Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет ___Комп'ютерна інженерія та управління_____
(повна назва)

Кафедра Автоматизації проектування обчислювальної техніки_____
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

_____другий (магістерський)_____
(рівень вищої освіти)

_____ГЮІК.4664ХХ.001 ПЗ_____
(позначення документа)

_____Реалізація системи допомоги прийняття рішення при_____
оцінюванні якості доставлення пакетів в мультисервісних мережах_____
(тема)

Виконав: студент 2 курсу, групи СКСм-17-1

_____Кулік І.С._____
(прізвище, ініціали)

Спеціальність *123 _ Комп'ютерна інженерія*

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

Освітня програма_____

*Спеціалізовані комп'ютерні системи*_____
(шифр і назва спеціальності, освітньої прграми)

Керівник _____Шкіль О.С._____
(прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ _Чумаченко С.В.__
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет_____Комп'ютерної інженерії та управління _____

Кафедра_____Автоматизації проектування обчислювальної техніки_____

Рівень вищої освіти____другий (магістерський)_____

Спеціальність_____123_Комп'ютерна інженерія _____
(шифр і назва)

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

Освітня програма _____Спеціалізовані комп'ютерні системи_____
(повна назва

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові___Куліку Ігорю Сергійовичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи (проекту)_Реалізація системи допомоги прийняття рішення при оцінюванні якості доставлення пакетів в мультисервісних мережах_____
Implementation of Decision Support System for Packages Delivery Quality Evaluation in Next-generation Networks_____
затверджена наказом по університету від "12"_листопада_ 2018 р. № _1626 Ст_____
2. Термін подання студентом роботи (проекту) ___10.06.20_____
3. Вихідні дані до роботи (проекту)_____
_Мультисервісна мережа для передачі трафіку реального часу_____
_Системи нечіткого логічного виводу на основі мереж Петрі_____
_Налаштування серверу IP-АТС Asterisk_____
_Аналізатор мережевих протоколів Wireshark_____
_____
_____
4. Зміст пояснювальної записки (перелік питань, що потрібно розробити) _____
1 Аналіз якості трафіка в мультисервісних мережах_____
2_Система підтримки прийняття рішення по забезпеченню якості передачі трафіка реального часу_____
3_Забезпечення якості мультисервісної мережі на базі протоколів RTP/RTCP
_____
_____

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслеників, плакатів)_____23 слайд_____
_____
_____
_____

6. Консультанти розділів роботи (проекту)

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

7. Дата видачі завдання ____30.03.2018_____

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи (проекту)	Термін виконання етапів проекту (роботи)	Примітка
1.	Видача теми роботи, її узгодження та затвердження	30.03.2018 − 5.04.2018	
2.	Аналіз проблемної області, постановка задачі, вибір засобів реалізації	06.04.2018 − 10.05.2018	
3.	Аналіз характеристик якості обслуговування та методів її підвищення	11.05.2018− 10.06.2018	
4.	Аналіз трафіка реального часу та протоколу його передачі RTP/RTCP. Розробка метода зменшення та концентрації службового трафіку	11.06.2018 − 15.07.2018	
5.	Розробка нечіткої моделі системи підтримки прийняття рішення	16.07.2018 − 15.09.2018	
6.	Моніторинг мережі за допомоги серверу Asterisk	16.09.2018 − 15.11.2018	
7.	Оформлення пояснювальної записки	16.11.2018 − 31.12.2018	
8.	Перевірка виконаного проекту, допуск до захисту	02.01.2019 − 15.01.2019	
9.	Захист роботи	15.01.2019 − 20.01.2019	

Студент _____
(підпис)

Керівник роботи (проекту) _____ доц. каф. АПОТ Шкіль О.С.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить: 127 сторінок, 59 рисунків, 8 таблиць, 37 джерел та 1 додаток.

МУЛЬТИСЕРВІСНА МЕРЕЖА, ПЕРЕДАЧА ДАНИХ, ТРАФІК РЕАЛЬНОГО ЧАСУ, ЯКІСТЬ ОБСЛУГОВУВАННЯ, RTP, RTCP.

Метою даної магістерської атестаційної роботи є розробка системи підтримки прийняття рішення при оцінці якості доставки пакетів в мультисервісній мережі шляхом концентрації службового трафіку (RTCP-пакетів) на одному діагностичному вузлі.

Розглядаються механізми процесів передачі даних в реальному масштабі часу, моделі зворотного зв'язку для протоколу RTCP, їх недоліки та переваги у вирішенні завдання зниження навантаження на мережу і збалансованості широкомовного RTP / RTCP трафіку. З метою концентрації службового трафіку використовується розширена модель зворотного зв'язку RTCP з введенням діагностичного вузла. Для оцінки якості доставки пакетів в МСМ запропонована система підтримки прийняття рішення, в основі якої лежить нечітка мережа Петрі. Отримані графіки демонструють адекватність побудованої моделі. Об'єктом дослідження є трафік реального часу, а предметом – підвищення якості передачі пакетів.

ABSTRACT

Certification diploma contains: 127 pages, 59 figures, 8 tables, 37 sources and 1 application.

MULTISERVICE NETWORKS, DATA TRANSMISSION, REAL-TIME TRAFFIC, QUALITY OF SERVICE, RTP, RTCP.

The aim of certification diploma is to develop a decision support system to assess the quality of packet delivery in a multiservice network by concentrating of the service traffic (RTCP-packets) on one diagnostic node.

Processes' mechanisms of data transfer in real time, feedback models for the RTCP protocol, their advantages and disadvantages in the task of reducing the network utilization and balancing of the broadcast RTP / RTCP traffic are considered. In order to concentrate the service traffic the expanded feedback model of RTCP which based on the diagnostic node is used. To assess the quality of packet delivery in MSN, a decision support system for quality assessment, which bases on fuzzy Petri net, is proposed. Obtained diagrams show the adequacy of the developed model. The object of research is the real-time traffic, and the subject – increasing the packet delivery quality.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

H.323 – Рекомендація ITU-T, яка визначає системи мультимедійного зв'язку в мережах з пакетною комутацією, що не забезпечують гарантовану якість обслуговування;

IP – Internet протокол;

IPDV – Варіація задержки IP-пакетів;

IREP – Частка спотворених IP-пакетів;

IPLR – Частка загублених IP-пакетів;

MCM – Мультисервісна мережа;

MPLS – Multi-Protocol Label Switching, багатопротокольна комутація по мітках;

NGN – Next generation network, мережа нового покоління;

QoS – Quality of services, якість обслуговування;

RTP – Real-Time Transport Protocol, протокол транспортування інформації в реальному часі;

RTCP – Real-Time Transport Control Protocol, протокол контролю транспортування інформації в реальному часі;

SIP – Session Initiation Protocol, протокол встановлення сеансу, протокол передачі даних, що описує спосіб встановлення і завершення користувацького інтернет-сеансу, що включає обмін мультимедійним вмістом (IP-телефонія, відео-та аудіоконференції, миттєві повідомлення, онлайн-ігри);

VoIP – Voice over Internet Protocol, технологія, що дозволяє використовувати MCM для передачі мовної інформації/

ВСТУП

Сучасна телекомунікаційна індустрія витрачає величезні кошти на розробку і підтримку мереж нового покоління (Next Generation Network, NGN), пакетних мереж, здатних надавати інфокомунікаційні послуги [1]. Технології NGN дозволяють інтегрувати всіх користувачів в єдину широкосмугову мережу, яка надає всі види сервісів − високошвидкісний доступ до Інтернету, телебачення, IP-телефонію, організацію офісних і будинкових мереж і різні мультимедійні сервіси (рис. В.1).

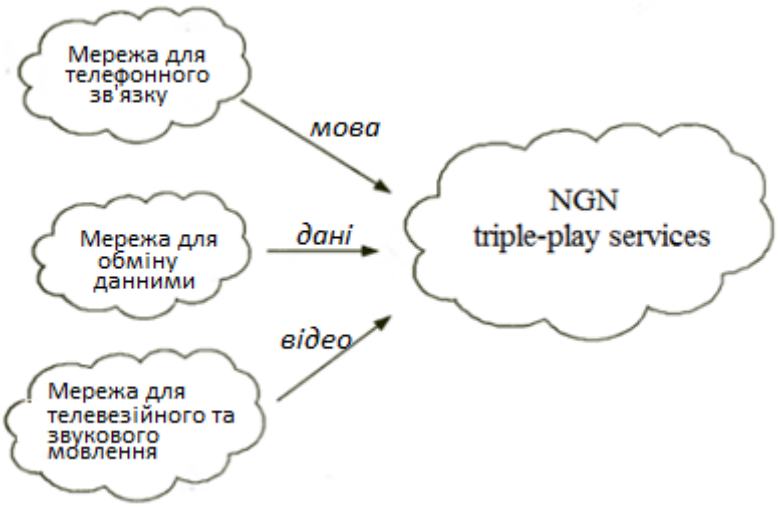


Рисунок В.1 – Концепція NGN як процес інтеграції мереж

Як видно з рисунку В.1 термін «triple-play services» вказує на здатність NGN мереж обслуговувати трафік мови, даних та відео.

В даний час для опису мережі нового покоління використовується термін «мультисервісна мережа» (МСМ), яка являє собою універсальну багатоцільову середу, призначену для передачі мови, зображення і даних з використанням технології комутації пакетів (IP) [2]. Мультисервісна мережа відрізняється ступенем надійності, характерної для телефонних мереж (на противагу негарантованої якості зв'язку через Інтернет) і забезпечує низьку

вартість передачі в розрахунку на одиницю об'єму інформації (наближену до вартості передачі даних по Інтернету).

Згідно з прогнозом Cisco [3], опублікованому в щорічному звіті «Наочний індекс розвитку мережевих технологій», в період з 2017 по 2022 рр. світовий IP-трафік потроїться (рис. В.2). Така популярність МСМ диктує необхідність забезпечення якості обслуговування (Quality of services, QoS), сукупності характеристик послуги електрозв'язку, які мають відношення до її можливості задовольняти встановлені і очікувані потреби користувача послуги [4].

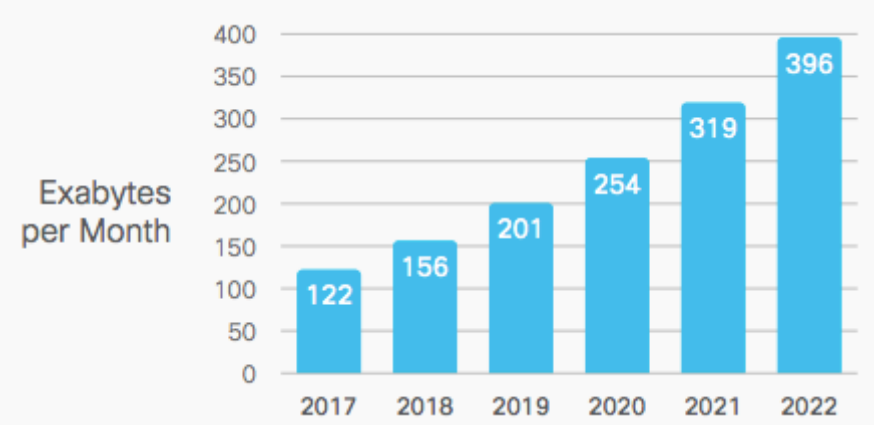


Рисунок В.2 – Зростання IP-трафіку в МСМ

На сьогоднішній день існує величезна кількість публікацій, присвячених питанням підвищення якості обслуговування в мультисервісних мережах зв'язку.

Так, наприклад, в статтях [5, 6] розглянуті моделі оцінки якості послуг в мережах наступного покоління з точки зору задоволеності споживачів. У статті [7] авторами запропонована методика забезпечення QoS в MPLS-мережах з використанням технологій балансування і прогнозування трафіку. У статті [8] розглянуті різні методи оцінки якості передачі мовних пакетів, які дозволяють правильно оцінити якість роботи мережі NGN. Авторами отримані тимчасові характеристики впливу затримки на якість мови, а також залежність останньої від втрати пакетів і типів використовуваних кодеків. У

статті [9] запропоновані оцінки навантаження службовим трафіком комп'ютерної мережі з урахуванням достатньої забезпеченості інформативності процесу моніторингу. Автори статті [10] пропонують метод маршрутизації мереж з різними рівнями ієрархії, що забезпечує підвищення пропускної здатності за рахунок зниження потоку внутрішньо-системних перешкод. Дані публікації ще раз дозволяють переконатися в актуальності обраної теми.

Однак слід також відзначити, що з ростом розмірів і топології мережі ускладняється завдання оцінки якості її обслуговування. Традиційний підхід базується на моніторингу мережі, тобто спостереженні за мережею і зборі інформації. У разі складної мережі аналіз результатів моніторингу – завдання, що має багато критеріїв та часто слабо формалізується, так як ґрунтується на суб'єктивній думці фахівця-експерта з мережевого управління (мережевого адміністратора).

Адміністратор, виступаючи в ролі експерта повинен:

– знати все апаратне і програмне забезпечення, що використовується, щоб швидко інтерпретувати зміни будь-яких параметрів мережі;

– знати всю топологію мережі, щоб швидко визначити причину і джерела таких змін;

– вміти виділити з величезного числа повідомлень більш пріоритетні і відкинути ті, які є наслідком перших;

– нести адміністративну відповідальність за ефективне використання ресурсів (дорогого устаткування, каналів зв'язку, обслуговуючого персоналу). Від його роботи залежить економічна ефективність підприємства.

Таким чином, складне устаткування МСМ, великий обсяг інформації, що надходить, труднощі вирішення погано формалізованих та слабо структурованих задач при відсутності повної та достовірної інформації про стан мережі, короткий час на прийняття рішення призводять до того, що адміністратор не може ефективно керувати мережею. Вихід з цього

становища полягає в створенні систем підтримки прийняття рішень (СППР), які допомагали б особі, що приймає рішення (ОПР), об'єктивно та оперативно приймати рішення при оцінці якості обслуговування МСМ [11].

Існують приклади успішного застосування методів штучного інтелекту в управлінні якістю послуг. Так, наприклад стаття [12] присвячена питанням вибору варіантів реалізації експертної системи контролю, що вводиться в мережу передачі даних для поліпшення якості обслуговування (QoS). Розглядається узагальнена структура мережі передачі даних, що містить основні елементи експертної системи контролю. Наводяться характеристики сучасних експертних систем контролю, заснованих на програмних (Cisco IP SLA, ProLAN SLA-ON) і програмно-апаратних (WiSLA, FOSS) засобах.

А в статті [13] запропонована системи управління якістю корпоративної інформаційно-обчислювальної мережі. Для створення такої системи запропонована методологія нечіткого моделювання, яка включає в себе метод оцінки якості на основі нечіткої моделі. В [14] проаналізовані різні моделі для вимірювання та моніторингу якості передачі голосу при використанні Random Neural Networks (RNN). В [15] представлений метод управління якістю для додатків реального часу: нейронні мережі забезпечують раннє та точне передбачення часу виконання неконтрольованих акцій, що дозволяє вибирати адекватні параметри рівня якості.

У зв'язку з цим, розробка моделі інтелектуальної СППР для оцінки якості передачі пакетів в сучасній МСМ є актуальною науково-технічною задачею, вирішення якої і присвячена ця дослідницька робота.

1 АНАЛІЗ ЯКОСТІ ТРАФІКА В МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ

Мультисервісна мережа (МСМ) утворює єдину інформаційно-телекомунікаційну структуру, яка підтримує всі види трафіку (дані, голос, відео) і надає всі види послуг (традиційні та нові, базові та додаткові) в будь-якій точці, в будь-який час, в будь-якому наборі і обсязі. До базових послуг мультисервісної мережі відносяться традиційні послуги передачі і доступу: передача традиційного телефонного трафіку; передача трафіку даних Інтернету; передача трафіку даних корпоративної мережі; передача трафіку мобільних мереж; доступ в мережу Інтернет; доступ до мереж передачі даних. До додаткових послуг відносяться такі: передача голосового трафіку IP-телефонії; передача відео-трафіку для організації відеоконференцій; організація віртуальної приватної мережі; послуги із забезпечення гарантованого рівня обслуговування.

Трафік МСМ можна уявити потоками трьох основних типів.

Перший тип − це так званий еластичний трафік (data), тобто незалежний від пропускної здатності ділянки мережі. Однак еластичний трафік чутливий до втрат, але практично не чутливий до затримок (до декількох хвилин в залежності від програми). В якості транспортного протоколу використовує TCP. Прикладом служить трафік таких сервісів, як e-mail, пересилання файлів, web-додатки і т.п.

Другий тип − потоковий трафік (stream). Потоковий трафік можна отримати при Інтернет-мовленні, аудіо або відео на вимогу. Його відрізняє допуск чималих затримок і втрат. На прийомі зазвичай використовується буфер, що дозволяє згладжувати нерівномірність затримки шляхом внесення додаткової затримки шляхом внесення додаткової затримки буфера. Для передачі цього типу трафіку цілком можливе використання в якості транспортних протоколів як UDP, так і TCP.

Третій тип − трафік реального часу (real time). Характеризується високою чутливістю до затримок і відносно малою чутливістю до втрат. Це може бути трафік IP-телефонії та відеоконференцзв'язку, трафік, що передається від систем відеоспостереження. Класу обслуговування обумовлює їх конкретні значення втрат і затримок. Трафік реального часу, породжений такими процесами, як сигнали управління різними об'єктами і процесами (трафік транзакцій), наприклад, on-line ігри пред'являє високі вимоги до затримки, тобто відноситься до надчуттєвого до затримок типу. Для передачі цього типу трафіку цілком можливе використання в якості транспортних протоколів як UDP, TCP так і RSVP, RTP, RTCP.

У мультисервісної мережі можемо спостерігати різні комбінації цих трьох видів трафіку.

1.1 Методи передачі даних

Передача трафіку по транспортним каналам мультисервісних мереж здійснюється в трьох режимах:

– unicast (одноадресна передача) − процес відправки пакета від одного хоста до іншого хосту;

– multicast (многоадресна передача) − процес відправки пакета від одного хоста до деякої обмеженої групи хостів;

– broadcast (широкомовна передача) − процес відправки пакета від одного хоста до всіх хостам в мережі.

Ці три типи передачі даних використовуються для різних цілей, давайте розглянемо більш докладно.

Одноадресна передача unicast. Такий тип передачі даних використовується для звичайної передачі даних від хоста до хосту (рис. 1.1).

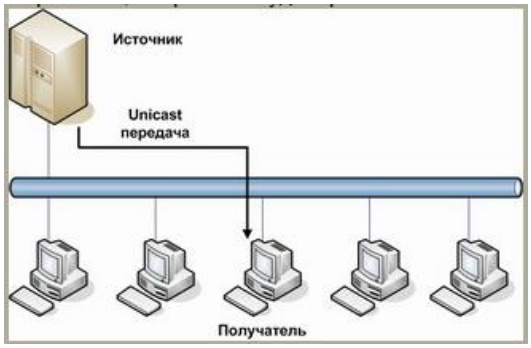


Рисунок 1.1 – Передача трафіка по технології Unicast

Спосіб Unicast працює в клієнт-серверних і пірінгових (peer-to-peer, від рівного до рівного) мережах. У unicast пакетах в якості IP адреси призначення використовується конкретний IP адресу пристрою, для якого цей пакет призначений. IP адреса конкретного пристрою складається з порції адреси мережі (в якій знаходиться цей пристрій) і порції адреси хоста (порції, що визначає це конкретне стійко в його мережі). Це все призводить до можливості маршрутизації unicast пакетів по всій мережі.

Багатоадресне передача multicast. Такий Тип передачі multicast розроблявся для заощадження пропускної здатності в MCM мережах. Такий тип зменшує трафік, дозволяючи хостам відправити один пакет обраній групі хостів (рис. 1.2).

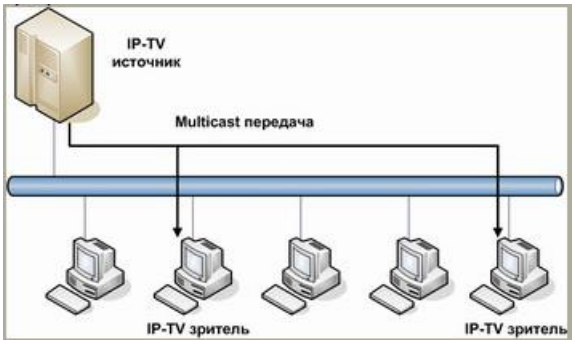


Рисунок 1.2 – Передача трафіку за технологією Multicast

Для досягнення декількох хостів призначення використовуючи передачу даних unicast, хосту джерела було б необхідно відправити кожному хосту призначення один і той же пакет. З типом передачі даних multicast,

хост джерело може відправити всього один пакет, який може досягти тисячі хостів одержувачів. Приклади multicast передачі даних: відео і аудіо розсилка; обмін інформацією про маршрути, використовуваний в маршрутизованих протоколах; поширення програмного забезпечення; стрічки новин.

Хости, які хочуть отримати певні multicast дані, називаються multicast клієнтами. Multicast клієнти використовують сервіси ініційовані (розпочаті) клієнтськими програмами для розсилки multicast даних групам. Кожна multicast група являє собою один multicast IP адреса призначення. Коли хост розсилає дані для multicast групи, хост поміщає multicast IP адреса в заголовок пакета (в розділ пункту призначення). Для multicast груп виділено спеціальний блок IP адрес, від 224.0.0.0 до 239.255.255.255.

Широкомовна передача broadcast. Через те, що тип передачі broadcast використовується для відправки пакетів до всіх хостам в мережі, пакети використовую спеціальний broadcast IP адреса. Коли хост одержує пакет, в заголовку якого в якості адреси отримувача вказано broadcast адреса, він обробляє пакет так, як ніби це unicast пакет. Коли хосту необхідно передати якусь інформацію всім хостам в мережі використовується спосіб передачі даних broadcast (рис. 1.3).

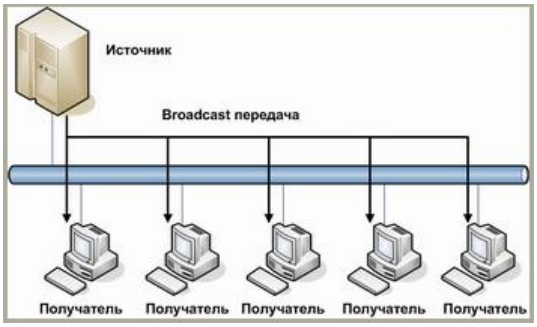


Рисунок 1.3 – Передача трафіку за технологією Broadcast

Приклади використання broadcast передача даних: створення карти приналежності адрес верхнього рівня до нижніх (наприклад, який IP адреса

на конкретному пристрої зі своїм MAC адресою); запит адреси (як приклад можна взяти протокол ARP); протоколи маршрутизації обмінюються інформацією про маршрути (RIP, EIGRP, OSPF). Коли хосту потрібна інформація, він відправляє запит на широкомовна адресу. Всі інші хости в мережі отримають і оброблять цей запит. Один або кілька хостів вкладуть запитувану інформацію та дадуть відповіді на запит. В якості типу передачі даних, що відповідають на запит, будуть використовувати unicast. Подібним чином, коли хосту необхідно відправити інформацію всім хостам в мережі, він створює широкомовний пакет з його інформацією і передає його в мережу.

Існує два типи broadcast передачі даних: спрямоване широкомовлення і обмежене широкомовлення. Спрямований broadcast відправляється всім хостам якоїсь конкретної мережі. Цей тип широкомовлення зручно використовувати для відправки broadcast трафіку всім хостам за межами локальної мережі. Обмежений broadcast використовується для передачі даних всім хостам в локальній мережі. У такі пакети як кінцеву точку маршруту вставляється IP адреса 255.255.255.255. Маршрутизатор такий широкомовний трафік не передають. Пакети, передані обмеженим broadcast будуть поширюватися тільки в локальній мережі. З цієї причини локальні мережі IP також називають широкомовною доменом (broadcast domain). Маршрутизатор утворюють кордон для широкомовного домену. Без кордону пакети б поширювалися по всій мережі, кожному хосту, зменшуючи швидкодію мережевих пристроїв і забиваючи пропускну здатність каналів зв'язку.

1.2 Основні протоколи передачі трафіку в мультисервісних мережах

У додатках реального часу (аудіо- і відеоконференції, живе відео, віддалена діагностика в медицині, комп'ютерна телефонія, ігри, моніторинг в

реальному часі і ін.). Протокол транспортного рівня − TCP не підходить для додатків реального часу:

– TCP дозволяє встановити з'єднання тільки між двома кінцевими точками, отже, він не підходить для многоадресної передачі;

– TCP передбачає повторну передачу втрачених сегментів, що прибувають, коли додаток реального часу вже їх не чекає;

– TCP не має зручного механізму прив'язки інформації про синхронізацію до сегментів.

Доступ окремих абонентських пристроїв до мультимедійного трафіку в мультисервісних мережах забезпечується за допомогою ряду протоколів.

1. Протокол RTSP (англ. Real Time Streaming Protocol, або, потоковий протокол реального часу) − це прикладний протокол, розроблений IETF в 1998 році і описаний в RFC 2326 [16], в якому описані команди для управління відеопотоком. RTSP не виконує стиснення, а також не визначає метод інкапсуляції мультимедійних даних і транспортні протоколи. Передача потокових даних сама по собі не є частиною протоколу RTSP. Більшість серверів RTSP використовують для цього стандартний транспортний протокол реального часу, який здійснює передачу аудіо- і відеоданих.

За синтаксису і операцій протокол RTSP схожий на HTTP. Однак між протоколами RTSP і HTTP є ряд істотних відмінностей. Одне з основних полягає в тому, що в першому і сервер, і клієнт здатні генерувати запити. Наприклад, відеосервер може надіслати запит для установки параметрів відтворення певного відеопотоку. Далі, протоколом RTSP передбачається, що управління станом або зв'язком повинен здійснювати сервер, тоді як HTTP взагалі ніякого відношення до цього не має. Нарешті, в RTSP дані можуть передаватися поза основною смуги (out-of-band) іншими протоколами, наприклад RTP, що неможливо в разі HTTP. RTSP-повідомлення надсилаються окремо від мультимедійного потоку (рис. 1.4). Для них використовується спеціальний порт з номером 554.

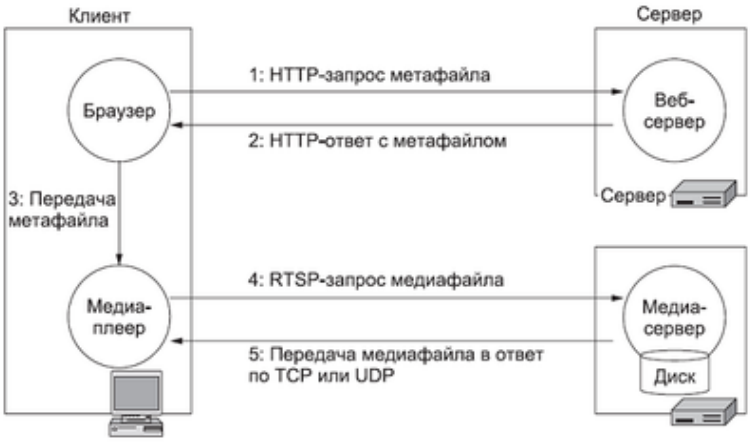


Рисунок 1.4 – Приклад використання протоколу RTSP

2. Протокол IGMP (англ. Internet Group Management Protocol, протокол групового управління в Інтернеті) − протокол керування груповою (multicast) передачею даних в мережах, заснованих на протоколі IP. Він був розроблений в 1989 році для забезпечення більш ефективної розсилки інформації по IP-адресами, ніж традиційні методи одноадресної і широкомовної передачі. Існує три версії IGMP: IGMPvl (RFC 1112), IGMPv2 (RFC 2236) hIGMPv3 (RFC 3376).

IGMP розташований вище мережевого рівня, хоча, по суті, діє не як транспортний протокол. IGMP не протокол маршрутизації пакетного передавання; це протокол, який управляє членством групи. У будь-якій мережі є один або більше маршрутизаторів групової розсилки пакетів, які розподіляють пакети, що розсилаються за багатьма адресами хостів або інших маршрутизаторів. Протокол IGMP дає інформацію маршрутизаторам групової розсилки про стан членства хостів (маршрутизаторів), підключених до мережі. Маршрутизатор групового розсилання може отримати тисячі пакетів групової розсилки кожен день для різних груп. Якщо маршрутизатор не має ніякої інформації про стан членства хостів, він повинен широкомовно передати всі ці пакети. Це створює великий трафік і знижує пропускну здатність. Краще рішення полягає в тому, щоб зберегти список груп в мережі, для якої є принаймні один відомий член. IGMP допомагає маршрутизатору групового розсилання створювати і оновлювати цей список. У загальному

випадку протокол IGMP визначає наступні типи повідомлень: запит про належність до групи (Membership Query); відповідь про належність до групи (Membership Report); Ви збираєтесь вийти з групи (Leave Group Message).

IGMP може використовуватися для підтримки потокового відео і онлайн-ігор. Для таких типів додатків він дозволяє використовувати мережеві ресурси більш ефективно.

2. Протокол RTP / RTCP. Протокол RTP (англ. Real-Time Transport Protocol, протокол реального часу) був розроблений IETF [17] для перенесення в реальному часі мовної та відеоінформації по мережі з комутацією пакетів. Спільно з протоколом UDP, RTP реалізує функції транспортного рівня. Протокол UDP здійснює сервіс доставки пакетів без встановлення з'єднання і надає протоколу RTP послуги мультиплексування і виявлення помилок на основі контрольної суми. При виявленні помилок пошкоджені сегменти відкидаються, а функції упорядкування пакетів лягають на RTP, який здійснює нумерацію пакетів в потоці. Як протоколів транспортного рівня RTP може використовувати і інші протоколи.

Служба RTP передбачає зазначення типу корисного навантаження і послідовного номера пакета в потоці, а також застосування тимчасових міток. Відправник позначає кожен RTF-пакет тимчасової міткою, а одержувач витягує її і обчислює сумарну затримку. Різниця в затримці пакетів дозволяє визначити джиттер і пом'якшити його вплив − всі пакети будуть видаватися з додатком з однаковою затримкою.

Таким чином, головна особливість RTP − це обчислення середньої затримки деякого набору прийнятих пакетів і видача їх призначеному для користувача додатку з постійною затримкою, рівною цьому середньому значенню. Однак слід мати на увазі, що тимчасова мітка RTP відповідає моменту кодування першого дискретного сигналу пакета. Тому, якщо RTF-пакет, наприклад, із відео, розбивається на кілька пакетів нижчого рівня, то тимчасова мітка вже не буде відповідати теперішньому часу їх передачі, оскільки вони перед передачею можуть бути організовані в чергу.

Протокол контролю транспортування інформації в реальному часі RTCP (англ. Real-Time Transport Control Protocol) формує звіти, що містять інформацію про комунікаційну RTP. Протокол RTCP передає відомості (як від приймача, так і від відправника) про кількість переданих і втрачених пакетів, значенні джиттера, затримки і т.д., підтримуючи зв'язок між відправником і отримувачем шляхом обміну пакетами − звіт приймача і звіт джерела. На практиці протокол RTP невіддільна від протоколу RTCP (RTP control protocol). Останній служить для моніторингу QoS і для передачі інформації про учасників обміну в ході сесії.

1.3 Особливості трафіку реального часу в мультисервісних мережах

Всі процеси передачі інформації в МСМ повинні відбуватися в режимі реального часу і де особливо важлива динаміка передачі сигналу, яка забезпечується сучасними методами кодування і передачі інформації; в результаті збільшується пропускна здатність каналів в порівнянні з традиційними телефонними мережами [18].

Організація ITU-T серйозно займалася дослідженням проблем, пов'язаних із затримками при передачі голосу по мережі. В результаті був розроблений стандарт ITU-T G.114 [19], який рекомендує, щоб затримка при передачі голосу в одному напрямку не перевищувала 150 мілісекунд. Також стандарт рекомендує розглядати затримку від 150 до 400 мілісекунд як прийнятну. У тому випадку, коли затримка сягає 400 мілісекунд і більше, вона стає помітною. Стандарт також встановлює, що при передачі голосу затримка більш ніж 400 мілісекунд є неприйнятною.

Найбільш надійним способом порівняльної оцінки якості переданої мови є суб'єктивний метод спільної думки MOS (Mean Opinion Score). Оцінки MOS розраховуються після прослуховування групою людей тестованого тракту передачі мови за п'ятибальною шкалою.

Спочатку MOS представляв собою середнє арифметичне всіх оцінок якості, даних людьми, які прослуховували тестовий дзвінок і давали йому свою оцінку. На сьогоднішній день для оцінки якості звукового потоку людської участі не потрібно. Сучасний інструментарій оцінки якості VoIP включає в себе штучні програмні моделі для розрахунку MOS.

Показник MOS є досить надійним інструментом в оцінці якості, проте в ній відсутня можливість кількісно врахувати чинники, що впливають на якість мови. Зокрема, не враховуються: наскрізна (end-to-end) затримка між мовцем по телефону і слухають; вплив варіації затримки (джиттера); вплив втрат пакетів.

В якості альтернативи MOS в 2012 р. МСЕ прийняв Рекомендацію G.107, в якій був описаний підхід до менш суб'єктивній оцінки якості послуг в телекомунікаціях. В його основу покладено так звана E-модель, яка відкрила новий напрямок в оцінці якості послуг, пов'язане з вимірюванням характеристик терміналів і мереж. Результатом обчислень відповідно до E-моделі є число, зване R-фактором («коефіцієнтом рейтингу»).

R-Factor (quality rating) є альтернативним способом оцінки якості звуку. Бальна шкала від 0 до 100 на відміну від скороченою шкали MOS (1-5) дозволяє робити більш точну оцінку показника якості. При розрахунку R-фактора враховуються 20 параметрів, в числі яких: однонаправлена затримка; коефіцієнт втрати пакетів; втрати даних через переповнення буфера джиттера; спотворення, що вносяться при перетворенні аналогового сигналу в цифровий і подальшому стисненні (обробка сигналу в кодеках); вплив луни і ін. Таким чином, E-модель і R-фактор можуть бути використані для об'єктивної оцінки якості передачі мови в технології VoIP.

1.4 Характеристики якості обслуговування

Виходячи з передбачуваного призначення мережі, повинна бути визначена сукупність параметрів QoS, які, як передбачається, будуть мати

основне значення. Для цих параметрів QoS можуть бути встановлені контрольні показники якості. В рекомендації Y.1540 [20] розглядаються наступні мережеві характеристики, як найбільш важливі за ступенем їх впливу на наскрізне якість обслуговування (від джерела до одержувача), що оцінюється користувачем: продуктивність мережі; надійність мережі / мережевих елементів; параметри доставки пакетів.

Продуктивність мережі (або швидкість передачі даних) користувача визначається як ефективна швидкість передачі, яка вимірюється в бітах в секунду. Слід зазначити, що значення цього параметра не збігається з максимальною пропускною спроможністю мережі, яка помилково називається (причому, досить часто) пропускною здатністю. Мінімальне значення продуктивності зазвичай гарантується провайдером послуг, який, в свою чергу, повинен мати відповідні гарантії від мережевого провайдера. В Рекомендації Y.1540 не наведено нормативні характеристики продуктивності мережі, які розрізняються для різних областей застосування.

Надійність мережі / мережевих елементів. Надійність мережі може бути визначена через ряд параметрів, з яких найбільш часто використовується коефіцієнт готовності, який вираховується як відношення часу простою об'єкта до сумарного часу спостереження об'єкта, що включає час простою і час між відмовами. В ідеальному випадку коефіцієнт готовності повинен бути рівний 1, що означає стовідсоткову готовність мережі. На практиці коефіцієнт готовності оцінюється числом «дев'яток». У таблиці 1.1 наведені дані по час простою для різної кількості «дев'яток».

Таблиця 1.1 – Коефіцієнти готовності і часу простою

Коефіцієнт готовності	Час простою
0,99	3,7 днів на рік
0,999	9 годин на рік
0,9999	53 хвилини на рік
0,99999	5,5 хвилин на рік
0,99999999	30 секунд на рік

Необхідно відзначити, що забезпечення коефіцієнта готовності «п'ять дев'яток» в мережах IP, побудованих на традиційному обладнанні даних (сервери, маршрутизатори), є досить серйозною проблемою. Причина цього полягає в тому, що обробка інформаційних потоків в мережах IP в значної частини базується на програмному забезпеченні (а не на апаратній, як це має місце в ТМЗК). У той же час статистика відмов у МСМ мережах можна класифікувати за такими групами: 1 група (45% ... 70%) − природне старіння елементів апаратного забезпечення маршрутизаторів (в першу чергу знос інтерфейсних плат), 2 група (20%) − некоректні операції технічного обслуговування, 3 група (17%) − збої в програмному забезпеченні маршрутизаторів, 4 група (16%) − збої в електроживленні, 5 група (84%) − збої оптичного устаткування (стосовно до транспортних мереж) (рис. 1.5) [21].

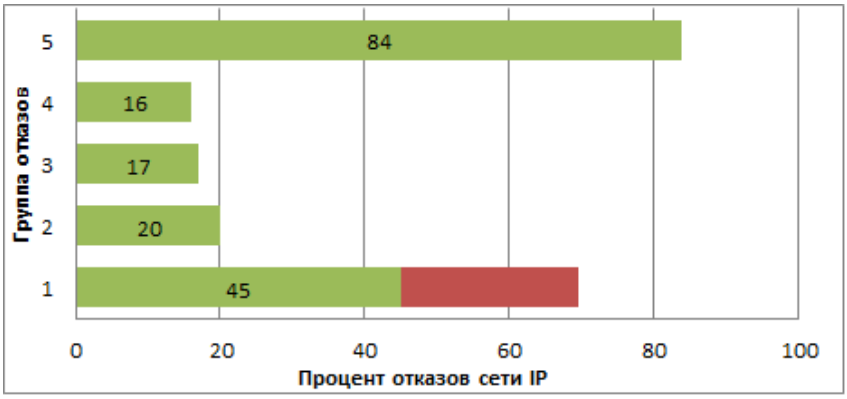


Рисунок 1.5 – Причини відмов мережевого обладнання

Рекомендація MCE-T Y.1540 визначає наступні параметри, що характеризують доставку IP-пакетів.

1. Затримка доставки пакета IP (IP packet transfer delay, IPTD). Параметр IPTD визначається як час (t2 − t1) між двома подіями − введенням пакета у вхідні точку мережі в момент t1 і висновком пакета з вихідний точки мережі в момент t2, де (t2> t1) і (t2 − t1) ≤ Tmax. Загалом, параметр IPTD визначається як час доставки пакета між джерелом і одержувачем для всіх пакетів − як успішно переданих, так і уражених помилками.

Середня затримка доставки пакета IP − параметр, специфікований в Рекомендації Y.1540, визначається як середня арифметична величина затримок пакетів в обраному наборі переданих і прийнятих пакетів. Значення середньої затримки залежить від переданого в мережі трафіку і доступних мережевих ресурсів, зокрема, від пропускної здатності. Зростання навантаження і зменшення доступних мережевих ресурсів ведуть до зростання черг у вузлах мережі і, як наслідок, до збільшення середніх затримок доставки пакетів. Мовна інформація і, почасти, відеоінформація є прикладами трафіку, чутливого до затримок, тоді як додатки даних в основному менш чутливі до затримок. Коли затримка доставки пакета перевищує певні значення Tmax, такі пакети відкидаються.

У додатках реального часу (наприклад, в IP-телефонії) це веде до погіршення якості мови. Обмеження, пов'язані з середньою затримкою пакетів IP, грають ключову роль для успішного впровадження технології Voice over IP (VoIP), відео-конференцій та інших додатків реального часу. Цей параметр багато в чому буде визначати готовність користувачів прийняти подібні додатки.

2. Варіація затримки пакета IP (IP packet delay variation, IPDV). Для IP-пакета визначається між вхідний і вихідний точками мережі у вигляді різниці між абсолютною величиною затримки Xi при доставці пакета з індексом i, і певною еталонною (або опорної) величиною затримки доставки пакета IP, dl, 2, для тих ж мережевих точок: IPDV = Xi − d1,2. Еталонна затримка доставки пакета IP, d1,2, між джерелом і одержувачем визначається як абсолютне значення затримки доставки першого пакету IP між даними мережевими точками. Варіація затримки пакета IP, або джиттер, проявляється в тому, що послідовні пакети прибувають до одержувача в нерегулярні моменти часу. У системах IP-телефонії це, наприклад, веде до спотворень звуку і в результаті до того, що мова стає нерозбірливою.

3. Коефіцієнт втрати пакетів IP (IP packet loss ratio, IPLR). Коефіцієнт IPLR визначається як відношення сумарного числа втрачених пакетів до

загальної кількості прийнятих в обраному наборі переданих і прийнятих пакетів. Втрати пакетів в мережах IP виникають в тому випадку, коли значення затримок при їх передачі перевищує нормоване значення, визначене вище як Tmax. Якщо пакети губляться, то при передачі даних можлива їх повторна передача по запиту приймаючої сторони. У системах VoIP пакети, що прийшли до одержувача з затримкою, що перевищує Tmax, відкидаються, що веде до провалів в прийнятої мови. Серед причин, що викликають втрати пакетів, необхідно відзначити зростання черг у вузлах мережі, що виникають при перевантаженнях.

4. Коефіцієнт помилок пакетів IP (IP packet error ratio, IPER). Коефіцієнт IPER визначається як сумарна кількість пакетів, прийнятих з помилками, до суми успішно прийнятих і пакетів, прийнятих з помилками.

Значення параметрів, наведені в табл. 1.2, являють собою, відповідно, верхню межу для середніх затримок, джиттера, втрат і помилок пакетів згідно з рекомендаціями Y.1541 [22].

Таблиця 1.2 – Характеристики мереж за класами якості обслуговування

Мережеві характеристики	Класи QoS					
	0	1	2	3	4	5
Затримка доставки пакета IP, IPTD	100 мс	400 мс	100 мс	400 мс	1 с	Н
Варіація затримки пакета IP, IPDV	50 мс	50 мс	Н	Н	Н	Н
Коефіцієнт втрати пакетів IP, IPLR	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	Н
Коефіцієнт помилок пакетів IP, IPER	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	Н

Рекомендація Y.1541 встановлює відповідність між класами якості обслуговування і додатками:

– клас 0 − додатки реального часу, чутливі до джиттеру, що характеризуються високим рівнем інтерактивності (VoIP, відеоконференції);

– клас 1 − додатки реального часу, чутливі до джиттеру, інтерактивні (VoIP, відеоконференції);

– клас 2 − транзакції даних, що характеризуються високим рівнем інтерактивності (наприклад, сигналізація);

– клас 3 − транзакції даних, інтерактивні;

– клас 4 − додатки, що допускають низький рівень втрат (короткі транзакції, масиви даних, потокове відео);

– клас 5 − традиційні застосування мереж IP.

1.5 Постановка мети і завдань дослідження

До сучасних мультисервісних мереж пред'являються високі вимоги щодо забезпечення якості обслуговування трафіку. До найбільш вимогливого трафіку відноситься трафік реального часу (IP-телефонія та відеоконференцзв'язок, процеси управління, ігри-online і т.д.). Передача такого трафіку була б неможлива без використання спеціальних протоколів.

У 1996 році Audio-Video Transport Working Group розробила протокол RTP (англ. Real-time Transport Protocol) і опублікувала як стандарт RFC 1 889 (виведений з ужитку оновленням RFC 3550 у 2003 році). Спільно з протоколом UDP, RTP реалізує функції транспортного рівня (рис. 1.6).

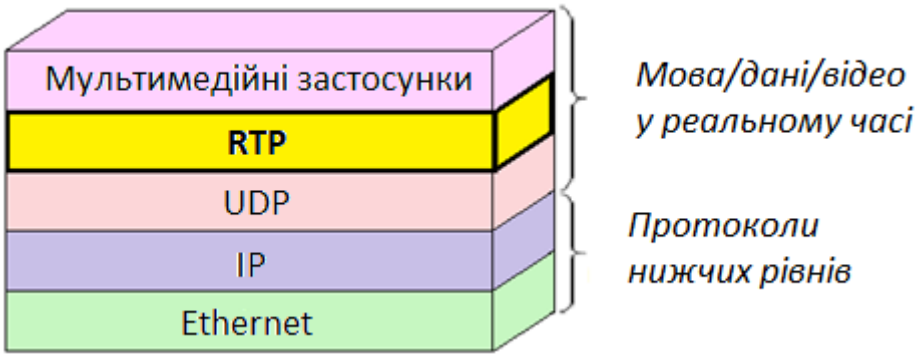


Рисунок 1.6 – Рівні протокола RTP/UDP/IP

На практиці протокол RTP невіддільний від протоколу RTCP (Real-Time Transport Control Protocol). Останній служить для моніторингу QoS і для передачі інформації про учасників обміну в ході сесії. Протокол RTCP формує звіти, що містять інформацію про комунікаційну RTP. Протокол нижчого рівня повинен забезпечити мультиплексування інформаційних і керуючих пакетів, наприклад, з використанням різних номерів портів UDP.

Завдяки многоадресній природі протоколів RTP / RTCP, всі учасники сеансу передачі мультимедійних даних отримують звіти зворотного зв'язку інших учасників і, таким чином, кожен з них може оцінити загальну і індивідуальну якість прийому і передачі під час сеансу зв'язку, а саме: оцінити швидкість передачі даних, рівень загублених пакетів і рівень нерівномірності передачі. Передбачається, що частина смуги пропускання, що виділяється для RTCP, повинна бути встановлена рівної 5%.

У разі якщо частка службового RTCP-трафіку перевищує 5%, протокол RTP автоматично «ріже» RTCP-пакети. Даний підхід з одного боку дозволяє зменшити широкомовний службовий трафік, проте веде до несвоєчасну реакцію учасників сеансу на зміну умов передачі і до реальної загрози втратити вихідну функціональність RTCP, тобто службовий трафік не буде давати повної картини стану МСМ.

Відповідно до стандарту RFC 3550, в процесах передачі групового RTCP-трафіку може брати участь третя сторона (додатковий учасник сеансу), звана монітором, яка може і не брати участь в мультимедіа сесії. Однак монітор виконує збір та аналіз RTCP-звітів на предмет оцінки стану каналів зв'язку сесії, а також накопичує статистику за даними RTCP-звітів в тренді. Таким чином, з метою скорочення групового трафіку RTCP, що генерується звітами одержувачів (Receiver Reports, RR) і відправників (Sender Reports, SR) в централізовану архітектуру відео-конференцзв'язку (ВКЗ) було введено поняття діагностичного вузла (ДВ). На підставі RTCP-звітів, сконцентрованих на ДВ, експерт (адміністратор) може зробити висновок про те, які заходи необхідно провести для покращення якості зв'язку.

Таким чином, метою атестаційної роботи є розробка системи підтримки прийняття рішення при оцінці якості доставки пакетів в МСМ шляхом концентрації службового трафіку (RTCP-пакетів) на одному діагностичному вузлі.

Об'єктом дослідження є трафік реального часу, а предметом − підвищення якості доставки пакетів.

Для досягнення поставленої мети необхідно вирішити такі завдання.

1. Проаналізувати стандарти щодо забезпечення якості обслуговування в МСМ, вибрати найбільш значимі параметри, що впливають на QoS.

2. Дослідити способи передачі трафіку реального часу, а також методи забезпечення QoS.

3. Застосувати розширену модель зворотного зв'язку RTCP з введенням діагностичного вузла для скорочення обсягу і концентрації RTCP-трафіку.

4. Створити нечітку модель оцінки якості доставки пакетів в МСМ.

5. Спроектувати структуру системи підтримки прийняття рішення при оцінці якості доставки пакетів.

6. Виконати аналіз ефективності нечіткої моделі оцінки якості доставки пакетів в МСМ.

7. Виконати експеримент з настройки сервера IP-телефонії Asterisk, для його подальшого використання в якості діагностичного вузла.

2 ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ В МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ

Сприянням розвитку і продуктивної експлуатації засобів електрозв'язку (телекомунікацій) з метою підвищення ефективності послуг електрозв'язку та їх доступності для населення займається міжнародний союз електрозв'язку (МСЕ), який є спеціалізованою установою Організації Об'єднаних Націй в області електрозв'язку і інформаційно-комунікаційних технологій (ІКТ). Сектор стандартизації електрозв'язку МСЕ (МСЕ-Т) − постійний орган МСЕ. Основними продуктами МСЕ-Т є Рекомендації − стандарти, що визначають порядок функціонування та взаємодії мереж електрозв'язку. Рекомендація МСЕ-Т Е.800 [23] визначає якість обслуговування QoS як сукупність характеристик послуги електрозв'язку, які мають відношення до її можливості задовольняти встановлені і передбачувані потреби користувача послуги. В Рекомендації МСЕ-Т Е.802 [24] наводиться уточнююче визначення якості як сумарного ефекту характеристик обслуговування, який визначає ступінь задоволеності користувача даною послугою. Якість передачі мультимедійних даних (зазвичай поєднання голосової, текстової, відео- і аудіоінформації) оцінюється шляхом порівняння характеристик сигналу передачі на виході з мережі і його характеристиками на вході в мережу (end-to-end). Така модель QoS називається наскрізною (рис. 2.1).

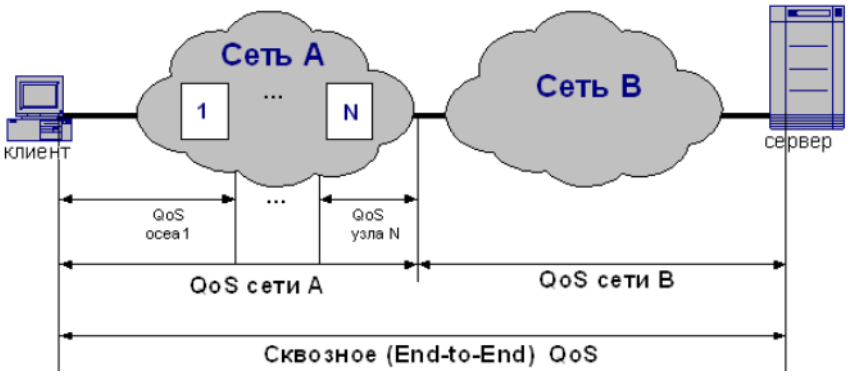


Рисунок 2.1 – Еталонна модель наскрізного QoS

В цілому QoS визначається набором кількісних параметрів, які можуть бути виміряні (об'єктивні параметри), і якісних параметрів, які можуть бути виражені лише через судження людини (суб'єктивні параметри).

2.1 Моделі забезпечення якості обслуговування

Численними тематичними групами розроблялися і продовжують розроблятися рішення щодо забезпечення необхідної якості обслуговування для передачі різнотипного трафіку (реального часу, потокового і еластичного) по єдиній мережі, це моделі обслуговування PQ / CQ / WFQ / CBWFQ / LLQ / RPQ +, моделі DiffServ / IntServ- RSVP, технологія MPLS і т.д.

Мережевий трафік складається з безлічі потоків, що згенеровані застосунками кінцевих станцій. Ці застосунки відрізняються один від одного різними вимогами до обслуговування та до роботи даного продукту мережі. Таким чином, вимога до обслуговування кожного потоку повністю визначається вимогами згенерувати цей потік застосунку [4]. Розглянемо моделі доставки даних.

1. Модель негарантованої доставки даних (best-effort) полягає у забезпеченні зв'язності вузлів мережі без гарантії часу і самого факту доставки пакета в точку призначення. Слід зазначити, що відкидання пакету може статися тільки в разі переповнення буфера вхідної або вихідної черги маршрутизатора. Насправді негарантована доставка пакетів не є частиною QoS внаслідок відсутності гарантії якості обслуговування і гарантії забезпечення доставки пакетів. Слід зазначити, що негарантована доставка пакетів є на сьогоднішній день єдиною послугою, яку підтримує в Internet. Незважаючи на деяке зниження продуктивності, для більшості застосунків, орієнтованих на передачу інформації (наприклад, додатків, що забезпечують взаємодію по протоколу передачі файлів (File Transfer Protocol − FTP)), ця послуга є цілком достатньою. В цілому ж оптимальні умови функціонування

всіх застосунків включають в себе вимоги до виділення певних мережевих ресурсів в термінах смуги пропускання, затримки і рівня втрати пакетів.

2. Модель інтегрованого обслуговування (IntServ)

Інтегроване обслуговування передбачає резервування мережевих ресурсів з метою задоволення специфічних вимог до обслуговування з боку потоків трафіку. Протокол функціонує наступним чином [25]: вузел-джерело до передачі даних, що вимагають певного нестандартної якості обслуговування (наприклад, постійної смуги пропускання для передачі відеоінформації) посилає по мережі спеціальне повідомлення про шляхи (path message), що містить дані про тип переданої інформації і необхідної пропускної здатності. Повідомлення передається між маршрутизаторами по всій лінії від вузла-відправника до адреси призначення, при цьому визначається послідовність маршрутизаторів, в яких необхідно зарезервувати певну смугу пропускання. Маршрутизатор, отримавши таке повідомлення, перевіряє свої ресурси з метою визначення можливості виділення необхідної пропускної спроможності. При її відсутності маршрутизатор запит відкидає. Якщо необхідна пропускна здатність досяжна, то маршрутизатор налаштовує алгоритм обробки пакетів таким чином, щоб вказаною потоку завжди надавалася необхідна пропускна здатність, а потім передає повідомлення наступного маршрутизатора уздовж шляху. В результаті по всьому шляху від вузла-відправника до адреси призначення резервується необхідна пропускна здатність.

Інтегроване обслуговування досить часто називають ще «жорстким» QoS (hard QoS) у зв'язку з пред'явленням строгих вимог до ресурсів мережі.

На жаль, резервування ресурсів на всьому шляху проходження окремих потоків трафіку неможливо реалізувати в масштабах магістралі Internet, яка обслуговує в окремий момент часу тисячі потоків даних. Виправити положення покликане агреговане резервування ресурсів, що вимагає зберігання в базових маршрутизаторах Internet всього лише невеликої кількості інформації. Застосунки, що вимагають інтегрованого

обслуговування, включають в себе мультимедійні застосунки, які проводять передачу голосової інформації та відео-зображень. Інтерактивні програми, орієнтовані на передачу мови по Internet, можуть функціонувати нормально (тобто, не викликаючи незручності у користувачів) лише в тому випадку, якщо значення латентності менше 100 мс. Слід зазначити, що аналогічний рівень латентності є прийнятним для більшості мультимедійних додатків. А ось для застосунків Intenet-телефонії вже знадобиться канал передачі інформації з пропускною спроможністю щонайменше 8 Кбіт/с. Для того щоб задовольнити подібні вимоги до інтегрованого обслуговування, мережа повинна мати певний запас ресурсів.

Сервісна модель IntServ в поєднанні з RSVP дозволяє організувати гнучке обслуговування різнотипного трафіку, максимально враховуючи потреби кожної програми, а використання методу обробки черг WFQ для обслуговування пакетів гарантує максимально допустиме значення затримки. Ця особливість робить IntServ ідеальної для обслуговування мультимедійного трафіку.

Однак слід зазначити, що висока гнучкість і «бажання» задовольнити потреби поодиноких потоків є джерелом слабких місць IntServ. Основним недоліком моделі вважається низька масштабованість. Продуктивність IntServ залежить від кількості оброблюваних потоків, отже, таку сервісну модель практично неможливо реалізувати в мережі з мільйонами користувачів. Тому для великих мереж потрібна більш проста і масштабована технологія, а область застосування IntServ обмежилася внутрішніми і кінцевими мережами.

3. Модель диференційованого обслуговування (DiffServ) передбачає розділення трафіку на класи на основі вимог до якості обслуговування. Кожен клас трафіку диференціюється і обробляється мережею відповідно до заданих для цього класу механізмами QoS. Робота DiffServ грунтується на ідентифікатор DSCP (Differentiated Services Code Point). DSCP − поле в IP-пакеті, що дозволяє призначити мережному трафіку різні рівні

обслуговування. Для досягнення цього кожен пакет в мережі позначається кодом DSCP і відповідним йому рівнем обслуговування. Змінюючи значення цього ідентифікатора, різні види трафіку можна розподілити за пріоритетами в черзі. Слід зазначити, що диференційоване обслуговування саме по собі не передбачає забезпечення гарантій, що надаються. Відповідно до даної схеми трафік розподіляється по класах, кожен з яких має свій власний пріоритет. З цієї причини диференційоване обслуговування досить часто називають «м'яким» QoS (soft QoS).

Однією з реалізацій моделі DiffServ є технологія многопротокольной комутації на основі міток (Multiprotocol Label Switching − MPLS), яка на сьогоднішній день стала однією з основних для побудови великих мереж операторів, що надають послуги із забезпеченням якості обслуговування.

4. Multiprotocol Label Switching (MPLS, багатопротокольна комутація з використанням міток) − це технологія швидкої комутації пакетів в багато протокольних мережах, заснована на використанні міток. MPLS розробляється і позиціонується як спосіб побудови високошвидкісних IP-магістралей, однак область її застосування не обмежується протоколом IP [26].

Технологією MPLS і DiffServ схожі − обидва стандарти використовують маркування пакетів у вхідних точках мережі, тобто аналіз, класифікація трафіку відбувається на кордоні доменів. Однак, на відміну від DiffServ, що використовує для DSCP вже існуюче поле TOS в пакеті IP, в MPLS до пакету додається спеціальна 32-розрядна інформаційна мітка. Мітка поміщається між заголовками другого/третього рівня і використовується для визначення наступного маршрутизатора на шляху до пункту призначення.

Використання мітки для переадресації пакетів в MPLS дозволяє значно знизити час обробки пакетів в маршрутизаторі. Маршрутизатор, що підтримує MPLS і здатний, крім того, аналізувати заголовки і виробляти пересилання пакетів, що не містять міток, називається маршрутизатором

комутації по мітках. Технологія MPLS передбачає наявність маршрутизаторів двох типів:

– LER (Label Enge Routers) − прикордонні маршрутизатори MPLS;

– LSR (Label Switching Routers) − транзитні маршрутизатори MPLS.

У точці входу в мережу MPLS стоять прикордонні маршрутизатори, на які покладаються функції класифікації пакетів за різними класами FEC і реалізація різноманітних додаткових послуг. Вхідний LER додає мітку всіх пакетів, що надходять в мережу MPLS, а вихідний LER видаляє мітку і, або здійснює маршрутизацію на основі IP-адреси.

Крім функції комутації, кожен маршрутизатор MPLS виконує функцію управління по формуванню таблиці маршрутизації. Ця таблиця називається таблицею пересилання LIB (Label Information Base). LIB складається з вхідної мітки і однієї або декількох вкладених записів. Кожен такий запис включає вихідну мітку, номер вихідного інтерфейсу і адреса наступного маршрутизатора в LSR.

Переваги технології MPLS: відділення вибору маршруту від аналізу IP-адреси (дає можливість надавати широкий спектр додаткових сервісів при збереженні масштабованості мережі); прискорена комутація (скорочує час пошуку в таблицях); гнучка підтримка QoS, інтегрованих сервісів і віртуальних приватних мереж; ефективне використання явного маршруту; поділ функціональності між ядром і граничної областю мережі.

Технологія MPLS характеризується високою масштабованість і розглядається в якості найбільш перспективної для передачі IP-трафіку.

2.2 Управління перевантаженнями. Механізм черг

Перевантаження виникає в разі переповнення вихідних буферів обладнання, що передає трафік. Основними механізмами виникнення перевантажень (або, що рівнозначно, скупчень − congestions) є агрегація трафіку (коли швидкість вхідного трафіку перевищує швидкість вихідного) і

неузгодженість швидкостей на інтерфейсах. Управління пропускною здатністю в разі перевантажень (вузьких місць) здійснюється за допомогою механізму черг. Пакети поміщаються в черзі, які впорядковано обробляються за певним алгоритмом. Фактично, управління перевантаженнями − це визначення порядку, в якому пакети виходять з інтерфейсу (черг) на основі пріоритетів. Якщо перевантажень немає − черги не працюють (і не потрібні).

Розглянемо методи обробки черг.

1. Елементарна черга з послідовним проходженням пакетів, що працює за принципом перший прийшов − перший пішов (First In First Out, FIFO) (рис. 2.2).

Рисунок 2.2 – Черга FIFO

У всіх пристроях з комутацією пакетів алгоритм FIFO використовується за умовчанням, так що така черга також зазвичай називається чергою «за замовчуванням». Перевагами цього підходу є простота реалізації і відсутність потреби в конфігурації. Однак йому притаманний і недолік − неможливість диференційованої обробки пакетів різних потоків. Всі пакети очікують в загальній черзі на рівних підставах.

2. Черга пріоритетів (Priority Queuing, PQ) забезпечує безумовний пріоритет одних пакетів над іншими (рис. 2.3).

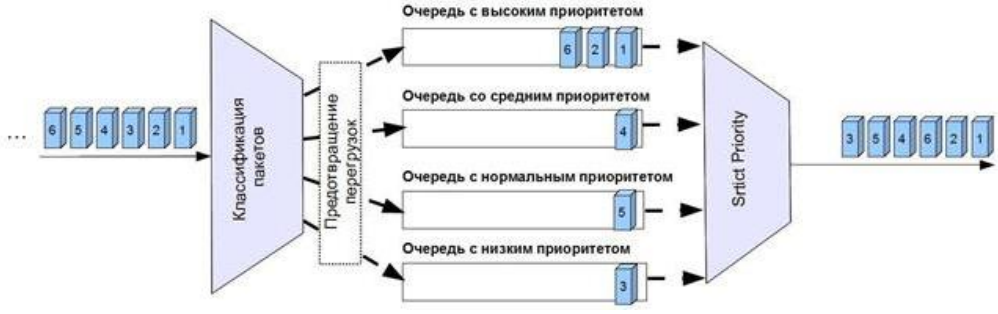


Рисунок 2.3 – Черга PQ із суворим пріоритетом

Всього 4 черги: з високим (high), середнім (medium), нормальним (normal) і низьким (low) пріоритетами. Обробка ведеться послідовно (від high до low), починається з високопріоритетних черг і до її повного очищення не переходить до менш пріоритетних черг. Таким чином, можлива монополізація каналу високопріоритетними чергами. Трафік, пріоритет якого явно не вказано, потрапить в чергу за замовчуванням (default).

3. Довільні черги (Custom Queuing, CQ) забезпечує черги, що настроюються. Передбачається управління часткою смуги пропускання каналу для кожної черги. Підтримується 17 черг. Системна 0 черга зарезервована для керуючих високопріоритетних пакетів (маршрутизація і т.п.) і недоступна користувачеві (рис. 2.4).

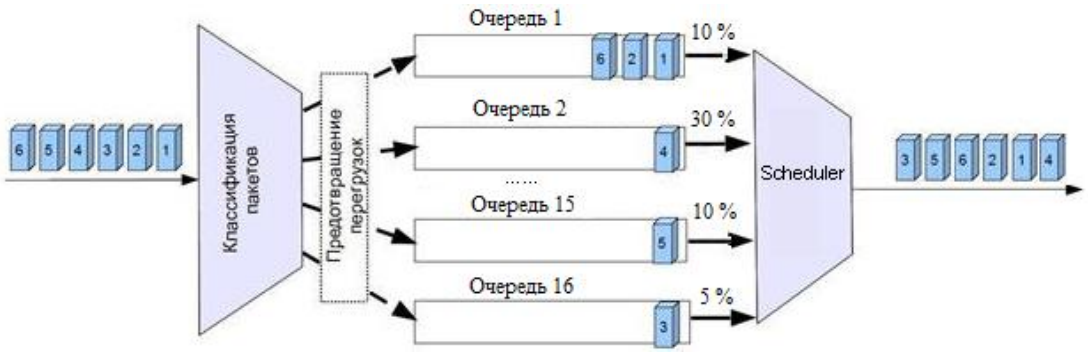


Рисунок 2.4 – Довільні черги CQ

Черги обходяться послідовно, починаючи з першої. Кожна черга містить лічильник байт, який на початку обходу містить задане значення і зменшується на розмір пакета, пропущеного з цієї черги. Якщо лічильник не рівний нулю, то наступний пакет пропускається цілком, а не його фрагмент, рівний залишку лічильника. Так для прикладу, представленому на рисунку 8, при перевантаженнях в кожному циклі з першої черги забирається 10% даних, з другої 30%, з третьої − 10%, з четвертої − 5%. В результаті кожному потоку дістається гарантований мінімум пропускної здатності, що в багатьох випадках є більш бажаним результатом.

4. Зважені справедливі черги (Weighted Fair Queuing, WFQ) автоматично розбивають трафік на потоки (flows). За замовчуванням їх число дорівнює 256, але це може бути змінено (параметр dynamic-queues в команді fair-queue). Якщо потоків більше, ніж черг, то в одну чергу поміщається кілька потоків. Належність пакета до потоку (класифікація) визначається на основі значення поля TOS (Type of services, тип сервісу), протоколу, IP адреси джерела, IP адреси призначення, порту джерела і порту призначення. Кожен потік використовує окрему чергу.

Оброблювач WFQ (scheduler) забезпечує рівномірний (fair, чесне) поділ смуги між існуючими потоками. Для цього доступна смуга ділиться на число потоків і кожен отримує рівну частину. Крім того, кожен потік отримує свою вагу (weight), з деяким коефіцієнтом обернено пропорційний IP пріоритету (ToS). Вага потоку також враховується оброблювачем.

На рисунку 2.5 представлений приклад справедливої черги, де обробник WFQ (scheduler) вибирає спочатку три пакети (вага 3) з першої черги, один пакет (вага 1) − з другої черги, два пакети (вага 2) з 254-ї черги і один пакет (вага 1) з 255-ї черги.

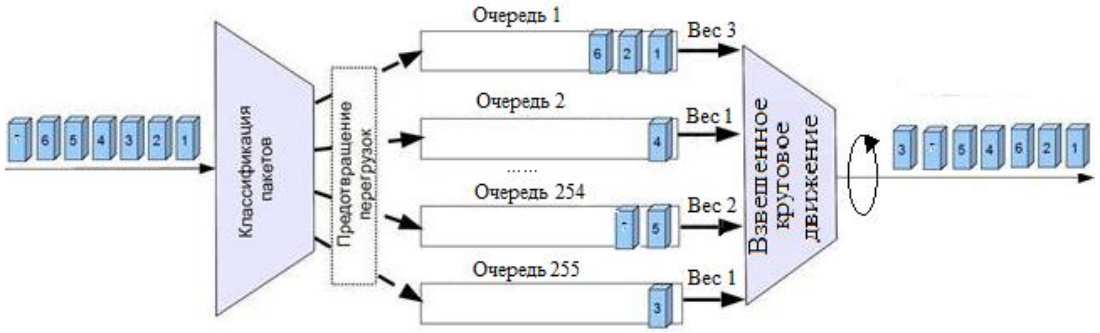


Рисунок 2.5 − Зважені справедливі черги WFQ

В результаті WFQ автоматично справедливо розподіляє доступну пропускну здатність, додатково враховуючи ToS. Потоки з однаковими IP пріоритетами ToS отримають рівні частки смуги пропускання; потоки з великим IP пріоритетом − велику частку смуги. У разі перевантажень

ненавантажені високопріоритетні потоки функціонують без змін, а фонові високонавантажені − обмежуються.

5. Зважені справедливі черги, що базуються на класах (Class Based Weighted Fair Queuing, CBWFQ) відповідає механізму обслуговування черг на основі класів. Весь трафік розбивається на 64 класа на підставі наступних параметрів: вхідний інтерфейс, аксесс лист (access list), протокол, значення DSCP, мітка MPLS QoS. Загальна пропускна здатність вихідного інтерфейсу розподіляється за класами. Кожному класу виділяється смуга пропускання, що визначається як абсолютне значення (bandwidth в Kbit/s) або у відсотках (bandwidth percent) щодо встановленого значення на інтерфейсі (рис. 2.6).

Пакети, які не потрапляють в сконфігуровані класи, потрапляють в клас за замовчуванням, який можна додатково налаштувати і який отримує залишкову вільну смугу пропускання каналу. При переповненні черги будь-якого класу пакети даного класу ігноруються.

Алгоритм відхилення пакетів всередині кожного класу можна вибирати: включене за замовчуванням звичайне відкидання (tail-drop, параметр queue-limit) або WRED (параметр random-detect). Тільки для класу за замовчуванням можна включити рівномірний (чесний) розподіл смуги (параметр fair-queue). CBWFQ підтримує взаємодію з RSVP.

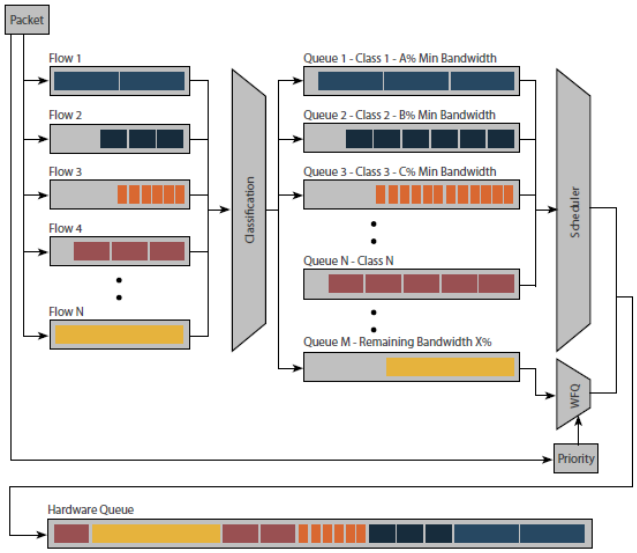


Рисунок 2.6 − Зважені справедливі черги на основі класів

6. Черговість з низькою затримкою (Low Latency Queuing, LLQ) можна розглядати як механізм CBWFQ з пріоритетною чергою PQ (LLQ = PQ + CBWFQ) (рис. 2.7).

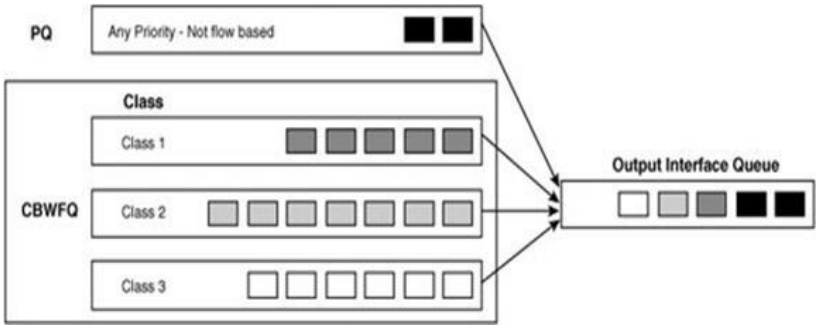


Рисунок 2.7 − Черговість з низькою затримкою LLQ

PQ в LLQ дозволяє забезпечити обслуговування чутливого до затримки трафіку. LLQ рекомендується в разі наявності голосового (VoIP) трафіку. Крім того, він добре працює з відео-конференціями.

2.3 Забезпечення якості MCM на базі протоколів RTP/RTCP

Протокол RTP був розроблений IETF (RFC 1889) для перенесення в реальному часі мовної та відеоінформації по мережі з комутацією пакетів. Передача пакетів RTP ведеться поверх протоколу UDP, що працює, в свою чергу, поверх IP. Протокол RTP передбачає індикацію типу корисного навантаження і порядкового номера пакета в потоці, а також застосування тимчасових міток. Відправник позначає кожен RTP-пакет тимчасової міткою, одержувач витягує її і обчислює сумарну затримку. Різниця в затримці різних пакетів дозволяє визначити джиттер і пом'якшити його вплив − все пакети будуть видаватися з додатком з однаковою затримкою.

Протокол RTP передбачає такі функції.

1. Ідентифікація відправника − кожен RTP-пакет містить ідентифікатор відправника, який вказує, хто з учасників генерує дані.

2. Ідентифікація типу корисного навантаження − спеціальне поле ідентифікує формат трафіку RTP і визначає його інтерпретацію додатком. Типи корисного навантаження RTP наведені в таблиці 2.1.

3. Визначення порядку і моменту декодування кожного пакету. На стороні-відправника кожному вихідному пакету присвоюється тимчасова мітка і порядковий номер. На приймаючій стороні ці дані вказують на те, в якій послідовності і з якими затримками їх необхідно відтворювати, а також дозволяють інтерполювати втрачені пакети.

4. Виявлення втрачених пакетів − порядкові номери роблять можливим і це.

5. Синхронізація − використання тимчасових міток робить можливим синхронне відтворення мультимедійних даних.

Таблиця 2.1 – Типи корисного навантаження аудіо та відео в RTP

Ідентифікатор типу	Кодек	Частота дискретизації, Гц	Опис
0	PCMU	8000	ITU G.711 PCM μ-Law Audio 64 Kbps
1	1016	8000	CELP Audio 4.8 Kbps
2	G721	8000	ITU G721 ADPCM Audio 32 Kbps
3	GSM	8000	European GSM Audio 13 Kbps
5	DVI4	8000	DVI ADPCM Audio 32 Kbps
6	DVI4	16000	DVI ADPCM 64 Kbps
7	LPC	8000	Experimental LPC Audio
8	PCMA	8000	ITU G.711 PCM A-Law Audio 64 Kbps
9	G722	8000	ITU G.722 Audio
10	L16	44100	Linear 16-bit Audio 705.6 Kbps
11	L16	44100	Linear 16-bit Stereo Audio 1411.2 Kbps
14	MPA	90000	MPEG-I or MPEG-II Audio Only
15	G728	8000	ITU G.728 Audio 16 Kbps
25	CELB	90000	CelB Video
26	JBEG	90000	JBEG Video
28	NV	90000	nv Video
31	H261	90000	ITU H.261 Video
32	MPV	90000	MPEG-I and MPEG-II Video
33	MP2T	90000	MPEG-II transport stream Video

Пакет RTP включає до свого складу фіксований заголовок, необов'язкове розширення заголовка змінної довжини і поле даних (рис. 2.8).

Пакет RTP складається, як мінімум, з 12 байтів. У двох перших бітах RTP заголовка (поле біта версії, V) вказується версія протоколу IP (в даний час це версія 2). Наступне за ними поле містить два біта: біт P, який вказує, чи були додані в кінці поля з корисним навантаженням символи-наповнювачі (вони зазвичай додаються, якщо транспортний протокол або алгоритм кодування вимагає використання блоків фіксованого розміру), і біт X, який вказує, чи використовується розширений заголовок. Якщо він використовується, то перше слово розширеного заголовка містить загальну довжину розширення. Далі, чотири біта CC визначають число CSRC-полів в кінці RTP-заголовка, тобто число джерел, які формують потік. Маркерний біт M дозволяє наголошувати істотні події, наприклад, початок відеокадра, початок слова в аудіоканали і т.п. За ним слідує поле типу даних PT (7 бітів), де вказується код типу корисного навантаження, що визначає вміст поля корисного навантаження − дані додатки {Application Data), наприклад, нестиснене 8-бітове аудіо MP3 і т.п. За цим кодом застосунок може дізнатися, що потрібно робити, щоб декодувати дані.

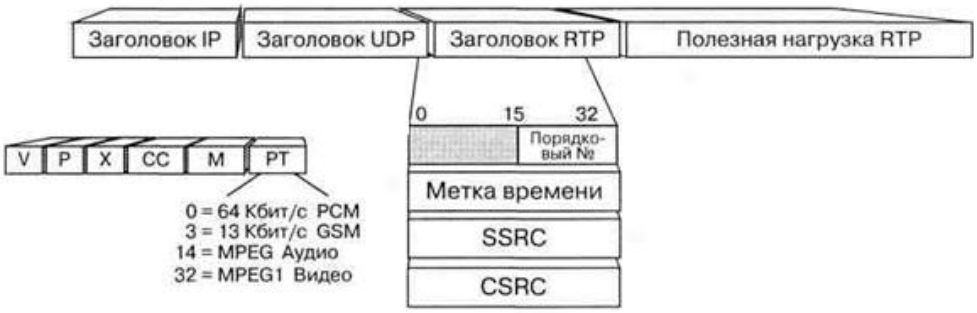


Рисунок 2.8 – Структура пакета RTP

Інша частина заголовка фіксованої довжини складається з поля порядкового номера (Sequence Number), поля мітки часу (Time Stamp) для запису моменту створення першого слова пакета і поля джерела синхронізації SSRC, яке ідентифікує це джерело. В останньому полі можна вказувати єдиний пристрій, що має тільки одну мережеву адресу, множинні

джерела, які можуть представити різні мультимедійні середовища (аудіо, відео і т.д.), або різні потоки одного і того ж середовища. Так як джерела можуть бути на різних пристроях, SSRC-ідентифікатор вибирається випадковим чином, щоб шанс отримувати дані відразу від двох джерел під час RTP-сеанса був мінімальним. Однак визначено також і механізм вирішення конфліктів, якщо вони виникають. За фіксованою частиною RTP-заголовка можуть слідувати ще до 15 окремих 32-розрядних CSRC-полів, які ідентифікують джерела даних.

2.3.1 Протокол Real Time Control Protocol

Доставка RTP-пакетів контролюється спеціальним протоколом RTCP (Real Time Control Protocol). Протокол RTCP передає відомості (як від приймача, так і від відправника) про кількість переданих і втрачених пакетів, значенні джіттера, затримки і т.д., підтримуючи зв'язок між відправником і отримувачем шляхом обміну пакетами − звіт приймача і звіт джерела. RTCP завжди використовується разом з RTP для контролю якості і для передачі інформації про учасників існуючої сесії. Повідомлення RTCP несе таку інформацію, як число переданих та отриманих пакетів, число втрачених пакетів, величини затримки і варіації затримки (джіттер).

Протокол RTCP виконує чотири основні функції.

1. Головна функція − це забезпечення зворотного зв'язку для оцінки якості розподілу даних. Це невід'ємна функція RTP, як транспортного протоколу, вона пов'язана з функціями управління потоком і перевантаженнями інших транспортних протоколів. Зворотний зв'язок з одержувачами також важливо мати для діагностики дефектів при поширенні інформації. Посилка звітів зворотного зв'язку про прийом даних всім учасникам дозволяє при спостереженні проблем, оцінювати, чи є вони локальними або глобальними. З механізмом розподілу IPM для таких об'єктів, як постачальники послуг мережі, можливо також отримувати інформацію зворотного зв'язку і діяти в якості монітору третьої сторони при

діагностиці проблем мережі. Ця функція зворотного зв'язку забезпечується звітами відправника і приймача RTCP.

2. RTCP підтримує стійкий ідентифікатор джерела даних RTP на транспортному рівні, званий «канонічним ім'ям» (CNAME − canonical name). Так як ідентифікатор SSRC може змінюватися, якщо виявлений конфлікт або перезапущено програма, то одержувачам для відстеження кожного учасника вимагає канонічне ім'я CNAME. Одержувачі також вимагають CNAME для відображення безлічі потоків інформації від даного учасника на безліч пов'язаних сеансів RTP, наприклад, при синхронізації звукового та відеосигналу.

3. Перші дві функції вимагають, щоб всі учасники надсилали пакети RTCP, отже, для надання можливості масштабування числа учасників протоколом RTP повинна регулюватися частота передачі таких пакетів. При посилці кожним учасником телеконференції керуючих пакетів всім іншим учасникам, кожен може незалежно оцінювати загальне число учасників. Це число використовується при обчисленні частоти відправлення пакетів.

4. Четверта, додаткова функція, RTCP повинен забезпечувати інформацію управління сеансом (наприклад, ідентифікацію учасника), яка буде відображена в інтерфейсі користувача. Найбільш ймовірно, що це буде корисним в «вільно керованих» сеансах, де учасники вступають в групу і виходять з неї без контролю приналежності або узгодження параметрів.

Щоб забезпечити виконання всіх цих функцій, учасники сеансу обмінюються спеціальними керуючими повідомленнями протоколу RTCP, розглянутими нижче.

1. Пакети звіту RTCP, що забезпечують зворотний зв'язок − оцінку якості прийому, можуть брати одну з двох форм в залежності від того, є отримувач також і відправником чи ні: Report (RR) або Sender Report (SR).

1.1 Звіт відправника − Receiver Report (RR). Ці пакети створюються учасниками сеансу, які не є активними відправниками. Вони містять таку інформацію, як підтвердження отримання пакетів, дані про

розсинхронизацію вхідних пакетів і затримку, пов'язану з підтвердженням прийому. На рисунку 2.9 представлена структура RTCP пакета звіту відправника.

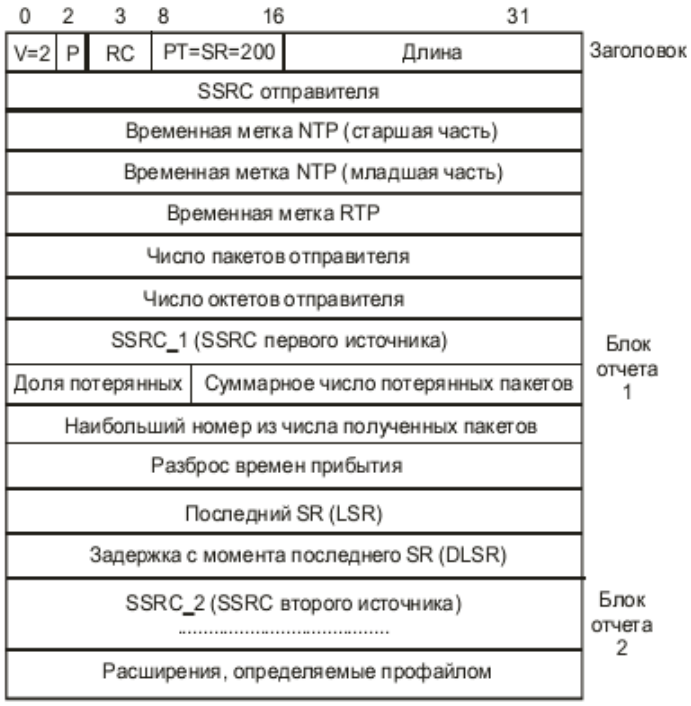


Рисунок 2.9 – Формат RTCP пакета звіту відправника

1.2 Звіт одержувача − Sender Report (SR). SR передається, якщо учасник сеансу посилав будь-які пакети даних протягом інтервалу, починаючи з передачі останнього або попереднього звіту, в іншому випадку передається RR. Єдина відмінність між формами звіту відправника і звіту одержувача, крім коду типу пакета, − це те, що звіт відправника включає 20-байтовий розділ інформації відправника для використання активними відправниками. Цей розділ включає дані про внутрішню аудіовізуальну синхронізації і кількості відправлених пакетів і байтів. На рисунку 2.10 представлена структура RTCP пакета звіту одержувача.

Рисунок 2.10 – Формат RTCP пакета звіту одержувача

2. Пакет опису джерела − Source Description Items (SDES). Пакети цього типу містять інформацію про учасників сеансу. На рисунку 2.11 представлена структура RTCP пакета опису джерела.

Рисунок 2.11 – Формат RTCP пакета опису джерела

3. Пакет завершення зв'язку − BYE. Це «прощальний» пакет, за допомогою якого користувач відключається від сеансу. На рисунку 2.12 представлена структура RTCP пакета завершення зв'язку.

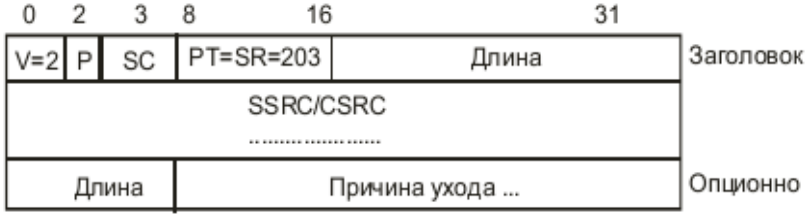


Рисунок 2.12 – Формат RTCP пакета завершення зв'язку

4. Пакет, який визначається застосункам − APP. Пакет APP призначений для експериментального використання при розробці нових додатків і програмних засобів без реєстрації нової величини типу пакета. Пакети APP з нерозпізнаними іменами повинні ігноруватися. Після випробування, якщо виправдано більш широке використання, рекомендується, щоб кожен пакет APP був перевизначений без полів підтипу і імені та зареєстрований в IANA з виділенням для нього нового типу пакета RTCP. У пакет входять відомості про специфічні функції програми. На рисунку 2.13 представлена структура RTCP пакета, що задається застосунком.

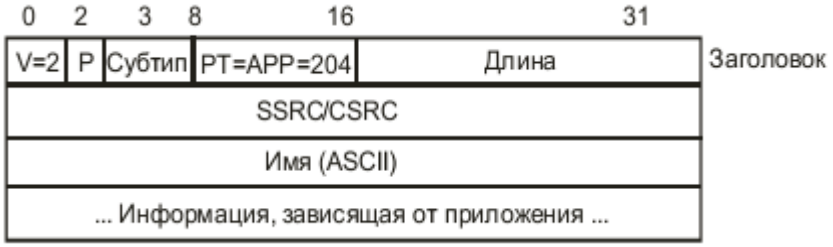


Рисунок 2.13 – Формат RTCP пакета, що задається застосунком

Розглянемо функціонування проколів RTP / RTCP на прикладі такого трафіку реального часу, як аудіо-конференцзв'язок і відео-конференцзв'язок.

Для організації групового аудіо-конференцзв'язку потрібно багато користувачів групового адреса і два порти. При цьому один порт необхідний для обміну звуковими даними, а інший використовується для пакетів управління протоколу RTCP. Інформація про груповий адрес і порти передається ймовірним учасникам телеконференції. Якщо потрібно секретність, то інформаційні та керуючі пакети можуть бути зашифровані, в цьому випадку також повинен бути згенерований і розподілений ключ шифрування.

Застосунок аудіо-конференцзв'язку, що використовується кожним учасником конференції, посилає звукові дані малими порціями, наприклад, тривалістю 20 мс. Кожній порції звукових даних передує заголовок RTP і

дані по черзі формуються (інкапсулюються) в пакет UDP. Заголовок RTP показує, який тип кодування звуку (наприклад, ІКМ, АДІКМ або LPC) використовувався при формуванні даних в пакеті. Це дає можливість змінювати тип кодування в процесі конференції, наприклад, при появі нового учасника, який використовує лінію зв'язку з низькою пропускною здатністю, або при перевантаженнях мережі.

У мережі Internet, як і в інших мережах передачі даних з комутацією пакетів, пакети іноді губляться і змінюються порядок їх надходження, а також вони можуть затримуватися на різний час. Для протидії цим подіям заголовок RTP містить тимчасову мітку і порядковий номер, які дозволяють одержувачам відновити синхронізацію в початковому вигляді так, щоб, наприклад, ділянки звукового сигналу відтворювалися динаміком безперервно кожні 20 мс. Ця реконструкція синхронізації проходить окремо і незалежно для кожного джерела пакетів RTP в аудіо-конференції. Порядковий номер може також використовуватися одержувачем для оцінки кількості втрачених пакетів. Так як учасники аудіо-конференції можуть вступати і виходити з неї під час її проведення, то корисно знати, хто бере участь в ній в даний момент, і як добре учасники конференції отримують звукові дані. Для цієї мети кожен екземпляр звукового застосунка під час конференції періодично видає на порт управління (порт RTCP) для застосунків усіх інших учасників повідомлення про прийом пакетів із зазначенням імені свого користувача. Повідомлення про прийом вказує, як добре чуємо поточний оратор, і може використовуватися для управління адаптивними кодерами. На застосунок до імені користувача, може бути включена також інша інформація ідентифікації для контролю смуги пропускання. При виході з конференції сайт посилає пакет BYE протоколу RTCP.

Відео-конференцзв'язок. Якщо в аудіо-конференції використовуються і звукові, і відеосигнали, то вони передаються окремо. Для передачі кожного типу трафіку незалежно від іншого специфікацією протоколу вводиться

поняття сеансу зв'язку RTP. Сеанс визначається конкретної парою транспортних адресів призначення (одна мережева адреса плюс пара портів для RTP і RTCP). Пакети для кожного типу трафіку передаються з використанням двох різних пар портів UDP і / або групових адрес. Ніякого безпосереднього з'єднання на рівні RTP між аудіо- та відео-сеансами зв'язку немає, за винятком того, що користувач, який бере участь в обох сеансах, повинен використовувати одне і те ж канонічне ім'я в RTCP-пакетах для обох сеансів так, щоб сеанси могли бути пов'язані. Одна з причин такого поділу полягає в тому, що деяким учасникам конференції необхідно дозволити отримувати тільки один тип трафіку, якщо вони цього бажають. Незважаючи на поділ, синхронне відтворення мультимедійних даних джерела (звуку і відео) може бути досягнуто при використанні інформації таймування, яка переноситься в пакетах RTCP для обох сеансів.

Слід зазначити, що протокол RTP/RTCP сам по собі не забезпечує якості послуг (QoS) і не гарантує коректну доставку даних.

2.3.2 Моделі зворотного зв'язку для протоколу RTCP

Завдяки многоадресній природі протоколів RTP/RTCP, всі учасники сеансу передачі мультимедійних даних отримують звіти зворотного зв'язку інших учасників і, таким чином, кожен з них може оцінити загальний і індивідуальне якість прийому і передачі під час сеансу зв'язку, а саме: оцінити швидкість даних, рівень загублених пакетів і рівень нерівномірності передачі. Хоча трафік RTCP передається таким чином, що його частка в RTP-сеансі не перевищує 5%, проте, це може призвести до двох проблем.

По-перше, зростання щільності мультимедійного трафіку призводить до зменшення RTCP-трафіку і, як результат, знижує ймовірність своєчасної реакції учасників сеансу на зміну умов передачі. По-друге, в разі, якщо частка службового широкомовного трафіка перевищує 5%, то щоб уникнути широкомовного шторму RTCP пакети відкидаються. Останнє хоча і не призводить до безпосереднього погіршення якості передачі даних, проте веде

до втрати службової інформації, яка може стати корисною для поліпшення якості передачі IP-пакетів.

Таким чином, зниження рівня многоадресного RTCP-трафіку, яке дозволить уникнути перевантажень в мережі і зберегти вихідну функціональність RTCP, є досить актуальним завданням.

В якості вирішення згаданого вище завдання пропонується проста модель зворотного зв'язку [27]. Проста модель зворотного зв'язку (рис. 2.14) − базовий механізм «відображення» RTCP-трафіку, де кожен учасник сеансу передачі мультимедійних даних відсилає широкомовним чином спеціальний пакет зворотного зв'язку, а, так званий, звіт одержувача (англ. Receiver Report, RR), до цільового вузла зворотного зв'язку (англ. Feedback Target), який пересилає дані звіти в початковому вигляді до джерела розсилки (англ. Distribution Source). Далі, джерело розсилки «відображає» звіти одержувача широкомовним чином всім учасникам сеансу передачі даних.

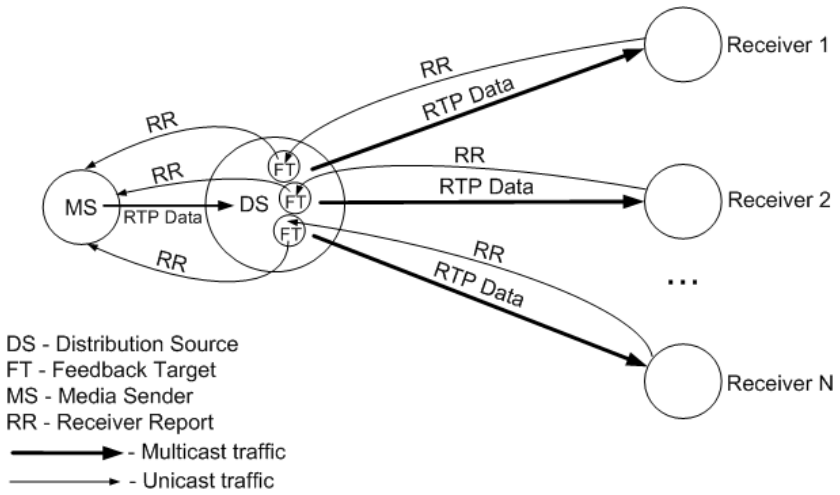


Рисунок 2.14 – Проста модель зворотного зв'язку

Перевага даного методу полягає в тому, що для його використання існуюча реалізація модуля одержувача вимагає лише незначної модифікації. Замість розсилки звітів по груповій адресі, одержувач використовує одноадресну передачу, в той же час отримуючи «відбитий» RTCP-трафік широкомовним чином.

Таким чином, механізм «відображення» є непоганою альтернативою комунікаційному каналу «багато до багатьох», але в той же час, використання односпрямованого каналу призводить до іншої проблеми − обмеження за кількістю з'єднань і значного скорочення масштабованості для великих мультимедійних сеансів (наприклад, IPTV). Більш того, пересилання всіх звітів одержувача від кожного учасника сеансу мультимедійної передачі даних по односпрямованому каналу неефективна. Наприклад, в разі обчислення тимчасових міток RTP, які можуть бути корисні тільки джерелу мультимедійних даних, немає ніякої необхідності пересилати їх до групи учасників мультимедіа-сеансу [28].

Крім простої моделі зворотного зв'язку, в області оптимізації трафіку зворотного зв'язку протоколу RTP є і інші моделі і методи зворотного зв'язку:

- метод резюмування;
- фільтрування зворотного зв'язку;
- алгоритм зсуву;
- ієрархічне агрегування зворотного зв'язку.

Заключна модель зворотного зв'язку джерела розсилки − схема зведеної звітності, що забезпечує економічне використання пропускної здатності шляхом збору звітів одержувача джерелом розсилки. Така модель може бути реалізована за допомогою цільового вузла зворотного зв'язку, в зведені (підсумкові) пакети потім розсилаються всім одержувачам (рис. 2.15).

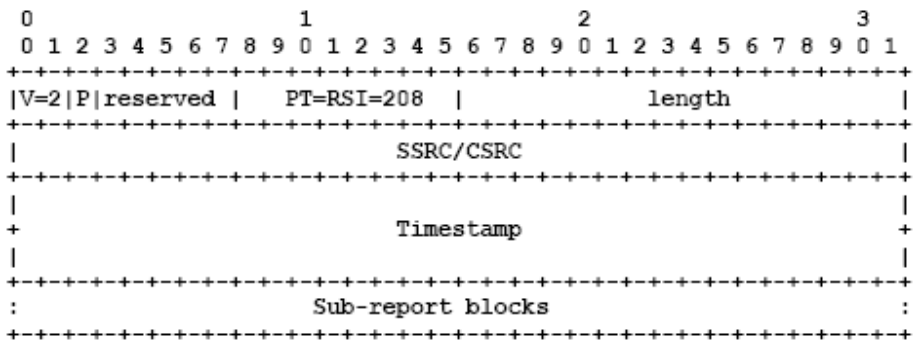


Рисунок 2.15 – Структура пакета RTCP-RSI (Report Summary Information)

Перевага використання останньої схеми найкраще проявляється в сеансах передачі мультимедійного трафіку для великих груп, в яких при використанні механізму «відображення» RTCP-трафіку, описаного раніше, має місце генерація значного числа пакетів, що пересилаються під час реплікації всієї інформації на всіх одержувачів. Ясно, що метод резюмування вимагає, щоб всі учасники сеансу розуміли новий формат зведеного пакета (рис. 2.16). До того ж, резюмуюча схема надає оптимальний механізм розсилки інформації про дані зворотного зв'язку, викладених всією групою, у вигляді значень розподілу або гістограми.

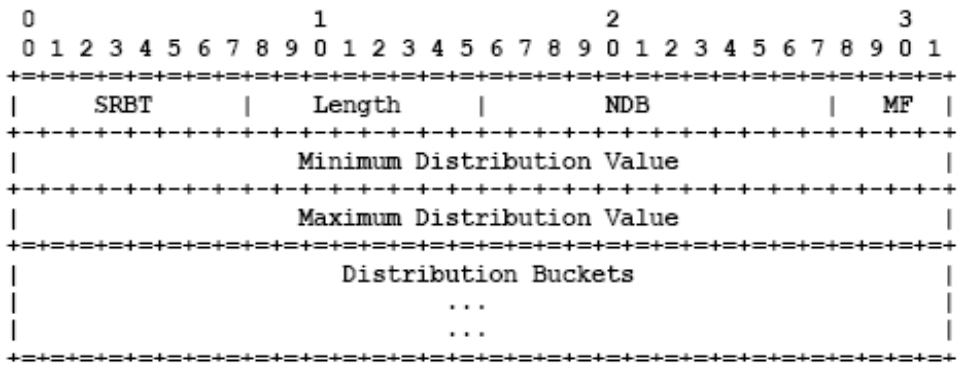


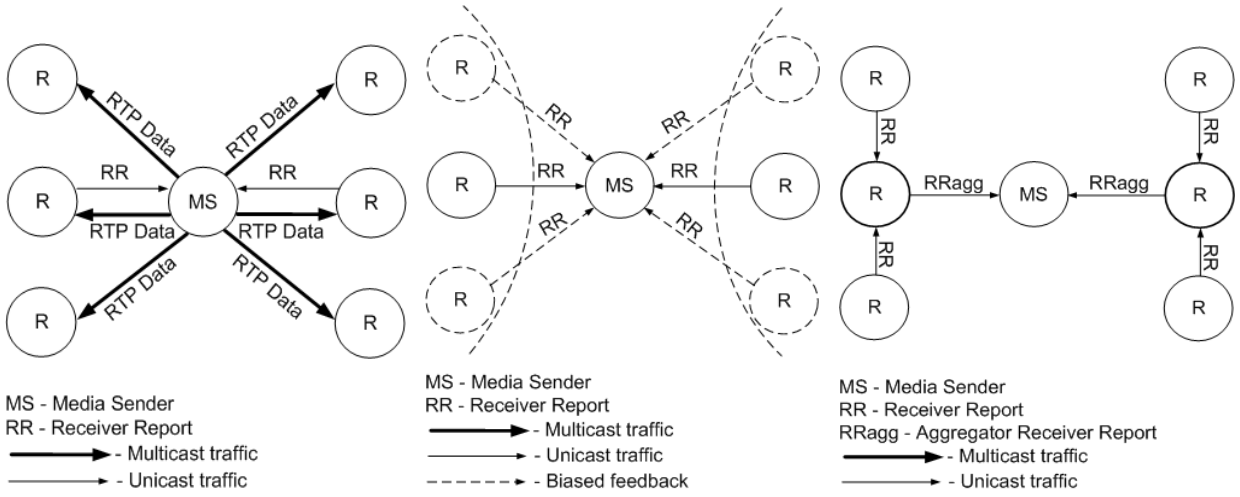
Рисунок 2.16 – Загальна форма блоку звіту

Для однозначного розпізнавання кожного з розглянутих методів розсилки звітів вводиться новий ідентифікатор SDP. Причому, метод розсилки звітів повинен бути обраний перед початком сеансу передачі мультимедійних даних і повинен залишатися незмінним протягом усього сеансу.

До недоліку резюмування можна віднести те, що деяка інформація зворотного зв'язку, орієнтована на одержувача, така як відображення значень зворотного зв'язку в мережеві адреси, більше одержувачам недоступна. Але для великих груп (які передбачаються для IPTV-сервісу, наприклад) підсумкові звіти як індикатори групових явищ більш корисні, ніж індивідуальні звіти одержувача. Таким чином, резюмування ще і забезпечує можливість реалізації функцій моніторингу та налагодження мультисервісної

мережі, які в свою чергу можуть бути доповнені персоналізованими звітами, якщо такі потрібні в заданих умовах функціонування мережі.

Модель зворотного зв'язку з фільтруванням (рис. 2.17 (а)) базується на концепції, згідно з якою в організації зворотного зв'язку медіа-сервера з одержувачами будуть задіяні тільки деякі, так звані виділені, учасники сеансу передачі мультимедійних даних. Тут основним завданням, що вимагає рішення, є коректний з точки зору значущості для якості сеансу зв'язку і повноти покриття вибір виділених учасників мультимедіа-сеансу.



(а) (б) (в)

Рисунок 2.17 – Моделі зворотного зв'язку:

а) з фільтруванням; б) зі зміщенням; в) з ієрархічним агрегуванням

Метод зсуву (рис. 2.17 (б)) досить схожий на реалізацію зворотного зв'язку з фільтруванням і також базується на виборі ряду учасників сеансу передачі мультимедійних даних в якості виділених. Однак, на відміну від моделі зворотного зв'язку зі зміщенням, тут звіти одержувачів відсилаються джерела RTP-трафіку від всіх учасників сеансу, але трафік зворотного зв'язку від виділених учасників є більш пріоритетним і інтенсивність його передачі не залежить від ширини смуги пропускання, займаної трафіком даних мультимедіа. Таким чином, результати даного методу більш об'єктивні.

Більш того, підгрупа виділених учасників може бути реорганізована у відповідності зі значимістю поведінки іншої частини групи учасників сеансу.

Однак, зазначений алгоритм чутливий до варіабельності розмірів зміщених груп внаслідок мобільності учасників сеансу передачі мультимедійних даних (приходу нових і підтримки старих членів групи), а також до високої динамічності значень зворотного зв'язку членів зміщеною групи. Обидва явища впливають не тільки на точність алгоритму зсуву, але і на стандартний RTCP.

Для масштабних сеансів передачі мультимедійних даних більш кращий метод ієрархічного агрегування (рис. 2.17 (в)). Він базується на концепції, в якій дані зворотного зв'язку не надсилаються безпосередньо джерелу мультимедіа даних від кожного учасника сеансу, а виконується розбиття всіх учасників сеансу на підгрупи, переважно рівні, в кожній підгрупі вибирається один учасник, так званий агрегатор, який і є відповідальним за збір звітів від кожного члена підзвітною йому підгрупи і передачу даних зворотного зв'язку джерела трафіку RTP.

Реалізація ієрархічного агрегування також може бути представлена в багаторівневому вигляді і розширюватися до практично будь-яких розмірів. Єдине завдання, яке необхідно вирішити, полягає у виборі відповідних агрегаторів.

Головний недолік ієрархічного агрегування полягає в додаткових тимчасових витратах на передачу даних зворотного зв'язку. Інший недолік полягає в тому, що даний механізм залежить від ефективного розміщення агрегаторів і гарантії відсутності недоліків топології, яка закладається ще на етапі проектування комп'ютерної мережі. Наприклад, до серйозних наслідків може привести зациклення шляху проходження через комутатори.

У світлі сказаного вище, можна визначити ряд проблем, властивих в даний час процесу передачі трафіку в реальному масштабі часу за допомогою використання протоколів RTP/RTCP. Використання багатоадресної розсилки, що є природним типом трафіку для RTP, в разі передачі керуючого трафіку і

трафіку зворотного зв'язку може призвести до неоптимальному використання смуги пропускання корисним потоком даних. Використовуваний механізм масштабування з метою управління завантаженістю може привести до того, що при високій інтенсивності передачі трафіку і великій кількості учасників передачі дані, що переносяться пакетами RTCP, в момент доставки вже можуть втратити свою актуальність.

Тому стає актуальним використання модифікованого механізму зворотного зв'язку з метою підвищення його адаптивності і зниження навантаження на мережу.

2.3.3 Розширена модель зворотного зв'язку RTCP

Відповідно до стандарту RFC 3550, в процесах передачі групового RTCP-трафіку може брати участь третя сторона, яка називається монітором, яка необов'язково бере участь в мультимедіа сесії, але виконує збір та аналіз RTCP-звітів на предмет оцінки стану каналів зв'язку сесії, а також накопичує статистику по даними RTCP-звітів в тренді.

Таким чином, з метою скорочення групового трафіку RTCP, що генерується звітами одержувачів (Receiver Reports, RR) і відправників (Sender Reports, SR) в централізовану архітектуру MCM можна ввести поняття діагностичного вузла (ДВ), не знижуючи ефективності механізмів зворотного зв'язку і діагностування.

На рисунку 2.18 вершина DN позначає діагностичний вузол, S − джерело RTP-трафіку в поточний момент часу, R1 ... Rn − вузли-одержувачі RTP-трафіку в поточний момент часу, RR − Receiver Report (звіт одержувача), SR − Sender Report (звіт відправника), DNR − Diagnostic Node Report (звіт діагностичного вузла).

Діагностичний вузол може бути реалізований як додатковий сервіс на пристрої управління MCM (в даному випадку, на вузлі модератора сесії).

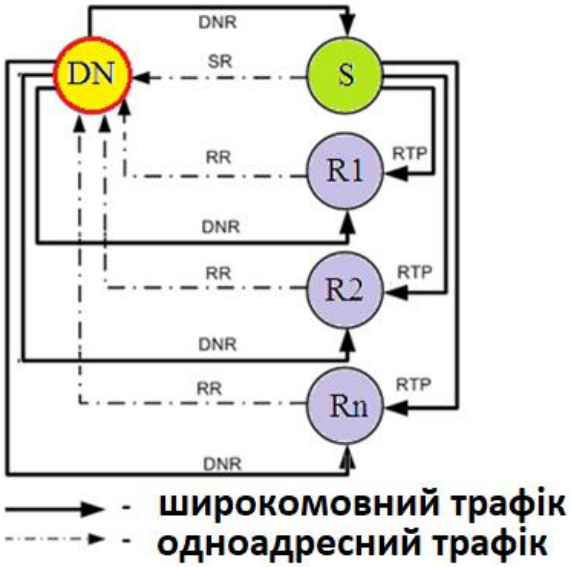


Рисунок 2.18 – Схема впровадження ДВ в централізовану архітектуру МСМ

Як видно з рисунку 2.18, приймаючи звіти (пакети SR і RR) від усіх вузлів-учасників RTP-сесії одноадресним чином, ДУ виконує їх обробку і формує з них пакет DNR, який потім розсилається стандартним для RTCP-трафіку чином всім учасникам RTP-сесії.

В даному випадку було прийнято рішення відмовитися від використання складеного пакета RTCP, рекомендованого стандартом, так як в подальшому планується застосування методів статистичної обробки даних, відправлених в RTCP-звітах і розсилка в пакетах DNR результатів цієї обробки, а не сукупності «сирих» пакетів RTCP, як показано зараз. Застосування методів статистичної обробки дозволить реалізувати поліпшені функції діагностики і моніторингу в рамках сесії, а також скоротити обсяг даних, що пересилаються за зворотнім зв'язком як за рахунок видалення надлишкових службових заголовків IP і UDP, так і за рахунок більш компактного представлення інформації в блоках звітів.

Пакет DNR включає в себе заголовок DNR, службові поля (в тому числі і ідентифікатори) і блоки звітів SR і RR, кожен з яких відправлений діагностичному вузлу одноадресним чином (рисунок 2.19).

Пакети RTCP типів SDES, BYE і APP у запропонованій моделі зворотного зв'язку не розглядаються і в пакет DNR не включаються. Це пов'язано з тим, що дані пакети характеризуються невеликим розміром, невисокою частотою передачі і некритичні для вирішення завдання статистичної обробки даних з метою диференціювання інтервалу посилки звітів. Тому, звіти RTCP перерахованих вище типів, їх формат і поведінку, у запропонованої моделі залишаються без змін і відповідають стандартному опису.

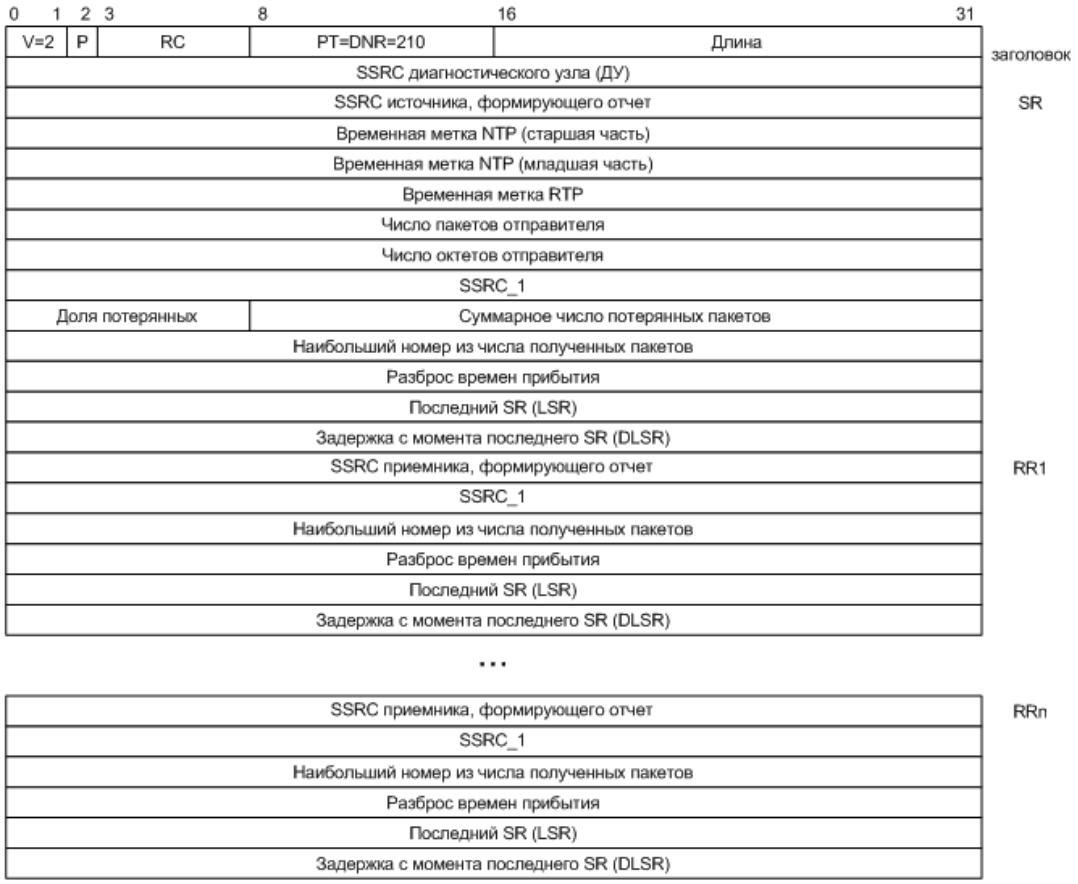


Рисунок 2.19 – Формат пакета DNR для зв'язку з одним джерелом

2.3.4 Аналіз ефективності розширеної моделі RTCP

Для оцінки ефективності моделі зворотного зв'язку RTCP з ДВ розрахуємо утилізацію (або обсяг трафіку) в рамках одного інтервалу посилки звітів для МСМ при організації зворотного зв'язку RTCP відповідно до стандарту RFC 3550 і при впровадженні ДВ з формуванням пакета DNR.

Розрахунок утилізації буде виконуватися тільки для тих елементів моделі зворотного зв'язку RTCP, формат чи характер передачі яких зазнали змін у запропонованій моделі. Такими елементами є пакети звітів SR, RR і DNR. Утилізація буде розраховуватися для випадку максимального завантаження смуги пропускання пакетами RTCP протягом інтервалу посилки звітів, коли кожен учасник сесії MCM відправляє звіт.

Розрахунок утилізації для моделі зворотного зв'язку RTCP без введення ДВ:

$$U_{SR} = m * (n-1) * PL_{SR}, \quad (2.1)$$

$$U_{RR} = (n-m) * (n-1) * PL_{RR}, \quad (2.2)$$

$$U_1 = U_{SR} + U_{RR}, \quad (2.3)$$

де n − загальна кількість учасників мультимедійної сесії, m − число медіа-серверів або активних учасників мультимедійної сесії; PL_{SR}, PL_{RR} і PL_{DNR} − довжини пакетів SR, RR і DNR відповідно.

Розрахунок утилізації для моделі зворотного зв'язку з введенням ДВ:

$$U_{SR} = m * PL_{SR}, \quad (2.4)$$

$$U_{RR} = (n-m) * PL_{RR}, \quad (2.5)$$

$$U_{DNR} = n * PL_{DNR}, \quad (2.6)$$

$$U_2 = U_{SR} + U_{RR} + U_{DNR}, \quad (2.7)$$

де n − загальна кількість учасників мультимедійної сесії, m − число медіа-серверів або активних учасників мультимедійної сесії, PL_{SR}, PL_{RR} і PL_{DNR} – довжини пакетів SR, RR і DNR відповідно.

Для мережі централізованої архітектури з модерацією m = 1 в будь-який момент часу, тому формули розрахунку утилізації можна звести до наступного вигляду:

– модель зворотного зв'язку RTCP без введення ДВ:

$$U_{SR} = (n-1) * PL_{SR}, \quad (2.8)$$

$$U_{RR} = (n-1)^2 * PL_{RR}, \quad (2.9)$$

$$U_1 = U_{SR} + U_{RR}; \quad (2.10)$$

– модель зворотного зв'язку з введенням ДВ:

$$U_{SR} = PL_{SR}, \quad (2.11)$$

$$U_{RR} = (n-1) * PL_{RR}, \quad (2.12)$$

$$U_{DNR} = n * PL_{DNR}, \quad (2.13)$$

$$U_2 = U_{SR} + U_{RR} + U_{DNR}. \quad (2.14)$$

Виконаємо розрахунок значень PL_{SR}, PL_{RR} та PL_{DNR}:

– PL_{SR} = *заголовок Eth (14 байт) + заголовок IP (20 байт) + заголовок UDP (8 байт) + заголовок SR (8 байт) + тіло SR (44 байта)* = 94 байта,

– PL_{RR} = *заголовок Eth (14 байт) + заголовок IP (20 байт) + заголовок UDP (8 байт) + заголовок RR (8 байт) + тіло RR (24 байта)* = 74 байта,

– PL_{DNR} = *заголовок Eth (14 байт) + заголовок IP (20 байт) + заголовок UDP (8 байт) + заголовок DNR (8 байт) + SSRC SR (4 байта) + тіло SR (24 байта) + SSRC RR1 (4 байта) + тіло RR1 (24 байта) + SSRC RR2 (4 байта) + тіло RR2 (24 байта) + … + SSRC RRn (4 байта) + тіло RRn (24 байта) = 78 + 4*(n-m) + 24*(n-m)* = 78 + 28*(n-1) байт.

При підстановці отриманих значень PL_{SR}, PL_{RR} і PL_{DNR} в формули (2.8 – 2.14) утилізація для стандартної моделі зворотного зв'язку RTCP приймає наступний вигляд:

$$U_1 = U_{SR} + U_{RR} = (n-1) * PL_{SR} + (n-1)^2 * PL_{RR} = 94*(n-1) + 74*(n-1)^2, \quad (2.15)$$

а для запропонованої моделі:

$$U_2 = U_{SR} + U_{RR} + U_{DNR} = PL_{SR} + (n-1) * PL_{RR} + n * PL_{DNR} = \\ = 94 + 74*(n-1) + n*(78 + 28*(n-1)). \quad (2.16)$$

Графіки залежностей обсягу трафіку RTCP від кількості учасників сесії для стандартної моделі зворотного зв'язку RTCP (графік I) і для запропонованої моделі з ДВ (графік II) показані на рисунку 2.20.

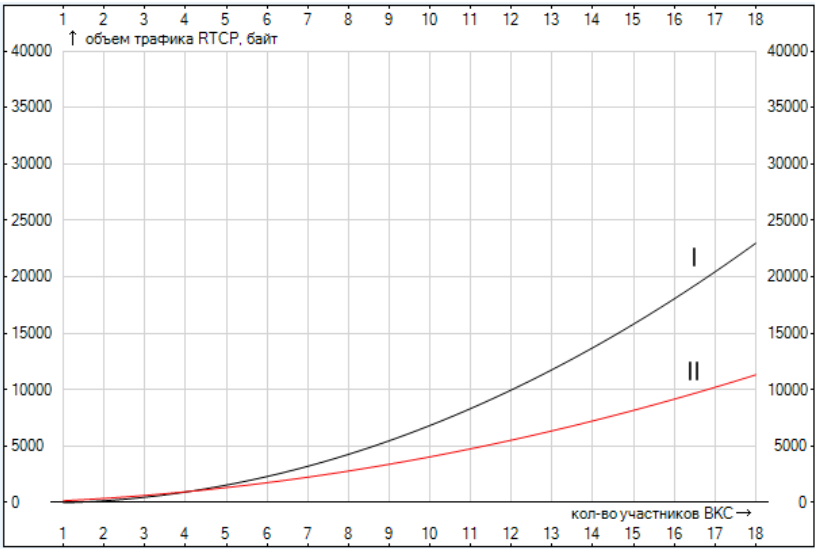


Рисунок 2.20 – Розрахункова залежність обсягу трафіку RTCP (вісь Y) від кількості учасників сесії (вісь X)

З графіка видно, що чим більша кількість учасників сесії МСМ, тим очевидніше проявляється тенденція скорочення обсягу трафіку при використанні запропонованої моделі зворотного зв'язку в порівнянні зі стандартною моделлю. При невеликих розмірах сесії МСМ (n<5) скорочення обсягу трафіку RTCP в запропонованої моделі не спостерігається.

Таким чином, введення діагностичного вузла в модель зворотного зв'язку RTCP для мережі з централізованою архітектурою дозволяє скоротити обсяг групового RTCP-трафіку, наслідком чого буде:

– зменшення інтервалу передачі RTCP-звітів;

– забезпечення адекватної оцінки стану учасників сесії;

– зменшення службового трафіку, і, як наслідок, збільшення пропускної здатності мережі, а та, в свою чергу, є головною складовою продуктивності МСМ.

3 СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ПО ЗАБЕЗПЕЧЕННЮ ЯКОСТІ ПЕРЕДАЧІ ТРАФІКУ РЕАЛЬНОГО ЧАСУ

Під терміном система підтримки прийняття рішень (СППР) зазвичай розуміється інструментарій вироблення рекомендацій для особи, що приймає рішення, на основі ранжування кінцевої множини альтернатив (рішень) або оптимізації їх на нескінченній множині.

В контексті даної атестаційної роботи СППР – це комп'ютерна автоматизована система, метою якої є допомога адміністраторам, які приймають рішення в складних умовах для повного і об'єктивного аналізу якості передачі трафіку в МСМ.

Аналіз літератури [29] показує, що всі численні методи розв'язання багатокритеріальних задач можна звести до трьох груп:

- метод головного показника;
- метод результуючого показника;
- лексикографічні методи (методи послідовних поступок).

Запропонована модель експертного оцінювання оцінка якості МСМ базується на методі результуючого показника якості. Він заснований на формуванні узагальненого показника шляхом інтуїтивних оцінок впливу різних показників якості $q_1, \ldots, q_m$ на результуюче якість виконання системою її функцій (тобто на QoS). Оцінки такого впливу даються фахівцем-експертом (групою експертів), що має досвід розробки подібних систем. Найбільш поширеними показниками якості є: адитивний, мультиплікативний і максиміний показники.

Скористаємося адитивним показником якості, який являє собою суму зважених нормованих показників і має вигляд:

$$Q = \sum_{j=1}^{m} k_j q_j \ , \qquad (3.1)$$

де q_j – нормоване значення j-го показника; k_j – ваговий коефіцієнт j-го показника, який має тим більшу величину, ніж більше він впливає на якість системи:

$$\sum_{j=1}^{m} k_j = 1, \text{ при } k_j > 0 \text{ та } j = \overline{1,m}.$$

Головною особливістю адитивного показника є те, що при його застосуванні може відбуватися взаємна компенсація окремих показників. Це означає, що зменшення одного з показників аж до нульового значення може бути компенсовано зростанням іншого показника.

Розглянемо приклад розрахунку інтегрального (узагальненого) показника якості обслуговування МСМ. Припустимо, є експертні оцінки:

- q1 – оцінка якості доставки пакетів в МСМ [1-100];
- q2 – оцінка продуктивності мережі [1-100];
- q3 – оцінка надійності мережі [1-100].

Тоді інтегральна оцінка якості обслуговування в МСМ, згідно формули (3.1), буде мати наступний вигляд:

$$Q = \sum_{j=1}^{3} k_j \cdot q_j = k_1 \cdot q_1 + k_2 \cdot q_2 + k_3 \cdot q_3, \qquad (3.2)$$

де k_1, k_2, k_3 – вагові коефіцієнти, що визначають ступінь впливу того чи іншого параметра оцінки на якість обслуговування МСМ, за умови, що $k_1 + k_2 + k_3 = 1$.

Розглянемо приклад, коли експертні оцінки стану кожного компонента КС мають таке значення $q_1 = 70$, $q_2 = 40$, $q_3 = 90$, при цьому внесок кожного компонента визначено як $k_1 = 0.7$, $k_2 = 0.2$, $k_3 = 0.1$. тоді

$$Q = 0.7*70 + 0.2*40 + 0.1*90 = 66\,\%.$$

Дотримуючись заздалегідь виробленим рекомендаціям для МСМ, дана оцінка буде говорити про достатній рівень якості обслуговування.

Для аналізу і вироблення пропозицій в СППР використовуються різноманітні методи. Це можуть бути: інформаційний пошук, рішення задач оптимізації, обробка експертних оцінок, інтелектуальний аналіз даних,

міркування на основі прецедентів, імітаційне моделювання, еволюційні обчислення і генетичні алгоритми, нейронні мережі, ситуаційний аналіз, когнітивне моделювання, методи геоінформатики тощо.

У більшості випадків СППР видає рішення на основі аналізу ситуації в даній області, який неможливий без математичного моделювання відповідних процесів.

Розглянемо класифікацію моделей, що використовуються в СППР [30].

1. З точки зору часу моделі поділяються на:

– статичні – описують стан об'єктів, що моделюються без урахування фактору часу;

– динамічні (темпоральні) – розглядають процеси, що протікають у часі.

2. За ступенем структурованості даних моделі поділяються на:

– структуровані – засновані на виявленні регулярної структури предметної області;

– слабоструктуровані – регулярна структура предметної області не визначена або вона не існує в даному випадку;

– формальні – регулярна структура предметної області визначена, але для модельного її подання використовуються формальні мови.

– неструктуровані – вербальні моделі, тобто моделі, які описують реальність у вигляді текстів на природній мові.

В свою чергу структуровані моделі також поділяються на наступні класи.

1. Безперервно-детерміновані моделі (D-схеми), де в якості робочого апарату використовуються диференціальні рівняння. Процеси, що відбуваються в моделях даного типу, залежать від безперервного (фізичного) часу. При цьому всі параметри рівнянь передбачаються точно відомими (детермінованими). Це саме можна сказати і про зовнішні впливи, що також розглядаються у вигляді детермінованих сигналів. Найбільшого поширення

цей вид моделей отримав в теоретичній механіці, механіці суцільних середовищ, а також в класичній теорії автоматичного управління.

2. Дискретно-детерміновані моделі (F-схеми), де час передбачається дискретним, тобто всі процеси, що відбуваються в системі, прив'язуються до послідовності часових кроків, або тактів. Функції стану системи визначаються на множині моментів дискретного часу. Робочим апаратом таких моделей служать різницеві рівняння, що описують стан системи в певний момент часу на основі інформації про стани в попередні моменти дискретного часу. Всі параметри системи і все вхідні впливу, як і в попередньому випадку, передбачаються детермінованими. До цього класу моделей відносять кінцеві автомати (F-автомати). Кінцевий автомат при своїй роботі за певним законом переходить з одного стану в інший залежно від зовнішніх впливів і власного стану в даний і попередні моменти дискретного часу. Найбільш широка область застосування теорії кінцевих автоматів – моделювання цифрових та інших дискретних пристроїв. До даного виду моделей можна віднести також мережі Петрі, які будуть розглянуті нижче.

3. Дискретно-стохастичні моделі (P-схеми), де на відміну від попередніх моделей перехід з одного стану в інший здійснюється випадковим чином. При цьому вже неможливо говорити про те, в якому саме стані знаходиться система, мова йде про розподіл ймовірності перебування в тому чи іншому стані. До таких моделей відносять імовірнісні автомати (P-автомати). Імовірнісний кінцевий автомат при своїй роботі з певною ймовірністю переходить з одного стану в інший залежно від зовнішніх впливів і власного стану в даний і попередні моменти дискретного часу. Прикладом таких автоматів можуть служити моделі, побудовані на формалізмі ланцюгів Маркова, а також мережі Петрі з імовірнісним поведінкою.

4. Безперервно-стохастичні моделі (Q-схеми) розглядаються в безперервному часу, але їх поведінка носить випадковий характер. Найбільш

відомий клас таких моделей представляють собою системи масового обслуговування. Як правило, розглядаються випадкові потоки заявок, що надходять в систему, їх обробка системою. Визначаються, наприклад, такі параметри, як час обслуговування заявок, довжина черги на обслуговування. У термінах систем масового обслуговування вдається описувати багато технологічних і економічних процесів, системи передачі даних, комп'ютерні мережі.

5. Мережеві моделі (N-схеми) використовуються для опису складних систем, що складаються з самостійно працюючих та взаємодіючих підсистем. Найбільш відомими моделями даного виду є мережі Петрі різних модифікацій.

6. Комбіновані моделі (A-схеми) реалізують комбінований підхід до формального опису систем, що включає всі раніше розглянуті види моделей. A-схема повинна одночасно виконувати декілька функцій: бути адекватним математичним описом об'єкта моделювання, служити підставою для побудови алгоритмів і програм при машинній реалізації моделі, виробляти чисельні розрахунки і, бажано, аналітичні дослідження поведінки модельованої системи.

Сучасні системи моделювання, як правило, реалізують комбінований підхід. Вони дозволяють у візуальному режимі описувати модельований об'єкт в будь-якій зручній для дослідника формі (безперервній, дискретній, детермінованій, ймовірнісній, мережевій), а потім проводити в інтерактивному режимі складні дослідження його поведінки, отримуючи інформацію в наочній графічній, табличній або текстовій формі. Прикладами систем моделювання, що реалізують комбінований підхід, є MatLab, MVS, AnyLogic.

В даній атестаційній роботі були обрані мережеві моделі підтримки прийняття рішення, а саме на мережі Петрі. Мережі Петрі були розроблені і використовуються для підтримки прийняття рішень шляхом моделювання і дослідження складних систем. За допомогою різних модифікацій цих мереж

можна описати багато систем, особливо системи з незалежними елементами, наприклад, апаратне і програмне забезпечення ЕОМ, системи телекомунікацій, фізичні, хімічні, економічні, соціальні та інші системи [31].

3.1 Мережева модель підтримки прийняття рішення

Серед мережевих моделей (N-схеми) виділився підхід, заснований на використанні мереж спеціального виду, запропонований Карлом Петрі в 1962 році для моделювання асинхронних інформаційних потоків в системах обробки даних. Ця методологія, що отримала назву мереж Петрі, набула широкого поширення. Розглянемо детальніше використання мереж Петрі при створенні системи підтримки прийняття рішень.

Для опису МСМ достатньо підібрати список діагностичних ознак (ДО), значення яких в повній мірі характеризують її стан. Для забезпечення принципу єдності вимірювань необхідно вибрати об'єктивні показники якості таким чином, щоб вони були добре відомі, однозначно зрозумілі і адекватно передавали загальну картину якості. Найзручніше для цього скористатися низкою рекомендацій Міжнародного союзу електрозв'язку (МСЕ). Так, для широко поширених мереж пакетної комутації на основі IP-протоколу МСЕ випустив рекомендації Y.1221, Y.1540, Y.1541. В рекомендації Y.1540 визначаються об'єктивні показники якості, які слід контролювати при визначенні рівня послуг в мережах IPv4 і IPv6.

Найчастіше знання експертів, які відображають їх професійний досвід, накопичений в процесі діяльності в області технічної діагностики та адміністрування мереж, існують у фахівця підсвідомо. Саме цей факт і зумовив вибір нечіткої логіки в якості алгоритму логічного висновку для роботи СППР, структура якої представлена на рисунку 3.1. Згідно зі структурою на рис. 3.1 до складу СППР входять блоки фазифікації та дефазифікації. В ході фазифікації фіксований вектор діагностичних

параметрів перетворюється у вектор нечітких множин, а в ході дефазифікації вихідна нечітка множина перетворюється у чітке число.

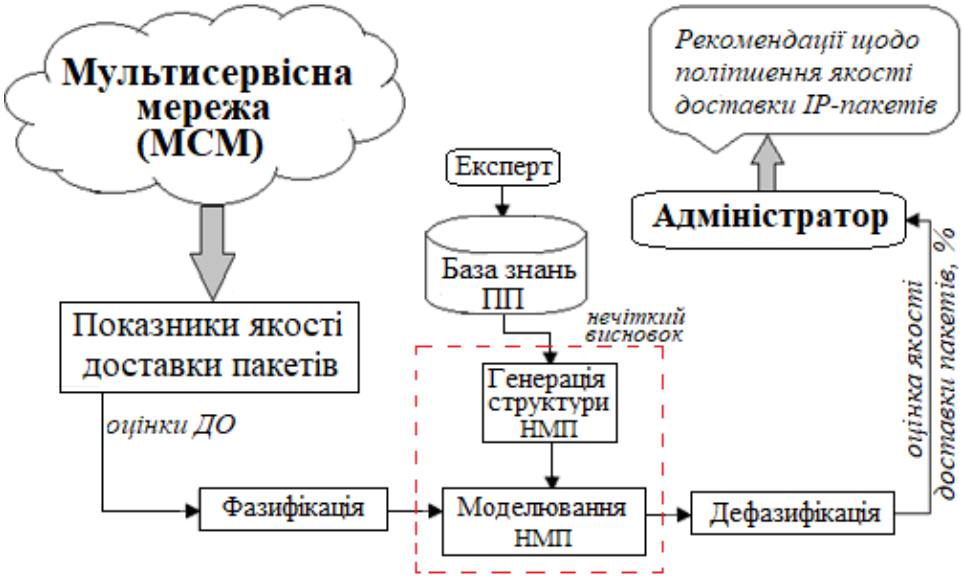


Рисунок 3.1 – Структурна схема запропонованої СППР

База знань такої СППР легко може бути представлена у формі продукційних правил (ПП), що описують вплив діагностичних ознак (ДО) на оцінку якості доставки пакетів. Спираючись на рекомендації МСЕ в якості ДО будемо використовувати три параметри, що представлені на рис. 3.2.

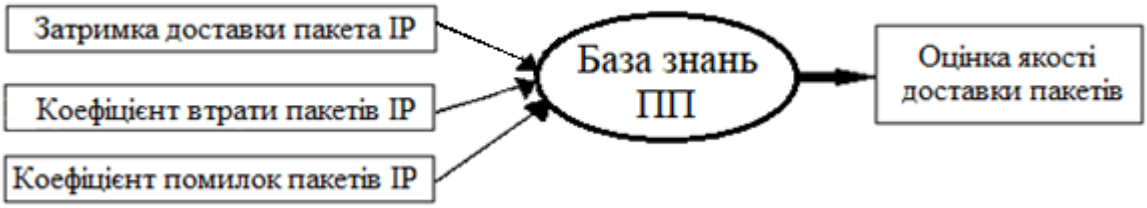
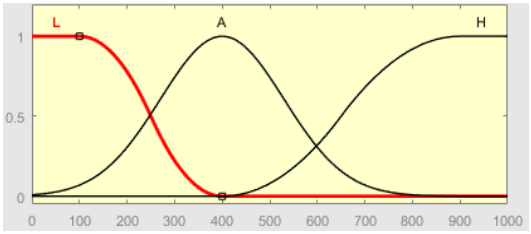


Рисунок 3.2 – Модель бази знань для оцінки якості доставки пакетів

На етапі фазифікації кожній ДО ставиться у відповідність нечітка лінгвістична змінна (ЛЗ): DF1 – затримка доставки пакета IP в мілісекундах (IP packet transfer delay); DF2 – коефіцієнт втрат пакетів IP у відсотках (IP

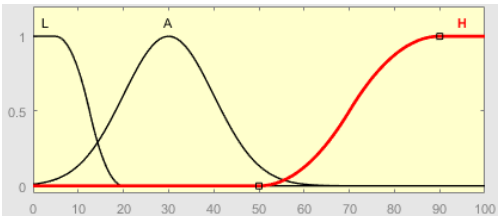
packet loss ratio); DF3 – коефіцієнт помилок у пакетах IP в процентах (IP packet error ratio).

Функції приналежності (ФП) та їх параметри для усіх змінних представлені на рисунку 3.3.



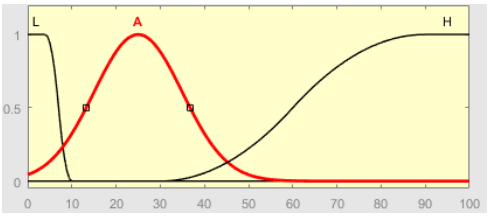
Терми		Діапазони		Тип ФП	Параметри
H	Low	0	400	zmf	[100 400]
C	Average	100	700	gaussmf	[130 400]
B	High	500	1000	smf	[400 900]

(а)



Терми		Діапазони		Тип ФП	Параметри
H	Low	0	20	zmf	[5 20]
C	Average	5	55	gaus smf	[10 30]
B	High	50	100	smf	[50 90]

(б)



Терми		Діапазони		Тип ФП	Параметри
H	Low	0	10	zmf	[4 10]
C	Average	5	45	gaus smf	[10 25]
B	High	30	100	smf	[30 90]

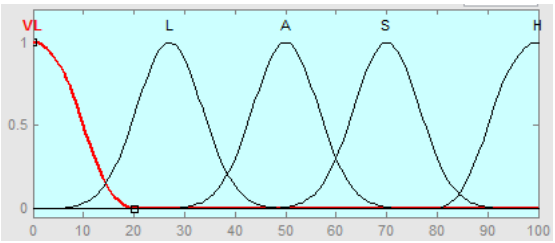
(в)

Рисунок 3.3 – ФП та їх параметри: лінгвістичної змінної «DF1» (а), лінгвістичної змінної «DF2» (б) , лінгвістичної змінної «DF3» (в)

Як видно з таблиці всі вхідні змінні характеризується трьома терм-множинами: «низький» (H, Low), «середній» (C, Average), «високий» (B, High). Вибір трирівневої шкали оцінки якості обумовлений тим, що з області психології відомо, що в короткочасній (робочої) пам'яті людини одночасно

утримується 7 ± 2 понять. Тому в зв'язку з великою кількістю оброблюваних критеріїв доцільно використовувати саме трирівневу шкалу оцінки якості.

Вихідна ЛЗ IP_QoS – якість доставка IP пакетів в МСМ (IP delivery quality), характеризується п'ятьма терм-множини: «дуже низький» (ДН, Very low), «низький» (Н, Low), «середній» (С, Average), «достатній» (Д, Sufficient), «високий» (В, High), ФП та параметри яких представлені на рисунку 3.4. Така градація досить близька до традиційної п'ятибальною шкалою оцінювання та полегшує прийняття рішення експертом про якість доставки пакетів в МСМ.



Терми		Діапазони		Тип ФП	Параметри
ДН	Very low	0	20	zmf	[0 20]
Н	Low	10	40	gaussmf	[6.5 27]
С	Average	30	70	gaussmf	[6.5 50]
Д	Sufficient	50	90	gaussmf	[6.5 70]
В	High	80	100	smf	[80 100]

Рисунок 3.4 – ФП та параметри лінгвістичної змінної «IP_QoS»

Результатом роботи СППР є оцінка якості доставки пакетів (ДН, Н, С, Д, В). Якісне визначення кожного рівня представлено в таблиці 3.1.

Таблиця 3.1 – Рівень якості доставки IP-пакетів

Рівень якості	Визначення
ДН (VL)	Якість доставки IP-пакетів дуже низька. Потрібна повна реконфігурація мережі для ефективного розподілу ресурсів.
Н (L)	Якість доставки IP-пакетів низька. Потрібна часткова реконфігурація мережі для ефективного розподілу ресурсів.
С (A)	Прийнятна якість доставки IP-пакетів, але для покращення якості такої МСМ необхідно працювати вжити заходів.
Д (S)	Якість доставки IP-пакетів досить висока. Даний рівень якості слід вважати бажаним для передачі трафіку реального часу.
В (H)	Якість доставки IP-пакетів повністю задовольняє вимогам користувачів. Мережа не вимагає коректування параметрів.

Запропоновані рекомендації дозволяють системному адміністратору підвищити рівень працездатності за рахунок збільшення швидкості прийняття рішення про якість передачі трафіку реального часу в МСМ в умовах відсутності повної та достовірної інформації про його стан і багатокритеріальності розв'язуваної задачі.

Нечіткі продукційні правила (27 ПП), що описують вплив вхідних ЛЗ на вихідну представлені на рисунку 3.5.

1. If (DF1 is L) and (DF2 is L) and (DF3 is L) then (IP__QoS is H) (1)
2. If (DF1 is L) and (DF2 is L) and (DF3 is A) then (IP__QoS is S) (1)
3. If (DF1 is L) and (DF2 is L) and (DF3 is H) then (IP__QoS is S) (1)
4. If (DF1 is L) and (DF2 is A) and (DF3 is L) then (IP__QoS is S) (1)
5. If (DF1 is L) and (DF2 is A) and (DF3 is A) then (IP__QoS is A) (1)
6. If (DF1 is L) and (DF2 is A) and (DF3 is H) then (IP__QoS is A) (1)
7. If (DF1 is L) and (DF2 is H) and (DF3 is L) then (IP__QoS is A) (1)
8. If (DF1 is L) and (DF2 is H) and (DF3 is A) then (IP__QoS is A) (1)
9. If (DF1 is L) and (DF2 is H) and (DF3 is H) then (IP__QoS is L) (1)
10. If (DF1 is A) and (DF2 is L) and (DF3 is L) then (IP__QoS is S) (1)
11. If (DF1 is A) and (DF2 is L) and (DF3 is A) then (IP__QoS is S) (1)
12. If (DF1 is A) and (DF2 is L) and (DF3 is H) then (IP__QoS is A) (1)
13. If (DF1 is A) and (DF2 is A) and (DF3 is L) then (IP__QoS is A) (1)
14. If (DF1 is A) and (DF2 is A) and (DF3 is A) then (IP__QoS is A) (1)
15. If (DF1 is A) and (DF2 is A) and (DF3 is H) then (IP__QoS is L) (1)
16. If (DF1 is A) and (DF2 is H) and (DF3 is L) then (IP__QoS is L) (1)
17. If (DF1 is A) and (DF2 is H) and (DF3 is A) then (IP__QoS is L) (1)
18. If (DF1 is A) and (DF2 is H) and (DF3 is H) then (IP__QoS is L) (1)
19. If (DF1 is H) and (DF2 is L) and (DF3 is L) then (IP__QoS is A) (1)
20. If (DF1 is H) and (DF2 is L) and (DF3 is A) then (IP__QoS is L) (1)
21. If (DF1 is H) and (DF2 is L) and (DF3 is H) then (IP__QoS is L) (1)
22. If (DF1 is H) and (DF2 is A) and (DF3 is L) then (IP__QoS is L) (1)
23. If (DF1 is H) and (DF2 is A) and (DF3 is A) then (IP__QoS is L) (1)
24. If (DF1 is H) and (DF2 is A) and (DF3 is H) then (IP__QoS is VL) (1)
25. If (DF1 is H) and (DF2 is H) and (DF3 is L) then (IP__QoS is VL) (1)
26. If (DF1 is H) and (DF2 is H) and (DF3 is A) then (IP__QoS is VL) (1)
27. If (DF1 is H) and (DF2 is H) and (DF3 is H) then (IP__QoS is VL) (1)

Рисунок 3.5 – База продукційних правил

Нечіткий логічний висновок відбувається на основі бази продукційних правил шляхом генерації нечіткої мережі Петрі (НМП).

Так як в основі запропонованої СППР лежить апарат нечітких мереж Петрі, то необхідно в першу чергу розглянути нечіткі мережі Петрі та процес їх використання для представлення продукційних правил.

Запропонована структура нечіткої СППР є інструментом адміністратора для об'єктивної оцінки якості доставки IP-пакетів в МСМ. Отримавши інтегральну оцінку якості доставки пакетів, при відомих значення пропускної здатності і надійності мережі, адміністратор може зробити висновок і про якість обслуговування в цілому (формула 3.1).

3.1.1 Основи мереж Петрі

Мережа Петрі – це математична модель дискретних динамічних систем (паралельних програм, операційних систем, ЕОМ і їх пристроїв, мереж ЕОМ), орієнтована на якісний аналіз і синтез таких систем (виявлення блокувань, тупикових ситуацій і вузьких місць, автоматичний синтез паралельних програм і компонентів ЕОМ та ін.).

Мережа Петрі може бути представлена 4-ма множинами:

$$PN = (\Theta, P, T, F, M_0),$$

де $\Theta = \{\theta = 0,1,2, \dots\}$ – множина дискретних моментів часу; $P = \{p_1, p_2, \dots, p_n\}$ – непорожня множина елементів мережі, які називаються позиціями; $T = \{t_1, t_2, \dots, t_m\}$ – непорожня множина елементів мережі, які називаються переходами. Множини позицій та переходів не перетинаються: $P \cap T = \emptyset$.

Функція інцидентності F визначається як:

$$F: (P \times T) \cup (T \times P) \to \{0,1,2, \dots, k, \dots\},$$

де k – кратність дуги.

Початкове маркування позицій M_0 визначає стартове стан мережі Петрі:

$$M_0: P \to \{0,1,2,\dots\}.$$

Функція інцидентності може бути представлена у вигляді $F = F^p \cup F^t$ і фактично задає два відображення:

1) $F^p\,(p,t) = P \times T \to \{0,1,2,\dots\}$, тобто для кожної позиції вказуються пов'язані з нею переходи (з урахуванням їх кратності);

2) $F^t\,(t,p) = T \times P \to \{0,1,2,\dots\}$, тобто для кожного переходу вказуються пов'язані з ним позиції (також з урахуванням кратності).

Ці функції, в загальному випадку залежать від часу, можуть бути представлені матрицями інцидентності:

$$F^p = \begin{matrix} t_1 & t_2 & \dots & t_m \end{matrix}\begin{matrix} \\ \\ \\ \end{matrix}$$
$$\begin{matrix} t_1 \\ \dots \\ t_m \end{matrix}\begin{bmatrix} f_{11}^p & f_{12}^p & \cdots & f_{1m}^p \\ \dots & & \dots & \dots \\ f_{n1}^p & f_{n2}^p & \cdots & f_{nm}^p \end{bmatrix},$$

$$F^t = \begin{matrix} p_1 & p_2 & \dots & p_n \end{matrix}\begin{matrix} \\ \\ \\ \end{matrix}$$
$$\begin{matrix} t_1 \\ \dots \\ t_m \end{matrix}\begin{bmatrix} f_{11}^t & f_{12}^t & \cdots & f_{1n}^t \\ \dots & & \dots & \dots \\ f_{m1}^t & f_{m2}^t & \cdots & f_{mn}^t \end{bmatrix}.$$

З вершини-позиції $p_i \in P$ веде дуга в вершину-перехід $t_j \in T$ тоді і тільки тоді, коли $f_{ij}^p > 0$. У цьому випадку говорять, що t_j – вихідний перехід позиції p_i.

Множина всіх позицій p_k, для яких t_j – вихідний перехід, будем позначати P^j. Іншими словами, $P^j = \{p_k: f_{kj}^p > 0\}$.

Аналогічно з кожної вершини-переходу $t_j \in T$ дуга веде до вершини-позиції $p_i \in P$ тоді і тільки тоді, коли $f_{ji}^t > 0$. При цьому говорять, що p_i – вихідна позиція переходу t_j.

Множина всіх переходів t_l, для яких p_i – вихідна позиція, будемо позначати T^i. Таким чином, $T^i = \{t_l: f_{li}^t > 0\}$. При $f_{ij}^p > 0$ and $f_{ji}^t > 0$ ці величини називаються кратністю відповідних дуг.

Кожна позиція $p_i \in P$ може містити деякий цілочисельний ресурс $\mu(p) \geq 0$, що часто відображається відповідним числом точок (фішок) всередині позиції. Вектор $M = [\mu_1 \dots \mu_n]$ називають маркуванням (розміткою) мережі Петрі.

Зміна маркувань (починаючи з M_0) здійснюється в результаті спрацьовування переходів мережі. Перехід $t_j \in T$ може бути запущений при маркуванні M, якщо для всіх $p_i \in P^j$ виконується умова

$$\mu_i(\theta) - f_{ij}^p(\theta) \geq 0,$$

тобто якщо кожна вхідна позиція для даного переходу $p_i \in P^j$ містить як мінімум стільки фішок, яка кратність дуги, що веде до t_j.

В результаті спрацьовування переходу t_j в момент часу θ маркування $M\ (\theta)$ змінюється маркуванням $M\ (\theta\ +\ 1)$ за правилом:

$$\mu_i(\theta + 1) = \mu_i(\theta) - f_{ij}^p(\theta) + f_{jl}^t(\theta),$$

де $i = 1, \dots n,\ j = 1, \dots, m, i \in P^j, j \in T^i$.

Іншими словами, перехід t вилучає з кожної своєї вхідних позиції число фішок, що дорівнює кратності вхідних дуг, і посилає в кожну свою вихідну позицію число фішок, що дорівнює кратності вихідних дуг. Якщо може спрацювати кілька переходів, то спрацює один, будь-який з них. Функціонування мережі зупиняється, якщо при деякому маркуванні (тупикове маркування) жоден з її переходів не може спрацювати.

Графовим представленням мережі Петрі є двочастковий орієнтований мультиграф мережі Петрі.

Цей граф містить (рис. 3.6):

– позиції (місця), що позначаються кружками;

– переходи, що позначаються планками;

– орієнтовані дуги (стрілки), що з'єднують позиції з переходами і переходи з позиціями. Кратні дуги позначаються кількома паралельними дугами.

В випадку великої кратності дуг цю кратність можна вказувати цифрами на відповідній дузі.

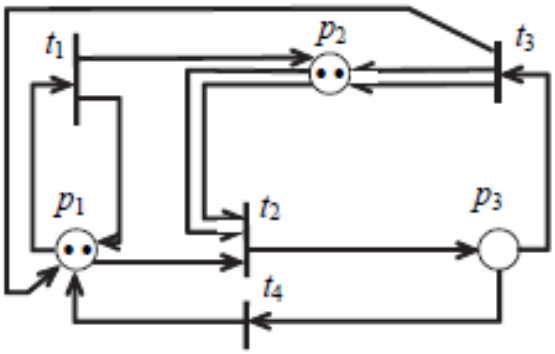


Рисунок 3.6 – Приклад мережі Петрі

Для мережі, зображеної на рис. 3.1, матриці інцидентності мають вид:

$$F^p = \begin{matrix} \\ p_1 \\ p_2 \\ p_3 \end{matrix}\begin{matrix} \begin{matrix} t_1 & t_2 & t_3 & t_4 \end{matrix} \\ \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \end{matrix}, \qquad F^t = \begin{matrix} \\ t_1 \\ t_2 \\ t_3 \\ t_4 \end{matrix}\begin{matrix} \begin{matrix} p_1 & p_2 & p_3 \end{matrix} \\ \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 2 & 0 \\ 1 & 0 & 0 \end{bmatrix} \end{matrix}.$$

Початкова маркування, як видно з рис. 3.6, M_0 = [2 2 0]. Матричне і графове представлення взаємно однозначно відповідають один одному.

Існує багато різновидів мереж Петрі. Розглянемо їх класифікацію та оберемо ту мережу Петрі, що підходить для нашої задачі.

Мережі Петрі поділяються на інгібіторні, маркіровані, стохастичні, кольорові, часові, автоматні, потокові, мережі вільного вибору, нечіткі [32]. Вибір тієї чи іншої мережі Петрі залежить від об’єкта дослідження.

В нашому випадку при побудові СППР оцінки якості обслуговування в МСМ треба взяти до уваги те, що знання і досвід експертів мають суб'єктивний характер і погано піддаються формалізації, тому, що особа, яка приймає рішення (адміністратор МСМ) найчастіше працює саме з нечіткою інформацією, представленої користувачами мережі в словесній формі (наприклад, розмова по IP-телефону «переривається», передача файлу «зависає», приходять «биті» файли). В цьому випадку, користувачі МСМ служать своєрідним індикатором її стану: якщо вона працює гірше, ніж

зазвичай, то негайно викликається адміністратор. Природно, що спеціальних знань, щоб точно описати симптоми проблеми, у рядового користувача зазвичай не вистачає. Більш того, опис, яке дає користувач, найчастіше є суб'єктивним і неточним.

Саме нечіткі мережі Петрі (НМП) знайшли найбільше практичне застосування при вирішенні прикладних задач, що характеризуються урахуванням різних факторів невизначеності.

3.1.2 Нечіткі мережі Петрі для представлення продукційних правил

Можна виділити наступні класи нечітких мереж Петрі [33]:

– часові мережі Петрі з нечіткістю в завданні структури (Θ, P, T, F, M_0);

– часові мережі Петрі з нечіткістю в завданні початкового маркірування M_0;

– часові мережі Петрі з нечіткістю в завданні початкового маркірування M_0 та часових затримок маркерів у позиціях та часу спрацьовування активних переходів;

– часові мережі Петрі з нечіткістю в завданні правил, що визначають процес функціонування мережі.

Одним з найбільш відомих застосувань НМП є їх використання для наочного представлення правил нечітких продукцій і виконання на їх основі виводу нечітких висновків [34].

Правило нечіткої продукції виду «ПРАВИЛО і: ЯКЩО А, то Б» представляється як деякий перехід $t_i \in T$ мережі Петрі, при цьому умові «А» цього правила відповідає вхідна позиція $p_i \in P$ цього переходу, а висновку – вихідна позиція $p_k \in P$ цього переходу t_i (рис. 3.7 (а)).

Якщо умова правила нечіткої продукції складається із декількох підумов, з'єднаних операцією нечіткої кон'юнкції $A = A_1 \wedge A_2 \wedge \ ... \ \wedge A_i$, то всі

ці підумови представляються як вхідні позиції відповідного переходу (рис. 3.7 (б) для випадку $l = 3$).

Якщо висновок правила нечіткої продукції складається з декількох підвисновків, з'єднаних операцією нечіткої кон'юнкції $\mathrm{B} = \mathrm{B}_1 \wedge \mathrm{B}_2 \wedge \ldots \wedge \mathrm{B}_\mathrm{i}$, всі ці підвисновки також представляються як вихідні позиції відповідного переходу (рис. 3.7 (в) для випадку $l = 3$).

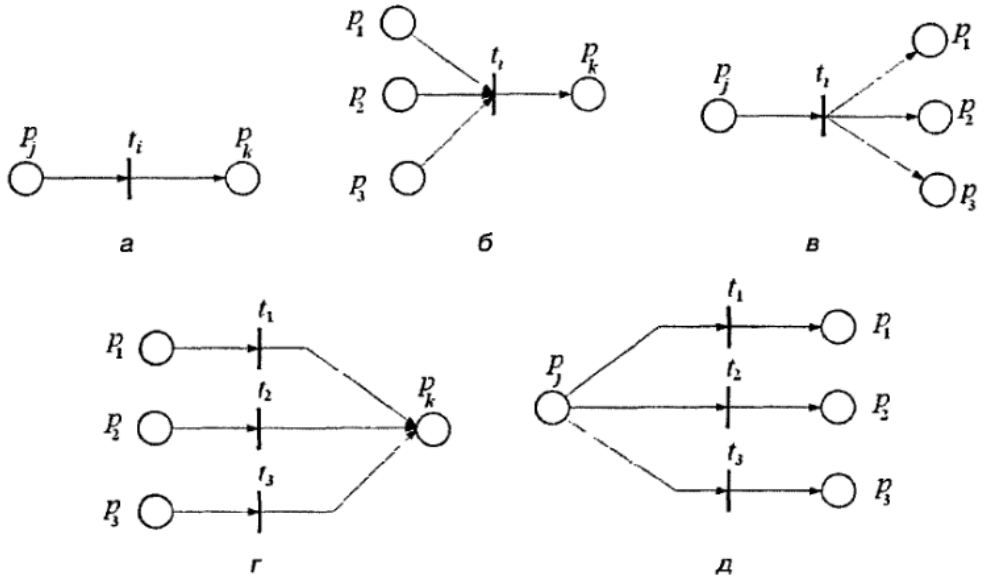


Рисунок 3.7 – Фрагменти нечітких мереж Петрі для представлення різних варіантів правил нечітких продукцій

Інший випадок, коли умова правила нечіткої продукції складається із декількох підумов, з'єднаних операцією нечіткої диз'юнкції $\mathrm{A} = \mathrm{A}_1 \vee \mathrm{A}_2 \vee \ldots \vee \mathrm{A}_\mathrm{i}$, то всі ці підумови представляються як вхідні позиції окремих переходів t_i для $i \in \{1,2, \ldots l\}$ (рис. 3.7 (г) для випадку $l = 3$). Якщо ж висновок правила нечіткої продукції складається з декількох підвисновків, з'єднаних операцією нечіткої диз'юнкції $\mathrm{B} = \mathrm{B}_1 \vee \mathrm{B}_2 \vee \ldots \vee \mathrm{B}_\mathrm{i}$, то всі ці підвисновки представляються як вихідні позиції окремих переходів t_i для $i \in \{1,2, \ldots l\}$ (рис. 3.7 (д) для випадку $l = 3$).

Таким чином, будь-яке правило нечіткої продукції може бути представлено у вигляді фрагмента нечіткої мережі Петрі.

При цьому ваги або коефіцієнти визначеності F_i правил нечітких продукцій перетворюються у вектор $f = (f_1, f_2, \dots, f_u)$ значень функції приналежності нечіткого спрацьовування переходів, а ступенями істинності підумови правил відповідають значення компонентів початкового маркування $m_0 = (m_1^0, m_2^0, \dots, m_n^0)$, яке в цьому випадку описує поточну ситуацію проблемної області, що моделюється.

Для представлення продукційних правил, що запропоновані на рисунку 3.5. створимо НМП. Так як умови всіх правил нечітких продукцій складаються із декількох підумов, з'єднаних операцією нечіткої кон'юнкції, то всі ці підумови представляються як вхідні позиції відповідного переходу (табл. 3.2).

Таблиця 3.2 – Генерація позицій НМП

Підумови та підвисновки ПП	Позиція
DF1 is L	p1
DF2 is L	p2
DF3 is L	p3
DF1 is A	p4
DF2 is A	p5
DF3 is A	p6
DF1 is H	p7
DF2 is H	p8
DF3 is H	p9
IP__QoS is H	p10
IP__QoS is S	p11
IP__QoS is A	p12
IP__QoS is L	p13
IP__QoS is VL	p14

Так, наприклад, продукційне правило № 1:

If (DF1 is L) and (DF2 is L) and (DF3 is L) then (IP__QoS is H)

можна представити наступним чином:

If (p1) and (p2) and (p3) then (p10).

Таким чином, кількість позицій дорівнює кількості підумов (p1,…, p14), а кількість переходів – кількості продукційних правил (t1…t27).

На рисунку 3.8 представлена розроблена мережа Петрі. В якості програмного забезпечення для створення та аналізу мереж Петрі використана програма «Сеть Петри» [35].

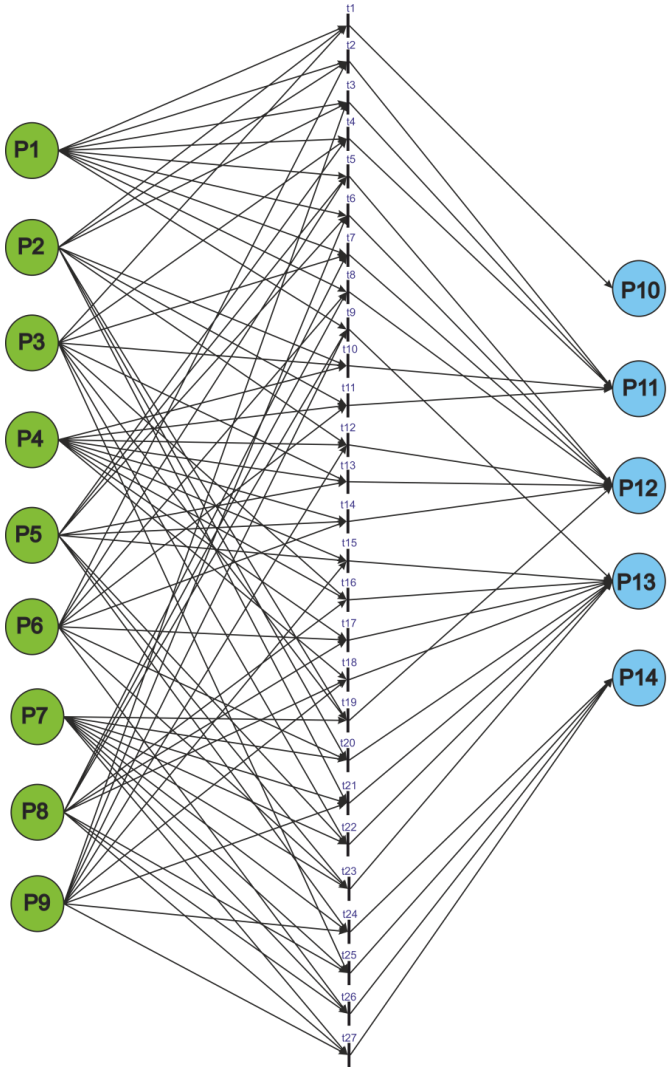


Рисунок 3.8 – Мережа Петрі

Для перевірки коректності запропонованої структури мережі Петрі задаймо початкове маркування наступним чином M_0 = [00011000100000]. Одиниці відповідають наявності маркерів у позиціях p4, p5 та p9 (рис. 3.9).

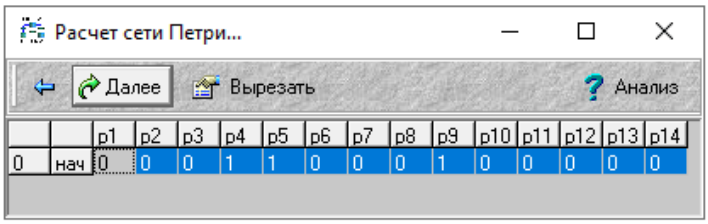


Рисунок 3.9 – Перевірка коректності мережі Петрі

В результаті розрахунку мережі Петрі шляхом натискання на кнопку «Далее», бачимо що спрацював перехід t15. В результаті чого, мітка перейде до позиції p13 (рис. 3.10).

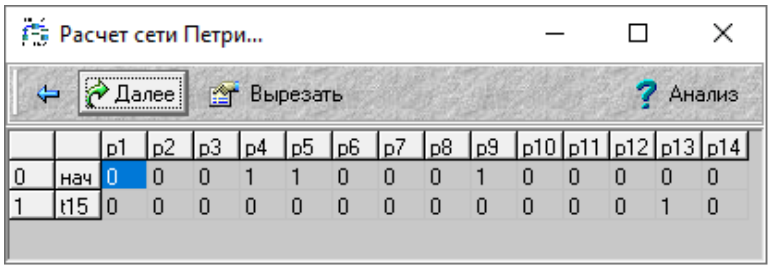


Рисунок 3.10 – Результат моделювання мережі Петрі

Що співпадає з продукційним правилом № 15, а саме:

If (DF1 is A) and (DF2 is A) and (DF3 is H) then (IP__QoS is L).

Розглянемо інше початкове маркування M_0 = [10010010000000]. Одиниці відповідають наявності маркерів у позиціях p1, p4 та p7. В результаті розрахунку мережі Петрі шляхом натискання на кнопку «Далее», бачимо що не спрацював жодний перехід (рис. 3.11).

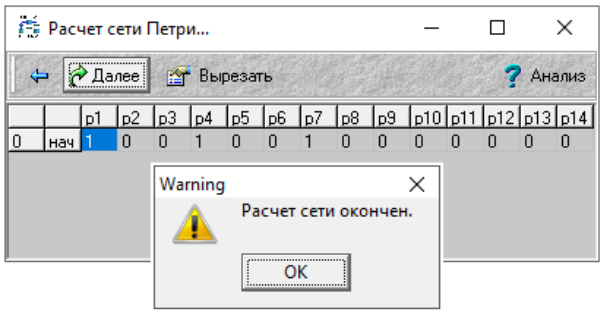


Рисунок 3.11 – Результат моделювання мережі Петрі

Як видно з рисунку 3.11 система моделювання видала попередження, тим самим підтверджуючі той факт, що не може одна і теж діагностична ознака мати різні значення.

Таким чином, результати моделювання показали можливість використання мережі Петрі для представлення ПП. Матриці інцидентності розробленої мережі Петрі представлені на рисунку 3.12.

Матрица позиций :

Q	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10	p11	p12	p13	p14
t1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
t2	1	1	0	0	0	1	0	0	0	0	0	0	0	0
t3	1	1	0	0	0	0	0	0	1	0	0	0	0	0
t4	1	0	1	0	1	0	0	0	0	0	0	0	0	0
t5	1	0	0	0	1	1	0	0	0	0	0	0	0	0
t6	1	0	0	0	1	0	0	0	1	0	0	0	0	0
t7	1	0	1	0	0	0	0	1	0	0	0	0	0	0
t8	1	0	0	0	0	1	0	1	0	0	0	0	0	0
t9	1	0	0	0	0	0	0	1	1	0	0	0	0	0
t10	0	1	1	1	0	0	0	0	0	0	0	0	0	0
t11	0	1	0	1	0	1	0	0	0	0	0	0	0	0
t12	0	1	0	1	0	0	0	0	1	0	0	0	0	0
t13	0	0	1	1	1	0	0	0	0	0	0	0	0	0
t14	0	0	0	1	1	1	0	0	0	0	0	0	0	0
t15	0	0	0	1	1	0	0	0	1	0	0	0	0	0
t16	0	0	1	1	0	0	0	1	0	0	0	0	0	0
t17	0	0	0	1	0	1	0	1	0	0	0	0	0	0
t18	0	0	0	1	0	0	0	1	1	0	0	0	0	0
t19	0	1	1	0	0	0	1	0	0	0	0	0	0	0
t20	0	1	0	0	0	1	1	0	0	0	0	0	0	0
t21	0	1	0	0	0	0	1	0	1	0	0	0	0	0
t22	0	0	1	0	1	0	1	0	0	0	0	0	0	0
t23	0	0	0	0	1	1	1	0	0	0	0	0	0	0
t24	0	0	0	0	1	0	1	0	1	0	0	0	0	0
t25	0	0	1	0	0	0	1	1	0	0	0	0	0	0
t26	0	0	0	0	0	1	1	1	0	0	0	0	0	0
t27	0	0	0	0	0	0	1	1	1	0	0	0	0	0

Матрица переходов :

R	p1	p2	p3	p4	p5	p6	p7	p8	p9	p10	p11	p12	p13	p14
t1	0	0	0	0	0	0	0	0	0	1	0	0	0	0
t2	0	0	0	0	0	0	0	0	0	0	1	0	0	0
t3	0	0	0	0	0	0	0	0	0	0	1	0	0	0
t4	0	0	0	0	0	0	0	0	0	0	1	0	0	0
t5	0	0	0	0	0	0	0	0	0	0	0	1	0	0
t6	0	0	0	0	0	0	0	0	0	0	0	1	0	0
t7	0	0	0	0	0	0	0	0	0	0	0	1	0	0
t8	0	0	0	0	0	0	0	0	0	0	0	1	0	0
t9	0	0	0	0	0	0	0	0	0	0	0	0	1	0
t10	0	0	0	0	0	0	0	0	0	0	1	0	0	0
t11	0	0	0	0	0	0	0	0	0	0	1	0	0	0
t12	0	0	0	0	0	0	0	0	0	0	0	1	0	0
t13	0	0	0	0	0	0	0	0	0	0	0	1	0	0
t14	0	0	0	0	0	0	0	0	0	0	0	1	0	0
t15	0	0	0	0	0	0	0	0	0	0	0	0	1	0
t16	0	0	0	0	0	0	0	0	0	0	0	0	1	0
t17	0	0	0	0	0	0	0	0	0	0	0	0	1	0
t18	0	0	0	0	0	0	0	0	0	0	0	0	1	0
t19	0	0	0	0	0	0	0	0	0	0	0	1	0	0
t20	0	0	0	0	0	0	0	0	0	0	0	0	1	0
t21	0	0	0	0	0	0	0	0	0	0	0	0	1	0
t22	0	0	0	0	0	0	0	0	0	0	0	0	1	0
t23	0	0	0	0	0	0	0	0	0	0	0	0	1	0
t24	0	0	0	0	0	0	0	0	0	0	0	0	0	1
t25	0	0	0	0	0	0	0	0	0	0	0	0	0	1
t26	0	0	0	0	0	0	0	0	0	0	0	0	0	1
t27	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Рисунок 3.12 – Матриці інцидентності

Згідно з матрицею позицій можна легко побачити, що до кожного переходу входять три дуги від трьох різних позицій. Це відповідає тому факту, що кожне правило має три підумови.

Матриця переходів показує, що з кожного переходу виходить тільки одна дуга до різних позицій. Це відповідає тому факту, кожен перехід відповідає тому чи іншому продукційному правилу.

Безсумнівною перевагою уявлення бази правил у формі МП і подальше рішення задач логічного виводу на їх основі є наочність і візуалізація всіх проміжних результатів.

3.2 Аналіз якості доставки пакетів з використанням мережі Петрі

Нечітка модель Петрі для оцінки якості доставки пакетів в МСМ передбачає використання ступеней істинності підумов правил в якості початкового маркування $m_0 = (m_1^0, m_2^0, \dots, m_n^0)$, яке в цьому випадку описує поточну ситуацію в мережі, що моделюється.

Розглянемо приклад аналізу якості доставки пакетів.

Допустимо, що користувач оцінив вхідні діагностичні параметри наступним чином: затримка доставки пакета 500 мс, коефіцієнт втрат пакетів 10%, коефіцієнт помилок у пакетах 80%. Тобто DF1= 500, DF2 =10, DF3 = 80.

Згідно з запропонованими функціями приналежності (рис. 3.3) ступені істинності підумов усіх ПП для цього випадку представлені в табл. 3.3.

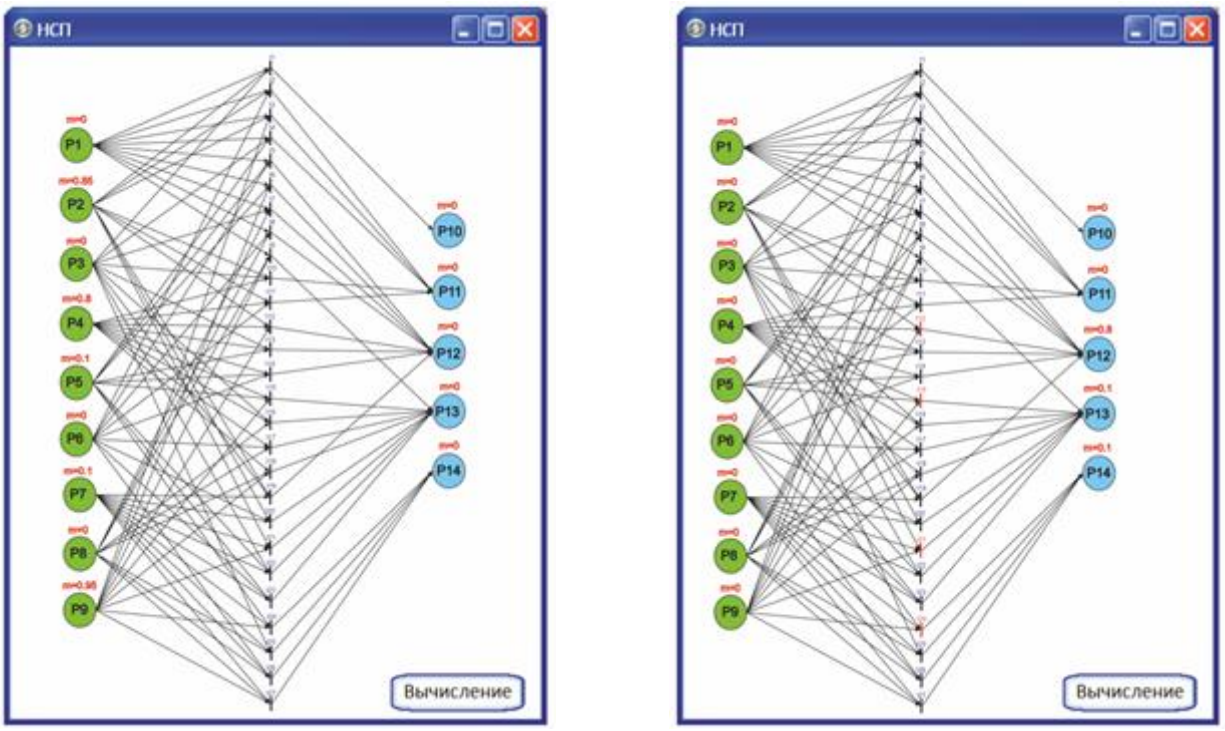
Таблиця 3.3 – Ступені істинності підумов для експерименту №1

Підумови ПП	Позиції	Ступені істинності
DF1 is L	p1	0
DF2 is L	p2	0.85
DF3 is L	p3	0
DF1 is A	p4	0.8
DF2 is A	p5	0.1
DF3 is A	p6	0
DF1 is H	p7	0.1
DF2 is H	p8	0
DF3 is H	p9	0.95

Ступені істинності з таблиці 3.3 складають вектор початкового маркування M_0 = [0 0.85 0 0.8 0.1 0 0.1 0 0.95 0 0 0 0 0] для проведення моделювання нечіткої мережі Петрі згідно з даними експерименту. Для моделювання НМП використано програму, що наведена у [36]. Останні п’ять

нулів вектору відповідають вихідним позиціям, значення маркування яких ми маємо дізнатися.

На рисунку 3.13 (а) показано стан НМП до проведення експерименту, тобто до того, як спрацювали ті чи інші переходи.



(а) (б)

Рисунок 3.13 – Нечітка мережа Петрі до (а) та після (б) спрацювання переходів t_{12}, t_{15}, t_{21} та t_{24}

Стан НМП на рисунку 3.13 (б) пояснюється алгоритмом нечіткого виводу, що закладений у програму моделювання.

Згідно цього алгоритму значення функції приналежності (ступеня істинності ПП) обчислюється як мінімальне значення серед усіх ступеней істинності підумов, а ступень істинності підзаключень – як максимальне значення (табл. 3.4).

Таблиця 3.4 − Ступені істинності ПП

№ПП	Ступені істинності підумов			Ступені істинності ПП
	DF1	DF2	DF3	
1	0	0.85	0	0
2	0	0.85	0	0
3	0	0.85	0.95	0
4	0	0.1	0	0
5	0	0.1	0	0
6	0	0.1	0.95	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0.95	0
10	0.8	0.85	0	0
11	0.8	0.85	0	0
12	0.8	0.85	0.95	0.8
13	0.8	0.1	0	0
14	0.8	0.1	0	0
15	0.8	0.1	0.95	0.1
16	0.8	0	0	0
17	0.8	0	0	0
18	0.8	0	0.95	0
19	0.1	0.85	0	0
20	0.1	0.85	0	0
21	0.1	0.85	0.95	0.1
22	0.1	0.1	0	0
23	0.1	0.1	0	0
24	0.1	0.1	0.95	0.1
25	0.1	0	0	0
26	0.1	0	0	0
27	0.1	0	0.95	0

Цей аналіз показав, що спрацювали переходи t_{12}, t_{15}, t_{21} та t_{24}. Що співпадає з результатами моделювання та доводить коректність результатів роботи НМП (рис. 3.13, б). Натиснув на кнопку “Вычисление” отримаємо результат нечіткого виводу на базі алгоритму Мамдані (рис. 3.14).

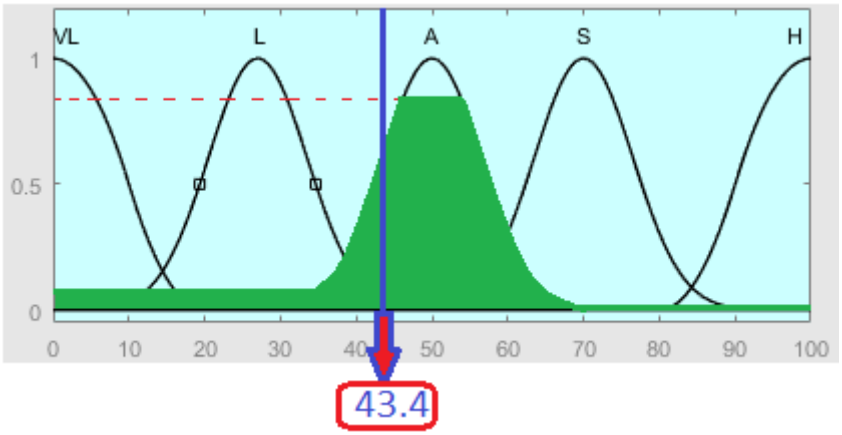


Рисунок 3.14 – Результат роботи НМП

Рисунок 3.14 показав, що при значенні діагностичних параметрів DF1=500, DF2=10, DF3=80, НМП видає результат 43,4 %. Цей результат відповідає середньому рівню якості доставки пакетів в МСМ.

Виконавши аналіз результатів нечіткого виводу, можливо побудувати графіки, що покажуть залежність якості доставки пакетів від того чи іншого параметру:

$$IP\_delivery\_quality = f\,(DF1, DF2, DF3),$$

де *IP_delivery_quality* – якість доставки пакетів, %; *DF1*– затримка доставки пакета, мс; *DF2* – коефіцієнт втрати пакетів, %; *DF3* – коефіцієнт помилок пакетів, %.

При проведенні експерименту проаналізовані RTCP-пакети, що пересилаються всередині МСМ. Значення параметрів доставки (оцінок діагностичних параметрів) подаються на вхід СППР (рис. 3.1). НМП, як ядро системи, генерує значення вихідної змінної, що описує таку залежність:

$$IP\_delivery\_quality = f\,(DF1, 40, 20),$$

де перші два параметра зафіксовані в такий спосіб: DF2 = 40, DF3 = 20.

Отриманий графік відображає вплив параметра DF1 (затримка доставки, мс) на якість доставки IP пакетів в МСМ (рис. 3.15).

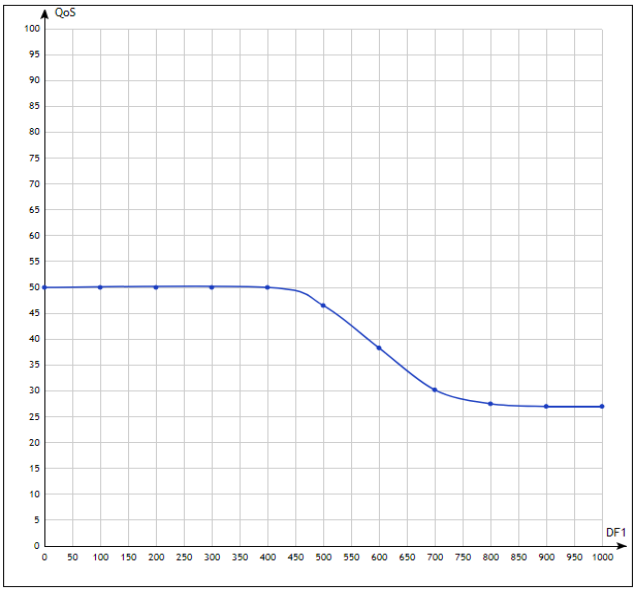


Рисунок 3.15 – Графік залежності *IP_delivery_quality = f (DF1)* при DF2 = 40, DF3 = 20

Отриманий графік показує, що якість доставки пакетів дорівнює 50% і різко падає з ростом затримки доставки пакетів до 27 %.

Розглянемо залежність: *IP_delivery_quality = f (500, DF2, 20),* де перший та третій параметри зафіксовані в такий спосіб: DF1 = 500, DF3 = 20.

Отриманий графік відображає вплив параметра DF2 (коефіцієнт втрати пакетів, %) на якість доставки IP пакетів в МСМ (рис. 3.16).

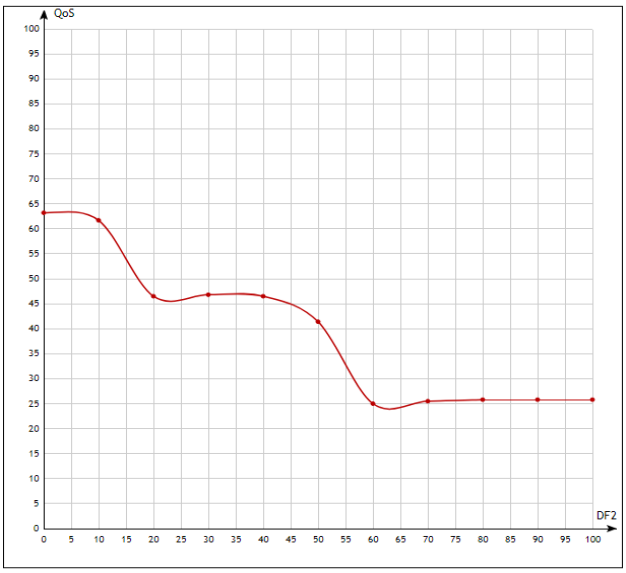


Рисунок 3.16 – Графік залежності *IP_delivery_quality = f (DF2)* при DF1 = 500, DF3 = 20

Отриманий графік показує, що якість доставки пакетів не перевищує 65% та стрибкоподібно падає з ростом коефіцієнта втрати пакетів до 25 %.

Розглянемо залежність: *IP_delivery_quality = f (500, 40, DF3),* де перший та другий параметри зафіксовані в такий спосіб: DF1 = 500, DF2 = 40. Отриманий графік відображає вплив параметра DF3 (коефіцієнт помилок пакетів, %) на якість доставки IP пакетів в МСМ (рис. 3.17).

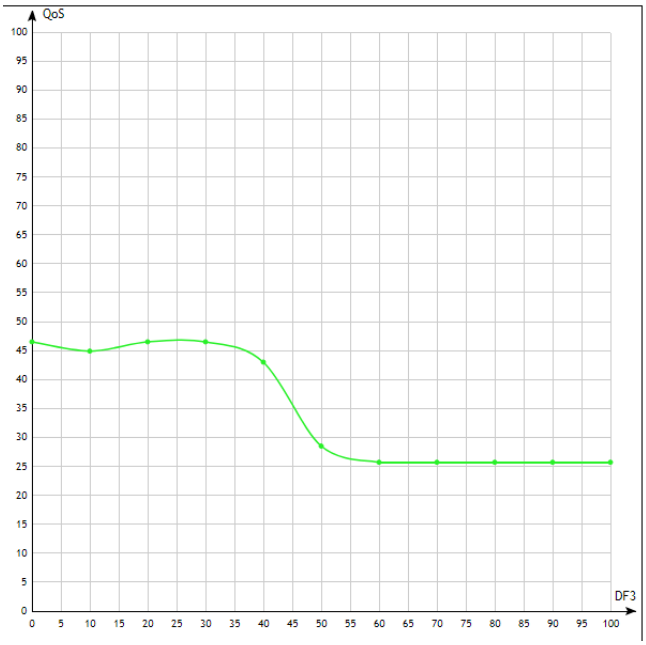


Рисунок 3.17 – Графік залежності *IP_delivery_quality = f (DF3)* при DF1 = 500, DF2 = 40

Отриманий графік показує, що якість доставки пакетів не перевищує 47% та стрибкоподібно падає з ростом коефіцієнта втрати пакетів до 25 %.

Таким чином, результатом аналізу стали графіки, на підставі яких можна виконати розрахунок впливу діагностичних параметрів і оцінити роль кожного з них у зміні величини результативного показника − якості доставки IP-пакетів в МСМ, тобто на базі отриманих графіків можна визначити значення того чи іншого параметра, при якому досягається необхідне (бажане) значення якості доставки пакетів.

4 АНАЛІЗ ПЕРЕДАЧІ ТРАФІКУ РЕАЛЬНОГО ЧАСУ В МУЛЬТИСЕРВІСНІЙ МЕРЕЖІ IP-ТЕЛЕФОНІЇ

4.1 Загальна інформація про систему Asterisk

Asterisk − це платформа для телефонії з відкритим початковим кодом, яке встановлюється практично на будь-яку платформу Linux. Потужність цієї системи − в її природі, що настроюється, у поєднанні з відповідністю стандартам, що не має аналогів. Жодна інша офісна автоматична телефонна станція (АТС) не надає такі широкі можливості по варіантах її розгортання. Такі застосування, як голосова пошта, конференц-зв'язок, черги викликів і агенти, музика під час очікування і паркування викликів, усе це стандартні функції, вбудовані безпосередньо в програмне забезпечення.

З точки зору вимог до ресурсів Asterisk подібна до вбудованих систем реального часу переважно тим, що вона повинна мати пріоритетний доступ до процесора і системних шин. Тому украй важливо, щоб усі інші функції системи, не пов'язані безпосередньо із завданнями Asterisk по обробці викликів, якщо такі взагалі виконуються, повинні виконуватися з нижчим пріоритетом. Для невеликих і любительських систем це може і не представляти особливої проблеми. Проте для високопродуктивних систем недостатня продуктивність викликатиме проблеми з якістю аудіосигналу, що отримується користувачем, часто у вигляді луна-камери, перешкод і тому подібне. Приблизно так поводяться пристрої мобільного зв'язку при виході із зони обслуговування, але тут причина цих проблем інша. У міру збільшення навантаження на систему зростатимуть складнощі з обслуговуванням з'єднань. Для офісної АТС подібна ситуація − справжня катастрофа, тому в процесі вибору платформи вимоги до продуктивності мають бути вирішальним критерієм. У таблиці 4.1 представлені деякі найосновніші рекомендації до планування системи.

Таблиця 4.1 – Вибір технічних характеристик системи Asterisk

Призначення	Кількість каналів	Рекомендовані мінімальні параметри
Любительська система	не більше 5	400 МГц ×86, 256 Мб оперативної пам'яті
SOHO-система (малый офис)	від 5 до 10	1 ГГц ×86, 512 Мб оперативної пам'яті
Мала бізнес-система	до 25	3 ГГц ×86, 1 Гб оперативної пам'яті
Середня і велика система	більше 25	Два ЦП, можливо також декілька серверів в розподіленій архітектурі

Для великих установок Asterisk функціональність зазвичай розподіляють між декількома серверами. Один або більш центральних модулів займатимуться обробкою викликів; їх доповнять один або більш допоміжних серверів, обслуговуючих периферійні пристрої (такі, як система баз даних, система голосової пошти, система конференц-зв'язку, система управління, веб-інтерфейс, міжмережевий екран і так далі). Asterisk, як і багато Linux -систем, може розширюватися із зростанням вимог до неї: мала система, яка прекрасно справлялася з усіма завданнями по обробці викликів і обслуговуванню периферійних пристроїв, може бути розподілена між декількома серверами, коли вимоги зростуть і перевищать її поточні можливості.

Гнучкість − основна причина, по якій Asterisk виключно рентабельна для швидко зростаючого бізнесу; для неї не існує ефективного максимального або мінімального розміру, який слід враховувати при складанні кошторису на купівлю.

Революційні перетворення, яким сприяє Asterisk, включають і еволюцію телефону : від простого пристрою аудіозв'язку до мультимедійного терміналу зв'язку, що надає всілякі функції, які поки що складно навіть представити. Коротко розглянемо різні види пристроїв, звані нині "телефонами" (усі вони без зусиль можуть бути інтегровані з Asterisk).

1. Фізичні телефони – пристрої, основним призначенням якого є замикання на вимогу лінії аудіозв'язку між двома точками.

1) Аналогові телефони – їх завдання уловлювати ці звуки і перетворювати їх у формат, придатний для передачі по дротах. Сигнал, що передається є аналогом звукових хвиль, що створюються об'єктом, який говорить.

2) Спеціалізовані цифрові телефони функціонально ідентичні аналоговому телефонному апарату, і часто вони сумісні один з одним, при цьому аналоговий сигнал дискретизуватиметься і перетвориться у цифровий. Основна перевага цифрового сигналу в тому, що він може передаватися на необмежені відстані без втрати якості.

3) ISDN-телефони. До появи VoIP щонайближче до стандартизованного цифрового телефону був термінал ISDN BRI (Basic Rate Interface). Було розроблено безліч BRI-пристроївв, проте BRI був переважно знехтуваний на користь швидших і дешевших технологій, таких як ADSL, кабельні модеми і VoIP. BRI як і раніше дуже широко використовується як устаткування для видеоконференц-зв’язку, оскільки забезпечує лінію з фіксованою смугою пропускання. Також для BRI не характерні проблеми з якістю, які можуть виникати при VoIP-з’єднання, оскільки це інтерфейс з комутацією каналів.

4) IP-телефони. Багатство можливостей, пропонованих цими пристроями, зумовить шквал цікавих застосувань, починаючи від відеотелефонів до пристроїв для мовлення з високою якістю, безпровідних мобільних рішень, спеціалізованих телефонних апаратів, призначених для конкретних галузей, і гнучких мультимедійних систем "Усе в одному"

2. Програмні телефони (software telephone, софтфон) – це застосування, яке забезпечує функціональність телефону пристрою, що не є телефоном, такому як ПК або персональний цифровий секретар. Софтфон не потребує додаткових апаратних рішень, за виключенням, хіба що, комп'ютерної гарнітури або веб-камери для здійснення відеодзвінків. Програмне

забезпечення для софтфона, як правило, розробляється на основі відкритих протоколів зв'язку SIP або H.323.

Софтфон по суті своїй є програмою, яка замінює вам апаратний IP-телефон на комп'ютері. Як ми вже писали вище, для повноцінної роботи софтфона потрібна телефонна гарнітура (в крайньому випадку - навушники і зовнішній мікрофон). Переваги софтфона наступні, по-перше, це розширений інтерфейс, який неможливо обмежити маленьким телефонним екраном. По-друге, це велика телефонна книга, яку фізично нереально реалізувати на апаратному телефоні. Також до переваг софтфонів можна додати і функцію вашого он-лайн статусу, можливість передачі текстових повідомлень і факсів, відеодзвінки. Софтфони бувають як платні, так і безкоштовні. Найбільш поширені програми для IP-телефонії - це 3CX, iSoftphone, Bria, ZoiPer, ShoreTel Sky Softphone, Октофон і інші.

3. Телефонні адаптери можна описати як пристрій для кінцевого споживача, який забезпечує об'єднання ліній зв'язку, що використовують різні протоколи. VoIP-адаптер також відомий під ім'ям "SIP-адаптера", оскільки основним протоколом встановлення сеансу зв'язку в IP -телефонии являється SIP (Session Initiation Protocol). Зустрічаються ще два найменування цих пристроїв − "ATA" (аналоговий телефонний адаптер) і "адаптер FXS" (у останньому вказано, що пристрій має порт FXS, що підключається кабелем до порту FXO на телефонному або факс-аппарате). Найчастіше ці пристрої використовуються для перетворення цифрового сигналу (IP або спеціалізованого) в аналоговий, з яким можуть працювати стандартні телефони або факси.

Такі адаптери можна було б називати шлюзами, тому що це − їх функція. Проте популярний термін "телефонний шлюз", ймовірно, краще всього описав би багатопортовий телефонний адаптер, як правило, що виконує складніші функції маршрутизації.

Телефонні адаптери вживатимуться доки, поки існує необхідність сполучати несумісні стандарти і старі пристрої з новими мережами. З часом

необхідність в цих пристроях відпаде, як це сталося з модемами, які поступово зникають зважаючи на непотрібність.

Для реалізації IP АТС Asterisk потрібний системний блок з тією або іншою конфігурацією і телефонні апарати (рис. 4.1).

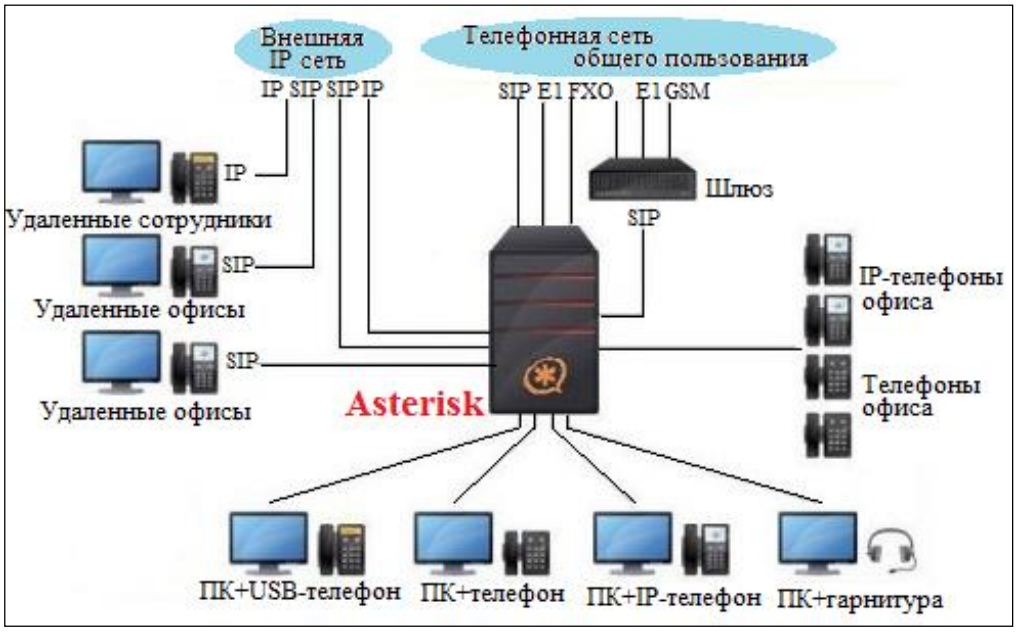


Рисунок 4.1 – Загальна схема IP-АТС Asterisk

До програмної IP-АТС Asterisk можуть бути підключені як програмні телефони (софтфоны), так і усі різновиди апаратних телефонів, призначених для користувача IP телефонів (з інтерфейсами IP, USB, Wi-Fi).

4.2 Інструментальні засоби аналізу трафіка IP-телефонії

Wireshark – це аналізатор мережевих протоколів, програмне забезпечення якого виводить інформацію про прийняті, відправлені і втрачені пакети на графічно відображений інтерфейс, званий вікном відстежування трафіку, для подальшого детального розбору зібраних даних. Представляє з себе потужну систему пошуку і фільтрації пакетів по безлічі критеріїв. З 1998 р. програма мала назву Ethereal, але в 2006 р. вона була перейменована в Wireshark [37].

Аналізатор поширюється під ліцензією GNU GPL, тобто має вільний доступ до його використання або модифікації. Існують версії для більшості типів операційних систем UNIX, у тому числі GNU/Linux, Solaris, FreeBSD, NetBSD, OpenBSD, MacOSX, а також для ОС Windows.

Програма Wireshark являється некомерційним сніффером і має необхідні інструменти для моніторингу трафіку мережі і полегшення контролю мережі. Викачати її можна з офіційного сайту https://www.wireshark.org/download.html.

Wireshark здійснює моніторинг величезного числа мережевих протоколів, наприклад: IP, TCP, UDP, FTP, TFTP, DNS, HTTP, HTTPS, ICMP, SSH, NFS, SIP, RTP, RTCP, MEGACO (H.248), MGCP, стека протоколів H.323, SIGTRAN і т. д. Підтримує такі технології фізичного і канального рівнів, як Ethernet, TokenRing і FDDI, ATM.

Wireshark використовується:

- для виявлення і вирішення проблем в мережі;
- для вивчення мережевих протоколів;
- для відладки та налаштування мережевих протоколів.

Wireshark не генерує трафік, відповідно ніяк не показує себе в мережі. При цьому, не маючи системи виявлення вторгнень, виявить себе хорошим помічником у пошуках проблеми.

Wireshark має безперечну перевагу при вирішенні проблем в роботі мережі на канальному і мережевому рівнях. Це безкоштовне рішення і всі витрати зводяться до часу: встановити, освоїти і вирішити чи спробувати вирішити проблему. Кількість копій не обмежена, і можна озброїти всіх IT-фахівців, включаючи системних адміністраторів. Ідеальне і зручне рішення для перегляду пакетів, переданих по мережі.

Основним візуальним інтерфейсом аналізатора Wireshark є дамп поточного трафіка у мережі (рис. 4.2).

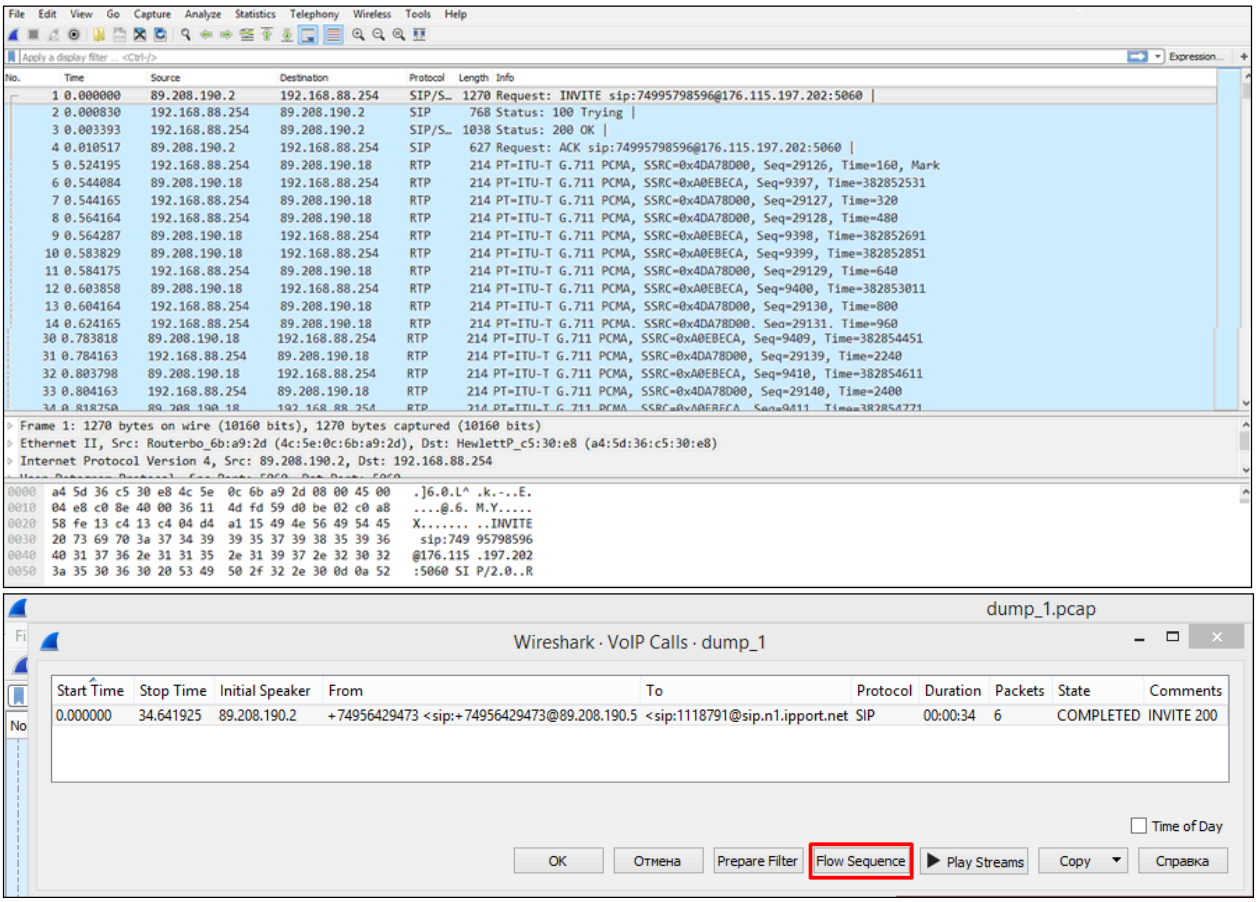


Рисунок 4.2 – Дамп трафіка Wireshark

Wireshark має безперечну перевагу при вирішенні проблем в роботі мережі на канальному і мережевому рівнях. Це безкоштовне рішення і всі витрати зводяться до часу: встановити, освоїти і вирішити чи спробувати вирішити проблему. Кількість копій не обмежена, і можна озброїти всіх IT-фахівців, включаючи системних адміністраторів. Ідеальне і зручне рішення для перегляду пакетів, переданих по мережі.

Наочне представлення набагато виразніше, ніж множина рядків в таблиці і дозволяє заощадити багато часу при аналізі, якщо пакети вбудовані в структуру і наочно видно їх послідовність. Wireshark має можливість переглядати часову діаграму потоків (рис. 4.3).

Для діагностики важливо знати час встановлення з'єднання з сервером, час проходження пакета по мережі SYN і SYN ACK, час отримання запиту HTTP до сервера і час початку відповіді на нього. Wireshark показує нам все

це, але в діаграмі присутні і інші фрейми, які ходять між пристроями. Це заважає сконцентруватися на вирішенні проблеми. Час зліва показує єдине час з моменту початку спілкування між пристроями і все дельти необхідно вираховувати вручну, щоб зрозуміти, де відбуваються основні втрати часу.

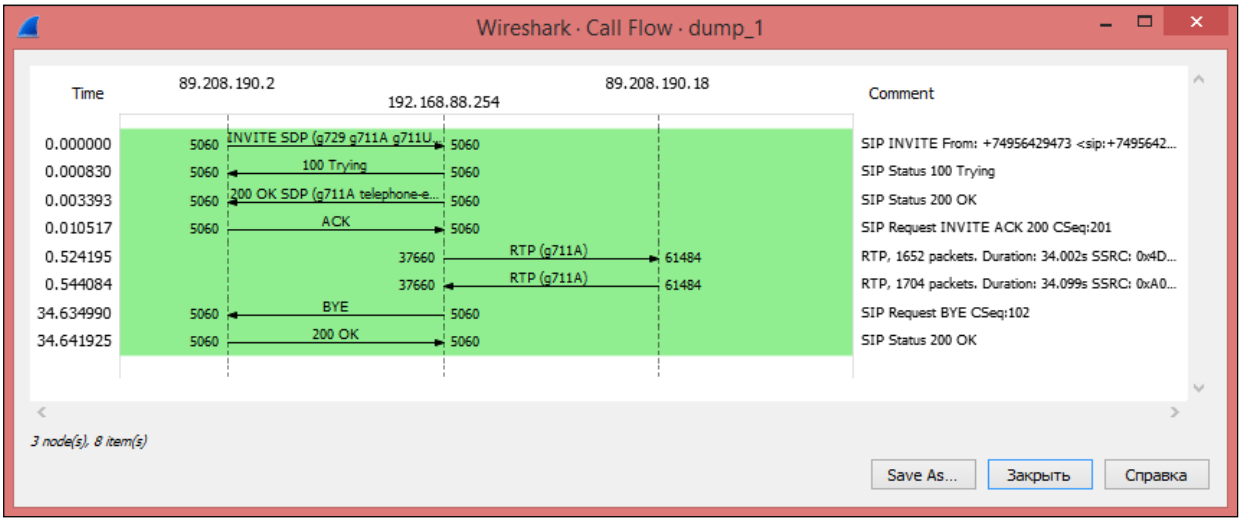


Рисунок 4.3 – Часова діаграма потоків трафіку Wireshark

При виникненні проблем в роботі додатків і сервісів дуже складно визначити справжню причину гальмування. І найпоширеніший відповідь − це мережа працює повільно, канали вузькі, оператори зв'язку не забезпечують SLA. Адже нікому не цікаво переглядати тисячі пакетів з аналізатора протоколів (сніффер). Але дуже часто проблема виявляється саме в роботі самого додатка або сервера, на якому воно розгорнуто.

Основна проблема при аналізі продуктивності інфраструктури − це зрозуміти, де відбуваються основні гальма в мережі або сервері. Для точної відповіді на це питання доводиться здійснювати захоплення трафіку на стороні користувача і на стороні сервера. Цей метод дозволить швидко відповість на поставлене запитання. При вирішенні даного завдання і Wireshark і комерційні рішення можуть працювати спільно. За допомогою Wireshark здійснюється захоплення трафіку в двох місцях (рис. 4.4).

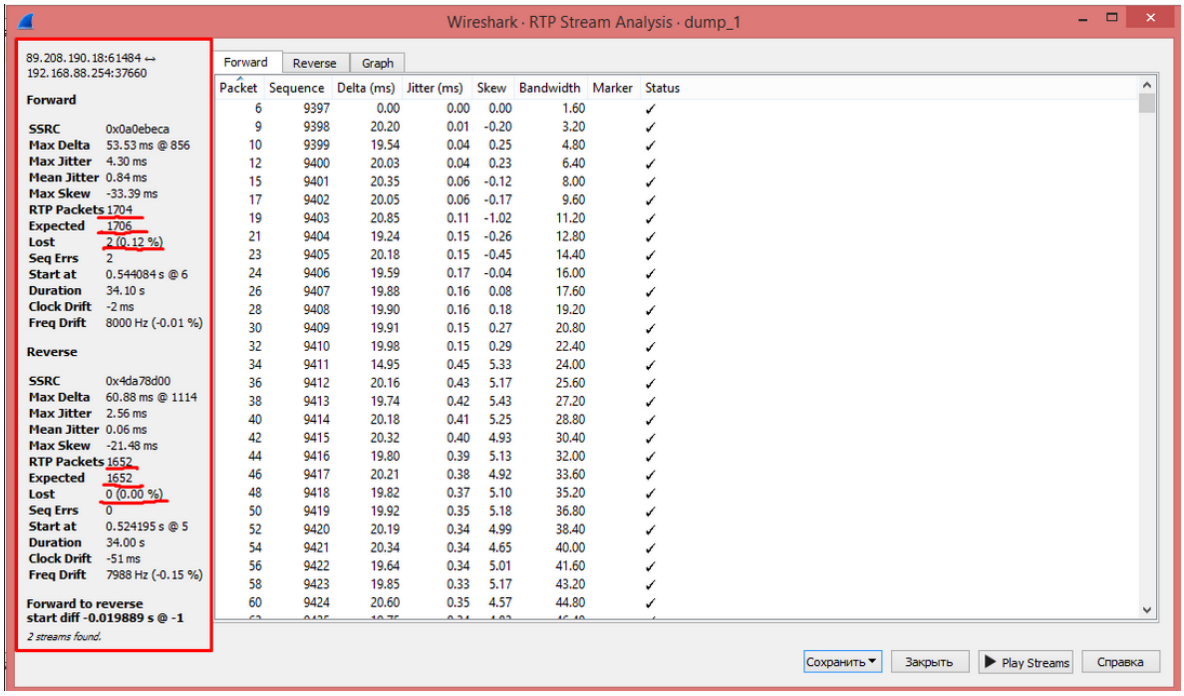


Рисунок 4.4 – Дамп трафіка обміну пакетами між двома користувачами

Ґрунтуючись на даній інформації дуже просто зрозуміти, що робити далі. Якщо час відгуку сервера істотно вище часу встановлення з'єднання (connection setup time) і немає повторних передач (TCP retransmissions), то проблема на стороні сервера. Мережа в даному прикладі ні при чому.

Якщо затримок в даній транзакції не виявлено, то потрібно переміщатися до іншого запиту, уважно відстежуючи кількість часу, який було витрачено сервером на відповідь користувача. Поступово отримавши досвід захоплення трафіку на стороні клієнта, можна переходити до аналізу трафіку на стороні сервера, так як цей аналіз дозволить зрозуміти, чим був зайнятий сервер, відповідаючи на запит користувача протягом 4,38 секунд.

4.3 Використання сервера IP-телефонії Asterisk в якості діагностичного вузла

При усіх достоїнствах розглянутої системи Asterisk, у неї є і недоліки, а саме, відсутність можливості для аналізу трафіку, що проходить через нього.

Якщо настроїти Asterisk таким чином, що звіти від усіх вузлів-учасників RTP-сессии одноадресним чином посилалися йому, то сконцентровані таким чином RTCP-пакети даватимуть усю необхідну діагностичну інформацію.

Для дослідження цієї гіпотези була розгорнута система IP-телефонії на базі IP-АТС Asterisk (рис. 4.5).

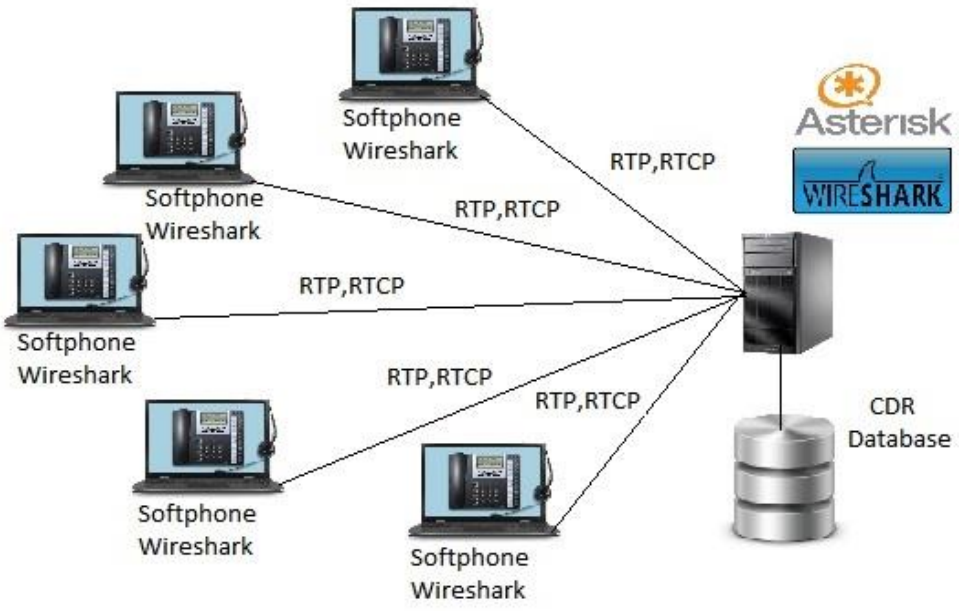


Рисунок 4.5 – Архітектура дослідницької платформи

Серверна частина PBX Asterisk була розгорнута на базі операційної системи Ubuntu, на клієнтській стороні використовувалися програмні VOIP-клиенти, так звані софтфоны, під операційною системою Windows.

Аналізатор Wireshark розташовуючись на станції хоста, використовує нерозбірливий режим прослуховування, тобто драйвер мережевого адаптера починає перехоплювати увесь трафік з каналу (promiscuous mode). Оскільки кожна ОС веде обробку трафіку по-своєму, існує загальна бібліотека Libpcap (для Linux) і WinPcap (для Windows), щоб надати загальне посилання для програмістів. Далі перехоплений трафік передається декодеру пакетів аналізатора, який розпізнає і розділяє пакети по відповідних рівнях ієрархії. ПО аналізатора вивчає пакети і відображує інформацію про них на екрані

хоста у вікні відстежування пакетів. Залежно від того які функції має продукт, представлена інформація згодом може додатково аналізуватися і фільтруватися. Крім того, Wireshark знає структуру самих різних мережевих протоколів, і тому дозволяє розібрати мережевий пакет, відображуючи значення кожного поля протоколу будь-якого рівня. Отже, цей аналізатор буде корисний для аналізу RTP/ RTCP трафіку в реальному часі при проведенні аудио-конференцзв'язку на нашому тестовому стенді.

Кожен дзвінок, здійснений будь-яким з учасників конференції, проходить через сервер IP-телефонии Asterisk. Також усі дії з кожного з дзвінків реєструються в лог-файлах сервера, які можна переглядати в режимі он-лайн (рис. 4.6).

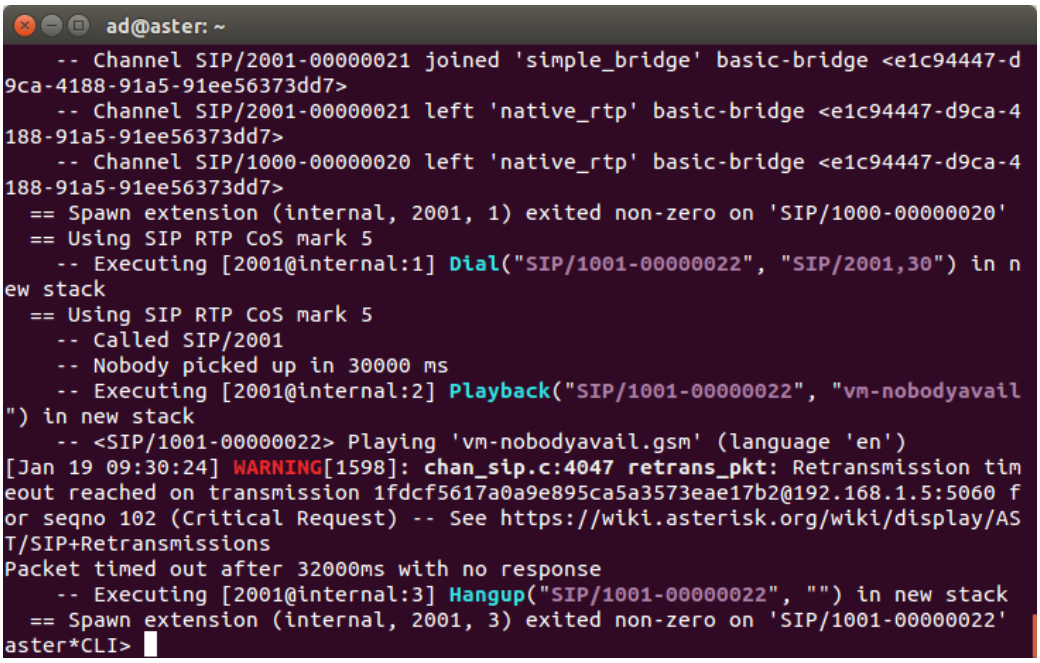


Рисунок 4.6 – Консоль Asterisk: лог дзвінка

Уся інформація про телефонні розмови записується в CDR файл (Call Detail Record). За умовчанням Asterisk записує дані CDR в CSV-файлы, що знаходяться в каталозі /var/log/asterisk/cdr, - csv.

Виконати аналіз CDR записів безпосередньо використовуючи систему Asterisk не представляється можливим. Тому для набуття значень необхідних

параметрів доставки IP-пакетов скористаємося мережевим аналізатором Wireshark, встановленим на сервері IP-телефонії Asterisk.

Мережевий аналізатор протоколів Wireshark дозволяє перехопити увесь трафік, як на серверній, так і на клієнтських сторонах. З цього трафіку за допомогою фільтрів можна виділити RTP і RTCP трафік і розглянути пакети цих протоколів зсередини (рис. 4.7, 4.8)

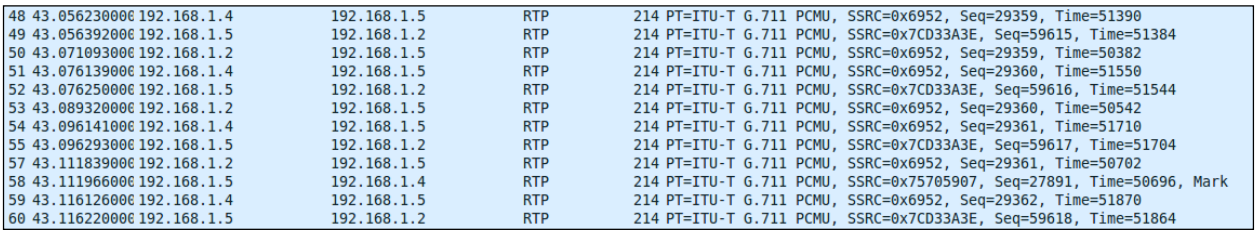


Рисунок 4.7 – Дамп перехопленого RTP-трафіка

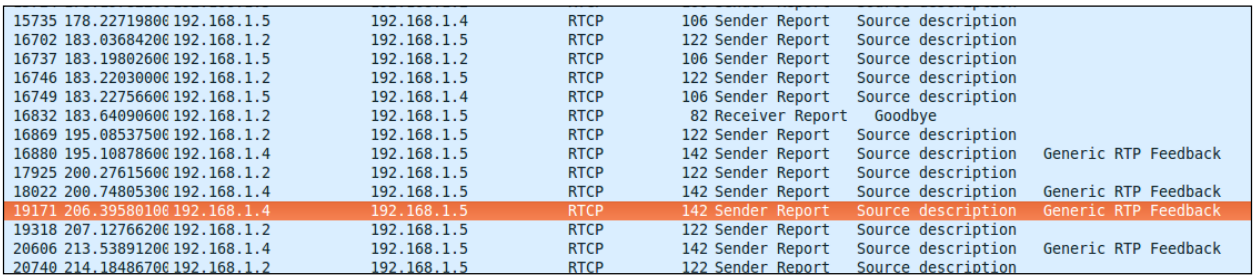


Рисунок 4.8 – Дамп перехопленого RTCP-трафіка

Аналізуючи інформацію по кожному RTCP-пакету (рис. 4.9), можна зібрати необхідну діагностичну інформацію для подальшого аналізу за допомогою запропонованої раніше СППР.

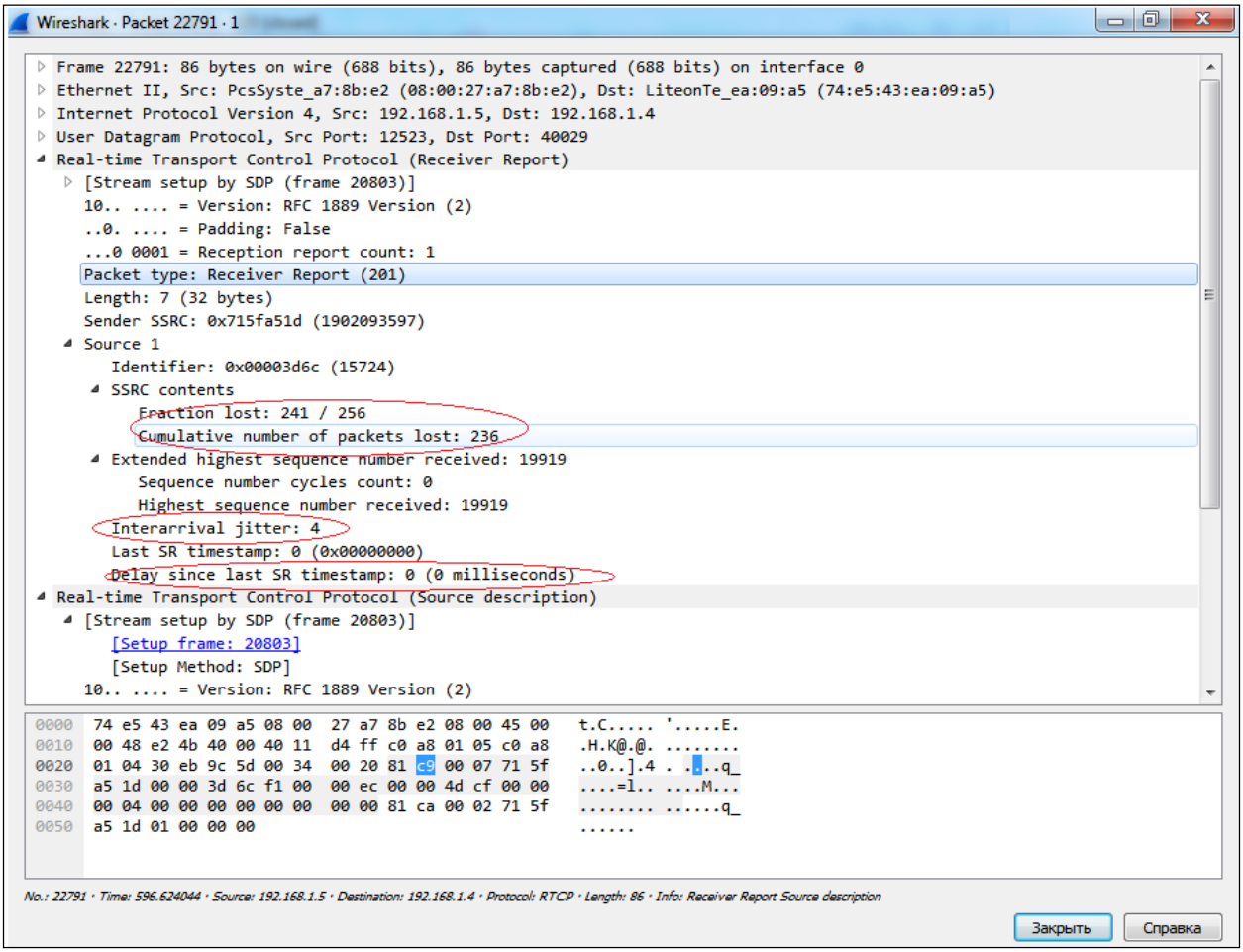


Рисунок 4.9 – Приклад детальної інформації по RTCP-пакету

На рисунку 4.10 представлена схема взаємодії сервера IP-телефонії з нечіткою СППР.

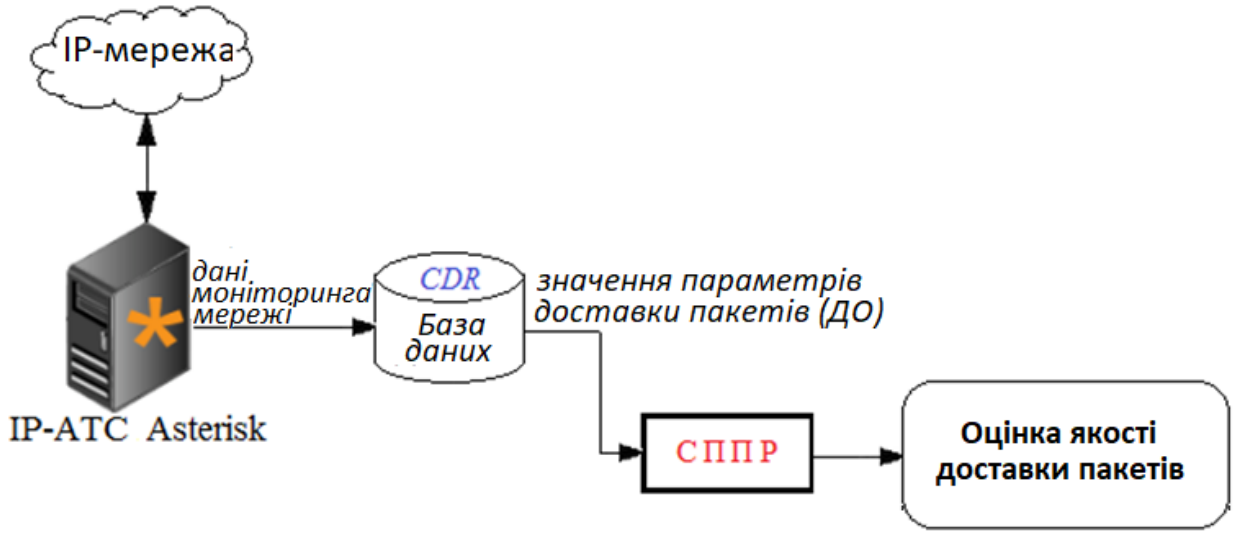


Рисунок 4.10 – Взаємодія запропонованої моделі СППР з IP-АТС Asterisk

Очевидно, що діагностичний вузол може бути реалізований як апаратно, так і програмно, але це вимагає значних витрат ресурсів. Крім того, таке завдання і не було метою цієї роботи. Для демонстрації можливості застосування концепції "діагностичного вузла" на практиці, був обраний легший шлях, де як ДВ виступав сам сервер IP-телефонії.

4.4 Рекомендації щодо поліпшення якості доставки IP-пакетів в мультисервісних мережах

Сучасні IP мережі повинні забезпечувати надійну передачу пакетів, особливо якщо мова йде про трафік реального часу. Скориставшись запропонованою моделлю системи підтримки прийняття рішення, мережеві адміністратори і інженери можуть отримати об'єктивну оцінку якості доставки IP-пакетів.

Інформація про рівень якості ляже в основу прийняття рішення про реконфігурацію параметрів мережі шляхом настройки параметрів затримки, резервування смуги пропускання, контролю за втратою пакетів і т.п.

Наведемо рекомендації щодо поліпшення якості передачі IP-пакетів в МСС, що безпосередньо впливають на той чи інший показник якості (діагностична ознака).

4.4.1 Методи зменшення затримки

В основному, в сучасних корпоративних мережах можна виділити наступні типи затримки.

1. Затримка обробки: час, який витрачає маршрутизатор на отримання пакета на вхідному інтерфейсі і відправку його в вихідну чергу на вихідний інтерфейс. Затримка обробки залежить від наступних факторів: швидкості центрального процесора, утилізації центрального процесора, архітектури маршрутизатора, налаштованих опцій на вхідних і вихідних інтерфейсів.

2. Затримка черги: час, яке пакет знаходиться в черзі на відправку. Даний вид затримки залежить від таких факторів як кількість і розмір пакетів, які вже знаходяться в черзі, смуга пропускання інтерфейсу і механізм черг.

3. Затримка сериалізаії: час, необхідний для переміщення фрейма в фізичну середу передачі.

4. Затримка поширення: час, яке займає шлях пакета від джерела до одержувача по каналу зв'язку. Ця затримка сильно залежить від середовища передачі.

Можливі методи зменшення затримки.

1. Збільшення пропускної здатності – при достатньої пропускної спроможності, скорочується час очікування в вихідної черги, тим самим, скорочується затримка серіалізації.

2. Пріоритезація чутливого до затримок трафіку – даний метод є більш гнучким. Алгоритми пріоритетності трафіку мають значний вплив на затримку, що вноситься чергою. Перерахуємо існуючі механізми QoS:

– priority queuing (PQ, пріоритетна чергу або CQ, Custom queuing);

– modified deficit round robin (MDRR, модифікований циклічний алгоритм з додатковою чергою (маршрутизатори Cisco 1200 серії));

– розподілений тип обслуговування, або Type of service (ToS) і алгоритм зважених черг (WFQ) (маршрутизатори Cisco 7x00 серії);

– class-Based weighted fair queuing (CBWFQ) або алгоритм черг, який базується на класах;

– low latency queuing (LLQ) або чергу з малою затримкою.

3. Оптимізація використання каналу шляхом компресії поля корисного навантаження. Стиснення поля корисного навантаження зменшує загальний розмір пакета, тим самим, по суті, збільшує пропускну здатність каналу передачі. Так як стислі пакети менше звичайних за розміром, їх передача займає менше часу. Важливо пам'ятати, що алгоритми стиснення досить

складні, і компресія поряд з декомпресією можуть додати додаткові затримки.

4. Стиснення заголовків пакетів – даний метод не так сильно потребує ресурсів центрального процесора, як стиснення поля корисного навантаження, тому, даний механізм часто використовується поряд з іншими алгоритмами зменшення затримки. Стиснення заголовків особливо актуально для голосового трафіку.

4.4.2 Методи зменшення частки втрачених пакетів

Втрата пакетів відбувається в мережах будь-якого типу. У кожному мережевому протоколі розроблені методи для боротьби з цією проблемою той чи інший спосіб. Наприклад, в протоколі TCP передбачена гарантована передача за рахунок повторних запитів для втрачених пакетів. Інформація передається через мережу шматочками інформації, і зазвичай розмір цих шматочків варіюється від 1 байта до 1500 байт. По дорозі через глобальну мережу Інтернет, такі пакети можуть пройти через декілька маршрутизаторів і шлюзів. Деякі з цих перевалочних пунктів можна побачити за допомогою утиліти Traceroute. Але це далеко не все реальні транзитні вузли, наприклад ви не побачите тут ті вузли, через які трафік пройшов тунелюватись (MPLS VPN, GRE і т.д.). При цьому з ненульовий часткою ймовірності, який-небудь з транзитних вузлів буде в момент проходження трафіку сильно завантажений, і знищить пакет, щоб не допускати перевантаження мережі. І чим більше таких транзитних вузлів, тим більша ймовірність втрати пакета в мережі.

Як приклад можна привести графік 4.11, показує, як може змінюватися відсоток втрачених пакетів з плином часу на одному і тому ж каналі зв'язку.

Теоретично, таке відкидання пакетів цілком нормально, так як за цілісність передачі даних стежить спеціальний протокол TCP. Але як завжди, є нюанси. Нюанси полягають у тому, що протокол TCP, в разі втрати пакету, повинен буде послати його через мережу заново.

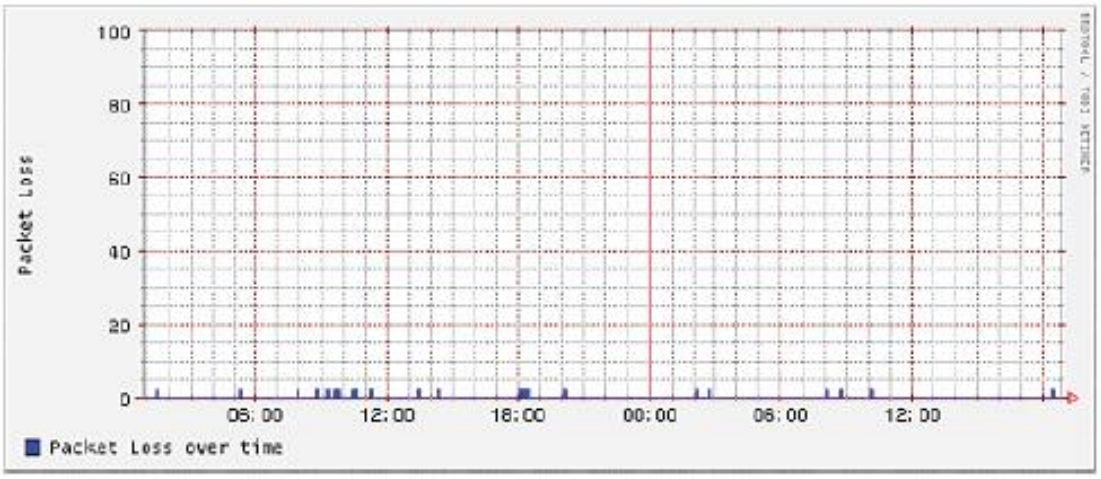


Рисунок 4.11 – Графік залежності числа втрати пакетів від часу доби

Але для того, щоб прийняти рішення про пересилку, потрібно дочекатися повідомлення від приймальної сторони, що черговий пакет не отримано. І тут на перший план виходить такий параметр мережі, як затримка сигналу. Чим вона довше, тим довше передає сторона буде в невіданні, і тим повільніше буде відбуватися передача інформації.

Нижче наведені графіки залежності швидкості передачі трафіку від затримки в каналі зв'язку і відсотка втрати пакетів (4.12).

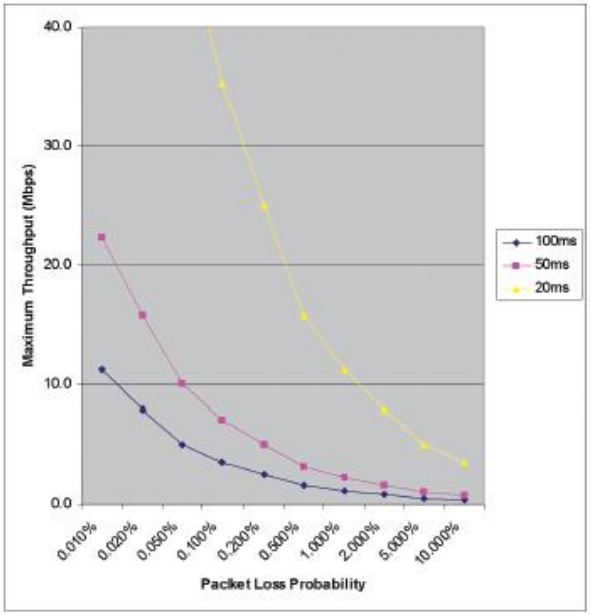


Рисунок 4.12 – Графік залежності пропускної спроможності від втрат пакетів і від затримки

Графік показує, що основна втрата в швидкості передачі в каналі з типовою для мережі Інтернет затримкою 50-100 мілісекунд, відбувається при ще цілком, здавалося б, незначному відсотку втрат 1-2%.

Якщо ж говорити про додатки, що працюють через UDP, і орієнтованих на роботу в режимі реального часу, наприклад протокол RTP, то в них не передбачений і не виправданий механізм повторної передачі. І якщо є втрати, то обов'язково вилазять артефакти у вигляді «квакання», «заїкань», і розсипається періодично зображенні.

Зазвичай втрата пакетів відбувається за умови переповнення буфера маршрутизатора. Наприклад, пакети знаходяться у вихідному на інтерфейсі черзі. У якийсь момент розмір черги досягає свого максимуму, і, нові приходять пакети просто відкидаються.

В цілому, втрата пакетів відбувається з наступних причин.

1. Втрата на вхідній черзі в разі нестачі потужності CPU маршрутизатора, в результаті чого пакети можуть бути втрачені ще на вхідному інтерфейсі.

2. Ігнорування пакетів, що відбувається в разі, якщо буфер маршрутизатора переповнений, отже, приходять пакети просто ігноруються.

3. Помилка у фреймах, наприклад, помилка CRC (Cyclic Redundancy Check).

Як правило, втрата пакетів є результатом надмірної завантаження інтерфейсу. Використовуються такі методи і алгоритми для запобігання втрат пакетів.

1. Збільшення пропускної здатності щоб запобігти перевантаженню на інтерфейсі;

2. Забезпечення достатньої пропускної спроможності і збільшення буферного простору для гарантованого переміщення чутливого до затримок трафіку в початок черги;

3. Обмежити перевантаження шляхом відкидання пакетів з низьким пріоритетом до того, як відбудеться переповнення інтерфейсу. Для

забезпечення цієї мети, може використовуватися алгоритм Weighted Random Early Detection (WRED), який буде випадково відкидати нечутливий до втрат і трафік і пакети, з заздалегідь налаштованими низькими пріоритетами.

4. Приховування втрачених пакетів (Packet Loss Concealment, PLC). Хоча в протоколі передачі даних може бути простий повторний запит втраченого пакета, у МСС немає часу чекати, поки такий пакет буде доставлений. Для підтримки якості дзвінка втрачені пакети замінюються деякими усередненими (згладженими) значеннями. Тобто даний метод передбачений для маскування ефекту зниклих пакетів в IP-мережах.

У різних реалізаціях можуть бути застосовані різні методи: заміщення нулем (zero substitution) є найбільш простим PLC-методом з мінімальними вимогами по обчислювальних ресурсів. Це простий алгоритм, в якому відсутні фрагменти звуку заміщуються тишею, що дає найгірше якість звуку, коли втрачено значну частину пакетів.

Заміщення формою сигналу (waveform substitution) використовується в старих протоколах і полягає в заміщенні втрачених пакетів новими, згенерували штучно. У найпростішому випадку втрачений пакет заміщається останнім прийнятим. На жаль, при втраті довгого ланцюжка пакетів голос, відновлений даним методом, виходить неприродним, з машинним звучанням.

Найбільш досконалі алгоритми використовують інтерполяцію пропущених ділянок, в результаті чого виходить найкращу якість звуку. Правда, за це доводиться розплачуватися підвищеною обчислювальної навантаженням. Найвдаліші рішення на базі подібних алгоритмів можуть впоратися з втратою до 20% пакетів без істотного погіршення якості звучання голосу. Незважаючи на те, що деякі PLC-методи працюють краще за інших, ніяке маскування не здатна компенсувати значні втрати пакетів. Коли внаслідок перевантаження мережі відбуваються втрати цілих серій пакетів, спостерігається помітне падіння якості звуку.

Всі розглянуті методи працюють на програмному рівні. Один із сучасних підходів боротьби за смугу пропускання на апаратному рівні запропонований компанією Silver Peak Systems.

Підхід заснований на використанні одного зі спеціальних методів кодування. Такі методи дозволяють виявляти помилки, а деякі з них навіть виправляти помилки в інформації. Наприклад, ECC коди і коди Ріда-Соломона, вперше промислово використані ще в 70-х роках при появі CD дисків. Загальний сенс таких кодів в тому, що вони вносять деяку надмірність, причому ця надмірність може адаптивно підлаштовуватися під поточні характеристики каналу. Іншим, більш наочним прикладом, може служити технологія захисту інформації на дискових масивах RAID5, яка передбачає один надлишковий дисковий накопичувач на кожні 3, 4, 5 і більше дисків з даними. У разі пакетної передачі, аналогом дисків є безпосередньо пакет – на кожні N пакетів, створюється один надлишковий.

Але проблема полягає в тому, що такі технології, що має загальне англомовне назву Forward Error Correction (FEC) застосовуються, зазвичай, тільки на фізичному рівні каналу передачі даних. І жодним чином не можуть усунути втрати інформації, пов'язані з перевантаженнями в мережі, динамічними перестроюваннями топології і т.д.

Silver Peak реалізували технологію FEC на канальному рівні так, що між будь-якими двома пристроями Silver Peak створюється свій «тунель», в якому підтримується і адаптивно підлаштовується кілька надлишкових пакетів. Типова топологія каналу зв'язку із застосуванням цього рішення і технології FEC, показана на рисунку 4.13.

На рисунку видно як пристрій на передавальній стороні генерує надмірний пакет, а пристрій на приймальній стороні відтворює на його основі іншої втрачений пакет.

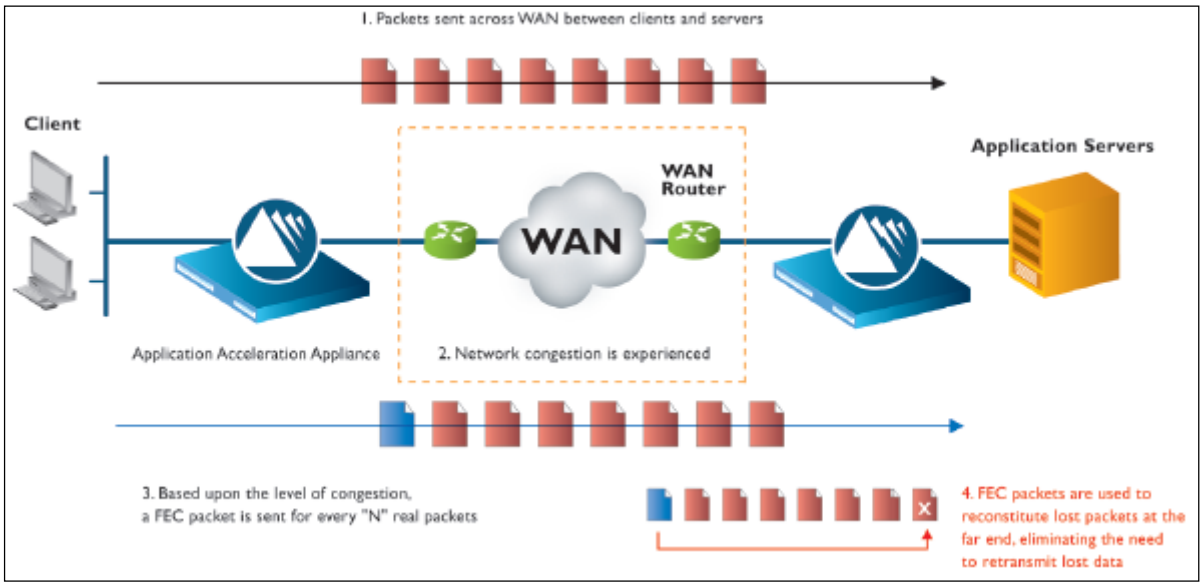


Рисунок 4.13 – Канал зв'язку із застосуванням технології FEC

Щоб оцінити ефективність застосування FEC для усунення втрат пакетів, можна подивитися на час передачі файлу через мережу Інтернет з певним відсотком втрати трафіку (рис. 4.14). З даного графіка видно, що навіть незначний відсоток надмірності, дозволяє в кілька разів підвищити швидкість передачі файлу, а проблеми «заїкання» в аудіоконференції і спотворення картинки під час відеоконференції відсутні.

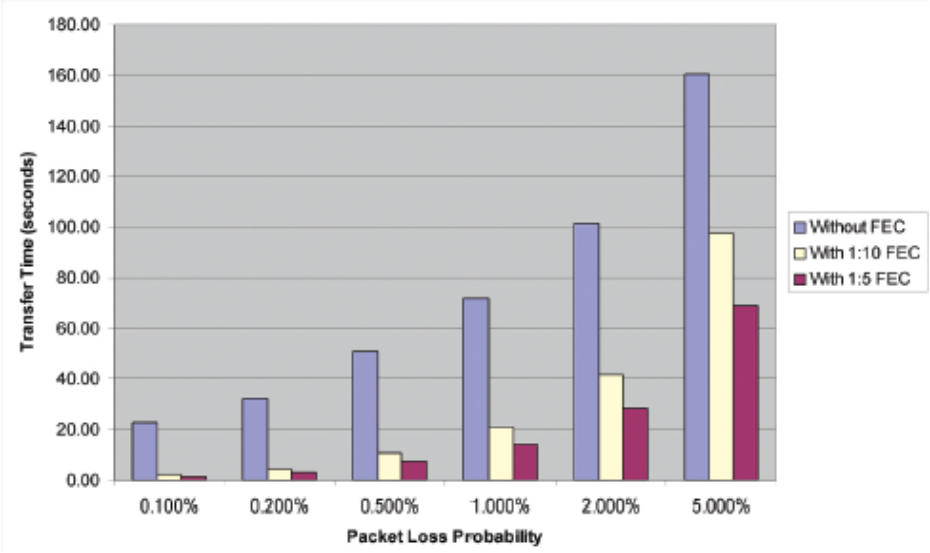


Рисунок 4.14 – Залежність часу передачі файлу від втрати пакетів при / без використання методу кодування FEC

4.4.3 Методи зменшення помилок в IP-пакеті

Пакети з даними проходять по мережі незалежно один від одного і можуть при цьому піддаватися різним затримок в залежності від точного шляху проходження. Пакети поза послідовності не зважають проблемою для передачі даних, оскільки протоколи передачі даних можуть зробити повторний запит таких пакетів і відтворити дані без спотворень. Оскільки голосові комунікації повинні відбуватися в реальному режимі часу, в IP-системах повинні бути передбачені зовсім інші методи обробки пакетів, таких не по порядку.

Деякі IP-пристрої просто відкидають всі пакети з помилками послідовності, інші відкидають їх тільки, якщо вони виходять за рамки внутрішнього буфера, що, в свою чергу, викликає джиттер. Помилки послідовності серйозно знижують якість дзвінка.

Помилки послідовності можуть виникати через способів маршрутизації пакетів. Пакети можуть проходити різними маршрутами через різні мережі, при цьому, природно, виникають різні часові показники затримки. В результаті цього пакети, що мають більш низькі порядкові номери, можуть досягати IP-пристрої пізніше в порівнянні з пакетами, порядковий номер яких вище. Пакунок зазвичай приймаються в буфер, що дає можливість станції розташувати по порядку ті пакети, які вибилися з послідовності і відновити тим самим вихідний сигнал. Однак розмір буфера обмежений для контролю джиттера, і значні відмінності в порядку прибуття пакетів за призначенням можуть привести до відкидання станцією пакетів, що в свою чергу призводить до джиттеру і втрати пакетів.

Роутінг VoIP-дзвінків по надійним маршрутами і недопущення проходження пакетів від одного дзвінка по різних шляхах може істотно знизити кількість помилок послідовності.

ВИСНОВКИ

Широка популярність мультисервісних мереж зв'язку диктують необхідність забезпечення якості обслуговування. Особа, яка приймає рішення про якість обслуговування в МСМ, а саме мережевий адміністратор, повинен знати все апаратне і програмне забезпечення мережі, її топологію, а також вміти об'єктивно оцінювати інформацію про стан мережі, отриману безпосередньо від користувачів. У такій ситуації задача прийняття оптимального рішення з оцінки якості обслуговування в МСМ найчастіше пов'язана з вибором великої і різноманітної безлічі параметрів. Як інструмент при прийнятті рішення адміністратору пропонується використовувати СППР. Для цього достатньо вибрати діагностичні ознаки, значення яких в повній мірі будуть характеризувати стан МСМ.

В якості основної характеристики якості обслуговування в мультисервісних мережах розглядаються параметри доставки IP-пакетів, а саме затримка, частка втрачених пакетів і частка помилок в переданих пакетах. Інформацію про ці показниках несуть в собі службові пакети, що відносяться до протоколу RTCP. При цьому в МСМ з ростом числа учасників зв'язку збільшується і частка широкомовного службового трафіку. Даний трафік повинен бути обмежений малою часткою смуги пропускання: настільки малою, щоб не завдати шкоди основній функції транспортного протоколу − переносу інформації.

Стандартом RFC 3550 передбачено, що частка трафіку, виділена на RTCP, фіксується на рівні не більше 5%. При перевищенні даного порогу всі RTCP пакети відкидаються, а з ними втрачається і частина діагностичної інформації про стан мережі. Дана атестаційна робота присвячена питанням аналізу трафік реального часу для підвищення якості доставки пакетів.

У даній роботі розглядаються механізми і основні вимоги, що пред'являються до передачі даних в реальному масштабі часу; основні

параметр, що визначають якість обслуговування. Також були розглянуті моделі зворотного зв'язку для протоколу RTCP, використання яких дозволяє вирішити проблему зниження навантаження на мережу і концентрації широкомовного RTP/RTCP трафіку. Досліджено їх особливості, переваги та недоліки.

Для досягнення поставленої мети використовувалася розширена модель зворотного зв'язку RTCP з введенням діагностичного вузла, яка дозволила замінити трансляцію розсилки службового трафіку від вузлів відправників, на одноадресну розсилку діагностичному вузлу. Таким чином, інформація, отримана з ДВ, стала вхідною інформацією для СППР.

В основі запропонованої СППР оцінки якості доставки пакетів в МСМ лежить розроблена нечітка мережа Петрі. Отримані результати дають можливість адміністратору мережі зробити висновок про те, яким саме чином параметри мережі впливають на якість доставки, і дати рекомендації по їх покращенню.

Крім того, виконано моделювання роботи RTCP-протоколу с діагностичним вузлом шляхом настройки сервера IP-телефонії Asterisk. Проведені експерименти показали, що без використання додаткового аналізатора протоколу (в нашому випадку Wireshark), аналіз RTCP-пакетів не можливий. Подальша робота може бути продовжена в цьому напрямку, а саме, реалізація діагностичного вузла, як надбудови над існуючими аналізаторами протоколів або безпосередньо як модуль Asterisk.

ПЕРЕЛІК ПОСИЛАНЬ

1. Степанов, С. Н. Основы телетрафика мультисервисных сетей / С. Н. Степанов. – Эко-Трендз, 2010. – 392 с.

2. Величко В.В. Телекомуникационные системы и сети. Мультисервисные сети: учебное пособие, том 3 / В. В. Величко, Е. А. Субботин. – М.: Горячая линия, 2005. – 592 с.

3. Cisco Visual Networking Index [Електронний ресурс] // Cisco system inc. – Режим доступа: https://www.digitaltveurope.com/2018/11/27/cisco-more-internet-traffic-in-2022-than-all-other-years-combined-driven-by-video/. – Дата доступу: 20.04.2020. – Загол. з екрану.

4. Вегешна, Ш. Качество обслуживания в сетях IP: пер. с англ. / Шринивас Вегешна. − М.: Издательский дом «Вильямс», 2003. – 368 с.

5. Князева Н. А. Оценка качества услуг связи с позиции удовлетворенности потребителей / Н. А. Князева, А. С. Кальченко // Science and education a new dimension: Natural and technical science. – Budapest. – 2013. − Vol. 8. − С. 156-161.

6. Вередюк А. М. Експертна оцінка якості IP-телефонії споживачами / А. М. Вередюк, Т. В. Мелешко // Вісник інженерної академії України. – 2010. – №3-4. – С. 66-69.

7. Поштаренко В. М. Обеспечение качества обслуживания на критических участках мультисервисной сети / В. М. Поштаренко, А. Ю. Андреев, Амаль Мерсни // Вісник НТУ «ХПІ». Серія: Техніка та електрофізика високих напруг. – 2013. − № 60 (1033). – С. 94-100.

8. Мурадова А. А. Методы оценки качества передачи речевых пакетов при исследовании надежности сети NGN / А. А. Мурадова // Ежемесячный научный журнал «Молодой ученый». Раздел: Технические науки. – Казань, 2013. – №10 (57). – С. 162-168.

9. Саенко В. И. Метод уменьшения нагрузки служебного трафика в компьютерной сети / В. И. Саенко, Т. А. Коленцева // Радиоэлектроника и інформатика – 2011. – Вып. 2. – С. 35-40.

10. Спирина Е. И. Метод маршрутизации, обеспечивающий повышение пропускной способности IP сетей в условиях внутрисистемных помех / Е. И. Спирина, С. В. Козлов [Электронный ресурс] // Журнал радиоэлектроники. − 2015. − № 12. − Режим доступа: http://jre.cplire.ru/koi/dec15/3/text.pdf − Дата доступа: 02.03.16. – Загл. с экрана.

11. Pascual D.G. Artificial intelligence tools: Decision support systems in condition monitoring and diagnosis / D.G. Pascual. – Boca Raton: CRC Press, 2015. – 549 P.

12. Язловецкий Я.С. Сравнительный анализ экспертных систем контроля качества обслуживания в сетях передачи данных / Я.С. Язловецкий, Л.Н. Величко // Вестник связи: Стандартизация и метрология. – 2015. – № 2 (130). – P. 49-54.

13. Герасимова Е.К. Создание системы оценки и управления качеством корпоративной информационно-вычислительной сети / Е. К. Герасимова, Г. И. Горемыкина, И. Н. Мастяева // Фундаментальные исследования. – 2014. – № 8 (часть 4). – С. 903-908.

14. Jaber, M. Using neural networks for quality management / M. Jaber, J. Combaz, L. Strus, J.-C. Fernandez // Emerging technologies and factory automation. – 2008. – P. 1441-1448.

15. Golmohammadi A. Prioritizing service quality dimensions: a neural network approach / A. Golmohammadi, B. Jahandideh // World Academy of Science, Engineering & Technology. – 2010. – Issue 42. – P.602-605.

16. Schulzrinne A. Real Time Streaming Protocol (RTSP) / A. Schulzrinne, A. Rao, R. Lanphier [Электронный ресурс] // RFC 2326, 1998. − Режим доступа: https://www.ietf.org/rfc/rfc2326.txt .− Дата доступа: 02.03.16. – Загл. с экрана.

17. Schulzrinne H. RTP: A Transport Protocol for Real-Time Applications / H. Schulzrinne, S. Casner , R. Frederick, V. Jacobson // RFC 3550, 2003. – 89 p.

18. Гольдштейн Б. С. Протоколы IP-телефонии: RTP, RTCP: учебное пособие / Б. С. Гольдштейн, В. Ю. Гойхман, Ю. В Столповская. – СПб.: Изд-во «Теледом» ГОУВПО СПбГУТ, 2012. – 50 с.

19. МСЭ-Т Recommendation G.114. One-way transmission time // December 2002.

20. МСЭ-Т Recommendation Y.1540. IP Packet Transfer and Availability Performance Parameters // December 2002. – 56 p.

21. Макаренко С. И. Время сходимости маршрутизации при отказах в сети / С. И. Макаренко // Системы управления, связи и безопасности. – 2015. − №2. – С. 45-98.

22. МСЭ-Т Recommendation Y.1541. Network Performance Objectives for IP-Based Services//May 2002 – 78 p.

23. Рекомендация МСЭ-Т Е.800. Определение терминов, относящихся к качеству обслуживания [Электронный ресурс] // Международный союз электросвязи. – Режим доступа: www.itu.int. − Дата доступа: 02.03.20. – Загл. с экрана.

24. Рекомендация МСЭ-Т Е.802. Принципы и методики определения и применения параметров QoS [электронный ресурс] // Международный союз электросвязи. – Режим доступа: www.itu.int . − Дата доступа: 02.03.20. – Загл. с экрана.

25. Braden R. Resource ReSerVation Protocol (RSVP). Version 1. Functional Specification [электронный ресурс] / R. Braden, L. Zhang, S. Berson, S. Herzog, S. Jamin // RFC 2205, 1997. − Режим доступа: https://tools.ietf.org/pdf/rfc2205.pdf. − Дата доступа: 02.03.20. – Загл. с экрана.

26. Гольдштейн А. Б. Технология и протоколы MPLS / А. Б. Гольдштейн, Б. С. Гольдштейн. – СПб.: БХВ-Петербург, 2005.– 304 с.

27. Кривуля, Г.Ф. Ввод диагностического узла в модель обратной связи RTCP для видеоконференций с централизованной архитектурой / Г. Ф. Кривуля, А. В. Бабич, А. Ю. Мова // Информационно-управляющие системы на железнодорожном транспорте. – Харьков: УкрГАЖТ, 2012. – Вып. №4 (95). – С. 67-70.

28. Ott J. RTCP Extensions for Single-Source Multicast Sessions with Unicast Feedback / J. Ott, J. Chesterfield, E. Schooler // IETF draft, AVT-RTCP-SSM, March 2007. – 66 p.

29. Орлов, А. И. Экспертные оценки: учебное пособие /А. И. Орлов. – М.: Изд-во «Экзамен», 2002. – 31 с.

30. Ситник В. Ф. Питання таксономії СППР // Зб. “Проблеми впровадження інформаційних технологій в економіці та бізнесі”. – Ірпінь: Академія ДПС України, 2001. – С. 428-432.

31. Леоненков, А. В. Нечеткое моделирование в среде MATLAB и fuzzyTECH / А. В. Леоненков. – СПб.: БХВ-Петербург, 2005. – 736 с.

32. Симанков, В.С. Моделирование сложных объектов в режиме реального времени на основе сетей Петри / В.С. Симанков, Д.М. Толкачев // Вестник Адыгейского государственного университета. Сер.: Естественно-математические и технические науки. – 2012. – Вып. 4. – С. 202-209.

33. Кузьмук В.В. Класифікація мереж Петрі та приклади їх застосування для розв‘язання прикладних задач / В.В. Кузьмук, А.М. Парнюк, О.А. Супруненко // Восточно-Європейский журнал передових технологій. – 2011. – № 2/9 (50). – С. 40- 43.

34. Борисов В.В. Нечеткие модели и сети / В.В. Борисов, В.В. Круглов, А.С. Федулов. – 2-е изд., стереотип. – М.: Горячая линия –Телеком, 2012. – 284 с.

35. Проститенко, О.В. Моделирование дискретных систем на основе сетей Петри : учебное пособие / О .В. Проститенко, В.И. Халимон, А.Ю. Рогов. – СПб.: СПбГТИ(ТУ), 2017. − 69 с.

36. Акинина Н.В. Теория и практика применения нечетких сетей Петри для мониторинга экологических рисков / Н.В. Акинина, В.Г. Псоянц, А.Н. Колесенков, А.И. Таганов // Вестник Томского государственного университета. Управление, вычислительная техника и информатика. – 2017. – № 41. – С. 4-11.

37. Анализ и получение аудио из RTP в Wireshark [Электронный ресурс] / VoxLink – IP-телефония на базе Asterisk. – Режим доступа: www / URL: https://voxlink.ru/kb/asterisk-configuration/analiz-i-poluchenie-audio-iz-rtp-v-wireshark/ – 26.03.2020 г. – Загл. с экрана.