МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ Скарга-Бандурова І.С.
«____»_____ 20__ р.

МАГІСТЕРСЬКА РОБОТА

НА ТЕМУ:

Система підтримки прийняття рішень для оцінки якості функціонування спеціалізованих комп'ютерних мереж

Освітньо-кваліфікаційний рівень "Магістр"
Спеціальність 123 "Комп'ютерна інженерія"
(освітня програма - "Комп'ютерні системи і мережі")

Науковий керівник роботи: _____ (підпис) В.А. Ларгін (ініціали, прізвище)

Консультант з охорони праці: _____ (підпис) Я.О.Критська (ініціали, прізвище)

Студент: _____ (підпис) І.О. Калюжний (ініціали, прізвище)

Група: КСМ -16дм

Сєвєродонецьк 2018

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра комп'ютерних наук та інженерії
Освітньо-кваліфікаційний рівень "магістр"
Спеціальність 123 – "Комп'ютерна інженерія"
(шифр і назва)
Спеціалізація "Комп'ютерні системи і мережі"
(шифр і назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри комп'ютерної інженерії
д.т.н., доц. *І.С. Скарга-Бандурова*
«_____» _____20____р.

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Калюжному Ігору Олексійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Система підтримки прийняття рішень для оцінки якості функціонування спеціалізованих комп'ютерних мереж

керівник проекту (роботи) Ларгін В.А., к.т.н., доцент
(прізвище, ім.'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від «18» 10 2017 р. № ____
2. Строк подання студентом роботи 18.01.2018
3. Вихідні дані до роботи Матеріали науково-дослідної практики.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз якості трафіку в мультисервісних мережах; моделі забезпечення якості обслуговування; технологія MPLS; управління перевантаженнями; забезпечення якості МСМ на базі протоколів RTP/RTCP; експертне оцінювання якості обслуговування в МСМ; моделювання трафіку реального часу в МСМ, побудованої на базі IP АТС Asterisk; рекомендації щодо поліпшення якості доставки IP-пакетів в мультисервісних мережах; охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Електронні плакати

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	*Критська Я.О.*		

7. Дата видачі завдання *06.09.2017*

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Формування технічного завдання	*19.10.17-25.10.17*	
2	Збір необхідної інформації щодо механізмів процесів передачі даних в реальному масштабі часу	*26.10.17-05.11.17*	
3	Дослідження та аналіз якості трафіку в мультисервісних мережах	*06.11.17-20.11.17*	
4	Розробка моделі забезпечення якості обслуговування	*21.11.17-30.11.17*	
5	Розробка системи підтримки прийняття рішення при оцінці якості доставки пакетів в мультисервісній мережі	*01.12.17-26.12.17*	
6	Охорона праці	*27.12.17-03.01.18*	
7	Оформлення пояснювальної записки	*04.01.18-17.01.18*	

Студент _____ *Калюжний І.О.*
(підпис) (прізвище та ініціали)

Науковий керівник _____ *Ларгін В.А.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Калюжний І.О. Система підтримки прийняття рішень для оцінки якості функціонування спеціалізованих комп'ютерних мереж.

Метою роботи є розробка системи підтримки прийняття рішення (СППР) при оцінці якості доставки пакетів в мультисервісній мережі (МСМ) 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. Для оцінки якості доставки пакетів в МСМ запропонована система підтримки прийняття рішення, в основі якої лежить нечітка модель оцінки якості.

Ключові слова: мультисервісна мережа, передача даних, трафік реального часу, якість обслуговування, RTP, RTCP.

АННОТАЦИЯ

Калюжный И.А. Система поддержки принятия решений для оценки качества функционирования специализированных компьютерных сетей.

Целью работы является разработка системы поддержки принятия решения (СППР) при оценке качества доставки пакетов в мультисервисной сети (МСС) путем концентрации служебного трафика (RTCP-пакетов) на одном диагностическом узле. Рассматриваются механизмы процессов передачи данных в реальном масштабе времени, модели обратной связи для протокола RTCP. Для оценки качества доставки пакетов в МСС предложена СППР, в основе которой лежит нечеткая модель оценки качества.

Ключевые слова: мультисервисные сети, передача данных, трафик реального времени, качество обслуживания, RTP, RTCP.

ABSTRACT

Kalyuzhniy I.O. Decision support system for assessing the quality of functioning of specialized computer networks.

The aim of certification diploma is to develop a decision support system (DSS) 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. To assess the quality of packet delivery in MSN, a decision support system, which bases on fuzzy model of the quality assessment, 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.

Keywords: multiservice networks, data transmission, real-time traffic, quality of service, RTP, RTCP.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

NGN - Next generation network, мережа нового покоління

МСМ - Мультисервісні мережі зв'язку

QoS - Quality of services, якість обслуговування

IP - Internet протокол

IPDV - Варіація затримки IP-пакетів

IREP - Частка спотворених IP-пакетів

IPLR - Частка втрачених IP-пакетів

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

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

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

VoIP - Voice over Internet Protocol, технологія, що дозволяє використовувати МСМ для передачі мовної інформації

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

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)

СППР - Системи підтримки прийняття рішень

МСЕ - Міжнародний союз електрозв'язку

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 в Інтернет, телебачення, IP-телефонію, організацію офісних і будинкових мереж і різні мультимедійні сервіси.

В даний час для опису мережі нового покоління використовується термін «мультисервісна мережа», яка представляє собою універсальну багатоцільову середу, призначену для передачі мови, зображення і даних з використанням технології комутації пакетів (IP) [2]. Мультисервісна мережа відрізняється ступенем надійності, характерною для телефонних мереж (на противагу негарантованій 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 2014 по 2019 рр. світовий IP-трафік потроїться і досягне рекордного показника в 2 зеттабайт. 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 передбачувані потреби користувача послуги [4].

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

внутрішньосистемних перешкод. Дані публікації ще раз дозволяють переконатися в актуальності обраної теми.

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

Адміністратор, виступаючи в ролі експерта повинен:

- знати все задіянє апаратне і програмне забезпечення, щоб швидко інтерпретувати зміни будь-яких параметрів мережі;
- знати всю топологію мережі, щоб швидко визначити причину і джерела таких змін;
- вміти виділити з величезної кількісті повідомлень 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 формульованих і 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 управляти мережею. Вихід з цього становища полягає в створенні систем підтримки прийняття рішень, які допомагали б особі, що приймає рішення (ОПР), об'єктивно і 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 система 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 і 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, вирішенню якої і присвячена ця дослідницька робота.

Об'єктом дослідження магістерської роботи є трафік реального часу.

Предметом дослідження є підвищення якості доставки пакетів.

Мета і задачі дослідження. Метою 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. Для досягнення поставленої мети сформульовані та вирішені наступні задачі:

- аналіз стандартів щодо забезпечення якості обслуговування в МСМ, вибір найбільш значимих параметрів, що впливають на QoS;
- дослідження способів передачі трафіку реального часу, а також методів забезпечення QoS;
- застосування розширеної моделі зворотного зв'язку RTCP з введенням діагностичного вузла для скорочення обсягу і концентрації RTCP-трафіку;
- створення нечіткої моделі оцінки якості доставки пакетів в МСМ;
- проектуватння структури системи підтримки прийняття рішення при оцінці якості доставки пакетів;
- аналіз ефективності нечіткої моделі оцінки якості доставки пакетів в МСМ;
- реалізація експерименту по налаштуванню сервера IP-телефонії Asterisk для його подальшого використання в якості діагностичного вузла.

Наукова новизна одержаних результатів. Одержали подальший розвиток моделі зворотного зв'язку для протоколу RTCP, використання яких дозволяє вирішити проблему зниження навантаження на мережу і концентрації широкомовного RTP/RTCP трафіку.

Апробація результатів роботи. Основні результати магістерської атестаційної роботи докладалися на VIII всеукраїнської науково-практичої конференції «Майбутній науковець – 2017» (м. Сєвєродонецьк).

Практичне значення отриманих результатів полягає у можливості підвищення якості доставки пакетів.

Публікації. Основні результати магістерської атестаційної роботи опубліковано в науковій праці: матеріалах конференції.

Структура і обсяг роботи. Магістерська робота складається зі вступу, 4 розділів, висновків на 1 сторінці, списку використаних джерел з 41 найменування на 4 сторінках, додатків на 21 сторінкці. Загальний обсяг роботи складає 145 сторінок. В магістерській роботі міститься 18 таблиць, 85 рисунків.

1 АНАЛІЗ ЯКОСТІ ТРАФІКУ В МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ

Мультисервісна мережа 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 Інтернет;
- 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 щодо 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.ін.
- Другий тип - потоковий трафік (stream). Його відрізняє допуск чималих затримок і втрат. На прийомі зазвичай використовується буфер, що дозволяє згладжувати нерівномірність 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. Залежно від класу обслуговування обумовлюються 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'являють високі вимоги до затримки, тобто відносяться до надчуттєвого до затримок типу. Він характеризується високою чутливістю до втрат і змінною біговою швидкістю, тобто відрізняється високим ступенем непередбачуваності. Трафік реального часу, породжений такими процесами, як мова або відео, відрізняється більшою стійкістю до втрат (тобто відноситься до малочутливих до затримок типам додатків), є ізохронним. Це означає, що він має поріг чутливості до затримок, при перевищенні якого функціональність програми різко падає, що характеризує високий ступінь передбачуваності трафіку.

У таблиці 1.1 представлені характеристики кожного виду трафіку мультисервісної мережі.

Таблиця 1.1 - Класифікація трафіку МСМ за додатками

Тип трафика	Додатки	Вимоги	Протоколи транспортного рівня
Трафік реального часу	IP-телефонія і відео-конференцзв'язок	– чутливість до затримки; – чутливість до джиттеру затримки; – мала чутливість до втрат.	RSVP, RTP, RTCP, UDP
	Процеси управління, ігри-online	– чутливість до затримки; – чутливість до джиттеру затримки; – мала чутливість до втрат.	UDP, TCP
Потоковий	Аудіо на вимогу, відео на вимогу, інтернет-мовлення	– мала чутливість до затримки – чутливість до джиттеру затримки; – чутливість до втрат.	RSVP, SCTP, UDP, TCP
Еластичний	Конференція документів	– мала чутливість до затримки; – мала чутливість до джиттеру затримки; – висока чутливість до втрат.	TCP
	Анімація, передача файлів, e-mail	– дуже мала чутливість до затримки; – мала чутливість до джиттеру затримки; – висока чутливість до втрат.	

Таким чином, в мультисервісній мережі можемо спостерігати різні комбінації цих трьох видів трафіку.

1.1 Методи передачі даних

Передача трафіку по транспортним каналам МСМ 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 всім хостам в мережі.

Ці три типи передачі даних використовуються для різних цілей.

1.1.1 Одноадресна передача Unicast

Тип передачі даних Unicast (індивідуальний) використовується для звичайної передачі даних від хоста до хосту (рис. 1.1).

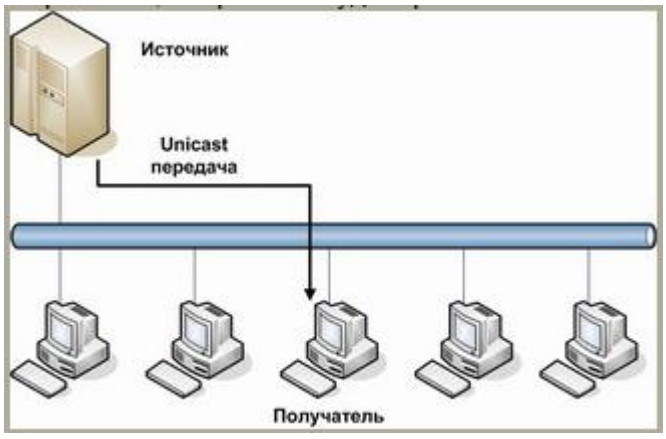


Рисунок 1.1 - Передача трафіку за технологією Unicast

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 конкретна IP адреса пристрою, для якої 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 місце в його мережі). Це все призводить до можливості маршрутизації Unicast пакетів по всій мережі.

Multicast і Broadcast пакети, на відміну від Unicast пакетів, мають свої власні спеціальні (зарезервовані) IP адреси для використання їх в заголовку пакетів як кінцеву точку маршруту. Через це Broadcast пакети в основному обмежені межами локальної мережі. Multicast трафік також може бути обмежений межами локальної мережі, але з іншого боку також може і маршрутизуватися між мережами.

Для типу передачі даних Unicast, адреси хостів призначаються двом кінцевим пристроям і використовуються (ці адреси) як IP адреса джерела і IP адреса одержувача.

Протягом процесу інкапсуляції хост розміщує свій IP адреса в заголовок Unicast пакета у вигляді адреси джерела, а IP адреса приймаючого хоста розміщується в заголовку у вигляді адреси одержувача. Використовуючи ці два IP адреси, пакети Unicast можуть передаватися через всю мережу (тобто через все підмережі).

1.1.2 Багатоадресна передача Multicast

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).

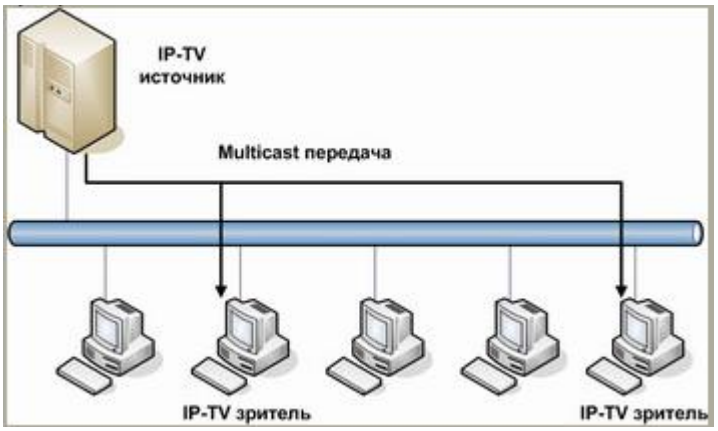


Рисунок 1.2 - Передача трафіку за технологією Multicast

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, який використовується 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 одну Multicast IP адресу призначення. Коли хост розсилає дані для Multicast групи, хост поміщає Multicast IP адресу 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.

1.1.3 Широкомовна передача Broadcast

Через те, що тип передачі Broadcast використовується для відправки пакетів до всіх хостів в мережі, пакети використовують спеціальниу Broadcast IP адресу. Коли хост одержує пакет, в заголовку якого в якості адреси отримувача вказано Broadcast адрес, 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).

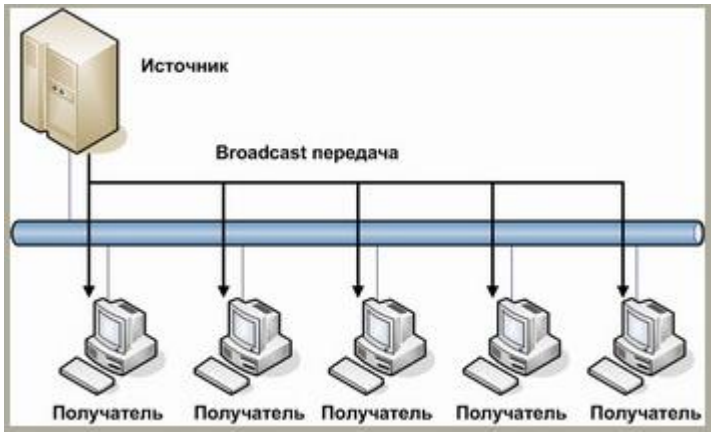


Рисунок 1.3 - Передача трафіку за технологією Broadcast

Ще коли адреса спеціальних сервісів (служб) або пристроїв заздалегідь невідома, то для виявлення також використовується Broadcast (широкомовлення).

Приклади, коли використовується Broadcast передача даних:

– створення карти приналежності адрес верхнього рівня до нижніх (наприклад, яка IP адреса на конкретному пристрої зі своєю 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, ті хто відповідає 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.

На відміну від Unicast передачі, де пакети можуть бути маршрутизовані через всю мережу, Broadcast пакети, як правило, обмежуються локальною мережею. Це обмеження залежить від налаштувань маршрутизатора, який обмежує мережу і стежить за типом широкомовлення (Broadcast).

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.

Наприклад, хост хоче відправити пакет всім хостам в мережі 172.16.5.0/24, але сам хост знаходиться в іншій мережі. В даному випадку хост-відправник вкладе в заголовок пакета в якості адреси пункту призначення Broadcast адресу 172.16.5.255. Хоча маршрутизатори повинні обмежувати (не передавати) спрямований широкомовний трафік, їх можна налаштувати на дозвіл передачі Broadcast трафіку.

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. Маршрутизатори такий широкомовний трафік не передають. Пакети, передані обмеженим Broadcast, будуть поширюватися тільки в локальній мережі. З цієї причини локальні мережі IP також називають широкомовним доменом (Broadcast domain). Маршрутизатори 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.

Приклад обмеженого Broadcast: хост знаходиться всередині мережі 172.16.5.0/24 і хоче передати пакет всім хостам в його мережі. Використовуючи як кінцеву точку

маршруту IP адреса 255.255.255.255, він відправляє широкомовний пакет. Цей пакет візьмуть і оброблять всі хости тільки в цій локальній мережі (172.16.5.0/24).

1.2 Основні протоколи передачі трафіку по мультисервісним мережам

У додатках реального часу (аудіо- і відеоконференції, живе відео, віддалена діагностика в медицині, комп'ютерна телефонія, ігри, моніторинг в реальному часі та ін.) відправник генерує потік даних з постійною швидкістю, а одержувач (або одержувачі) повинен надати ці дані додатку з тією ж самою швидкістю.

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 багатоадресної передачі;

– TCP передбачає повторну передачу втрачених сегментів, які 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 - 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 транспортних протоколів. 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 синтаксисом і операціями протокол RTSP схожий на HTTP. Однак між протоколами RTSP і HTTP є ряд істотних відмінностей. Одна 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 смугою (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.

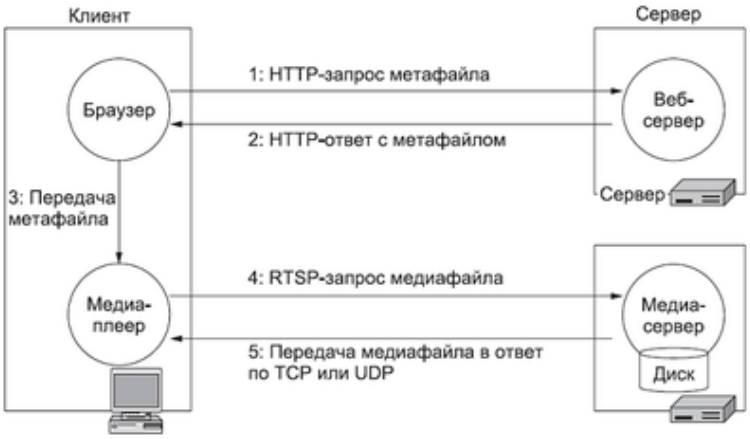


Рисунок 1.4 - Приклад використання протоколу RTSP

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); вихід 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.

IGMP вразливий до певних атак, і, якщо в ньому немає необхідності, брандмауери зазвичай дозволяють користувачеві відключити функцію IGMP.

3. 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 протокол транспортного рівня RTP може використовувати також 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 тимчасовою 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 користувачеві. 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, значення джиттера, затримки і т.д., підтримуючи зв'язок між відправником і отримувачем шляхом обміну пакетами - звіт приймача і звіт джерела. На практиці протокол RTP схожий з протоколом 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, 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].

Для більшості мультимедійних послуг, реалізованих «від кінця-в-кінець» на прикладному рівні, досить важливими параметрами є затримка пакета «від кінця-в-кінець» і джиттер, в той час як випадкова втрата пакета, найчастіше, не є перешкодою. На практиці втрата більше 1% викликає певні неприємні відчуття. При 2% розмова виявляється утрудненою. При значеннях більше 4% розмова вже практично неможлива. На рисунку 1.5 показаний процес передачі мови в мережах IP.

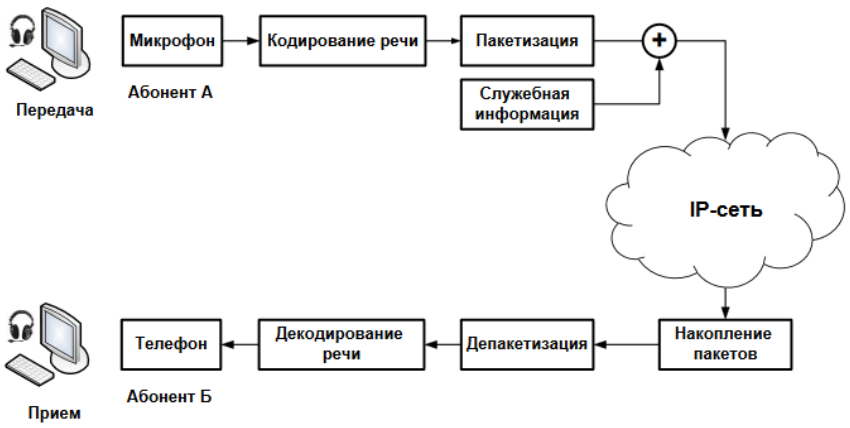


Рисунок 1.5 - Процес передачі мови по МСМ

Розглянемо, які чинники визначають сумарну величину затримки доставки пакета (наскрізна затримка доставки пакета «від кінця-в-кінець», end-to-end delay) [19].

IPTD визначається як сума чотирьох складових:

$$IPTD = Dp + Dп + Dnn + Dбд,$$

де Dp - затримка поширення: час проходження електричного сигналу в середовищі передачі даних. Цей час залежить від фізичної відстані між точкою входу і точкою виходу з мережі.

Dп - затримка пакетизації: час, який необхідно витратити в кодеку для перетворення аналогового сигналу в цифровий і формування пакету. Чим нижче швидкість сигналу на виході кодека, тим вище затримка пакетизації, оскільки кодек витрачає більше часу на процеси компресії і декомпресії сигналу;

Dnn - затримка перенесення пакета: час проходження пакета через всі пристрої мережі, розташовані уздовж шляху передачі пакета, включаючи маршрутизатори, шлюзи, мережеві екрани, обробники трафіку, сегменти мережі з відносно малою пропускною здатністю в умовах перевантаження і т.д. Для деяких пристроїв, наприклад, синхронних мультиплексорів, ця величина постійна, для інших, таких, як маршрутизатори, затримка перенесення змінюється зі зміною навантаження в мережі;

Dбд - затримка на приймальній стороні в буфері джиттера: буфер джиттера використовується для зменшення варіацій між моментами надходження пакетів на вхід приймального пристрою. Буфер може накопичувати від однієї до кількох датаграмм.

На рисунку 1.6 представлені джерела затримки при передачі мови.

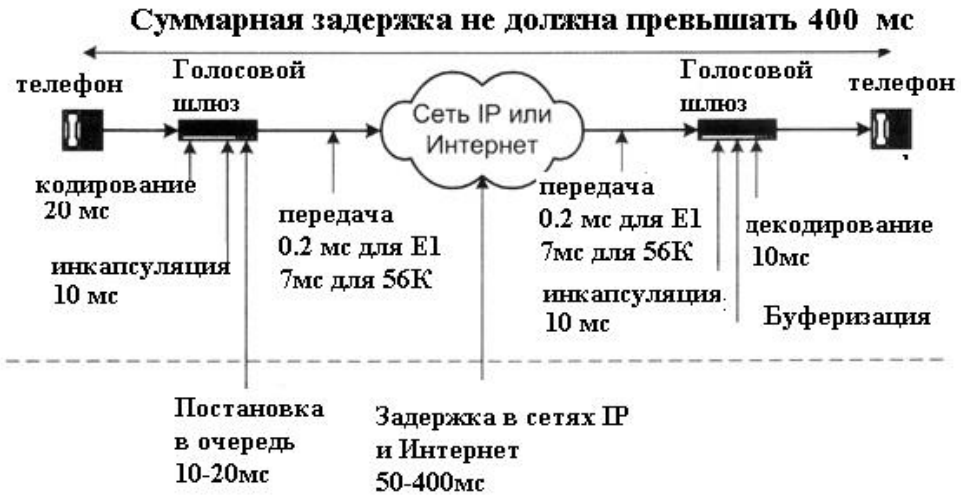


Рисунок 1.6 - Джерела затримки при передачі мови по мережі

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 [20], 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. Для порівняння можна навести спілкування через супутник: затримка при передачі по супутниковому зв'язку в одному напрямку становить приблизно 170 мілісекунд; при цьому не враховується затримка, що виникає в пристроях, розташованих на землі. Стандарт також встановлює, що при передачі голосу затримка більш ніж 400 мілісекунд є неприйнятною.

Можливі випадки, коли при передачі мови по мережі виникають набагато більші затримки, які, до того ж, змінюються випадковим чином. Цей факт є проблемою. Затримка

(або час запізнювання) визначається як проміжок часу, що витрачається на те, щоб мовний сигнал пройшов відстань від мовця до слухача. Покажемо, що і як впливає на кількісні характеристики цього проміжку часу.

Можна виділити наступні причини затримки при передачі мови від джерела до приймача:

- Затримка накопичення (іноді називається алгоритмічною затримкою): ця затримка обумовлена необхідністю збору кадру мовних відліків, яка виконується в мовному кодері. Величина затримки визначається типом мовного кодера і змінюється від невеликих величин (0,125 мкс) до одиниць мілісекунд.
- Затримка обробки: процес кодування і збору закодованих відліків в пакети для передачі через пакетну мережу створює певні затримки. Затримка кодування або обробки залежить від швидкості роботи процесора і типу алгоритму обробки.
- Мережева затримка: затримка обумовлена фізичним середовищем і протоколами, які застосовуються для передачі мовних даних, а також буферами, які застосовуються для видалення джиттера пакетів на прийомному кінці.

Ще одне явище, характерне для IP-телефонії - джиттер, або, інакше, випадкова затримка поширення пакета. Обумовлюється джиттер трьома факторами: обмежена смуга пропускання або некоректна робота активних мережевих пристроїв; висока затримка поширення сигналу; теплові шуми.

Найбільш часто застосовується метод боротьби з джиттером - джиттер-буфер, який зберігає певну кількість пакетів.

Його завдання зібрати пакети в правильному порядку відповідно тимчасовим мітками і видати їх кодеку з правильними інтервалами і в правильному порядку (рис. 1.7).

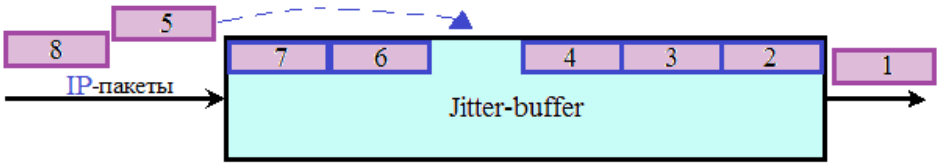


Рисунок 1.7 - Джиттер-буфер

Зазвичай передбачається динамічне підстроювання довжини буфера протягом всього часу існування з'єднання. Для вибору найкращої довжини використовуються евристичні алгоритми. Крім того, необхідно враховувати, що при стисненні інформація стає більш чутливою до помилок, які виникають при передачі, і їх не можна виправляти шляхом перезапиту саме через необхідність передачі в реальному часі.

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 слухачем;
– 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'єктивної оцінки якості послуг в телекомунікаціях. В його основу покладено так звану Е-модель, яка відкрила новий напрямок в оцінці якості послуг, пов'язаний з вимірюванням характеристик терміналів і мереж. Після створення Е-моделі було проведено велике число випробувань, в яких змінювався рівень впливу спотворюючих мережевих факторів. Дані цих тестів були використані в Е-моделі для обчислення об'єктивних оцінок. Результатом обчислень відповідно до Е-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 скороченої 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) та ін.

Таким чином, Е-модель і R-фактор можуть бути використані для об'єктивної оцінки якості передачі мови в технології VoIP.

У таблиці 1.2 відображено вплив MOS і R-Factor на сприймання якості звуку.

Таблиця 1.2 - Оцінка QoS на основі R- фактора і оцінок MOS

Рівень задоволеності користувачів	MOS		R-Factor
	категорія	Оцінка	
Дуже задоволені	Найкраща (best)	4.34-5.0	90-100
Задоволені	Висока (high)	4.03-4.34	80-90
Деякі користувачі задоволені	Середня (medium)	3.60-4.03	70-80
Багато користувачів незадоволено	Низька (low)	3.10-3.60	60-70
Практично всі користувачі незадоволені	Погана (poor)	2.58-3.10	50-60
Робота не рекомендується	Неприпустима (unacceptable)	1.0-2.58	Менщ ніж 50

Одиниці MOS пов'язані з R складної нелінійної залежністю (рис. 1.8).

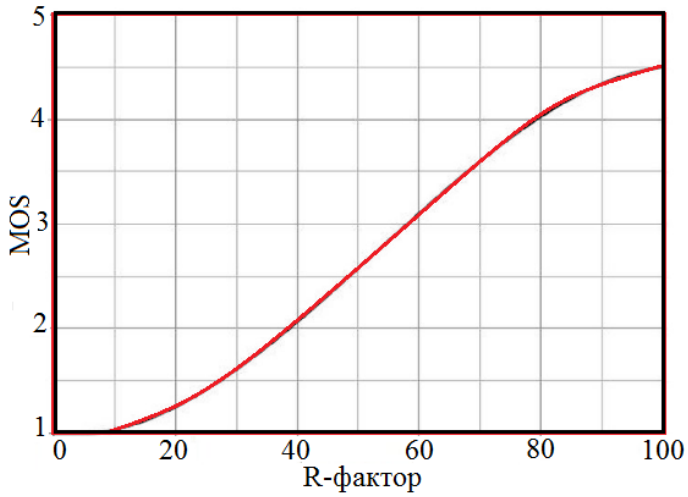


Рисунок 1.8 - Залежність MOS і R-оцінок якості передачі мови

Вищої якості R = 100 відповідає MOS = 4,5. На практиці для швидкого перерахунку в найбільш важливому діапазоні 2,5 <MOS <4,4 зручна проста лінійна апроксимація: MOS = R/20. Її похибка менше 5%, що цілком допустимо, з огляду на розкид при суб'єктивній оцінці.

Таким чином, для з'єднання хорошої якості бажано обмежитися першими трьома категоріями, забезпечити R> 70 або MOS> 3,5.

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 [21] розглядаються наступні мережеві характеристики, як найбільш важливі за ступенем їх впливу на наскрізну якість обслуговування (від джерела до одержувача), що оцінюється користувачем: продуктивність мережі; надійність мережі/мережевих елементів; параметри доставки пакетів.

1.4.1 Продуктивність мережі

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 додатків. Разом з тим, в Рекомендації Y.1541 [22] відзначено, що параметри, пов'язані з ефективною швидкістю передачі, можуть бути визначені через дескриптор трафіку мережі.

1.4.2 Надійність мережі/мережевих елементів

Користувачі зазвичай очікують високий рівень надійності від систем зв'язку. 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».

Наприклад «три дев'ятки» означають, що коефіцієнт готовності становить 0,999, що відповідає 9 годинам часу недоступності (простою) мережі в рік. Готовність телефонної мережі загального користування (ТМЗК) оцінюється величиною «п'ять дев'яток», що

означає 5,5 хв. простою в рік. У таблиці 1.3 наведені дані по часу простою для різної кількості «дев'яток».

Таблиця 1.3 - Коефіцієнти готовності і часу простою

Коефіцієнт готовності	Час простою
0,99	3,7 днів у рік
0,999	9 годин у рік
0,9999	53 хвилин у рік
0,99999	5,5 хвилин у рік
0,99999999	30 секунд у 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 значній частині базується на програмному забезпеченні (а не на апаратній, як це має місце в ТМЗК). У той же час статистику відмов в 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. 1.9) [23].

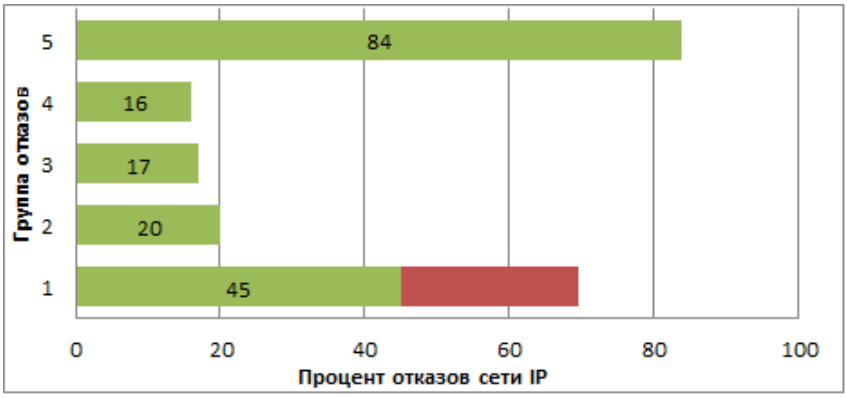


Рисунок 1.9 - Причини відмов мережевого обладнання

1.4.3 Параметри доставки пакетів IP

У загальному випадку сеанс зв'язку складається з трьох фаз - встановлення з'єднання, передачі інформації і роз'єднання. В Рекомендації Y.1540 з трьох фаз сеансу зв'язку розглядається тільки друга - фаза доставки пакетів IP. Такий підхід відображає природу мереж IP, що не орієнтовані на встановлення з'єднань. Специфікацію робочих характеристик і параметрів QoS для двох інших фаз (встановлення і роз'єднання з'єднання) планується провести в подальшому.

Рекомендація МСЕ-Т 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 вхідну точку мережі в момент t1 і виведення пакета з вихідної 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, частково, відеоінформація є прикладами трафіку, чутливого до затримок, тоді як додатки даних в основному менш чутливі до затримок. Коли затримка доставки пакета перевищує певні значення T_{max}, 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 з індексом і цей параметр визначається між вхідними і вихідними точками мережі у вигляді різниці між абсолютною величиною затримки X_i при доставці пакета з індексом і, та

певною еталонною (або опорної) величиною затримки доставки пакета IP, $d_{l,2}$, для тих ж мережевих точок: IPDV = X_i - $d_{1,2}$.

Еталонна затримка доставки пакета IP, $d_{1,2}$, 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 (рис. 1.10).

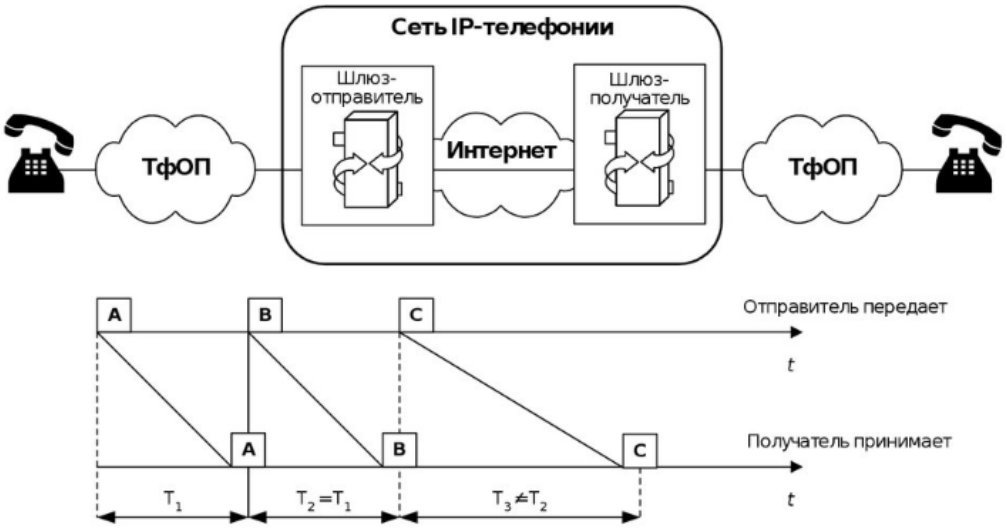


Рисунок 1.10 – Джиттер

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 T_{max}. 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 T_{max}, відкидаються, що веде до провалів в прийнятій мові. 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.

В рекомендації Y.1541 представлені норми на певні мережеві характеристики. Значення параметрів, наведені в табл. 1.4, являють собою, відповідно, верхня межа для середніх затримок, джиттера, втрат і помилок пакетів. В рекомендації Y.1541 представлені специфікації набору параметрів, які пов'язані з вимірюванням реальних значень мережевих характеристик - періоду спостережень, довжини тестових пакетів, числа пакетів і т. д. Зокрема, при оцінці якості передачі пакетів мовлення в IP-телефонії мінімальний інтервал спостереження повинен бути порядку 1-20 с при типовій швидкості передачі 50 пакетів/с. Рекомендований інтервал вимірювань для затримки, джиттера і втрат повинен становити не менше 60 с, а інформаційне поле одного пакета 1500 байт (максимальна довжина).

Таблиця 1.4 - 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 1889 (виведений з ужитку оновленням RFC 3550 у 2003 році). Спільно з протоколом UDP, RTP реалізує функції транспортного рівня (рис. 1.11).

На практиці протокол RTP невіддільний від протоколу RTCP. Останній служить для моніторингу QoS і для передачі інформації про учасників обміну в ході сесії. Протокол RTCP формує звіти, що містять інформацію про сеани зв'язку RTP. Протокол нижчого рівня повинен забезпечити мультиплексування інформаційних і керуючих пакетів, наприклад, з використанням різних номерів портів UDP.

Рисунок 1.11 - Рівні протокола RTP/UDP/IP

Завдяки багатоадресній природі протоколів RTP/RTCP, всі учасники сеансу передачі мультимедійних даних отримують звіти зворотнього 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 рівна 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 несвоєчасної реакції 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 мультимедія 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 відеоконференцзв'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 по налаштуванню 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, 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 [24] 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 [25] 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).

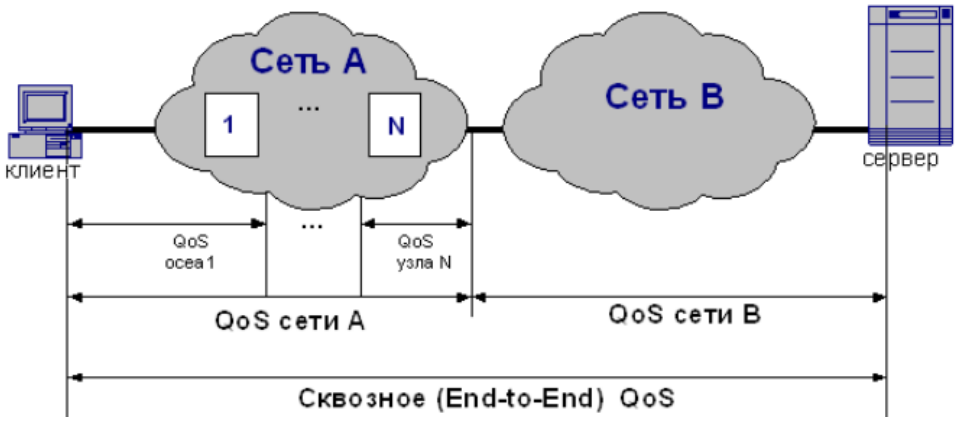


Рисунок 2.1 - Еталонна модель наскрізного QoS

Якість обслуговування можна розглядати з різних точок зору [26], а саме:

1) вимоги користувача/клієнта до QoS - заява про рівень якості, необхідну для додатків клієнтів/користувачів послуги;

2) QoS, пропоноване постачальником послуг - заява про рівень якості, який, як очікується, буде забезпечений для клієнта постачальником послуги;

3) QoS, що забезпечує/досягається постачальником послуг - заява про рівень фактичної якості, яке досягається і забезпечується для клієнта;

4) QoS, сприймається користувачем/клієнтом - заява, що відбиває рівень якості, який, на думку клієнтів, їм надається.

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, згенерованих додатками кінцевих станцій. Ці додатки 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 додатку [4].

Отже, для того щоб з'ясувати структуру існуючих в мережі запитів, необхідно визначити типи мережних додатків. Здатність мережі забезпечувати різні рівні обслуговування, запитувані тими чи іншими мережевими додатками, поряд з проведенням контролю за характеристиками продуктивності - пропускною здатністю, затримкою / тремтінням і втратою пакетів - може бути класифікована за трьома перерахованим нижче категоріями.

2.1.1 Модель негарантованої доставки даних (best-effort)

Забезпечення 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 вхідний або вихідний 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 додатків, 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 додатків включають в себе вимоги до виділення певних мережевих ресурсів в термінах смуги пропускання, затримки і рівня втрати пакетів.

Потенційно обслуговування різнорідного трафіку на базі моделі best-effort викликає дві проблеми: мережеві перевантаження і несправедливий розподіл ресурсів, звідки виникає неприйнятна якість послуг.

2.1.2 Модель інтегрованого обслуговування (IntServ)

Інтегроване обслуговування передбачає резервування мережевих ресурсів з метою задоволення специфічних вимог до обслуговування з боку потоків трафіку. Розглянемо структурну схему IntServ, представлену на рисунку 2.2.

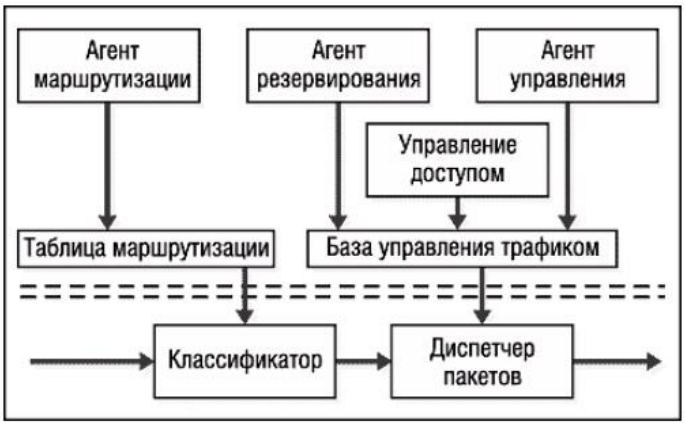


Рисунок 2.2 − Модель IntServ

У кожному вузлі, що підтримує IntServ, має бути кілька обов'язкових елементів:

- класифікатор - направляє пакет в один з класів обслуговування згідно з інформацією, отриманою з заголовків (мережевого і транспортного рівнів) пакета. Клас обслуговування реалізується у вигляді окремої черги. Всі пакети в межах одного класу обслуговування повинні отримувати однаковий QoS;
- диспетчер пакетів - витягує з кожної черги пакети і направляє їх на канальний рівень. Для IntServ запропонований двоступінчастий диспетчер пакетів. Всі вступники пакети обробляються відповідно до дисципліни обслуговування WFQ

(Weighted Fair Queuing, зважені справедливі черги) для ізоляції потоків, які отримують гарантовані послуги, від всіх інших. Потоки з керованим навантаженням і потоки best-effort поділяються за допомогою пріоритетів;

– блок управління доступом (admission control) - приймає рішення про можливість отримання трафіком необхідної кількості ресурсів, не впливаючи при цьому на раніше надані гарантії. Управління доступом виконується на кожному вузлі для прийняття або відхилення запиту на виділення ресурсів по всьому шляху проходження потоку;
– протокол резервування ресурсів - інформує учасників з'єднання (відправника, одержувача, проміжні маршрутизатори) про необхідні параметри обслуговування. Для моделі IntServ рекомендується використовувати протокол RSVP (Resource ReSerVation Protocol, протокол резервування мережевих ресурсів).

Протокол функціонує наступним чином [27]: вузол-джерело до передачі даних, що вимагають певної 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 вказаному потоку завжди надавалася необхідна пропускна здатність, а потім передає повідомлення наступному маршрутизатору уздовж шляху. В результаті по всьому шляху від вузла-відправника до адреси призначення резервується необхідна пропускна здатність. Приклад організації RSVP шляху представлений на рисунку 2.3.

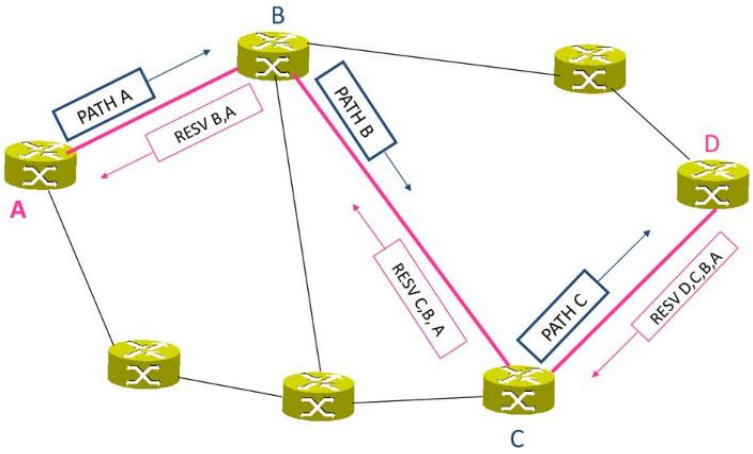


Рисунок 2.3 - Організація RSVP шляху

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. Додатки, що вимагають інтегрованого обслуговування, включають в себе мультимедійні додатки, 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 додатків Intenet-телефонії вже знадобиться канал передачі інформації з пропускною спроможністю щонайменше 8 Кбіт/с та затримки підтвердження прийому 100 мс. 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 ідеальною 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.

Але найбільший недолік IntServ пов'язаний з масштабністю RSVP, особливо в високошвидкісних магістральних мережах. Дійсно, обсяг ресурсів, які необхідні маршрутизаторам для обробки і зберігання інформації RSVP, збільшується пропорційно кількості потоків QoS. Вимірювання трафіку показують, що більшість з'єднань IP «від краю до краю» існує дуже недовго, і в кожен момент часу магістральним маршрутизатором підтримується кілька тисяч активних сполук. Отже, численні потоки IntServ в каналі з великою пропускною здатністю значно збільшують навантаження на маршрутизатори. Більш того, кожен раз при зміні топології всі зарезервовані шляхи необхідно прокладати заново.

2.1.3 Модель диференційованого обслуговування (DiffServ)

Диференціювання обслуговування 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 ідентифікаторі DSCP (Differentiated Services Code Point). DSCP - поле в IP-пакеті, що дозволяє призначити мережевому 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. Модель DiffServ описує архітектуру мережі як сукупність прикордонних ділянок і ядра. Приклад мережі відповідно до моделі DiffServ показаний на рисунку 2.4.

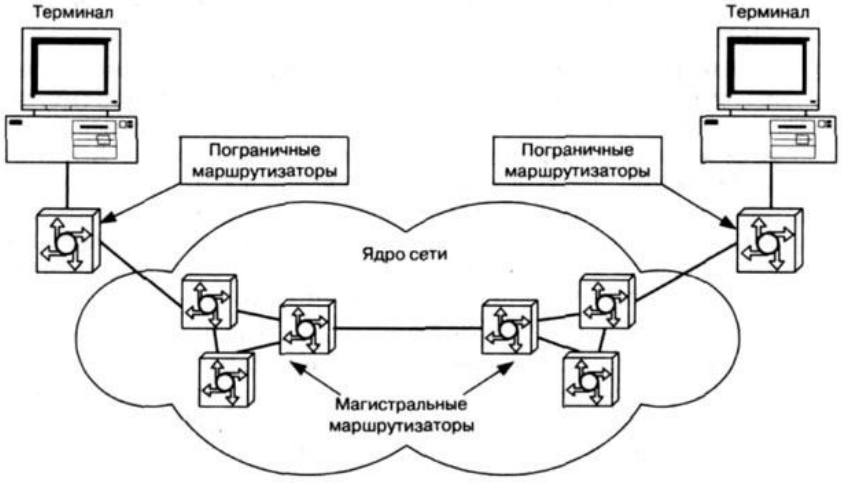


Рисунок 2.4 − Модель DiffServ

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).

Диференційоване обслуговування зручно застосовувати в мережах з інтенсивним трафіком додатків. У цьому випадку важливо забезпечити відділення адміністративного трафіку мережі від усього іншого трафіку і призначити йому пріоритет, що дозволяє в будь-який момент часу бути впевненим у зв'язності вузлів мережі.

Переваги моделі DiffServ:

- забезпечує єдине розуміння того, як повинен оброблятися трафік певного класу;
- дозволяє розділити весь трафік на відносно невелике число класів і не аналізувати кожен інформаційний потік окремо;
- немає необхідності в організації попереднього з'єднання і в резервуванні ресурсів;
- не потрібна висока продуктивність мережевого обладнання.

Однією з реалізацій моделі DiffServ є технологія многопротокольної 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. Дана технологія призначена для прискорення комутації пакетів в транспортних мережах. Основна її відмінність від раніше розглянутих в тому, що MPLS спочатку не є технологією забезпечення якості і стає такою тільки при використанні протоколу RSVP-TE (розширення протоколу RSVP для управління трафіком (Traffic Engineering)).

2.2 Технологія MPLS

Multiprotocol Label Switching - 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, а поширюється на графік будь-якої маршрутизації мережевого протоколу [28].

Технології 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.

Розмір мітки становить 4 байти: 20 біт відводяться під безпосередню ідентифікацію, 3 біта задіяні під CoS (class of services), також є 1 стоповий біт і 8 біт відведені під поле TTL (time to live) (рис. 2.5).

Рисунок 2.5 - Заголовок MPLS-мітка

Тема MPLS-мітки складається з наступних полів:

- мітка (20 біт) використовується для вибору відповідного шляху комутації по мітках;
- поле експериментальних бітів містить 3 біта, які резервовані для подальших досліджень і експериментування. В даний час проводиться робота, спрямована на створення узгодженого стандарту використання цих бітів для підтримки диференційованого обслуговування різнотипного трафіку і ідентифікації класу обслуговування (CoS). При наданні диференційованих послуг MPLS-мережі це поле може вказувати певний клас обслуговування, наприклад, аналогічний класам DiffServ;
- поле MPLS-стека S містить 1 біт і є засобом підтримки ієрархічної структури стека міток MPLS. У заголовку останньої мітки біт S = 1, а у всіх інших - біт S = 0;
- час життя TTL (8 біт) дублює аналогічне поле IP-пакета, яке є засобом скидання пакетів в мережі внаслідок утворення закільцьованих маршрутів.

Принцип роботи IP/MPLS мережі полягає в наступному. Будь-який IP-пакет на вході в мережу MPLS, незалежно від того надходить цей пакет від відправника або ж він прийшов з суміжної мережі, яка може бути MPLS-мережею більш високого рівня, відноситься до певного класу еквівалентної пересилання FEC (Forwarding Equivalence Class). Аналіз заголовка IP-пакета і призначення FEC проводиться тільки один раз на вході в мережу.

FEC ідентифікується певною міткою, що представляє собою поле фіксованої довжини, і має локальне значення на ділянці між двома сусідніми маршрутизаторами. При

переадресації пакета на наступному кроці, мітка надсилається разом з ним, таким чином, пакети виявляються поміченими ще до того, як будуть переадресовані. Прийнята з пакетом мітка використовується маршрутизатором як покажчик входу таблиці, яка визначає черговий маршрутизатор для пересилання до нього пакету, а також нову мітку для FEC, до якого відноситься цей пакет. Модуль комутації по мітках, який міститься в пакеті, як правило, замінює мітку, деякою новою міткою перед її пересиланням на наступну ділянку маршруту (label swapping). Для прийняття рішення про те, куди пересилати пакети, використовується алгоритм точного збігу міток.

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.

На рисунку 2.6 наведено приклад домену MPLS-мережі, що складається з двох граничних (LER1, LER2) і двох внутрішніх (LSR1, LSR2) маршрутизаторів комутації міток.

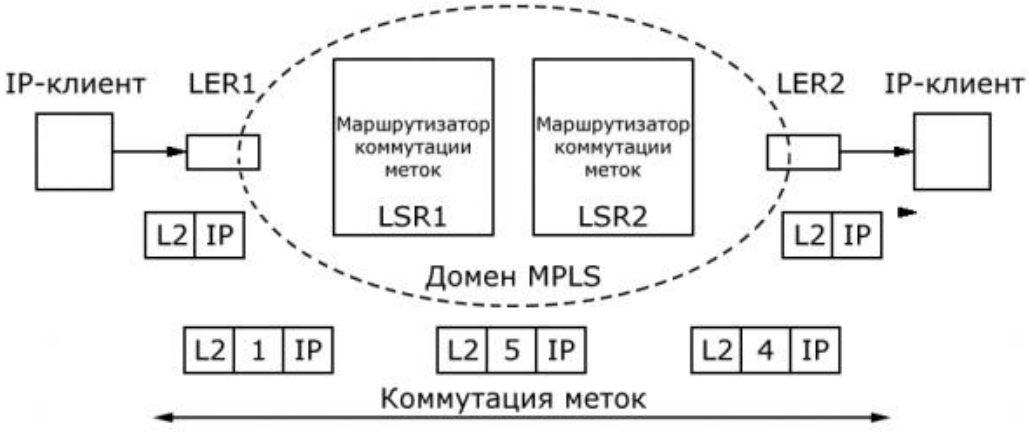


Рисунок 2.6 - Приклад комутації пакетів «дані»

Граничний маршрутизатор виконує функції призначення і видалення міток (LER1 вставляє мітку 1 пакету між заголовком IP і заголовком рівня 2 (L2), а LER2 видаляє мітку 4 в цьому пакеті IP). Шлях проходження пакетів в мережі MPLS визначається тим класом еквівалентності при пересиланні FEC, який встановлений для цього потоку у вхідному граничному маршрутизаторі LER. Такий шлях носить назву комутованого по мітках тракту LSP (Label-Switched Path) і ідентифікується набором міток у внутрішніх маршрутизаторах (LSR), розташованих на шляху прямування потоку від відправника до одержувача. Внутрішній маршрутизатор комутує пакет з міткою від одного інтерфейсу до іншого інтерфейсу з заміною мітки. LER1 приймає пакет з міткою 1 і відправляє цей пакет LSR2 з міткою 5. LSR2 приймає пакет і відправляє LER2 з міткою 4. Таким чином, мітка LER і LSR має локальне значення, як і логічні номери віртуальних каналів в мережах ATM, Frame Relay, X .25. Як видно з рисунка 2.6 просування IP-пакета відбувається на основі IP-адресної інформації тієї технології, яку MPLS використовує на ділянці між крайовою станцією і доменом MPLS і на основі міток всередині домену MPLS. L2 тут означає рівень 2.

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. Кожна така запис включає вихідну мітку, номер вихідного інтерфейсу і адресу наступного маршрутизатора в LSR.

Всі вузли MPLS використовують протоколи маршрутизації TCP/IP для обміну відповідною інформацією маршрутизації з іншими вузлами MPLS-мережі при створенні таблиці LIB. Внутрішні LSR комутують ці службові пакети не по мітках, а за звичайними IP-заголовками. Просування кадру в MPLS-мережі відбувається на основі мітки MPLS і техніки комутованого по мітках тракту LSP, а не на основі адресної інформації і тієї технології, формат кадру якої використовує MPLS. Наприклад, якщо в MPLS застосовується кадр Ethernet, то MAC-адреси джерела і приймача, хоча і присутні у відповідних полях Ethernet, але для просування кадра не задіюються.

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;
- збереження інвестицій у встановлене ATM-обладнання;

– поділ функціональності між ядром і граничною областю мережі.

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

2.3 Управління перевантаженнями. Механізм черг

Перевантаження виникає в разі переповнення вихідних буферів передавального трафік обладнання. 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).

Перерахуємо методи обробки черг.

1. Перший увійшов - перший вийшов (First In First Out, FIFO).

Елементарна черга з послідовним проходженням пакетів, що працює за принципом перший прийшов - перший пішов (FIFO) (рис. 2.7).

Рисунок 2.7 – 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 корінний недолік - неможливість диференційованої обробки пакетів різних потоків. Всі пакети стоять в загальній черзі на рівних підставах. Разом виявляються і пакети чутливого до затримок голосового трафіку, і пакети нечутливого до затримок, але дуже інтенсивного трафіку резервного копіювання, тривалі пульсації якого можуть надовго затримати голосовий пакет.

2. Черги пріоритетів (Priority Queuing, PQ).

PQ забезпечує безумовний пріоритет одних пакетів над іншими (рис. 2.8).

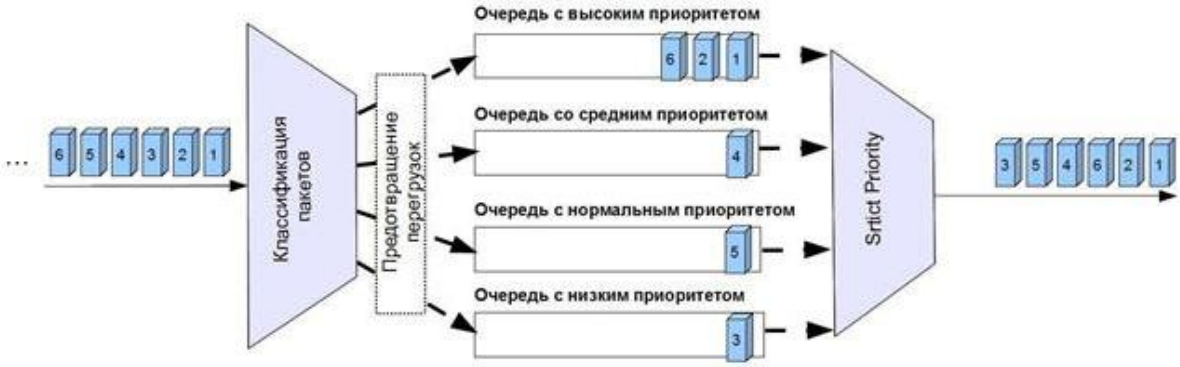


Рисунок 2.8 - Черги PQ із суворим пріоритетом

Всього 4 черги: високим (high), середнім (medium), нормальним (normal) і низьким (low). Обробка ведеться послідовно (від high до low), починається з високопріоритетної черги 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).

CQ забезпечує черги, які 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 користувачеві недоступна (рис. 2.9).

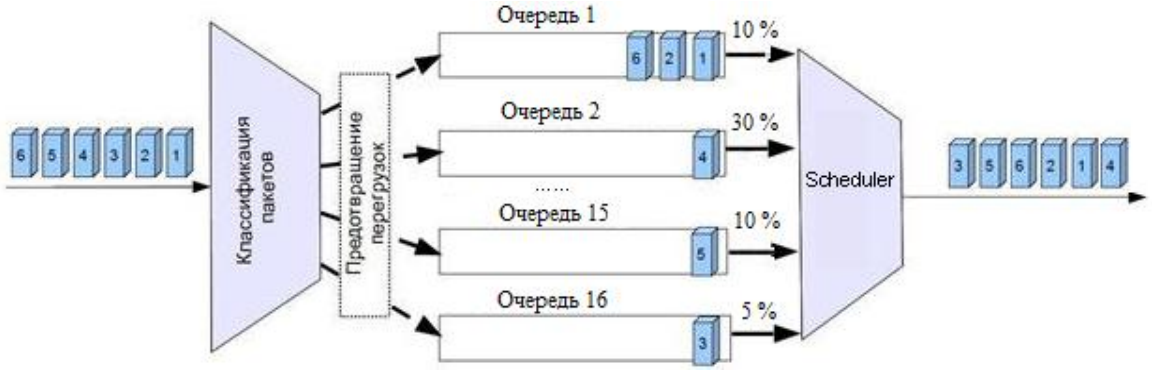


Рисунок 2.9 - Довільні черги CQ

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 нуль, то пропускається наступний пакет цілком, а не його фрагмент, рівний залишку лічильника. Так для прикладу,

представленому на рисунку 2.9, 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, ніж придушення фонових класів високопріоритетним.

4. Зважені справедливі черги (Weighted Fair Queuing, WFQ).

WFQ автоматично розбиває трафік на потоки (flows). За замовчуванням їх число дорівнює 256, але 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 2.10 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.

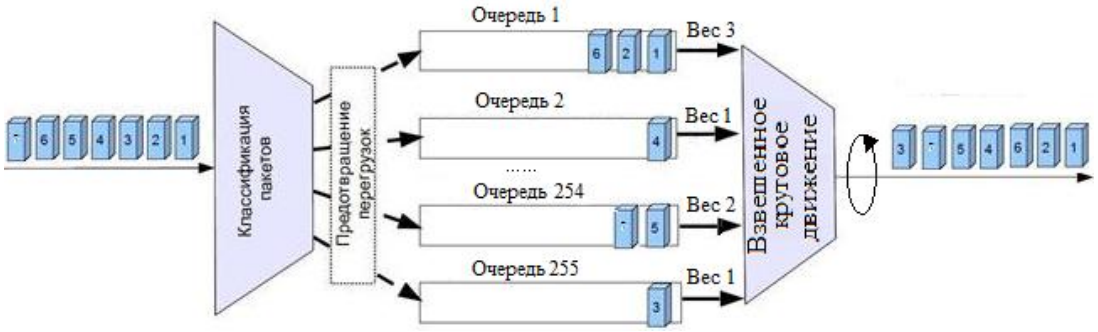


Рисунок 2.10 - Зважені справедливі черги WFQ

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).

CBWFQ відповідає механізму обслуговування черг на основі класів. Весь трафік розбивається на 64 класи на підставі наступних параметрів: вхідний інтерфейс, аксесс лист (access list), протокол, значення DSCP, мітка MPLS QoS. Загальна пропускна здатність вихідного інтерфейсу розподіляється за класами. Виділяєтму кожному класу смугу пропускання можна визначати як абсолютне значення (bandwidth в Kbit / s) або у відсотках (bandwidth percent) щодо встановленого значення на інтерфейсі (рис. 2.11).

Пакети, які не потрапляють в сконфігуровані класи, потрапляють в клас за замовчуванням, який можна додатково налаштувати і який отримує вільну смугу пропускання каналу, яка залишилася. 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.

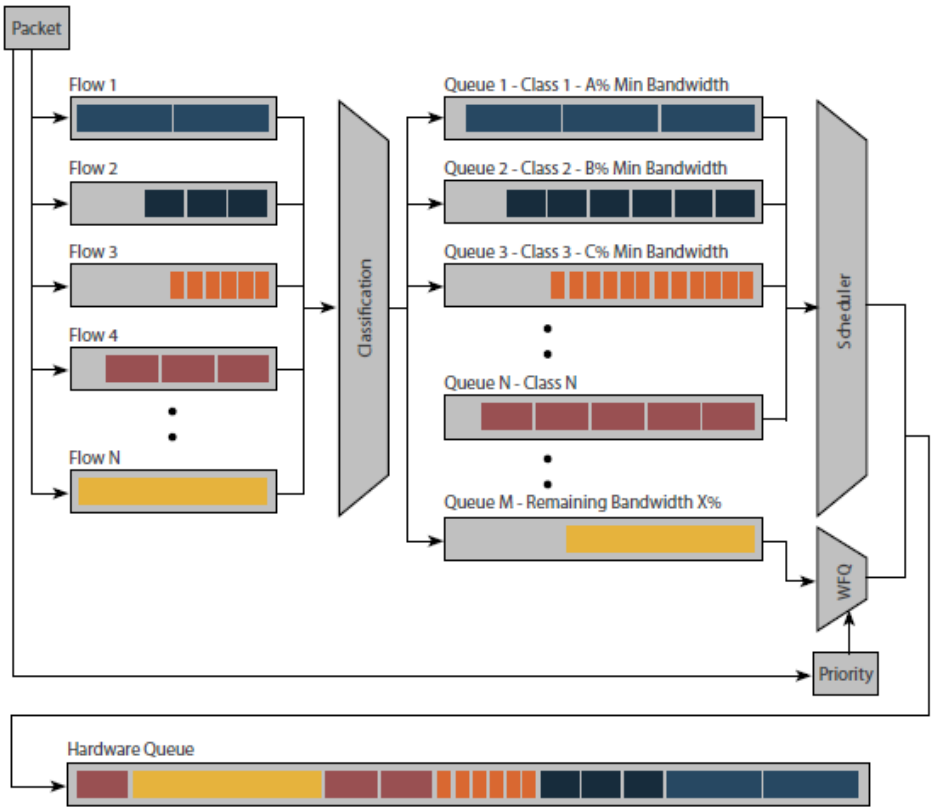


Рисунок 2.11 - Зважені справедливі черги на основі класів

6. Черговість з низькою затримкою (Low Latency Queuing, LLQ).

LLQ можна розглядати як механізм CBWFQ з пріоритетною чергою PQ (LLQ = PQ + CBWFQ) (рис. 2.12).

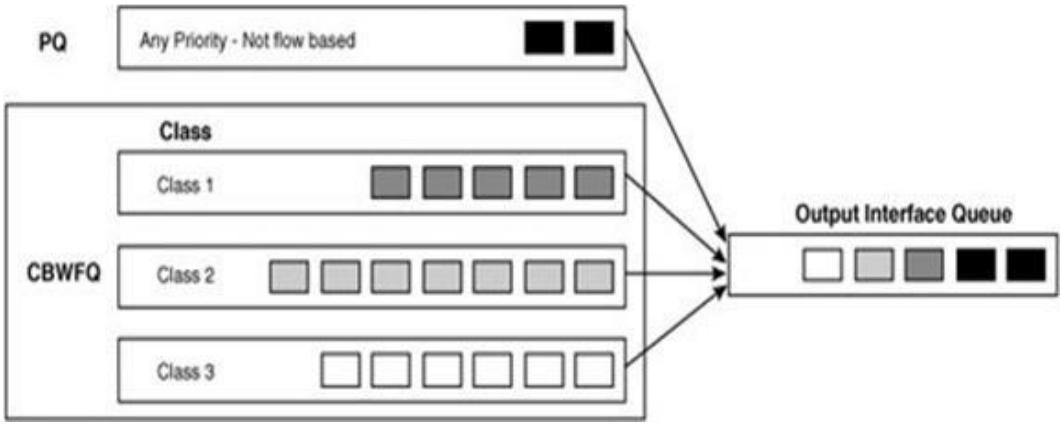


Рисунок 2.12 - Черговість з низькою затримкою LLQ

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

2.4 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 (рис. 1.11). Протокол RTP передбачає індикацію типу корисного навантаження і порядкового номера пакета в потоці, а також застосування тимчасових міток. Відправник позначає кожен RTP-пакет тимчасовою 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 пакету, що виходить, 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.2.13). 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). Ясно, що при такій структурі заголовка можлива максимум ще тільки одна версія RTP. 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 на тому, що стандарт визначає як істотні події, наприклад, початок видеокадра, 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 додатку {Application Data), наприклад, нестиснене 8-бітове аудіо MP3 і т.п. За цим кодом додаток може дізнатися, що потрібно робити, щоб декодувати дані.

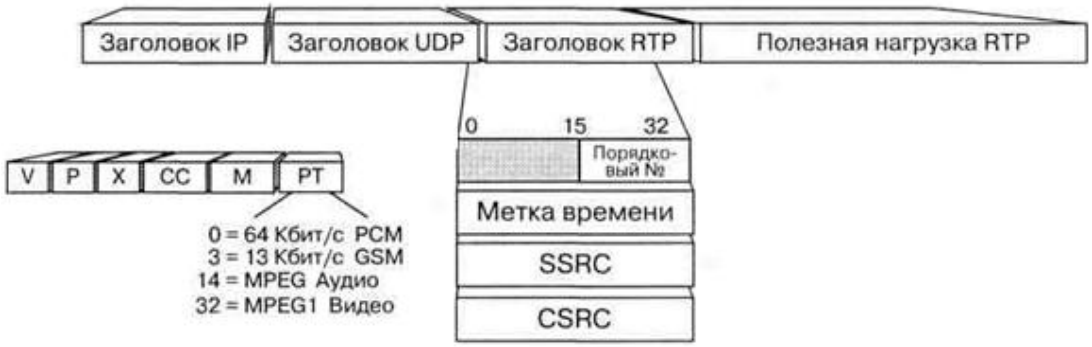


Рисунок 2.13 – Структура пакета RTP

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.

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 джиттера, 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 (джітера).

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 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 при діагностиці проблем мережі, як монітор третьої сторони. 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 програму, то одержувачам для відстеження кожного учасника вимагається 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 повинна 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 розсинхронізацію вхідних пакетів і затримку, пов'язану з підтвердженням прийому. На рисунку 2.14 представлена структура RTCP пакета звіту відправника.

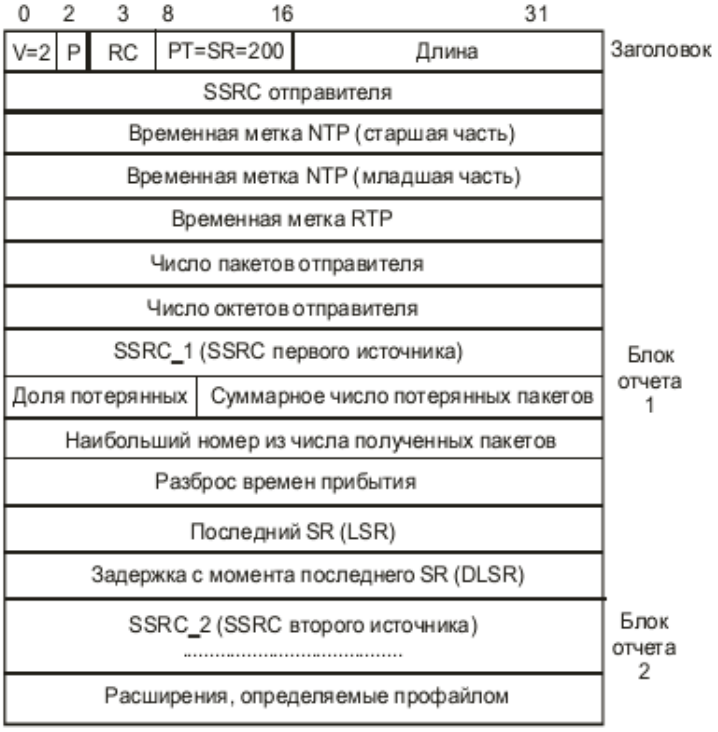


Рисунок 2.14 - Формат RTCP пакета звіту відправника

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 синхронізацію і

кількість відправлених пакетів і байтів. На рисунку 2.15 представлена структура RTCP пакета звіту одержувача.

Рисунок 2.15 - Формат RTCP пакета звіту одержувача

2. Пакет опису джерела - Source Description Items (SDES). Пакети цього типу містять інформацію про учасників сеансу. На рисунку 2.16 представлена структура RTCP пакета опису джерела.

Рисунок 2.16 - Формат RTCP пакета опису джерела

3. Пакет завершення зв'язку - BYE. Це «прощальний» пакет, за допомогою якого користувач відключається від сеансу. На рисунку 2.17 представлена структура RTCP пакета завершення зв'язку.

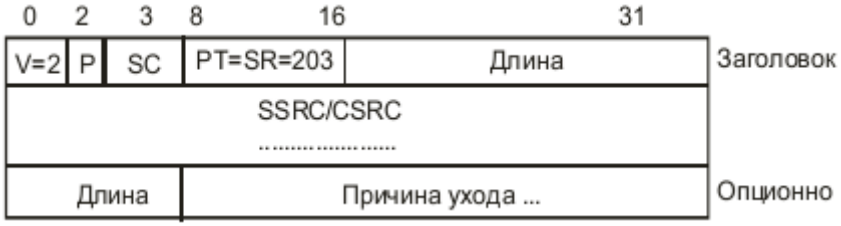


Рисунок 2.17 - Формат RTCP пакета завершення зв'язку

4. Пакет, який визначається додатком - 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 2.18 представлена структура RTCP пакета, що задається додатком.

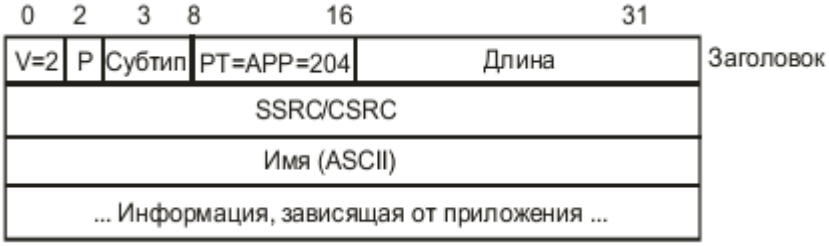


Рисунок 2.18 - Формат RTCP пакета, що задається додатком

Розглянемо функціонування проколів RTP/RTCP на прикладі такого трафіку реального часу, як аудіоконференцзв'язок і відеоконференцзв'язок.

Для організації групового аудіоконференцзв'язку потрібно багатокористувальницька групова адреса і два порти. При цьому один порт необхідний для обміну звуковими даними, а інший використовується для пакетів управління протоколу RTCP. Інформація про групову адресу і портах 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.

Додаток аудіоконференцзв'язку, що використовується кожним учасником конференції, посилає звукові дані малими порціями, наприклад, тривалістю 20 мс. Кожній порції звукових даних передує заголовок RTP; 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 змінюється порядок, а також затримуються 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 виконується 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 додатка під час конференції періодично видає на порт управління (порт RTCP) для додатків усіх інших учасників повідомлення про прийом пакетів із зазначенням імені свого користувача. Повідомлення про прийом вказує, як добре чутно поточного оратора, і може використовуватися для управління адаптивними кодерами. У доповнення до імені користувача, може бути включена також інша інформація ідентифікації для контролю смуги пропускання. При виході з конференції сайт посилає пакет BYE протоколу RTCP.

Відеоконференцзв'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 конкретною парою транспортних адрес 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 сенсах, повинен використовувати однеі тей 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.

2.4.1 Моделі зворотного зв'язку для протоколу RTCP

Завдяки багатоадресній 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 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 багатоадресного 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 [29]. Проста модель зворотного зв'язку (рис. 2.19) - базовий механізм «відображення» RTCP-трафіку, де кожен учасник сеансу передачі мультимедійних даних відсилає ні 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 мультимедійних даних.

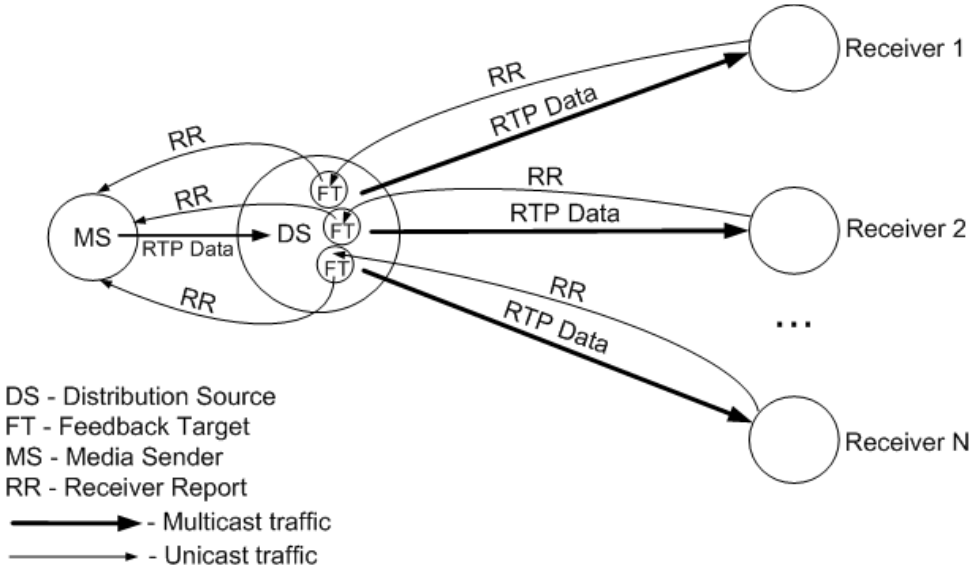


Рисунок 2.19 - Проста модель зворотного зв'язку

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 [30].

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 злиття звітів одержувача на джерелі розсилки, необов'язково, але можливо за допомогою цільового

вузла зворотного зв'язку, в зведені (резюмують) пакети, які потім розсилаються всім одержувачам (рисунок 2.20).

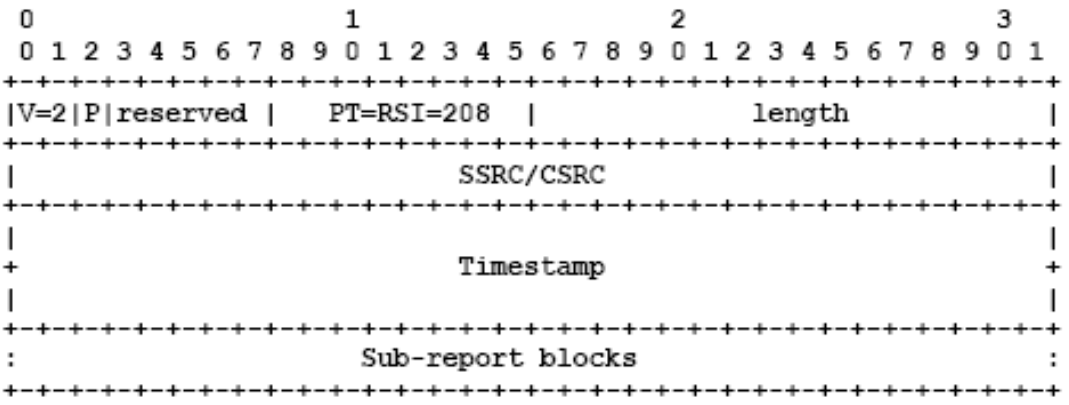


Рисунок 2.20 - Структура пакета RTCP-RSI (Report Summary Information)

Перевага використання останньої схеми найкраще проявляється в сеансах передачі мультимедійного трафіку для великих груп, при використанні в яких 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. 2.21). До того ж, резюмуюча схема надає опціональний механізм розсилки інформації про дані зворотного зв'язку, викладених всією групою, у вигляді значень розподілу або гістограми.

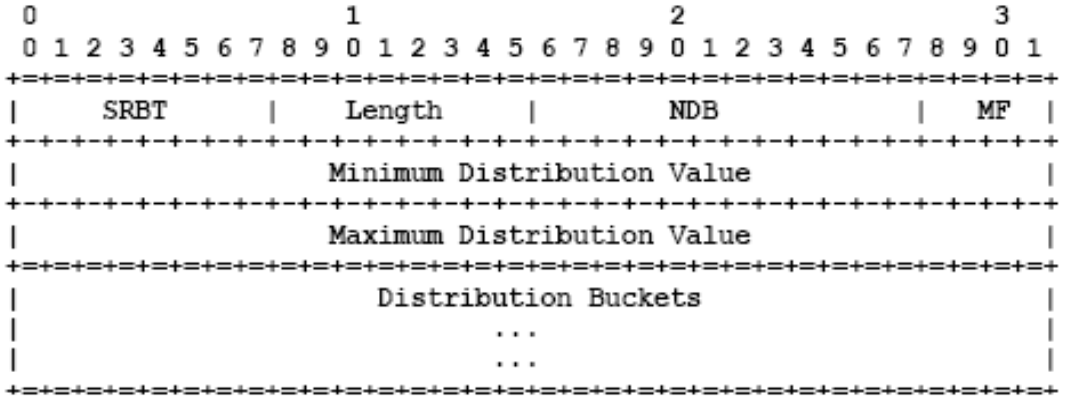


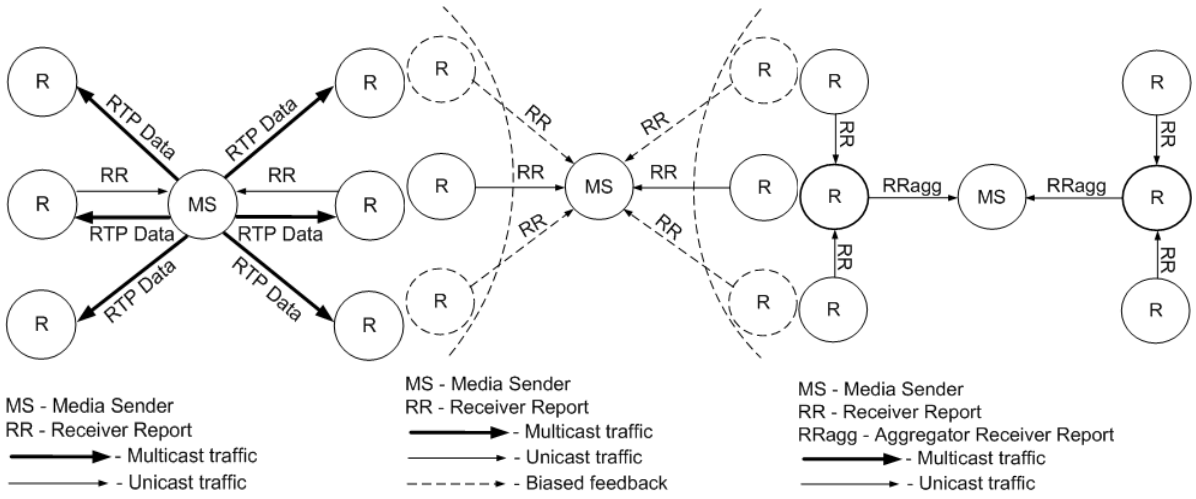
Рисунок 2.21 - Загальна форма блоку звіту

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) резюмуютчи 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. 2.22 (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 2.22 - Моделі зворотного зв'язку:

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

Метод зсуву (рис. 2.22 (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 джерелу 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 уходу старих членів групи), а також до високої динамічності значень зворотного зв'язку членів зміщеної 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. 2.22 (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. У кожній підгрупі вибирається один учасник, так званий агрегатор, який і є відповідальним за збір звітів від кожного члена підзвітної йому підгрупи і передачу даних зворотного зв'язку джерелу 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 залежим 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, в даний час властивих процесу передачі трафіку в реальному масштабі часу за допомогою використання протоколів RTP/RTCP. Використання багатоадресних розсилки, що є природним типом трафіку для RTP, в разі передачі керуючого трафіку і трафіку зворотного зв'язку може призвести до неоптимального використання смуги пропускання корисних потоків даних. Використовуваний механізм масштабування з метою управління завантаженістю може привести до того, що при високій інтенсивності передачі трафіку і великій кількості учасників передачі даних, 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.

2.4.2 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, не знижуючи ефективності механізмів зворотного зв'язку і діагностування [29].

На рисунку 2.23 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).

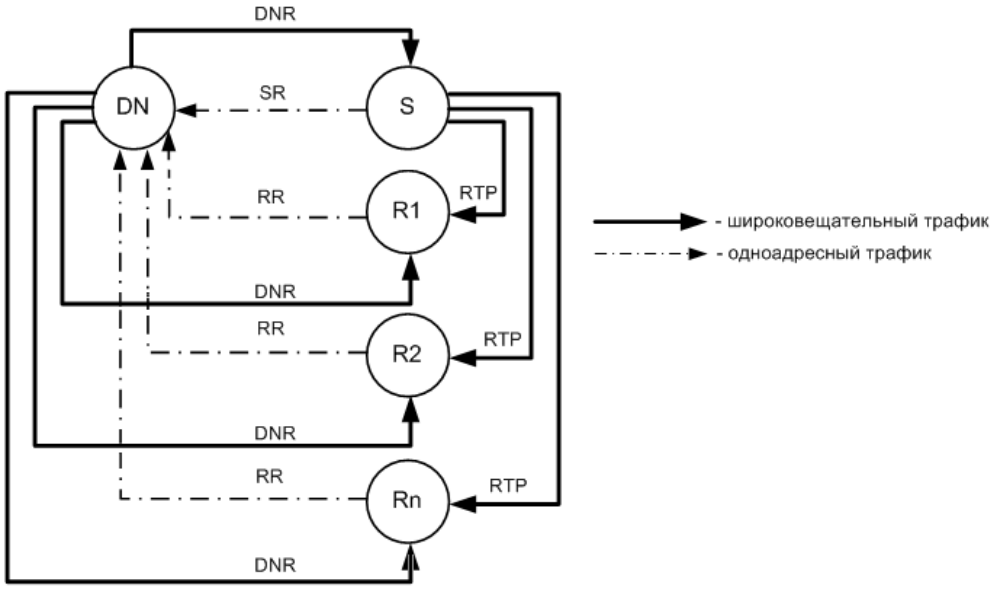


Рисунок 2.23 - Схема впровадження ДВ в централізовану архітектуру MCM

Як видно з рисунка 2.23, приймаючи звіти (пакети SR і RR) від усіх вузлів-учасників RTP-сесії одноадресним чином, ДВ 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, зворотного зв'язку 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 2.24).

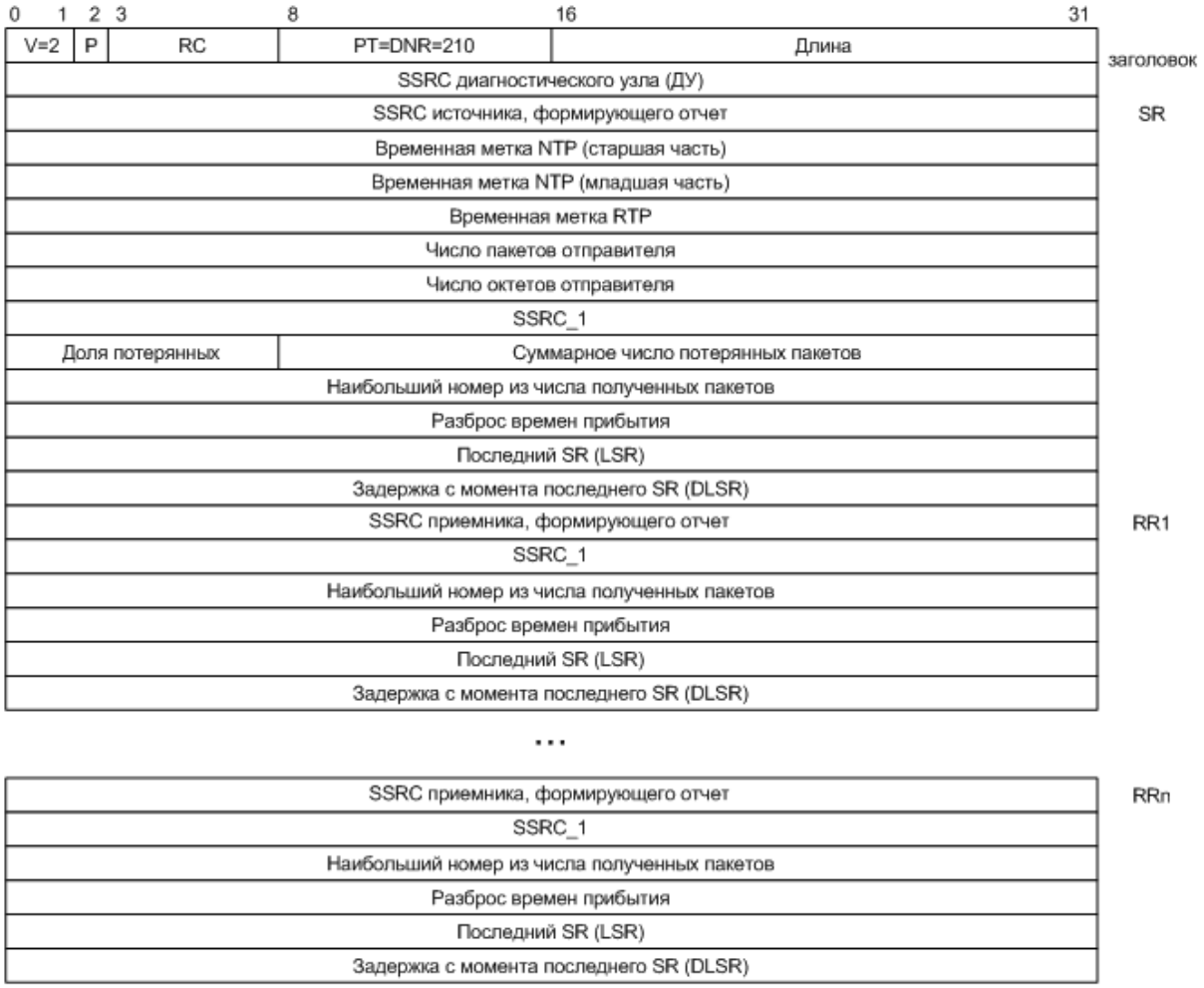


Рисунок 2.24 - Формат пакета DNR для зв'язку з одним джерелом

Пакети RTCP типів SDES, BYE і APP в пропонованій 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, в пропонованій моделі залишаються без змін і відповідають стандартному опису.

2.4.3 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 ВКЗ 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 в пропонованій 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 ВКЗ відправляє звіт.

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

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

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

$$U_1 = U_{SR} + U_{RR}, \tag{2.3}$$

де n - загальна кількість учасників мультимедійної сесії, m - число медіа-серверів або активних учасників мультимедійної сесії, PLSR, PLRR і PLDNR - довжини пакетів SR, RR і DNR відповідно.

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

$$U_{SR} = m * PL_{SR}, \tag{2.4}$$

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

$$U_{DNR} = n * PL_{DNR}, \tag{2.6}$$

$$U_2 = U_{SR} + U_{RR} + U_{DNR}, \tag{2.7}$$

де n - загальна кількість учасників мультимедійної сесії, m - число медіа-серверів або активних учасників мультимедійної сесії, PLSR, PLRR і PLDNR - 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:

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

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

$$U_1 = U_{SR} + U_{RR}; \tag{2.10}$$

– модель зворотного зв'язку з введенням ДВ:

$$U_{SR} = PL_{SR}, \tag{2.11}$$

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

$$U_{DNR} = n * PL_{DNR}, \tag{2.13}$$

$$U_2 = U_{SR} + U_{RR} + U_{DNR}. \tag{2.14}$$

Виконаємо розрахунок значень PLSR, PLRR і PLDNR:

– PLSR = заголовок Eth (14 байт) + заголовок IP (20 байт) + заголовок UDP (8 байт) + заголовок SR (8 байт) + тіло SR (44 байта) = 94 байта,
– PLRR = заголовок Eth (14 байт) + заголовок IP (20 байт) + заголовок UDP (8 байт) + заголовок RR (8 байт) + тіло RR (24 байта) = 74 байта,
– PLDNR = 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 * (nm) + 24 * (nm) = 78 + 28 * (n-1) байт.

При підстановці отриманих значень PLSR, PLRR і PLDNR в формули (2.8 - 2.14) утилізація для стандартної моделі зворотного зв'язку RTCP приймає наступний вигляд:

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

а для пропонованої моделі:

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

Графіки залежностей обсягу трафіку RTCP від кількості учасників сесії для стандартної моделі зворотного зв'язку RTCP (графік I) і для пропонованої моделі з ДВ (графік II) показані на рисунку 2.25.

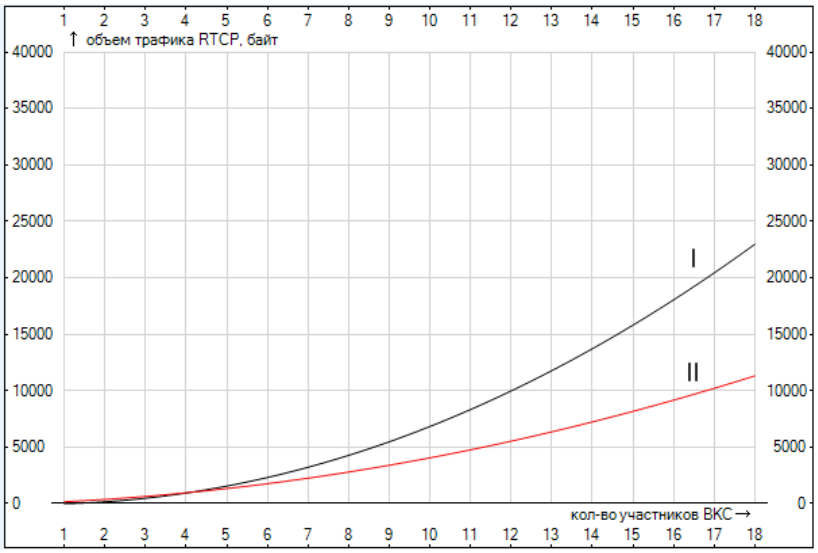


Рисунок 2.25 - Розрахункова залежність обсягу трафіку RTCP (вісь Y) від кількості учасників сесії (вісь X)

З графіка видно, що чим більше кількість учасників сесії ВКЗ, тим більше явно проявляється тенденція скорочення обсягу трафіку при використанні пропонованої моделі зворотного зв'язку в порівнянні зі стандартною моделлю. При невеликих розмірах сесії ВКЗ (n <5) скорочення обсягу трафіку RTCP в пропонованої 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 ЩОДО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ПЕРЕДАЧІ ТРАФІКУ РЕАЛЬНОГО ЧАСУ

В даний час найбільш важливим помічником керівника або менеджера підприємства стає інформаційна система підтримки прийняття управлінських рішень (СППР, Decision Support System, DSS). Дані системи дозволяють змоделювати ситуацію і зробити правильний, обгрунтований вибір управлінського рішення в даній ситуації.

В контексті даної дослідницької роботи СППР - 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.

Завдання прийняття оптимального рішення з оцінки якості обслуговування в МСМ найчастіше пов'язане з вибором великої і різноманітної безлічі параметрів. Аналіз літератури [31] 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 оцінки якості МСМ базується на методі результуючого показника якості. Він заснований на формуванні узагальненого показника шляхом інтуїтивних оцінок впливу приватних показників якості $q_1,\ldots, q_m$ на результуючу якість виконання системою її функцій (тобто на QoS). Оцінки такого впливу даються фахівцем-експертом (групою експертів), що має досвід розробки подібних систем. Найбільше застосування серед результуючих показників якості отримали: адитивний, мультиплікативний показники.

Скористаємося адитивним показником якості, який являє собою суму зважених нормованих приватних 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, чим більше він впливає на якість системи:

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

Головною особливістю адитивного показника є те, що при його застосуванні може відбуватися взаємна компенсація приватних 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:

- q_1 – дефазіфіцірована оцінка якості доставки пакетів в МСМ [1-100];
- q_2 - оцінка продуктивності мережі [1-100];
- q_3 - оцінка надійності мережі [1-100].

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

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

де k_1, k_2, k_3 - вагові коефіцієнти, що визначають ступінь впливу того чи іншого параметра 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 q1 = 70, q2 = 40, q3 = 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.

У сучасних технологіях в якості СППР нерідко застосовують технології Data-mining ("видобуток даних"). При цьому можна сказати, що Data-mining - це набір методів штучного інтелекту: нейронних мереж, генетичних алгоритмів, нечіткої логіки, дерев рішень і т.д., які спираються на сучасні засоби зберігання та обробки даних. Реалізація ядра сучасної СППР повинна бути на базі одного з цих методів, в зв'язку з тим, що за допомогою сучасних СППР зазвичай вирішуються складні завдання, з предметною областю, що важко формалізується, складним взаємозв'язком внутрішніх компонент і стохастичним зовнішнім середовищем.

У даній дослідницькій роботі вибір припав на апарат нечіткої логіки. Даний підхід виправдовує себе не тільки з точки зору того, що експерти, чиї знання і досвід, що лежать в основі СППР, мають суб'єктивний характер і погано піддаються формалізації, а й тому, що особа, яка приймає рішення (адміністратор), часто працює саме з нечіткою

інформацією, представленою 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, який дає користувач, найчастіше є суб'єктивним і неточним. Таким чином, в якості інструменту при ухваленні рішення про якість обслуговування в МСМ адміністратору пропонується використовувати СППР, в основі якої лежить нечіткий алгоритм виведення.

3.1 Експертне оцінювання якості обслуговування в МСМ

Згідно [32], експертне оцінювання - це судження висококваліфікованих фахівців-професіоналів, висловлені у вигляді змістовної, якісної або кількісної оцінки об'єкта. Експертне оцінювання передбачає наявність декількох етапів: підбір експертів, розробка регламенту проведення збору та аналізу експертних думок [33].

Для сучасного етапу використання методів експертного оцінювання характерно широке застосування комп'ютерних систем підтримки прийняття рішення. Це пояснюється тим, що людина не може моментально дати відповідь на будь-яке питання навіть в тій сфері, в якій вона є професіоналом. Даний факт є наслідком того, що досвід конкретної людини слабшає, він повинен постійно практикуватися, щоб зберегти свій професійний рівень. Людина робить висновок з можливими суб'єктивними помилками, а в екстремальних ситуаціях може забути важливе правило.

Для опису МСМ досить 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 підсумкову 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.

Методи експертних оцінок базуються на гіпотезі, що, використовуючи знання одного (індивідуальні оцінки ДО) або декількох (колективні оцінки ДО) фахівців-експертів, вдасться створити модель майбутнього стану мережі близьку до реальної.

Найчастіше знання експертів, які відображають їх професійний досвід, накопичений в процесі діяльності в області технічної діагностики, є трудновиразним, так як існує 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.

Запропонована структура нечіткої СППР є інструментом адміністратора для об'єктивної оцінки якості доставки IP-пакетів в МСМ.

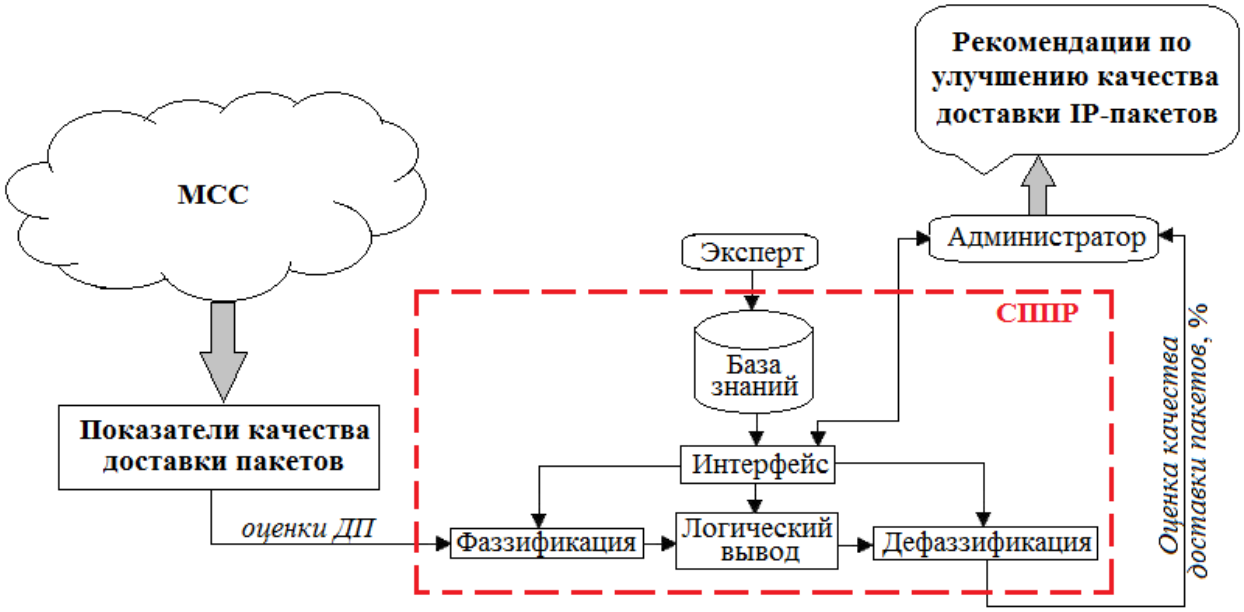


Рисунок 3.1 - Структурна схема запропонованої СППР

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). Так як в основі запропонованої СППР лежить апарат нечіткої логіки, то необхідно в першу чергу розробити нечітку модель якості доставки пакетів в МСМ.

3.1.1 Нечітка модель якості доставки пакетів в МСМ

Модель оцінки якості доставки пакетів в МСМ можна представити в наступному вигляді (рис. 3.2).

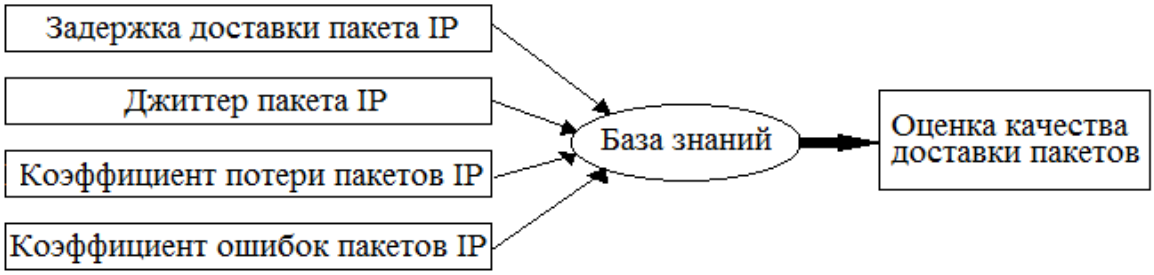


Рисунок 3.2 - Модель оцінки якості доставки пакетів

У загальному випадку нечітка модель повинна містити наступні блоки [34]:

– фазіфікатор - перетворює фіксований вектор діагностичних параметрів, що впливають, в вектор нечітких множин, необхідних для виконання нечіткого логічного висновку;
– нечітка база знань - містить інформацію про залежності вихідної змінної від вхідних змінних у вигляді лінгвістичних правил типу ЯКЩО - ТО;
– машина нечіткого логічного висновку - на основі правил бази знань визначає значення вихідної змінної у вигляді нечіткої множини, відповідного нечітким значенням вхідних змінних;
– дефазіфікатор - перетворює вихідну нечітку множину в чітке число.

Нечітка модель оцінки якості доставки IP-пактів була реалізована в MatLab з використанням пакета Fuzzy Logic Toolbox. Вибір MatLab обумовлений його високою ефективністю обчислень і візуалізацією результатів. На рис. 3.3 показана структура ядра запропонованої СППР, за допомогою якої за вхідними змінним IPTD, IPDV, IPLR, IPER, які є діагностичними параметрами і розглянуті далі, на основі бази нечітких правил визначається оцінка якості доставки IP-пакетів в МСМ.

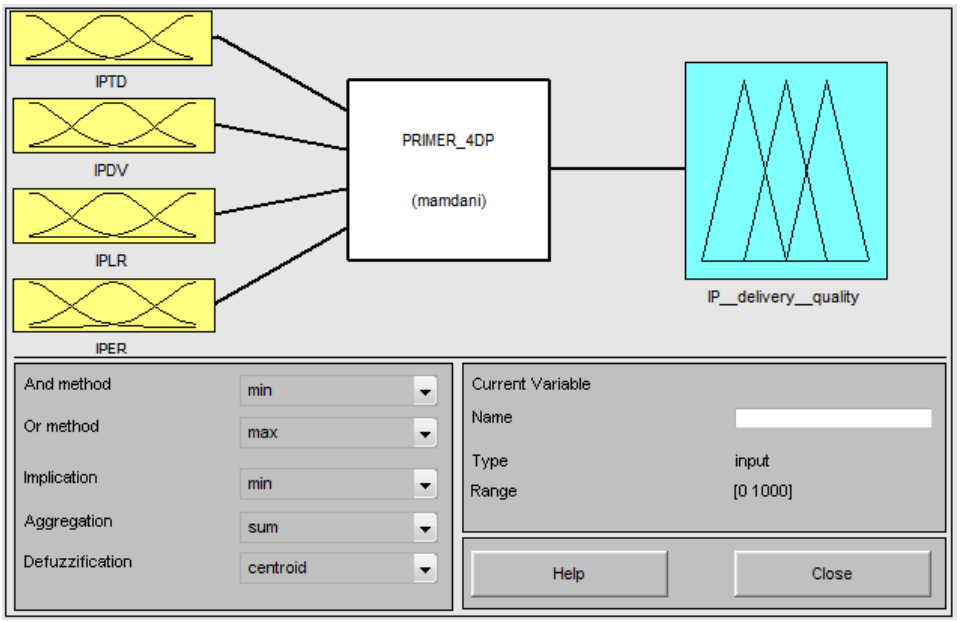


Рисунок 3.3 - Ядро нечіткої СППР

Розглянемо чотири діагностичних ознаки для визначення якості доставки IP пакетів в МСМ, кожен з яких представлений у вигляді лінгвістичної змінної (ЛЗ).

1. IPTD (IP packet transfer delay) - затримка доставки пакета IP в мілісекундах. Змінна «IPTD» характеризується трьома терм-множинами: «низький» (H, Low), «середній» (C, Average), «високий» (B, High), параметри функцій приналежності (ФП) яких представлені в таблиці 3.1.

Вибір трирівневої шкали оцінки якості обумовлений тим, що з області психології відомо, що в короткочасній (робочій) пам'яті людини одночасно утримується 7 ± 2 понять. Тому в зв'язку з великою кількістю оброблюваних критеріїв доцільно використовувати саме трирівневу шкалу оцінки якості.

Таблиця 3.1 – Характеристики ЛЗ «IPTD»

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]

Функція приналежності змінної «IPTD» представлена на рисунку 3.4.

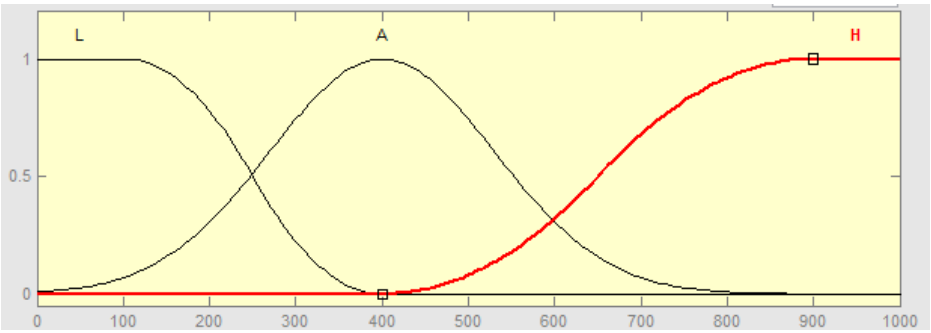


Рисунок 3.4 - ФП лінгвістичної змінної «IPTD»

2. IPDV (IP packet delay variation) - варіація затримки або джиттер пакета IP в мілісекундах. Параметри ФП змінної «IPDV» представлені в таблиці 3.2.

Таблиця 3.2 – Характеристики ЛЗ «IPDV»

Терми		Діапазони		Тип ФП	Параметри
H	Low	0	8	Zmf	[0 10]
C	Average	5	45	Gaussmf	[8.5 23]
B	High	35	60	Smf	[30 50]

ФП змінної «IPDV» представлена на рисунку 3.5.

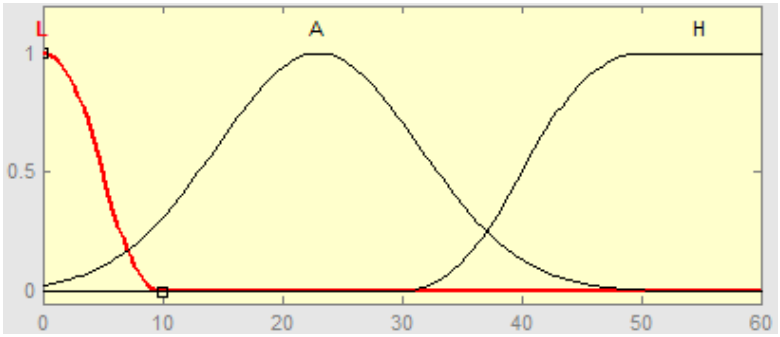


Рисунок 3.5 - ФП лінгвістичної змінної «IPDV»

3. IPLR (IP packet loss ratio) - коефіцієнт втрати пакетів IP у відсотках. Параметри ФП змінної «IPLR» представлені в таблиці 3.3.

Таблиця 3.3 – Характеристики ЛЗ «IPLR »

Терми		Діапазони		Тип ФП	Параметри
H	Low	0	0.2	zmf	[3e-005 0.0002]
C	Average	0.005	0.55	gaussmf	[0.0001 0.0003]
B	High	0.5	0.001	smf	[0.0005 0.0009]

ФП змінної «IPLR» представлена на рисунку 3.6.

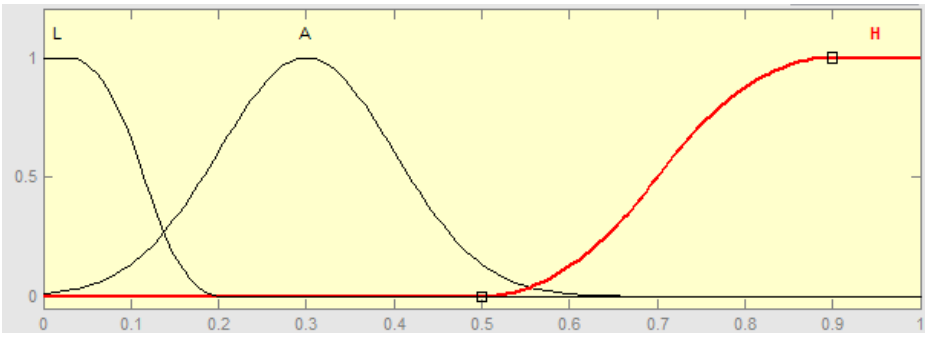


Рисунок 3.6 - ФП лінгвістичної змінної «IPLR»

4. IPER (IP packet error ratio) - коефіцієнт помилок пакетів IP у відсотках. Параметри ФП змінної «IPER» представлені в таблиці 3.4.

Таблиця 3.4 – Характеристики ЛЗ «IPER»

Терми		Діапазони		Тип ФП	Параметри
H	Low	0	0.1	zmf	[2e-007 1e-006]
C	Average	0.2	1.4	gaussmf	[1e-006 2.5e-006]
B	High	0.3	0.0001	smf	[3e-006 8e-006]

ФП змінної «IPER» представлена на рисунку 3.7.

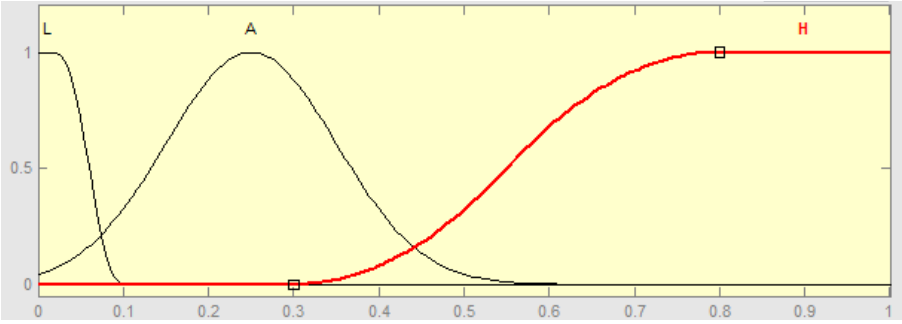


Рисунок 3.7 - ФП лінгвістичної змінної «IPER»

Вихідна ЛЗ - якість доставки IP пакетів в МСМ (IP_delivery_quality), характеризується п'ятьма терм-множинами: «дуже низький» (ОН, Very low), «низький» (Н, Low), «середній» (С, Average), «достатній »(Д, Sufficient),«високий »(в, High), параметри ФП яких представлені в таблиці 3.5. Така градація досить близька до

традиційної п'ятибальної шкали оцінювання та полегшує прийняття рішення експертом про якість доставки пакетів в МСМ.

Таблиця 3.5 – Характеристики ЛЗ «IP_delivery_quality»

Терми		Діапазони		Тип ФП	Параметри
ОН	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]

ФП змінної «IP_delivery_quality» представлена на рисунку 3.8.

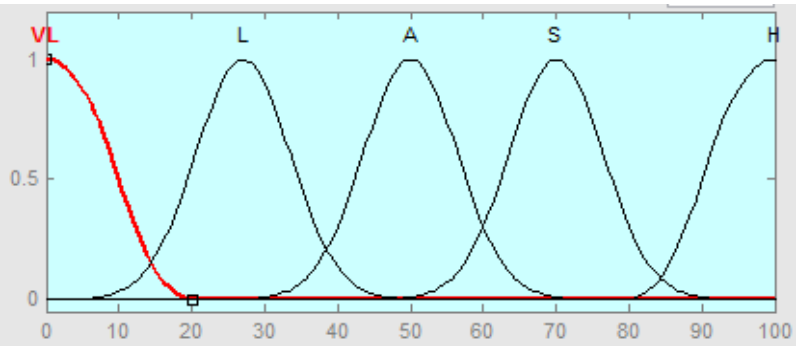


Рисунок 3.8 - ФП лінгвістичної змінної «IP_delivery_quality»

В основі будь-якої СППР лежить база знань. У нашому випадку моделлю представлення знань була обрана модель продукційних правил. Через великий обсяг тут наведено лише фрагмент продукційних правил (рис. 3.9). Повний набір ПП представлений в додатку А.

1. If (IPTD is L) and (IPDV is L) and (IPLR is L) and (IPER is L) then (IP__delivery__quality is H) (1)
2. If (IPTD is L) and (IPDV is L) and (IPLR is L) and (IPER is A) then (IP__delivery__quality is S) (1)
3. If (IPTD is L) and (IPDV is L) and (IPLR is A) and (IPER is L) then (IP__delivery__quality is S) (1)
4. If (IPTD is L) and (IPDV is A) and (IPLR is L) and (IPER is L) then (IP__delivery__quality is S) (1)
5. If (IPTD is A) and (IPDV is L) and (IPLR is L) and (IPER is L) then (IP__delivery__quality is S) (1)
6. If (IPTD is L) and (IPDV is L) and (IPLR is L) and (IPER is H) then (IP__delivery__quality is S) (1)
7. If (IPTD is L) and (IPDV is L) and (IPLR is H) and (IPER is L) then (IP__delivery__quality is S) (1)
8. If (IPTD is L) and (IPDV is H) and (IPLR is L) and (IPER is L) then (IP__delivery__quality is S) (1)
9. If (IPTD is H) and (IPDV is H) and (IPLR is L) and (IPER is L) then (IP__delivery__quality is S) (1)
10. If (IPTD is L) and (IPDV is L) and (IPLR is A) and (IPER is A) then (IP__delivery__quality is S) (1)
11. If (IPTD is L) and (IPDV is A) and (IPLR is A) and (IPER is L) then (IP__delivery__quality is S) (1)
12. If (IPTD is A) and (IPDV is A) and (IPLR is L) and (IPER is L) then (IP__delivery__quality is S) (1)
13. If (IPTD is L) and (IPDV is A) and (IPLR is L) and (IPER is A) then (IP__delivery__quality is S) (1)
14. If (IPTD is A) and (IPDV is L) and (IPLR is A) and (IPER is L) then (IP__delivery__quality is S) (1)
15. If (IPTD is A) and (IPDV is L) and (IPLR is L) and (IPER is A) then (IP__delivery__quality is S) (1)

Рисунок 3.9 - База продукційних правил

Процес функціонування пропонованої системи представлений в підрозділі 3.1.2. Результатом роботи СППР є оцінка якості доставки пакетів (ОН, Н, С, Д, В). Якісне визначення кожного рівня представлено в таблиці 3.6.

Таблиця 3.6 - Рівні якості доставки IP-пакетів

Рівень якості	Визначення
ОН (VL)	Якість доставки IP-пакетів дуже низька. Потрібна повна реконфігурація мережі для ефективного розподілу ресурсів.
Н (L)	Якість доставки IP-пакетів низька. Потрібне часткова реконфігурація мережі для ефективного розподілу ресурсів.
С (A)	Прийнятна якість доставки IP-пакетів, але для збільшення ступеня придатності такої МСМ необхідно працювати над підвищенням якості.
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 її стан і багатокритеріальності розв'язуваної задачі.

3.1.2 Аналіз якості доставки пакетів з використанням Matlab

У середовищі MatLab з використанням пакета Fuzzy Logic Toolbox був проведений ряд експериментів. При цьому було обрано такі параметри системи нечіткого виведення: для виконання логічного висновку - алгоритм Мамдані, для виконання логічної кон'юнкції - метод мінімального значення, для виконання логічної диз'юнкції - метод максимального значення, для активізації логічного висновку в кожному з нечітких правил - метод мінімального значення, для виконання агрегування - метод суми, для виконання дефазифікації - метод центру тяжіння геометричної фігури (рис. 3.3).

Суть експериментів полягає в аналізі залежності:

$$IP\_delivery\_quality = f\ (IPTD, IPDV, IPLR, IPER),$$

де IP_delivery_quality - якість доставки пакетів,%; IPTD - затримка доставки пакета, мс; IPDV - варіація затримки пакета (джиттер), мс; IPLR - коефіцієнт втрати пакетів,%; IPER - коефіцієнт помилок пакетів,%.

Експеримент № 1. При проведенні експерименту проаналізовані RTCP-пакети, що пересилаються всередині МСМ. Значення параметрів доставки (оцінок діагностичних параметрів) подаються на вхід СППР (рис. 3.1), яка генерує тривимірну модель, що описує таку залежність:

$$IP\_delivery\_quality = f\ (500, 40, IPLR, IPER),$$

де перші два параметра зафіксовані в такий спосіб: IPTD = 500 (затримка = 500 мс), IPDV = 40 (джиттер = 40 мс).

Отримана 3-вимірна поверхня відображає вплив останніх двох параметрів IPLR (втрати) і IPER (помилки) на якість доставки IP пакетів в МСМ (рис. 3.10).

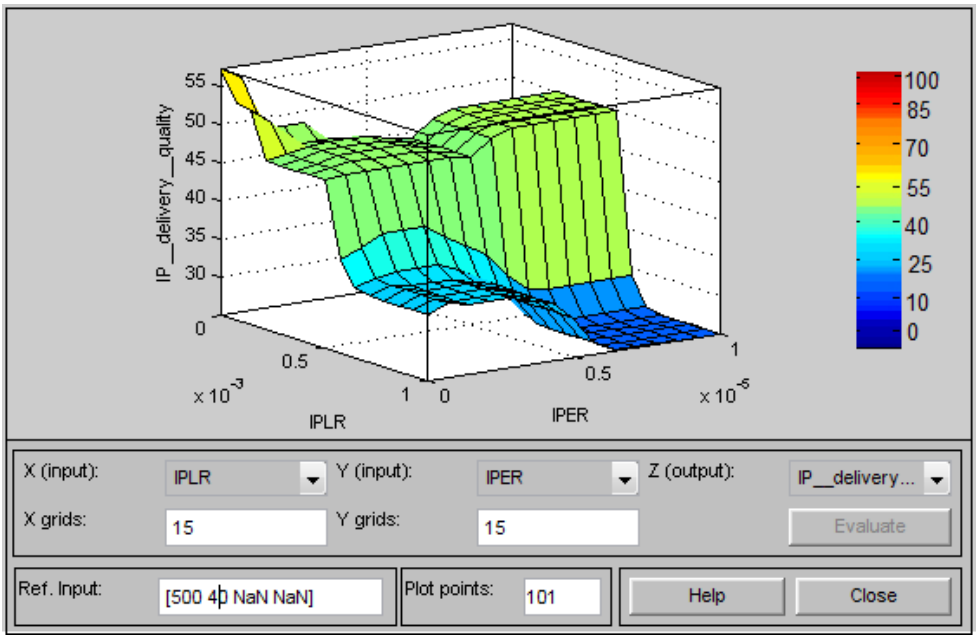


Рисунок 3.10 - Тривимірна модель, що відповідає 1-му експерименту

Отриманий графік показує, що якість доставки пакетів не перевищує 58% і різко падає з ростом частки втрачених пакетів до 10^{-3} і при підвищенні частки помилкових пакетів до 10^{-5}.

На рисунках 3.11 - 3.14 представлені криві, які, демонструючи залежності якості доставки пакетів від кожного параметра, підтверджують вищесказане. Так на рисунку 3.11 представлено перетин отриманої поверхні для змінної IPLR (втрати) при мінімально можливій помилки IPER = 0.

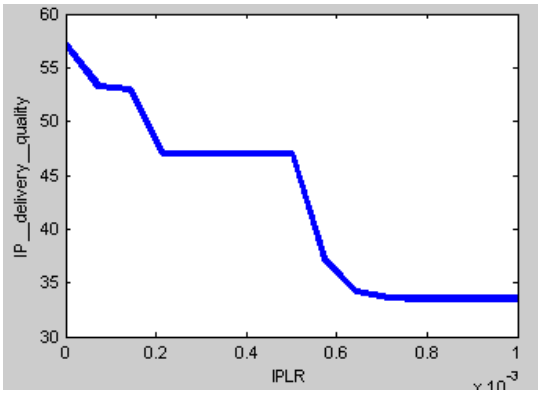


Рисунок 3.11 - Графік залежності IP_delivery_quality = f (IPLR) при IPER = 0%

За даним графіком легко зробити висновок, що при відсутності помилкових пакетів (IPER = 0%) якість доставки (IP_delivery_quality) падає з ростом відсотка втрачених пакетів (IPLR) з 58% до 32%.

Перетин поверхні для змінної IPLR (втрати) при максимально можливій помилки IPER = 1×10^{-5} представлено на рисунку 3.12.

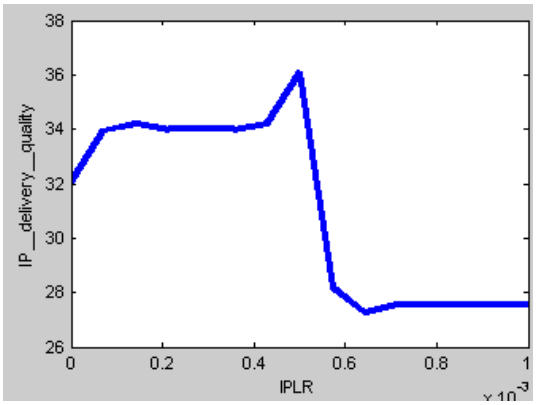


Рисунок 3.12 - Графік залежності IP_delivery_quality = f (IPLR) при IPER = 1×10^{-5}

Даний графік показує, що при максимально допустимому відсотку помилкових пакетів (IPER = 1×10^{-5}%) якість доставки (IP_delivery_quality) перебуває на рівні 32-46%, а при досягненні значення відсотка втрачених пакетів, що дорівнює ½ від максимально допустимого значення (при IPLR = 0,5%), різко падає до рівня нижче 28%.

Перетин поверхні для змінної IPER (помилки) при мінімально можливих втратах IPLR = 0 представлено на рисунку 3.13.

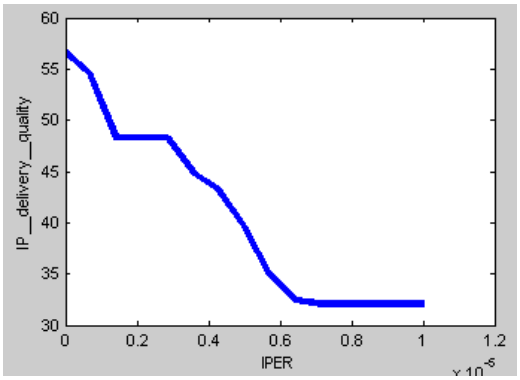


Рисунок 3.13 - Графік залежності IP_delivery_quality = f (IPER) при IPLR = 0%

За графіком видно, що при мінімальних втратах пакетів (IPER = 0%) якість доставки (IP_delivery_quality) падає з ростом відсотка помилкових пакетів (IPLR) з 56% до 32%.

Перетин поверхні для змінної IPER (помилки) при максимально можливих втратах IPLR = 1×10^{-3} представлено на рисунку 3.14.

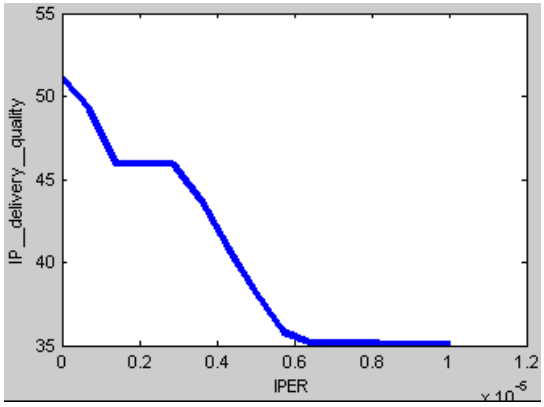


Рисунок 3.14 - Графік залежності IP_delivery_quality = f (IPER) при IPLR = 1×10^{-3}%

Згідно з цим графіком, при максимально допустимих втратах пакетів (IPER = 1×10^{-3}%) якість доставки (IP_delivery_quality) падає з ростом відсотка помилкових пакетів (IPLR) з 51% до 35%, причому різкий скачок спостерігається в діапазоні IPLR = [0.3 , 0.6], а після IPLR = 0.6 якість приймає константне значення 35%.

Експеримент № 2. При проведенні другого експерименту проаналізовані ті ж RTCP-пакети, що пересилаються всередині МСМ. Значення параметрів доставки подаються на вхід СППР (рис. 3.1), яка генерує тривимірну модель, що описує таку залежність:

$$IP\_delivery\_quality = f\ (IPTD, IPDV, 1 \times 10^{-3}, 1 \times 10^{-5}),$$

де останні два параметри зафіксовані в такий спосіб: IPLR = 1×10^{-3} (втрати = 1×10^{-3} %), IPER = 1×10^{-5} (помилки = 1×10^{-5} %).

Отримана 3-вимірна поверхня відображає вплив перших двох параметрів IPTD (затримка) і IPDV (джиттер) на якість доставки IP пакетів в МСМ (рис. 3.15).

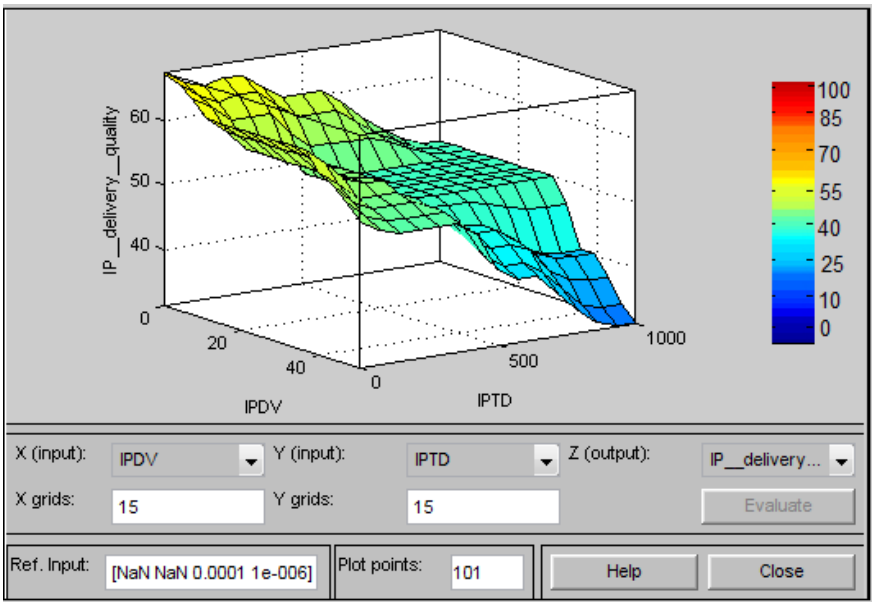


Рисунок 3.15 - Тривимірна модель, відповідна 2-му експерименту

Якість доставки пакетів не перевищує 70% і помірно зменшується з ростом затримки IP-пакетів до 1000 мс і різко падає при підвищенні значення джиттера до 60 мс, що відповідає практичним спостереженнями за мультисервісними мережами. На рисунках 3.16 - 3.20 представлені криві, які, демонструючи залежності якості доставки пакетів від кожного параметра, підтверджують вищесказане.

Так на рисунку 3.16 представлено перетин поверхні для змінної IPTD (затримка) при мінімально можливому джиттері IPDV = 0.

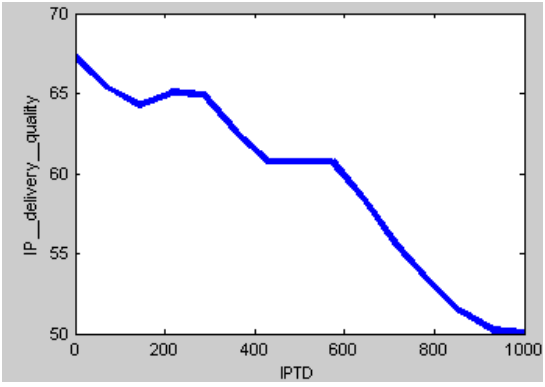


Рисунок 3.16 - Графік залежності IP_delivery_quality = f (IPTD) при IPDV = 0 мс

За даним графіком можна зробити висновок, що при мінімальному джиттером (IPDV = 0 мс) якість доставки (IP_delivery_quality) падає з ростом затримки пакетів (IPTD) з 68% до 50%.

Перетин поверхні для змінної IPTD (затримка) при максимально можливому джиттером IPDV = 50 представлено на рисунку 3.17.

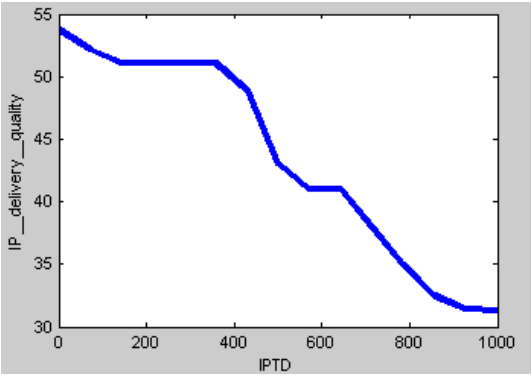


Рисунок 3.17 - Графік залежності IP_delivery_quality = f (IPTD) при IPDV = 50 мс

Даний графік свідчить, що при максимально допустимому джиттері (IPDV = 50 мс), якість доставки (IP_delivery_quality) падає з ростом затримки пакетів (IPTD) з 54% до 31%, різке падіння спостерігається вже при затримці IPTD = 400 мс.

Перетин поверхні для змінної IPDV (джиттер) при мінімально можливих втратах IPTD = 0 представлено на рисунку 3.18.

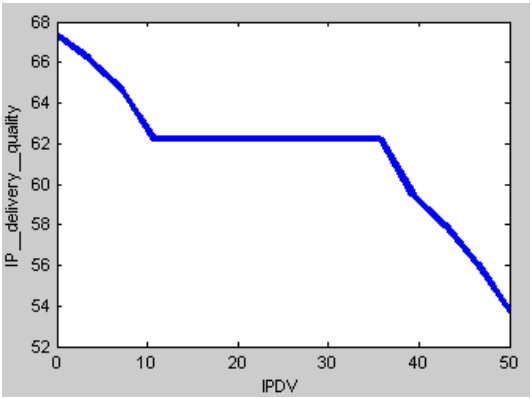


Рисунок 3.18 - Графік залежності IP_delivery_quality = f (IPDV) при IPTD = 0 мс

Згідно з цим графіком, при мінімально можливій затримки пакетів (IPTD = 0 мс) якість доставки (IP_delivery_quality) падає зі збільшенням джиттера (IPDV) з 68% до 54%, при чому в діапазоні IPTD = [10,35] спостерігається збереження рівня якості рівне 62%.

Перетин поверхні для змінної IPDV (джиттер) при максимально допустимій затримці 1000 мс представлено на рисунку 3.19.

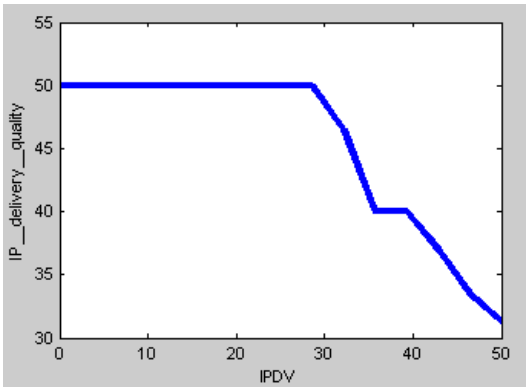


Рисунок 3.19 - Графік залежності IP_delivery_quality = f (IPDV) при IPTD = 1000 мс

Отриманий графік показує, що при максимально допустимій затримки пакетів (IPTD = 1000 мс) якість доставки (IP_delivery_quality) дорівнює 50% при значенні джиттера в діапазоні IPDV = [0,30], а при джиттері IPDV = 30 мс спостерігається різке падіння рівня якості до 31%.

Таким чином, результатом експериментів стали тривимірні моделі, 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.

3.2 Моделювання трафіку реального часу в МСМ, побудованої на базі IP АТС Asterisk

3.2.1 Загальна інформація про систему Asterisk

Asterisk - це платформа для телефонії з відкритим вихідним кодом, який встановлюється практично на будь-яку платформу Linux. Міць цієї системи - в її природі, що настроюється, в поєднанні з яким відповідністю стандартам, яким немає аналогів. Жодна інша офісна АТС не надає такі широкі можливості за варіантами її розгортання. Такі програми, як голосова пошта, конференц-зв'язок, черги викликів і агенти, музика під час очікування і парковка викликів, - все це стандартні функції, вбудовані безпосередньо в програмне забезпечення.

З точки зору вимог до ресурсів Asterisk подібна вбудованим системам реального часу переважно тим, що вона повинна мати пріоритетний доступ до процесора і системних шин. Тому вкрай важливо, щоб всі інші функції системи, не пов'язані безпосередньо з завданнями Asterisk по обробці викликів, якщо такі взагалі виконуються, повинні виконуватися з більш низьким пріоритетом. Для невеликих і аматорських систем це може і не представляти особливої проблеми. Однак для високопродуктивних систем недостатня продуктивність буде викликати проблеми з якістю аудіосигналу, одержуваного користувачем, часто у вигляді перешкод і т. п. 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 труднощі з обслуговуванням з'єднань. Для офісної АТС подібна ситуація - справжня катастрофа, тому в процесі вибору платформи вимоги до продуктивності повинні бути вирішальним критерієм. У таблиці 3.7 представлені деякі основні рекомендації до планування системи.

Таблиця 3.7 - Вибір технічних характеристик системи Asterisk

Приначення	Кількість каналів	Рекомендовані мінімальні параметри
Любительска система	не більш ніж 5	400 МГц ×86, 256 Мб оперативної пам'яті
SOHO-система (малий офіс)	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 та велика система	більш ніж 25	Два ЦП, можливо також кілька серверів в розподіленій архітектурі

Для великих установок Asterisk функціональність зазвичай розподіляють між декількома серверами. Один або більше центральних модулів будуть займатися обробкою викликів; їх доповнять один або більше допоміжних серверів, які обслуговують периферійні пристрої (такі, як система баз даних, система голосової пошти, система конференц-зв'язку, система управління, веб-інтерфейс, міжмережевий екран і т.д.). Asterisk, як і багато Linux-системи, може розширюватися з ростом вимог до неї: мала система, яка чудово справлялася з усіма завданнями з обробки викликів і обслуговування 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 покупку.

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 уявити. Коротко розглянемо різні види пристроїв, звані в даний час «телефонами» (всі вони без зусиль можуть бути інтегровані з Asterisk).

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

1.1 Аналогові телефони - вловлювати ці звуки і перетворювати їх у формат, придатний для передачі по проводах. Інфрачервоний промінь є аналогом звукових хвиль, створюваних промовистим об'єктом.

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

1.3 ISDN-телефони. До появи VoIP найближче до стандартизованого цифрового телефону був термінал ISDN BRI (Basic Rate Interface). Було розроблено безліч BRI-пристроїв, однак BRI був переважно відкинутий на користь більш швидких і дешевих технологій, таких як ADSL, кабельні модеми та VoIP. BRI як і раніше дуже широко використовується як обладнання для відеоконференц-зв'язку, оскільки забезпечує лінію з фіксованою смугою пропускання. Також для BRI не характерні проблеми з якістю, які можуть виникати при VoIP-з'єднанні, оскільки це інтерфейс з комутацією каналів.

1.4 IP-телефони. Багатство можливостей, запропонованих цими пристроями, зумовив шквал найцікавіших застосувань, починаючи від відеотелефонів до пристроїв для мовлення з високою якістю, бездротових мобільних рішень, спеціалізованих телефонних апаратів, призначених для конкретних галузей, і гнучких мультимедійних систем «все в одному».

2. Програмні телефони (software telephone, софтфон) - це додаток, який забезпечує функціональність телефону пристрою, який не є телефоном, такому як ПК або персональний цифровий секретар. Софтфон не потребує додаткових апаратних рішень, за винятком, 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 апаратний IP-телефон на комп'ютері. 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.

Такі адаптери можна було б називати шлюзами, тому що це - їхня функція. Однак популярний термін «телефонний шлюз», ймовірно, найкраще описав би багатопортовий телефонний адаптер, як правило, виконує більш складні функції маршрутизації.

Телефонні адаптери будуть вживатися до тих пір, поки існує необхідність поєднувати несумісні стандарти і старі пристрої з новими мережами. Згодом необхідність в цих пристроях відпаде, як це сталося з модемами, які поступово зникають через непотрібність.

Для реалізації IP АТС Asterisk необхідний системний блок з тією чи іншою конфігурацією і телефонні апарати (рис. 3.20).

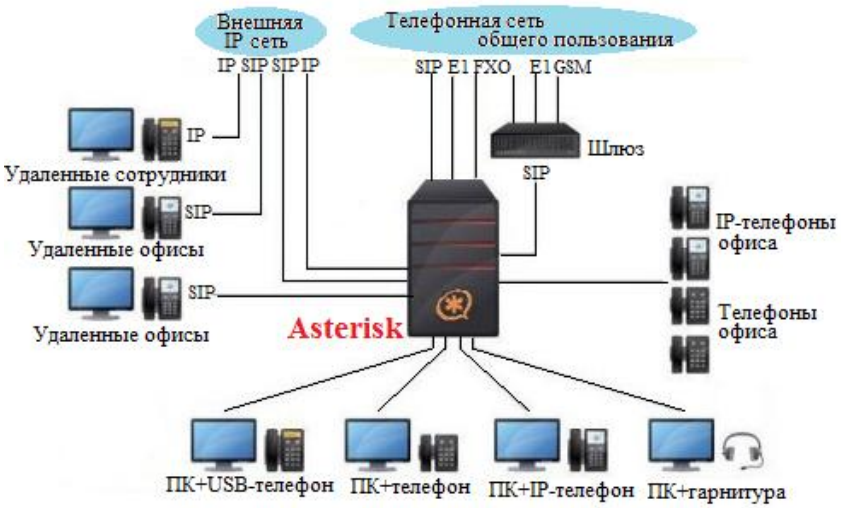


Рисунок 3.20 - Загальна схема IP АТС Asterisk

До програмної IP АТС Asterisk можуть бути підключені як програмні телефони (софтфони), так і всі різновиди апаратних користувальницьких IP телефонів (з інтерфейсами IP, USB, Wi-Fi).

3.2.2 Впровадження діагностичного вузла в МСМ на базі Asterisk

При всіх перевагах розглянутої системи Asterisk, у неї є і недоліки, а саме, відсутність можливості для аналізу трафіку, який проходить через неї. Якщо налаштувати Asterisk таким чином, що звіти від усіх вузлів-учасників RTP-сесії одноадресним чином посилалися йому, то сконцентровані таким чином RTCP-пакети будуть давати всю необхідну діагностичну інформацію.

Для дослідження даної гіпотези була розгорнута система IP-телефонії на базі IP АТС Asterisk (рис. 3.21).

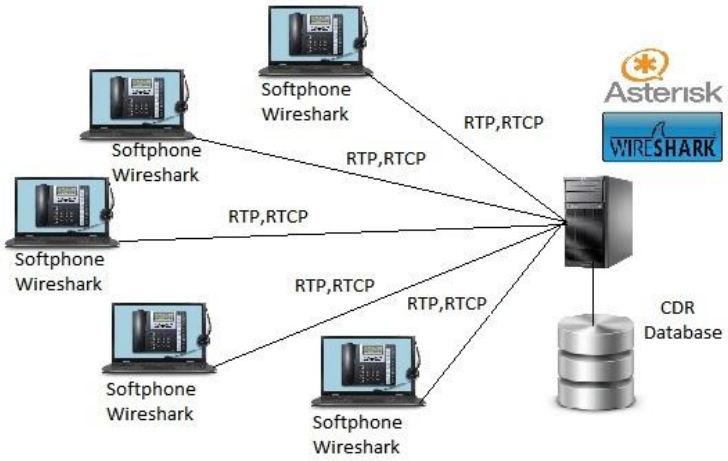


Рисунок 3.21 - Архітектура дослідницької платформи

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

Аналізатор Wireshark, розташовуючись на станції хоста, використовує нерозбірливий режим прослуховування, тобто драйвер мережевого адаптера починає перехоплювати весь трафік з каналу (promiscuous mode). Так як 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 відповідним рівням ієрархії. ПЗ аналізатора вивчає пакети і відображає інформацію про них на екрані хоста в вікні відстеження пакетів. Залежно від того, якими функціями володіє продукт, представлена інформація згодом може додатково аналізуватися і фільтруватися. Крім того, Wireshark знає структуру самих різних мережевих протоколів, і тому дозволяє розібрати мережевий пакет, відображаючи значення кожного поля протоколу будь-якого

рівня. Отже, даний аналізатор буде корисний для аналізу RTP/RTCP трафіку в реальному часі при проведенні аудіо-конференц-зв'язку на нашому тестовому стенді.

Кожен дзвінок, здійснений будь-яким з учасників конференції, проходить через сервер IP-телефонії Asterisk. Також всі дії по кожному з дзвінків реєструються в лог-файлах сервера, які можна переглядати в режимі онлайн (рис. 3.22).

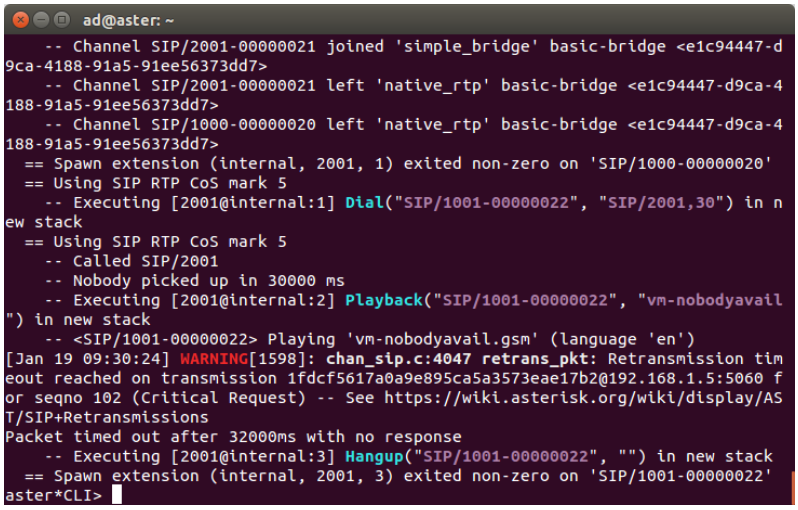


Рисунок 3.22 - Консоль Asterisk: лог дзвінка

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

Виконати аналіз CDR записів, безпосередньо використовуючи систему Asterisk, не представляється можливим. Тому для отримання значень необхідних параметрів доставки IP-пакетів скористаємося мережевим аналізатором Wireshark, встановленим на сервері IP-телефонії Asterisk.

Мережевий аналізатор протоколів Wireshark дозволяє перехопити весь трафік, як на серверній, так і на клієнтській сторонах. З цього трафіку за допомогою фільтрів можна виділити RTP і RTCP трафік і розглянути пакети даних протоколів зсередини (3.23, 3.24).

48	43.056230006	192.168.1.4	192.168.1.5	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x6952, Seq=29359, Time=51390
49	43.056392006	192.168.1.5	192.168.1.2	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x7CD33A3E, Seq=59615, Time=51384
50	43.071093006	192.168.1.2	192.168.1.5	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x6952, Seq=29359, Time=50382
51	43.076139006	192.168.1.4	192.168.1.5	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x6952, Seq=29360, Time=51550
52	43.076250006	192.168.1.5	192.168.1.2	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x7CD33A3E, Seq=59616, Time=51544
53	43.089320006	192.168.1.2	192.168.1.5	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x6952, Seq=29360, Time=50542
54	43.096141006	192.168.1.4	192.168.1.5	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x6952, Seq=29361, Time=51710
55	43.096293006	192.168.1.5	192.168.1.2	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x7CD33A3E, Seq=59617, Time=51704
57	43.111839006	192.168.1.2	192.168.1.5	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x6952, Seq=29361, Time=50702
58	43.111966006	192.168.1.5	192.168.1.4	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x75705907, Seq=27891, Time=50696, Mark
59	43.116126006	192.168.1.4	192.168.1.5	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x6952, Seq=29362, Time=51870
60	43.116220006	192.168.1.5	192.168.1.2	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x7CD33A3E, Seq=59618, Time=51864

Рисунок 3.23 - Приклад перехопленого RTP-трафіку

15735 178.22719806	192.168.1.5	192.168.1.4	RTCP	106	Sender Report	Source description	
16702 183.03684206	192.168.1.2	192.168.1.5	RTCP	122	Sender Report	Source description	
16737 183.19802606	192.168.1.5	192.168.1.2	RTCP	106	Sender Report	Source description	
16746 183.22030006	192.168.1.2	192.168.1.5	RTCP	122	Sender Report	Source description	
16749 183.22756606	192.168.1.5	192.168.1.4	RTCP	106	Sender Report	Source description	
16832 183.64090606	192.168.1.2	192.168.1.5	RTCP	82	Receiver Report	Goodbye	
16869 195.08537506	192.168.1.2	192.168.1.5	RTCP	122	Sender Report	Source description	
16880 195.10878606	192.168.1.4	192.168.1.5	RTCP	142	Sender Report	Source description	Generic RTP Feedback
17925 200.27615606	192.168.1.2	192.168.1.5	RTCP	122	Sender Report	Source description	
18022 200.74805306	192.168.1.4	192.168.1.5	RTCP	142	Sender Report	Source description	Generic RTP Feedback
19171 206.39580106	192.168.1.4	192.168.1.5	RTCP	142	Sender Report	Source description	Generic RTP Feedback
19318 207.12766206	192.168.1.2	192.168.1.5	RTCP	122	Sender Report	Source description	
20606 213.53891206	192.168.1.4	192.168.1.5	RTCP	142	Sender Report	Source description	Generic RTP Feedback
20740 214.18486706	192.168.1.2	192.168.1.5	RTCP	122	Sender Report	Source description	

Рисунок 3.24 - Приклад перехопленого RTCP-трафіку

Аналізуючи інформацію по кожному RTCP-пакету (3.25), можна зібрати необхідну діагностичну інформацію для подальшого аналізу за допомогою запропонованої раніше СППР.

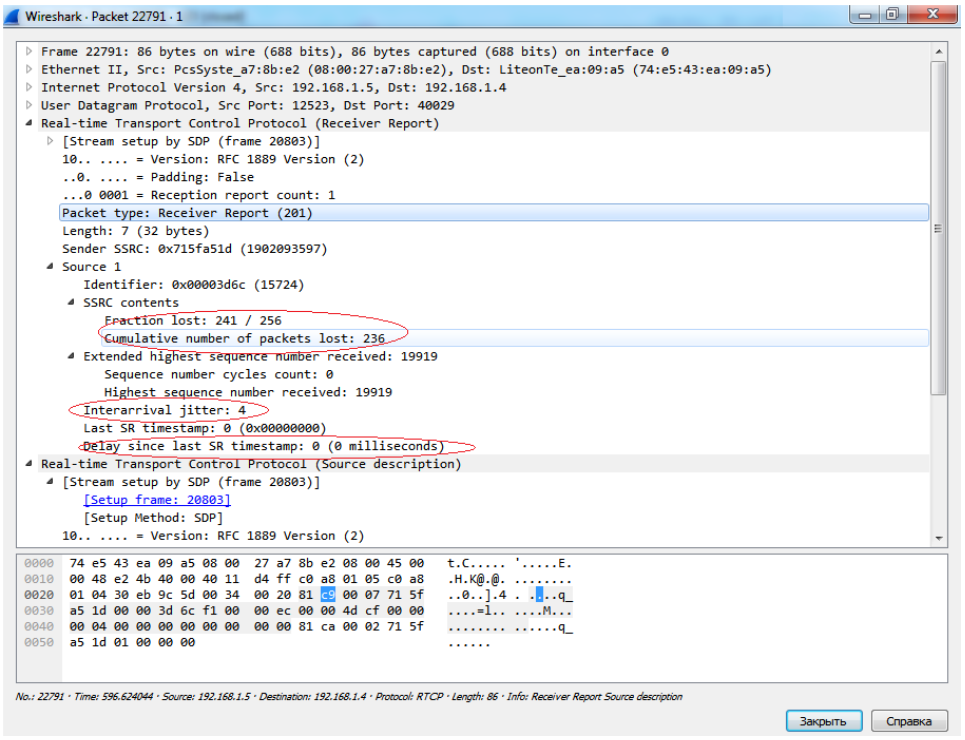


Рисунок 3.25 - Приклад детальної інформації по RTCP-пакету

На рисунку 3.26 представлена схема взаємодії сервера IP-телефонії з нечіткою СППР.

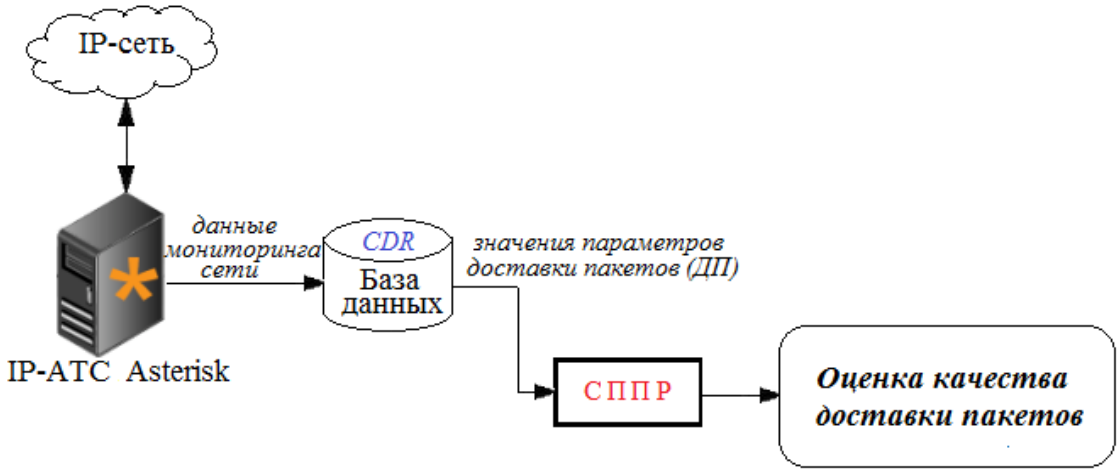


Рисунок 3.26 - Взаємодія запропонованої моделі СППР з АТС Asterisk

Очевидно, що діагностичний вузол може бути реалізований як апаратно, так і програмно, але це вимагає значних витрат ресурсів. Крім того, таке завдання і не стояло. Для демонстрації можливості застосування концепції «діагностичного вузла» на практиці, був обраний більш легкий шлях, де в якості ДВ виступав сам сервер IP-телефонії.

3.3 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 можу отримати об'єктивну оцінку якості доставки IP-пакетів.

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

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

3.3.1 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 інтерфейсах.

2. Затримка черги: час, який 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 сериализации: час, необхідний для переміщення фрейма в фізичну середу передачі.

4. Затримка поширення: час, який 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 достатній пропускній спроможності скорочується час очікування в вихідній черзі, 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 черга 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 черга 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.

3.3.2 Методи зменшення частки втрачених пакетів

Втрата пакетів відбувається в мережах будь-якого типу. У кожному мережевому протоколі розроблені методи для боротьби з цією проблемою тим чи іншим способом. 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 безліч маршрутизаторів і шлюзів. Деякі з цих перевалочних пунктів можна побачити за допомогою утиліти Traceroute. Але це далеко не все реальні транзитні вузли, наприклад не побачите тут ті вузли, через які трафік пройшов тунельованним (MPLS VPN, GRE і т.д.). При цьому з ненульовою 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 3.27, який показує, як може змінюватися відсоток втрачених пакетів з плином часу на одному і тому ж каналі зв'язку.

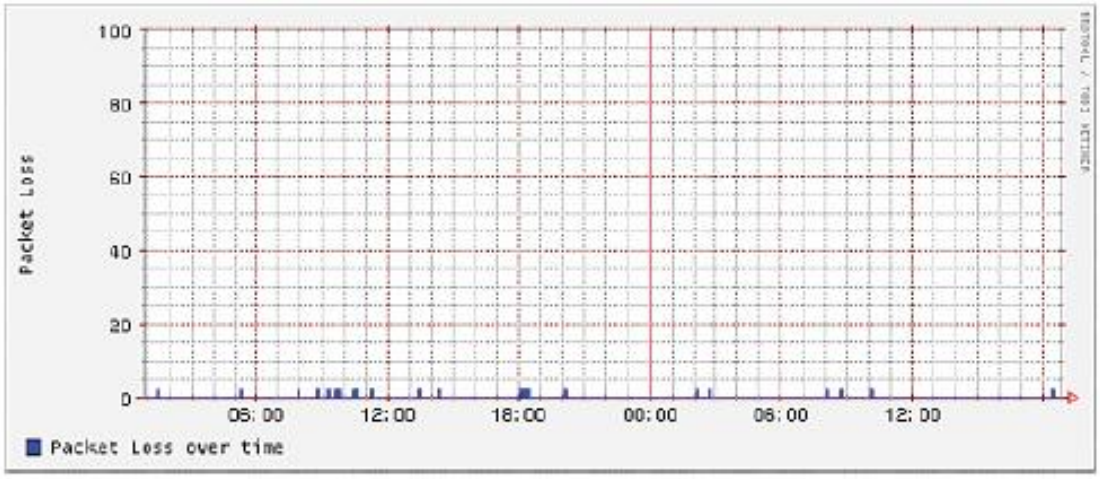


Рисунок 3.27 - Графік залежності числа втрати пакетів від часу доби

Теоретично, таке відкидання пакетів цілком нормально, так як за цілісністю 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. Але для того, щоб прийняти рішення про перепосилку, 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 сторона, що передає, буде в невіданні, і тим повільніше буде відбуватися передача інформації.

Нижче наведені графіки залежності швидкості передачі трафіку від затримки в каналі зв'язку і відсотки втрати пакетів (рис. 3.28).

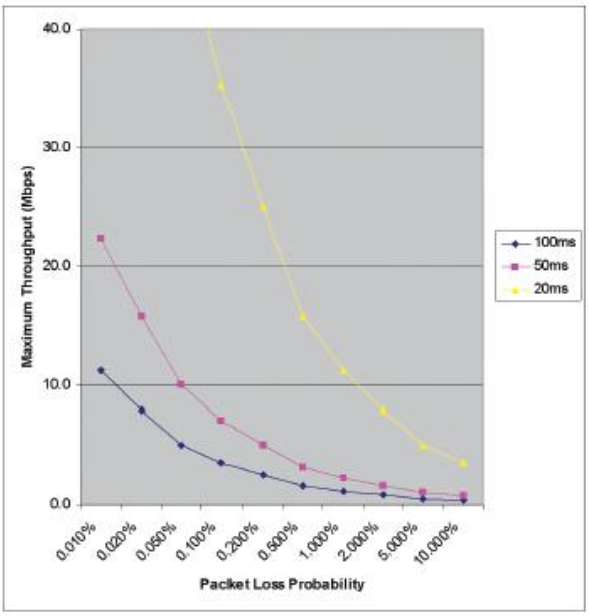


Рисунок 3.28 - Графік залежності пропускної спроможності від втрат пакетів і від затримки

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 непередбачений і невиправданий механізм повторної передачі. І якщо є втрати, то обов'язково вилазять артефакти у вигляді «квакання», «заїкань», і картинки, що періодично розсипається.

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

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

Як правило, втрата пакетів є результатом надмірного 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. Обмеження 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 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 МСМ 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 обчислювальним ресурсам. Це простий алгоритм, в якому відсутні фрагменти звуку заміщуються тишею, що дає найгіршу якість звуку, коли втрачено значну частину пакетів.

Заміщення формою сигналу (waveform substitution) використовується в старих протоколах і полягає в заміщенні втрачених пакетів новими, які генеруються 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 найкраща якість звуку. Правда, за це доводиться розплачуватися підвищеним обчислювальним 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 інші, ніяке маскування не здатно 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 мають загальну англомовну 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 3.29.

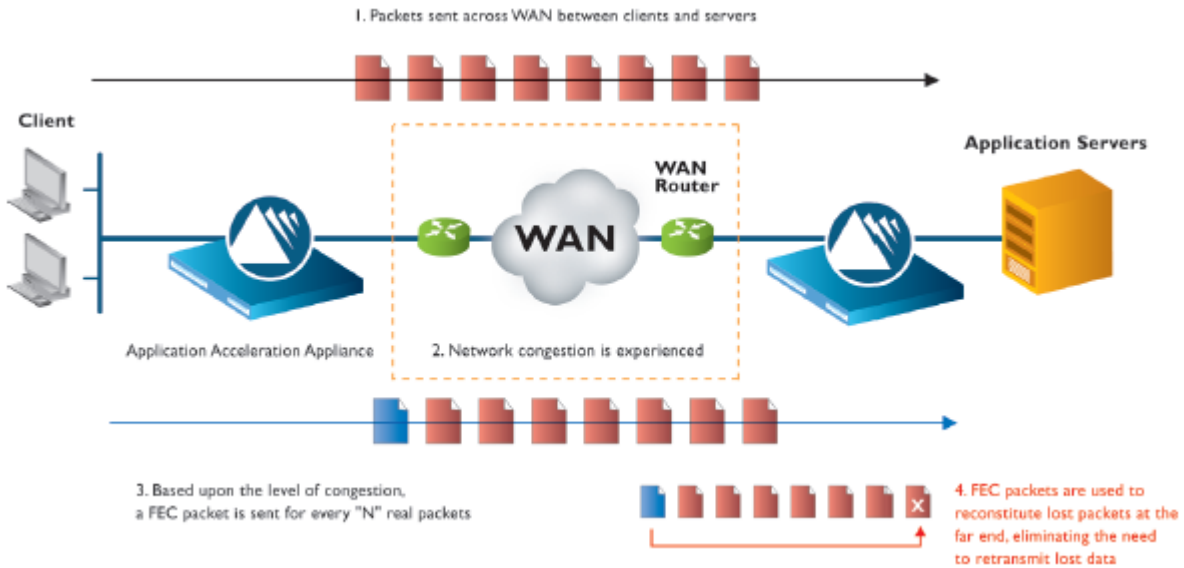


Рисунок 3.29 - Канал зв'язку із застосуванням технології FEC

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

Щоб оцінити ефективність застосування FEC для усунення втрат пакетів, можна подивитися на час передачі файлу через мережу Інтернет з певним відсотком втрати трафіку (рис. 3.30). З даного графіка видно, що навіть незначний відсоток надмірності, дозволяє в кілька разів підвищити швидкість передачі файлу, а проблеми «заїкання» в аудиоконференції і спотворення картинки під час відеоконференції відсутні.

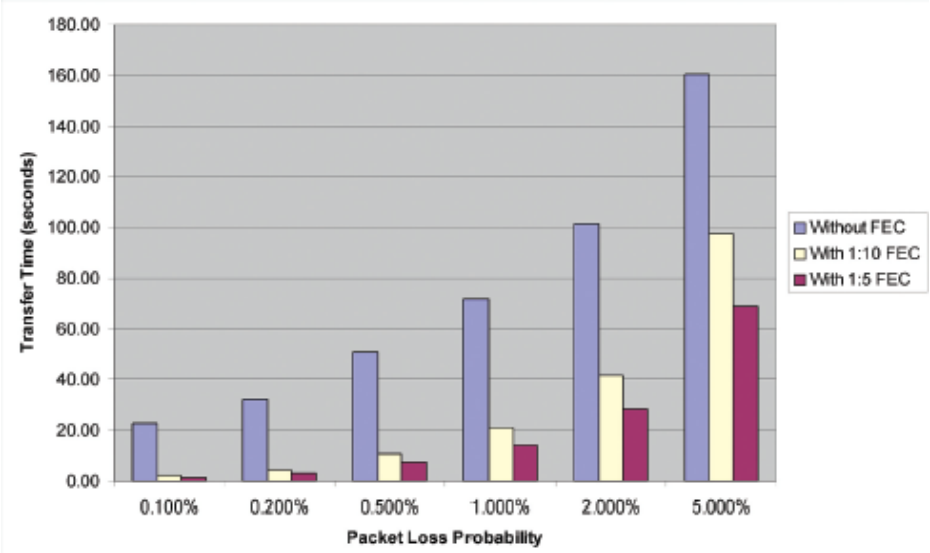


Рисунок 3.30 - Залежність часу передачі файлу від втрати пакетів при/без використання методу кодування FEC

3.3.3 Методи зменшення значення джиттера

Джиттер (jitter, варіація затримки) - це особливий показник для IP-мереж, який при виході з-під контролю може вплинути на якість переданого звуку.

На відміну від природної затримки при передачі в мережі, джиттер з'являється не через самий факт затримки, а через флуктуації часу затримки від пакета до пакету. У міру того, як IP-пристрої намагаються компенсувати джиттер шляхом збільшення розміру пакетного буфера, джиттер призводить до пауз у розмові. Якщо розкид стає занадто великим і перевищує 150 мс, то сторони зазвичай помічають ці затримки і розмова починає нагадувати розмову по рації.

Можна зробити деякі кроки для скорочення джиттера, як на мережевому рівні, так і на рівні IP-пристроїв (програмні IP-телефони, звичайні IP-телефони або VoIP-адаптери):

1. Скорочення затримок в мережі за визначенням дозволить тримати буфер в рамках 150 мс навіть у випадках наявності значних розбігів. Хоча зниження затримок зовсім необов'язково усуне їх варіацію, проте воно значно знизить ефект до такої міри, що він буде непомітний для мовців.

2. Пріоритезація VoIP-трафіку і шейпінг смуги пропускання можуть також знизити варіацію затримок пакетів.

3. Оптимізація джиттер-буфера в IP-пристрої також істотно впливає на результат. Хоча більший розмір буфера знижує або взагалі усуває джиттер, розмір буфера, що перевищує 150 мс, істотно впливає на сприймаєму якість розмови. Часто виявляються ефективними адаптивні алгоритми контролю розміру буфера в залежності від поточних мережевих умов.

4. Підбір розміру пакетів або використання іншого кодека (наприклад, G.711) часто допомагають контролювати джиттер.

Використання мережевого аналізатора для ідентифікації причини джиттера. Хоча джиттер частіше викликаний затримками в мережі, ніж самими IP-станціями, в певних системах з жорсткими обмеженнями ресурсів, які працюють в конкурентних середовищах (програмні VoIP-телефони), можуть бути присутніми значні і непередбачувані варіації в затримках пакетів. При розробці IP-станцій або при дослідженні проблем якості дзвінка в існуючій інфраструктурі IP вкрай важливим є ідентифікація самої причини джиттера. Мережевий аналізатор може бути надзвичайно корисний для швидкої і ефективної локалізації джерела проблеми. Гарний мережний аналізатор здатний розрахувати джиттер для кожного RTP-потоку і побудувати графіки залежності від часу як самого джиттера, так і його відхилення.

3.3.4 Методи зменшення помилок в IP-пакеті

Пакети з даними проходять по мережі незалежно один від одного і можуть при цьому піддаватися різним затримкам в залежності від точного шляху проходження. Пакети поза послідовністю не вважаються 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, які слідують 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 способи 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. Пакети 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 маршрутам і недопущення проходження пакетів від одного дзвінка по різних шляхах може істотно знизити кількість помилок послідовності.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ. ЕКОЛОГІЯ

В даному розділі проведено аналіз потенційних небезпечних та шкідливих виробничих факторів, причин пожеж. Розглянуті заходи, які дозволяють забезпечити гігієну праці і виробничу санітарію. На підставі аналізу розроблені заходи з техніки безпеки та рекомендації з пожежної профілактики.

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

Так як в процесі проектування використовувалося різне програмне забезпечення, то аналіз потенційно небезпечних і шкідливих виробничих чинників виконується для персонального комп'ютера.

4.1 Загальні питання з охорони праці

Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. В законі України «Про охорону праці» визначається, що охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

При роботі з обчислювальною технікою змінюються фізичні і хімічні фактори навколишнього середовища: виникає статична електрика, електромагнітне випромінювання, змінюється температура і вологість, рівень вміст кисню і озону в повітрі. Повітря забруднюється шкідливими хімічними речовинами антропогенного походження за рахунок деструкції полімерних матеріалів, які використовуються для обробки приміщень та обладнання. Неправильна організація робочого місця сприяє загальному і локальній напрузі м'язів шиї, тулуба, верхніх кінцівок, викривлення хребта і розвитку остеохондрозу. На всіх підприємствах, в установах, організаціях повинні створюватися безпечні і нешкідливі умови праці. Забезпечення цих умов покладається на власника або уповноважений ним орган (далі роботодавець). Умови праці на робочому місці, безпека

технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. Роботодавець повинен впроваджувати сучасні засоби техніки безпеки, які запобігають виробничому травматизмові, і забезпечувати санітарно-гігієнічні умови, що запобігають виникненню професійних захворювань працівників. Він не має права вимагати від працівника виконання роботи, поєднаної з явною небезпекою для життя, а також в умовах, що не відповідають законодавству про охорону праці. Працівник має право відмовитися від дорученої роботи, якщо створилася виробнича ситуація, небезпечна для його життя чи здоров'я або людей, які його оточують, і навколишнього середовища.

4.1.1 Правові та організаційні основи охорони праці

Основним організаційним напрямом у здійсненні управління в сфері охорони праці є усвідомлення пріоритету безпеки праці і підвищення соціальної відповідальності держави, і особистої відповідальності працівників.

Державна політика в галузі охорони праці визначається відповідно до Конституції України Верховною Радою України і спрямована на створення належних, безпечних і здорових умов праці, запобігання нещасним випадкам та професійним захворюванням. Відповідно до статті 3 Закону України «Про охорону праці» (далі – Закону) законодавство про охорону праці складається з Закону, Кодексу законів про працю України, Закону України "Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності" та прийнятих відповідно до них нормативно-правових актів, норм міжнародного договору (ратифіковані Конвенції і Рекомендації МОТ, директиви Європейської Ради).

На законодавчому рівні визначено такі пріоритетні напрямки з безпеки праці:

– кожен працівник несе безпосередню відповідальність за порушення зазначених Законом, нормами і правилами вимог;

– напрямки реалізації конституційного права громадян на їх життя і здоров’я в процесі трудової діяльності:

– пріоритет життя і здоров’я працівників по відношенню до результатів виробничої діяльності підприємства;

– повна відповідальність роботодавця за створення належних – безпечних і здорових умов праці;

– соціальний захист працівників, повне відшкодування збитків особам, які потерпіли від нещасних випадків на виробництві та професійних захворювань;

– комплексне розв'язання завдань охорони праці;

– підвищення рівня промислової безпеки шляхом забезпечення суцільного технічного контролю за станом виробництв, технологій та продукції, а також сприяння підприємствам у створенні безпечних та нешкідливих умов праці;

– соціальний захист працівників, повне відшкодування збитків особам, які потерпіли від нещасних випадків на виробництві та професійних захворювань;

– використання економічних методів управління охороною праці, участь держави у фінансуванні заходів щодо охорони праці;

– використання світового досвіду організації роботи щодо поліпшення умов і підвищення безпеки праці на основі міжнародної співпраці.

Користувачі персональних комп'ютерів, для яких ця робота є головною, підлягають медичним оглядам: попереднім — під час влаштування на роботу і періодичним — протягом професійної діяльності раз на два роки. Жінок з часу встановлення вагітності та в період годування дитини грудьми до роботи з ПК не допускають.

4.1.2 Організаційно-технічні заходи з безпеки праці

В організації/підприємстві проводиться навчання і перевірка знань з питань охорони праці відповідно до вимог Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого наказом Держнаглядохоронпраці України від 26.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511 [43].

Також впроваджені організаційні заходи з пожежної безпеки - навчання і перевірку знань відповідно до вимог Типового положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 29.09.2003 N 368, зареєстрованого в Міністерстві юстиції України 11.12.2003 за N 1148/8469 [44].

Обов'язковими вимогами враховане наступне:

– не слід допускати до роботи осіб, що в установленому порядку не пройшли навчання, інструктаж та перевірку знань з охорони праці, пожежної безпеки та цих Правил.

– на підприємстві/організації, де експлуатуються ЕОМ з відео дисплейними

терміналами (ВДТ) і периферійними пристроями (ПП), розробляється інструкція з охорони праці відповідно до Положення про розробку інструкцій з охорони праці, затвердженого наказом Держнаглядохоронпраці від 29.01.98 N 9, зареєстрованого в Міністерстві юстиції України 07.04.98 за N 226/2666 (НПАОП 0.00-4.15-98).

– ознайомлення з правилами безпеки праці, одержання відповідних інструктажів засвідчується у журналі інструктажів.

– перед допуском до самостійної роботи кожен працівник має право на навчання з питань охорони праці і роботодавець зобов'язаний, і проводить таке навчання у вигляді двох інструктажів з питань охорони праці:

1) вступного, який проводять працівники служби охорони праці об'єкта господарювання з усіма працівниками, яких приймають на роботу незалежно від їхньої освіти та стажу роботи за програмою, в якій подають загальні питання охорони праці із врахуванням її особливостей на об'єкті господарювання;

2) первинного, який проводять керівники структурних підрозділів на місці праці з кожним працівником до початку їхньої роботи на цьому робочому місці.

Проходження працівником цих інструктажів з питань охорони праці підтверджується записами у відповідних журналах обліку інструктажів і скріплюється підписами осіб, які проводили інструктажі та осіб, які отримали інструктажі.

3) Повторний (не рідше одного разу в 6 місяців);

А) Позаплановий (при зміні правил охорони праці);

5) Поточний (проводять з працівниками перед виконанням робіт, на яких оформляється наряд-допуск)

– обов'язкові організаційні заходи перед початком, під час і після завершення роботи повинні включати перевірку (візуально) наявності і справності електрообладнання та його заземлення, а під час виконання роботи вимогу «не залишати без нагляду обладнання, яке працює». Після закінчення роботи - вимагається прибирання робочого місця, відключення всіх електроприладів від електромережі.

Не допускається:

– виконувати обслуговування, ремонт та налагодження ЕОМ з ВДТ і ПП безпосередньо на робочому місці оператора;

– зберігати біля ЕОМ з ВДТ і ПП папір, дискети, інші носії інформації, запасні блоки, деталі тощо, якщо вони не використовуються для поточної роботи;

– відключати захисні пристрої, самочинно проводити зміни у конструкції та складі ЕОМ з ВДТ і ПП або їх технічне налагодження;

– працювати з ВДТ, у яких під час роботи з'являються нехарактерні сигнали,

нестабільне зображення на екрані тощо;

– працювати з матричним принтером за відсутності вібраційного килимка та зі знятою (піднятою) верхньою кришкою.

4.2 Аналіз стану умов праці

Робота над створенням системи проходитиме в приміщенні багатоквартирного будинку. Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп'ютером.

4.2.1 Вимоги до приміщень

Геометричні розміри приміщення зазначені в табл. 4.1.

Таблиця 4.1 – Розміри приміщення

Найменування	**Значення**
Довжина, м	5
Ширина, м	5
Висота, м	3
Площа, $м^2$	25
Об'єм, $м^3$	75

Згідно з [45] розмір площі для одного робочого місця оператора персонального комп'ютера має бути не менше 6 кв. м, а об'єм — не менше 20 куб. м. Отже, дане приміщення цілком відповідає зазначеним нормам.

Робочий процес пов'язаний з багатьма документами для чого приміщення облаштоване принтером і шафою для зручності. Задля дотримання визначеного рівня мікроклімату в будівлі встановлено систему опалення та кондиціонування.

Для забезпечення потрібного рівного освітленості кімната має вікно та систему загального рівномірного освітлення, що встановлена на стелі. Для дотримання вимог пожежної безпеки встановлено порошковий вогнегасник та систему автоматичної пожежної сигналізації.

4.2.2 Вимоги до організації місця праці

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця за [46] і відповідними фактичними значеннями для

робочого місця, констатуємо повну відповідність.

Таблиця 4.2 - Характеристики робочого місця

Найменування параметра	Фактичне значення	Нормативне значення
Висота робочої поверхні, мм	700	680 ÷800
Висота простору для ніг, мм	700	не менше 600
Ширина простору для ніг, мм	600	не менше 500
Глибина простору для ніг, мм	700	не менше 650
Висота поверхні сидіння, мм	450	400 ÷500
Ширина сидіння, мм	430	не менше 400
Глибина сидіння, мм	450	не менше 400
Висота поверхні спинки, мм	500	не менше 300
Ширина опорної поверхні спинки, мм	500	не менше 380
Радіус кривини спинки в горизонтальній площині, мм	400	400
Відстань від очей до екрану дисплея, мм	750	700 ÷800

Робочий стіл на досліджуваному місці також містить достатньо простору для ніг. Крісло, що використовується в якості робочого сидіння, є підйомно-поворотним, має підлокітники і можливість регулювання за висотою і кутом нахилу спинки.

Екран монітору знаходиться на відстані 0.8 м, клавіатура має можливість регулювання кута нахилу 5-15°. Отже, за всіма параметрами робоче місце відповідає нормативним вимогам.

Приміщення кабінету знаходиться на третьому поверсі трьох поверхової будівлі і має об'єм 75 $м^3$, площу – 25 $м^2$. У цьому кабінеті обладнано два місця праці, з яких обидва укомплектовані ПК.

Температура в приміщенні протягом року коливається у межах 19–24°С, відносна вологість — близько 50%. Швидкість руху повітря не перевищує 0,2 м/с. Шум знаходиться на рівні 50 дБА. Система вентилювання приміщення — природна неорганізована, а опалення — централізоване.

Розміщення вікон забезпечує природне освітлення з коефіцієнтом природного освітлення не менше 1,5%, а загальне штучне освітлення, яке здійснюється за допомогою восьми люмінесцентних ламп, забезпечує рівень освітленості не менше 200 Лк.

У кабінеті є електрична мережа з напругою 220 В, яка створює небезпеку ураження електричним струмом. ПК та периферійні пристрої можуть бути джерелами електромагнітних випромінювань, аерозолів та шкідливих речовин (часток тонеру, оксидів нітрогену та озону).

За ступенем пожежної безпеки приміщення належить до категорії В. Кабінет оснащений переносним вуглекислотним вогнегасником ВВК-5 .

4.2.3 Навантаження та напруженість процесу праці

Як приклад наведено опис процесу праці *"оформлення роботи"* під час виконання магістерської роботи: за фізичним навантаженням робота відноситься до категорії легкі роботи (Іа), її виконують сидячи з періодичним ходінням. Щодо характеру організування виконання дипломної роботи, то вона підпадає під нав'язаний режим, оскільки певні розділи роботи необхідно виконати у встановлені конкретні терміни. За ступенем нервово-психічної напруги виконання роботи можна віднести до II – III ступеня і кваліфікувати як помірно напружений – напружений за умови успішного виконання поставлених завдань.

Під час виконання робіт використовують ПК та периферійні пристрої (лазерні), що призводить до навантаження на окремі системи організму. Такі перекоси у напруженні різних систем організму, що трапляються під час роботи з ПК, зокрема, значна напруженість зорового аналізатора і довготривале малорухоме положення перед екраном, не тільки не зменшують загального напруження, а навпаки, призводять до його посилення і появи стресових реакцій.

Найбільшому ризику виникнення різноманітних порушень піддаються: органи зору, м'язово скелетна система, нервово-психічна діяльність, репродуктивна функція у жінок.

Тобто наявне психофізіологічні небезпечні та шкідливі фактори:

а) фізичного перевантаження:

- статичного;
- динамічного;

б) нервово-психічного перевантаження:

- розумового перенапруження;
- монотонності праці;
- перенапруження аналізаторів;
- емоційних перевантажень.

Рекомендовано застосування екранних фільтрів, локальних світлофільтрів (засобів індивідуального захисту очей) та інших засобів захисту, а також інші профілактичні заходи наведені в [46]

Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви:

- для розробників програм тривалістю 15 хв через кожну годину роботи;
- для операторів персональних комп'ютерів тривалістю 15 хв через дві години роботи;
- для операторів комп'ютерного набору тривалістю 10 хв через кожну годину роботи.

4.3 Виробнича санітарія

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації), пожежної безпеки можуть бути надалі вирішені питання необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо.

4.3.1 Аналіз небезпечних та шкідливих факторів при виробництві (експлуатації) виробу

Роботу, пов'язану з ЕОП з ВДТ, у тому числі на тих, які мають робочі місця, обладнані ЕОМ з ВДТ і ПП, виконують із забезпеченням виконання НПАОП 0.00.-1.28-10 «Правил охорони праці під час експлуатації електронно-обчислювальних машин», які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ЕОМ з ВДТ і ПП. Переважно роботи за проектами виконують у кабінетах чи інших приміщеннях, де використовують різноманітне електрообладнання, зокрема персональні комп'ютери (ПК) та периферійні пристрої.

Основними робочими характеристиками персонального комп'ютера є наступні:

– робоча напруга U = +220В ± 5%;
– робочий струм I = 2А;
– споживана потужність P = 350 Вт.

Робочі місця мають відповідати вимогам Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин, затверджених постановою Головного державного санітарного лікаря України від 10.12.98 N 7 [46].

За умов роботи з ПК виникають наступні небезпечні та шкідливі чинники: несприятливі мікрокліматичні умови, освітлення, електромагнітні випромінювання, забруднення повітря шкідливими речовинами (джерелом, яких можуть бути: принтер, сканер та інші джерела виділення багатьох хімічних речовин - напр., озону, оксидів азоту та аерозолів високодисперсних частинок тонера), шум, вібрація, електричний струм, електростатичне поле, напруженість трудового процесу та інше.

Аналіз небезпечних та шкідливих виробничих факторів виконується у табличній формі (табл. В.1 додатку В).

4.3.2 Пожежна безпека

Небезпека розвитку пожежі на обчислювальному центрі обумовлюється застосуванням розгалужених систем електроживлення ЕОМ, вентиляції і кондиціювання,. Небезпека загоряння пов'язана з особливістю комп'ютерів - із значною кількістю щільно розташованих на монтажній платі і блоках електронних вузлів і схем, електричних і комутаційних кабелів, резисторів, конденсаторів, напівпровідникових діодів і транзисторів. Надійна робота окремих елементів і мікросхем в цілому забезпечується тільки в певних інтервалах температури, вологості і при заданих електричних параметрах. При відхиленні реальних умов експлуатації від розрахункових можуть виникнути пожежонебезпечні ситуації.

Висока щільність елементів в електронних схемах призводить до значного підвищення температури окремих вузлів (80…100 ℃). При проходженні електричного струму по провідниках і деталей виділяється тепло, що в умовах їх високої щільності може привести до перегріву, і може служити причиною запалювання ізоляційних матеріалів. Слабкий опір ізоляційних матеріалів дії температури може викликати порушення ізоляції і привести до короткого замикання між струмоведучими частинами обладнання (шини, електроди). Також ймовірна небезпека внаслідок перевантаження напруги, розрядки зарядів статичної електрики, пошкодження обладнання та електропроводки. Електростатичний розряд виникає під час тертя двох ізольованих матеріалів. Розряд статичної електрики може виникнути під час роботи вентилятора або комп'ютер. Кабельні лінії є найбільш пожежонебезпечними місцем. Наявність пального ізоляційного матеріалу, ймовірних джерел запалювання у вигляді електричних іскор і дуг, розгалуженість і недоступність роблять кабельні лінії місцем найбільш ймовірного виникнення і розвитку пожежі. Для зниження займистості і здатності поширювати полум'я кабелі покривають вогнезахисними покриттями. Проектом передбачено прокладати

проводку: приховано, під знімною підлогою розділяючи негорючими діафрагмами, в малодоступних місцях.

Для гасіння пожеж в офісному приміщенні пропонується використовувати порошкові або вуглекислотні вогнегасники, так як вони є універсальними. Заземлені конструкції, що знаходяться в приміщеннях, де розміщені робочі місця (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном), надійно захищені діелектричними щитками та/або сітками з метою недопущення потрапляння працівника під напругу. Дане приміщення оснащено системою автоматичної пожежної сигналізації, має 1 вогнегасник ВП-5 із зарядом вогнегасної речовини 8-12 кг, відповідно до вимог чинного законодавства України. Проходи до засобів пожежогасіння вільні, не захаращуються та у разі потреби забезпечувати евакуацію всіх людей, які перебувають у приміщенні через один евакуаційний вихід з дверима на шляху евакуації, що відчинятися в напрямку виходу з будівлі від робочого місця. В приміщенні наявна затверджена «План-схема евакуації з кабінету (приміщення)».

Пожежна безпека при застосуванні ЕОМ забезпечується:

1) системою запобігання пожежі,

2) системою протипожежного захисту,

3) організаційно-технічними заходами.

Запобігти утворенню горючого середовища (замінити горючі речовини і матеріали на негорючі і важкогорючі) не надається технічно можливим. Тому проектом передбачаються способи і засоби запобігання утворення (або внесення) в горюче середовище джерел запалювання, таких як:

1) застосування електроустаткування, відповідної пожежонебезпечної і вибухонебезпечної зонам відповідно до ПУЕ;

2) застосування в конструкції швидкодійних засобів захисного відключення можливих джерел запалення;

3) виключення можливості появи іскрового розряду в горючому середовищі з енергією, рівної і вище мінімальної енергії запалення.

Згідно НАПБ Б.03.002-2007 таке приміщення, площею 25 м^2, відноситься до категорії "В" (пожежонебезпечної) та для протипожежного захисту в ньому проектом передбачено устаткування автоматичною пожежною сигналізацією із застосуванням датчиків-сповіщувачів РІД-1 (сповіщувач димовий ізоляційний) в кількості 1 шт., і застосуванням первинних засобів пожежогасіння. Відповідно до норм первинних засобів пожежогасінні пропонується використовувати:

- ручний вуглекислий вогнегасник ОУ-5 в кількості 1 шт. або хімічний пінний

ОХП-10 – 1 шт;

- повсть 1 1 м^2, кошму 2×1,5 м^2 або азбестове полотно 2×2 м^2 в кількості 1 шт.

Виникнення пожежі можливе, якщо на об'єкті є горючі речовини, окислювач і джерела запалювання. Вірогідність пожежної небезпеки приймається значною, якщо ймовірна взаємодія цих трьох чинників. Горючими компонентами є: будівельні матеріали для акустичної і естетичної обробки приміщень, перегородки, підлоги, двері, ізоляція силових, сигнальних кабелів і т.д.

Горючими матеріалами в приміщенні, де розташовані ЕОМ, є:

1) поліамід – матеріал корпусу мікросхем, горюча речовина, температура самозаймання 420º С,

2) полівінілхлорид – ізоляційний матеріал, горюча речовина, температура запалювання 335º С, температура самозаймання 530º С,

3) склотекстоліт ДЦ – матеріал друкарських плат, важкогорючий матеріал, показник горючості 1.74, не схильний до температурного самозаймання,

А) пластикат кабельний №.489 – матеріал ізоляції кабелів, горючий матеріал, показник горючості більше 2.1,

5) деревина – будівельний і обробний матеріал, з якого виготовлені меблі, горючий матеріал, показник горючості більше 2.1, температура запалювання 255º С, температура самозаймання 399º С.

Для відводу теплоти від ЕОМ діє потужна система кондиціонування. Тому кисень, як окиснювач процесів горіння, є в будь-якій точці приміщень ВЦ.

Простори усередині приміщень в межах, яких можуть утворюватися або знаходиться пожежонебезпечні речовини і матеріали відповідно до [47] відносяться до пожежонебезпечної зони класу П-IIа. Це обумовлено тим, що в приміщенні знаходяться тверді горючі та важкозаймисті речовини та матеріали. Приміщенню, у якому розташоване робоче місце, присвоюється II ступень вогнестійкості.

Потенційними джерелами запалювання можуть бути:

1) іскри і дуги короткого замикання;

2) електрична іскра при замиканні і розмиканні ланцюгів;

3) перегріви від тривалого перевантаження,

4) відкритий вогонь і продукти горіння,

5) наявність речовин, нагрітих вище за температуру самозаймання,

6) розрядна статична електрика.

Причинами можливого загоряння і пожежі можуть бути:

1) несправність електроустановки;

2) конструктивні недоліки устаткування;

3) коротке замикання в електричних мережах;

4) запалювання горючих матеріалів, що знаходяться в безпосередній близькості від електроустановки.

Продуктами згорання, що виділяються на пожежі, є: окис вуглецю; сірчистий газ; окис азоту; синильна кислота; акромін; фосген; хлор і ін. При горінні пластмас, окрім звичних продуктів згорання, виділяються різні продукти термічного розкладання: хлорангідридні кислоти, формальдегіди, хлористий водень, фосген, синильна кислота, аміак, фенол, ацетон, стирол. (ГОСТ 12.1.044-89).

Для захисту персоналу від дії небезпечних і шкідливих чинників пожежі проектом передбачається застосування промислового протигаза, що фільтрує, з коробкою марки «В» із сірою відміткою забарвлення – захист від неорганічних газів (хлор, фтор, бром, сірководень, сірковуглець, хлорциан, галогени), а цей фільтр не захистить від СО (тобто від чадного газу).

Можливе також відповідне застосування фільтрувальної коробки з маркуванням «СО» із фіолетовим забарвленням на фільтрі означає, що він захищає від Чадного газу. Або фільтру для протигазу з літерним маркуванням «SX» із фіолетовим забарвленням захистить від спец речовин таких як (зарин, зоман та фосген).

4.3.3 Електробезпека

На робочому місці виконуються наступні вимоги електробезпеки: ПК, периферійні пристрої та устаткування для обслуговування, електропроводи і кабелі за виконанням та ступенем захисту відповідають класу зони за ПУЕ (правила улаштування електроустановок), мають апаратуру захисту від струму короткого замикання та інших аварійних режимів. Лінія електромережі для живлення ПК, периферійних пристроїв і устаткування для обслуговування, виконана як окрема групова три- провідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників мають спеціальні контакти для підключення нульового захисного провідника. Електромережа штепсельних розеток для живлення персональних ПК, укладено по підлозі поруч зі стінами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання. Металеві труби та гнучкі металеві рукави заземлені. Захисне заземлення включає в себе заземлюючих пристроїв і провідник,

який з'єднує заземлюючий пристрій з обладнанням, яке заземлюється - заземлюючий провідник.

4.4 Гігієнічні вимоги до параметрів виробничого середовища

4.4.1 Мікроклімат

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря. В даному приміщенні проводяться роботи, що виконуються сидячи і не потребують динамічного фізичного напруження, то для нього відповідає категорія робіт Іа. Отже оптимальні значення для температури, відносної вологості й рухливості повітря для зазначеного робочого місця відповідають [48] і наведені в табл. 4.3:

Таблиця 4.3 – Норми мікроклімату робочої зони об’єкту

Період року	**Категорія робіт**	**Температура C^0**	**Відносна вологість %**	**Швидкість руху повітря, м/с**
Холодна	легка-1 а	22 - 24	40 – 60	0,1
Тепла	легка-1 а	23 - 25	40 – 60	0,1

Дане приміщення обладнане системами опалення, кондиціонування повітря або припливно-витяжною вентиляцією. У приміщенні на робочому місці забезпечуються оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря у відповідності до [48]. Рівні позитивних і негативних іонів у повітрі мають відповідати [48]. Для забезпечення оптимальних параметрів мікроклімату в приміщенні проводяться перерви в роботі співробітників, з метою його провітрювання. Існують спеціальні системи кондиціонування, які забезпечують підтримання в приміщенні балансу оптимальних параметрів мікроклімату. Контроль параметрів мікроклімату в холодний і теплий період року здійснюється не менше 3-х разів на зміну (на початку, середині, в кінці).

4.4.2 Освітлення

Світло є природною умовою існування людини. Воно впливає на стан вищих психічних функцій і фізіологічні процеси в організмі. Хороше освітлення діє тонізуюче, створює гарний настрій, покращує протікання основних процесів вищої нервової

діяльності.

Збільшення освітленості сприяє поліпшенню працездатності навіть в тих випадках, коли процес праці практично не залежить від зорового сприйняття. При поганому освітленні людина швидко втомлюється, працює менш продуктивно, виникає потенційна небезпека помилкових дій і нещасних випадків.

Освітленість приміщення має велике значення при роботі на ПЕОМ. Вона багато в чому визначається колірною і мережевий обстановкою. Для зменшеного поглинання світла стеля і стіни вище панелей (1,5-1,7м.). Якщо вони не облицьовані звукопоглинальним матеріалом, фарбуються білою водоемульсійною фарбою (коефіцієнт відбиття повинен бути не менше 0,7). Для забарвлення стіни панелей рекомендується віддавати перевагу світлим фарбам.

Основний потік природного світла при цій повинен бути зліва. Не допускається спрямування основного світлового потоку природного світла праворуч, ззаду і спереду працівника на ПЕОМ.

Робота на ПЕОМ може здійснюватися за таких видах освітлення:

- загальному штучному освітленні, коли відео монітори розташовуються по периметру приміщення або при центральному розташуванні робочих місць у два ряди по довжині кімнати з екранами, звернені в протилежні сторони;

- суміщене освітлення (природне + штучне) тільки при одному і трьох рядном розташуванні робочих місць, коли екран і поверхню робочого столу знаходяться перпендикулярно світла несучій стіні. При цьому штучне освітлення буде виконане стельовими або підвісними люмінесцентними світильниками, рівномірно розміщеними по стелі рядами паралельно світловим прорізам так, щоб екран відео монітора знаходився в зоні захисного кута світильника, і його проекції не доводилися на екран. Працюючі на ПЕОМ не повинні бачити відображення світильників на екрані. Застосовувати місцеве освітлення при роботі на ПЕОМ не рекомендується.

Природне освітлення, коли робочі місця з ПЕОМ розташовуються в один ряд по довжині приміщення на відстані 0,8 - 1,0 м від стіни з віконними прорізами, і екрани знаходяться перпендикулярно цієї стіни. Основний потік природного світла при цій повинен бути зліва. Не допускається спрямування основного світлового потоку природного світла праворуч, ззаду і спереду працює на ПЕОМ. Оптимальна відстань очей до екрана відео монітора повинна становити 60-70 см, допустиме не менше 50 см. Розглядати інформацію ближче 50 см не рекомендується.

У проекті, що розробляється, передбачається використовувати суміщене освітлення. У світлий час доби використовуватиметься природне освітлення приміщення

через віконні отвори, в решту часу використовуватиметься штучне освітлення. Штучне освітлення створюється газорозрядними лампами.

Штучне освітлення в робочому приміщенні передбачається здійснювати з використанням люмінесцентних джерел світла в світильниках загального освітлення, оскільки люмінесцентні лампи мають високу потужність (80 Вт), тривалий термін служби (до 10000 годин), спектральний складом випромінюваного світла, близький до сонячного. При експлуатації ЕОМ виконується зорова робота IV в розряду точності (середня точність). При цьому нормована освітленість на робочому місці (Ен) рівна 200 лк. Джерелом природного освітлення є сонячне світло.

У приміщенні, де розташовані ЕОМ передбачається природне бічне освітлення, рівень якого відповідає СНіП 11-4-79. Джерелом природного освітлення є сонячне світло. Регулярно повинен проводитися контроль освітленості, який підтверджує, що рівень освітленості задовольняє СНіП і для даного приміщення в світлий час доби достатньо природного освітлення.

Розрахунок освітлення.

Для будівель виробництв світловий коефіцієнт приймається в межах 1/6 - 1/10:

$$\sqrt{a^2+b^2}\cdot S_b = 1/8 \div 1/10 \cdot S_n \qquad (4.1)$$

де S_b – площа віконних прорізів, м^2;

S_n – площа підлоги, м^2.

$S_n = a \cdot b = 5 \cdot 5 = 25$ м^2

$S_{вік} = 1/8 \cdot 25 = 3{,}125$ м^2

Приймаємо 2 вікна площею $S = 1{,}6$ м^2 кожне.

Світильники загального освітлення розташовуються над робочими поверхнями в рівномірно-прямокутному порядку. Для організації освітлення в темний час доби передбачається обладнати приміщення, довжина якого складає 5 м, ширина 5 м, світильниками ЛПО2П, оснащеними лампами типу ЛБ (дві по 80 Вт) з світловим потоком 5А00 лм кожна.

Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників *n* виробляється по формулі (4.2):

$$n = \frac{E \cdot S \cdot Z \cdot K}{F \cdot U \cdot M} \tag{4.2}$$

де E – нормована освітленість робочої поверхні, визначається нормами – 300 лк;

S – освітлювана площа, м^2; S = 25 м^2;

Z – поправочний коефіцієнт світильника (Z = 1,15 для ламп розжарювання та ДРЛ; Z = 1,1 для люмінесцентних ламп) приймаємо рівним 1,1;

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0,575

M – число люмінесцентних ламп в світильнику – 2;

F – світловий потік лампи – 5А00лм (для ЛБ-80).

Підставивши числові значення у формулу (4.2), отримуємо:

$$\text{n} = \frac{300 \cdot 25 \cdot 1{,}1 \cdot 1{,}5}{5400 \cdot 0{,}575 \cdot 2} \approx 2.$$

Приймаємо освітлювальну установку, яка складається з 2-х світильників, які складаються з двох люмінесцентних ламп загальною потужністю 160 Вт, напругою – 220 В.

4.5 Шум та вібрація, електромагнітне випромінювання

Рівень шуму, що супроводжує роботу користувачів персональних комп’ютерів (зумовлений як роботою системних блоків, клавіатури, так і друкуванням на принтерах, а також зовнішніми чинниками), коливається у межах 50–65 дБА [49]. Шум такої інтенсивності на тлі високого ступеня напруженості праці негативно впливає на функціональний стан користувачів. Тому на практиці рекомендують знижувати фактичний рівень шуму у приміщеннях, де створюють комп’ютерні програми, виконують теоретичні та творчі роботи, проводять навчання до 40 дБА, а в приміщеннях, де виконують роботу, що потребує зосередженості, — до 55 дБА. У залах опрацювання інформації та комп’ютерного набору рівні шуму не повинні перевищувати 65 дБА.

Шум часто є причиною зниження рівня працездатності, підвищення рівня загальної та професійної захворюваності, частоти виробничих травм. Шум є загальнобіологічним подразником, який негативно впливає на всі органи і системи організму. У разі тривалого систематичного впливу шуму може виникнути патологія з переважним ураженням слуху, центральної нервової і серцево- судинної систем.

Для зниження шуму на шляху його поширення передбачається розміщення в приміщенні штучних поглиначів. Для зниження рівня шуму стелю або стіни вище 1.5 - 1.7 метра від підлоги повинні облицьовуватися звукопоглинальним матеріалом з максимальним коефіцієнтом звукопоглинання в області частот 63-8000 Гц. Додатковим звукопоглинанням в КВТ можуть бути фіранки, підвішені в складку на відстані 15-20 см. Від огорожі, виконані з щільної, важкої тканини. У приміщенні з ЕОМ коректований рівень звукової потужності не перевищує 45 дБА. Оскільки рівень шуму не перевищує гранично допустимих величин, які встановлені санітарними нормами, заходи для зниження шуму не проводяться.

Віброізоляція можливо здійснювати за допомогою спеціальної прокладки під системний блок, який послаблює передачу вібрацій робочого столу. Вібрація на робочому місці в приміщенні, що розглядається, відповідає нормам [49]. Допустимий рівень вібрацій на робочому місці: для 1 ступеня шкідливості до 3 дБ; для 2-3 - 1-6 дБ; для 3 - більше 6 дБ.

Для захисту від електромагнітного випромінювання передбачаються наступні заходи:

1) застосування нових плазмових моніторів, LG W2271TC,

2) віддалення робочого місця не менше, ніж на 0,4-0,5 м, оскільки напруженість електричного поля зменшується при віддаленні від джерела поля,

3) встановлення раціональних режимів роботи персоналу (обмеження часу перебування),

4) раціональне розміщення в робочому приміщенні устаткування, що випромінює електромагнітну енергію.

4.6 Вентилювання

У приміщенні, де знаходяться ЕОМ, повітрообмін реалізується за допомогою природної організованої вентиляції (вентиляційні шахти) і установки в віконному отворі автономного кондиціонера БК-2000. Цей метод забезпечує приплив потрібної кількості свіжого повітря, що визначається в СНіП (30 $м^3$ на годину на одного працюючого).

Також має здійснюватися провітрювання приміщення, в залежності від погодних умов, тривалість повинна бути не менше 10 хв. Найкращий обмін повітря здійснюється при наскрізному провітрюванні.

4.7 Заходи з організації виробничого середовища та попередження виникнення надзвичайних ситуацій

Відповідно до санітарно-гігієнічних нормативів та правил експлуатації обладнання наводимо приклади деяких заходів безпеки.

1) Заходи безпеки під час експлуатації персонального комп'ютера та периферійних пристроїв передбачають:

- правильне організування місця праці та дотримання оптимальних режимів праці та відпочинку під час роботи з ПК;
- експлуатацію сертифікованого обладнання;
- дотримання заходів електробезпеки;
- забезпечення оптимальних параметрів мікроклімату;
- забезпечення раціонального освітлення місця праці (освітленість робочого місця не перевищувала 2/3 нормальної освітленості приміщення);
- облаштовуючи приміщення для роботи з ПК, потрібно передбачити припливно-витяжну вентиляцію або кондиціювання повітря:

а) якщо об'єм приміщення 20 $м^3$, то потрібно подати не менш як 30 $м^3$/год повітря;

б) якщо об'єм приміщення у межах від 20 до 40 $м^3$, то потрібно подати не менш як 20 $м^3$/год повітря;

в) якщо об'єм приміщення становить понад 40 $м^3$, допускається природна вентиляція, у випадку, коли немає виділення шкідливих речовин.

- зниження рівня шуму та вібрації:

а) у джерелі виникнення, шляхом застосування раціональних конструкцій, нових матеріалів і технологічних процесів;

б) звукоізоляція устаткування за допомогою глушників, резонаторів, кожухів, захисних конструкцій, оздоблення стін, стелі, підлоги тощо;

в) використання засобів індивідуального захисту).

2) Заходи безпеки під час експлуатації інших електричних приладів передбачають дотримання таких правил:

- постійно стежити за справним станом електромережі, розподільних щитків, вимикачів, штепсельних розеток, лампових патронів, а також мережевих кабелів живлення, за допомогою яких електроприлади під'єднують до електромережі;

- постійно стежити за справністю ізоляції електромережі та мережевих кабелів, не допускаючи їхньої експлуатації з пошкодженою ізоляцією;

- не тягнути за мережевий кабель, щоб витягти вилку з розетки;

- не закривати меблями, різноманітним інвентарем вимикачі, штепсельні розетки;

- не підключати одночасно декілька потужних електроприладів до однієї розетки, що може викликати надмірне нагрівання провідників, руйнування їхньої ізоляції, розплавлення і загоряння полімерних матеріалів;

- не залишати включені електроприлади без нагляду;

- не допускати потрапляння всередину електроприладів крізь вентиляційні отвори рідин або металевих предметів, а також не закривати їх та підтримувати в належній чистоті, щоб уникнути перегрівання та займання приладу;

- не ставити на електроприлади матеріали, які можуть під дією теплоти, що виділяється, спалахнути (канцелярські товари, сувенірну продукцію тощо).

Вимоги безпеки при надзвичайних ситуаціях:

1) При раптовому припиненні подачі електричної енергії вимкнути всі пристрої ПК в такій послідовності: периферійні пристрої, ВДТ, системний блок, стабілізатор (або блок безперервного живлення). Витягнути вилки з розеток. При наявності ознак горіння (дим, запах горілого) необхідно вимкнути всі пристрої ПК, знайти місце загоряння і виконати всі можливі заходи для його ліквідації, попередивши терміново про це керівництво. У випадку виникнення пожежі негайно попередити про це пожежну частину та керівництво, виконати усі можливі заходи по евакуації людей з приміщення і розпочати гасіння пожежі первинними засобами пожежогасіння.

2) При замиканні, перевантаженні електричного струму на електричному обладнанні, внаслідок ураження грозової блискавки та ймовірної небезпеки ураженням електричним струмом, приймають наступне:

- попередження замикання здійснюється правильним вибором, монтажем експлуатації мереж;

- застосування захисту схем у вигляді швидкодіючих реле, а також вимикачів, плавких запобіжників, автоматичних вимикачів.

а) У випадку дотику до корпусу та інших струмоведучих частин електроустановки, що опинилися під напругою використовують захисне заземлення - зниження до безпечних значень напруги дотику і кроку, обумовлених замиканням на корпус та ін. Це досягається

шляхом, зменшення потенціалу заземленого обладнання (за рахунок підйому потенціалу підстави, на якому стоїть людина, до значення, близького до значення потенціалу заземленого обладнання) та відключення від загальної електромережі ураженого обладнання.

б) У випадку замикання фази на корпус, зниження ізоляції мережі нижче визначеної межі і, нарешті, в разі дотику людини безпосередньо до частини, що знаходиться під напругою. Основними елементами пристрою захисного відключення є прилад захисного відключення і автоматичний вимикач.

Прилад захисного відключення - сукупність окремих елементів, які приймають вхідну величину, реагує на її зміни і при заданому значенні дають сигнал на її відключення вимикача:

- датчику - вхідна ланка пристрою, що сприймають впливу ззовні і здійснюють перетворення цього впливу в відповідний сигнал;

- підсилювача, призначений для посилення сигналу датчика, якщо він виявляється недостатньо потужним;

- ланцюгів контролю, службовці періодичної перевірки справності захисного відключення;

- допоміжних елементів - сигнальні лампи і вимірювальні прилади, що характеризують стан електроустановки.

Автоматичний вимикач - апарат, призначений для включення і вимикання від ланцюгів під навантаженням і при коротких замиканнях. Він повинен включати ланцюг автоматично при надходженні сигналу від приладу захисного відключення.

Також застосовують різні **електричні захисні засоби від ураження струмом**:

а) Ізолюючі - ізолюють людини від струмоведучих або заземлених частин, а так-же від землі. Вони діляться на основні та додаткові.

б) Основні - володіють ізоляцією, здатної довго витримувати робоче напругу електроустановки і тому ними дозволяється стосуватися струмоведучих частин, знаходячи-трудящих під напругою. До них відносяться: в електроустановках до 1000 Вт - діелектричної рукавички, ізолюючі штанги, ізолюючі і електровимірювальні кліщі і т.д .; понад 1000Вт - ізолюючі штанги, і електровимірювальні кліщі, а також кошти для ремонтних робіт під напругою понад 1000Вт.

в) Запобіжні - володіють ізоляцією нездатною витримати робоча напруга електроустановки, і тому вони не можуть самостійно захищати людину від ураження струмом під цим напругою. Їх значення - посилити захисні дії основних і ізолюючих засобів, разом з якими вони повинні застосовуватися, при чому при використання

основних захисних засобів достатньо застосування одного запобіжного захисного засобу. До запобіжних відносяться засоби в електроустановках до 1000Вт - діелектричні калоші килимки, а також ізолюючі підставки.

Розрахунок захисного заземлення (забезпечення електробезпеки будівлі).

Загальний опір захисного заземлення визначається за формулою:

$$R_{ззп} = \frac{R_з \cdot R_п}{R_п \cdot n \cdot \eta_з + R_з \cdot \eta_п}, \quad (4.3)$$

де Rз - опір заземлення, якими когут бать труби, опори, кути і т.п., Ом;

Rш - опір опори, яке з'єднує заземлювачі, Ом;

п - кількість заземлювачів;

ηз - коефіцієнт екранування заземлювача; приймається в межах 0,2 ÷ 0,9; ηз = 0,7

ηш - коефіцієнт екранування сполучної стійки; приймається в межах 0,1 ÷ 0,7; ηш = 0,5;

Опір заземлення визначається за формулою:

$$R_з = \frac{\rho}{2\pi \cdot l} \cdot \left(\ln \frac{2 \cdot l}{d} + \frac{1}{2} \ln \frac{4 \cdot t + l}{4 \cdot t - l} \right), \quad (4.4)$$

де ρ - питомий опір ґрунту, залежить від типу грунту, Ом·м;

для піску - А00 ÷ 700 Ом·м; приймаємо ρ = А00 Ом·м;

l - довжина заземлювача, м; для труб - 2-3 м; l= 3 м;

d - діаметр заземлювача, м; для труб - 0,03-0,05 м; d = 0,05 м;

t - відстань від середини забитого в ґрунт заземлювача до рівня землі, м; t = 2 м.

$$R_з = \frac{400}{2 \cdot 3{,}14 \cdot 3} \left(\ln \frac{2 \cdot 3}{0{,}05} + \frac{1}{2} \ln \frac{4 \cdot 2 + 3}{4 \cdot 2 - 3} \right) = 110, \text{ Ом}$$

Опір смуги, що з'єднує заземлювачі, визначається за формулою:

$$R_ш = \frac{\rho}{2\pi \cdot L} \cdot \ln \frac{2 \cdot L^2}{b \cdot t^1}, \quad (4.5)$$

де L - довжина смуги, що з'єднує заземлювачі (м) і приблизно дорівнює периметру будівлі: $П_{буд.} = 42 \cdot 2 + 38 \cdot 2 = 160$ м; L = 160 м;

b - ширина смуги, м; b = 0,03 м;

t_1 - глибина заземлення від рівня землі, м; $t_1 = 0,5$ м.

$$R_n = \frac{400}{2 \cdot 3,14 \cdot 160} \cdot \ln \frac{2 \cdot 160^2}{0,03 \cdot 0,5} = 5,99, \text{ Ом}$$

Кількість заземлювачів захисного заземлення визначається за формулою:

$$n = \frac{2 \cdot R_з}{4 \cdot \eta_з}, \tag{4.6}$$

де 4 - допустимий загальний опір, Ом;

2 - коефіцієнт сезонності.

Визначаємо загальний опір захисного заземлення:

$$R_{ззп} = \frac{110 \cdot 5,99}{5,99 \cdot 79 \cdot 0,7 + 110 \cdot 0,5} = 1,7 \text{ Ом}$$

Висновок: дане захисне заземлення буде забезпечувати електробезпеку будівлі, так як виконується умова: $R_{ззп} < 4$ Ом.

3) При виникненню пожеж при роботі на ПЕОМ від таких можливими джерел запалювання як:

– іскри і дуги коротких замикань;

– перегрів провідників, резисторів та інших радіодеталей ПЕОМ, від тривалої перевантаження та наявність перехідного опору;

– іскри при розмиканні і розмиканні ланцюгів;

– розряди статичної електрики;

– необережному поводженню з вогнем, а також вибухи газо-повітряних і паро-повітряних сумішей.

Важливу увагу слід звернути на пожежну безпеку підприємства в цілому і окремих його приміщень. В приміщеннях не повинно накопичуватися сміття, непотрібний папір, мотлох та ін. речі, які не використовуються у виробничому процесі. Наявний вільний аварійний вихід за межі приміщення в разі пожежі, бути передбачені вогнегасники. Вони

повинні бути в робочому стані і перевірятися згідно з нормами. У приміщеннях повинна бути пожежна сигналізація, вогнегасник. У разі виникнення пожежі необхідно повідомити в найближчу пожежну частину, убезпечити інших працівників і по можливості прийняти кроки по запобіганню можливих наслідків та усуненню пожежі.

4.8 Охорона навколишнього природного середовища

4.8.1 Загальні дані з охорони навколишнього природного середовища

Діяльність за темою магістерської роботи, процес виконання якої впливає на навколишнє природнє середовище і регламентується нормами діючого законодавства: Законом України «Про охорону навколишнього природного середовища», Законом України «Про забезпечення санітарного та епідемічного благополуччя населення», Законом України «Про відходи», Законом України «Про охорону атмосферного повітря», Законом України «Про захист населення і територій від надзвичайних ситуацій техногенного та природного характеру», Водний кодекс України.

Основним екологічним аспектом в процесі діяльності за даними спеціальностями є процеси впливу на атмосферне повітря та процеси поводження з відходами, які утворюються, збираються, розміщуються, передаються на знешкодження, утилізацію, тощо в ІТ галузі.

Вплив на атмосферне повітря при нормальних умовах праці не оказує, бо не має в приміщенні сканерів, принтерів та інших джерел викиду забруднюючих речовин в повітря робочої зони.

В процесі діяльності аналізу математичних методів оцінки надійності БСМ і програмних продуктів для імітаційного моделювання БСМ, вибіру найбільш підходящої системи для оцінки працездатності БСМ та оцінки впливу перешкод і потужності передачі радіосигналу на працездатність БСМ.виникають процеси поводження з відходами ІТ галузі. Нижче надано перелік відходів, що утворюються в процесі роботи:

— Відпрацьовані люмінесцентні лампи - I клас небезпеки
— Батарейки та акумулятори (малі) -III клас небезпеки
— Акумулятор для джерел безперебійного живлення -III клас небезпеки
— Змінні носії інформації - IV клас небезпеки
— Відходи друкуючих пристроїв - IV клас небезпеки
— Макулатура - IV клас небезпеки
— Матеріали пакувальні пластмасові забруднені (ємності з-під тонеру, фарби, інш.) - IV клас небезпеки

— Побутові відходи - IV клас небезпеки

4.8.2 Вимоги до збору, пакування та розміщення відходів ІТ галузі

Наводяться вимоги зберігання виявлених за своєю роботою відходів відповідно до вимог Державних санітарних правил і норм ДСанПіН 2.2.7.029.

Відходи в міру їх накопичення збирають у тару, відповідну класу небезпеки, з дотриманням правил безпеки, після чого доставляють до місця тимчасового зберігання відходів відповідно до затвердженої схеми їх розміщення Зазначені для зберігання відходів місця чи об'єкти повинні використовуватися лише для заявлених відходів.

Не допускається зберігання відходів у невстановлених схемою місцях, а також перевищення норм тимчасового зберігання відходів.

Способи тимчасового зберігання відходів визначаються видом, агрегатним станом і класом небезпеки відходів:

- Відходи I класу небезпеки зберігаються в герметичній тарі (сталеві бочки, контейнери). У міру наповнення тару з відходами закривають герметично сталевий кришкою;

- Відходи II класу небезпеки в залежності від агрегатного стану зберігаються в поліетиленових мішках, бочках, сховищах та інших видах тари, яка запобігає поширенню шкідливих речовин;

- Відходи III класу небезпеки зберігаються в тарі, яка забезпечує локалізацію зберігання, дозволяє виконувати вантажно-розвантажувальні і транспортні роботи і виключає поширення в ОС шкідливих речовин;

- Відходи IV класу небезпеки можуть зберігатися відкрито на промисловому майданчику у вигляді конусоподібної купи, звідки їх автонавантажувачем перевантажують у самоскид і доставляють на місце утилізації або захоронення;

- В разі тимчасового зберігання відходів у стаціонарних складах або промислових приміщеннях повинні бути забезпечені санітарно-гігієнічними етичні вимоги до повітря робочої зони згідно з ГОСТ 12.1.005.

Не допускається змішування відходів різних видів і класів небезпеки з будівельними і побутовими відходами, відходами дерев'яної, металевої, синтетичної тари, відходами текстильних матеріалів (старий спецодяг, ганчірки) і ін.

Проведення заготовки, здачі, переробки та реалізації металобрухту встановлені окремо Законом України «Про металобрухт».

Особливий контроль наділяється збору і зберіганню відпрацьованих ртутьвмісних ламп (енергоощадних) як відходам І класу небезпеки, що збираються і обов'язково передаються на утилізацію підприємствам, що мають ліцензію на поводження з такими небезпечними відходами.

Всі відходи, що утворюються в процесі діяльності/роботи, підлягають обліку.

Під час роботи з відходами (прибирання виробничих приміщень, збір і сортування, навантаження, транспортування, розвантаження та ін.) працівники та обслуговуючий персонал підприємства повинні бути забезпечені засобами індивідуального захисту та дотримуватися вимог інструкцій з охорони праці, що діють на підприємстві.

Наведено перелік деяких відходів, які передаються на утилізацію організаціям, які мають ліцензію на поводження з відходами як вторинної сировини:

- лом і кускові відходи міді, бронзи, латуні, алюмінію, свинцю;
- брухт чорних металів;
- макулатура;
- склобій;
- матеріали текстильні вторинні;
- відходи деревини кускові;
- відпрацьовані фільтрувальні засоби індивідуального захисту;
- відпрацьовані вогнегасники;
- матеріали пакувальні вторинні.

Відвантаження таких відходів здійснюється відповідно до договору (контракту).

Побутові та будівельні відходи вивозяться на полігон твердих побутових відходів міста, також відповідно до договору з комунальним дорожньо-експлуатаційним управлінням.

Особи, винні в порушенні встановленого порядку поводження з відходами (порушення правил обліку відходів, самовільне складування і видалення відходів, передача відходів в інші підприємства/організації з порушенням встановлених правил), згідно законодавства несуть дисциплінарну, адміністративну або кримінальну відповідальність.

4.8.3 Визначення впливу та заходів щодо поводження з відходами ІТ галузі

З метою визначення та прогнозування впливу відходів на навколишнє середовище, своєчасного виявлення негативних наслідків, їх запобігання відповідно до Закону України «Про відходи» повинен здійснюватися моніторинг місць утворення, зберігання, і

видалення відходів. Відомості про місце утворення та місце розташування відходів зазначаються на «План схемі місці розміщення відходів організації/виробництва» та наводяться у таблиці В.2 в додатку В, а Відомості про склад і властивості відходів, що утворюються, а також ступінь їх небезпечності для навколишнього природного середовища та здоров'я людини у табл. В.3 додатку В.

Висновки до розділу

В результаті проведеної роботи було зроблено аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник. Було визначено параметри і певні характеристики приміщення для роботи над запропонованим проектом, описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для робітника. Приведені рекомендації щодо організації робочого місця, а також важлива інформація щодо пожежної та електробезпеки. Була наведена схема, розміри приміщення та наведено значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці робітника, а також – наведені інструкції з охорони праці, техніки безпеки при роботі на комп’ютері.

А також визначені основні екологічні аспекти впливу на навколишнє природнє середовище та зазначені заходи щодо поводження з ними.

ВИСНОВКИ

Широка популярність мультисервісних мереж зв'язку диктує необхідність забезпечення якості обслуговування. Особа, яка приймає рішення про якість обслуговування в МСМ, а саме мережевий адміністратор, повинна 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, джиттер, 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 трафіку 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 параметри, 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 широкомовну розсилку 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 лежить розроблена нечітка модель оцінки якості доставки пакетів в МСМ. 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 [электронный ресурс] // Cisko system inc. - Режим доступа: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html. - Дата доступа: 20.05.2016. – Загл. с экрана.

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. - Київ, 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. – Харків, 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 информатика : науч.-техн. журн. – Х. : Изд-во ХНУРЭ, 2011. – Вып. 2. – С. 35-40.

10. Спирина Е. И. Метод маршрутизации, обеспечивающий повышение пропускной способности IP сетей в условиях внутрисистемных помех [электронный ресурс] / Е. И. Спирина, С. В. Козлов // 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.- Минск, 2015. - № 2 (130). - pp. 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) [электронный ресурс] / A. Schulzrinne, A. Rao, R. Lanphier // 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 pp.

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. Яновский Г. Г. Качество обслуживания в сетях IP / Г. Г. Яновский // Вестник связи. – 2008. – №1.− С. 65-74.

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

21. МСЭ-Т Recommendation Y.1540. IP Packet Transfer and Availability Performance Parameters // December 2002.

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

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

24. Рекомендация МСЭ-Т Е.800. Определение терминов, относящихся к качеству обслуживания [электронный ресурс] // Международный союз электросвязи. - Режим доступа: www.itu.int. − Дата доступа: 02.03.16. – Загл. с экрана.

25. 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: 02.03.16. – Загл. с экрана.

26. Рекомендация МСЭ-Т G.1010. Категории качества обслуживания конечного пользователя [электронный ресурс] // Международный союз электросвязи. − Режим доступа: www.itu.int . − Дата доступа: 02.03.16. – Загл. с экрана.

27. 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: 02.03.16. – Загл. с экрана.

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

29. 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.

30. 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 pp.

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

32. Джарратано, Д. Экспертные системы: принципы разработки и программирования, 4-е издание: пер. с англ. / Д. Джарратано, Г. Райли. – М.: Вильямс, 2007. – 1152 с.

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

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

35. Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці (НПАОП 0.00-4.12-05) [Електронний ресурс] / Законодавство України - Режим доступу: www.URL: http://zakon0.rada.gov.ua/laws/show/z0231-05 - 21.12.2017 р.

36. Типове положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України (НАПБ Б.02.005-2003) [Електронний ресурс] / Законодавство України - Режим доступу: www.URL: http://zakon0.rada.gov.ua/laws/show/z1148-03 - 21.12.2017 р.

37. Санітарні норми мікроклімату виробничих приміщень (ДСН 3.3.6.042.-99) [Електронний ресурс] / Законы Украины - Режим доступу: www.URL: http://uazakon.com/documents/date_42/pg_ikcfxj.htm - 22.12.2017 р.

38. Правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин (ДСанПіН 3.3.2.007-98) [Електронний ресурс] / Педрада - Режим доступу: www.URL: http://zakon.pedrada.com.ua/regulations/10637/478672/ - 22.12.2017 р.

39. Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою (НАПБ Б.03.002-2007) [Електронний ресурс] / ДНАОП - Режим доступу: www.URL: https://dnaop.com/html/32980/doc-НАПБ_Б.03.002.-2007 - 23.12.2017 р.

40. Санітарні норми мікроклімату виробничих приміщень (ДСН 3.3.6.042-99) [Електронний ресурс] / UAinfo - Режим доступу: www.URL: http://ua-info.biz/legal/basetp/ua-zmptae.htm - 23.12.2017 р.

41. Санітарні норми виробничого шуму, ультразвуку та інфразвуку (ДСН 3.3.6.037-99) [Електронний ресурс] / Нормативно-директивні документи МОЗ України - Режим доступу: www.URL: http://mozdocs.kiev.ua/view.php?id=1789 - 23.12.2017 р.

ДОДАТОК А

Опис бази знань СППР

ДП1 - «результативність», ДП2 - «продуктивність», ДП3 - «безпека», ДП4 - «відповідність очікуванням», РД - якість ПЗ.

У розгорнутому вигляді ці ПП приймають такий вигляд:

1. If (ДП1 is Н) and (ДП2 is Н) and (ДП3 is Н) and (ДП4 is Н) then (РД is ОН)
2. If (ДП1 is Н) and (ДП2 is Н) and (ДП3 is Н) and (ДП4 is С) then (РД is Н)
3. If (ДП1 is Н) and (ДП2 is Н) and (ДП3 is С) and (ДП4 is Н) then (РД is Н)
4. If (ДП1 is Н) and (ДП2 is С) and (ДП3 is Н) and (ДП4 is Н) then (РД is Н)
5. If (ДП1 is С) and (ДП2 is С) and (ДП3 is Н) and (ДП4 is Н) then (РД is Н)
6. If (ДП1 is Н) and (ДП2 is Н) and (ДП3 is Н) and (ДП4 is В) then (РД is Н)
7. If (ДП1 is Н) and (ДП2 is Н) and (ДП3 is В) and (ДП4 is Н) then (РД is Н)
8. If (ДП1 is Н) and (ДП2 is В) and (ДП3 is Н) and (ДП4 is Н) then (РД is Н)
9. If (ДП1 is В) and (ДП2 is Н) and (ДП3 is Н) and (ДП4 is Н) then (РД is Н)
10. If (ДП1 is Н) and (ДП2 is Н) and (ДП3 is С) and (ДП4 is С) then (РД is Н)
11. If (ДП1 is Н) and (ДП2 is С) and (ДП3 is Н) and (ДП4 is С) then (РД is Н)
12. If (ДП1 is Н) and (ДП2 is С) and (ДП3 is С) and (ДП4 is Н) then (РД is Н)
13. If (ДП1 is С) and (ДП2 is Н) and (ДП3 is Н) and (ДП4 is С) then (РД is Н)
14. If (ДП1 is С) and (ДП2 is Н) and (ДП3 is С) and (ДП4 is Н) then (РД is Н)
15. If (ДП1 is С) and (ДП2 is С) and (ДП3 is Н) and (ДП4 is Н) then (РД is Н)
16. If (ДП1 is С) and (ДП2 is С) and (ДП3 is С) then (РД is С)
17. If (ДП1 is С) and (ДП2 is С) and (ДП4 is С) then (РД is С)
18. If (ДП1 is С) and (ДП3 is С) and (ДП4 is С) then (РД is С)
19. If (ДП2 is С) and (ДП3 is С) and (ДП4 is С) then (РД is С)
20. If (ДП1 is Н) and (ДП2 is Н) and (ДП3 is С) and (ДП4 is В) then (РД is С)
21. If (ДП1 is Н) and (ДП2 is Н) and (ДП3 is В) and (ДП4 is С) then (РД is С)
22. If (ДП1 is Н) and (ДП2 is С) and (ДП3 is Н) and (ДП4 is В) then (РД is С)
23. If (ДП1 is Н) and (ДП2 is С) and (ДП3 is В) and (ДП4 is Н) then (РД is С)
24. If (ДП1 is Н) and (ДП2 is В) and (ДП3 is Н) and (ДП4 is С) then (РД is С)
25. If (ДП1 is Н) and (ДП2 is В) and (ДП3 is С) and (ДП4 is Н) then (РД is С)
26. If (ДП1 is С) and (ДП2 is Н) and (ДП3 is Н) and (ДП4 is В) then (РД is С)
27. If (ДП1 is С) and (ДП2 is Н) and (ДП3 is В) and (ДП4 is Н) then (РД is С)
28. If (ДП1 is С) and (ДП2 is В) and (ДП3 is Н) and (ДП4 is Н) then (РД is С)
29. If (ДП1 is В) and (ДП2 is Н) and (ДП3 is Н) and (ДП4 is С) then (РД is С)
30. If (ДП1 is В) and (ДП2 is Н) and (ДП3 is С) and (ДП4 is Н) then (РД is С)
31. If (ДП1 is В) and (ДП2 is С) and (ДП3 is Н) and (ДП4 is Н) then (РД is С)
32. If (ДП1 is Н) and (ДП2 is Н) and (ДП3 is В) and (ДП4 is В) then (РД is С)
33. If (ДП1 is Н) and (ДП2 is В) and (ДП3 is Н) and (ДП4 is В) then (РД is С)
34. If (ДП1 is Н) and (ДП2 is В) and (ДП3 is В) and (ДП4 is Н) then (РД is С)
35. If (ДП1 is В) and (ДП2 is Н) and (ДП3 is Н) and (ДП4 is В) then (РД is С)
36. If (ДП1 is В) and (ДП2 is Н) and (ДП3 is В) and (ДП4 is Н) then (РД is С)
37. If (ДП1 is В) and (ДП2 is В) and (ДП3 is Н) and (ДП4 is Н) then (РД is С)
38. If (ДП1 is Н) and (ДП2 is С) and (ДП3 is С) and (ДП4 is В) then (РД is С)
39. If (ДП1 is Н) and (ДП2 is С) and (ДП3 is В) and (ДП4 is С) then (РД is С)
40. If (ДП1 is Н) and (ДП2 is В) and (ДП3 is С) and (ДП4 is С) then (РД is С)
41. If (ДП1 is С) and (ДП2 is Н) and (ДП3 is С) and (ДП4 is В) then (РД is С)
42. If (ДП1 is С) and (ДП2 is Н) and (ДП3 is В) and (ДП4 is С) then (РД is С)
43. If (ДП1 is С) and (ДП2 is С) and (ДП3 is Н) and (ДП4 is В) then (РД is С)

44. If (ДП1 is С) and (ДП2 is С) and (ДП3 is В) and (ДП4 is Н) then (РД is С)
45. If (ДП1 is С) and (ДП2 is В) and (ДП3 is Н) and (ДП4 is С) then (РД is С)
46. If (ДП1 is С) and (ДП2 is В) and (ДП3 is С) and (ДП4 is Н) then (РД is С)
47. If (ДП1 is В) and (ДП2 is Н) and (ДП3 is С) and (ДП4 is С) then (РД is С)
48. If (ДП1 is В) and (ДП2 is С) and (ДП3 is Н) and (ДП4 is С) then (РД is С)
49. If (ДП1 is В) and (ДП2 is С) and (ДП3 is С) and (ДП4 is Н) then (РД is С)
50. If (ДП1 is Н) and (ДП2 is С) and (ДП3 is В) and (ДП4 is В) then (РД is С)
51. If (ДП1 is Н) and (ДП2 is В) and (ДП3 is С) and (ДП4 is В) then (РД is С)
52. If (ДП1 is Н) and (ДП2 is В) and (ДП3 is В) and (ДП4 is С) then (РД is С)
53. If (ДП1 is С) and (ДП2 is Н) and (ДП3 is В) and (ДП4 is В) then (РД is С)
54. If (ДП1 is С) and (ДП2 is В) and (ДП3 is Н) and (ДП4 is В) then (РД is С)
55. If (ДП1 is С) and (ДП2 is В) and (ДП3 is В) and (ДП4 is Н) then (РД is С)
56. If (ДП1 is В) and (ДП2 is Н) and (ДП3 is С) and (ДП4 is В) then (РД is С)
57. If (ДП1 is В) and (ДП2 is Н) and (ДП3 is В) and (ДП4 is С) then (РД is С)
58. If (ДП1 is В) and (ДП2 is С) and (ДП3 is Н) and (ДП4 is В) then (РД is С)
59. If (ДП1 is В) and (ДП2 is С) and (ДП3 is В) and (ДП4 is Н) then (РД is С)
60. If (ДП1 is В) and (ДП2 is В) and (ДП3 is Н) and (ДП4 is С) then (РД is С)
61. If (ДП1 is В) and (ДП2 is В) and (ДП3 is С) and (ДП4 is Н) then (РД is С)
62. If (ДП1 is В) and (ДП2 is В) and (ДП3 is В) and (ДП4 is С) then (РД is Д)
63. If (ДП1 is В) and (ДП2 is В) and (ДП3 is С) and (ДП4 is В) then (РД is Д)
64. If (ДП1 is В) and (ДП2 is С) and (ДП3 is В) and (ДП4 is В) then (РД is Д)
65. If (ДП1 is С) and (ДП2 is В) and (ДП3 is В) and (ДП4 is В) then (РД is Д)
66. If (ДП1 is В) and (ДП2 is В) and (ДП3 is В) and (ДП4 is Н) then (РД is Д)
67. If (ДП1 is В) and (ДП2 is В) and (ДП3 is Н) and (ДП4 is В) then (РД is Д)
68. If (ДП1 is В) and (ДП2 is Н) and (ДП3 is В) and (ДП4 is В) then (РД is Д)
69. If (ДП1 is Н) and (ДП2 is В) and (ДП3 is В) and (ДП4 is В) then (РД is Д)
70. If (ДП1 is С) and (ДП2 is С) and (ДП3 is В) and (ДП4 is В) then (РД is Д)
71. If (ДП1 is С) and (ДП2 is В) and (ДП3 is С) and (ДП4 is В) then (РД is Д)
72. If (ДП1 is С) and (ДП2 is В) and (ДП3 is В) and (ДП4 is С) then (РД is Д)
73. If (ДП1 is В) and (ДП2 is С) and (ДП3 is С) and (ДП4 is В) then (РД is Д)
74. If (ДП1 is В) and (ДП2 is С) and (ДП3 is В) and ДП4 is С) then (РД is Д)
75. If (ДП1 is В) and (ДП2 is В) and (ДП3 is С) and (ДП4 is С) then (РД is Д)
76. If (ДП1 is В) and (ДП2 is В) and (ДП3 is В) and (ДП4 is В) then (РД is В)

ДОДАТОК Б

Перелік графічних матеріалів

Рисунок Б.1 - Слайд №1

Рисунок Б.2 - Слайд №2

Характеристики QoS в мультисервисной сети. Рекомендация МСЭ-Т Y.1540

Производительность сети		
Надежность сети		
Параметры доставки пакетов	Задержка доставки пакетов	
	Вариация задержки пакета (джиттер)	
	Коэффициент потери пакетов	
	Коэффициент ошибок пакетов	

Сетевые характеристики	Классы QoS					
	0	1	2	3	4	5
Задержка доставки пакета IP, IPTD	100 мс	400 мс	100 мс	400 мс	1 с	Н
Вариация задержки пакета IP, IPDV	50 мс	50 мс	Н	Н	Н	Н
Коэффициент потери пакетов IP, IPLR	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	$1x10^{-3}$	Н
Коэффициент ошибок пакетов IP, IPER	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	$1x10^{-4}$	Н

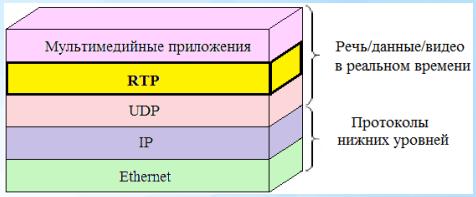
- **класс 0** – приложения реального времени, характеризуемые высоким уровнем интерактивности (VoIP, видеоконференции);
- **класс 1** – приложения реального времени, интерактивные (VoIP, видеоконференции);
- **класс 2** – транзакции данных, характеризуемые высоким уровнем интерактивности (например, сигнализация);
- **класс 3** – транзакции данных, интерактивные;
- **класс 4** – приложения, допускающие низкий уровень потерь (короткие транзакции, потоковое видео);
- **класс 5** – традиционные применения сетей IP.

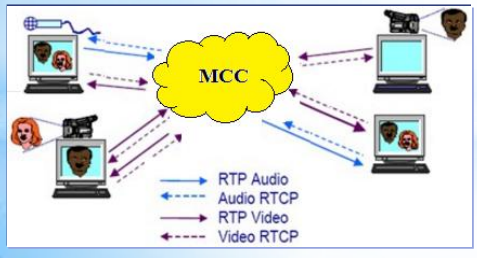
4

Рисунок Б.3 - Слайд №3

Протокол RTP/RTCP

К наиболее требовательному виду трафика относится **трафик реального времени** (*IP-телефония и видеоконференцсвязь, процессы управления, игры-online и т.д.*). Передача такого трафика была бы невозможна без использования специальных протоколов **Real-time Transport Protocol (RTP)**. На рисунке представлены уровни протокола RTP/UDP/IP.





На практике протокол RTP не отделим от протокола **RTCP (Real-Time Transport Control Protocol)**. Благодаря многоадресной природе протоколов RTP/RTCP, все участники сеанса связи получают отчеты обратной связи остальных участников и, таким образом, каждый из них может оценить скорость передачи данных, уровень утерянных пакетов, задержки и т.д.

При этом стандартом RFC 3550 установлено, что часть полосы пропускания, выделяемая для RTCP, не может превышать 5%.

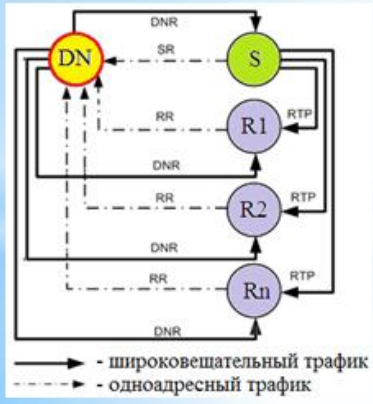
5

Рисунок Б.4 - Слайд №4

Расширенная модель обратной связи RTCP

Если доля служебного широковещательного трафика **превышает 5%**, то во избежание широковещательного шторма **RTCP пакеты отбрасываются**. Последнее хотя и не приводит к непосредственному ухудшению качества передачи данных, однако ведет к потере служебной информации, которая может стать полезной для улучшения качества передачи IP-пакетов.

Для сокращения и концентрации служебного трафика была использована **модель обратной связи RTCP с диагностическим узлом (ДУ)**.



На основании анализа RTCP-отчетов, сконцентрированных на ДУ, администратор может принять решение о том, какие мероприятия необходимо провести для улучшения качества связи.

В качестве инструмента предлагается использовать систему поддержки принятия решения (СППР).

6

Рисунок Б.5 - Слайд №5

Цель и задачи исследования

Цель исследования – разработка системы поддержки принятия решения при оценке качества доставки пакетов в МСС путем концентрации служебного трафика (RTCP-пакетов) на одном диагностическом узле.

Задачи исследования:

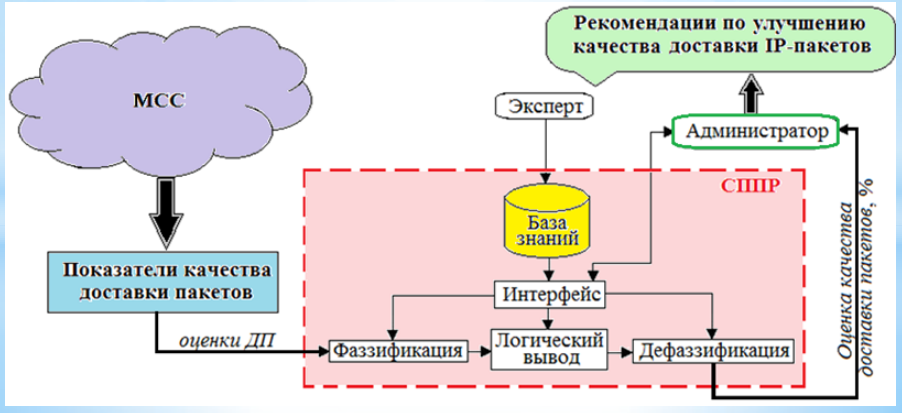
- Проанализировать стандарты по обеспечению качества обслуживания в МСС, выбрать наиболее значимые параметры, влияющие на QoS.
- Исследовать способы передачи трафика реального времени, а также методы обеспечения QoS.
- Применить расширенную модель обратной связи RTCP с вводом диагностического узла для сокращения объема и концентрации RTCP-трафика.
- Создать нечеткую модель оценки качества доставки пакетов в МСС.
- Спроектировать структуру системы поддержки принятия решения при оценке качества доставки пакетов.
- Выполнить анализ эффективности нечеткой модели оценки качества доставки пакетов в МСС.
- Выполнить эксперимент по настройки сервера IP-телефонии Asterisk для его дальнейшего использования в качестве диагностического узла.

Рисунок Б.6 - Слайд №6

Система поддержки принятия решения о качестве доставки IP-пакетов

Администратору зачастую приходиться работать с нечеткой информацией, представленной пользователями сети в словесной форме (*например, разговор по IP-телефону «прерывается», передача файла «зависает», приходят «битые» файлы*).

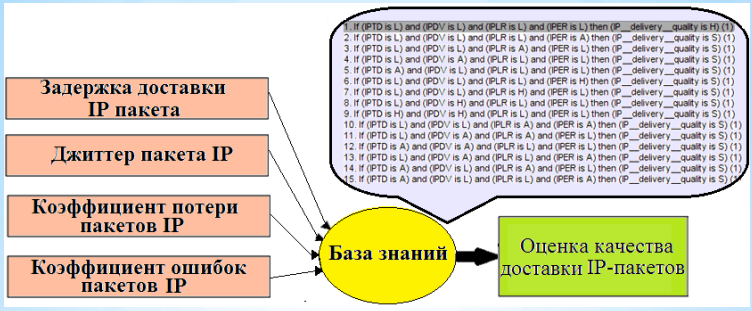
Таким образом, в качестве инструмента при принятии решения о качестве доставки пакетов в МСС администратору предлагается использовать **СППР**, в основе которой лежит **нечеткий алгоритм вывода**.



8

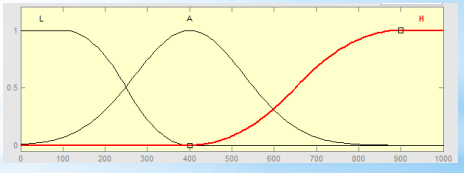
Рисунок Б.7 - Слайд №7

Нечеткая модель оценки качества доставки IP-пакетов



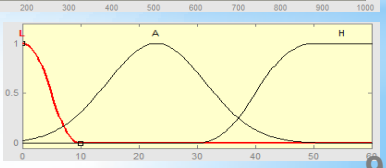
1) **IPTD** (IP packet transfer delay)

Термы		Диапазоны		Тип ФП	Параметры
H	Low	0	400	zmf	[100 400]
C	Average	100	700	gaussmf	[130 400]
B	High	500	1000	smf	[400 900]



2) **IPDV** (IP packet delay variation)

Термы		Диапазоны		Тип ФП	Параметры
H	Low	0	8	zmf	[0 10]
C	Average	5	45	gaussmf	[8.5 23]
B	High	35	60	smf	[30 50]



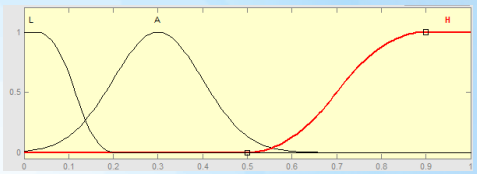
9

Рисунок Б.8 - Слайд №8

Нечеткая модель оценки качества доставки IP-пакетов

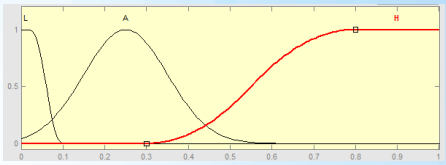
3) **IPLR** (IP packet loss ratio)

Термы		Диапазоны		Тип ФП	Параметры
H	Low	0	0.2	zmf	[3e-005 0.0002]
C	Average	0.005	0.55	gaussmf	[0.0001 0.0003]
B	High	0.5	0.001	smf	[0.0005 0.0009]



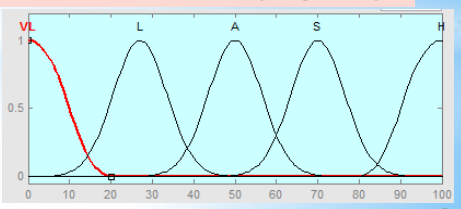
4) **IPER** (IP packet error ratio)

Термы		Диапазоны		Тип ФП	Параметры
H	Low	0	0.1	zmf	[2e-007 1e-006]
C	Average	0.2	1.4	gaussmf	[1e-006 2.5e-006]
B	High	0.3	0.0001	smf	[3e-006 8e-006]



Выходная лингвистическая переменная – IP_delivery_quality

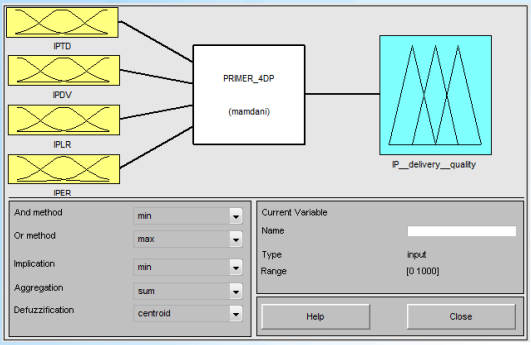
Термы		Диапазоны		Тип ФП	Параметры
OH	Very low	0	20	zmf	[0 20]
H	Low	10	40	gaussmf	[6.5 27]
C	Average	30	70	gaussmf	[6.5 50]
Д	Sufficient	50	90	gaussmf	[6.5 70]
B	High	80	100	smf	[80 100]



10

Рисунок Б.9 - Слайд №9

Анализ качества доставки пакетов в МСС с использованием Matlab (FLT)



*Ядро СППР реализовано в MatLab (**Fuzzy Logic Toolbox**), где IPTD, IPDV, IPLR, IPER – диагностические параметры. Оценка качества доставки IP-пакетов в МСС формируется на основе базы нечётких правил.*

Диагностический эксперимент по оценки качества доставки пакетов заключается в анализе служебного RTCP-трафика. Полученная трехмерная модель отражает следующую зависимость:

IP_delivery_quality = f (IPTD, IPDV, IPLR, IPER),

где ***IP_delivery_quality*** – качество доставки пакетов, %;
IPTD – задержка доставки пакета, мс;
IPDV – вариация задержки пакета (джиттер), мс;
IPLR – коэффициент потери пакетов, %;
IPER – коэффициент ошибок пакетов, %.

11

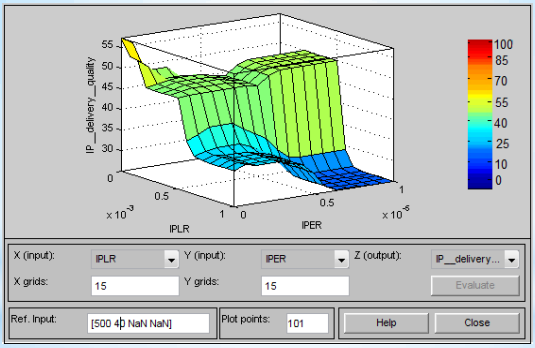
Рисунок Б.10 - Слайд №10

Эксперимент № 1

Проанализированы RTCP-пакеты, пересылаемые внутри МСС. Значения параметров доставки (оценки диагностических параметров) поступают на вход СППР (см. слайд 8), которая генерирует трехмерную модель, описывающую следующую зависимость:

IP_delivery_quality = f (500, 40, IPLR, IPER),

где IPTD = 500 (задержка = 500 мс), IPDV = 40 (джиттер = 40 мс).



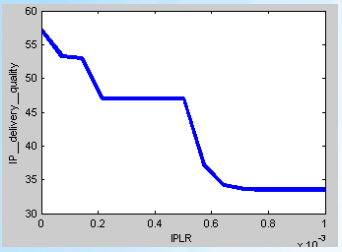
Полученный график показывает, что качество доставки пакетов не превышает 58 % (при отсутствии потерянных и ошибочных пакетов) и резко падает с ростом доли потерянных пакетов (max 10^{-3}) и при повышении доли ошибочных пакетов (max 10^{-5}).

12

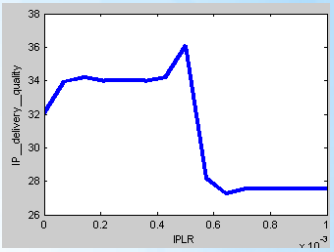
Рисунок Б.11 - Слайд №11

Эксперимент № 1 (продолжение)

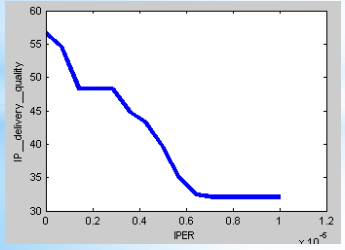
На слайде представлены кривые, которые, демонстрируя зависимости качества доставки пакетов от каждого параметра, подтверждают вышесказанное.



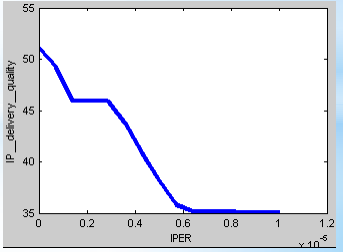
IP_delivery_quality = f (IPLR) при *IPER= 0 %*



IP_delivery_quality = f (IPLR) при *IPER=1×10^{-5}*



IP_delivery_quality = f (IPER) при *IPLR=0 %*



IP_delivery_quality = f (IPER) при *IPLR=1×10^{-3} %*

13

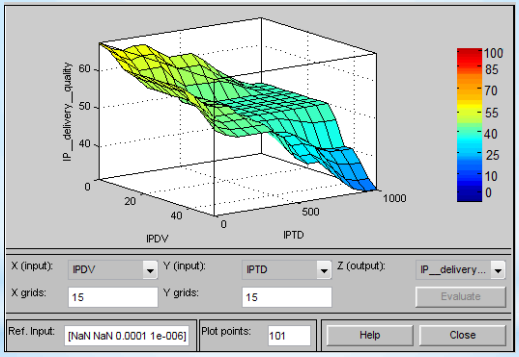
Рисунок Б.12 - Слайд №12

Эксперимент № 2

При проведении второго эксперимента проанализированы те же RTCP-пакеты, пересылаемые внутри МСС. СППР моделирует следующую зависимость:

IP_delivery_quality = f (IPTD, IPDV, 1×10^{-3}, 1×10^{-5}),

где IPLR = 1×10^{-3} (потери = 1×10^{-3} %), IPER = 1×10^{-5} (ошибки = 1×10^{-5} %).



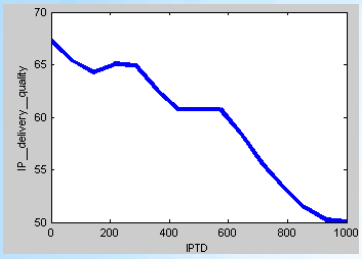
Качество доставки пакетов не превышает 68 % (при отсутствии задержки и джиттера пакетов) и умеренно уменьшается с ростом задержки IP-пакетов (max 1000 мс) и резко падает при повышении значения джиттера (max 60 мс).

14

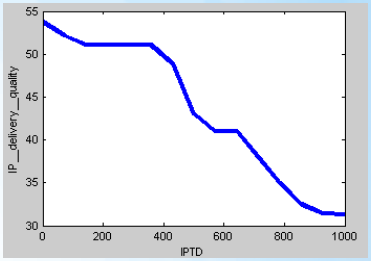
Рисунок Б.13 - Слайд №13

Эксперимент № 2 (продолжение)

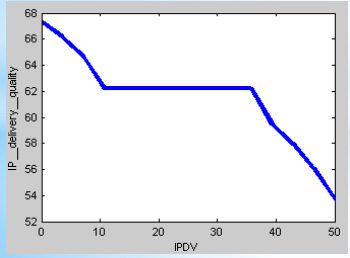
На слайде представлены кривые, которые, демонстрируя зависимости качества доставки пакетов от каждого параметра, подтверждают вышесказанное.



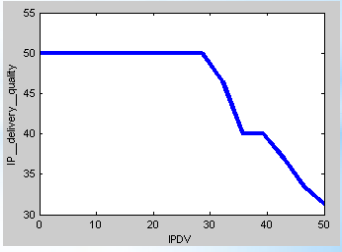
IP_delivery_quality = f (IPTD) при *IPDV=0* мс



IP_delivery_quality = f (IPTD) при *IPDV=50 мс*



IP_delivery_quality = f (IPDV) при *IPTD=0 мс*



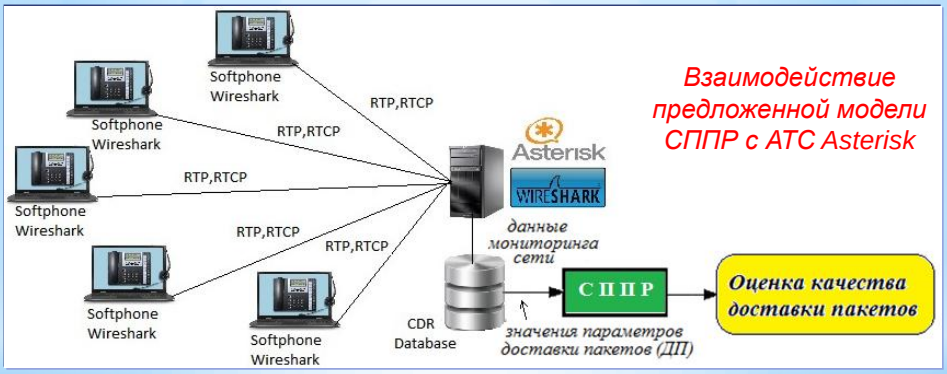
IP_delivery_quality = f (IPDV) при *IPTD=1000 мс*

15

Рисунок Б.14 - Слайд №14

Интеграция IP-сервера Asterisk в СППР

Для моделирования работы RTCP протокола с диагностическим узлом была развернута система IP-телефонии на базе IP АТС Asterisk.



Вся информация о телефонных разговорах записывается в CDR файл (Call Detail Record). Выполнить анализ CDR записей непосредственно используя систему Asterisk не представляется возможным.

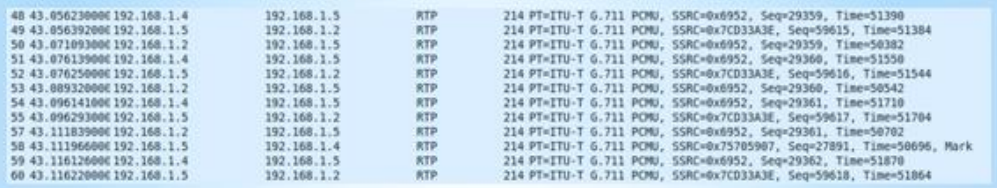
Для получения значений необходимых параметров доставки IP-пакетов воспользуемся сетевым анализатором **Wireshark**, установленным на сервере IP-телефонии Asterisk.

16

Рисунок Б.15 - Слайд №15

Анализатор протоколов Wireshark

Сетевой анализатор позволяет перехватить весь трафик, как на серверной, так и на клиентских сторонах.



RTP – *трафик*

RTCP – *трафик*

Рисунок Б.16 - Слайд №16

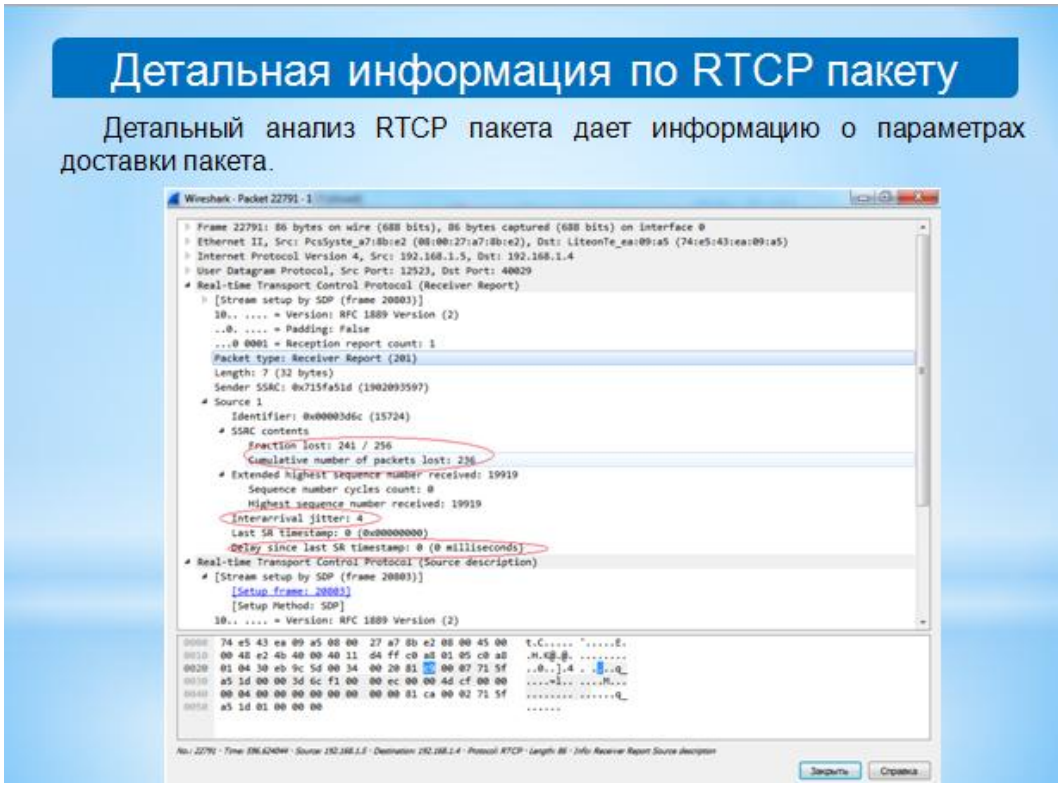


Рисунок Б.17 - Слайд №17

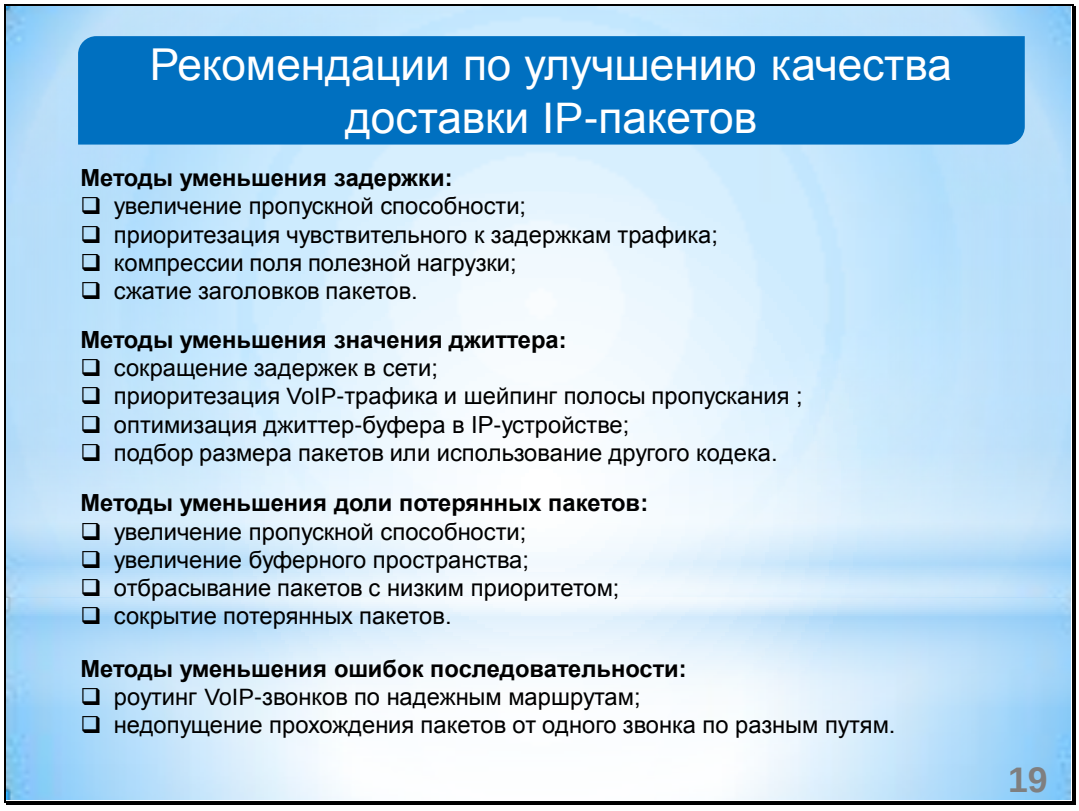


Рисунок Б.18 - Слайд №18

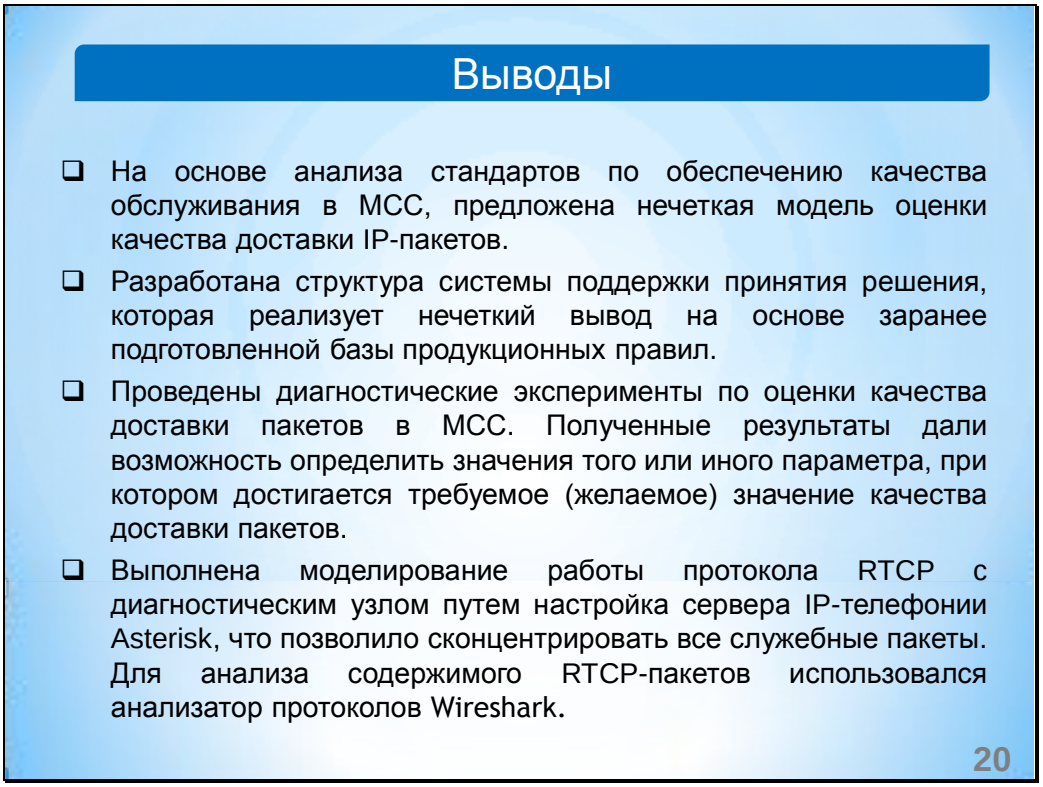


Рисунок Б.19 - Слайд №19

ДОДАТОК В

Таблиця В.1 – Аналіз небезпечних і шкідливих виробничих факторів

Небезпечні і шкідливі виробничі фактори	Джерела факторів (види робіт)	Кількісна оцінка	Нормативні документи
1	2	3	4
Фізичні			
- підвищена температура поверхонь обладнання	експлуатація ЕОМ, принтерів, сканерів чи/або серверного обладнання для роботи	2	ДСН 3.3.6.042-99
- підвищений рівень шуму на робочому місці	-//-	2	ДСН 3.3.6.037-99
- підвищений рівень вібрації	-//-	2	ДСН 3.3.6.039-99 ДСТУ ГОСТ 12.1.012-90
- підвищена або знижена вологість повітря	-//-	2	ДСН 3.3.6.042-99
- підвищена або знижена рухливість повітря	-//-	1	ДСН 3.3.6.042-99
- підвищений рівень іонізуючого випромінення в робочій зоні	-//-	2	ДСН 3.3.6.042-99 ГОСТ 12.1.006-84
- підвищений рівень електромагнітного випромінення	-//-	2	ГОСТ 12.1.006-84
- підвищений рівень напруги електричної мережі, замикання якої може відбутися через тіло людини	-//-	4	ГОСТ 12.1.030-81 ГОСТ 13109-97
- підвищена напруженість електричного поля	-//-	2	ГОСТ 12.1.006-84
- підвищена напруженість магнітного поля	-//-	2	ГОСТ 12.1.006-84
- недостатність природного світла	порушення умов праці (вимог до приміщень)	2	ДБН В.2.5-28:2015
- недостатнє освітлення робочої зони	порушення гігієнічних параметрів виробничого середовища	3	ДБН В.2.5-28:2015
- підвищена яскравість світла	порушення умов праці (організації місця праці-налагодження моніторів)	1	ДСанПіН 3.3.2.007-98

1	2	3	4
- понижена контрастність	-//-	1	ДСанПіН 3.3.2.007-98
хімічні:			
- загазованість повітря робочої зони, яка впливає на організм людини через органи дихання та надає токсичну і канцерогенну дію	від експлуатації сканерів, принтерів для роботи – O_3, оплавлення електричних і комутаційних кабелів, резисторів, конденсаторів, напівпровідникових діодів, транзисторів й інше в ЕОМ та системах кондиціонування повітря - CO, CO_2, SO_2, P_2O_5, H_2S, HCl, H, NH_3, ClF_3, F_2O_2, F_2O_3, SeO_2. SeF_6, TeF_6, $COCl_2$, SO_2F_2, інш.	3	НПАОП 40.1-1.21-98 ДБН В.2.5-67:2013 ГОСТ 12.1.005-88 ГОСТ 12.1.044-89
психофізіологічні:			
- нервово-психічна перевантаження (розумове, перенапруження аналізаторів-зорових)	- пошук інформації для постановки теми; - пошук та аналіз аналогів і літератури; - пошук наявних технологій, моделювання та аналіз алгоритмів; - виконання роботи за темою диплома, тестування; - оформлення роботи	4	НПАОП 0.00-1.28-10 ДСанПіН 3.3.2.007-98
- фізичні (статичне – сидіння)	порушення умов праці (організації місця праці- сидіння користувача,) та організації робочого часу - безпервна робота)	2	НПАОП 0.00-1.28-10 ДСанПіН 3.3.2.007-98

Таблиця В.2 - Відомості про місце утворення та місце розташування відходів

№ з/п	Код та найменування відходів за ДК -005-96	Технологічний процес або виробництво, де утворюються відходи/клас небезпеки	Місце розташування відходу, тара та її кількість, місткість, розміри у разі наявності майданчиків розташування відходів необхідно зазначити тип покриття та наявність даху)	№ на схемі (додається масштабна схема місць розміщення відходів)
1	2	3	4	5
1	7710.3.1.26 Лампи люмінесцентні, та відходи, які містять ртуть, інші зіпсовані або відпрацьовані (Відпрацьовані ртутьвмісні люмінесцентні лампи)	1	буд.84, в приміщені кладової S=100м^2, в кількість 50 од.	8401-ТХ
3	7720.3.1.01 Відходи комунальні (міські) змішані, у т.ч. сміття з урн (Побутові відходи)	4	зовнішній майданчик зберігання побутових відходів біля буд .84 S=5м² V= 2,08м³- 2од.	8401-ТХ
4	7710.3.1.01 Макулатура паперова та картонна (Макулатура)		буд .84 4 поверх кім. 412 S =5,0 м.^{2}	8401-ТХ
5	7710.3.1.03 Бій скла технічного та скловиробів, що не підлягає спеціальному обробленню. (Склобій)	4	буд .84 1 поверх кладова S=2м² V= 0,2м³- 1од.	8401-ТХ
8	7730.3.1.02 Матеріали пакувальні пластмасові зіпсовані, відпрацьовані чи забруднені (Матеріали пакувальні забруднені	4	буд.84, контейнер V=0,9м3 (3 од.)	8401-ТХ

1	2	3	4	5
9	Змінні носії інформації	4	буд. 84, кім. 412 V=0,0005 м^3	8401-ТХ
10	Відходи системних блоків (в комплекті) Пакувальні матеріали батарейки Відходи друкуючих пристроїв. Акумулятор для джерел безперебійного харчування	4	буд. 84, кім. 412 m=5,0 кг.	8401-ТХ
11	Пакувальні матеріали, що не вміщують целюлозу	4	буд. 84, кім. 412 S =5,0 м.^{2}	8401-ТХ
12	Батарейки та акумулятори (малі)	3	буд. 84, кім. 412 V=0,0005 м^3	8401-ТХ
13	Відходи друкуючих пристроїв.	4	буд. 84, кім. 412 V=1,0 м^3	8401-ТХ
14	Акумулятор для джерел безперебійного живлення	3	буд. 84, кім. 412 S =5,0 м.2	8401-ТХ

Таблиця В.3 – Відомості про склад і властивості відходів, що утворюються, а також ступінь їх небезпечності для навколишнього природного середовища та здоров'я людини

№ п/п	Назва відходу	Клас небезпеки	Хімічний (у долях відсотків складників або інших одиницях виміру) та морфологічний склад	Фізико-хімічні властивості	Негативний вплив на навколишнє середовище та здоров'я людини
	Відпрацьовані люмінесцентні лампи	I	**Ртуть** - 0,013 **Hg** **Скло** - 98,787 **(Na, K)$_2$O 2SiO$_2$** **Алюміній** - 1,2 **Al**	**Ртуть** - $T_{кип.}$ = 356,58°C $T_{плав.}$ = **- 38,87° C** **Скло** - $T_{плав.}$ = 800°C **Алюміній** - $T_{кип.}$ = 2348°C $T_{плав.}$ = 660,1°C	Негативний вплив на ОС і людини визначається його хімічним складом. **Ртуть** У природних водах міститься в концентрації 0,00003 ... 0,0028 мг / л. Являючись потужним кумулятивним отрутою, з можливою канцерогенною і мутагенною дією. Процеси самоочищення водойм порушують концентрація ртуті понад 0,018 мг / л, порогова концентрація ртуті за впливом на санітарний режим водойм-0,01 мг / л. Наприкінці концентрація понад 0,03 є токсичною практично для всіх видів водних організмів. Надзвичайно токсична при попаданні з питною водою для тепло-кровних організмів, надходження ртуті з питною водою в кількості 75,0 ... 300,0 мг / сут є смертельним. Відрізняється високою токсичністю для будь-яких форм життя. При отруєнні па-рами спостерігається слабкість, головний біль, біль в шлунку, роздратування по-чек, навіть нефрит; катаральні явища. Розвивається тремтіння рук, ніг, всього тіла. Виникає стан підвищеної психічної збудливості [5]. Пари ртуті проявляють нейротоксичність, особливо страждають вищі відділи нервової системи [2]. **Скло** Нетоксичні, безпечно в навколишньому середовищу, не шкідлива в нирках і водоймах. Вдихання скляного пилу (волокон) призводить до силікоз в зв'язку з високим вмістом сполук кремнію. Шкідливої дії не робить, але є небезпека механічних пошкоджень (порізи, травми). **Алюміній** Токсичний для водної біоти, теплокровних тварин і людей, в концентрації> 1 мг / л чинить

					негативний впливав на зростання с /г культур. У концентрації> 1 мг / л гальмує зростання мікрофлори водойм і стримує процеси самоочищення водойм. Рівень токсичності визначається формою, в якій знаходиться елемент. Впливає на обмін речовин і функції нервової системи [2]. При попаданні на ґрунт, в воду і атмосферними повітря надає негативного впливу на НС і здоров'я людини.
	Макулатура	II	**Цинк** - 0,000053 – 0,000056 **Zn** **Свинець** - 0,000049 – 0,000051 **Pb** **Хром** - 0,000051 – 0,000054 **Cr** **Мідь** - 0,000033 – 0,000035 **Cu**	Уривки та обрізки з паперових мішків **Цинк** $T_{кип.}$= 913°С $T_{плав.}$= 4,19°С **Свинець** $T_{кип.}$= 1751°С $T_{плав.}$= 327,3°С **Хром** $T_{кип.}$= 1890°С $T_{плав.}$= 2480°С **Мідь** $T_{кип.}$= 2580°С $T_{плав.}$= 1083°С **Целюло**	Негативний вплив на ОС і людини визначається його хімічним складом. **Цинк** Малотоксичний для теплокровних тварин при надходженні з їжею і питної водою-концентрація в питній воді 11,2 ... 26,6 мг / л переноситься без будь-яких ознак інтоксикації. Дуже корисний для флори, будучи одним з найважливіших мікроелементів харчування, однак лише в концентрації до 0,2 мг / л, крім того, елемент силяється до кумуляції в грантах. Дуже токсичний для водних організмів, порушуючи процеси самоочищення водойм і стаючи токсичним для іхтіофауни в концентрації 0,15 ... 5,0 мг / л. Мутагенна і онкогенна небезпеку [2]. **Свинець** У природних водах міститься в концентрації 0,001 - 0,023 мг / л. У концентрації 2,0 мг / л надає воді металевий присмак. Можливо має мутагенну і канцерогенну дію, значно збільшує токсичну дію інших металів. В конценрації 1,90 мг / л згубно діє на дафній, концентрація 0,1 мг / л погіршує процеси самоочищення водойм. Свинець токсичний для рослин в концентрації понад 5,0 мг / кг ґрунту. Помірно токсичний. Викликає хронічне отруєння. Має здатність вражати центральну і периферичну нервову систему, кістковий мозок і кров, судини, синтез білка, генетичний апарат клітини [2]. **Хром** Міститься в природних водах в концентрації 0,001 ... 0,112 мг / л. LK50 Cr (VI) для риб-30,0 ... 50,0 мг / л, LK50 Cr (III) для риб- 117,0 мг / л. Низькі концентрації хрому позитивно впливають на ріст рослин, проте полив водою С / Г культур з концентрацією хрому 10,0 ... 50,0 мг / л гальмує їх розвиток. На тварин надає загально токсичне, подразнююче, кумулятивне, алергенну, канцерогенну і

			Целюлоза - 97,299 814 – 96,999 804 **$(C_6H_{10}O_5)_n$** **Вода** - 2,7 – 3,0	**за** $T_{возг.\ с\ обуглив.} \geq$ 100°С	мутагенну дію. Володіє канцерогенними властивістю (2) **Мідь** У природних водах міститься в концентраціях 0,001 ... 0,98 мг / л. У концентрації 0,5 мг / л забарвлює воду, в концентрації> 1,0 мг / л-помітно збільшує мутність води. Дуже токсична як для водних організмів, так і для рослин. У концентрації 0,001 мг / л гальмує розвиток синьо зелених водоростей, LK50 практично для всіх видів риб становить 0,18 ... 1,35 мг / л (короп, карась, окунь, щука, сом). Куммулюється ґрунтом і рослин-ями. У концентрації 0,1 ... 0,2 мг / л надає токсичну дію на ріст рослин. Високотоксичний метал. Викликає гостре отруєний-ня, має широкий спектр токсичної дії (2) **Целюлоза** Нетоксична. Досить легко підвержен біодеструкції лігнін- і целюлозоруйнуючими бактеріями і деякими класами низших грибів. У зв'язку з нетоксичністю LD50 для тваринах не установлена. Токсичність визначається за вмістом важких металів, здатних мігрувати з неї в навколишнє середовище. При попаданні на ґрунт, в воду і атмосферне повітря чинить негативний вплив на ОС і здоров'я людини.
	Склобій	III	**Кремія окис** - 52,0 – 81,74 **SiO_2** **Натрію**	Твердий, крихкий, прозорий матеріал, не розчиняється у воді **Кремія окис** - $T_{кип.}$= 2230°С $T_{плав.}$= 1500°С **Натрію**	Негативний вплив на ОС і людини визначається його хімічним складом. **Кремнію оксид** У природних водах може вміщатися у концентрації до 40,0 мг / л. Нетоксичний через не розчинених з'єднань кремнію в по-де. Для зрошення допускається вода з концентрацією кремнію 10,0 ... 50,0 мг / л. Поразка організму - через дихальні шляхи - пил при видобутку та переробки корисних копалин. Типові захворювання: пиловий пневмосклероз і силікоз [2] **Натрію окис** Сильно підвищує pH середовища, порушуя протікання нормальних біологічних процесів, однак дуже швидко нейтралізується вуглекислим газом, природними слабокислими водами, гуміновими кислотами грантів. LK50-27 ... 56 мг / л в залежності від виду риб, для мікроорганізмів (дафній) LD50- 156 мг / л. При отруєнні викликає нудоту, Печію, болі в епігастральній області, порушення функції нервової і травної систем,

			окис - 23,97 – 12,16 **Na_2O** **Калію окис** - 14,82 - 3,8 **K_2O** **Бора окис** - 9,21 – 2,3 **B_2O_3**	**окис** $T_{возг.}$ = 1275°С **Калію окис** $T_{разл.}$ = 350 - 400°С	подразнюють слизову верхніх дихальних шляхів [2]. **Калію окис** Вкрай малотоксичне для біоти. При надходженні в організм, як все гідроксиди. Надає прижигаючу дію. LD50 для тепло-кровних- 43 мг / кг, на відміну від сольових форм калію, концентрація яких в 1000 ... 2000 мг / л вважається допустимою в питній воді. Подразнює на слизові верхніх дихальних шляхів. При отруєнні викликає нудоту, печію, а також порушує функції нервової і травної систем [5]. При попаданні на ґрунт, в воду і атмосферне повітря чинить негативний вплив на ОС і здоров'я людини.
	Побутові відходи	IV	**Побутові відходи** - 100 – 100, в т. ч.: **Папір** -30 - 17; [**$(C_6H_{10}O_5)_n$** - целюлоза] **Поліетилен** -20 – 24; **$(-CH_2-CH_2-)_n$** **Деревина** -5 – 3; [**$(C_6H_{10}O_5)_n$** - целюлоза,	**Целюлоза** $T_{возг. с обуглив.} \geq$ 100°С **Поліетилен** - $T_{размяг.} \geq$ 150°С Твердий матеріал рослинного походження, не розчиняється у воді. Целюлоза, лігнін $T_{возг. с обуглив.} \geq$ 120°С	Негативний вплив на ОС і людини визначається його хімічним складом. **Целюлоза** Нетоксична. Досить легко піддавав біодеструкції лігнін- і целюлозоруйнуючими бактеріями і деякими класами низших грибів. У зв'язку з нетоксичністю LD50 для тваринах не установлена. Токсичність визначається за вмістом важких металів, здатних мігрувати з неї в навколишнє середовище **Поліетилен** Нетоксичний для всіх видів флори і фауни в зв'язку з дуже високою біологічною інертністю. Нерозчинний у водних середовищах і не впливає на санітарний режим водойм. Використання його не вимагає запобіжних заходів. Отруєння можливі при виробництві та переробці плівки, в результаті виділення окису вуглецю, альдегідів, органічних кислот [45] **Деревина** Нетоксична. Досить легко піддається біодеструкції лігнін- і целюлозоруйнуючими бактеріями і деякими класами нижчих грибів. У зв'язку з нетоксичністю LD50 для тварин не встановлена. Деревина нетоксична при використання. Але дія деревного пилу при рубці і переробці деревини викликає захворювання дихальних шляхів і шкіри. **Текстильне волокно** Нетоксичне в зв'язку з біогенним походженням, проте для біодеструкції

			лігнін] **Матеріали текстильні** -4 – 3; [$(C_6H_{10}O_5)_n$ - целюлоза **Мінеральні домішки (пісок, глина)** -4 – 9 **Харчові відходи** -37 –44;	Твердий матеріал рослинного походження, не розчиняється у воді. Целюлоза $T_{возг. с обуглив.} \geq 100°C$ **Харчові відходи** $T_{биоразл.} \geq 4° C$	необхідна наявність вологи. Нетоксична при використанні. Токсична дія виникає (як результат механічні дії -наслідок пилу) при виробництві тканів і при переробці вторинних матеріалів; слабкий алерген [8]. **Глина** Нетоксична. **Харчові відходи** Нетоксичні.