НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий Інститут телекомунікаційних систем

Кафедра електронних комунікацій та інтернету речей

«До захисту допущено»
ВО завідувача кафедри
_____ В’ячеслав НОСКОВ
«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Аналіз методів підвищення якісних показників інфокомунікаційних послуг в мережах NGN»

Виконав:
студент IV курсу, групи ТС-11
Пархоменко Ростислав Сергійович _____

Керівник:
Доцент кафедри ЕКІР, К.Т.Н., доцент.
Гатуров В.К. _____

Рецензент:
Незалежний експерт з телекомунікацій, к.т.н.
Мазор С. Ю. _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2025 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий Інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Освітня програма – «Системи електронних комунікацій та інтернету речей»

ЗАТВЕРДЖУЮ
ВО завідувача кафедри
_____ В’ячеслав НОСКОВ
«___»_____20__ р.

ЗАВДАННЯ
на дипломну роботу студенту
Пархоменко Ростиславу Сергійовичу

1. Тема роботи «Аналіз методів підвищення якісних показників інфокомунікаційних послуг в мережах NGN», керівник роботи доцент кафедри ТС, к.т.н. Гаттуров Віктор Кавич, затверджені наказом по університету від «26» травня 2025р. №1755 - с.

2. Термін подання студентом роботи 13 червня.

3. Вихідні дані до роботи: мережі NGN, якість обслуговування (QoS) мультисервісного трафіку - як один з важливих показників надійності мереж NGN, параметри QoS.

4. Зміст роботи: Аналіз стану мережі NGN та підвищення найдіності. Способи підвищення надійності NGN. Моделі та метод покращення параметрів QoS в мережі NGN.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) обсяг презентації 10 слайдів

6. Дата видачі завдання 15 березня.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Огляд літератури за даною темою.	15.03.2025	Виконано
2	Аналіз стану мереж NGN та проблем надійності	10.04.2025	Виконано
3	Надійність та якість зв’язку в мережі NGN.	01.05.2025	Виконано
4	Метод покращення параметрів якості обслуговування в мережі NGN.	20.05.2025	Виконано
5	Підведення підсумків.	04.06.2025	Виконано

Студент _____ Ростислав ПАРХОМЕНКО

Керівник роботи _____ Віктор ГАТУРОВ

РЕФЕРАТ

Обсяг роботи 69 сторінки, 1 ілюстрація, 2 таблиці, 22 джерел літератури.

Дипломна робота присвячена дослідженню методів підвищення надійності надання послуг зв’язку в мережах наступного покоління (NGN). У сучасних умовах NGN є основою телекомунікаційної інфраструктури, що забезпечує передачу голосу, відео та даних. Проте, через складність архітектури та високі вимоги до якості обслуговування, питання забезпечення надійності залишається актуальним.

Мета роботи – аналіз чинників, що впливають на надійність мереж NGN, а також розробка та дослідження методів її підвищення.

У роботі буде розглянуто:

- Архітектуру та принципи функціонування NGN;
- Основні ризики та проблеми, що впливають на надійність послуг;
- Метрики оцінки рівня надійності мереж NGN;
- Методи підвищення надійності, включаючи резервування, оптимізацію QoS, кібербезпеку та автоматизацію управління;

За результатами дослідження будуть сформульовані висновки щодо ефективності запропонованих методів та їх застосування для реальних NGN-мереж

Ключові слова: NGN (Next Generation Network), IP-мережі, конвергенція послуг, розподілена архітектура, масштабованість, відмовостійкість, автоматизація, резервування, QoS, MPLS, моніторинг мережі, безпека, VPN, покращення надійсності

ABSTRACT

The volume of the work is 69 pages, 1 illustration, 2 tables, 22 sources of literature.

The thesis is devoted to the study of methods for increasing the reliability of communication services in next-generation networks (NGN). In modern conditions, NGN is the basis of the telecommunications infrastructure, providing voice, video and data transmission. However, due to the complexity of the architecture and high requirements for the quality of service, the issue of ensuring reliability remains relevant.

The purpose of the work is to analyze the factors affecting the reliability of NGN networks, as well as to develop and study methods for its improvement.

The work will consider:

- Architecture and principles of NGN operation;
- Main risks and problems affecting the reliability of services;
- Metrics for assessing the level of reliability of NGN networks;
- Methods for increasing reliability, including redundancy, QoS optimization, cybersecurity and management automation;

Based on the results of the study, conclusions will be formulated regarding the effectiveness of the proposed methods and their application to real NGN networks.

Keywords: NGN (Next Generation Network), IP networks, service convergence, distributed architecture, scalability, fault tolerance, automation, redundancy, QoS, MPLS, network monitoring, security, VPN, improved reliability

Зміст

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

AS	Application Servers - сервери додатків
DSCP	Differentiated Service Code Point - Диференційований пункт обслуговування коду
IDN	Integrated Digital Network — інтегральні цифрові мережі
PSTN	Public Switched Telephone Network - Громадська комутована телефонна мережа
ISDN	Integrated Service Digital Network – цифрова мережа з інтеграцією служб
IP	Internet Protocol - інтернет протокол
ITU	International Telecommunication Union - Міжнародний союз телекомунікацій
IMS	IP-Multimedia Subsystem - IP-підсистема мультимедійного зв'язку
IN	Intelligent Network - інтелектуальна мережа
NGN	Next Generation Network — мережа зв'язку наступного покоління
SCE	Service Creation Environment - середовище створення послуг
SCF	Service Control Functions - функція управління послугами
SCP	Service Control Point - вузол керування послугами
SDP	Service Delivery Platform - платформа надання інтелектуальних послуг
SSF	Service Switching Function - функція перемикання послуг
SSP	Service Switching Point - вузол комутації послуг
SIP	Session Initiation Protocol - протокол ініціалізації сеансів зв'язку
SMP	Service Management Point - система експлуатаційного керування
QoS	Quality of service - якість обслуговування

ВСТУП

У сучасних телекомунікаційних системах мережі наступного покоління (NGN – Next Generation Networks) займають ключове місце, забезпечуючи високоякісні послуги зв’язку, інтеграцію різних технологій та масштабованість інфраструктури. NGN поєднує в собі передові технології передачі даних, підтримку мультимедійних сервісів та можливість гнучкого управління ресурсами мережі. Однак, із розвитком NGN зростає і потреба в забезпеченні високої надійності надання послуг, оскільки збої або нестабільність мережі можуть призвести до значних фінансових втрат та зниження якості обслуговування кінцевих користувачів.

Актуальність теми. Надійність мереж NGN є критичним параметром їхньої ефективності, оскільки від цього залежить якість переданого контенту, мінімізація затримок та безперебійна робота інформаційних сервісів. Використання NGN у різних сферах – від корпоративних мереж до національних операторів зв’язку – вимагає впровадження механізмів підвищення стійкості до збоїв, кіберзагроз та перевантажень. Одним із викликів є забезпечення ефективного управління якістю обслуговування (QoS), використання резервування, кібербезпеки та автоматизованих систем моніторингу. Саме тому дослідження методів підвищення надійності NGN є актуальним і практично значущим завданням.

Мета дипломної роботи – дослідження чинників, що впливають на надійність NGN, аналіз існуючих методів її підвищення та розробка рекомендацій щодо покращення стійкості мережі до збоїв.

Для досягнення мети роботи необхідно вирішити наступні **завдання:**

- Дослідити архітектуру та особливості функціонування мереж NGN;
- Визначити основні фактори, що впливають на надійність та якість надання послуг у таких мережах;

- Проаналізувати існуючі підходи до підвищення надійності, включаючи резервування, QoS-оптимізацію, захист від атак та автоматизацію управління мережею;
- Розробити та провести моделювання впровадження механізмів підвищення надійності NGN;
- Оцінити ефективність запропонованих рішень та розробити рекомендації щодо їх практичного використання.

Об’єктом дослідження є мережі наступного покоління (NGN) та їхні технологічні особливості.

Предметом дослідження виступають методи та механізми підвищення надійності надання послуг у NGN.

Для виконання дослідження застосовуються такі **методи:**

1. Теоретичний аналіз та огляд літератури щодо архітектури NGN та питань надійності;
2. Методи математичного моделювання для оцінки показників надійності;
3. Комп'ютерне моделювання сценаріїв роботи NGN із використанням симуляційних програм (наприклад, Cisco Packet Tracer, GNS3, NS3);
4. Аналіз експериментальних даних та порівняння результатів до та після впровадження механізмів підвищення надійності.

Структура роботи. Дипломна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків.

1 АНАЛІЗ СТАНУ МЕРЕЖ NGN ТА ПРОБЛЕМ НАДІЙНОСТІ

1.1 Огляд архітектури та особливостей NGN

Мережі зв’язку наступного покоління (NGN, Next Generation Network) являють собою конвергентні телекомунікаційні системи, що базуються на IP-протоколі та підтримують різні види мультимедійного трафіку, включаючи голосові виклики, відеоконференції, потокове мовлення та обмін даними. Основною характеристикою NGN є відокремлення контрольного та транспортного рівнів, що забезпечує гнучкість, підвищену стійкість до відмов і ефективне управління мережевими ресурсами. Впровадження NGN дозволяє операторам зв’язку спростити інтеграцію нових сервісів, оптимізувати маршрутизацію трафіку та підвищити якість обслуговування кінцевих користувачів. Завдяки підтримці відкритих стандартів та протоколів, таких як SIP, H.323 та MGCP, NGN сприяє сумісності між різними виробниками обладнання, що полегшує модернізацію мережевої інфраструктури.

NGN поєднує передачу голосу, відео, даних та інших сервісів в єдиній IP-мережі. Це забезпечує уніфікацію управління та значне скорочення витрат на інфраструктуру. Такий підхід дозволяє операторам зв’язку ефективніше використовувати мережеві ресурси, знижує витрати на технічне обслуговування та модернізацію обладнання. Крім того, конвергенція сприяє підвищенню якості обслуговування користувачів завдяки оптимізації маршрутизації трафіку та зменшенню затримок у передачі даних. Використання єдиної платформи для всіх типів трафіку також покращує гнучкість управління мережею та спрощує впровадження нових сервісів.

Завдяки розподіленій моделі, NGN забезпечує високу масштабованість та гнучкість розгортання нових послуг без значних змін у фізичній інфраструктурі. Мережа складається з незалежних модулів, які можуть розгортатися поступово, що дозволяє операторам адаптувати інфраструктуру відповідно до зростаючих потреб користувачів. Розподілена архітектура також сприяє підвищенню відмовостійкості, оскільки відмова окремого

модуля не призводить до збоїв у всій системі. Крім того, такий підхід дозволяє легко інтегрувати нові сервіси та технології, зменшуючи час впровадження та витрати на оновлення мережі.

На відміну від традиційних комутаційних мереж, в NGN функції управління та транспорту розділені, що покращує ефективність і дозволяє реалізовувати складні механізми управління трафіком та забезпечення якості обслуговування (QoS). Розподіл функцій означає, що контрольні елементи, такі як Softswitch або IMS (IP Multimedia Subsystem), займаються виключно управлінням викликами, автентифікацією користувачів, політиками безпеки та маршрутизацією сигналізації. Транспортні елементи, такі як маршрутизатори та медіа-шлюзи (Media Gateway), виконують функції комутації та передачі даних між вузлами. Це дозволяє динамічно балансувати навантаження на мережу, покращувати стійкість до відмов за рахунок географічного розподілу елементів та спрощувати впровадження нових послуг без значного впливу на основну інфраструктуру.

NGN використовує загальноприйняті протоколи, такі як SIP (Session Initiation Protocol), H.323, MGCP (Media Gateway Control Protocol), що сприяє сумісності між різними виробниками обладнання. Завдяки використанню відкритих стандартів, провайдери можуть впроваджувати обладнання від різних виробників без ризику несумісності. Це також дозволяє операторам легко інтегрувати нові сервіси та технології без значних змін у мережевій інфраструктурі. Окрім того, стандартизовані протоколи забезпечують підтримку взаємодії з традиційними мережами, такими як PSTN (Public Switched Telephone Network), що є важливим фактором під час переходу на NGN. Використання відкритих інтерфейсів також сприяє розвитку інновацій, оскільки сторонні розробники можуть створювати нові програмні рішення, сумісні з NGN.

Мережа підтримує механізми QoS, що дозволяють забезпечувати пріоритетність трафіку та гарантувати необхідний рівень обслуговування для критичних сервісів, таких як IP-телефонія та потокове відео.

Використовуються такі методи, як диференційоване обслуговування (DiffServ), інтегровані служби (IntServ) та механізми управління чергами (WFQ, PQ, RED), що забезпечують ефективний розподіл ресурсів між користувачами. Також реалізовано механізми адаптивного управління трафіком, які дозволяють в реальному часі перенаправляти потоки даних через оптимальні маршрути, уникати перевантажень та знижувати затримки. Це критично важливо для забезпечення стабільного зв’язку, особливо у випадку високої завантаженості мережі або при непередбачуваних змінах у трафіку.

Архітектура NGN побудована на основі концепції рівневої моделі, що включає наступні основні рівні. Така архітектура забезпечує модульність, масштабованість та можливість гнучкої адаптації до змін у технологічному середовищі. Кожен рівень виконує специфічні функції та взаємодіє з іншими рівнями через стандартизовані інтерфейси, що забезпечує високу сумісність та підтримку широкого спектра послуг. Крім того, рівнева структура дозволяє впроваджувати нові технології без значних змін у всій інфраструктурі, що зменшує витрати на модернізацію та обслуговування мережі.

Рівень доступу забезпечує підключення абонентів до мережі через різні технології, включаючи оптичний зв’язок (FTTH, GPON), бездротові мережі (Wi-Fi, LTE, 5G) та традиційні кабельні рішення (xDSL, DOCSIS). Цей рівень є критично важливим для забезпечення якості обслуговування (QoS), оскільки безпосередньо впливає на пропускну здатність, затримки та стабільність з'єднання. Важливим аспектом є використання механізмів аутентифікації та управління доступом, таких як 802.1X, RADIUS та TACACS+, що забезпечують контроль і безпеку підключень. Крім того, застосовуються методи керування пропускною здатністю (Traffic Shaping, Bandwidth Management) та адаптивні технології вибору каналу, що дозволяють оптимізувати навантаження на мережу. Використання інтелектуальних антенних систем, зокрема MIMO в LTE та 5G, покращує

ефективність спектра та підвищує стійкість з’єднання у складних умовах поширення сигналу.

Використовується для передачі трафіку між вузлами мережі та реалізований на основі IP/MPLS-технологій. Цей рівень підтримує маршрутизацію, балансування навантаження та механізми забезпечення якості обслуговування (QoS). Використання технології MPLS (Multiprotocol Label Switching) дозволяє значно зменшити затримки передачі, оптимізувати використання ресурсів мережі та забезпечити стійкість до відмов шляхом динамічного перемикання трафіку. Для покращення ефективності маршрутизації застосовуються механізми TE (Traffic Engineering), які дозволяють коригувати маршрутизацію залежно від завантаженості каналів. Крім того, на цьому рівні реалізовані протоколи швидкого відновлення зв’язку, такі як MPLS Fast Reroute (FRR) та Bidirectional Forwarding Detection (BFD), що забезпечують мінімізацію часу відновлення з’єднання у разі виходу з ладу одного з вузлів або каналів зв’язку. Завдяки цим технологіям транспортний рівень NGN гарантує високу надійність та адаптивність до змін у мережевому середовищі.

Цей рівень відповідає за управління викликами, сигналізацію, авторизацію, автентифікацію та забезпечення безпеки мережі. Головним елементом є Softswitch – програмний комутатор, який керує викликами між користувачами, маршрутизує сигналізацію та взаємодіє із сервісними платформами. Також Softswitch забезпечує політику доступу до ресурсів мережі та інтеграцію з традиційними телефонними мережами (PSTN, ISDN).

До ключових протоколів цього рівня належать SIP (Session Initiation Protocol) – для встановлення, управління та завершення сеансів зв’язку, H.248 (Megaco) – для керування шлюзами медіа-трафіку, та Diameter – для авторизації, автентифікації та білінгу. Крім того, використовується протокол RADIUS для централізованого керування доступом до мережевих сервісів.

Контрольний рівень також реалізує механізми сигналізації та балансування навантаження між серверами викликів, що сприяє підвищенню надійності роботи мережі. Використання резервування та географічно розподілених контрольних елементів дозволяє зменшити ризики простоїв та покращує відмовостійкість NGN.

Забезпечує реалізацію широкого спектра послуг, таких як VoIP, IPTV, хмарні сервіси, інтерактивні мультимедійні додатки, а також корпоративні рішення для обробки даних та управління бізнес-процесами. Для їх реалізації використовуються сервери додатків, що інтегрують різні сервіси через стандартизовані API, забезпечуючи взаємодію між користувачами, провайдерами послуг та мережевою інфраструктурою. Також використовуються технології віртуалізації (NFV) та програмно-налаштовані мережі (SDN), які покращують гнучкість розгортання сервісів, спрощують управління ресурсами та забезпечують масштабованість у відповідь на зростаючі вимоги користувачів.

Резервування та відмовостійкість. У NGN передбачено дублювання критичних компонентів (серверів, маршрутизаторів, комутаторів) та використання механізмів швидкого переключення трафіку у разі відмови одного з вузлів.

Механізми якості обслуговування (QoS). NGN підтримує різні механізми керування трафіком, включаючи пріоритизацію пакетів, поліси трафіку та адаптивну маршрутизацію.

Захист та безпека. Використання механізмів шифрування, VPN, брандмауерів та систем виявлення вторгнень (IDS/IPS) забезпечує захист мережі від кібератак та несанкціонованого доступу.

Моніторинг та управління мережею. Використовуються системи управління мережею (NMS, Network Management Systems), що дозволяють контролювати стан обладнання, аналізувати трафік та оперативно реагувати на збої.

1.2 Класифікація послуг, що надаються NGN

IP-телефонія є однією з ключових послуг, що надаються мережею NGN. Вона дозволяє здійснювати голосові виклики через IP-мережі, використовуючи такі протоколи, як SIP (Session Initiation Protocol) та H.323. Основною перевагою IP-телефонії є зниження витрат на зв'язок завдяки ефективному використанню пропускної здатності мережі, а також підтримка широкого спектра додаткових сервісів, таких як переадресація викликів, голосова пошта та конференц-зв'язок. Завдяки інтеграції з традиційними телефонними мережами (PSTN), IP-телефонія забезпечує гнучкість у виборі засобів комунікації, дозволяючи абонентам з'єднуватися як через інтернет, так і через традиційні телефонні лінії. Важливим аспектом є забезпечення якості голосового зв’язку, що досягається шляхом впровадження механізмів QoS та адаптивних алгоритмів стиснення аудіосигналу.

Відеозв’язок у мережах NGN забезпечує високоякісну передачу аудіо- та відеосигналу в реальному часі, що робить його важливим засобом для проведення відеоконференцій, віддаленого навчання та телемедицини. Для організації відеозв’язку використовуються протоколи SIP, H.323 та WebRTC, які дозволяють підтримувати різні формати відеопотоків та інтегрувати відеозв’язок у бізнес-додатки. Важливим параметром є адаптація до умов мережевого середовища, що дозволяє автоматично регулювати якість відео відповідно до доступної пропускної здатності. Використання технологій стиснення відео, таких як H.264 та H.265, допомагає зменшити навантаження на мережу без втрати якості зображення. Завдяки розвитку NGN, відеозв’язок стає доступним на мобільних пристроях, що розширює можливості користувачів у спілкуванні та роботі на відстані.

Передача даних у NGN включає широкий спектр послуг, що охоплюють доступ до інтернету, обмін файлами, віддалений доступ до серверів та хмарні сервіси. Завдяки високій пропускній здатності та підтримці протоколів оптимізації трафіку, таких як MPLS та SDN, мережі

NGN забезпечують стабільну та ефективну передачу даних з мінімальними затримками. Використання сучасних технологій маршрутизації та балансування навантаження дозволяє підвищити продуктивність мережі та забезпечити рівномірний розподіл трафіку між користувачами. Крім того, передача даних у NGN включає механізми безпеки, такі як VPN, шифрування та автентифікація користувачів, що гарантує захист інформації від несанкціонованого доступу та втручання. Завдяки інтеграції з хмарними платформами, користувачі отримують можливість працювати з великими обсягами даних та використовувати ресурси віддалених обчислювальних потужностей без необхідності інвестувати в локальну інфраструктуру.

Якість обслуговування (QoS) у NGN відіграє ключову роль у забезпеченні стабільної роботи мережі та підтримці належного рівня обслуговування користувачів. QoS визначає пріоритетність трафіку, що дозволяє ефективно розподіляти мережеві ресурси між різними видами сервісів, такими як голосовий зв’язок, відеоконференції та передача даних. Основні механізми QoS включають класифікацію та маркування трафіку, управління чергами (WFQ, PQ, RED) та контроль пропускної здатності. Використання QoS дозволяє мінімізувати затримки, джитер та втрати пакетів, що особливо важливо для послуг реального часу, таких як IP-телефонія та відеозв’язок. Крім того, впровадження QoS підвищує загальну надійність NGN, оскільки забезпечує резервування критично важливих ресурсів, балансування навантаження та механізми швидкого відновлення у разі збоїв. Завдяки цьому мережі NGN здатні гарантувати високу якість зв’язку навіть у складних умовах експлуатації, що робить їх оптимальним рішенням для сучасних телекомунікаційних потреб.

1.3 Фактори, що впливають на надійність NGN

Перевантаження мережі та проблеми з трафіком становлять серйозну перешкоду для побудови та експлуатації мереж наступного покоління (NGN).Оскільки такі мережі використовують єдину IP-інфраструктуру для передачі голосу, відео та даних, критично важливо ефективно управляти ресурсами та контролювати навантаження, щоб забезпечити стабільну роботу всіх сервісів. Основні причини перевантаження включають нерівномірний розподіл трафіку, обмежену пропускну здатність каналів, атаки на мережу, неефективну маршрутизацію та недостатню оптимізацію механізмів Quality of Service (QoS).

Перевантаження може відбуватися як у локальних сегментах мережі (наприклад, у магістральних комутаторах, вузлах доступу), так і на глобальному рівні (зокрема, у міжконтинентальних оптичних магістралях). Найбільш критичними є ситуації, коли велика кількість користувачів одночасно генерує високу кількість трафіку, наприклад, під час відеотрансляцій або масового завантаження великих файлів. В таких випадках затримки зростають, збільшується ймовірність втрати пакетів, що особливо критично для сервісів реального часу, таких як IP-телефонія або відеоконференції.

Механізми управління трафіком включають використання політик QoS, які дозволяють класифікувати пакети за пріоритетністю, надаючи перевагу критичним потокам, а також механізми балансування навантаження, які рівномірно розподіляють трафік між доступними ресурсами. Додатково застосовуються технології кешування контенту, які допомагають зменшити навантаження на магістральні канали, та алгоритми динамічної маршрутизації, що дозволяють автоматично адаптувати шляхи передачі даних відповідно до поточного стану мережі.

Щоб наочно пояснити проблему перевантаження, уявимо схему мережі, в якій кілька користувачів одночасно надсилають великі обсяги

даних через один маршрутизатор, пропускна здатність якого обмежена. У такому випадку мережевий пристрій буде змушений або відкидати деякі пакети, або ставити їх у чергу, що призведе до затримок. Якщо в мережі реалізований QoS, то критично важливі пакети, наприклад, голосового зв’язку, будуть оброблятися першочергово, а менш пріоритетний трафік, наприклад, завантаження файлів, може бути обмежений або відкладений.

Рисунок 1.1 - Проблема перевантаження мережі

Рис. 1.1 показує, як багато користувачів одночасно передають великий обсяг даних через маршрутизатор із обмеженою пропускною здатністю. Видно, що маршрутизатор стає вузьким місцем, через що пакети даних накопичуються в черзі, а деякі з них можуть втрачатися через перевантаження. Також схематично відображено механізм QoS (якість обслуговування), де голосові пакети мають вищий пріоритет порівняно з іншими видами трафіку.

Мережі наступного покоління (NGN) мають складну інфраструктуру, яка включає апаратні й програмні компоненти, що можуть зазнавати різних загроз та відмов. Надійність і стійкість NGN залежить від здатності системи ефективно протидіяти несправностям, атакам та програмним помилкам.

Фізична інфраструктура NGN складається з маршрутизаторів, комутаторів, серверів, базових станцій, оптичних ліній зв'язку та інших апаратних компонентів, які можуть вийти з ладу через знос, виробничі дефекти, несприятливі зовнішні умови чи людські помилки.

Основні фактори відмов обладнання включають:

- Перегрів – активне мережеве обладнання потребує якісного охолодження, інакше воно може вийти з ладу.
- Зношення компонентів – електронні модулі мають обмежений термін експлуатації, і з часом їх продуктивність падає.
- Фізичні пошкодження – кабелі можуть бути випадково перерізані під час будівельних робіт, обладнання пошкоджене через удари або аварії.
- Збої в електропостачанні – відключення живлення або перепади напруги можуть призвести до зупинки критично важливих систем.

Щоб мінімізувати вплив таких відмов, оператори NGN використовують резервування обладнання (hot standby), автоматичне перемикання на альтернативні маршрути та джерела живлення, а також проактивний моніторинг стану систем.

Оскільки NGN базується на IP-технологіях, вона вразлива до широкого спектра кіберзагроз, аналогічних до атак на традиційні комп'ютерні мережі.

Основні типи атак:

1. DDoS-атаки (розподілені атаки відмови в обслуговуванні) – зловмисники перевантажують мережеві вузли або сервіси масованим трафіком, викликаючи затримки, втрату даних або повне блокування зв'язку.

2. Атаки на сигналізаційні протоколи (SIP, H.248, Diameter) – зламуючи механізми сигналізації, хакери можуть перехоплювати дзвінки, змінювати маршрутизацію трафіку або спричиняти збої.
3. Перехоплення трафіку (Man-in-the-Middle, MITM) – атакуючі можуть отримати доступ до незашифрованих комунікацій, підміняти дані або здійснювати шпигунство.
4. Експлуатація вразливостей програмного забезпечення – якщо NGN працює на незахищеному або застарілому ПЗ, зловмисники можуть скористатися вразливостями для віддаленого виконання команд, отримання контролю над обладнанням чи викрадення даних.

Для захисту від кібератак застосовують сегментацію мережі, брандмауери, системи виявлення та запобігання вторгненням (IDS/IPS), шифрування трафіку, а також регулярні оновлення програмного забезпечення.

NGN значною мірою залежить від складних програмних рішень для маршрутизації, управління трафіком, обробки дзвінків та інших функцій. Помилки у коді або некоректні оновлення можуть спричиняти серйозні збої.

Основні причини програмних збоїв у NGN:

1. Баги в коді – неправильна логіка обробки даних, некоректна обробка виключень або пам’яткові витоки можуть викликати зависання сервісів або їх некоректну роботу.
2. Конфлікти між версіями ПЗ – при оновленні компонентів системи можуть виникати несумісності, що призводять до збоїв у зв’язку або зниження продуктивності.
3. Ненавмисне видалення або модифікація критичних конфігурацій – оператори можуть помилково змінити налаштування маршрутизації, QoS або безпеки, що спричинить перебої в роботі мережі.
4. Недостатнє тестування оновлень – якщо перед розгортанням оновлення не перевіряється в тестовому середовищі, можливі непередбачувані наслідки для реальної мережі.

Щоб зменшити ризики, провайдери використовують автоматизовані системи управління конфігураціями, тестові середовища для перевірки оновлень, механізми відкату змін, а також моніторинг продуктивності та стабільності програмних компонентів.

1.4 Метрики оцінки надійності NGN

MTBF – це показник, що характеризує середній час безвідмовної роботи мережевого обладнання або системи між двома послідовними відмовами. Чим вище значення MTBF, тим надійнішою є система.

Формула розрахунку MTBF:

$$MTBF = \frac{T_{total}}{N}$$

де:

- T_{total} – загальний час роботи обладнання або системи,
- N – кількість відмов за цей період.

Фактори, що впливають на MTBF:

- Якість виробництва обладнання – надійні компоненти мають вищий MTBF.
- Умови експлуатації – перегрів, волога, механічні навантаження можуть скорочувати MTBF.
- Технічне обслуговування – регулярне профілактичне обслуговування може продовжити термін безвідмовної роботи.
- Програмне забезпечення – стабільність прошивки та оновлення впливають на тривалість роботи системи без збоїв.

Приклад: Якщо мережевий комутатор працює 10 000 годин і за цей час відбулося 5 відмов, то його MTBF буде

$$MTBF = \frac{10000}{5} = 2000 \text{ годин}$$

Це означає, що в середньому комутатор працюватиме 2000 годин до наступної відмови.

MTTR – це середній час, необхідний для відновлення працездатності системи після відмови. Він включає діагностику проблеми, ремонт або заміну обладнання, тестування та повторний запуск системи.

Формула розрахунку MTTR:

$$MTTR = \frac{T_{repair}}{N}$$

де:

T_{repair} – загальний час усунення несправностей,

N – кількість відмов, які усувалися.

Фактори, що впливають на MTTR:

1. Швидкість виявлення проблеми – наявність моніторингових систем дозволяє швидко визначити місце збою.
2. Доступність резервних компонентів – якщо запасні модулі є в наявності, час ремонту скорочується.
3. Кваліфікація персоналу – досвідчений персонал усуває несправності швидше.
4. Автоматизація процесів – використання автоматичних механізмів перемикання на резервні лінії зменшує час простою.

Приклад: Якщо сумарний час усунення несправностей у мережі за місяць становить 20 годин і за цей час сталося 4 відмови, то:

$$MTTR = \frac{20}{4} = 5 \text{ годин}$$

Це означає, що в середньому на кожну відмову витрачається 5 годин на її усунення.

Availability (Доступність системи) – це показник, що визначає частку часу, протягом якого система була доступною для використання. Він виражається у відсотках і є ключовою метрикою для оцінки надійності NGN.

$$A = \frac{MTBF}{MTBF + MTTR} \times 100\%$$

Фактори, що впливають на Availability:

1. Високий MTBF (довгий час безвідмовної роботи) збільшує доступність.
2. Низький MTTR (швидке відновлення) також сприяє високому значенню Availability.
3. Використання резервних механізмів та автоматичного переключення на дублюючі системи мінімізує час простою.
4. Надійність програмного забезпечення та оперативність оновлень.

Приклад розрахунку Availability:

Якщо система має MTBF = 2000 годин і MTTR = 5 годин, то її доступність буде:

$$A = \frac{2000}{2000 + 5} \times 100\% = \frac{2000}{2005} \times 100\% = 99.75\%$$

Це означає, що система буде працювати безперебійно 99.75% часу, а можливий простій складатиме 0.25% від загального часу.

Таблиця 1.1 - Категорії доступності систем

Доступність	Максимальний час простою на рік
99%	~ 87.6 годин
99.9%	~ 87.6 годин
99.99%	~ 52.56 хвилин
99.999%	~ 5.26 хвилин

Чим вище рівень доступності, тим менше часу NGN перебуватиме у стані відмови або ремонту.

У NGN-мережах ключовими параметрами продуктивності є втрата пакетів (Packet Loss), затримка (Latency) і джитер (Jitter), оскільки вони визначають стабільність і якість переданих даних. Від їхніх значень залежить надійність роботи сервісів та комфорт користувачів при взаємодії з мережею.

Цей показник відображає частку пакетів, які не доходять до пункту призначення через перевантаження мережі, помилки маршрутизації, збої в обладнанні або вплив атак. Він виражається у відсотках від загальної кількості переданих пакетів:

$$PL(\%) = \frac{P_{lost}}{P_{sent}} \times 100$$

Де:

- P(lost) – кількість втрачених пакетів,
- P(sent) – загальна кількість відправлених пакетів.

Допустимий рівень втрати пакетів залежить від типу сервісу:

- Для потокового відео та VoIP: < 1%
- Для звичайної передачі файлів: до 5%
- Для критичних застосунків (онлайн-ігри, відеоконференції): < 0.1%

Якщо рівень втрат перевищує порогові значення, це призводить до спотворень голосу, зниження якості відео або навіть повного розриву з'єднання.

Цей показник визначає час, необхідний для проходження пакета від відправника до отримувача. Вимірюється в мілісекундах (мс). В NGN можна розрізняти три основні типи затримок:

1. Одностороння (One-Way Delay) – час проходження пакета в одному напрямку.
2. Кругова (Round-Trip Time, RTT) – час, необхідний для передачі пакета і отримання відповіді.

3. End-to-End Delay – загальна затримка при передачі між двома кінцевими вузлами.

Допустимі значення затримки для різних сервісів:

- Інтерактивний голосовий трафік (VoIP): < 150 мс (рекомендовано ITU-T G.114)
- Відеоконференції: < 200 мс
- Онлайн-ігри: < 100 мс
- Передача файлів: може бути вище 500 мс

Висока затримка викликає ефект "відлуння" в розмовах, розсинхронізацію аудіо та відео, а в онлайн-іграх – значні затримки в діях користувача.

Високий джитер унеможливлює коректне відтворення голосу або відео. Вимірюється у мілісекундах:

$$Jitter = \mid D_n - D_{n-1} \mid$$

Де Dn – затримка поточного пакета, а D(n−1) – затримка попереднього пакета.

Для забезпечення якісного VoIP та відеозв’язку джитер повинен бути менше 30 мс.

Щоб мінімізувати негативний вплив цих показників, у NGN використовуються такі технології:

- QoS-пріоритизація – розподіл ресурсів на основі класів сервісу (голосовий трафік отримує вищий пріоритет).
- Механізми корекції втрат (FEC – Forward Error Correction) – відправлення резервних пакетів для відновлення втрачених даних.
- Буферизація та компенсація джитера (Jitter Buffer) – затримка відтворення для усереднення часу надходження пакетів.
- Оптимізація маршрутизації – використання найшвидших і найменш завантажених маршрутів для передачі трафіку.

1.5 Висновки до розділу 1

У першому розділі було здійснено всебічний аналіз архітектурних особливостей мереж наступного покоління (NGN) та виокремлено основні фактори, що впливають на їхню надійність. Зокрема, було встановлено, що NGN базується на принципах конвергенції сервісів, модульності, розподілу функцій керування та комутації, а також підтримці відкритих стандартів і протоколів, що дозволяє створювати масштабовані, гнучкі та взаємодіючі між собою середовища зв’язку.

Особливу увагу приділено моделі взаємодії елементів NGN, яка побудована за рівневим принципом і охоплює доступ, транспорт, контроль та застосування. Детальний аналіз кожного рівня показав, що їх узгоджена взаємодія забезпечує ефективне управління трафіком, підтримку якісного обслуговування (QoS) та оперативну реакцію на зміну умов у мережі.

Розглянуто класифікацію послуг NGN, таких як IP-телефонія, відеозв’язок і передача даних, що доводить широкі функціональні можливості платформи. Показано, що рівень якості обслуговування напряму залежить від ефективності застосування механізмів QoS, що забезпечують пріоритезацію трафіку та контроль параметрів затримки, втрат і джитера.

Окремо досліджено фактори, що впливають на надійність NGN: проблеми перевантаження мережі, апаратні відмови, кібератаки та програмні збої. Було виявлено, що поєднання фізичних і логічних загроз вимагає комплексного підходу до їх нейтралізації, зокрема — резервування обладнання, впровадження механізмів IDS/IPS, сегментації трафіку та системного моніторингу.

Нарешті, проведено аналіз ключових метрик оцінки надійності: MTBF, MTTR та Availability. Наведені приклади розрахунків дозволили наочно продемонструвати, як інженерно-технічні параметри впливають на загальну доступність сервісів. Також було охарактеризовано параметри втрат пакетів, затримок і джитера — основні індикатори якості послуг у реальному часі.

Сукупність отриманих даних дозволяє зробити висновок, що забезпечення високої надійності NGN вимагає не лише вдосконаленої архітектури, але й комплексного застосування інженерних, програмних та організаційних рішень для постійного контролю та підвищення стійкості мережі.

2 СПОСОБИ ПІДВИЩЕННЯ НАДІЙНОСТІ NGN

2.1 Резервування та відмовостійкість

Дублюючі маршрути є критично важливим механізмом для забезпечення відмовостійкості та безперебійного функціонування NGN. Вони дозволяють автоматично перенаправляти трафік альтернативним шляхом у разі несправності основного каналу зв’язку. Це особливо важливо для підтримки безперервної роботи сервісів реального часу, таких як IP-телефонія, відеозв’язок і передача даних. Використання дублюючих маршрутів є основним підходом у динамічній маршрутизації, що дозволяє автоматично обирати найоптимальніший шлях для передачі пакетів на основі поточного стану мережі.

Застосування протоколів OSPF (Open Shortest Path First) та BGP (Border Gateway Protocol) сприяє швидкому визначенню альтернативного маршруту у разі виходу з ладу одного з вузлів. OSPF дозволяє маршрутизаторам обирати найкоротший доступний шлях, а BGP ефективно управляє маршрутами між автономними системами в глобальній мережі Інтернет. Використання таких протоколів дає змогу значно зменшити час простою мережі та підвищити її продуктивність, запобігаючи втраті пакетів і збоям у роботі сервісів.

У сучасних NGN-мережах дублюючі маршрути реалізуються за допомогою технологій MPLS (Multiprotocol Label Switching), які забезпечують швидке перемикання трафіку у разі аварійної ситуації. Наприклад, у разі виходу з ладу одного маршрутизатора система миттєво перемикає трафік на альтернативний маршрут завдяки попередньо налаштованим резервним шляхам. Це значно скорочує час відновлення зв’язку та зменшує ризик втрати критичних даних.

Практичний приклад застосування дублюючих маршрутів можна знайти у великих дата-центрах та операторських мережах. Наприклад, магістральний канал між двома великими вузлами може мати основний

маршрут через одне місто і резервний через інше. У разі стихійного лиха або фізичного пошкодження кабелю в основному маршруті система миттєво перемикає трафік на резервний, забезпечуючи безперервність роботи мережі.

Окрім цього, дублюючі маршрути часто застосовуються у VPN-з'єднаннях для забезпечення надійного віддаленого доступу. Наприклад, якщо основний тунель VPN через Інтернет стає недоступним, трафік автоматично перемикається на альтернативне з'єднання через мобільну мережу або супутниковий зв'язок. Такий підхід гарантує стабільний зв'язок незалежно від стану основної інфраструктури.

Загалом, використання дублюючих маршрутів є ключовим компонентом забезпечення високої надійності NGN. Впровадження таких рішень дозволяє операторам зв'язку та великим підприємствам знизити ризики, пов'язані з відмовами мережевого обладнання та зменшити негативний вплив можливих збоїв на кінцевих користувачів.

Дублюючі маршрути дозволяють автоматично перенаправляти трафік через альтернативний шлях у разі виходу з ладу основного з'єднання. Завдяки цьому забезпечується безперервність зв'язку та стабільне функціонування таких критично важливих сервісів, як IP-телефонія, відеоконференції та передача даних.

Приклад: якщо магістральний канал між двома вузлами виходить з ладу, система автоматично перемикає трафік на резервний канал, який використовує інший маршрут. Це гарантує, що передача даних не переривається, навіть у разі серйозного збою. Такий механізм є основою динамічної маршрутизації і широко застосовується в сучасних мережах, зокрема за допомогою протоколів OSPF (Open Shortest Path First) та BGP (Border Gateway Protocol). OSPF дозволяє маршрутизаторам обирати найкоротший доступний шлях передачі даних, а BGP визначає оптимальні маршрути між автономними системами в глобальній мережі Інтернет. Окрім цього, реалізація таких підходів забезпечує автоматичне балансування навантаження, знижуючи ймовірність перевантаження окремих вузлів

мережі. Наприклад, у великих корпоративних мережах або мережах операторів зв’язку застосовується резервування шляхів між ключовими вузлами для мінімізації ризиків втрати підключення внаслідок аварійного пошкодження оптичних волокон або відмови обладнання.

Резервування є одним із основних методів забезпечення безперебійного функціонування NGN-мереж. Розглянемо три основні моделі: N+1, 1+1 і 2N, які застосовуються для підвищення відмовостійкості та мінімізації наслідків можливих збоїв.

Модель N+1 є однією з найпоширеніших і економічно ефективних. Вона передбачає наявність одного резервного елемента на групу з N основних елементів. Це означає, що у випадку виходу з ладу будь-якого з основних компонентів, резервний елемент негайно бере на себе його функції, забезпечуючи мінімальний час простою. Наприклад, у великому центрі обробки даних, де працюють сотні серверів, використання N+1 дозволяє мати лише кілька резервних, що значно зменшує витрати на обладнання та обслуговування. Однак, слід пам'ятати, що ця модель не захищає від одночасного виходу з ладу двох або більше основних елементів. У такому випадку система може зіткнутися з серйозними проблемами. Для підвищення надійності в деяких випадках застосовують модифікацію N+X, де X - кількість резервних елементів.

На противагу цьому, модель 1+1 забезпечує найвищий рівень надійності за рахунок повного дублювання кожного елемента. Трафік одночасно передається через обидва елементи, і в разі відмови одного з них, інший миттєво перебирає на себе навантаження. Це гарантує практично безперервний зв'язок, що є критично важливим для систем, де час простою неприпустимий. Наприклад, у фінансових установах, де кожна секунда простою може призвести до величезних збитків, використання 1+1 є необхідністю. Цікаво, що в деяких системах, де час переключення є критичним, використовують так зване "гаряче резервування", коли резервний елемент постійно активний і готовий до негайної заміни. Це дозволяє

мінімізувати час переключення до мілісекунд, що робить переривання зв'язку практично непомітним для користувачів.

Модель 2N – це вершина надійності, де вся система повністю дублюється. Це означає, що є дві абсолютно ідентичні системи, які працюють паралельно. У разі виходу з ладу однієї з них, друга повністю перебирає на себе її функції, забезпечуючи безперервну роботу. Ця модель дозволяє навіть проводити технічне обслуговування однієї з систем без переривання послуг. Однак, вартість такого рішення є найвищою, тому воно застосовується лише в критично важливих сферах, таких як авіація або ядерна енергетика, де навіть найменший збій може мати катастрофічні наслідки. Наприклад, у системах управління повітряним рухом, де будь-який збій може призвести до трагічних наслідків, використання 2N є обов'язковим.

Сучасні мережі NGN часто використовують гібридні підходи, комбінуючи різні моделі резервування для досягнення оптимального балансу між надійністю та вартістю. Наприклад, можна використовувати 1+1 для критично важливих компонентів мережі та N+1 для менш важливих.

2.2 Оптимізація QoS для покращення надійності

В умовах сучасного інтернет-трафіку, що включає відеоконференції, потокове мовлення, VoIP-зв’язок, транзакції фінансових систем і критично важливі комунікації, ефективний механізм пріоритезації дозволяє забезпечити стабільність роботи сервісів навіть у разі високого навантаження на мережу. Основними підходами до пріоритезації трафіку є інтегрована модель обслуговування (Integrated Services, IntServ) та диференційована модель обслуговування (Differentiated Services, DiffServ).

IntServ — це модель управління трафіком, яка забезпечує гарантії якості обслуговування через механізм резервування ресурсів. Вона працює за принципом встановлення виділених каналів для окремих потоків трафіку та

використовує протокол RSVP (Resource Reservation Protocol) для бронювання необхідних ресурсів по всьому шляху передачі.

Головним принципом IntServ є те, що кожен потік трафіку реєструється та обробляється окремо, що дозволяє мережі забезпечити жорсткі гарантії QoS. Це особливо важливо для таких застосувань, як VoIP або потокове відео, де затримки та втрати пакетів можуть суттєво вплинути на якість передачі.

Переваги IntServ:

1. Гарантія QoS. Завдяки механізму резервування ресурсів IntServ може забезпечити високий рівень надійності для критично важливих сервісів. Це дозволяє підтримувати стабільний рівень продуктивності для таких застосувань, як відеоконференції, віддалена робота та медичні телекомунікаційні послуги.
2. Чітке управління трафіком. Використання RSVP дозволяє контролювати всі потоки даних і забезпечувати відповідну пропускну здатність. Адміністратори мереж можуть точно прогнозувати навантаження та налаштовувати систему відповідно до потреб користувачів.
3. Мінімізація затримок. Оскільки ресурси виділяються наперед, затримки та джитер зменшуються. Це особливо важливо для реального часу, таких як IP-телефонія та потокове мовлення, де кожна мілісекунда може впливати на якість зв'язку.
4. Високий рівень безпеки. Оскільки кожне з'єднання проходить через процес реєстрації та бронювання ресурсів, IntServ забезпечує додатковий рівень контролю та безпеки для критично важливих додатків.

Недоліки IntServ:

1. Масштабованість. Оскільки кожен окремий потік потребує реєстрації, ця модель погано підходить для великих мереж через надмірну адміністративну складність. У великих інфраструктурах значна кількість потоків може спричинити перевантаження системи керування

мережевими ресурсами, що ускладнює забезпечення ефективного функціонування.

2. Високі витрати на ресурси. Через необхідність резервування смуги пропускання навіть у випадках, коли з'єднання тимчасово не використовується, це може призводити до неефективного використання доступної пропускної здатності. Наприклад, якщо у мережі зарезервовано канал для відеоконференції, а вона наразі не проводиться, ці ресурси не можуть бути використані іншими типами трафіку.
3. Залежність від RSVP. Багато сучасних мереж не підтримують RSVP або використовують інші механізми управління трафіком, що ускладнює інтеграцію IntServ у загальну архітектуру мережі. Крім того, RSVP потребує додаткового обчислювального навантаження на маршрутизатори, що може знижувати їх продуктивність у великих масштабах.
4. Потреба в складному управлінні. Впровадження IntServ потребує ретельного налаштування і постійного моніторингу, оскільки адміністратори повинні враховувати змінні умови навантаження, доступність ресурсів та динаміку мережевого середовища. Це вимагає значних технічних знань і додаткових зусиль з боку IT-персоналу.

DiffServ — це більш гнучка та масштабована модель, яка використовує механізм класифікації трафіку та пріоритезації даних. У цій моделі трафік розподіляється на різні класи, і кожен клас обробляється відповідно до визначених правил. Це дозволяє мережевим пристроям швидко визначати пріоритети без необхідності індивідуального бронювання ресурсів.

У DiffServ використовується поле DSCP (Differentiated Services Code Point) у заголовку IP-пакета, яке визначає рівень пріоритету трафіку. Маршрутизатори та комутатори на основі цього значення визначають, який тип обслуговування надавати пакету.

Основні класи обслуговування в DiffServ:

1. Expedited Forwarding (EF). Найвищий пріоритет трафіку, який використовується для сервісів реального часу, таких як IP-телефонія та потокове відео.
2. Assured Forwarding (AF). Гарантує певний рівень пропускної здатності для конкретних потоків, наприклад, для бізнес-додатків або корпоративного трафіку.
3. Best Effort (BE). Стандартний трафік без спеціальних гарантій, який використовується для звичайного веб-серфінгу, електронної пошти тощо.

Переваги DiffServ:

1. Гнучкість. На відміну від IntServ, ця модель не потребує збереження стану кожного окремого з'єднання.
2. Масштабованість. Оскільки трафік класифікується на рівні окремих класів, а не окремих потоків, DiffServ легко адаптується до великих мереж.
3. Ефективне використання ресурсів. Трафік з низьким пріоритетом не блокує ресурси для критичних сервісів.

Недоліки DiffServ:

1. Відсутність жорстких гарантій QoS. Оскільки DiffServ працює на основі пріоритетів, а не резервування ресурсів, можливе погіршення якості обслуговування в умовах перевантаження мережі.
2. Залежність від налаштувань мережі. Для коректної роботи всі маршрутизатори та комутатори повинні бути налаштовані відповідним чином, що може ускладнити впровадження.

IntServ та DiffServ мають різні підходи до управління трафіком, і вибір між ними залежить від специфіки мережі. IntServ краще підходить для невеликих або спеціалізованих мереж, де потрібні жорсткі гарантії QoS. DiffServ є більш придатним для великих мереж, таких як операторські або корпоративні інфраструктури, де необхідна гнучкість та масштабованість.

Таблиця 2.1 - Порівняння IntServ та DiffServ

Параметр	IntServ	DiffServ
Принцип роботи	Резервування ресурсів	Класифікація трафіку
Масштабованість	Низька	Висока
QoS	Жорсткі гарантії	Відносні гарантії
Гнучкість	Низька	Висока
Основний механізм	RSVP	DSCP

Використання технологій MPLS (Multiprotocol Label Switching) та VPN (Virtual Private Network) дозволяє значно підвищити надійність, продуктивність і стійкість з'єднання в мережах наступного покоління (NGN).

MPLS (Multiprotocol Label Switching) — це технологія комутації пакетів, яка використовує мітки (labels) для швидкого та ефективного маршрутизації трафіку через мережу. Основний принцип роботи MPLS полягає в тому, що замість класичної маршрутизації IP-пакетів за допомогою таблиць маршрутизації, використовується попередньо визначений шлях, яким трафік передається між вузлами. Це значно прискорює передачу даних і підвищує надійність мережі.

Ключові компоненти та принципи роботи MPLS

1. Додавання міток (Label Switching)

Коли IP-пакет входить в MPLS-мережу, його заголовок доповнюється спеціальною міткою (label), яка містить інформацію про те, як цей пакет має бути оброблений у мережі.

Мітка додається на вході в MPLS-мережу спеціальним пристроєм — Label Edge Router (LER).

2. Форвардинг трафіку за мітками

Кожен проміжний маршрутизатор у мережі MPLS — Label Switching Router (LSR) — не аналізує IP-адресу пакета, а лише дивиться на його мітку.

На основі таблиці комутації міток (Label Forwarding Information Base, LFIB) LSR швидко визначає наступний вузол маршруту і замінює поточну мітку на нову.

3. Видалення мітки та передача пакета далі

На виході з MPLS-мережі, мітка видаляється пристроєм egress LER, і пакет передається далі у звичайну IP-мережу.

Основні елементи MPLS

FEC (Forwarding Equivalence Class) – групування трафіку, що отримує однакову обробку. Наприклад, весь трафік VoIP може належати до одного FEC.

LSP (Label Switched Path) – попередньо встановлений маршрут, яким передається трафік через MPLS-мережу.

LDP (Label Distribution Protocol) – основний протокол для розповсюдження міток між маршрутизаторами.

Приклад роботи MPLS

IP-пакет надходить на вхідний маршрутизатор MPLS.

LER додає мітку (наприклад, 100) і передає пакет далі.

Проміжний LSR змінює мітку з 100 на 200 і відправляє пакет далі.

На виході egress LER видаляє мітку, і пакет продовжує шлях у звичайній IP-мережі.

Переваги MPLS

Швидке комутування трафіку завдяки використанню міток замість складної IP-маршрутизації.

Гарантована якість обслуговування (QoS) завдяки гнучкому управлінню пріоритетами трафіку.

Підтримка різних транспортних протоколів (IP, ATM, Frame Relay).

Можливість створення VPN із високим рівнем безпеки.

VPN використовується для створення захищених віртуальних каналів у загальнодоступних або приватних мережах. В умовах NGN VPN допомагає підвищити стійкість з’єднання та захистити передані дані.

Основні типи VPN:

1. PPTP (Point-to-Point Tunneling Protocol) – базовий протокол для створення тунелів між вузлами, проте має слабкий рівень безпеки.
2. L2TP/IPSec (Layer 2 Tunneling Protocol + IP Security) – поєднує переваги тунелювання L2TP та шифрування IPSec, що забезпечує високий рівень безпеки.
3. SSL VPN (Secure Sockets Layer VPN) – використовує SSL для шифрування та створення безпечного каналу зв’язку через веб-браузер.
4. MPLS VPN – об’єднує можливості MPLS і VPN, створюючи ізольовані віртуальні мережі з високою продуктивністю та стійкістю.

Об’єднання технологій MPLS та VPN дозволяє отримати найкращі характеристики щодо надійності та безпеки. MPLS забезпечує швидку маршрутизацію та QoS, а VPN – захист трафіку від несанкціонованого доступу. Наприклад, у корпоративних мережах MPLS VPN використовується для з’єднання віддалених філій, забезпечуючи високошвидкісні, захищені та стійкі з’єднання.

2.3 Захист NGN від атак та збоїв

Методи кібербезпеки та захисту від DDoS-атак є необхідними для забезпечення стабільної роботи інформаційних систем, особливо у великих корпоративних і провайдерських мережах. Вони включають комплекс заходів, що дозволяють запобігти несанкціонованому доступу, виявляти атаки на ранніх стадіях і ефективно реагувати на загрози. Сучасний підхід до кіберзахисту базується на поєднанні апаратних, програмних та організаційних рішень, які разом утворюють багаторівневу систему безпеки.

Основу кібербезпеки становить фільтрація трафіку на рівні маршрутизаторів та міжмережевих екранів. Використання сучасних

брандмауерів дозволяє блокувати підозрілу активність, налаштовувати правила доступу та відстежувати трафік у режимі реального часу. Брандмауери можуть працювати на різних рівнях: мережевому (перевіряючи IP-адреси та порти), транспортному (контролюючи сесії) і прикладному (аналізуючи вміст переданих даних). Додатковий рівень захисту забезпечують системи виявлення та запобігання вторгненням (IDS/IPS), що аналізують поведінкові патерни трафіку, виявляють аномальні запити та автоматично блокують потенційні атаки.

Одним із найбільш небезпечних типів атак є DDoS (Distributed Denial of Service), що спрямовані на виведення з ладу серверів або мережевої інфраструктури шляхом перевантаження їх запитами. Для боротьби з такими загрозами застосовують різні стратегії, починаючи від простого обмеження кількості запитів з одного джерела до складних механізмів аналізу аномалій. Одним із найефективніших методів є використання спеціалізованих рішень для балансування навантаження, які рівномірно розподіляють трафік між кількома серверами, запобігаючи їх перевантаженню.

Ще одним способом протидії DDoS-атакам є чорні та білі списки IP-адрес. Якщо атакуючі сервери або ботнети мають відомі адреси, їх можна заблокувати ще на рівні маршрутизаторів. Однак такий підхід має обмежену ефективність, оскільки зловмисники часто змінюють IP або використовують розподілені атаки через проксі-сервери. Тому більш просунуті рішення включають аналіз поведінки користувачів та автоматичне виявлення шкідливого трафіку за допомогою технологій машинного навчання.

Великі компанії та провайдери часто використовують сервіси митигування атак, які функціонують у хмарних інфраструктурах. Такі сервіси здатні приймати на себе потік шкідливого трафіку, фільтрувати його та передавати тільки легітимні запити. Це дозволяє захищати навіть масштабні системи, що обслуговують велику кількість користувачів. Деякі з найпоширеніших рішень у цій сфері включають Cloudflare, Akamai та Radware, які мають глобальні розподілені мережі для обробки атак.

Крім апаратних і програмних методів, важливу роль відіграє правильна організація політик безпеки всередині компаній. Регулярне оновлення програмного забезпечення, використання сучасних засобів шифрування та багатофакторної аутентифікації зменшує ймовірність успішних атак. Також важливо проводити навчання співробітників щодо безпечного користування мережевими ресурсами, оскільки соціальна інженерія залишається одним із найпоширеніших методів злому.

Захист мереж також включає сегментацію трафіку, що дозволяє ізолювати критичні служби від загальнодоступних ресурсів. Наприклад, внутрішні корпоративні сервери можуть бути недоступними ззовні, що значно ускладнює зловмисникам доступ до конфіденційних даних. Додатково можна застосовувати VPN-тунелі, які шифрують трафік між віддаленими вузлами та запобігають його перехопленню.

Сучасні рішення у сфері кібербезпеки також включають аналіз логів і поведінки користувачів для раннього виявлення підозрілих активностей. Системи Security Information and Event Management (SIEM) збирають та аналізують події в реальному часі, що дозволяє оперативно реагувати на потенційні загрози. Деякі SIEM-рішення інтегруються з автоматизованими засобами реагування (SOAR), що дозволяє швидко блокувати атаки без втручання оператора.

Ефективна стратегія кіберзахисту включає поєднання всіх перелічених методів, оскільки жоден із них не забезпечує абсолютної безпеки. Підхід до захисту має бути динамічним, регулярно переглядатися та адаптуватися до нових загроз, які постійно розвиваються.

У сучасних мережах велика кількість пристроїв, додатків і користувачів генерує значний обсяг подій, які необхідно відстежувати та аналізувати. Завдяки централізованому моніторингу адміністратори можуть виявляти проблеми на ранніх стадіях, запобігати аваріям і оптимізувати роботу інфраструктури.

Одним із ключових аспектів моніторингу є збір та обробка логів з усіх критичних систем. Журнали подій містять інформацію про всі дії, що відбуваються в мережі, включаючи спроби доступу, зміну конфігурацій, використання ресурсів і мережеву активність. Автоматизовані платформи моніторингу аналізують ці дані, шукаючи аномалії, потенційні загрози або збої в обладнанні. Системи Security Information and Event Management (SIEM) поєднують збір логів, кореляцію подій і аналітику загроз, що дозволяє швидко реагувати на небезпечні ситуації.

Моніторинг продуктивності мережі є ще одним важливим напрямком. Він дозволяє відстежувати навантаження на канали зв’язку, використання ресурсів серверів, швидкість обробки запитів і рівень затримок. Наприклад, якщо система реєструє аномальне зростання часу відповіді сервера, це може свідчити про перевантаження або атаку типу DDoS. У такому випадку адміністратори можуть оперативно вжити заходів, розподіливши навантаження або заблокувавши підозрілий трафік.

Автоматизовані засоби управління подіями дозволяють не лише фіксувати проблеми, а й реагувати на них у реальному часі. Інструменти Security Orchestration, Automation, and Response (SOAR) інтегруються з SIEM і забезпечують автоматичне виконання сценаріїв реагування. Наприклад, якщо система виявила підозрілу активність, вона може автоматично заблокувати IP-адресу атакуючого або змінити правила брандмауера. Це значно скорочує час реагування на інциденти та зменшує ризик їхнього негативного впливу.

Окрім мережевого моніторингу, важливе значення має контроль за продуктивністю серверного обладнання та баз даних. Більшість сучасних дата-центрів використовують спеціалізовані платформи для збору показників стану серверів, рівня використання оперативної пам’яті, навантаження на процесори та дискові підсистеми. Якщо спостерігається нестача ресурсів або перегрів обладнання, система може автоматично попередити адміністратора або запустити механізми балансування навантаження.

Системи моніторингу також застосовуються в кібербезпеці для виявлення загроз. Аналіз поведінки користувачів дозволяє виявляти підозрілу активність, таку як багаторазові спроби входу в систему, доступ до конфіденційних даних у неробочий час або нетипові переміщення трафіку в мережі. У таких випадках система може автоматично блокувати обліковий запис або запускати процедуру додаткової перевірки.

Одним із викликів для систем моніторингу є необхідність обробки великого обсягу даних у реальному часі. Для цього використовуються технології потокової аналітики, що дозволяють виконувати кореляцію подій і виявляти аномалії без затримок. Використання алгоритмів машинного навчання допомагає автоматично ідентифікувати потенційні загрози та прогнозувати можливі проблеми.

Ефективне використання систем моніторингу потребує належного налаштування та оптимізації. Недостатньо просто збирати дані — важливо визначити, які метрики є критичними, налаштувати правила кореляції та встановити процедури реагування. Без належної конфігурації навіть найпотужніші системи можуть бути малоефективними, оскільки або не виявлять загроз, або створюватимуть надмірну кількість помилкових сповіщень

Інтеграція систем моніторингу з інструментами управління інцидентами дозволяє покращити координацію дій між різними відділами. Наприклад, якщо система виявляє несправність у дата-центрі, вона може автоматично створити заявку в системі управління IT-інцидентами, сповістити відповідальних інженерів і запустити необхідні процедури для усунення проблеми.

Розвиток хмарних технологій також вплинув на підходи до моніторингу. У великих розподілених системах використовується централізоване керування подіями, що дозволяє отримувати єдине уявлення про стан інфраструктури, незалежно від того, де фізично знаходяться сервери

або користувачі. Це особливо важливо для компаній, які використовують гібридні хмарні рішення або масштабуються на міжнародному рівні.

Загалом, сучасні системи моніторингу та управління подіями дозволяють не лише контролювати стан мережі та обладнання, але й автоматизувати процеси реагування.

2.4 Автоматизація управління мережею

Автоматизація управління мережею стає необхідністю у сучасних інформаційних системах через зростання складності інфраструктури, підвищені вимоги до продуктивності та необхідність мінімізувати час простою. Використання штучного інтелекту (AI) та машинного навчання (ML) дозволяє не лише автоматизувати рутинні операції, але й передбачати можливі відмови, що значно підвищує ефективність управління мережею.

Один із найважливіших аспектів застосування AI та ML у мережевих системах – аналіз великих обсягів даних, що надходять з пристроїв, серверів та програмного забезпечення. Завдяки алгоритмам машинного навчання можна виявляти закономірності в роботі обладнання та прогнозувати можливі збої ще до їхнього виникнення. Наприклад, якщо певний комутатор починає демонструвати підвищену затримку або збільшення кількості помилок у пакетах, система може визначити, що ймовірність його відмови зростає, і попередити адміністраторів про необхідність заміни або профілактичного обслуговування.

Методи глибокого навчання дозволяють аналізувати історичні дані та моделювати сценарії можливих несправностей. Наприклад, нейромережі можуть навчатися на основі попередніх аварійних ситуацій і визначати, які комбінації подій зазвичай передують серйозним проблемам у мережі. Це дозволяє розробляти адаптивні механізми управління, які реагують не лише на очевидні ознаки несправностей, а й на приховані кореляції між різними параметрами мережевого середовища.

Автоматизовані системи, засновані на AI та ML, можуть не тільки прогнозувати відмови, але й самостійно приймати рішення щодо їхнього запобігання. Наприклад, якщо прогнозується перевантаження каналу зв’язку через аномальну активність, система може автоматично перенаправити трафік альтернативними маршрутами або динамічно масштабувати ресурси. Такий підхід особливо ефективний у великих дата-центрах та хмарних середовищах, де необхідно швидко адаптувати інфраструктуру до змін у навантаженні.

Одним із ключових компонентів автоматизованого управління є використання предиктивної аналітики. Вона дозволяє створювати математичні моделі для оцінки стану обладнання та визначення моменту, коли певний компонент наближається до критичного стану. Це дає можливість проводити обслуговування не за фіксованим графіком, а за реальними показниками, що значно зменшує експлуатаційні витрати та підвищує надійність мережі.

Застосування AI також корисне для виявлення аномалій у поведінці мережі. Наприклад, система може помітити, що певний сервер почав споживати більше ресурсів, ніж зазвичай, або що певний сегмент мережі демонструє незвично високу кількість підключень у неробочий час. У таких випадках алгоритми можуть не лише повідомити про потенційну загрозу, але й виконати автоматизовані дії, наприклад, ізолювати підозрілу активність або розподілити навантаження рівномірніше.

Завдяки машинному навчанню можна значно покращити ефективність політик балансування навантаження та управління трафіком. Система може навчатися на основі реальних даних про поведінку користувачів та прогнозувати, які ділянки мережі можуть піддатися піковим навантаженням у майбутньому. Це дозволяє завчасно перерозподіляти ресурси або розгортати додаткові потужності, забезпечуючи стабільність роботи сервісів навіть у найскладніших умовах.

Додатково AI дозволяє автоматизувати управління безпекою мережі, інтегруючись із системами виявлення вторгнень (IDS) та запобігання атакам (IPS). Алгоритми можуть аналізувати трафік у реальному часі та виявляти нетипові шаблони поведінки, що можуть вказувати на загрозу. Наприклад, система може зафіксувати підозрілі запити до певних серверів або виявити ознаки сканування портів та автоматично вжити заходів для їхнього блокування.

Реалізація AI-орієнтованих систем управління мережею потребує відповідної обчислювальної інфраструктури та великих обсягів якісних даних для навчання моделей. Для цього часто використовуються розподілені бази даних та платформи аналітики, які дозволяють у реальному часі обробляти величезні потоки інформації з тисяч пристроїв.

З розвитком технологій AI та ML методи прогнозування відмов стають дедалі точнішими та ефективнішими. Замість реагування на вже виниклі проблеми, мережеві системи починають працювати проактивно, запобігаючи можливим збоям і мінімізуючи ризики для критично важливих сервісів. Це відкриває нові можливості для підвищення продуктивності та стабільності сучасних мережевих інфраструктур

Автоматизовані механізми відновлення працюють на основі аналізу даних у реальному часі. Для цього використовуються спеціальні моніторингові платформи, які безперервно збирають інформацію про стан мережевого обладнання, серверів, програмного забезпечення та каналів зв’язку. Якщо система виявляє аномалії, що свідчать про можливий збій, вона може запустити процедуру відновлення ще до того, як користувачі помітять проблему. Наприклад, якщо виявлено критичне навантаження на сервері або погіршення продуктивності через апаратні несправності, система може автоматично перемістити робочі навантаження на резервний сервер без переривання роботи сервісів.

Одним із ключових підходів до автоматизованого відновлення є використання механізмів резервного копіювання та швидкого відновлення.

Багато сучасних систем включають функції створення знімків стану (snapshots) та реплікації даних у реальному часі. Наприклад, у разі збою бази даних автоматизована система може миттєво переключитися на резервну копію або розгорнути останній робочий знімок, відновлюючи цілісність даних. Використання хмарних сховищ дозволяє зберігати резервні копії у географічно розподілених центрах обробки даних, що захищає інформацію від втрати внаслідок фізичних пошкоджень обладнання або стихійних лих.

Сучасні методи автоматизованого відновлення також включають механізми самовідновлення мережевих з'єднань. Програмно визначені мережі (SDN) дозволяють динамічно змінювати маршрутизацію трафіку у разі збою одного з каналів зв’язку. Наприклад, якщо основний канал зв’язку між дата-центрами виходить з ладу, система може автоматично перенаправити трафік через альтернативний маршрут без втручання адміністратора. Це забезпечує безперервність з’єднання навіть у разі серйозних проблем з інфраструктурою.

Іншим ефективним механізмом є використання контейнеризації та оркестрації додатків. Наприклад, платформи на основі Kubernetes дозволяють автоматично розгортати, масштабувати та відновлювати сервіси у разі їхньої відмови. Якщо один із контейнерів виходить з ладу, система автоматично створює новий екземпляр і перенаправляє до нього запити користувачів. Це особливо важливо для критичних бізнес-додатків, які мають працювати безперервно, незалежно від стану окремих компонентів системи.

Автоматизоване відновлення після збоїв також включає методи прогнозування несправностей. За допомогою AI та ML можна створювати моделі поведінки системи та визначати ознаки можливих проблем ще до їхнього виникнення. Наприклад, алгоритми можуть виявляти поступове погіршення продуктивності мережевого обладнання або аномальні зміни у використанні ресурсів. На основі цих даних система може заздалегідь виконати заходи для запобігання відмові, такі як переведення трафіку на інші пристрої або запуск процесу гарячої заміни серверів.

Ще одним напрямком автоматизованого відновлення є інтеграція з кібербезпековими системами. Випадки кібератак, таких як DDoS-атаки або шкідливе програмне забезпечення, можуть спричинити серйозні збої в роботі інфраструктури. Використання автоматизованих засобів захисту дозволяє не лише виявити атаку, а й динамічно змінювати конфігурацію мережі, блокуючи шкідливий трафік та ізолюючи уражені вузли. Наприклад, система може автоматично перенести критично важливі сервіси у захищене середовище або активувати додаткові ресурси для нейтралізації навантаження.

Для підвищення ефективності автоматизованих механізмів відновлення використовуються розподілені обчислювальні системи та хмарні технології. Наприклад, у гібридних хмарах можна реалізувати стратегію аварійного перемикання (failover), коли сервіси автоматично переходять на резервні потужності у разі виходу з ладу основного середовища. Це дозволяє забезпечити безперервність роботи навіть у разі серйозних технічних проблем, таких як відключення електропостачання або вихід з ладу фізичних серверів.

Важливим аспектом автоматизованого відновлення є управління конфігураціями та оновленнями. У сучасних інфраструктурах використовується інфраструктура як код (Infrastructure as Code, IaC), яка дозволяє автоматично відтворювати потрібну конфігурацію мережі або серверного середовища у разі його порушення. Наприклад, якщо оновлення програмного забезпечення призвело до збою, система може автоматично відкотити зміни до останньої стабільної версії без необхідності ручного втручання.

Розвиток технологій автоматизованого відновлення дозволяє значно знизити ризики, пов’язані зі збоями в IT-інфраструктурі. Завдяки використанню AI, ML, SDN, контейнеризації та хмарних обчислень сучасні мережеві системи можуть швидко адаптуватися до змін і самостійно відновлювати свою працездатність. Це не лише підвищує надійність сервісів,

але й зменшує операційні витрати, оскільки зменшується необхідність у постійному ручному втручанні.

2.5 Висновки до розділу 2

У другому розділі було систематизовано та детально розглянуто сучасні методи і технології, що сприяють підвищенню надійності функціонування мереж наступного покоління (NGN). Встановлено, що забезпечення стабільності й безперервності надання послуг залежить не лише від апаратної надійності, але й від комплексного впровадження логічних і програмних рішень.

Перш за все, розглянуто принципи резервування та моделі відмовостійкості (N+1, 1+1, 2N), які дозволяють суттєво зменшити ризики збоїв і забезпечити відновлення функціонування систем у мінімальні строки. Дублювання маршрутів і ключових елементів інфраструктури, застосування протоколів динамічної маршрутизації та використання MPLS дають змогу знизити ймовірність втрати зв’язку навіть у разі критичних відмов.

У частині оптимізації QoS було детально досліджено моделі пріоритезації трафіку — IntServ і DiffServ. Було виявлено, що інтегрована модель підходить для малих або спеціалізованих мереж, у той час як диференційована модель є придатною для масштабних систем із високою динамікою навантаження. Окрім того, використання MPLS у поєднанні з VPN дозволяє гарантувати як захищеність даних, так і стабільність каналів зв’язку, що є особливо важливим у корпоративних та критично важливих інфраструктурах.

У контексті захисту NGN від атак та збоїв розглянуто системи кібербезпеки, зокрема IDS/IPS, міжмережеві екрани, SIEM, SOAR, VPN-технології, а також хмарні платформи для DDoS-захисту. Продемонстровано, що багаторівнева система безпеки дозволяє не тільки виявляти та блокувати

загрози в режимі реального часу, а й забезпечує централізоване реагування на інциденти.

Завершальним елементом дослідження стало вивчення автоматизації управління мережею та механізмів відновлення. Було показано, що застосування AI/ML для аналізу подій, прогнозування відмов та автоматичного балансування ресурсів дозволяє суттєво скоротити час простою і зменшити операційні витрати. Такі підходи, як інфраструктура як код (IaC), контейнеризація, автоматизоване резервне копіювання і оркестрація служб, підвищують гнучкість і адаптивність NGN до динамічних умов.

Таким чином, підвищення надійності NGN вимагає комплексного поєднання резервування, гнучкого управління якістю обслуговування, високого рівня кіберзахисту та інтелектуальної автоматизації. Реалізація цих підходів дозволяє створити мережу, здатну забезпечувати стійке та прогнозоване надання сервісів незалежно від технічних чи кіберзагроз.

3 МОДЕЛІ ТА МЕТОД ПОКРАЩЕННЯ ПАРАМЕТРІВ QOS В МЕРЕЖІ NGN

3.1 Модель віртуалізованого пакетного маршрутизатора із статичним та динамічним виділенням обчислювальних ресурсів

Різке зростання обсягів мережевого трафіку на фоні повільного розвитку пропускної здатності інфраструктури викликає потребу у пошуку нових рішень для забезпечення належної якості обслуговування. Для цього необхідні програмно-апаратні механізми, що впроваджуються в маршрутизаторах і комутаторах та здатні ефективно керувати ресурсами – такими як буфери, канали передачі, обчислювальні потужності та час реакції.

Одним з перспективних підходів до вирішення цієї задачі є впровадження технологій віртуалізації, які дозволяють створювати в межах одного фізичного маршрутизатора кілька віртуальних, кожен з яких буде відповідати за окремий клас сервісу з власними вимогами до QoS. Ключовою інновацією цієї роботи є розробка моделі віртуального маршрутизатора, що дозволяє ефективно розподіляти ресурси між різними потоками, зокрема – для сервісів реального часу з високими вимогами до затримок і втрат.

Сучасні системи комутації пакетів використовують інтерфейси з високою пропускною здатністю, а продуктивність їх внутрішньої комутаційної матриці може сягати сотень гігабіт за секунду.

Основними вимогами до такого обладнання є підвищення пропускної здатності та вдосконалення інших функціональних характеристик як самих пристроїв, так і всієї мережі. Складність полягає в потребі ефективної підтримки статистичного мультиплексування потоків, що проходять через системи комутації, та одночасному передаванні трафіку різних типів, кожен з яких має свої специфічні вимоги до параметрів роботи мережі.

Типовий маршрутизатор виконує кілька функцій: він приймає пакети, буферизує їх, визначає маршрут, регулює трафік і передає пакети на

відповідні вихідні порти. В загальному випадку, маршрутизація – це процес встановлення зв’язків між кінцевими вузлами через транзитні мережеві елементи, що охоплює:

- ідентифікацію потоків даних;
- визначення маршрутів їх передачі;
- інформування мережевих вузлів про знайдені маршрути;
- локальну комутацію на кожному вузлі;
- процеси мультиплексування/демультиплексування;
- гарантування якості обслуговування (QoS).

Узагальнено, маршрутизатор отримує пакет через один інтерфейс, визначає його адресата, використовуючи таблиці маршрутизації, і пересилає через відповідний вихідний інтерфейс. На відміну від інших комутаційних пристроїв, маршрутизатор будує свої таблиці на основі IP-адрес, тоді як комутатори або мости працюють із MAC-адресами.

Маршрутизатор реалізує дві основні функції: перемикання трафіку і підтримку мережевого середовища. Ці функції можуть виконуватися окремими процесорами або процесами – наприклад, перемикання може реалізовуватись апаратно або через процедури обробки переривань ядра, а підтримка середовища – фоновими службами.

Забезпечення QoS охоплює такі задачі, як класифікація трафіку, його пріоритезація, обмеження інтенсивності, управління чергами, а також маршрутизація з урахуванням вимог до затримок, втрат і пропускної здатності.

Розподіл каналів між потоками здійснюється через впорядкування обслуговування пакетів і побудову черг. Черги є ділянками пам’яті для зберігання пакетів з однаковим пріоритетом, а їх обробка регулюється обраними алгоритмами.

FIFO (First In – First Out) є найпростішим механізмом обслуговування, за яким пакети передаються на вихід у порядку, в якому вони надійшли на вхід. Він є алгоритмом за замовчуванням у всіх пристроях з комутацією

пакетів. Переваги: простота реалізації та відсутність конфігурування. Недолік: неможливість диференційованої обробки пакетів різних потоків.

Інший підхід – пріоритетна черга (Priority Queuing, PQ), припускає наявність вихідних під черг з високим, середнім, і низьким пріоритетом обслуговування. У межах черги пакети обробляються за FIFO. Пріоритетне обслуговування черг забезпечує високу якість обслуговування та мінімальний рівень затримок пакетів із черги з найвищим пріоритетом. Недоліки: необхідність ретельного контролю трафіку на етапі доступу в мережу з метою належного надання пріоритету; відсутність верхньої межі для кожного з рівнів пріоритету; високий ризик придушення низько пріоритетних потоків потоками з найвищим пріоритетом.

У контексті NGN-мереж (Next Generation Network) віртуалізація мережевих пристроїв набуває ключового значення. Це означає, що на одному або декількох фізичних пристроях можуть одночасно працювати кілька віртуальних елементів, кожен з яких виконує роль незалежного маршрутизатора для обслуговування трафіку певного типу.

З метою спрощення моделювання, розглядається сценарій, у якому обробляються три типи трафіку – голосовий, відео та дані, тобто сервіси типу "Triple Play". Для кожного з цих типів створюється окремий віртуальний маршрутизатор, що дозволяє виділити для кожного потоку специфічні апаратні ресурси відповідно до його потреб у якості обслуговування.

На вхід такого пристрою надходить агрегований трафік, що складається з трьох незалежних потоків. Цей трафік аналізується класифікатором на основі полів DSCP або ToS в IP-заголовках. Відповідно до значення цих полів, кожен пакет спрямовується до одного з трьох віртуальних маршрутизаторів. Такий підхід подібний до механізму пріоритетного обслуговування черг, однак реалізується на рівні розділення фізичних обчислювальних ресурсів.

Ключовим параметром, що впливає на формування черг і затримки, є ступінь завантаження віртуального пристрою. Це співвідношення між

середньою інтенсивністю трафіку, що надходить, і здатністю маршрутизатора обробляти цей трафік (в моделі позначається як TSi – середній час обробки пакета і-го потоку).

Перевага такої архітектури полягає у гнучкості керування – за допомогою менеджера ресурсів можна як статично, так і динамічно перерозподіляти ресурси (процесорні, пам’ять, пропускну здатність) між віртуальними маршрутизаторами згідно з поточними вимогами до QoS.

Таким чином, запропонований підхід до забезпечення якості обслуговування в NGN-вузлах полягає в динамічному управлінні обчислювальними ресурсами на основі рівня навантаження кожного пріоритетного класу трафіку, а також відповідності поточних показників встановленим нормативам.

Система управління виконує дві основні функції:

- періодичне вимірювання параметрів якості обслуговування (затримки, втрати для різних класів трафіку);
- автоматичне коригування обчислювальних ресурсів віртуальних маршрутів у відповідь на зміни навантаження.

3.2 Представлення параметрів якості обслуговування віртуальної інфраструктури

Розглянемо формальне представлення параметрів якості обслуговування в мережевому вузлі NGN, що підтримує віртуалізацію. Припустимо, що загальна пропускна здатність вузла дорівнює C, а обсяг буферної пам’яті – Q. Для аналітичного опису введемо такі змінні:

a(t) — обсяг вхідного трафіку на момент часу t;

l(t) — кількість відкинутого трафіку в цей самий момент;

r(t) — швидкість обслуговування на часі t.

Також використаємо поняття кривих прибуття та обслуговування, що описують обсяг даних у часовому проміжку $[t_1,t_2]$:

$$\int_{t_1}^{t_2} a(t)dt$$

Крива прибуття: $A(t_1,t_2)$ =

Вхідна крива: $Rin(t_1,t_2) = A(t_1,t_2) - \int_{t_1}^{t_2} l(t)dt$

Вихідна крива: $Rout(t_1,t_2) = \int_{t_1}^{t_2} r(t)dt$

Для подальшого спрощення запису приймемо:

$A(t) = A(0,t)$

$Rin(t) = Rin(0,t)$

$Rout(t) = Rout(0,t)$

Графічно ці залежності можна зобразити на часовій осі у вигляді кривих, де вертикальна відстань між Rin(t) та Rout(t) відображає довжину черги Q(t), а горизонтальна – затримку D(t). Відповідно, маємо такі формули:

Довжина черги:

$Q(t) = Rin(t) - Rout(t)$

Затримка:

$$D(t) = \max_{s \le t}\{s : Rin(s) \le Rout(t)\}$$

Середня затримка за інтервал часу T:

$$\overline{D} = \frac{1}{T}\int_0^T D(t)dt$$

Інтенсивніст втрат P(t):

$$P(t) = \frac{\int_{t_0}^{t} l(x)dx}{\int_{t_0}^{t} a(x)dx}$$

Тобто, ці формули дозволяють кількісно оцінювати якість обслуговування віртуальних маршрутизаторів, зокрема – затримку, довжину черги та втрати пакетів.

3.3 Покращення параметрів QoS на основі методу адаптивного управління структурними параметри віртуальних маршрутизаторів

В NGN-мережах важливу роль відіграє здатність гнучко адаптувати ресурси у відповідь на зміну характеристик трафіку. Методи управління

мережею передбачають можливість динамічного налаштування параметрів обслуговування залежно від рівня вхідного навантаження, яке генерується прикладними сервісами.

Однак, більшість підходів фокусуються на реактивному керуванні, не враховуючи задач планування мінімального набору ресурсів, необхідного для забезпечення гарантованих QoS. Це створює потребу в методах, які дозволяють визначати найменший можливий обсяг ресурсів для досягнення встановлених рівнів обслуговування.

Наприклад, імовірність втрати пакету у мережі розглядається як сума втрат у каналі та у вузлах. Через те, що сучасні канали передачі (зокрема ВОЛЗ) мають мізерну ймовірність помилок (~10^{-9}), основна частина втрат зумовлена саме перевантаженнями в вузлах мережі. Для віртуальних маршрутизаторів це можна формалізувати так:

Ймовірність втрат у віртуальному маршрутизаторі:

$$P = \frac{X_{ki}}{X}$$

де:

X — загальна кількість пакетів, що надійшли,

X_{ki} — кількість втрачених пакетів у і-му маршрутизаторі за період k.

Затримка в обслуговуванні:

$t = \frac{L}{C}$ + $t_{буфер}$ + $t_{обробки}$

де:

$L_{пак}$ — довжина пакета

$C_{інтерфейсу}$ — пропускна здатність інтерфейсів

$t_{буфер}$ — час очікування в черзі

$t_{обробки}$ — час обробки пакета процесором маршрутизатора

Джиттер (мінливість затримки):

$dt_i = | t_{ji} - t_{average} |$

Ці параметри можуть варіюватися в часі, і саме тому віртуальні маршрутизатори повинні мати механізми адаптивного управління - змінювати обчислювальні ресурси відповідно до поточних QoS-вимог:

Управління буфером:

$$\sum_i q_i \leq Q$$

Де q_i — розмір буфера і-го віртуального маршрутизатора.

Критерії розподілу ресурсів:

$t_{\text{поточне,і}} \leq T_{\text{допустиме,і}}$

$p_{\text{поточне,і}} \leq P_{\text{допустиме,і}}$

$dt_{\text{поточне,і}} \leq dT_{\text{допустиме,і}}$

Обчислювальні ресурси:

$$CPU_i \leq CPU, \quad RAM_i \leq RAM$$

Таким чином, при віртуалізації мережевого вузла параметри кожного віртуального елемента підлягають контролю, адаптації та оптимізації згідно зі змінами навантаження.

Дослідження властивостей інформаційних потоків у мультисервісних телекомунікаційних мережах засвідчують, що самоподібні моделі найточніше відображають реальну поведінку трафіку. Потоки даних у NGN характеризуються довготривалими залежностями, високою нерівномірністю та відхиленнями від класичних моделей, як-от пуассонівський розподіл.

У таких мережах трафік формується з різних сервісів, які мають власні параметри передавання — середню та пікову швидкість, структуру пакетів тощо. У результаті, виникає явище «пачкування» (burstiness) — коли пакети надходять у короткі, інтенсивні сплески, чергуючись із періодами низької активності. Це призводить до значної дисперсії інтенсивності, яка часто у десятки разів перевищує її середнє значення.

У віртуалізованих NGN-мережах фізична топологія трансформується у віртуальну однофункціональну інфраструктуру, де кожен тип трафіку (наприклад, голосовий) обробляється окремим віртуальним

маршрутизатором. Це спрощує процес моделювання, адже ми маємо справу з потоками з однаковими властивостями.

Незважаючи на це, адекватне моделювання все ще потребує точного врахування численних параметрів:

- кількості інтерфейсів (вхідних/вихідних);
- можливості паралельної або пріоритетної обробки;
- швидкодії шини та процесора;
- обсягу буфера;
- ймовірності втрат при перевантаженнях.

Тому створення моделі обслуговуючого пристрою повинно супроводжуватись верифікацією кожного елемента — з урахуванням технологічних допусків і реальних характеристик.

Наприклад, для адаптивного управління буферною пам’яттю застосовується модель, в якій обсяг черги змінюється згідно з поточною ситуацією:

$$\sum_{i=1}^{n} q_{\text{черги}_i} \leq Q_{\text{буф}},$$

Для кожного віртуального маршрутизатора обсяг буфера, частота процесора і обсяг оперативної пам’яті мають задовольняти встановлені граничні значення, при яких забезпечується:

- допустимий рівень затримок;
- мінімальні втрати пакетів;
- контрольований рівень джитера

Трафік, що передається в NGN мережах з комутацією пакетів, має довгострокові залежності в інтенсивності та ще більш суттєво відрізняється від пуассонівського потоку і навіть будь-яких інших потоків, що визначаються одномірною функцією розподілу ймовірності інтервалу часу між моментами надходження пакетів. Більш адекватною моделлю потоків у таких мережах є самоподібні процеси, проте дослідження характеристик якості обслуговування систем розподілу інформації в цих умовах є дуже складною математичною задачею. У мультисервісних пакетних мережах

трафік є різнорідним і з певними вимогами до QoS. Тут передачу потоків різних служб забезпечує одна і та ж сама мережа з єдиними протоколами та законами управління. Через те, що джерела кожної служби можуть мати різні швидкості передавання інформації та змінювати її в процесі сеансу зв‘язку (максимальна та середня швидкості), то об‘єднаному потоку пакетів властиве так зване «пачкування» трафіка (burstness), вимірюване коефіцієнтом пачкування. Це пачкування обумовлює ще більшу нерівномірність трафіка, за якої дисперсія інтенсивності трафіка перевищує її математичне сподівання від 20 до 60 разів і більше.

При розгортанні віртуальних маршрутизаторів топологія фізичної NGN мережі стає віртуальною моносервісною. Це в свою чергу дає змогу, спростити розв‘язок задачі побудови адекватної математичної моделі вхідного потоку в моносервісних мережах з однорідним трафіком. Такими, наприклад, є суто телефонні мережі з єдиною послугою телефонного зв‘язку, що й зумовлює однорідність трафіка.

Найбільш важливим є питання забезпечення параметрів якості сервісу вузлом. Змінюючи параметри структурно-функціональної моделі обслуговуючого вузла, можемо спостерігати за змінами кількісних та часових параметрів якості обслуговування. Завдання планування ресурсів зводиться до вибору параметрів структурно-функціональної моделі вузла обслуговування, які забезпечують дотримання бажаних (заданих, необхідних) часових та кількісних параметрів якості обслуговування.

Для трьох типів трафіку (голосового, відео, даних) було проведено розрахунки середньої затримки, імовірності втрати пакетів та завантаження ресурсу маршрутизатора. Припускаємо, що трафік надходить зі сталими інтенсивностями λ (голос – 180 п/с, відео – 90 п/с, дані – 60 п/с), середня довжина пакета 1500 біт, пропускна здатність лінка 100 Мбіт/с (що значно перевищує сумарний вхідний потік), та буфер маршрутизатора $Q_{max}=1000$ пакетів. У статичному режимі час обробки одного пакету фіксований (0,5 мс), що дає сервісну швидкість $\mu = 2000$ пак/с. У динамічному режимі

передбачається можливість адаптації ресурсів: ми моделюємо приклад, де голосовий трафік обробляється швидше (0,25 мс ≈ 4000 пак/с), відеотрафік – зі швидкістю 0,5 мс (2000 пак/с), а трафік даних – повільніше (1,0 мс ≈ 1000 пак/с), відповідно до вимог пріоритетності.

Голосовий трафік

Коефіцієнт завантаження процесора

$$\rho = \frac{\lambda}{\mu} = \begin{matrix} \frac{180}{2000} = 0{,}09 \\ \frac{180}{4000} = 0{,}045. \end{matrix}$$

Середня довжина черги

$$Lq = \frac{\rho 2}{2(1-\rho)} = \begin{matrix} \frac{0{,}092}{2(1-0{,}09)} \approx 0{,}0044 \\ \frac{0{,}0452}{2(1-0{,}045)} \approx 0{,}00106 \end{matrix}$$

Середній час очікування в черзі

$$Wq = \frac{Lq}{\lambda} = \begin{matrix} \frac{0{,}00445}{180} = 2{,}47 \times 10 - 5\ \text{с} = 0{,}0247\ \text{мс} \\ \frac{0{,}00106}{180} = 5{,}89 \times 10 - 6\ \text{с} = 0{,}00589\ \text{мс} \end{matrix}$$

Повний час перебування пакета в системі

$$D = Wq + \frac{1}{\mu} = \begin{matrix} 0{,}0247 + 0{,}500 = 0{,}525\ \text{мс} \\ 0{,}00589 + 0{,}250 = 0{,}256\ \text{мс} \end{matrix}$$

Ймовірність втрати

$$Pl_{oss} \approx (1-\rho)\rho^{Qmax} \Rightarrow \rho^{1000} \leq e^{-1000(1-\rho)} \ll 10^{-400}$$

тобто практично нульова в обох режимах.

Завантаження CPU

$$U = \rho \cdot 100\% = \begin{matrix} 0{,}09 \cdot 100 = 9\% \\ 0{,}045 \cdot 100 = 4{,}5\% \end{matrix}$$

для голосового трафіку, який характеризується найжорсткішими вимогами до параметрів якості обслуговування, впровадження динамічного розподілу ресурсів забезпечує майже дворазове скорочення повного часу перебування пакета в системі (0,256 мс проти 0,525 мс у статичному режимі) за рахунок збільшення сервісної швидкості процесора з 2000 до 4000 пак/с, що, у свою чергу, знижує коефіцієнт завантаження CPU з 9 % до 4,5 % і

мінімізує середню довжину черги до незначного рівня $1{,}06 \cdot 10^{-3}$ пакета; таким чином, динамічне керування дозволяє не лише гарантувати дотримання нормативів ITU-T щодо прийнятної затримки та джиттера для сервісів VoIP (≤ 150 мс енд-то-енд), а й створює резерв обчислювальних потужностей для обробки пікових навантажень без ризику перевищення порогових значень, водночас зберігаючи нульову ймовірність втрат завдяки достатньому буферу, що робить запропоновану модель особливо ефективною для підтримки стабільної якості мовних з'єднань у мультисервісних NGN-мережах.

Відеотрафік

Час обслуговування одного пакета дорівнює $t_{serv} = 0{,}5$ мс $= 0{,}0005$ с

Сервісна швидкість — це кількість пакетів, які процесор здатен обробити за секунду:

$$\mu = \frac{1}{t_{serv}} = 2000 \text{ пак/с}$$

Для відеопотоку середня інтенсивність прибуття $\lambda = 90$ пак/с

Коефіцієнт завантаження процесора

$$\rho = \frac{\lambda}{\mu} = 0{,}045$$

Середня довжина черги

$$L_q = \frac{\rho^2}{2(1-\rho)} = 0{,}045^2 / 2 \cdot 0{,}955 = 0{,}002025 / 1{,}91 \approx 0{,}00106 \text{ пакета}$$

Середній час очікування в черзі

$$W_q = L_q/\lambda \approx 1{,}18 \times 10^{-5} \text{ с} = 0{,}0118 \text{ мс}$$

Повний час перебування пакета в системі

$$D = W_q + \frac{1}{\mu} = 0{,}0000118\text{с} + 0{,}0005\text{с} = 0{,}0005118\text{с} \approx 0{,}512 \text{ мс}$$

Ймовірність втрати пакета

При великому буфері

Q_{max} = 1000 та малому завантаженні

$$Pl_{oss} \approx (1-\rho)\rho^{Q_{max}} \Rightarrow (1-0{,}045)0{,}045^{1000} \approx 0$$

отже втрати практично відсутні.

Процесорне навантаження у відсотках

$$U = \rho \times 100\% = 0{,}045 \times 100\% = 4{,}5\%$$

Для відеотрафіку, що надходить із середньою інтенсивністю $\lambda = 90$ пак/с і обслуговується маршрутизатором із незмінним часом сервісу t_serv = 0,5 мс, сервісна швидкість становить $\mu = 1000 / 0{,}5 = 2000$ пак/с; отже, коефіцієнт завантаження процесора дорівнює $\rho = \lambda / \mu = 90 / 2000 \approx 0{,}045$, а відтак середня довжина черги M/D/1 обчислюється за формулою $L_q = \rho^2 / [2 (1 – \rho)] = 0{,}045^2 / [2 (1 – 0{,}045)] \approx 1{,}06 \cdot 10^{-3}$ пакета; поділивши цей результат на інтенсивність, отримуємо середній час очікування $W_q = L_q / \lambda \approx (1{,}06 \cdot 10^{-3}) / 90 \approx 1{,}18 \cdot 10^{-5}$ с = 0,0118 мс, після чого повний час перебування пакета в системі становить $D = W_q + 1/\mu = 0{,}0118 + 0{,}5 \approx 0{,}512$ мс; ймовірність втрати, яку у разі великого буфера Q_max = 1000 оцінюємо наближенням P_loss ≈ (1 – ρ) ρ^{Q_max}, наближається до нуля, а завантаження ЦП у відсотках дорівнює $U = \rho \cdot 100 \approx 4{,}5$ %, тобто навіть без динамічної оптимізації система підтримує затримку на рівні півмілісекунди та практично нульові втрати.

Трафік даних

Розглядаються дві конфігурації: статичний і динамічний режими обслуговування

Статичний режим

Сервісна швидкість процесора

$$\mu = \frac{1}{\text{tstat}} = 2000 \text{ пак/с}$$

Коефіцієнт завантаження

$$\rho = \frac{\lambda}{\mu} = 0{,}03$$

Середня довжина черги

$$Lq = \frac{\rho 2}{2(1-\rho)} = 0{,}03^2 / 2(1-0{,}03) = 0{,}0009 / 2 \cdot 0{,}97 \approx 4{,}64 \times 10^{-4} \text{ пак}$$

Середній час очікування у черзі

$$Wq = Lq/\lambda \approx 4{,}64 \times 10^{-4} / 60 \text{ с} = 7{,}73 \times 10^{-6} \text{ с} = 0{,}0077 \text{ мс}$$

Повний час перебування пакета

$$D = Wq + \frac{1}{\mu} = 0{,}00000773c + 0{,}0005c = 0{,}00050773c \approx 0{,}508 \text{ мс}$$

Завантаження ЦП у відсотках

$$U = \rho \times 100\% = 0{,}03 \times 100\% = 3\%$$

Динамічний режим

Сервісна швидкість процесора

$$\mu = \frac{1}{tstat} = 1000 \text{пак/с}$$

Коефіцієнт завантаження

$$\rho = \frac{\lambda}{\mu} = 0{,}06$$

Середня довжина черги

$$Lq = \frac{\rho 2}{2(1-\rho)} = 0{,}06^2 / 2(1-0{,}06) \approx 1{,}92 \times 10^{-3} \text{ пак}$$

Середній час очікування у черзі

$$Wq = Lq/\lambda = 3{,}19 \times 10^{-5} \text{ с} = 0{,}0319 \text{ мс}$$

Повний час перебування пакета

$$D = Wq + \frac{1}{\mu} = 0{,}0000319c + 0{,}001c = 0{,}0010319c \approx 1{,}032\text{мс}$$

Завантаження ЦП у відсотках

$$U = \rho \times 100\% = 0{,}06 \times 100\% = 6\%$$

Ймовірність втрати пакета

Для обох режимів, через великий буфер Q_{max} = 1000 та малі значення ρ, використовують експоненціальну оцінку:

$$Pl_{oss} \approx (1-\rho)\rho^{Qmax}$$

Оскільки ρ^{1000} для ρ=0,03 або 0,060 дає величину порядку 10^{-600} і менше, втрати практично відсутні

Для трафіку даних, де інтенсивність дорівнює λ = 60 пак/с, маємо дві конфігурації: у статичному режимі час сервісу такий самий, як і для інших потоків (t_serv = 0,5 мс), отже μ_static = 2000 пак/с і ρ_static = 60 / 2000 = 0,03; підставляючи це значення у формулу L_q, отримаємо L_q_static = $0{,}03^2$ / [2 (1 – 0,03)] ≈ $4{,}64 \cdot 10^{-4}$ пакета, що дає час очікування W_q_static = ($4{,}64 \cdot 10^{-4}$) / 60 ≈ $7{,}73 \cdot 10^{-6}$ с = 0,0077 мс і кінцеву затримку D_static = 0,0077 + 0,5

≈ 0,508 мс; процесор завантажений лише на U_static = 3 %. У динамічному режимі ресурси спрямовуються на пріоритетні потоки, тому для даних задаємо подовжений час сервісу t_serv = 1,0 мс, що знижує сервісну швидкість до μ_dyn = 1000 пак/с і збільшує коефіцієнт завантаження до ρ_dyn = 60 / 1000 = 0,06; далі розрахунок дає L_q_dyn = 0,06² / [2 (1 – 0,06)] ≈ 1,92 · 10^{-3} пакета, W_q_dyn = (1,92 · 10^{-3}) / 60 ≈ 3,19 · 10^{-5} с = 0,0319 мс, а повна затримка підвищується до D_dyn = 0,0319 + 1,0 ≈ 1,032 мс; завантаження процесора зростає до U_dyn = 6 %, проте ймовірність втрат залишається практично нульовою завдяки великому буферу, а одержана затримка усе ще значно нижча за критичні для небажчого до затримки IP-трафіку межі.

Отже, проведене порівняльне моделювання функціонування віртуалізованого маршрутизатора у статичному та динамічному режимах підтвердило, що застосування адаптивного розподілу обчислювальних ресурсів є доцільним насамперед для сервісів реального часу з високими вимогами до затримки. Дійсно, за рахунок скорочення середнього часу обслуговування голосових пакетів удвічі (з 0,5 мс до 0,25 мс) динамічний режим забезпечує зменшення повного часу перебування пакета у системі з 0,525 мс до 0,256 мс та зниження середньої довжини черги більш ніж у чотири рази, одночасно майже удвічі розвантажуючи процесор (4,5 % проти 9 %). Для відеотрафіку, чия сервісна швидкість залишилась незмінною, характеристики QoS збереглись на рівні ~0,51 мс, що свідчить про відсутність негативного впливу перерозподілу ресурсів на потоки із середнім пріоритетом.

Що стосується даних, то штучне зниження швидкості обробки до 1 мс призвело до зростання затримки лише до 1,032 мс, що, з огляду на нечутливість більшості застосунків до таких величин, не виходить за межі допустимого, тоді як збільшення завантаження процесора до 6 % є статистично незначним і не загрожує стабільності системи. В усіх сценаріях сумарний коефіцієнт завантаження залишався далеким від порогових значень

($\rho_\Sigma \leq 0{,}06$), а величезний буфер (1000 пакетів) практично нівелював імовірність втрат, що забезпечує відповідність вимогам ITU-T G.1010 щодо енд-то-енд-затримок і відсутності деградації мовних та відеосервісів. Таким чином, запропонована модель динамічного керування ресурсами доводить свою ефективність: вона мінімізує затримку критичного трафіку, не погіршуючи показників сервісів із нижчим пріоритетом, забезпечує економне використання процесорних потужностей і створює необхідний резерв для обробки пікових навантажень, що у сукупності робить її практично придатним інструментом підвищення QoS у мультисервісних мережах наступного покоління.

3.4 Висновки до розділу 3

У третьому розділі було проведено теоретичне моделювання процесів, пов’язаних із забезпеченням якості обслуговування (QoS) в мультисервісних мережах наступного покоління NGN з використанням віртуалізованих маршрутизаторів. Особливу увагу приділено моделі, що передбачає поділ ресурсів між різними типами трафіку — голосовим, відео та даними — відповідно до їхніх специфічних вимог до затримки, втрат і джитера.

У результаті було запропоновано архітектуру віртуального маршрутизатора з можливістю як статичного, так і динамічного розподілу обчислювальних ресурсів між віртуальними інстанціями, що відповідають за обробку трафіку кожного окремого класу. Показано, що при динамічному керуванні процесорними ресурсами можна суттєво знизити середню затримку пакетів, скоротити довжину черги та зменшити завантаження CPU для найкритичніших до затримки потоків (насамперед VoIP).

Проведено формалізацію параметрів QoS у вигляді кривих прибуття та обслуговування, розраховано математичні показники: середню затримку, довжину черги, ймовірність втрати пакетів і завантаження процесора для кожного з трьох типів трафіку. Результати чисельного моделювання

підтвердили, що запропонована система адаптивного управління ресурсами є ефективною для обробки змішаного трафіку у віртуалізованих NGN-вузлах навіть за умови високої burst-активності (пачкування) та самоподібності вхідних потоків.

Також обґрунтовано доцільність використання моделей з динамічно змінними параметрами обслуговування відповідно до класу сервісу. Це дозволяє забезпечити гарантовані параметри якості без надлишкового виділення ресурсів, тобто з максимально ефективним їх використанням. Усі результати демонструють відповідність нормативам ITU-T та реальним вимогам до затримки в голосових і відеосервісах.

Таким чином, розроблена модель обробки трафіку у NGN-мережі підтверджує свою практичну придатність для підвищення QoS через інтелектуальне управління обчислювальними ресурсами маршрутизаторів. Отримані висновки можуть слугувати основою для подальших робіт у напрямку автоматизованого розподілу ресурсів у хмарних і віртуалізованих мережевих середовищах.

ВИСНОВКИ

У ході виконання дипломної роботи було здійснено всебічний аналіз архітектурних особливостей мереж наступного покоління (NGN) та виокремлено ключові чинники, що визначають їхню надійність. Зокрема, встановлено, що конвергентна модель, у якій розділено функції управління й транспорту, забезпечує гнучкість масштабування та підвищену стійкість до відмов, проте водночас породжує потребу в розвинутій системі контролю якості обслуговування (QoS) і віртуалізації мережевих ресурсів. Це дозволяє операторам швидко адаптуватися до динаміки трафіку, однак потребує від них впровадження додаткових методик моніторингу та автоматичного управління, щоб уникнути перевантажень і простоїв.

Другий важливий результат дослідження полягає у класифікації факторів, що негативно впливають на безперервність надання послуг у NGN: відмови апаратних компонентів, збої програмного забезпечення, навантаження пікових потоків та кібератаки. Було доведено, що показники MTBF, MTTR та Availability є ключовими метриками для оцінки загального стану мережі, а також обґрунтовано необхідність використання буферизації, FEC та адаптивного управління затримками й джитером для підтримки вимог реального часу.

У розділі, присвяченому способам підвищення надійності, було розглянуто класичні схеми резервування (N+1, 1+1, 2N) і механізми автоматичного переключення маршрутів з використанням протоколів OSPF, BGP та технології MPLS. Порівняльний аналіз моделей показав, що комбінування різних підходів (наприклад, 1+1 для критично важливих вузлів та N+1 для другорядних) дозволяє досягти балансу між ефективністю використання ресурсів і швидкістю відновлення послуг. Окрім того, доведено, що інтеграція VPN і шифрування підвищує стійкість до кібератак,

а системи IDS/IPS у поєднанні з хмарними сервісами митигування DDoS забезпечують захист від масованих атак.

Четвертий розділ присвячений оптимізації QoS через моделі IntServ та DiffServ і їхньому впровадженню в NGN. Було підтверджено, що протокол RSVP із жорстким резервуванням ресурсів доцільний для невеликих або спеціалізованих мереж із високими вимогами до затримок, тоді як DiffServ із DSCP-маркуванням краще підходить для великих операторських систем завдяки масштабованості та гнучкості. Надалі показано, як застосування MPLS-маршрутизації спільно з VPN дозволяє гарантувати потрібний рівень продуктивності та безпеки на всіх етапах передачі трафіку.

У підсумку, сформульовано практичні рекомендації для операторів і корпоративних замовників: поєднувати резервування різного рівня з адаптивними механізмами QoS, інтегрувати системи автоматичного моніторингу та аналізу збоїв, використовувати хмарні сервіси для захисту від DDoS і забезпечувати постійну актуалізацію ПЗ. Перспективами подальших досліджень є розробка алгоритмів машинного навчання для прогнозування збоїв і динамічного перерозподілу ресурсів у режимі реального часу, що зробить мережі NGN ще більш витривалими та ефективними.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антонів О. М., Стеля Д. О. Організація передачі пакетів мультимедійного трафіку в локальних обчислювальних мережах з гарантованою якістю обслуговування (QoS) // Інтелектуальні інформаційні технології сучасності: тези доп. наук.-практ. семінару (м. Львів, 26 квітня 2024 року) / Наук.-досл. ін-т інфокомунікацій ДУІТЗ. Львів: НДІІ ДУІТЗ, 2024. С. 37.
2. Будім А., Березко Л. О. Мультисервісна мережа NGN кампусу університету // 76-та Студентська науково-технічна конференція: збірник тез доповідей. Львів: Видавництво Львівської політехніки, 2018. С. 184–185.
3. Горішний О. Ю. Створення захищеної корпоративної інфраструктури на основі гіпервізора VMware ESXi : бакалаврська кваліфікаційна робота. Львів, 2024. 54 с.
4. Довбня В. С. Доцільність використання NGN мереж. URL: https://repository.kpi.kharkov.ua/server/api/core/bitstreams/4214e321-2d1a-4ec1-b225-a5b62fafe8db/content
5. Одарченко Р., Іванова М., Рябенко М. Метод аналізу взаємозалежностей параметрів QoE та QoS на основі алгоритмів машинного навчання // Наукоємні технології. 2022. Т. 56, № 4. – С. 305–316.
6. Харченко Т. П., Правило В. В. Якість обслуговування (QoS) в LTE // Перспективи телекомунікацій : міжнар. наук.-техн. конф. 2018. С. 71–74.
7. Янченков О. С. Програмне забезпечення для побудови сенсорної мережі на основі Raspberry Pi : кваліфікаційна робота. Київ : НАУ, 2022. 43 с.

8. Aggarwal P. Neural architectures for secure data transmission in next-gen networks // 2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG). 2023. P. 1–6.
9. Chocron E., Cohen I., Feigin P. Delay prediction for managing multiclass service systems: An investigation of queueing theory and machine learning approaches // IEEE Transactions on Engineering Management. 2022. Vol. 71. P. 4469–4479.
10. Gupta U., Pantola D., Bhardwaj A., Singh S. P. Next-generation networks enabled technologies: challenges and applications // In: Next generation communication networks for industrial internet of things systems. 2022. P. 191–216.
11. Hamdi M. M. et al. Performance evaluation of quality of service (QoS) by using hybrid algorithms in VANETs // 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA). IEEE, 2022. P. 1–7.
12. Hayyolalam V., Otoum S., Özkasap Ö. Dynamic QoS/QoE-aware reliable service composition framework for edge intelligence // Cluster Computing. – 2022. Vol. 25, No. 3. P. 1695–1713.
13. Kakooei S. et al. Application of queuing theory and simulation model to reduce waiting time in dental hospital // Journal of Oral Health and Oral Epidemiology. 2022. Vol. 11, No. 3. – P. 140–145. URL: https://johoe.kmu.ac.ir/article_92034.html
14. Kondratyeva A. et al. Characterization of dynamic blockage probability in industrial millimeter wave 5G deployments // Future Internet. 2022. Vol. 14, No. 7. Article ID: 193.
15. Milan A. A., Fernandes N. C., Medeiros D. S. A Monte Carlo approach for antenna blocking probability estimation in mobile networks // 2022 25th Conference on Innovation in Clouds, Internet and Networks (ICIN). IEEE, 2022. P. 146–150.

16. Pham Q. V. et al. Swarm intelligence for next-generation networks: Recent advances and applications // Journal of Network and Computer Applications. 2021. Vol. 191. Article ID: 103141. URL: https://www.sciencedirect.com/science/article/pii/S1084804521001582
17. Pourvaziri H. et al. Planning of electric vehicle charging stations: An integrated deep learning and queueing theory approach // Transportation Research Part E: Logistics and Transportation Review. 2024. Vol. 186. Article ID: 103568.
18. Rana S. O. H. A. I. L. et al. Deployment of NGN architecture for network services // Journal of Hunan University Natural Sciences. 2023. Vol. 60, No. 2. P. 16–28.
19. Rece L. et al. Queueing theory-based mathematical models applied to enterprise organization and industrial production optimization // Mathematics. 2022. Vol. 10, No. 14. Article ID: 2520.
20. Said O. Design and performance evaluation of QoE/QoS-oriented scheme for reliable data transmission in Internet of Things environments // Computer Communications. 2022. Vol. 189. P. 15174.
21. Saleh A. K. et al. Quality of service (QoS) comparative analysis of wireless network // INAJEEE (Indonesian Journal of Electrical and Electronics Engineering). 2022. Vol. 5, No. 2. P. 30–37.
22. Singh S., Jha R. K. A survey on software defined networking: Architecture for next generation network // Journal of Network and Systems Management. 2017. Vol. 25. P. 321–374. URL: https://link.springer.com/article/10.1007/s10922-016-9393-9