОГОЮ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ WIRESHARK

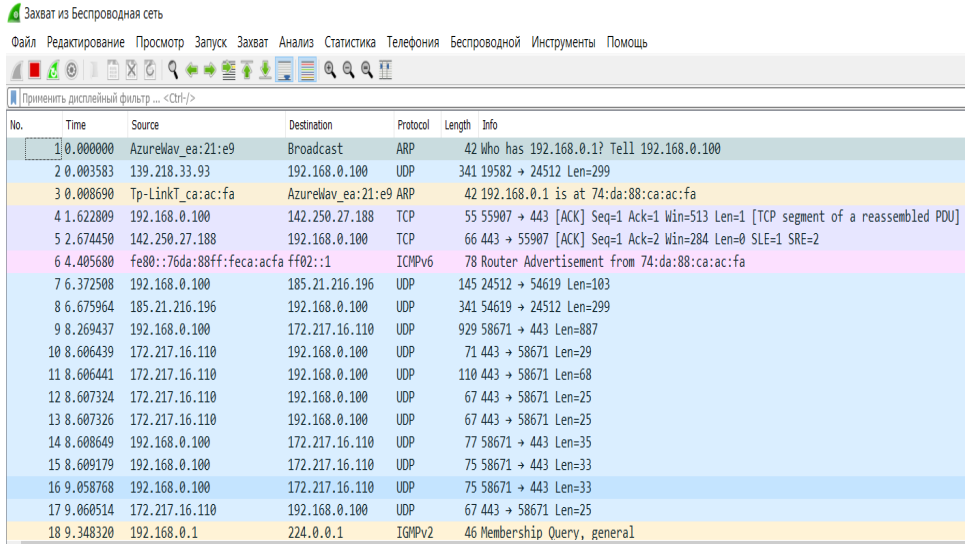


Рисунок 13.1 – Результат реєстрації потоку пакетів на інтерфейсі Ethernet

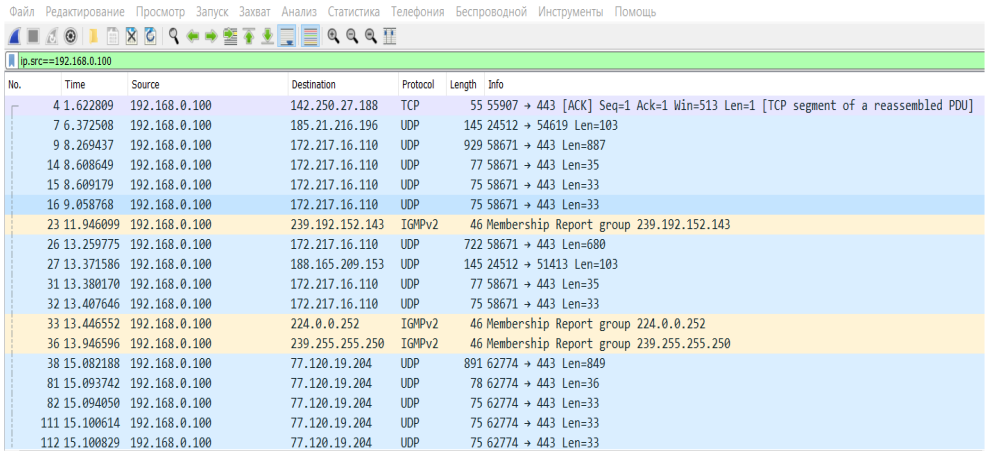
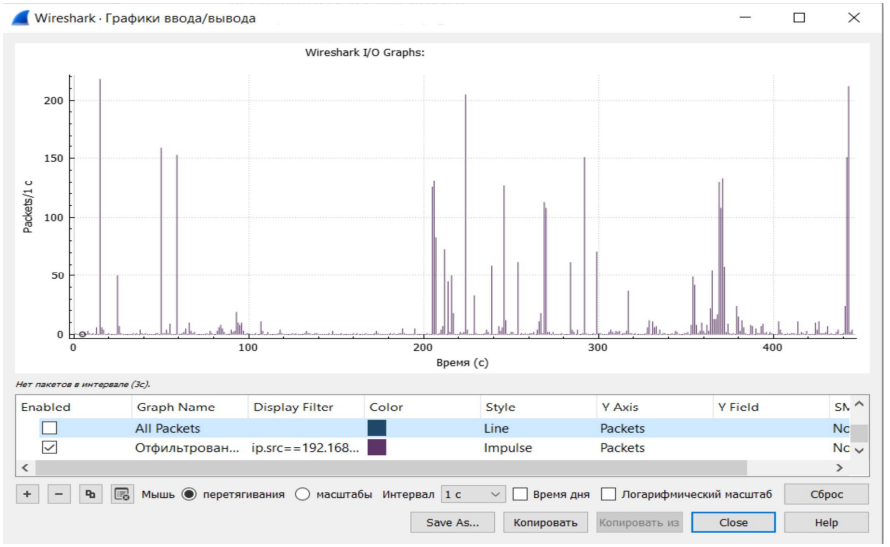


Рисунок 13.1 – Фільтрація потоку відеотрафіку



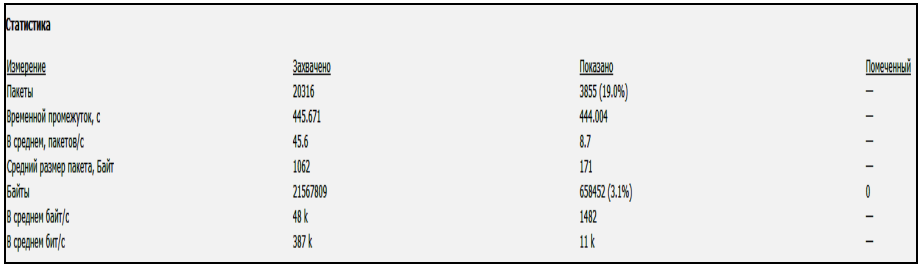


Рисунок 13.3- Графік розподілу відеотрафіку

Висновок. Згідно з отриманими статистичними даними (рисунок 13.3) визначаємо наступні характеристики відеотрафіку: $\lambda = 8,7$ пакета / с – інтенсивність пакетів; L=171 байти – середній розмір пакета, число пакетів - 3855 шт., а=11 Кбіт/ с – інтенсивність відеотрафіку / с за часовий діапазон – 444,004 с.

ВИСНОВКИ

1. Розглянуто принципи організації глобальної мережі, описана структура та протоколи мережі з пакетною комутацією повідомлень. Проведений аналіз комутованих технологій показав, що існує декілька технологій мереж - X.25, Frame Relay, ATM, Ethernet, що забезпечують задану якість сервісу та надають конвергентні послуги мережі. Показано, що найбільш перспективною технологією є Ethernet, який пропонує масштабованість 10/100/1000/10000 Мбіт/с, завдяки використання одного формату Ethernet кадру у всіх його модифікаціях, це дозволяє безперешкодно інтегрувати LAN, MAN та WAN та будувати високошвидкісні мережі з високою пропускною здатністю.

2. Виявлено, що швидкість широкосмугового зв'язку є вирішальним фактором, що сприяє IP - трафіку, яка, в свою чергу, залежить від пропускної здатності телекомунікаційної мережі.

3. Проведений аналіз сучасного трафіку глобальної мережі, який показав, що за прогнозами, кількість користувачів Інтернету до 2023 року сягне 5,3 мільярди, що складе 66 відсотків світового населення. Це вимагає удосконалення методів проведення оцінки необхідної пропускної здатності IP мережі.

4. Розглянуто стек протоколів TCP / IP, та представлена його архітектура. Показано, що основою усієї архітектури є міжмережний протокол IP за допомогою якого реалізується адресація вузлів мережі і доставка даних та транспортний протокол управління передачею TCP.

5. Розглянуто принципи комутації пакетів, описані основні режими комутації пакетів: віртуальних з'єднань та дейтаграмний режим, перевагою якого є можливість використання динамічної маршрутизації при передачі пакетів між абонентськими вузлами.

6. Розраховані типові затримки, що виникають при комутації пакетів. Розрахунки показали, що затримка передачі для кожного пакета зменшується при збільшенні кількості пакетів (з 1,1 мс при N = 1 шт. до 0,45 мс при N = 20 шт.). Існує граничне значення, при якому загальний витрачений час на початку зменшується (N = 1 шт., $t_{заг.}$=3,3 мс; N = 5 шт. $t_{заг.}$=2,1 мс). При збільшенні кількості пакетів після цього обмеження, загальний час починає збільшуватися (N = 10 шт., $t_{заг.}$= 2,4 мс; N = 20 шт., $t_{заг.}$= 3,3 мс). Якщо кількість пакетів дуже велика, то це займає набагато більше часу, ніж час, необхідний для передачі одного пакета.

7. Розглянуті основні положення теорії масового обслуговування, Показано, що при визначені пропускної здатності мережі необхідно враховувати параметри трафіку під час найбільшого навантаження. Описані механізми керування обслуговуванням черг. Показано, що при використанні механізму пріоритетного обслуговування черг в мережах голосової телефонії, забезпечується мінімізація впливу VoIP трафіку на інші, нижчі класи різного трафіку, що передається. Надані рекомендації для використання високошвидкісних комутаторів, які використовують буферизацію на вході з чергами віртуальних виходів для збільшення пропускної здатності мережі.

8. Наведений метод розрахунку пропускної здатності мережі VoIP телефонії з використанням моделей трафіку систем масового обслуговування (СМО) таких як: СМО з утриманням заблокованих викликів (розподіл Пуассона); СМО з заблокованими викликами, що перенапрямлені (модель трафіку Ерланг B); СМО з затриманими заблокованими викликами, що побудовані на теорії черг (модель трафіку Ерланг C), використання якого надає можливість проектувати трафік інтернет мереж, вирішувати проблеми якості зв'язку, визначити рівень обслуговування та коефіцієнт блокування мереж. Мережа, спроектована з використанням даного методу, має низький коефіцієнт блокування і високий рівень використання каналу.

9. За допомогою активних засобів моніторингу трафіку зроблено оцінку часу на прийом–передачу пакетів мережею Інтернет за допомогою спеціальних утиліт ping та tracert та програмного забезпечення, що призначене для діагностики мереж Інтернет: Visual Route Lite Edition та Wireshark. Побудований маршрут до місця призначення. Показано, що у кожного провайдера є безліч маршрутизаторів POP. Виконано трасування маршруту до віддалених серверів розташованих в різних частинах світу, визначений максимальний та мінімальний час передачі пакетів – RTT, при різній кількості скачків. Проведений аналіз параметрів трафіку потокового відео та визначенні його характеристики. Експериментальним шляхом отримані оцінки параметрів трафіку, що співпали з аналітичними розрахунками.

ДЯКУЮ ЗА УВАГУ!

Додаток Б

Тези доповіді на конференції

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Хмельницький національний університет

Військовий інститут Київського національного університету ім.Тараса Шевченка

ПВНЗ “Університет економіки і підприємництва”

Вінницький національний технічний університет

Західноукраїнський національний університет

Інтелектуальний потенціал - 2020

збірник наукових праць молодих науковців і студентів

сформовано за матеріалами
Всеукраїнської науково-практичної конференції
молодих науковців і студентів
«Інтелектуальний потенціал – 2020»

9-10 листопада 2020 р.

Частина 1

Хмельницький
2020

ББК 74.480.278
С.88

«Інтелектуальний потенціал – 2020» - збірник наукових праць молодих науковців і студентів / Колектив авторів – Хмельницький: ПВНЗ УЕП, 2020. – Частина 1. – 104 с.

ЗМІСТ

алгоритму адаптивної швидкості передачі даних (adaptive data rate, ADR) та використання технологій з розширенням спектру. За таким алгоритмом дані, які передаються від різних кінцевих вузлів з різними швидкостями не заважають один одному і створюють різні віртуальні канали, що збільшує пропускну здатність шлюзу. Максимальна швидкість передачі даних в мережах LoRaWAN дорівнює 50 Кбіт/с.

4. Віддалений комп'ютер, який може контролювати дії кінцевих вузлів або збирати дані з них.

5. Віддалений сервер (клієнтський додаток), що призначений для розшифрування переданої інформації. При цьому, кожен кінцевий пристрій має вбудований ідентифікатор за яким сервер додатків розпізнає приналежність кожного пакету даних певному IoT пристрою мережі.

Мережі LoRaWAN побудовані за фізичною топологією зірка, де кінцеві вузли LoRa через шлюзи утворюють прозорі мости для ретрансляції повідомлень та спілкуються з центральним сервером мережі. Зазвичай передбачається, що шлюзами і серверами володіє оператор LoRa мережі, а абоненти підключають свої модеми, по аналогії зі стільниковим зв'язком.

На сьогодні національним оператором lifecell сумісно з компанією IoT Ukraine планується національне покриття мережами LoRaWAN всієї території Україні, яка зможе обслуговувати до 7-10 млн. підключених до неї кінцевих пристроїв [4].

Перелік посилань

1. DataArt IoT trends and predictions for 2019: IoT goes mainstream. – Назва з екрану. – [Електроний ресурс]. – Режим доступу: http://surl.li/gkvb

2. What is LoRaWAN. – Назва з екрану. – [Електроний ресурс]. – Режим доступу: https://lora-alliance.org/resource-hub/what-lorawanr

3. Mehmet Ali Ertürk. A Survey on LoRaWAN Architecture, Protocol and Technologies / Mehmet Ali Ertürk, Muhammed Ali Aydın, Muhammet Talha Büyükakka and Hayrettin Evirgen //MDPI. – Future internet, 2019, no.11. – P. 34.

4. Тимур Ягофароф. Национальное LoRaWAN-покрытие появится к 2020 г. Назва з екрану. – [Електроний ресурс]. – Режим доступу: http://surl.li/gkvq

Пропускна здатність мережі голосової IP- телефонії

Кубатий Н. О.
Науковий керівник – к.т.н., доц. Таранчук А.А.
Хмельницький національний університет

Телекомунікаційні мережі для передачі голосу через Інтернет (англ. Voice over Internet Protocol, або іншими словами – VoIP телефонія)

створюються з урахуванням безлічі різних змінних. Якість зв'язку і витрати на розгортання мережі з пакетною комутацією – це два найбільш важливих фактори, які необхідно враховувати при проектуванні мережі. При цьому, такий параметр, як якість зв'язку вважається найбільш важливим для задоволення клієнта, а витрати завжди впливають на отриманий прибуток провайдером мережі [1].

При проектуванні і налагодженні мереж VoIP телефонії, які є чутливими до трафіку використовують кілька різних моделей трафіку, які необхідно правильно обирати та використовувати. Існуючи моделі теорії масового обслуговування дозволяють проектувальникам мереж робити припущення про роботу мереж на основі минулого досвіду [1,2].

Аналіз трафіку VoIP мереж дає можливість визначити необхідну пропускну здатність (продуктивність) мережі. Поняття трафіку включає відношення між спробами виклику обладнання, чутливого до трафіку, і швидкістю виконання цих викликів. Проектування трафіку направлено на вирішення проблем зв'язаними з визначенням таких параметрів якості зв'язку, як рівень обслуговування та коефіцієнт блокування. Зазвичай, для визначення навантаження, обирається період часу найбільшого навантаження на мережу, який характеризується максимальною інтенсивністю трафіку, який здатна витримати мережа. Результатом є величина інтенсивності трафіку, яка називається трафіком в час найбільшого навантаження (ТЧНН) [2].

Для аналізу трафіку систем масового обслуговування (СМО) [2,3], які використовують необмежену кількість джерел, випадкове надходження трафіку на вхід комутаційної системи та утримання заблокованих викликів за експоненціальним розподіленим часом утримання, застосовують так звану модель Пуассона. В такій моделі заблоковані виклики утримуються, поки канал не стане доступним. За моделлю Пуассона абонент може зробити тільки одну спробу здійснити виклик, і заблоковані виклики втрачаються. Модель Пуассона зазвичай використовується для розрахунку окремих груп магістральних каналів груп з запасом.

Для обчислення моделі трафіку Пуассона використовується наступний вираз [4]:

$$p_k(Y) = \frac{(Y)^k}{k!} e^{-Y}, \qquad (1)$$

де $p_k(Y)$ – імовірність надходження k викликів, $Y=203,6$ Ерл. – інтенсивність трафіку (розрахована для наступних змінних: кількість абонентів VoIP – телефонії в офісі провайдера –749 чол.; середня кількість викликів, які ініціює один абонент офісу – 3,4 викликів за годину).

Модель трафіку, що розрахована за розподілом Пуассона (1), наведена на рисунку 1.

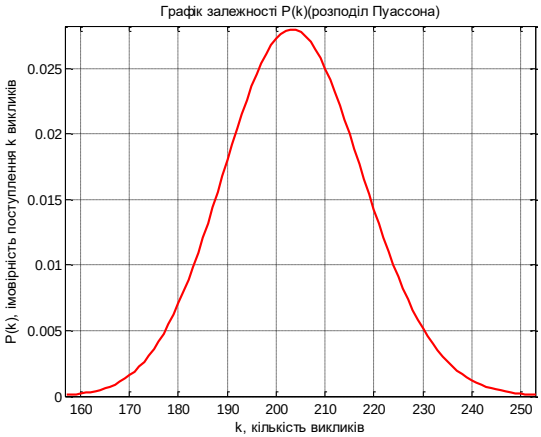


Рисунок 1 - Графік залежності $p_k(Y)$ від кількості викликів

Згідно розподілу Пуассона (рис.1) для обробки навантаження 203,6 Ерл. з ймовірністю блокування 2,4% СМО проектованої мережі може обслужити 216 викликів.

Модель трафіку Ерланг В використовується, при заблокованих викликах перенапрямлених без повернення до вихідної групи магістральних каналів. Ця модель передбачає випадкове надходження викликів. Абонент робить тільки одну спробу виклику. У випадку блокування цього виклику, він перенаправляється. Модель Ерланг В зазвичай використовується для розрахунку груп магістральних каналів з низьким коефіцієнт блокування, обслужених з першої спроби, без потреби врахування відсотку повторних викликів, тому що абоненти перенаправляються.

Для обчислення моделі трафіку Ерланг В використовується наступний вираз [3,4]:

$$E_v(Y) = \frac{Y^v / v!}{\sum_{i=1}^{v} Y^i / i!}, \qquad \textbf{(2)}$$

де $E_v(Y)$ - ймовірність блокування викликів; v - кількість каналів; Y - інтенсивність трафіку.

Використаємо модель трафіку Ерланг В для перепроектування вихідних груп магістральних каналів для міжміських викликів, які зараз блокуються під час години найбільшого навантаження. Врахуємо, що під час найбільшого навантаження на групу магістральних каналів надходить 203,6 Ерл. трафіку (рис.2). При розрахунках кількості каналів скористуємось методом підбору (2) та графічним методом [4].

При порівнянні між собою результатів, отриманих шляхом підбору за допомогою (2) і результатів отриманих графічним методом (рис. 2) можна зробити висновок, що отримана, за обома методами, необхідна кількість каналів однакова. За результатами моделювання (рис. 2) видно, що з ймовірністю блокування 0,024, необхідна кількість магістральних каналів для оброблення заданого навантаження трафіку дорівнює – 216 каналам.

Отже, програмна реалізація методу підбору в системі математичного моделювання Mathlab працює коректно.

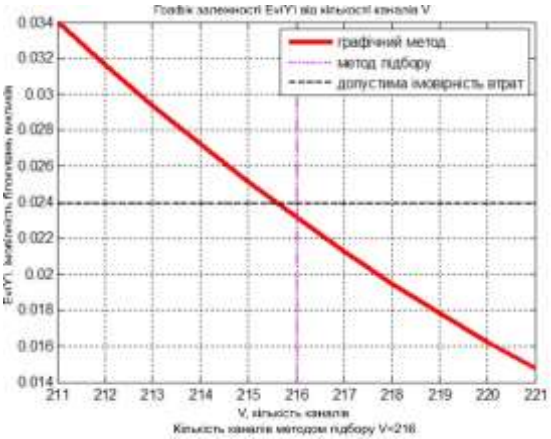


Рисунок 2 - Графік залежності Ev(Y) від кількості каналів

При використанні такої кількості магістральних каналів та за умови використання голосового кодека G.711 (загальна пропускна здатність кодека G.711 - 107,2 Кбіт/с [3, табл.4]), максимальна пропускна здатність мережі сягає 23,155 Мбіт/с.

Розрахунки показали, що магістральна мережа спроектована якісно, має високу продуктивність та низький коефіцієнт блокування. За таких даних, якість обслуговування значно підвищується, а витрати зменшуються.

Перелік посилань

1. Характеристики голосового трафика. – Назва з екрану. – [Електроний ресурс]. – Режим доступу: http://surl.li/gqpv.

2. Еременко, В.Т. Методы и модели теории телетрафика: учебное пособие / В.Т. Еременко [и др.]. – Орёл: ОГУ им. И.С. Тургенева, 2019. –244 с.

3. Ложковський А.Г. Теорія масового обслуговування в телекомунікаціях / А.Г. Ложковський. – Одеса: ОНАЗ ім. О.С. Попова, 2010. – 112 с.

4. Системи комутації – Назва з екрану. – [Електроний ресурс]. – Режим доступу: http://vnstele.com/system-komut.html.

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 1.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 9%**

ID: 82578 Название: Метод визначення пропускної здатності мереж з пакетною комутацією Добавлено в БД: 2020-12-06 Авторы: Кубатий Назар Олексійович Руководители: Таранчук Алла Анатоліївна Консультанты: Опоненты:	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
	88145	726	841 (1%)	11 (2%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

Имя пользователя:
Kafedra TMIT KhNU

ID проверки:
1005386795

Дата проверки:
07.12.2020 12:37:39 EET

Тип проверки:
Doc vs Internet + Library

Дата отчета:
07.12.2020 16:33:24 EET

ID пользователя:
100005657

Название файла: Кубатий_ТРм_19-1

Количество страниц: 76 Количество слов: 13775 Количество символов: 100753 Размер файла: 2.62 MB ID файла: 1005672064

101 слово помечено как "исключенное" и не учитывается в подсчете слов

Обнаружены модификации текста (могут влиять на процент совпадений)

8.2% Совпадения

Наибольшее совпадение: 1.72% с Интернет-источником (http://ni.biz.ua/8/8_3/8_34756_dlina-segmenta.html)

8.2% Источники из Интернета	78	Страница 78

Не найдены источники из Библиотеки

0% Цитат

Цитаты	1	Страница 79
Ссылки	1	Страница 79

0.02% Исключений

Некоторые источники исключены автоматически (фильтры исключения: количество найденных слов меньш...

Нет исключенных Интернет-источников

0.02% Исключенного текста из Библиотеки	10	Страница 79

Модификации

Обнаружены модификации текста. Подробная информация доступна в онлайн-отчете.

Замененные символы	24
Подозрительное форматирование	14 страниц

ВІДЗИВ

на дипломну роботу другого (магістерського) рівня студента групи ТРм-19-1
Кубатого Назара Олексійовича

«Метод визначення пропускної здатності мереж з пакетною комутацією»

При проектуванні мереж та їх адмініструванні, мережеві інженери та адміністратори потребують методів правильного визначення пропускної здатності проектованої мережі, або мережі, яка розширюється. Теорія масового обслуговування (МО) дає можливість проектувальникам мереж робити припущення про їх роботу на основі минулого досвіду та існуючих статистичних моделей. Тому дана дипломна робота, яка полягає в удосконаленні методу визначення пропускної здатності мереж пакетної комутації є актуальною.

Мета роботи полягає в удосконаленні методу визначення пропускної здатності мереж пакетної комутації.

Об'єктом дослідження є: процеси передачі трафіку в мережах з пакетною комутацією.

Предметом дослідження є: метод визначення пропускної здатності мереж з пакетною комутацією.

Для поставленої мети в дипломній роботі вирішений ряд задач, а саме:

1. Розглянуті принципи організації та використання мереж з пакетною комутацією.

2. Досліджені протоколи передачі даних та визначені основні характеристики мереж з комутацією пакетів.

3. Розрахована пропускна здатність мережі голосової IP – телефонії.

4. Проведений моніторинг трафіку мереж з пакетною комутацією.

За змістом робота є докладною та містить достатньо посилань на літературу. Викладення матеріалу є послідовним та логічно правильним.

Висновки мають достатнє обґрунтування та детальне пояснення. Мова викладення роботи є технічно грамотною, зрозумілою.

Дипломна робота представлена пояснювальною запискою обсягом 80 сторінок, складається з чотирьох основних розділів та 2-х додатків. Оформлення пояснювальної записки знаходиться на належному рівні.

Позитивними сторонами роботи є отримання наступного наукового результату:

1. Набув подальшого розвитку метод визначення здатності мережі VoIP телефонії з використанням моделей трафіку систем масового обслуговування (СМО), зокрема: СМО з утриманням заблокованих викликів на основі розподілу Пуассона; СМО з заблокованими викликами, що перенапрямлені на основі моделі Ерланга B; СМО з затриманими заблокованими викликами, що побудовані на основі моделі Ерланга C.

Серйозних недоліків робота не містить. Присутні незначні неточності, орфографічні та стилістичні помилки, які не впливають на суть роботи.

Вважаю, що дана робота відповідає загальним вимогам щодо дипломних робіт другого (магістерського) рівня, і заслуговує оцінки “добре”, а Кубатий Назар Олексійович – присвоєння кваліфікації магістра зі спеціальності 172 – “Телекомунікації та радіотехніка”.

Рецензент:
д.т.н., професор кафедри
телекомунікацій та радіотехніки Бойко Ю.М.

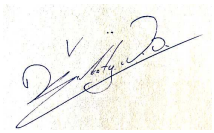
Завідувачу кафедри телекомунікацій
медійних та інтелектуальних технологій
д.т.н, доценту Підченко С.К.
здобувача вищої освіти
Кубатого Назара Олексійовича,
ФПКТС, 2 курс, ТРм-19-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

9.12.2020  Кубатий Н.О.

дата підпис

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ ПО КАФЕДРИ Телекомунікацій, медійних та інтелектуальних технологій (ТМІТ)

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: «Метод визначення пропускної здатності мереж з пакетною комутацією»

Автор: Кубатий Назар Олексійович

Спеціальність: 172 Телекомунікації та радіотехніка

Освітня програма: Телекомунікації та радіотехніка

Науковий керівник: Таранчук Алла Анатоліївна

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	**Відповідає**
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягненні. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Збіги (8,2%, найбільший збіг -1,72%), що виявленні в роботі не є плагіатом. Критичних запозичень немає. Усі поодинокі збіги відповідають назвам протоколів, стандартів з телекомунікацій, на які в роботі є посилання, а також частовживаним словосполученням.

Дипломна робота допускається до захисту.

9.12.2020 р.

Науковий керівник роботи
к.т.н., доц. Таранчук А.А.

Зав. каф. ТМІТ
д-р.т.н., доц. Підченко С.К.