ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Забезпечення QoS-трафіку в локальній корпоративній мережі з використанням правил безпеки»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерна інженерія
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

	Павло СТЕПАНЕНКО
(підпис)	*Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КІД-41
Павло СТЕПАНЕНКО
Ім'я, ПРІЗВИЩЕ
Керівник: Кирило СОКОЛОВ, PhD
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Рецензент:
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра 123 Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 Комп'ютерної інженерії

Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерної інженерії
_____ Наталія ЛАЩЕВСЬКА
_____
«_____» _____ 2026р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Степаненко Павло Олександрович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Забезпечення QoS-трафіку в локальній корпоративній мережі з використанням правил безпеки
керівник кваліфікаційної роботи Кирило СОКОЛОВ, PhD (доктор філософії),
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «20» лютого 2026р. № 51
2. Строк подання кваліфікаційної роботи «8» травня 2026р.
3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, архітектури забезпечення якості обслуговування IntServ, DiffServ, методи класифікації, маркування, пріоритезації трафіку; механізми керування чергами та контролю перевантаження; технології безпеки мереж ACL, сегментація VLAN.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Теоретичні основи організації локальних мереж і забезпечення якості обслуговування
2. Аналітичне обґрунтування та проєктування архітектури локальної корпоративної мережі
3. Розробка локальної корпоративної мережі з підтримкою QoS
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання «20» лютого 2026р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	25.03-30.03.2026	Виконано
2	Обробка матеріалу	31.03-04.04.2026	Виконано
3	Розробка теоретичної частини	6.04-9.04.2026	Виконано
4	Розробка моделі мережі	9.04-14.04.2026	Виконано
5	Висновки за результатами аналізу	14.04-20.05.2026	Виконано
6	Оформлення пояснювальної записки	20.04-03.05.2026	Виконано
7	Розробка презентації	04.05-05.05.2026	Виконано
8	Передзахист	04.05.-07.05.2026	Виконано
9	Здача в деканат	08.05.2026	Виконано

Здобувач вищої освіти _____ Павло СТЕПАНЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Кирило СОКОЛОВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 54 стор., 24 рис., 3 табл., 32 джерела.

Мета роботи – дослідити поняття якості обслуговування та розробити локальну корпоративну комп'ютерну мережу з використанням технологій забезпечення QoS для підприємства.

Об'єкт дослідження – аналіз роботи механізмів QoS з використанням базових правил безпеки в умовах локальної корпоративної мережі.

Предмет дослідження – методи, моделі та засоби забезпечення якості обслуговування у локальних корпоративних мережах на основі механізмів класифікації, маркування, чергування та керування мережевим трафіком.

Короткий зміст роботи: У першому розділі проведено аналіз теоретичних основ QoS, розглянуто основні параметри якості обслуговування, такі як пропускна здатність, затримка, варіація затримки та втрати пакетів. Також проаналізовано сучасні підходи до забезпечення QoS, зокрема архітектури IntServ та DiffServ, їх переваги та недоліки.

У другому розділі досліджені сучасні тенденції QoS, вплив перевантаження мережі на роботу з трафіком, проаналізовані рішення для впровадження QoS в корпоративній мережі.

У третьому розділі виконано проєктування локальної корпоративної мережі: розроблено топологію, здійснено сегментацію за допомогою VLAN, налаштовано базові мережеві сервіси та реалізовано механізми QoS для пріоритезації трафіку. Також впроваджено правила доступу (ACL) для підвищення рівня безпеки.

КЛЮЧОВІ СЛОВА*:* QoS, локальна мережа, DiffServ, VLAN, ACL, VoIP, трафік, якість обслуговування.

ABSTRACT

The text part of the bachelor's qualification work: 54 pages, 24 figures, 3 tables, 32 references.

Purpose of the work – to study the concept of Quality of Service (QoS) and to develop a local corporate computer network using QoS technologies for an enterprise.

Object of research – analysis of the operation of QoS mechanisms using basic security rules within a local corporate network.

Subject of research – methods, models, and tools for ensuring Quality of Service in local corporate networks based on traffic classification, marking, queuing, and traffic management mechanisms.

Brief content of the work: In the first chapter, the theoretical foundations of QoS are analyzed, and the main QoS parameters such as bandwidth, delay, jitter, and packet loss are considered. Modern approaches to QoS provisioning are also analyzed, including the IntServ and DiffServ architectures, along with their advantages and disadvantages.

In the second chapter, modern QoS trends are studied, the impact of network congestion on traffic performance is examined, and solutions for implementing QoS in a corporate network are analyzed.

In the third chapter, a local corporate network is designed: the topology is developed, segmentation using VLANs is implemented, basic network services are configured, and QoS mechanisms for traffic prioritization are applied. Access control rules (ACL) are also implemented to enhance network security.

KEYWORDS: QoS, local network, DiffServ, VLAN, ACL, VoIP, traffic, Quality of Service.

ЗМІСТ

ВСТУП……9
1 ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ ЛОКАЛЬНИХ МЕРЕЖ І ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ……10
1.1 Поняття комп'ютерних мереж……..10
1.2 Характеристики корпоративних мереж……..11
1.3 Поняття якості обслуговування……...15
1.4 Характеристики QoS……17
1.5 Методи та підходи в застосуванні QoS……...20
1.6 Архітектури забезпечення QoS……24
1.7 Взаємозв'язок QoS та правил безпеки……30
2 АНАЛІТИЧНЕ ОБҐРУНТУВАННЯ ТА ПРОЄКТУВАННЯ АРХІТЕКТУРИ ЛОКАЛЬНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ ……..32
2.1 Аналіз проблем мережі без застосування QoS……...32
2.2 Вибір середовища для побудови мережі……33
2.3 Аналіз мережевих сервісів і типів трафіку……34
2.4 Аналіз існуючих рішень та вибір архітектури для забезпечення QoS….36
2.5 Опис досліджуваної корпоративної мережі……39
3 РОЗРОБКА ЛОКАЛЬНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ З ПІДТРИМКОЮ QoS……..42
3.1 Побудова топології……42
3.2 Налаштування VLAN……42
3.3 Налаштування DHCP……45
3.4 Налаштування сервісу телефонії……47
3.5 Налаштування QoS……49
3.6 Тестування мережі……52
ВИСНОВКИ……...63
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ……64
Додаток А. Лістинг команд для налаштування ……....67

ВСТУП

У сучасних умовах стрімкого розвитку інформаційних технологій та цифровізації економіки, корпоративні комп'ютерні мережі є основою функціонування підприємств, організацій та установ. Зростання обсягів переданих даних, використання сервісів для спілкування в реальному часі та підвищення вимог до швидкості й надійності передачі інформації обумовлюють необхідність впровадження ефективних механізмів управління мережевим трафіком.

Актуальність роботи полягає у необхідності розробки ефективних рішень для забезпечення якості обслуговування в локальних корпоративних мережах в умовах зростаючого навантаження та різнорідності мережевого трафіку.

Метою роботи є розробка локальної корпоративної мережі з ефективним забезпеченням QoS-трафіку та впровадженням базових правил безпеки для підвищення продуктивності та захищеності мережі.

Об'єктом дослідження є дослідження роботи механізмів якості обслуговування у локальній корпоративній мережі.

Предметом дослідження є методи, моделі та засоби забезпечення якості обслуговування в корпоративних мережах, зокрема механізми класифікації, маркування, чергування та керування мережевим трафіком.

Практичне значення роботи полягає у можливості використання розробленої мережевої моделі та налаштувань QoS для впровадження в реальних корпоративних мережах з метою підвищення ефективності використання мережевих ресурсів, забезпечення стабільної роботи критичних сервісів та підвищення рівня інформаційної безпеки.

Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, переліку використаних джерел та додатку. В першому розділі розглянуто теоретичні основи забезпечення QoS. В другому розділі проведено аналіз актуальності теми та визначені засоби, які потрібні для розробки моделі локальної корпоративної мережі. В третьому розділі розроблено, налаштовано та протестовано модель локальної мережі з використанням засобів забезпечення QoS.

1 ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ ЛОКАЛЬНИХ МЕРЕЖ І ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ

1.1 Поняття комп’ютерних мереж

Комп’ютерна мережа являє собою сукупність комп’ютерів і інших пристроїв, взаємопов’язаних між собою засобами передавання даних. Вона є результатом інтеграції обчислювальної техніки та телекомунікацій, що дозволяє забезпечити обмін інформацією, спільне використання ресурсів і узгоджену роботу різних систем.[1]

У сучасних умовах використання одного комп’ютера, який би задовольняв усі потреби підприємства, є неефективним і непрактичним. Зі зростанням обсягів даних, кількості користувачів і складності задач виникла необхідність у розподіленій обробці інформації. Саме тому почали широко застосовувати системи, що складаються з багатьох окремих, але взаємопов’язаних комп’ютерів.[1]

Такі системи отримали назву комп’ютерних мереж і стали основою функціонування сучасних інформаційних технологій, забезпечуючи гнучкість, масштабованість і надійність обробки та передавання даних.[1]

З розвитком та розширенням комп’ютерних мереж, стало зрозуміло, що вони можуть використовуватися не тільки для обміну даними, а й також для комунікації в режимі реального часу. Тобто по суті, вони можуть виконувати роль телефонних мереж.[1]

Згодом, спілкування в мережі стало однією з найважливіших складових сучасного світу. Воно виступає не лише доступним способом підтримувати зв’язок із людьми на відстані, але й створює широкі можливості для дистанційного навчання та роботи. Багато компаній значною мірою залежать від оперативної взаємодії зі своїми працівниками, особливо в умовах віддаленої діяльності.[1]

Комунікація може здійснюватися через обмін текстовими повідомленнями,

однак такий формат не завжди є зручним і ефективним. Тому дедалі частіше використовуються аудіо- та відеодзвінки, які забезпечують більш природну та швидку взаємодію. Водночас передача мультимедійних даних у режимі реального часу є складнішим процесом порівняно з передачею інших типів інформації, що може впливати на якість зв’язку.[1]

Саме тому розвиток комп’ютерних мереж, спрямований на підвищення якості та розширення можливостей комунікації, набуває особливо важливого значення в сучасному інформаційному суспільстві.[1]

1.2 Характеристики корпоративних мереж

Як вже було зазначено, в більшості організацій (компаній, університетів тощо) використовується велика кількість комп’ютерів, які необхідні працівникам для виконання різноманітних завдань - від проєктування продукції до ведення фінансової документації. Як правило, ці комп’ютери об’єднуються в єдину мережу, що дозволяє ефективно організувати спільний доступ до даних, інформації та обчислювальних ресурсів.[2, 3]

Така мережа називається локальною (LAN, Local Area Network). Це означає, що вона функціонує в географічно обмеженому просторі, наприклад в офісній будівлі. Приклад такої мережі наведений на рис. 1.1.

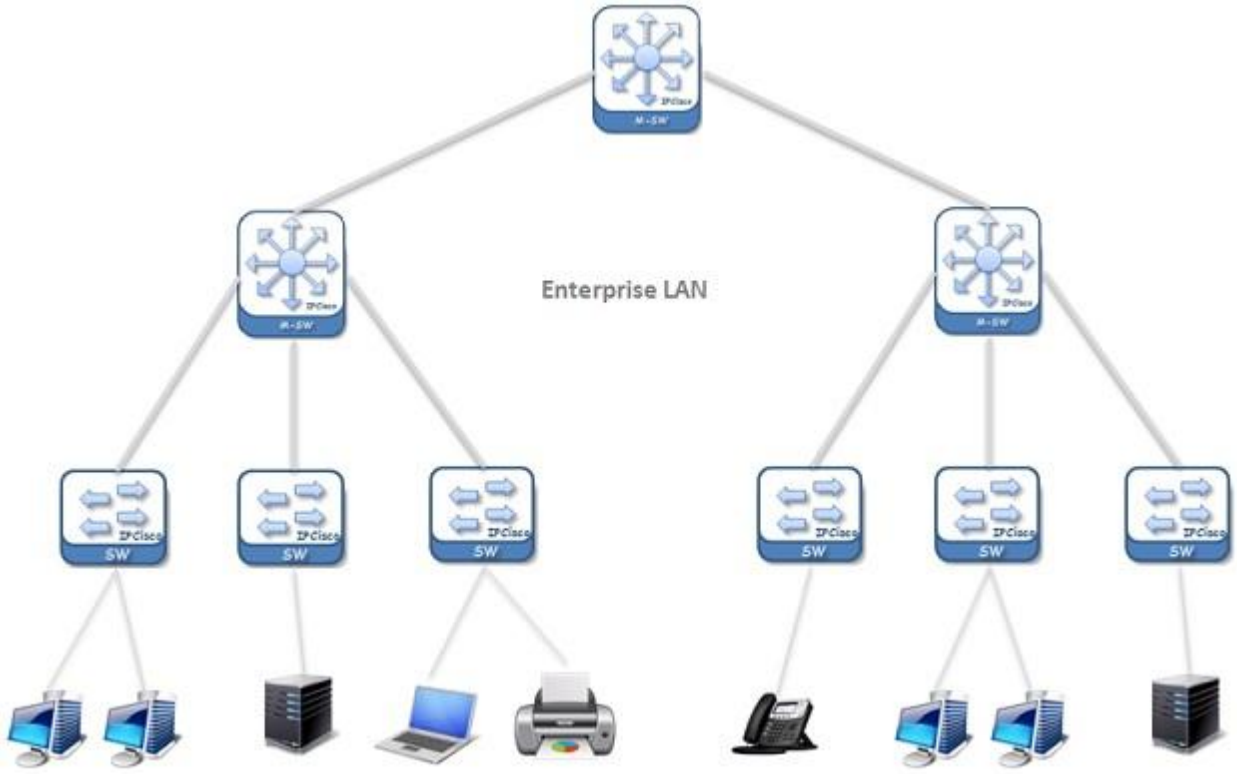


Рисунок 1.1 – Приклад корпоративної локальної мережі [3]

У локальних мережах використовується різноманіття технологій передавання даних. Найпоширенішими фізичними середовищами є мідні кабелі, коаксіальні лінії та оптоволоконні канали зв’язку. Оскільки розміри таких мереж обмежені, максимальний час поширення сигналу має визначену межу і може бути заздалегідь оцінений. Це дозволяє ефективніше проєктувати мережеві протоколи.

Дротові LAN забезпечують швидкість передавання даних у діапазоні від 100 Мбіт/с до 40 Гбіт/с. Вони характеризуються низькою затримкою (зазвичай не більше кількох десятків мілісекунд, а часто значно меншою) та високою надійністю, оскільки помилки передавання виникають рідко.

Порівняно з бездротовими мережами, дротові LAN мають меншу затримку, нижчий рівень втрат пакетів і вищу пропускну здатність. Хоча з розвитком технологій ця різниця поступово зменшується, передавання сигналів через кабельні середовища або оптоволокно й досі залишається простішим і стабільнішим, ніж передавання через повітря. [1, 2]

Більшість дротових локальних мереж побудовані на основі двоточкових

з’єднань між пристроями. Найпоширенішим стандартом таких мереж є IEEE 802.3, більш відомий як Ethernet. [4]

У комутованих мережах Ethernet кожен комп’ютер може підключатися до спеціального пристрою - комутатора (switch) за допомогою окремого з’єднання. Основне призначення комутатора полягає в передаванні пакетів даних між підключеними до нього пристроями.[5]

Кожен пакет містить адресу отримувача, завдяки якій комутатор визначає, якому саме комп’ютеру потрібно передати дані, забезпечуючи ефективну та впорядковану взаємодію в межах мережі.[5]

Одну фізично велику локальну мережу можна поділити на кілька менших логічних сегментів. Такий підхід застосовується у випадках, коли фізична структура мережі не відповідає організаційній структурі підприємства. Так, створення окремих віртуальних локальних мереж (VLAN) для розподілу даних значно спрощує адміністрування та підвищує рівень безпеки.[6]

У такій архітектурі кожному порту комутатора призначається умовне позначення, що відповідає певному типу даних. Комутатор передає пакети з даними таким чином, що пристрої з різних VLAN залишаються ізольованими один від одного, навіть якщо фізично підключені до одного обладнання. Наприклад, комп’ютери з однієї віртуальної підмережі не отримуватимуть широкомовні пакети, призначені для комп’ютерів з іншої віртуальної підмережі, ніби це окремі фізичні мережі. [6]

Попри те що локальна мережа географічно обмежена, вона може отримувати доступ до глобальної мережі (WAN, Wide Area Network) за допомогою маршрутизатора. Цей пристрій об’єднює LAN з WAN, а також визначає оптимальні шляхи передачі пакетів на основі IP-адрес призначення, забезпечуючи міжмережеву взаємодію та доступ до інших мереж.

Для кращого розуміння ролі мережевих пристроїв у передачі даних використовується модель OSI (Open Systems Interconnection), яка показана на рис. 1.2. Вона поділяє процес мережевої взаємодії на 7 рівнів, проте в локальних мережах застосовуються тільки 3, 2, та 1 рівні. Маршрутизатори (routers) працюють

на 3 (мережевому) рівні OSI, оскільки приймають рішення про пересилання пакетів на основі IP-адрес і таблиць маршрутизації. Комутатори (switches) працюють переважно на 2 (канальному) рівні OSI, де передача кадрів здійснюється на основі унікальних MAC-адрес кінцевих пристроїв.[7]

Тип даних	Рівень	Функції
Дані	7. Прикладний (Application)	Доступ до мережевих служб
	6. Представницький (Presentation)	Представлення і шифрування даних
	5. Сеансовий (Session)	Управління сеансом звязку
Сегменти	4. Транспортний (Transport)	Прямий звязок між кінцевими пунктами та надійність
Пакети	3. Мережевий (Network)	Визначення маршруту та логічна адресація
Кадри	2. Канальний (Data Link)	Фізична адресація
Біти	1. Фізичний (Physical)	Робота з середовищем передачі, сигналами та двійковими даними

Рисунок 1.2 – Рівні моделі OSI [7]

Широкомовні локальні мережі можуть використовувати два підходи до розподілу ресурсів — статичний і динамічний. У разі статичного підходу час поділяється на фіксовані інтервали, і кожен пристрій отримує можливість передавати дані лише у свій часовий проміжок. Проте це може призводити до неефективного використання каналу, якщо у відповідний момент пристрій не має даних для передачі. Тому на практиці частіше застосовується динамічний розподіл ресурсів, коли доступ до каналу надається за потребою. Методи такого розподілу поділяються на централізовані та децентралізовані. У централізованих системах керування доступом здійснюється єдиним вузлом (наприклад, базовою станцією), який визначає порядок передачі даних. У децентралізованих системах кожен пристрій самостійно вирішує, коли передавати інформацію. Незважаючи на можливу складність, існують спеціальні алгоритми, які забезпечують

впорядковану роботу мережі навіть без центрального керування. [1]

Спільне використання ресурсів (resource sharing) дає змогу зробити програми, обладнання та, передусім, дані доступними для всіх користувачів мережі незалежно від їхнього фізичного розташування. Простим прикладом є використання мережевого принтера: замість того щоб кожен працівник мав власний пристрій, доцільніше застосовувати один високопродуктивний принтер, який є економічнішим, швидшим і зручнішим в обслуговуванні. [1, 2]

Крім того, в LAN є вільний обмін даними. У сучасних організаціях працівники зазвичай мають онлайн-доступ до різноманітних даних, зокрема інформації про клієнтів і товари, складських запасів, фінансових і податкових звітів та інших ресурсів. [1, 2, 3]

Однак ще більш важливим є те, що комп'ютерні мережі можуть виконувати функції телефонного зв'язку всередині організації. За допомогою інтернету така технологія реалізується у вигляді VoIP (Voice over IP) - технології передавання мультимедійних даних у режимі реального часу з використанням протоколів сімейства TCP/IP. IP-телефонія являє собою систему зв'язку, у якій аналоговий голосовий сигнал перетворюється в цифрову форму (дискретизується), стискається та передається мережею до іншого абонента, де відбувається зворотний процес — декомпресія, декодування та відтворення звуку. [1]

1.3 Поняття якості обслуговування

Мабуть у кожного, хто хоч раз спілкувався в Інтернеті, виникали проблеми з якістю голосу або відео, такі як затримки, переривання звуку, спотворення зображення чи «зависання» голосу. Особливо це помітно у випадках, коли мережа одного із співрозмовників перевантажена. Такі ситуації виникають через те, що мережа не завжди здатна рівномірно обробляти всі потоки даних, особливо коли частина з них є більш чутливою до затримок і втрат пакетів. Тому, у відповідь на цю проблему виникло поняття якості обслуговування.

Якість обслуговування (QoS, Quality of Service) - це набір методів і

технологій, що забезпечують керовану та передбачувану якість обслуговування в комп’ютерних мережах. QoS застосовується для керування та пріоретизації мережевого трафіку з метою гарантування необхідної пропускної здатності, затримок і загальної продуктивності для критично важливих застосунків, таких як голосовий і відеозв’язок. Простими словами, для забезпечення «задоволення» від користування сервісами у мережі. [8, 9]

Для кращого розуміння роботи QoS, потрібно визначити поведінку застосунків, як вони будуть генерувати трафік у мережі, тому їх доцільно об’єднати в окремі класи. Це дає розуміння їхніх вимог до мережі, а також дозволяє керувати ресурсами мережі ефективніше. Загалом усі застосунки можна поділити на дві основні групи:

1. Адаптивні застосунки (Adaptable applications) – це тип застосунків, які націлені працювати навіть за умов зміни параметрів мережі. Втрата пропускної здатності, коливання затримки або втрати пакетів не здійснюють великий вплив на їх працездатність. Характер їх роботи, дозволяє пристосовуватися до обмежень зберігаючи прийнятний рівень функціонування. [9]

Адаптивні застосунки можна додатково класифікувати на такі підгрупи:

- Асинхронні застосунки характеризуються відсутністю жорстких вимог до часу обміну даними між сторонами. Вони можуть функціонувати навіть за значних коливань характеристик мережі. Типовим прикладом є електронна пошта: жорстких обмежень щодо часу доставки у неї немає. Такі застосунки можуть «поступатися» мережевими ресурсами більш вимогливим сервісам і здатні відновлюватися після втрат пакетів. Важливо зазначити, що рівень «асинхронності» може відрізнятися залежно від застосунку. Наприклад, передача електронної пошти на основі TCP може затримуватися на хвилини без істотного впливу на користувача, тоді як веб-застосунки (HTTP або HTTPS) мають більш жорсткі обмеження, оскільки користувач очікує швидкого завантаження сторінки. [9]

- Burst-застосунки генерують трафік нерівномірно — у вигляді короткочасних піків. У такі моменти швидкість передачі даних може значно

перевищувати середнє значення. [9]

- Bulk-застосунки передають великі обсяги даних із відносно стабільною швидкістю протягом тривалого часу. Прикладом є передача файлів за протоколом TCP. [9]

2. Застосунки реального часу (Real-time applications) – це застосунки, які мають суворі вимоги до QoS і не допускають відхилень від заданих параметрів. Порушення показників передачі даних у таких системах може призвести до критичного погіршення їхньої роботи та незадоволення користувача. До таких застосунків відносять IP-телефонію, відео-конференції, стримінгові сервіси та інші. [9]

1.4 Характеристики QoS

Оскільки QoS тісно пов’язаний із функціонуванням комп’ютерних мереж і безпосередньо впливає на процес передавання даних, для його оцінювання використовуються ті самі основні метрики, що й для аналізу якості мережевого з’єднання, а саме:

1. Пропускна здатність (Bandwidth) - максимальний обсяг даних, який може бути переданий каналом за одиницю часу і вимірюється в бітах в секунду (біт/с), кілобітах в секунду (Кбіт/с), мегабітах в секунду (Мбіт/с) і т.д. [8, 9]

Пропускна здатність відіграє головну роль у функціонуванні мереж, оскільки визначає обсяг доступних ресурсів для роботи застосунків. Вона задає граничну швидкість передавання даних, і це визначає, в яких умовах будуть функціонувати сервіси. При цьому важливим є не лише максимальне значення швидкості, а й її поведінка в різних умовах навантаження. [8, 9]

У межах локальних мереж проблема обмеженої пропускної здатності зазвичай є менш критичною, однак вона все одно може виникати у разі високого навантаження, великої кількості підключених пристроїв або інтенсивного передавання трафіку. Хоча завдяки переходу до комутованих архітектур і розвитку Ethernet-технологій сучасні LAN забезпечують значний запас швидкості, він не

завжди є достатнім у пікових режимах роботи. У WAN-мережах ситуація є складнішою, оскільки ресурси там більш обмежені через високу вартість каналів зв’язку, обмежену пропускну здатність між мережевими вузлами та складність розгортання інфраструктури, а використання високошвидкісних технологій часто не є економічно вигідним. [8, 9]

У результаті такі мережі нерідко працюють в умовах обмежених ресурсів, що може негативно впливати на QoS. Зокрема, маршрутизатори в подібних умовах стають потенційними точками перевантаження, оскільки змушені обробляти значні обсяги трафіку. Це робить механізми керування чергами та пріоритезації критично важливими для підтримання стабільної роботи мережі. [8, 9]

2. Латентність (Latency) - це показник затримки в мережі, що вимірюється як повний час обміну даними між вузлами, у мілісекундах (мс).

Latency у мережах зазвичай розглядається як загальний показник часу відгуку системи, який характеризує сумарну затримку взаємодії між вузлами або сервісами. У більшості випадків вона відображає практичну «відчутну» затримку роботи мережі. Складається з таких показників: Response Time (час на відгук), який відображає час обробки запиту на стороні клієнта та сервера, та час на повне проходження даних в обидві сторони, і таким чином відображає повний цикл «запит–відповідь»; Equipment Latency (затримка обладнання) відображає час на обробку пакетів на мережевих пристроях. Ця затримка визначається часом, який потрібен пристрою для прийому, аналізу та передачі пакета далі. До таких пристроїв належать маршрутизатори, комутатори, фаєрволи та сервери доступу. Комутатори зазвичай додають мінімальну затримку (на рівні мікросекунд), тоді як маршрутизатори можуть вносити більш значні затримки, особливо при високому навантаженні або обмежених ресурсах; Network Latency є показником часу, витраченого в процесі передавання даних від відправника до отримувача. А саме затримки мережевого обладнання (комутатори, маршрутизатори, фаєрволи), затримки провайдерів і магістральних мереж, затримки поширення та обробки сигналу в мережевій інфраструктурі. У локальних мережах ці значення зазвичай мінімальні, тоді як у глобальних мережах вони можуть суттєво зростати. [8, 9]

3. Затримка (Delay) - час доставки пакета від джерела до отримувача у мс.

На відміну від латентності, затримка зазвичай розглядається як більш «технічна» характеристика, що описує час проходження пакета до отримувача або на окремих етапах обробки. Виділяють декілька видів затримки: Propagation Delay (затримка поширення), яка фізично обумовлена часом проходження сигналу через середовище передачі (мідь, оптика, бездротові канали). У локальних мережах вона зазвичай незначна, але у великих розподілених мережах може досягати суттєвих значень; Transmission Delay (затримка передачі) тип затримки, який залежить від швидкості каналу зв'язку та розміру переданого пакета. Чим менша пропускна здатність каналу або більший пакет, тим довше відбувається його передача; Application Delay (затримка застосунку) виникає безпосередньо на рівні програмного забезпечення, де складається з часу від обробки отриманих даних та виконання програмного коду застосунку, а розмір цієї затримки залежить від продуктивності пристрою, операційної системи та оптимізації самого програмного забезпечення. [8, 9]

4. Джитер (Jitter) - це різниця у часі прибуття послідовних пакетів, тобто пакети можуть приходити не через однакові інтервали часу. Вимірюється у мс.

Для застосунків реального часу, таких як, VoIP або відео, критично важливо мати низький джитер, адже їхня коректна робота залежить від рівномірності потоку даних. Джитер виникає, коли мережеві пристрої обробляють трафік нервіномірно, а отже надсилають пакети з даними також нервіномірно. Суттєвим фактором появи джитера є нестабільність каналів на шляху сигналу, зокрема через електромагнітні перешкоди. Джитер може призводити не тільки до нерівномірної доставки, але й до порушення порядку надходження пакетів. Для TCP це не критично, оскільки протокол виправляє їх порядок. Але для UDP-застосунків, до яких відноситься і VoIP, потрібні додаткові механізми. [8, 9]

Щоб компенсувати джитер, використовується буфер (jitter buffer), який накопичує пакети і вирівнює їх подачу. [8, 9]

5. Втрати пакетів (Packet loss) - частка пакетів, що були втрачені, а тому не доставлені. Вимірюється в відсотковому коефіцієнті втрачених пакетів до кількості

відправлених пакетів.

Основною причиною втрат пакетів, є перевантаження маршрутизаторів, коли їхня пам’ять переповнюється і частина пакетів не може бути оброблена вчасно, у результаті чого вони відкидаються. Окрім цього, причиною втрат може бути неправильна маршрутизація, коли пакети надсилаються за некоректним маршрутом або не досягають кінцевого вузла через помилки в таблицях маршрутизації. [8, 9]

Помилки передачі сьогодні трапляються рідко завдяки сучасним технологіям (наприклад, оптоволоконним з’єднанням). [9]

1.5 Методи та підходи в застосуванні QoS

Далі слід розглянути основні методики, пов’язані з QoS, а також дати опис ключовим підходам, які застосовуються для забезпечення якості обслуговування в IP-мережах.

Важливим компонентом цих методик є обробка пакетів з даними. Загалом, обробка пакетів із забезпеченням QoS у маршрутизаторах і комутаторах може реалізовуватися двома основними підходами:

- потокова (flow-based) обробка пакетів [9, 10]
- класова (class-based) обробка пакетів [9, 10]

Потік відповідає односпрямованому (від джерела до призначення) потоку даних між застосунками. Потік зазвичай ідентифікується параметрами, такими як IP-адреси (джерела та/або призначення) і номери портів (джерела та/або призначення). Також потік може бути визначений за допомогою мітки, наприклад flow label, яка використовується в IPv6 та протоколі RSVP. [9, 11]

Таким чином, потік може представляти обмін пакетами між кінцевими застосунками, яка дозволяє дуже точно налаштовувати QoS для окремих з’єднань. [9, 11]

Важливою характеристикою потоків є їх висока гнучкість. Це означає, що для їх ідентифікації можуть додатково використовуватися різні параметри. Наприклад,

поле ToS (Type of Service) в IP-заголовку пакета може застосовуватися разом з IP-адресами та портами для більш точного визначення конкретного потоку.[9, 10]

У цьому контексті термін «потік пакетів» означає набір пакетів, що передаються мережею до одного або кількох отримувачів (unicast, multicast або широкомовною передачею).[9, 12]

Потоки та пакети можуть групуватися різними способами — наприклад, за певним вузлом, підмережею або їх комбінацією. Крім того, для формування груп можуть використовуватися параметри IP-заголовка, такі як адреси, порти та протоколи. Такі групи пакетів називають «класом». Клас — це набір пакетів із спільними ознаками (наприклад, спільний IP-префікс або приналежність до одного вузла), який фактично може включати кілька потоків. [9, 12]

При потоковій обробці пакетів обробка виконується на рівні окремих потоків. Іншими словами, пакети, що належать до конкретної пари «відправник–отримувач», обробляються з урахуванням необхідного рівня QoS. Перевагами потокової обробки є висока гнучкість, оскільки налаштування можна виконувати індивідуально для кожного користувача або з’єднання та завдяки ефективному розподілу ресурсів кожен потік може отримувати окремо налаштовані параметри обслуговування. [9, 10]

Основні недоліки потокової обробки:

- для точної ідентифікації потоків потрібна додаткова обчислювальна обробка; [9]

- погана масштабованість у великих мережах через можливе перевантаження кількістю потоків і станів; [9]

- велика кількість інформації про кожен потік, яку необхідно зберігати в мережевих пристроях, що створює проблеми з масштабуванням.[9]

При класовій обробці пакетів обробка виконується на рівні групи пакетів. Індивідуальні потоки при цьому не розглядаються окремо. [9]

Основні переваги класової обробки:

- хороша масштабованість навіть у мережах з великою кількістю користувачів, оскільки обсяг стану мінімальний; [9]

- зменшення обсягу аналізу заголовків пакетів маршрутизаторами, що знижує навантаження; [9]

- спрощення адміністрування мережі та впровадження політик тарифікації та управління. [9]

Основний недолік класової обробки полягає в тому, що вона не дозволяє точно налаштовувати обслуговування для окремих користувачів або потоків відповідно до їх індивідуальних вимог.[9]

Далі можна перейти до способів практичної реалізації QoS. Основні підходи до забезпечення якості обслуговування в IP-мережах включають:

1. Overdimensioning - передбачає забезпечення надлишкової пропускної здатності для всіх застосунків, щоб уникнути перевантаження мережі. Він не є механізмом QoS, але іноді використовується як альтернатива. Найчастіше він застосовується у невеликих локальних і корпоративних мережах та середовищах із відомою кількістю користувачів і передбачуваним трафіком. Проте продуктивність маршрутизаторів все одно може стати вузьким місцем, а попит користувачів і застосунків з часом зростає разом із можливостями мережі. Тому overdimensioning не гарантує довгострокового вирішення проблем QoS. [9]

2. Queue and scheduling - це механізми управління порядком обробки пакетів у чергах маршрутизатора. Вони потрібні для гарантування правильної роботи QoS, тому повинні справедливо розподіляти пропускну здатність для зменшення затримок або джитера. Основними алгоритмами є: FIFO (First In First Out) - найпростіший спосіб організації черги, де мережеві пакети обробляються у порядку їх отримання. Такий підхід простий у впровадженні, але не розділяє трафік за пріоритетами чи типами даних. Також недоліком є випадкові втрати пакетів. Тому для забезпечення QoS майже непридатний; Priority Queuing (PQ) – метод, при якому пакети розділяються за пріоритетами, високий пріоритет обслуговується першим, низький останнім, недоліком є висока затримка низькоприоритетних черг; Weighted Fair Queuing (WFQ) - механізм, який ділить пропускну здатність між різними типами трафіку відповідно до встановлених вагових коефіцієнтів, завдяки чому навіть менш пріоритетні потоки не залишаються без ресурсів і завжди

отримують певну частку каналу, що дозволяє зменшити затримку. [9]

3. Packet conditioning - це набір механізмів, які визначають пріоритет і поведінку пакетів у мережі. До основних методів належать пріоретизація пакетів, класифікація та маркування. Ці механізми зазвичай використовуються у поєднанні між собою, оскільки вони доповнюють один одного. Наприклад, класифікація пакетів може виконуватися перед їх маркуванням, а пріоритет обробки часто визначається на основі попереднього маркування трафіку. [9]

4. Policing і shaping - це механізми QoS, які використовуються для контролю та обмеження використання пропускної здатності. Обидва методи відстежують швидкість трафіку на інтерфейсі та порівнюють її з заданим значенням CIR (Committed Information Rate — гарантована швидкість). Якщо трафік перевищує цей поріг, застосовується певна дія відповідно до налаштувань. [9, 13]

Policing контролює швидкість трафіку та перевіряє, чи не перевищує вона задане значення CIR. Якщо новий пакет призводить до перевищення цього ліміту, пакет просто відкидається. Інколи замість цього він «перемарковується», змінюючи пріоритет. Policing можна застосовувати як на вхід, так і на вихід, але найчастіше його використовують саме на вхідному трафіку. [9, 13]

Shaping також обмежує швидкість трафіку відповідно до CIR, але працює інакше. Замість того щоб відкидати пакети, він тимчасово зберігає їх у буфері та передає пізніше, коли навантаження зменшиться. Однак через буферизацію виникає додаткова затримка. Shaping використовується тільки для вихідного трафіку. [9, 13]

5. Congestion control — набір методів для запобігання та усунення перевантаження в мережі. Перевантаження виникає, коли багато вхідних потоків спрямовуються до одного вихідного інтерфейсу, що перевищує пропускну здатність. Це призводить до втрат пакетів, підвищенням затримки і джитера. Основні методами є: Tail Drop - метод при якому пакети відкидаються при переповненні черги, але неефективний, тому що призводить до ще більших втрат пакетів; RED (Random Early Detection) - цей механізм випадковим чином відкидає пакети ще до того, як черга повністю переповниться, для цього він використовує

середнє значення довжини черги для завчасного виявлення ознак перевантаження та запобігання його подальшому зростанню; ECN (Explicit Congestion Notification), при цьому методі пакети не відкидаються, але позначаються як перевантажені, що дозволяє відправним вузлам зменшити кількість переданих пакетів без втрат даних. [9]

1.6 Архітектури забезпечення QoS

Для покращення QoS в комп'ютерних мережах, виникла необхідність в об'єднанні механізмів обробки пакетів, керуванням черг та пріорітетів, в певні архітектури. Вони відрізняються принципами обробки трафіку та рівнем гарантованих характеристик передачі даних. Основних архітектур дві - це Integrated Service (IntServ) та Differentiated Service (DiffServ). Також існує модель best-effort, але вона виконує скоріше допоміжну роль, тому що не може гарантувати ефективну доставку даних. Тому, такий підхід підходить для сервісів, де затримки та втрати пакетів не є критичними. [9, 10, 14]

Архітектура IntServ забезпечує якість обслуговування в IP-мережах через механізм резервування ресурсів для окремих потоків пакетів. Для цього маршрутизатори назначають кожному потоку у мережі певний стан. [9, 14]

Спочатку користувач або застосунок визначає необхідні параметри якості обслуговування, зокрема допустиму затримку та потрібну пропускну здатність. Далі ці вимоги передаються в мережу за допомогою сигнального протоколу, який називається RSVP. [9, 14]

Основна роль RSVP (Resource Reservation Protocol) полягає у створенні попереднього резерву пропускної здатності, ще до початку фактичної передачі даних (рис. 1.3). Особливістю цього механізму є те, що обсяг необхідних ресурсів визначає саме отримувач, оскільки він володіє повною інформацією про власні вимоги до QoS. При цьому сам протокол не залучений до перенесення користувацького трафіку, а лише координує обмін службовими повідомленнями для резервування ресурсів уздовж усього маршруту. [9, 14]

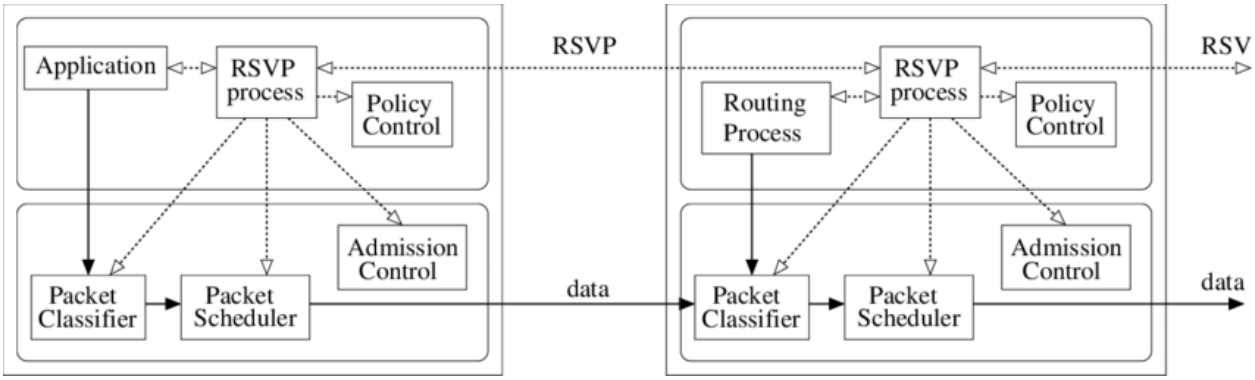


Рисунок 1.3 – Схема взаємодії компонентів архітектури IntServ та протоколу RSVP [15]

На рис. 1.4 наведені етапи встановлення наскрізного з’єднання в архітектурі IntServ. Для забезпечення з’єднання між пристроями, існує процедура admission control, під час якої кожен мережевий вузол перевіряє наявність вільних ресурсів для задоволення надісланого запиту. У разі позитивного рішення мережа офіційно схвалює запит, резервує необхідні потужності та гарантує стабільний рівень QoS, здійснюючи постійний моніторинг заданих параметрів. Завдяки такому підходу, IntServ забезпечує найвищий пріоритет для критичних потоків, тоді як решта мережевого трафіку обробляється за залишковим принципом best-effort. [9, 14]

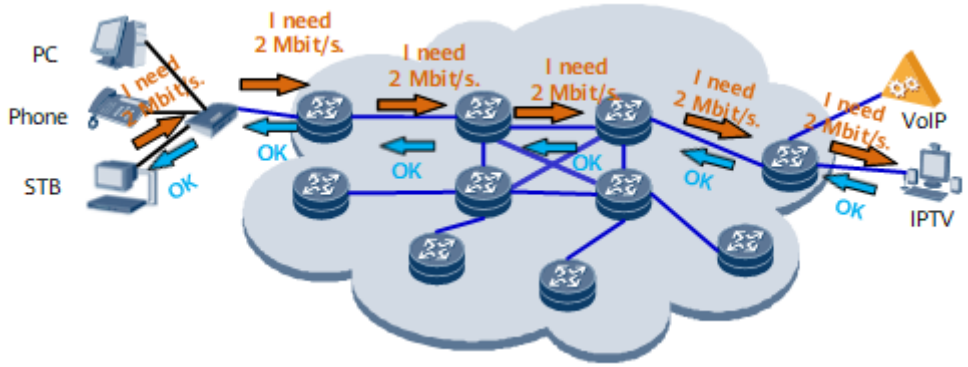


Рисунок 1.4 - Схема встановлення наскрізного (End-to-End) QoS-з'єднання в архітектурі IntServ. [10]

Архітектура IntServ має на меті зменшити непередбачуваність затримок, джитера та пропускної здатності, характерну для best-effort. Вона визначає два основні типи сервісів. [9, 11, 14]

Першим є Guaranteed Service (гарантований сервіс), який фактично створює аналог орендованого каналу, де мережеві ресурси жорстко закріплюються за конкретним інформаційним потоком. Завдяки такому підходу гарантований сервіс забезпечує сувору максимальну межу затримки, повну відсутність втрат пакетів через перевантаження черг, а також стабільну пропускну здатність. Через такі жорсткі параметри цей сервіс підходить для засобів VoIP та мультимедійних додатків, які висувають найвищі вимоги до часових показників мережі. [9, 11]

Його недоліком є те, що він гарантує лише чергову (queuing) затримку, тоді як загальна реальна затримка в мережі додатково включає час на передачу, обробку та безпосереднє поширення сигналу. [9, 11]

Другий сервіс називається Controlled-Load (контрольоване навантаження) і призначений для підтримання якості обслуговування на рівні, максимально наближеному до умов роботи ненавантаженої мережі, навіть у моменти виникнення перевантажень. Головними перевагами цього сервісу є забезпечення високої частки успішно доставлених пакетів, мінімальні коливання затримки та загальна стабільність передачі даних при помірному навантаженні на канали зв'язку. [9, 11]

Особливістю даного підходу є його адаптивність до змін у мережевому середовищі, що досягається завдяки механізмам контролю доступу та пріоритезації трафіку. Це робить Controlled-Load ідеальним рішенням для так званих «еластичних» застосунків, наприклад вебсервісів, які здатні підлаштовуватися під наявну пропускну здатність. [9, 11]

Загалом, архітектура IntServ є надійним інструментом для забезпечення жорстких гарантій якості обслуговування завдяки індивідуальному резервуванню ресурсів для кожного потоку. Однак необхідність кожного маршрутизатора підтримувати інформацію про стан кожного окремого потоку створює високе

навантаження на обладнання, що обмежує масштабованість цієї моделі у великих мережах. [9, 14]

Оскільки модель IntServ виявилася малопридатною для магістральних каналів зв'язку, було розроблено альтернативний підхід - DiffServ.

Архітектура DiffServ (Differentiated Services) базується на ідеї надання різних рівнів якості обслуговування не окремим потокам, а їхнім агрегованим групам. На рис. 1.5 видно, що на відміну від моделі IntServ, де кожен потік потребує індивідуальної обробки, DiffServ класифікує трафік за невеликою кількістю типів сервісу. Такий підхід дозволяє значно підвищити масштабованість системи, роблячи її придатною для використання у глобальних та великих локальних мережах. [9, 12]

Для реалізації диференційованої обробки голосу, відео та даних у межах єдиної IP-інфраструктури використовуються два ключові механізми: маркування пакетів та підтримка відповідних класів на мережевих вузлах. [9, 14]

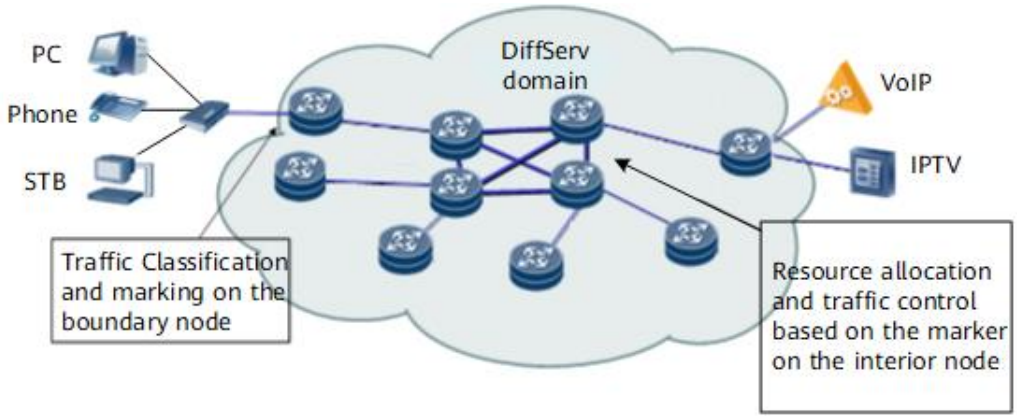


Рисунок 1.5 – Приклад мережі побудованої за допомогою моделі DiffServ [10]

В межах архітектури DiffServ взаємодія між клієнтом і провайдером регулюється угодою про рівень сервісу - SLA (Service Level Agreement). В межах SLA діють дві специфікації: SLS (Service Level Specification) - описує технічні параметри сервісу в мережі, та TCS (Traffic Conditioning Specification), який чітко визначає умови, для пропуску пакетів, їх затримки або відкидання у разі невідповідності встановленим нормам. [9, 12]

Основними механізмами DiffServ для керування трафіком є його класифікація, де маршрутизатор розпізнає та сортує вхідні пакети за певними ознаками, в основному за заголовком пакета, щоб визначити, до якої групи (класу) він належить та маркування, яке відбувається за допомогою спеціального DS-байта (Differentiated Services Field), де значення DSCP (Differentiated Services Code Point) вказує мережі, як саме слід обробляти цей пакет. [9, 12]

Першим етапом йде класифікація трафіку, вона починається з ідентифікації пакета за службовою інформацією вказаною на його полях. В архітектурі DiffServ використовується BA (Behavior Aggregate), метод, за яким пакет ідентифікується лише за вже наявним кодом DSCP, і є дуже зручний завдяки високій масштабованості та швидким назначенням міток. Також існує метод MF (Multi-Field), в ньому маршрутизатор аналізує сукупність полів пакета де вказані IP-адреси відправника/отримувача, номери портів (TCP/UDP) та тип протоколу, він є точнішим ніж BA, але використовує більше часу та ресурсів на класифікацію пакета [9, 12]

Наступний етап, це маркування, яке в більшості випадків здійснюється на маршрутизаторах, але таокж може здійснюватися на кінцевих вузлах користувачів, або у спеціалізованих пристроях, таких як VoIP-шлюзи. Завдяки цьому, пакет стає самодокументованим: будь-який наступний вузол у ядрі мережі просто зчитує мітку DSCP, не витрачаючи ресурси на повторну класифікацію. Не відмічені пакети зазвичай обслуговуються за принципом best-effort. [9, 12, 17]

Назви міток DSCP визначають пріорітет, за яким вже PHB (Per-hop Behavior), керує відміченими пакетами. В табл. 1.1 наведені назви та значення спеціальних міток, які визначають поведінку в мережі стосовно цих пакетів. [9, 12, 17]

Таблиця 1.1 - Параметри маркування пакетів DSCP [18]

Назва DSCP	Бінарне значення	Десяткове значення
AF11	001 010	10
AF12	001 100	12

Продовження таблиці 1.1

AF13	001 110	14
AF21	010 010	18
AF22	010 100	20
AF23	010 110	22
AF31	011 010	26
AF32	011 100	28
AF33	011 110	30
AF41	100 010	34
AF42	100 100	36
AF43	100 110	38
EF	101 110	46

Мітки складаються з двох видів: Expedited Forwarding та Assured Forwarding.

Expedited Forwarding (EF) застосовується спеціальна мітка для пакетів із застосунків реального часу. Вона забезпечує найвищу якість обслуговування з мінімальними затримками та втратами, що критично важливо для передачі голосу. [9, 12]

Assured Forwarding (AF) дозволяє більш гнучко налаштовувати обробку трафіку всередині класів. AF також присвоюються спеціальні цифри, які вказують на їх пріорітет. Перша цифра означає клас (чергу), а друга - рівень ймовірності відкидання пакета при перевантаженні. З цього виходить, що мітки AF11, AF21, AF31, AF41 вважаються "найкращими" підкласами всередині своїх груп. Вони мають найнижчу ймовірність бути відкинутими, якщо мережа перевантажена. Мітки AF12, AF22, AF32, AF42 мають середній рівень пріоритету всередині класу. Пакети з цими мітками будуть видалені раніше за попередні, якщо виникне черга. AF13, AF23, AF33, AF43 мають найвищий рівень відкидання. Це трафік, якого мережа позбавиться в першу чергу всередині відповідного класу. [9, 12]

Це технічна реалізація якості обслуговування на кожному конкретному мережевому пристрої є Per-hop Behavior (PHB). PHB визначає набір дій

(виставлення в черги, виділення смуги, правила відкидання), які маршрутизатор застосовує до пакетів з певною міткою DSCP. Для пакетів з мітками EF, PHB забезпечує найвищий пріоритет і мінімальні затримки, як для критичних сервісів. Пакетам з мітками AF пропонує гарантовану доставку з різними рівнями пріоритету відкидання. Для застосування PHB, вузол використовує механізми планування (scheduling), такі як пріоритетні черги (PQ) або зважені черги (WFQ), а також методи policy conditioning (policing та shaping).[9, 13]

Загалом, архітектура DiffServ характеризується високою масштабованістю та низьким навантаженням на мережеве обладнання, що досягається завдяки простій системі управління трафіком через класи та робить її надзвичайно ефективною для впровадження у великих мережах інтернет-провайдерів. Проте цій моделі властиві й суттєві обмеження, а саме складність забезпечення наскрізних (end-to-end) гарантій якості обслуговування та критична залежність результату від узгодженості політик між різними доменами. Однак завдяки високим можливостям масштабованість та зменшеним використанням ресурсів мережевих пристроїв, використовується вона частіше, ніж архітектура IntServ. [9]

1.7 Взаємозв’язок QoS та правил безпеки

QoS і безпека мережі тісно пов’язані між собою, оскільки неконтрольований або шкідливий трафік може суттєво впливати на роботу мережі та порушувати її стабільність навіть за наявності механізмів пріоритезації. У випадку відсутності належного контролю доступу та обмеження трафіку, мережеві ресурси можуть використовуватися неефективно, що призводить до погіршення ключових параметрів якості обслуговування.

Загрози безпеці безпосередньо впливають на такі характеристики мережі, як latency, jitter та packet loss. Наприклад, атаки типу DDoS здатні значно збільшувати затримку передачі пакетів і викликати їх втрати через перевантаження каналів та мережевих пристроїв. Flooding-трафік призводить до нерівномірного навантаження, що викликає зростання джитера та нестабільність доставки пакетів.

Несанкціонований або надлишковий трафік, у свою чергу, може займати значну частину пропускної здатності, зменшуючи доступні ресурси для критичних сервісів, таких як VoIP.[19]

Для мінімізації впливу таких факторів використовуються механізми безпеки, які одночасно виконують важливу роль у реалізації QoS. Одним із основних, та простих у реалізації інструментів є Access-Control List (ACL). Це спеціальний список, в якому визначаються правила фільтрації пакетів. Наприклад, можна заборонити проходити в мережі даним з певної IP-адреси, або обмежити їх передачу однією підмережею. Окрім забезпечення безпеки, ACL широко застосовуються для класифікації трафіку, що є важливим етапом у реалізації політик QoS. [19]

Іншим важливим механізмом є Traffic Policing, який дозволяє обмежувати швидкість передачі даних для окремих потоків. Це дає змогу запобігти перевантаженню мережі та забезпечити справедливий розподіл ресурсів між користувачами. Подібну функцію виконує також Rate Limiting, який контролює інтенсивність передачі трафіку та обмежує надмірну активність окремих джерел. [13]

Важливу роль відіграє також сегментація мережі за допомогою VLAN. Використання VLAN дозволяє сегментувати трафік, підвищуючи безпеку та продуктивність, дозволяючи пристроям взаємодіяти, ніби вони були в одній LAN, навіть перебуваючи в різних місцях. Це допомогає ізолювати трафік між різними підмережами, зменшити обсяг широкомовного трафіку та обмежити вплив потенційних загроз. [6]

Таким чином, механізми безпеки тісно інтегруються з механізмами QoS, а спільне використання цих підходів забезпечує не лише захист мережі, але й стабільну якість обслуговування для різних типів трафіку.

2 АНАЛІТИЧНЕ ОБҐРУНТУВАННЯ ТА ПРОЄКТУВАННЯ АРХІТЕКТУРИ ЛОКАЛЬНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Аналіз проблем мережі без застосування QoS

У сучасних корпоративних мережах передача різних типів трафіку відбувається одночасно в межах спільної інфраструктури. За відсутності механізмів керування якістю обслуговування всі пакети обробляються однаково, що призводить до суттєвих проблем у роботі критичних сервісів.

Вже було згадано, перевантаження каналу під час передачі великих обсягів даних негативно впливає на роботу мережі. Наприклад, використання FTP (File Transfer Protocol) може повністю зайняти доступну пропускну здатність, унаслідок чого інші сервіси не отримують необхідних ресурсів.

Актуальність проблеми значно зросла в останні роки. Стрімке поширення віддаленої та гібридної форми спілкування, широке впровадження відеоконференцій (Zoom, Microsoft Teams, Google Meet) та зростання використання хмарних сервісів призвели до різкого збільшення обсягу трафіку реального часу. Якщо раніше VoIP використовувався переважно для дзвінків на внутрішніх підприємствах, то сьогодні він став їх основним інструментом комунікації, від якого безпосередньо залежить продуктивність бізнес-процесів.

У компаніях, орієнтованих на клієнтський сервіс (продажі, підтримка, консалтинг), це безпосередньо впливає на рівень задоволеності клієнтів і репутацію бренду. Часті обриви дзвінків і затримки можуть призводити до втрати потенційних угод, скарг клієнтів та зниження лояльності. Тому за таких умов потрібно забезпечити стійкий трафік VoIP. [21]

Є декілька способів вирішення цієї проблеми. Найбільш очевидний з них, це використання дротового з'єднання через Ethernet замість бездротового зв’язку, який сильно залежить від відстані та перешкод на шляху сигналу. Однак, це не гарантує якісну передачу VoIP, адже дротове з'єдання також не має іммунітету від

перешкод сигналу. [21]

Можна уникати перевантаження мережі, особливо під час розмов через IP. Але і це не є справжнім рішенням проблеми, тому що іноді уникнути перевантажень мережі неможливо. [21]

Реальним рішенням залишається тільки QoS, який за роки свого існування довів свою високу ефективність і практичну цінність. Розроблений наприкінці 1990-х років, стандартизований, та підтримуваний IETF, він успішно застосовується в мільйонах корпоративних, операторських та дата-центрових мереж по всьому світу. Багаторічний досвід впровадження показав, що правильно налаштовані механізми QoS дозволяють суттєво підвищити якість роботи сервісів реального часу, зменшити вплив burst-трафіку та забезпечити стабільну продуктивність критичних бізнес-додатків навіть за умов значного навантаження на мережу. Саме тому QoS залишається одним з основних і перевірених часом інструментів управління трафіком у сучасних IP-мережах. [19]

Отже, можна зробити висновок, що QoS не тільки не втратив свою актуальність, а навпаки, з кожним роком стає дедалі більш необхідним і критичним елементом сучасних мереж.

2.2 Вибір середовища для побудови мережі

Для проектування мережі було обрано програмне середовище Cisco Packet Tracer - сучасне програмне середовище для моделювання комп’ютерних мереж, яке широко використовується як у навчальних цілях, так і для базового проєктування мереж. Даний інструмент дозволяє імітувати роботу більшості мережевих пристроїв, таких як маршрутизатори, комутатори, сервери та кінцеві вузли.

Середовище Cisco Packet Tracer було обрано для побудови локальної мережі з кількох причин. З них можна виділити зручність моделювання та простота у використанні, яка дозволяє швидко створювати, змінювати та тестувати топологію мережі, вбудована підтримка необхідних механізмів QoS та повноцінна робота з class-map, policy-map, маркуванням DSCP, policing, чергами пріоритетів та ACL.

Також важливою є візуалізація мережі, режим симуляції дозволяє спостерігати шлях пакетів, їх пріоритезацію, затримки та роботу ACL у реальному часі. Завдяки цьому, в ньому зручно проводити демонстрації концепцій QoS, VLAN, DHCP, VoIP та правил безпеки.

Є також і більш професійні інструменти, такі як GNS3, EVE-NG, Cisco CML, вони використовують реальні образи Cisco IOS і забезпечують вищий рівень реалістичності. Однак вони вимагають значно більше часу на налаштування та значно глибших знань. Для цілей даної роботи, де акцент зроблено на розумінні принципів роботи QoS та безпеки, та реалізації локальної корпоративної мережі, використання Packet Tracer є найбільш раціональним і ефективним рішенням.

2.3 Аналіз мережевих сервісів і типів трафіку

У досліджуваній корпоративній мережі одночасно можуть передаються різні типи трафіку, кожен з яких має суттєво відмінні вимоги до параметрів якості обслуговування. Основними сервісами є IP-телефонія (VoIP), веб-доступ (HTTP/HTTPS) та передача файлів (FTP). Вимоги для кожного сервісу наведені у табл. 2.1.

Таблиця 2.1 – Порівняльна характеристика видів трафіку [19]

Характеристика	**VoIP**	**Web (HTTP/HTTPS)**	**FTP**
Тип застосунку	Реального часу	Адаптивний	Адаптивний
Протокол	UDP (RTP)	TCP	TCP
Необхідна пропускна здатність	~64–100 кбіт/с	~0.5–5 Мбіт/с	від 1 Мбіт/с
Вимоги до затримки (delay)	< 150 мс	< 2–3 с	Некритична
Джитер (jitter)	< 20–30 мс	Некритичний	Некритичний

Продовження таблиці 2.1

Втрати пакетів	< 1%	до 2–3% допустимо	допустимі (TCP відновлює)
Пріоритет	Високий	Середній	Низький
Приклади реального використання	Голосові дзвінки, відеоконференції	Браузинг, хмарні сервіси, API	Резервне копіювання, обмін документами

Припустимо типовий сценарій пікового навантаження у мережі з пропускною здатністю 100 Мбіт/с: 5 одночасних VoIP-дзвінків, 10 користувачів працюють з веб-сервісами, 2 користувача виконують обмін файлами за FTP. Для FTP візьмемо значення 15 мбіт/с, для VoIP та веб-трафіку максимально можливе значення з табл. 2.1. Розрахунок:

$$5 \text{ дзвінків } VoIP = 5 * 100 \frac{\text{кбіт}}{\text{с}} = \ 500 \text{ кбіт/с } (0{,}500 \text{ Мбіт/с}) \quad (2.1)$$

$$\text{Веб} - \text{трафік } (10 \text{ користувачів}) = \ 10 \ \times \ 5 \text{ Мбіт/с} \ = \ 50 \text{ Мбіт/с} \quad (2.2)$$

$$FTP \ (2 \text{ користувачі}) = 2 \ \times \ 15 \text{ Мбіт/с} \ = \ 30 \text{ Мбіт/с} \quad (2.3)$$

$$VoIP + \text{Веб} - \text{трафік} + FTP = 0{,}500 + 50 + 30 \approx 80{,}5 \text{ Мбіт/с} \quad (2.4)$$

Для мережі з пропускною здатністю 100 Мбіт/с, навантаження 80,5 Мбіт/с становить приблизно 80% зайнятої пропускної здатності. У Cisco AVVID QoS Design Guide [16] вказано, що слід не перевищувати значення у 75% навантаження мережі для справної роботи VoIP. Можна зробити висновок, що у випадку вищевказаного сценарію, без налаштування QoS VoIP-трафік буде відчувати значну конкуренцію, і це призведе до погіршення зв’язку для користувачів.

Окрім прямої конкуренції за смугу пропускання, критичне значення мають наступні фактори:

- Використання UDP: VoIP використовує UDP (User Datagram Protocol), який порівняно з TCP доставляє дані швидше, але без підтвердження їх доставки. При значному перевантаженні мережі, пакети UDP просто не доходять до вузла призначення, внаслідок чого відбувається значне зменшення якості VoIP. [19, 21]

- Ефект TCP Global Synchronization: Коли FTP-трафік заповнює буфери маршрутизатора до максимуму (Tail Drop), відбувається одночасне відкидання пакетів багатьох TCP-сесій. Це змушує всі TCP-джерела синхронно зменшити швидкість, а потім знову її нарощувати. Такі «хвилі» навантаження створюють непередбачувані сплески затримок, які заважають стабільному проходженню VoIP. [19]

- Вплив джитеру: Для голосу важлива не лише швидкість, а й рівномірність надходження пакетів. FTP-трафік, що йде великими кадрами (1500 байт), затримує короткі пакети VoIP у черзі. Для цього існує Jitter Buffer, але коли кількість пакетів перевищують його місткість, ті що до нього не потрапили, ігноруються, що спричиняє ефект переривання голосу. [21]

- Співвідношення місткості черги та втрат: Без QoS маршрутизатор використовує алгоритм FIFO (First In, First Out). У випадку коли мережа перевантажена, черга стає практично постійно заповненою. Для TCP це сигнал до роботи, але для VoIP це означає, що кожен новий пакет голосу змушений чекати, поки обробляться масивні сегменти файлового пересилання, що штучно збільшує затримки понад 150-200 мс. [22]

Саме тому без механізмів пріоритезації QoS навіть при наявності вільної пропускної здатності якість VoIP суттєво знижується.

2.4 Аналіз існуючих рішень та вибір архітектури для забезпечення QoS

Вже відомо, що для забезпечення якості обслуговування в IP-мережах основними архітектурними підходами є Best-Effort, IntServ та DiffServ. Модель Best-Effort не забезпечує жодних гарантій і тому непридатна для сучасних

корпоративних мереж з мультимедійним трафіком, однак її можна використовувати з іншими підходами як допоміжну, наприклад для FTP трафіку.

Архітектура IntServ ідеально підходить для додатків з жорсткими вимогами, оскільки мережа «домовляється» про необхідні параметри (пропускну здатність, максимальну затримку) та резервує необхідні ресури мережі ще до початку передачі. Водночас суттєвим недоліком є необхідність зберігання детального стану кожного активного потоку на всіх проміжних маршрутизаторах. Це призводить до експоненційного зростання споживання оперативної пам’яті та процесорних ресурсів, що робить IntServ малопридатним для мереж із великою кількістю одночасних з’єднань.

На противагу цьому, DiffServ використовує агреговане, класо-орієнтоване обслуговування. Завдяки класифікації та маркуванню на вході в мережу за допомогою 6-бітового поля DSCP, такий підхід радикально підвищує масштабованість і знижує вимоги до ресурсів мережевого обладнання, оскільки пристроям у ядрі мережі не потрібно зберігати інформацію про окремі потоки. Однак, модель не забезпечує жорстких наскрізних гарантій і значною мірою залежить від узгодженості політик QoS між різними мережевими доменами.

Порівняльна характеристика архітектур наведена в таблиці 2.2.

Таблиця 2.2 Порівняльна характеристика архітекур QoS

Архітектура	**IntServ**	**DiffServ**	**Best-Effort**
Підхід	Per-flow, резервування ресурсів	Class-based, агрегування потоків	Відсутність гарантій
Механізм сигналізації	RSVP	DSCP-маркування	Відсутній
Масштабованість	Низька (зберігання стану кожного потоку)	Висока	Найвища

Продовження таблиці 2.2

Гарантії QoS	Жорсткі end-to-end	М’які, залежить від доменів	Відсутні
Складність реалізації	Висока	Середня	Низька
Рекомендоване застосування	Невеликі мережі, критичні потоки	Корпоративні та провайдерські мережі	Некритичний трафік

Більшість сучасних enterprise-компаній використовують саме модель DiffServ як основну архітектуру забезпечення QoS. Згідно з Cisco Enterprise QoS Solution Reference Network Design Guide (SRND) [19], DiffServ є рекомендованим підходом для корпоративних мереж завдяки високій масштабованості, гнучкості та ефективності при обробці змішаного трафіку (голос, відео та дані). Такі рішення успішно застосовуються в тисячах корпоративних мереж по всьому світу, зокрема в банківському секторі, виробничих компаніях, освітніх установах та великих офісних організаціях.и

У рамках даної кваліфікаційної роботи також обрано архітектуру DiffServ, оскільки вона найкраще відповідає масштабам і завданням моделюваної локальної корпоративної мережі малого підприємства.

Вибір цього методу обґрунтований його доброю масштабованістю при майбутньому збільшенні кількості користувачів і VLAN, відносною простотою реалізації на обладнанні Cisco за допомогою механізмів класифікації, маркування DSCP, class-map та policy-map. Він надає достатній рівень гарантій якості обслуговування для VoIP-трафіку та адміністративного трафіку в умовах локальної мережі. є можливість ефективної інтеграції з механізмами безпеки (ACL та VLAN сегментація).

Основними ризиками використання DiffServ є неправильне маркування трафіку, недостатнє узгодження політик між пристроями та відсутність жорстких end-to-end гарантій, що, втім, не є критичним для локальної корпоративної мережі.

Таким чином, для моделі корпоративної мережі малого підприємства (20 кінцевих пристроїв) з перспективою масштабування обрано архітектуру DiffServ.

Обрана архітектура DiffServ є оптимальним балансом між функціональністю, масштабованістю та складністю реалізації для умов даної роботи.

2.5 Опис досліджуваної корпоративної мережі

У даній роботі розглядає модель корпоративної локальної мережі, побудована на основі трирівневої ієрархічної архітектури Cisco. Згідно з цією концепцією, мережа поділяється на функціональні рівні, кожен з яких оптимізований для конкретних завдань. [23]

- Рівень розподілу (Distribution Layer): місце впровадження політик безпеки, інтелектуальної маршрутизації та агрегації каналів перед передачею трафіку на магістраль.

- Рівень ядра (Core Layer): відповідає за максимально швидку та безперебійну трансляцію масивних потоків даних без затримок на складну обробку пакетів.

- Рівень доступу (Access Layer): виступає безпосереднім інтерфейсом для кінцевих пристроїв, забезпечуючи їхнє входження в мережу та контроль доступу.

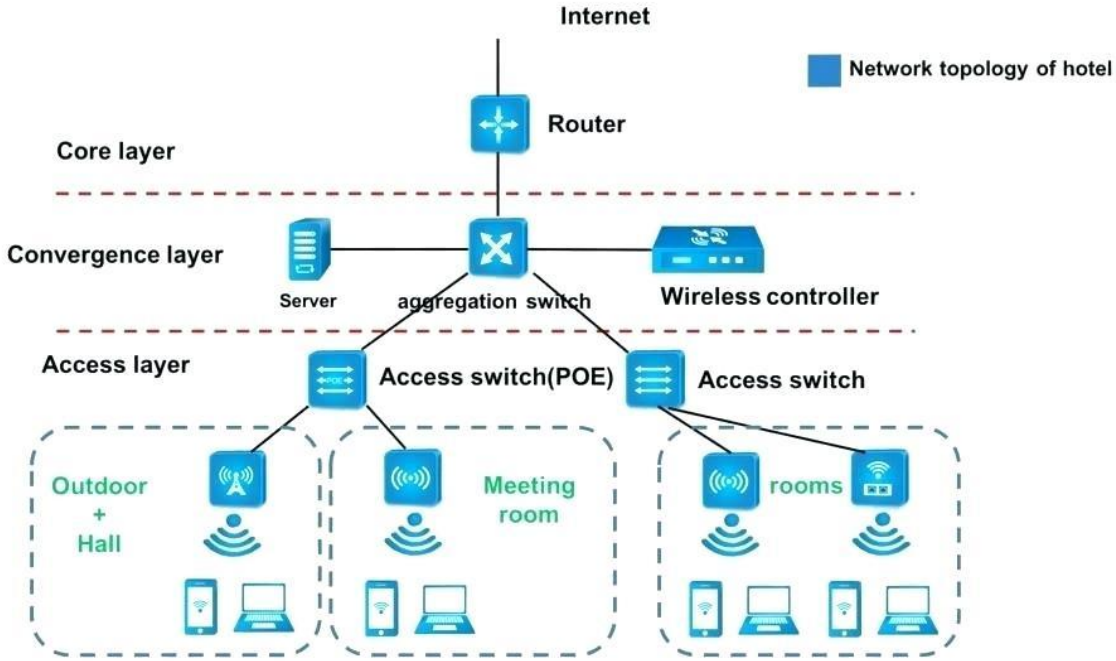


Рисунок 2.1 – Приклад мережі побудованої за зразком трирівневої ієрархічної моделі [23]

Для побудови мережі малого підприємства потрібно створити декілька логічних сегментів і використати для них наступне обладнання. Першим йде WAN-сегмент, до нього відносяться ISP Router, з’єднаний з Internet Server для симуляції зовнішньої мережі. Наступним сегментом є маршрутизація, де Edge Router знаходиться на рівні розподілу. Третім йде комутація, на ньому знаходятьсяодин Core Switch на рівні ядра та два Access Switch на рівні доступу, а також кінцеві пристрої у кількості: 5 IP-телефонів, 20 персональних комп’ютерів, та ноутбук.

Загальна структура мережі виглядає наступним чином: ISP Router з’єднаний з Internet Server виконує симуляцію WAN; Edge Router під’єднаний до ISP Router та Core Switch виконує функції маршрутизації в мережі; Core Switch об’єднує Edge Router і сегменти Access Switch, забезпечує роботу VLAN та технологій QoS, виконує роль сегментації та комутації між підмережами; роль Access switch полягає у тому, щоб забезпечити доступ кінцевих пристроїв до мережі через VLAN, відтворювати базову фільтрацію трафіку та передачу даних до Core Switch. Загальна топологія досліджуваної мережі представлена на рис. 2.2.

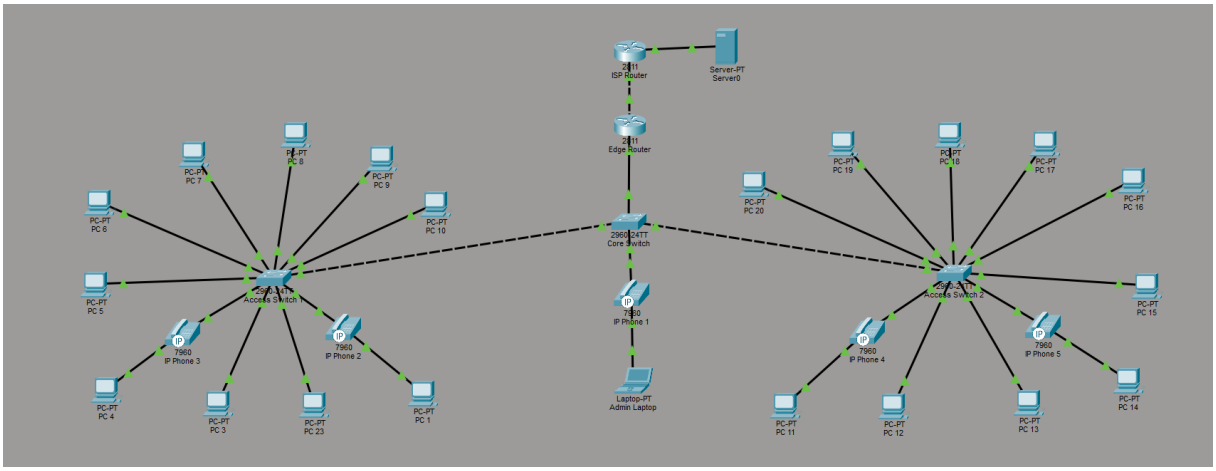


Рисунок 2.2 – Топологія локальної мережі підприємства

Для забезпечення якості обслуговування застосовуються наступні інструменти:

На Edge Router: маршрутизація VLAN, механізми Policing для надання пріорітетів пакетам, DHCP для автоматичного назначення IP-адрес кінцевим пристроям, IP-телефонія для забезпечення обміну VoIP, засосування ACL для підвищення рівня безпеки.

На комутаторах: сегментація за допомогою VLAN та забезпечення передачі пакетів у мережі.

Таким чином, актуальною задачею є розробка мережі, яка забезпечує пріоритезацію трафіку, ефективне використання пропускної здатності та базовий рівень безпеки.

3 РОЗРОБКА ЛОКАЛЬНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ З ПІДТРИМКОЮ QoS

3.1 Побудова топології

Початком побудови локальної корпоративної мережі буде розміщення та об’єднання пристроїв в структуру описану у другому розділі.

Після розміщення пристроїв, наступним кроком буде з’єднання пристроїв за допомогою кабелів Ethernet. Для однотипних з’єднань використовуються перехресні або кросс-кабелі (copper cross-over), в цьому випадку це маршрутизатори та комутатори. Для різнотипних з’єднань використовуються кабелі типу прямий (copper straight-through).

Далі, після фізичного з’єднання всіх пристроїв, виконується початкове налаштування мережевого обладнання, яке включає уввімкнення портів використовуючи команду, призначення IP-адрес інтерфейсам, комутаторів та маршрутизаторів, а також перевірку коректності встановлених з’єднань.

Коли початкові налаштування виконані можна переходити до введення команд налаштувань на пристроях. Повний перелік команд наведений у додатку А.

3.2 Налаштування VLAN

Наступним кроком буде налаштування VLAN для реалізації сегментації мережі. Для цього на Access Switch 1 потрібно відкрити CLI, та ввести такі команди: vlan 10 name VOICE; vlan 20 name DATA. Таким чином ми створюємо два VLAN: першому VLAN призначена назва VOICE та номер 10, тому він буде відповідати за голосовий трафік. Другий VLAN відповідає за решту даних, він має назву DATA і його номером буде 20. Далі надаємо доступ до VLAN портам кінцевих користувачів. Для цього вводимо команду interface і номер порту до якого під’єднаний кінцевий пристрій. Тепер вводимо команду switchport mode access.

Вводимо команду switchport access vlan 20 для закріплення VLAN за інтерфейсом. Додатково можна ввести команду spanning-tree portfast для пропуску стандартних етапів ініціалізації, що зменшить затримку підключення пристрою до мережі. Повторюємо такі ж дії на інших ПК. На портах з IP-телефонами додатково вводимо команду switchport voice vlan 10 для передачі VoIP-трафіку.

Після цього прокладаємо trunk-з'єднання до Core Switch для передачі трафіку кількох VLAN через один фізичний канал. Для цього використовується протокол IEEE 802.1Q, який додає тег VLAN до кожного кадру. Вводимо команду switchport mode trunk попередньо перейшовши на порт до якого під'єднаний Core Switch.

Виконуємо ті самі дії також і на Access Switch 2. Перевірка налаштувань наведена на рис. 3.1.

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up


AccessSwitch1>en
AccessSwitch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
AccessSwitch1(config)#exit
AccessSwitch1#
%SYS-5-CONFIG_I: Configured from console by console

AccessSwitch1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig0/1, Gig0/2
10   VOICE                            active    Fa0/2, Fa0/5
20   DATA                             active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
AccessSwitch1#
```

Рисунок 3.1 – Список налаштувань VLAN на Access Switch

Далі буде налаштування VLAN на Core Switch. Таким самим чином як і на Access Switch створюємо Voice VLAN та Data VLAN. Далі треба прокласти trunk-и до обох Access Switch та до Edge Router.

Найважливіші налаштування будуть виконуватися на Edge Router. На ньому потрібно налаштувати маршрутизацію VLAN трафіку. Для цього використовується схема Router-on-a-Stick, яка дозволяє створити декілька підінтерфейсів на одному інтерфейсі, що дозволяє призначити кожному з них свій VLAN. Для цього вводимо такі команди: interface fa0/1.10; encapsulation dot1Q 10; ip address 192.168.10.1 255.255.255.0. Першою командою ми створили підінтерфейс, наступною командою ми створили спеціальний тег, для того щоб розрізняти який це тип VLAN, а остання команда створила стандартний шлюз та маску підмережі для голосового типу трафіку. Відповідно для Data VLAN вводимо ці команди: interface fa0/1.20; encapsulation dot1Q 20; ip address 192.168.20.1 255.255.255.0. В кінці створюємо trunk до Core Switch.

```
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
2 FastEthernet interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.20, changed state to up


EdgeRouter>en
EdgeRouter#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  up                    up
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/1.10     192.168.10.1    YES manual up                    up
FastEthernet0/1.20     192.168.20.1    YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
EdgeRouter#
```

Рисунок 3.2 – Список налаштувань інтерфейсів на Edge Router

3.3 Налаштування DHCP

VLAN є важливою частиною розроблюваної мережі, але для коректної роботи пристроїв не вистачає повноцінної IP-адресації. Для цього використовується технологія DHCP.

DHCP – це мережевий протокол, який автоматично назначає IP-адреси, виключаючи необхідність назначати їх вручну. Завдяки цьому протоколу, можна створити окремі DHCP pool-и для кожної VLAN та ефективно реалізовувати політики QoS на рівні логічних сегментів мережі, а не окремих пристроїв.

Пристрій, який керуватиме DHCP буде Edge Router. Тому перейдемо до його налаштування.

Першою командою для введення буде - ip dhcp pool VOICE. Ця команда створює область IP-адрес для їх назначення IP-телефонам. Команда network 192.168.10.0 255.255.255.0 визначає мережу та діапазон з якого будуть братися IP-адреси. За замовчуванням це 192.168.10.2 – 192.168.10.254.

Цією командою default-router 192.168.10.1, ми вказуємо стандартний шлюз до якого буде звертатися пристрій.

Остання команда option 150 ip 192.168.10.1 є стандартною командою для налаштування IP-телефонів у VLAN.

Відповідно для створення області IP-адрес для ПК вводимо наступні команди: ip dhcp pool DATA; network 192.168.20.0 255.255.255.0; default-router 192.168.20.1. Перевірка наведена на рис. 3.3.

```
Press RETURN to get started!


%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.20, changed state to up


EdgeRouter>en
EdgeRouter#show ip dhcp pool

Pool VOICE :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 3
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.10.1         192.168.10.1     - 192.168.10.254    0    / 3     / 254

Pool DATA :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Excluded addresses             : 3
 Pending event                  : none

 1 subnet is currently in the pool
 Current index        IP address range                    Leased/Excluded/Total
 192.168.20.1         192.168.20.1     - 192.168.20.254    0    / 3     / 254
EdgeRouter#
```

Рисунок 3.3 – Список налашувань DHCP Pool

Для отримання IP-адрес на ПК, потрібно перейти до пристрою, відкрити вкладку Desktop, обрати додаток IP-Configuration та увімкнути DHCP. Побачити як це виглядає можна на рис. 3.4.

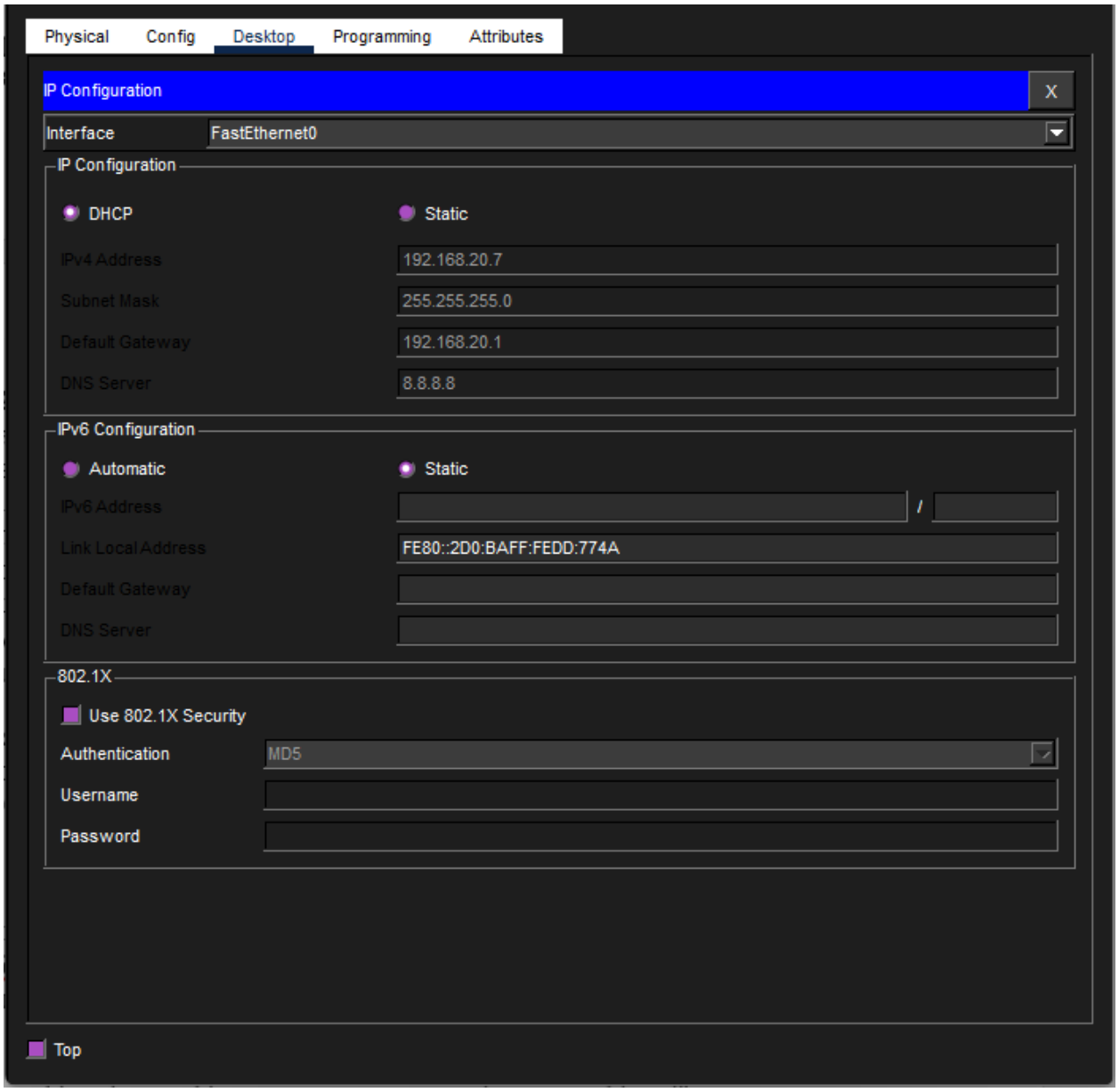


Рисунок 3.4 – Налаштований DHCP на ПК

3.4 Налаштування сервісу телефонії

Далі потрібно перейти до налаштування сервісу телефонії, для коректної роботи IP-телефонів.

Вносити команди потрібно також на Edge Router. Почнемо з команди telephony-service. Вона вмикає однойменний сервіс, завдяки якому на маршрутизаторі починає працювати локальна телефонна станція, яка керує IP-телефонами у мережі. Далі, командою max-ephones визначаємо максимальну

кількість телефонів у мережі (в нашому випадку 5), і відповідно наступною max-dn визначаємо максимальну кількість номерів.

Команда ip source-address 192.168.10.1 port 2000 визначає адресу та спеціальний SCCP- порт для адресації дзвінків. Командою auto assign 1 to 5, ми автоматично назначаємо номери IP-телефонам. Рештою команд створюємо телефонні лінії та відповідно назначаємо їм номери: ephone-dn 1; number 1001; ephone-dn 2; number 1002; ephone-dn 3; number 1003; ephone-dn 4; number 1004; ephone-dn 5; number 1005. Після введення команд, у мережі можна повноцінно спілкуватися через IP. Перевірка наведена на рис. 3.5.

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.20, changed state to up


EdgeRouter>en
EdgeRouter#show ephone

ephone-1 Mac:000B.BE24.9D7B TCP socket:[1] activeLine:1 UNREGISTERED
mediaActive:0 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:0.0.0.0 0 7960   keepalive 43 max_line 2
 button 1: dn 3  number 1003 CH1   DOWN

ephone-2 Mac:0090.0CE6.25A2 TCP socket:[1] activeLine:1 UNREGISTERED
mediaActive:0 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:0.0.0.0 0 7960   keepalive 43 max_line 2
 button 1: dn 1  number 1001 CH1   DOWN

ephone-3 Mac:0090.2BAC.106E TCP socket:[1] activeLine:1 UNREGISTERED
mediaActive:0 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:0.0.0.0 0 7960   keepalive 43 max_line 2
 button 1: dn 4  number 1004 CH1   DOWN

ephone-4 Mac:0001.96AD.A0D7 TCP socket:[1] activeLine:1 UNREGISTERED
mediaActive:0 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:0.0.0.0 0 7960   keepalive 43 max_line 2
 button 1: dn 2  number 1002 CH1   DOWN

ephone-5 Mac:0060.2F7E.4BA4 TCP socket:[1] activeLine:1 UNREGISTERED
mediaActive:0 offhook:1 ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:8
IP:0.0.0.0 0 7960   keepalive 43 max_line 2
 --More--
%IPPHONE-6-REGISTER: ephone-4 IP:192.168.10.2 Socket:2 DeviceType:Phone has registered.
 button 1: dn 5  number 1005 CH1   DOWN
EdgeRouter#
%IPPHONE-6-REGISTER: ephone-3 IP:192.168.10.4 Socket:2 DeviceType:Phone has registered.

%IPPHONE-6-REGISTER: ephone-2 IP:192.168.10.5 Socket:2 DeviceType:Phone has registered.

%IPPHONE-6-REGISTER: ephone-5 IP:192.168.10.3 Socket:2 DeviceType:Phone has registered.
```

Рисунок 3.5 – Список налаштувань IP-телефонії

3.5 Налаштування QoS

Головним етапом налаштування стане впровадження механізмів QoS за зразком моделі DiffServ, яка допоможе розділити трафік на важливий і звичайний для його кращої обробки.

Слід почати з впровадження маркування. На цьому етапі визначаються класи трафіку за значенням DSCP, пакети групуються відповідно до їхньої пріоритетності ще до обробки в мережі. Створюються класи за допомогою команди class-map match-any. Для голосового трафіку створюється клас VOICE -class-map match-any VOICE. Команда match ip dscp ef означає, що до класу VOICE потрапляють пакети з DSCP значенням Expedited Forwarding, які використовуються для голосового трафіку з мінімальною затримкою.

Для адміністративного трафіку створюється клас Admin: class-map match-any ADMIN; match ip dscp af21. Тут використовується клас AF21, який належить до Assured Forwarding і має середній пріоритет. Для звичайного трафіку створюється клас Data: class-map match-any DATA match ip dscp default. До цього класу потрапляє весь трафік без спеціального маркування, тобто по Best-effort.

На наступному етапі будуть налаштування policing. Тут ми визначаємо, які дозволи на використання ресурсів у мережі будуть визначені для кожного класу трафіку. Для цього створюємо політику QOS-POLICY вводячи команду policy-map QOS-POLICY. Далі задаємо пріоритет для голосового трафіку наступними командами: class VOICE; priority percent 30. Таким чином, для VOICE виділяється гарантований пріоритет і до 20% пропускної здатності, що забезпечить мінімальні затримки.

Для адміністративного трафіку вводимо команди class ADMIN та bandwidth percent 5. Комп’ютеру адміністратора було виділено 15% пропускної здатності, а у поєднанні з Assured Forwarding, він отримує вищий пріорітет передачі.

Для звичайного трафіку йдуть команди class DATA та bandwidth percent 40. Цьому класу виділяється 40% пропускної здатності за принципом Best Effort, тобто без гарантій жорстких параметрів QoS.

Після цього політика застосовується до інтерфейсу виходу на Core Switch: interface fa0/1; service-policy output QOS-POLICY, що означає, що всі вихідні пакети через інтерфейс fa0/1 обробляються відповідно до заданих класів QoS.

Тепер слід налаштувати списки доступу ACL для обмежень доступу до певних ресурсів, додаткової фільтрації та класифікації трафіку на основі IP-адрес та портів. Спочатку створимо ACL 110 для голосового трафіку. Команда access-list 110 permit udp any any eq 5060 активує дозвіл для UDP-трафіку через порт 5060, що необхідно для встановлення зв'язку; access-list 110 permit udp any any range 16384 32767 відкриває діапазон портів для передачі голосових пакетів; access-list 110 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255 виконує функцію безпеки, забороняючи прямий доступ між підмережами Voice та Data; access-list 110 permit ip any any дає дозвіл на пропуск усього іншого трафіку, що забезпечує нормальну роботу мережі для інших сервісів.

Далі створюється ACL 120 для обмеження доступу до усіх веб-сайтів, окрім тих що працюють на протоколі HTTPS (HyperText Transfer Protocol Secure). Команда access-list 120 permit tcp 192.168.20.0 0.0.0.255 any eq 443 визначає дозвіл на передачу пакетів TCP діапазону ip-адрес з підмережі Data до будь якої ip-адреси, яка працює через 443 порт, який закріплений за HTTPS. Команда access-list 120 deny ip 192.168.20.0 0.0.0.255 any обмежує усі інші типи з’єднань.

Тепер необхідно застосувати ACL до підінтерфейсів маршрутизатора: interface fa0/1.10, ip access-group 110 in; interface fa0/1.20, ip access-group 120 in. Таким чином, фільтрація виконується на вході в мережу через відповідні VLAN.

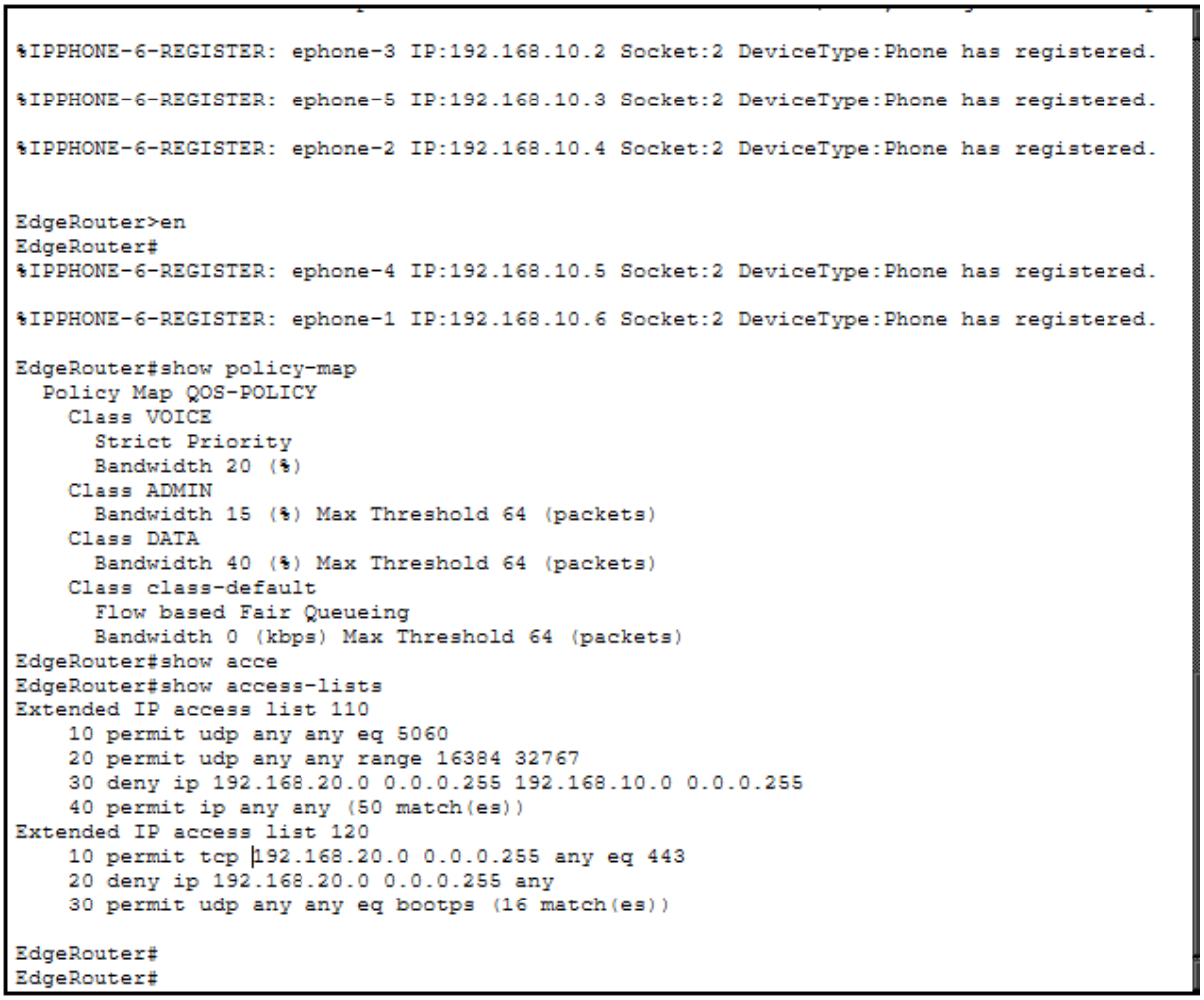


Рисунок 3.6 – Список налаштувань Policing та ACL

Наостанок, необхідно налаштувати ISP Router та Internet Server, для того щоб отримувати доступ у зовнішню мережу. На сервері задаються базові мережеві параметри: IP: 100.0.0.2; Mask: 255.255.255.0; Gateway: 100.0.0.1. Це дозволяє серверу взаємодіяти з іншими мережами через шлюз ISP.

На стороні ISP налаштовуються інтерфейси та шлюзи для доступу до серверу. Налаштовуємо шлюз та вмикаємо порт на інтерфейсі з підключеним Edge Router: interface fa0/0, ip address 192.168.100.1 255.255.255.0, no shutdown.

На Edge Router налаштовується інтерфейс до ISP та вмикається порт: interface fa0/0; ip address 192.168.100.2 255.255.255.0 no shutdown

Командою ip route 0.0.0.0 0.0.0.0 192.168.100.1 встановлюється маршрут за замовчуванням для перенаправлення даних на шлюз ISP.

Встановлюємо шлюз та вмикаємо порт для сервера: interface fa0/1, ip address

100.0.0.1 255.255.255.0, no shutdown.

Також додаються маршрути до внутрішніх мереж для перенаправлення трафіку з ISP на шлюз Edge Router. Для Voice VLAN вводимо ip route 192.168.10.0 255.255.255.0 192.168.100.2; Для Data VLAN вводиться ip route 192.168.20.0 255.255.255.0 192.168.100.2.

Це забезпечує вихід до зовнішнього сервера через ISP.

3.6 Тестування мережі

Завершальною частиною будування схеми є її тестування. Для перевірки роботи QoS, створимо навантаження на мережу, та встановимо з’єднання між двома IP-телефонами.

Для початку, потрібно перейти у режим симуляції, для повного відстежування шляху пакетів.

Найпростішим способом навантаження мережі буде відправка FTP-пакетів між кінцевими пристроями. Для цього в Packet Tracer існує утиліта Traffic Generator, яку можна використати з будь-якого комп’ютера в мережі. Для перевірки роботи ACL та налаштувань маршрутів, відкриємо сайт віддаленого серверу через веб-браузер, який також викликається з комп’ютера.

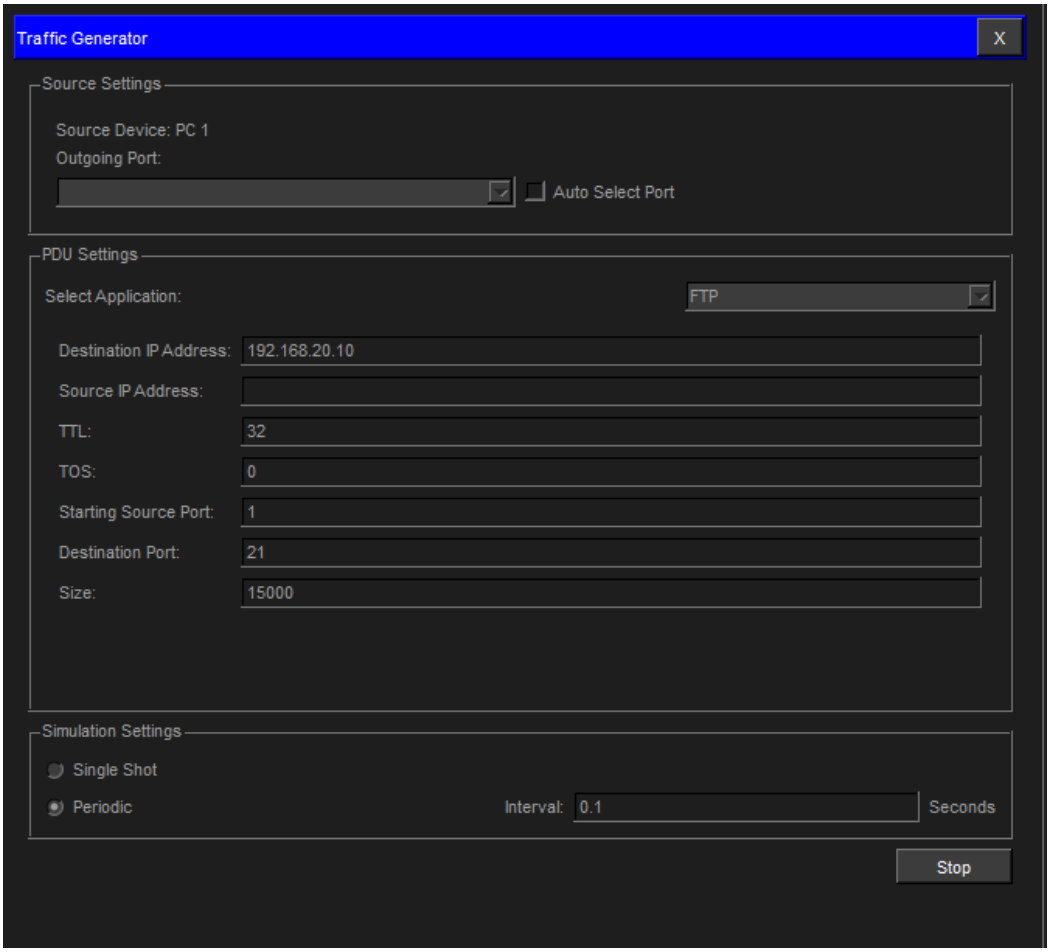


Рисунок 3.7 – Вікно налаштувань застосунку Traffic Generator

На рис. 3.7 наведені налаштування Traffic Generator, а саме кінцева IP-адреса, порти відправки та отримання, розмір, який ставляє 15000 байтів та інтервал у 0.1 секунду з яким будуть відправлятися пакети з даними. Такі налаштування будуть внесені до 10 ПК з адресою Admin Laptop з метою симулювати обмін файлами між ними.

Для початку перевіримо мережу без налаштувань policing та class-map. Створене навантаження наведено на рис. 3.8.

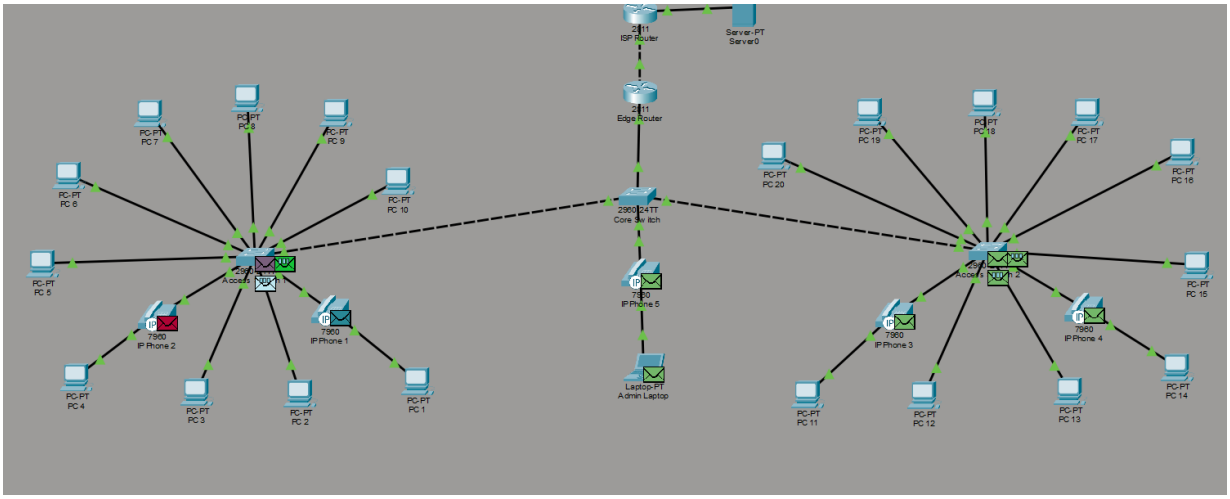


Рисунок 3.8 – Початок передачі пакетів з даними до пристроїв-отримувачів

Після створення навантаження на мережу, обираємо IP Phone 1 та вводимо номер телефону на який хочемо подзвонити. В нашому випадку, це буде IP Phone 5 і відповідно вводимо номер 1005, щоб ініціювати дзвінок.

Переключаємось до режиму симуляції, та натискаємо кнопку старту. На рис. 3.9 видно, що службовий пакет з даними про ініціювання дзвінку SCCP затримується на рівні маршрутизації, на відміну від пакету з даними TCP. З даних, наведених на рис. 3.10 можна побачити, що в мережі без застосувань механізмів QoS, початок відправлення RTP-пакетів починається тільки через 0.324 с або 324 мс, що не відповідає стандартам ITU-T G.114 про затримку у 150 мс для якісного спілкування через VoIP.

Можна зробити висновок, що передача даних у мережі відбувається за принципом Best-effort, і тому дзвінок проходить з затримками.

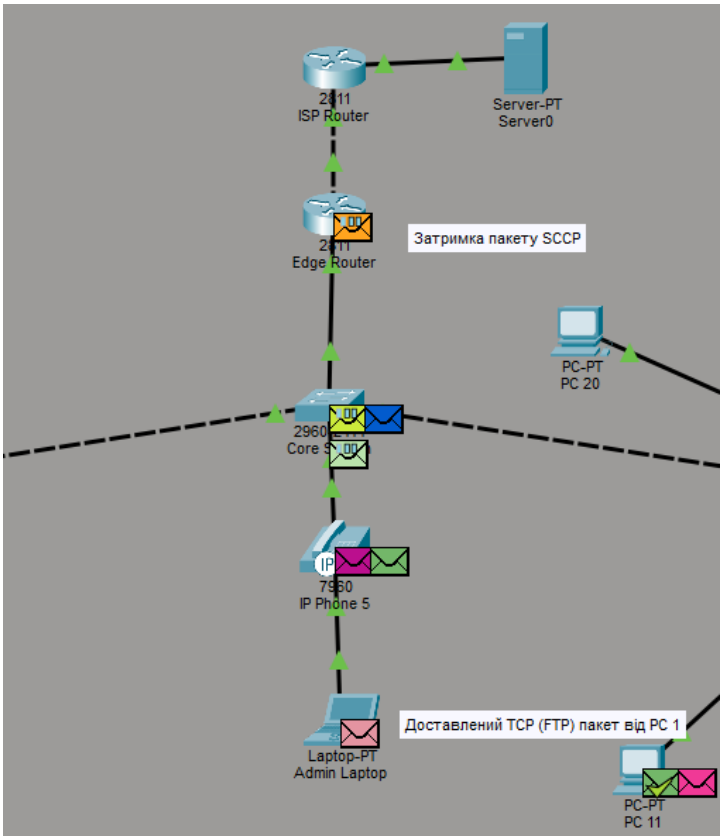


Рисунок 3.9 – Затримка службового пакету SCCP без налаштувань QoS

	0.320	IP Phone 5	Core Switch	SCCP
	0.320	IP Phone 1	Access Switch 1	SCCP
	0.321	Core Switch	Edge Router	SCCP
	0.321	Access Switch 1	Core Switch	SCCP
	0.322	Edge Router	Core Switch	SCCP
	0.322	Core Switch	Edge Router	SCCP
	0.323	Core Switch	Access Switch 1	SCCP
	0.323	Edge Router	Core Switch	SCCP
	0.324	Access Switch 1	IP Phone 1	SCCP
	0.324	Core Switch	IP Phone 5	SCCP
	0.324	--	IP Phone 1	RTP
	0.324	--	IP Phone 5	RTP
	0.325	IP Phone 1	Access Switch 1	RTP
	0.325	IP Phone 5	Core Switch	RTP
	0.326	Access Switch 1	Core Switch	RTP
	0.326	Core Switch	Access Switch 1	RTP
	0.326	PC 3	Access Switch 1	TCP
	0.326	PC 4	IP Phone 2	TCP

Рисунок 3.10 – Час надходження пакетів RTP з VoIP-даними

Тепер, перевіряємо мережу з налаштованими правилами пріорітезації та маркування. Створюємо таке саме навантаження в мережі, натискаємо кнопку старту симуляції та спостерігаємо за шляхом пакетів. На рис. 3.11 видно, що на

одному з проміжків часу пакети з даними від PC 1 затримуються, тоді як пакети з IP Phone 1 проходять до IP Phone 5 першими. Це наочно демонструє роботу механізму пріоритезації трафіку: комутатор ідентифікує голосові пакети як високий пріоритет і обробляє їх поза чергою, тоді як FTP-трафік від комп'ютера тимчасово буферизується, щоб уникнути затримок у розмові.

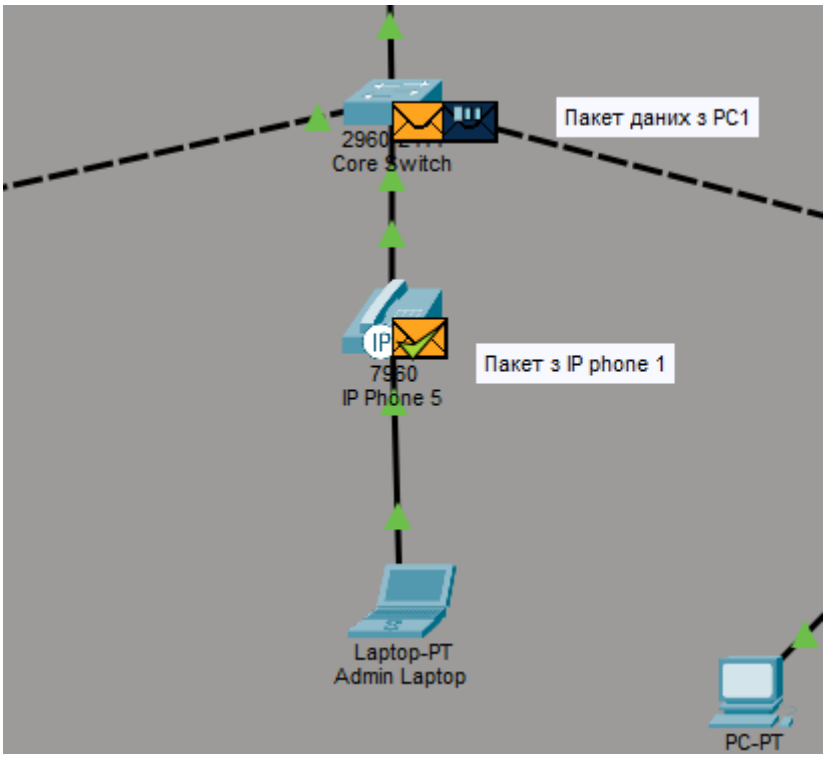


Рисунок 3.11 – Порядок надходження пакетів з даними

Далі, на рис. 3.12 можна побачити час проходження пакетів від пристрою до пристрою. В нашій мережі RTP пакети з даними VoIP почались передаватися через 0.026 с або 26 мс, що задовільняє вимоги міжнародних стандартів ITU-T G.114, про затримку в один бік до 150 мс, що вважається практично непомітною для людського вуха та забезпечує відмінну якість передачі голосу. Таким чином, завдяки застосуванню механізмів QoS було зменшено затримку голосових даних більш ніж в 10 разів.



Рисунок 3.12 – Час проходження пакетів

У нижній частині структури пакету на рис 3.13, можна побачити поле VoIP Data. Це саме ті оцифровані дані голосу, які були запаковані в пакети для пересилання мережею. Це сигналізує про успішний обмін голосовим трафіком після того, як усі правила пріоритезації були застосовані в мережі.

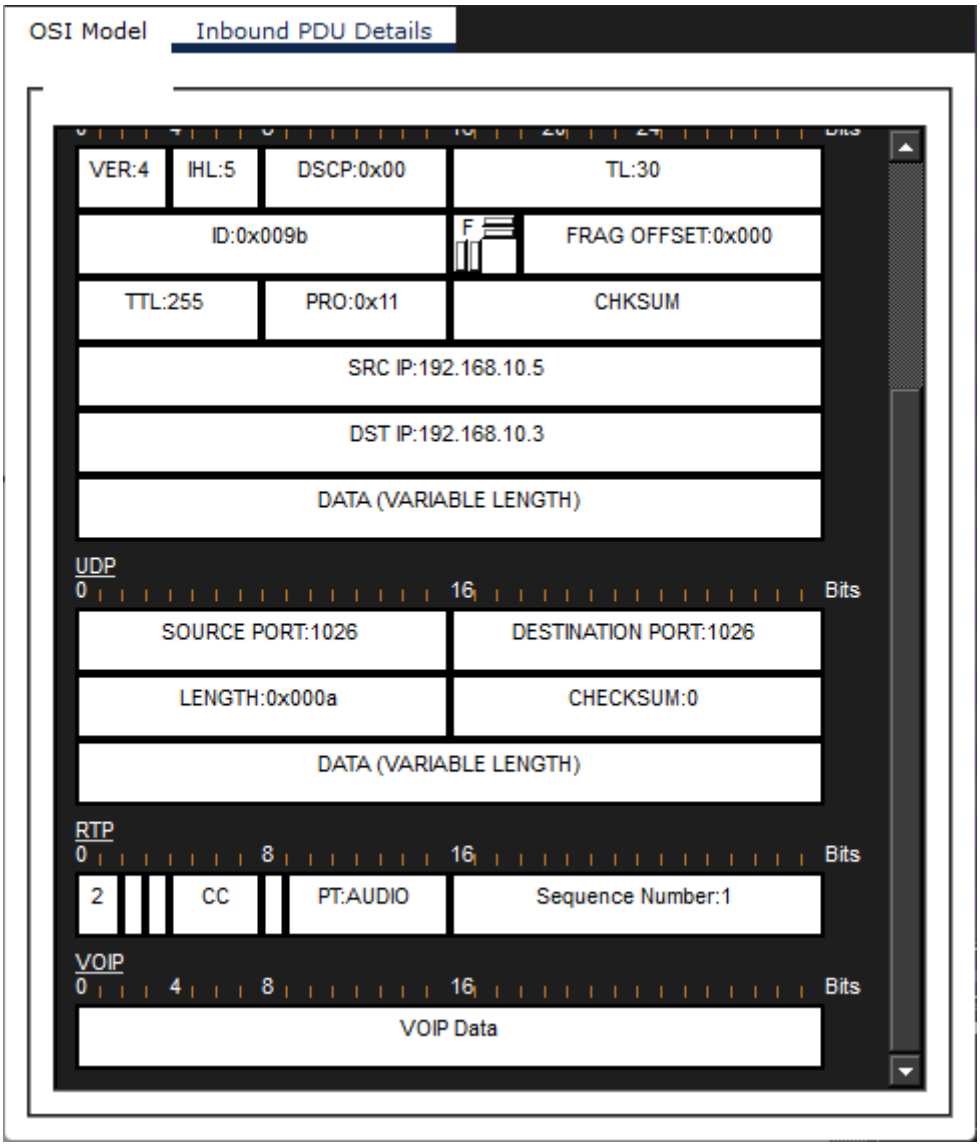


Рисунок 3.13 - Переданий RTP пакет з даними голосу

Далі можна перевірити роботу ACL. На рис. 3.14, можна побачити, що при спробі використати команду ping з комп’ютера в напряму до ip-телефона, він відкидається. Це підтверджує те, що запит на виклик не зміг пройти через налаштований ACL-список на маршрутизаторі, що задовільняє умовам безпеки.

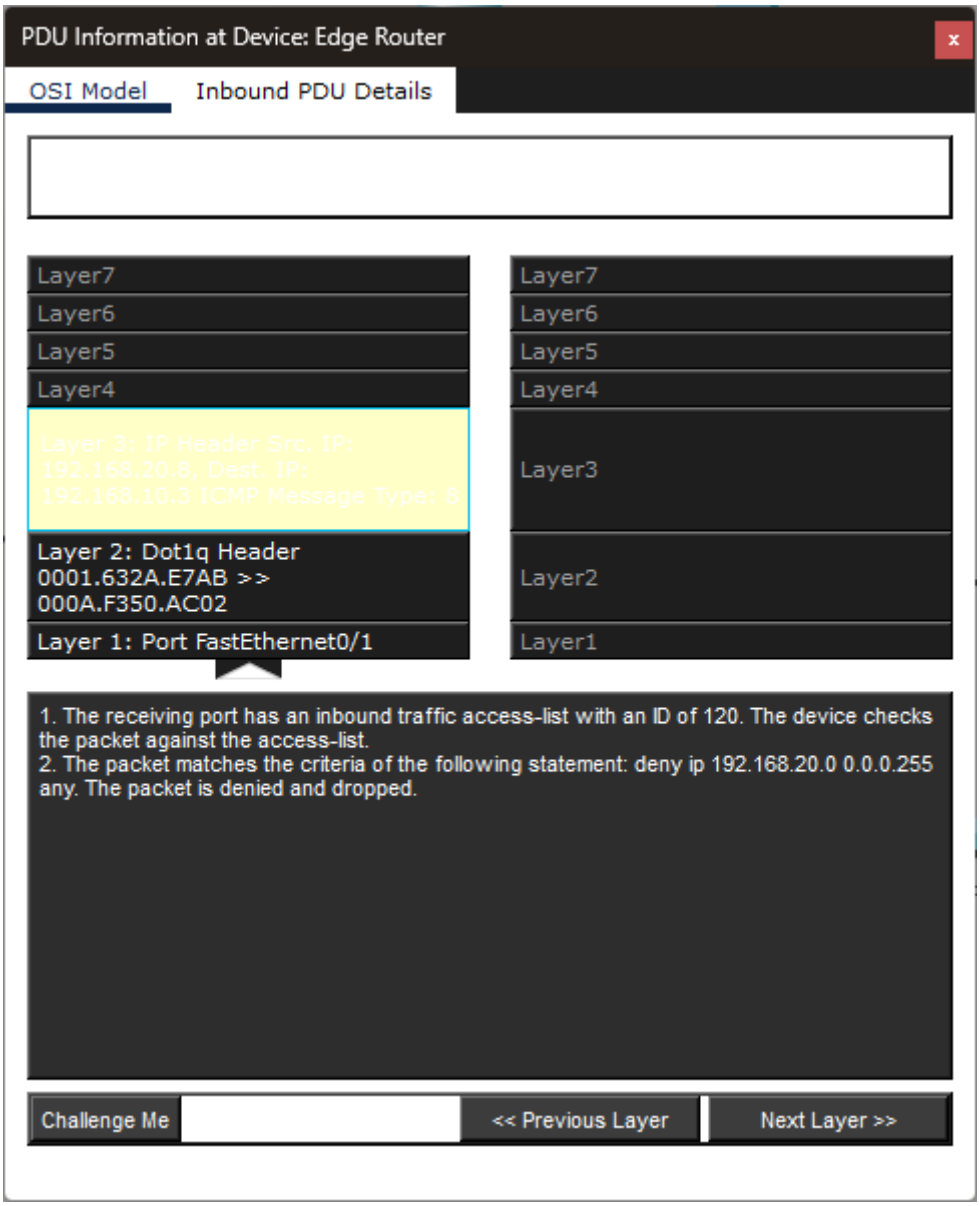


Рисунок 3.14 – Скинутий пакет з даними про ping IP-телефона

Наостанок, перевіримо доступ до веб-сайту на сервері. Спочатку спробуємо отримати доступ до незахищеного протоколу HTTP. На рис. 3.15. видно, що пакет було скинуто через правила налаштування ACL.

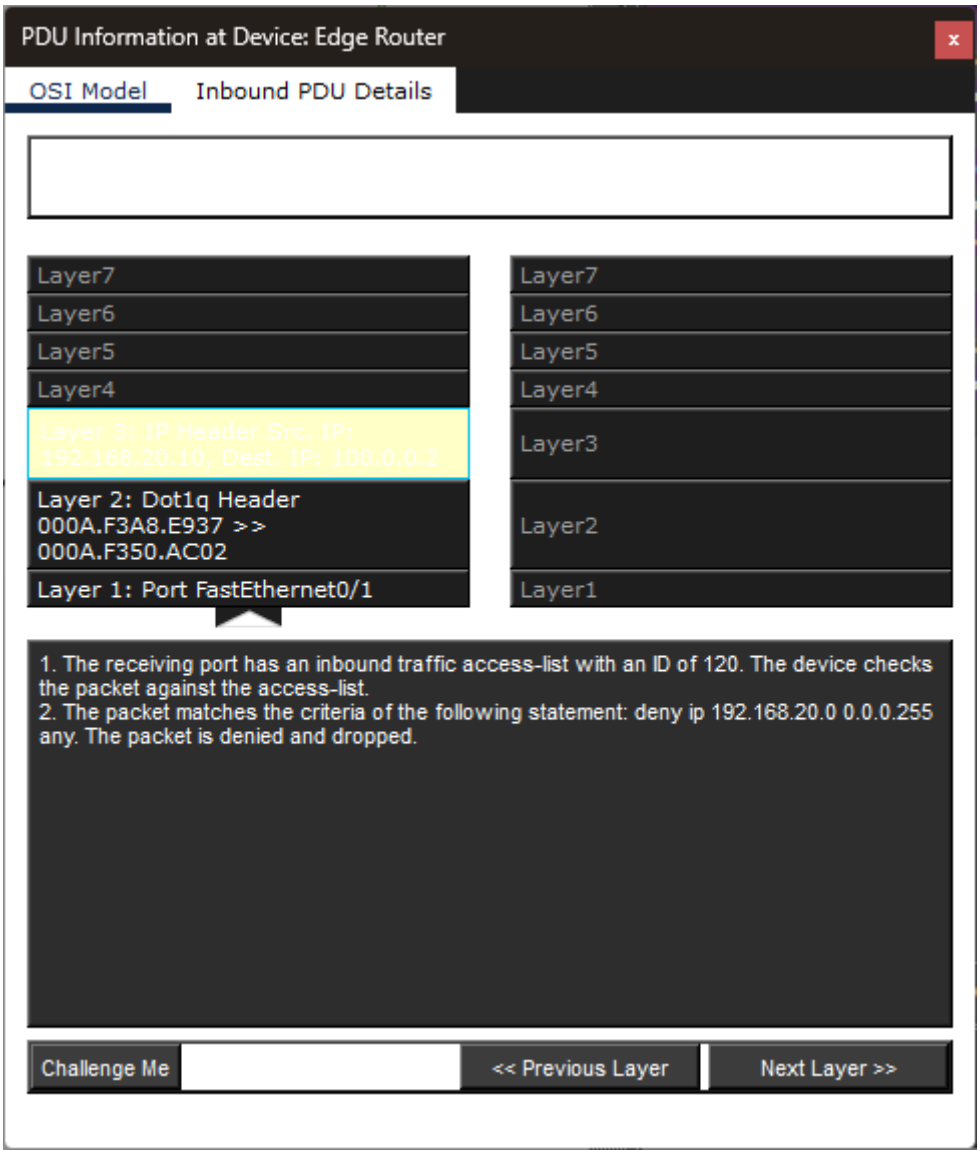


Рисунок 3.15 – Скинутий пакет з даними про доступ до HTTP

Тепер, отримаємо доступ до сайту через протокол HTTPS. На рис. 3.16 наведена інформація про дозвіл проходження пакету за ACL. Тому можна стверджувати, що маршрутизація та правила безпеки налаштовані вірно і не перешкоджають роботі дозволених сервісів. Успішне завантаження сторінки через HTTPS також показано на рис 3.17.

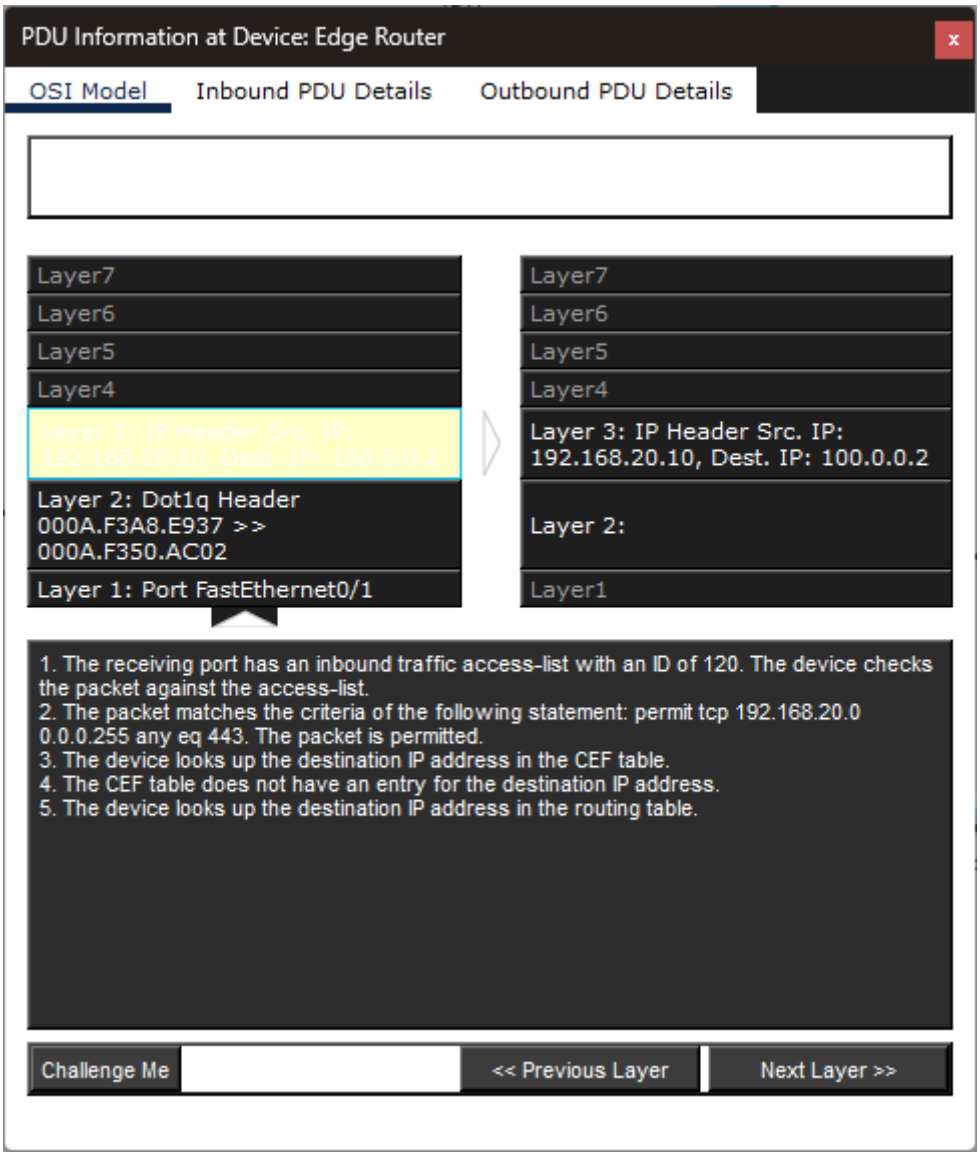


Рисунок 3.16 – Пакет з даними про доступ до HTTPS

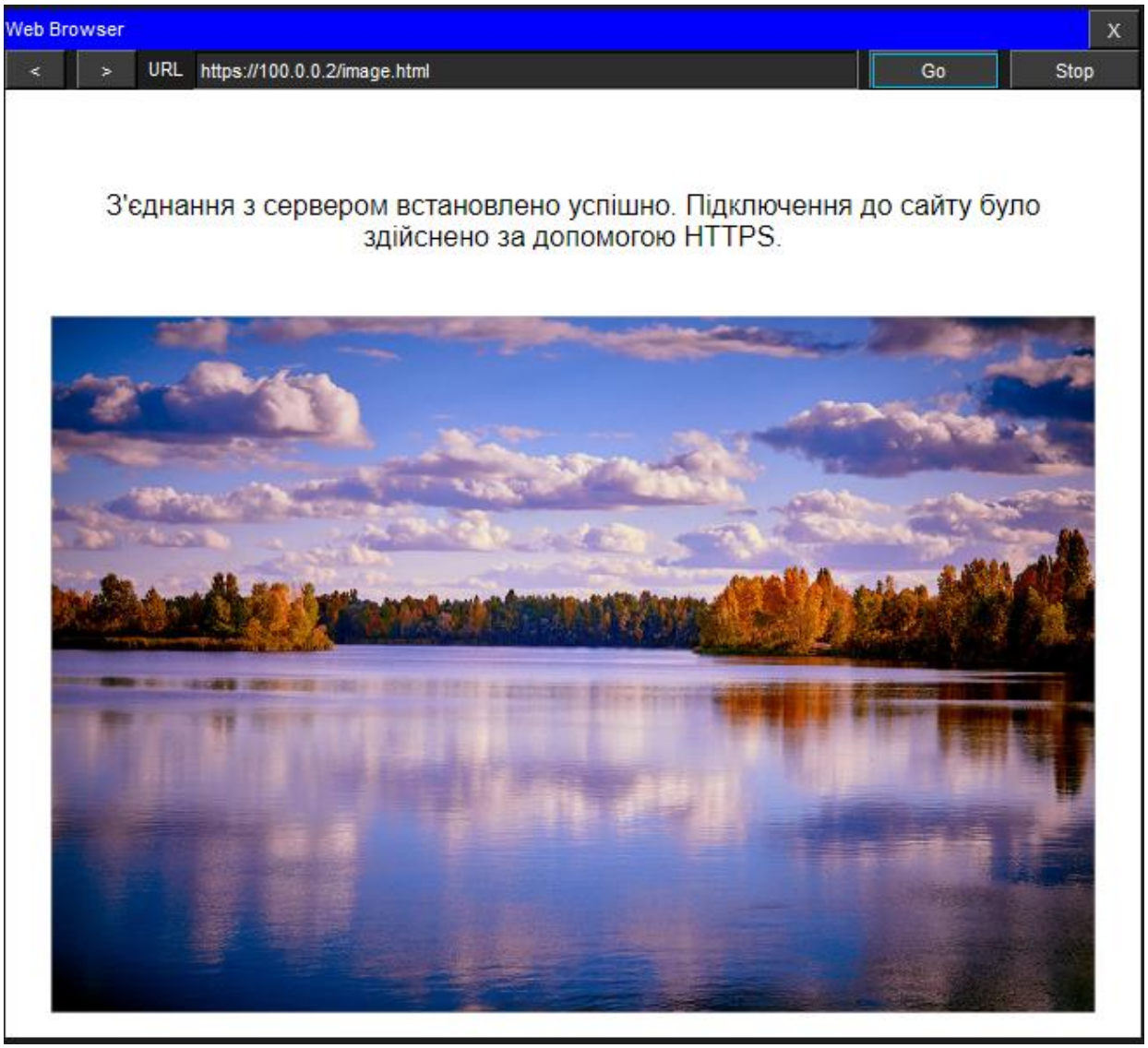


Рисунок 3.17 – Відкритий сайт на базі протоколу HTTPS

ВИСНОВКИ

У кваліфікаційній роботі були проаналізовані сучасні підходи до забезпечення якості обслуговування в корпоративних комп'ютерних мережах, а також розроблено варіант топології локальної мережі із застосуванням механізмів QoS та правил безпеки. Як окремий важливий елемент організації мережі розглянуто модель для реалізації якості обслуговування, з метою ефективно розподіляти мережеві ресурси між різними типами сервісів.

У роботі розглянуто типові завдання забезпечення якості обслуговування, зокрема управління затримками і втратами пакетів, а також задачі інформаційної безпеки, пов'язані з контролем доступу та сегментацією мережі. Проаналізовано вплив перевантажень на якість обслуговування, розглянуто традиційні підходи до організації мереж без використання QoS і визначено їх основні недоліки.

Для дослідження QoS, в середовищі Cisco Packet Tracer була розроблена локальна корпоративна мережа, з використанням методів пріоретизації, класифікування та маркування пакетів що, дозволило зменшити затримки у проходження пакетів VoIP у мережі більш ніж у 10 разів порівняно з варіантом мережі без забезпечення QoS. Зокрема в ній була реалізована сегментація та були введені списки доступу, які також підвищили ефективність та загальний рівень безпеки мережі.

Використання комплексного підходу до поєднання QoS і механізмів безпеки дозволило забезпечити стабільну роботу таких критично важливих сервісів, таких як VoIP, та HTTPS, тому, впроваджене рішення відповідає сучасним вимогам до рівня якості обслуговування в корпоративних мережах, забезпечує гнучкість, масштабованість і надійність їх функціонування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Е.Таненбаум, Н.Фімстер, Д.Везеролл. Комп'ютерні мережі 6-е видання.

2. Локальна Мережа. [Електронний ресурс] - Режим доступу: https://uk.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0

3. Local Area Networks. [Електронний ресурс] – Режим доступу: https://ipcisco.com/local-area-networks/

4. IEEE 802.3. [Електронний ресурс] - Режим доступу: https://uk.wikipedia.org/wiki/IEEE_802.3

5. Мережеве обладнання. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B5_%D0%BE%D0%B1%D0%BB%D0%B0%D0%B4%D0%BD%D0%B0%D0%BD%D0%BD%D1%8F

6. VLAN. [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/VLAN

7. Модель OSI [Електронний ресурс] - Режим доступу: https://javarush.com/ua/quests/lectures/ua.questservlets.level08.lecture01

8. Quality of service. [Електронний ресурс] - Режим доступу: https://en.wikipedia.org/wiki/Quality_of_service

9. Managing IP Networks: Challenges and Opportunities. [Електронний ресурс] -Режим доступу: https://www.researchgate.net/publication/303760331_Quality_of_Service_in_IP_Networks

10. Understanding QoS Basic [Електронний ресурс] - Режим доступу: https://support.huawei.cn/enterprise/en/doc/EDOC1100562995/dd1b06d9/understanding-qos-basic

11. Integrated Services in the Internet Architecture: an Overview. [Електронний ресурс] – Режим доступу: https://datatracker.ietf.org/doc/html/rfc1633

12. An Architecture for Differentiated Services. [Електронний ресурс] – Режим

доступу: https://datatracker.ietf.org/doc/html/rfc2475

13. Policing and shaping. [Електронний ресурс] – Режим доступу: https://www.networkacademy.io/ccna/network-services/policing-and-shaping

14. Лекція 19. Якість обслуговування QoS. [Електронний ресурс] - Режим доступу: https://e-tk.lntu.edu.ua/mod/page/view.php?id=3572

15. DiffServ/MPLS Network Design and Management. [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/27522342_DiffServMPLS_Network_Design_and_Management

16. Cisco AVVID QoS Design Guide. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/dam/global/de_at/assets/docs/qosdg_new.pdf

17. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. [Електронний ресурс] – Режим доступу: https://datatracker.ietf.org/doc/html/rfc2474

18. TOS / IP Precedence / DSCP / Decimal Table. [Електронний ресурс] – Режим доступу: https://www.dasblinkenlichten.com/tos-ip-precedence-dscp-decimal-table/

19. Enterprise QoS Solution Reference Network Design Guide (SRND). [Електронний ресурс] – Режим доступу: https://community.cisco.com/legacyfs/online/legacy/3/2/6/64623-qossrnd.pdf

20. A Complete Guide to QoS in Networking for Superior Performance and Optimization. [Електронний ресурс] – Режим доступу: https://nybsys.com/qos-in-networking/

21. Quick Overview: Common VoIP Problems. [Електронний ресурс] – Режим доступу: https://telxi.com/blog/voip-problems/

22. G.114 : One-way transmission time. [Електронний ресурс] – Режим доступу: https://www.itu.int/rec/T-REC-G.114-200305-I/en

23. Ієрархічна модель мережі. [Електронний ресурс] – Режим доступу: https://rci-c.com/technology/yerarkhycheskaia-model-sety/

24. Enterprise Network Design and Implementation using Cisco Packet Tracer. [Електронний ресурс] – Режим доступу:

https://www.researchgate.net/publication/349303352_Enterprise_Network_Design_and_Implementation_using_Cisco_Packet_Tracer

25. Implementing Quality of Service (QoS) in Networking. [Електронний ресурс] – Режим доступу: https://medium.com/@RocketMeUpNetworking/implementing-quality-of-service-qos-in-networking-7205cc11b246

26. What Is QoS, and How Does It Impact Your Business Network? [Електронний ресурс] – Режим доступу: https://planetechusa.com/what-is-qos-and-how-does-it-impact-your-business-network/

27. Network Operation with and without Quality of Service (QoS) Technology and their Impacts to the Organization. [Електронний ресурс] – Режим доступу: https://ligsuniversity.com/network-operation-with-and-without-quality-of-service-qos-technology-and-their-impacts-to-the-organization/

28. What is Quality of Service? [Електронний ресурс] – Режим доступу: https://www.paloaltonetworks.com/cyberpedia/what-is-quality-of-service-qos

29. A Business Model for Charging and Accounting of Internet Services. [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/221017276_A_Business_Model_for_Charging_and_Accounting_of_Internet_Services

30. QoS Fundamentals for Network Engineers: Boost Performance, Reduce Latency [CCNP Enterprise]. [Електронний ресурс] – Режим доступу: https://networkjourney.com/qos-fundamentals-for-network-engineers-boost-performance-reduce-latency-ccnp-enterprise/

https://telxi.com/blog/voip-problems/

31. Configuring QoS on Cisco Routers: A Hands-On Walkthrough. [Електронний ресурс] – Режим доступу: https://medium.com/@enyel.salas84/configuring-qos-on-cisco-routers-a-hands-on-walkthrough-161697e28d85

32. Address Allocation for Private Internets. [Електронний ресурс] – Режим доступу: https://datatracker.ietf.org/doc/html/rfc1918

Додаток А

Лістинг команд для налаштування

Core Switch

```
enable
conf t

#VLAN
vlan 10
name VOICE

vlan 20
name DATA

#Транк до Access Switch 1
interface fa0/2
switchport mode trunk

#Транк до Access Switch 2
interface fa0/3
switchport mode trunk

#Транк до Edge Router
interface fa0/1
switchport mode trunk

#Admin Laptop
interface fa0/4
```

switchport mode access
switchport access vlan 20
switchport voice vlan 10
spanning-tree portfast

#ПЕРЕВІРКА
show vlan brief
show interfaces trunk
show mac address-table

Access Switch 1

enable
conf t

vlan 10
name VOICE

vlan 20
name DATA

#Транк до core
interface fa0/1
switchport mode trunk

#ПК
interface range fa0/3 - 11
switchport mode access
switchport access vlan 20

spanning-tree portfast

#IP Phone
interface fa0/2
switchport mode access
switchport access vlan 20
switchport voice vlan 10
spanning-tree portfast

interface fa0/5
switchport mode access
switchport access vlan 20
switchport voice vlan 10
spanning-tree portfast

#Перевірка
show vlan brief
show interfaces trunk
show mac address-table

Access Switch 2

enable
conf t

vlan 10
name VOICE

```
vlan 20
name DATA

#Транк до core
interface fa0/1
switchport mode trunk

#ПК
interface range fa0/3 - 11
switchport mode access
switchport access vlan 20
spanning-tree portfast

#IP Phone
interface fa0/2
switchport mode access
switchport access vlan 20
switchport voice vlan 10
spanning-tree portfast

interface fa0/5
switchport mode access
switchport access vlan 20
switchport voice vlan 10
spanning-tree portfast


#Перевірка
show vlan brief
show interfaces trunk
```

Edge Router

```
enable
conf t

#Інтерфейс до Core Switch
interface fa0/1
no shutdown

#VLAN 10 (VOICE)
interface fa0/1.10
encapsulation dot1Q 10
ip address 192.168.10.1 255.255.255.0

#VLAN 20 (DATA)
interface fa0/1.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0

#DHCP VOICE
ip dhcp pool VOICE
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
option 150 ip 192.168.10.1

#DHCP DATA
ip dhcp pool DATA
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
```

#Telephony
telephony-service
max-ephones 5
max-dn 5
ip source-address 192.168.10.1 port 2000
auto assign 1 to 5
ephone-dn 1
number 1001
ephone-dn 2
number 1002
ephone-dn 3
number 1003
ephone-dn 4
number 1004
ephone-dn 5
number 1005

#Class maps
class-map match-any VOICE
match ip dscp ef

class-map match-any ADMIN
match ip dscp af21

class-map match-any DATA
match ip dscp default

#Policing

```
policy-map QOS-POLICY
class VOICE
priority percent 30

class ADMIN
bandwidth percent 5

class DATA
bandwidth percent 40

interface fa0/1
service-policy output QOS-POLICY

#ACL
access-list 110 permit udp any any eq 5060
access-list 110 permit udp any any range 16384 32767
access-list 110 deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 110 permit ip any any

access-list 120 permit tcp 192.168.20.0 0.0.0.255 any eq 443
access-list 120 deny ip 192.168.20.0 0.0.0.255 any

interface fa0/1.10
ip access-group 110 in

interface fa0/1.20
ip access-group 120 in
#Шлюз до ISP
```

interface fa0/0

ip address 192.168.100.2 255.255.255.0

no shutdown

ip route 0.0.0.0 0.0.0.0 192.168.100.1

#Перевірка

show ip interface brief

show ip dhcp binding

show ephone

show policy-map

show access-lists

show running-config

ISP

interface fa0/0

ip address 192.168.100.1 255.255.255.0

no shutdown

interface fa0/1

ip address 100.0.0.1 255.255.255.0

no shutdown

ip route 192.168.10.0 255.255.255.0 192.168.100.2

ip route 192.168.20.0 255.255.255.0 192.168.100.2

#Перевірка

show ip interface brief

show running-config

Додаток Б

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ



Навчально-науковий інститут Інформаційних технологій
Кафедра Комп'ютерної інженерії

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА

на тему: «Забезпечення QoS-трафіку в локальній корпоративній мережі з використанням правил безпеки»

Виконав студент групи КІД-41
Степаненко Павло Олександрович

Керівник кваліфікаційної роботи:
Соколов Кирило Анатолійович, Старший викладач, phD

Київ – 2026

Мета та завдання

Мета роботи – дослідити поняття якості обслуговування та розробити локальну корпоративної комп'ютерну мережу з використанням технологій забезпечення QoS для підприємства.

Об'єкт дослідження – аналіз роботи механізмів QoS з використанням базових правил безпеки в умовах локальної корпоративної мережі.

Предмет дослідження – методи, моделі та засоби забезпечення якості обслуговування у локальних корпоративних мережах на основі механізмів класифікації, маркування, чергування та керування мережевим трафіком.

Актуальність теми

У сучасних умовах стрімкого розвитку інформаційних технологій, зростання обсягів переданих даних, використання сервісів для спілкування в реальному часі та підвищення вимог до швидкості й надійності передачі інформації обумовлюють необхідність впровадження ефективних механізмів управління мережевим трафіком.

Комп'ютерні мережі можуть виконувати функції телефонного зв'язку всередині організації за допомогою технології VoIP (Voice over IP) - технології передавання мультимедійних даних у режимі реального часу з використанням протоколів сімейства TCP/IP. Але VoIP дуже чутливий до рівня затримок та перешкод, тому за умов перевантаження у мережі, він може передаватися нерівномірно, що призводить до поганої якості розмов. Вирішити цю проблему може впровадження до мережі якості обслуговування (QoS, Quality of Service) - набору методів і технологій, що забезпечують керовану та передбачувану якість обслуговування в комп'ютерних мережах.

Характеристики QoS

На функціонування мережі та можливість забезпечення якості обслуговування впливають певні метрики:

- Пропускна здатність (Bandwidth)
- Латентність (Latency)
- Затримка (Delay)
- Джитер (Jitter)
- Втрати пакетів (Packet loss)

5

Механізми для забезпечення QoS

Для забезпечення керованого та передбачуваного QoS в корпоративній мережі застосовуються наступні основні механізми:

- Queue and scheduling
- Packet conditioning
- Policing і shaping
- Congestion control

6

Архітектури забезпечення QoS

Для покращення QoS в комп'ютерних мережах, виникла необхідність в об'єднанні механізмів обробки пакетів, керуванням черг, в певні архітектури. Вони відрізняються принципами обробки трафіку та рівнем гарантованих характеристик передачі даних. Основних архітектур дві - це Integrated Service (IntServ) та Differentiated Service (DiffServ). Також існує модель best-effort, але вона виконує скоріше допоміжну роль, тому що не може гарантувати ефективну доставку даних.

IntServ

Архітектура IntServ забезпечує якість обслуговування в IP-мережах через механізм резервування ресурсів для окремих потоків пакетів. Для цього маршрутизатори назначають кожному потоку у мережі певний стан.

Спочатку користувач або застосунок визначає необхідні параметри якості обслуговування, зокрема допустиму затримку та потрібну пропускну здатність. Далі ці вимоги передаються в мережу за допомогою сигнального протоколу, який називається RSVP.

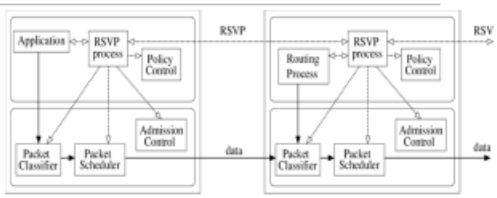


Рисунок 1.3 – Схема взаємодії компонентів архітектури IntServ та протоколу RSVP [15]

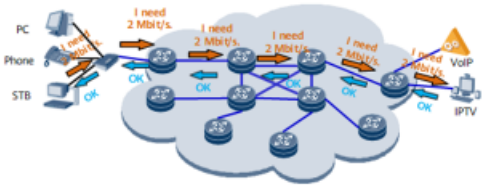


Рисунок 1.4 - Схема встановлення наскрізного (End-to-End) QoS-з'єднання в архітектурі IntServ. [10]

DiffServ

Архітектура DiffServ (Differentiated Services) базується на ідеї надання різних рівнів якості обслуговування не окремим потокам, а їхнім агрегованим групам. На відміну від моделі IntServ, де кожен мікропотік потребує індивідуальної обробки, DiffServ класифікує трафік за невеликою кількістю типів сервісу. Такий підхід дозволяє значно підвищити масштабованість системи, роблячи її придатною для використання у глобальних та великих локальних мережах.

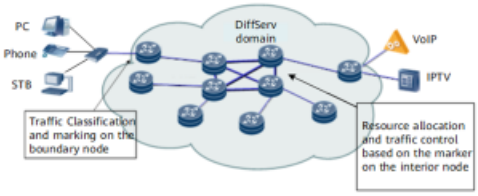


Рисунок 1.5 – Приклад мережі побудованої за допомогою моделі DiffServ. [10]

Взаємозв’язок QoS та правил безпеки

QoS і безпека мережі тісно пов’язані між собою, оскільки неконтрольований або шкідливий трафік може суттєво впливати на роботу мережі та порушувати її стабільність навіть за наявності механізмів пріоритезації. Для вирішення цих проблем використовують VLAN та ACL.

Використання VLAN дозволяє сегментувати трафік, підвищуючи безпеку та продуктивність, дозволяючи пристроям взаємодіяти, ніби вони були в одній LAN, навіть перебуваючи в різних місцях. Це допомогає ізолювати трафік між різними підмережами, зменшити обсяг широкомовного трафіку та обмежити вплив потенційних загроз

ACL - це спеціальний список, в якому визначаються правила фільтрації пакетів. Наприклад, можна заборонити проходити в мережі даним з певної IP-адреси, або обмежити їх передачу однією підмережею. Окрім забезпечення безпеки, ACL широко застосовуються для класифікації трафіку, що є важливим етапом у реалізації політик QoS.

Аналіз мережевих сервісів і типів трафіку

Таблиця 2.1 – Порівняльна характеристика видів трафіку [19]

Характеристика	**VoIP**	**Web (HTTP/HTTPS)**	**FTP**
Тип застосунку	Реального часу	Адаптивний	Адаптивний
Протокол	UDP (RTP)	TCP	TCP
Необхідна пропускна здатність	~64–100 кбіт/с	~0.5–5 Мбіт/с	від 1 Мбіт/с
Вимоги до затримки (delay)	< 150 мс	< 2–3 с	Некритична
Джитер (jitter)	< 20–30 мс	Некритичний	Некритичний
Втрати пакетів	< 1%	до 2–3% допустимо	допустимі (TCP відновлює)
Пріоритет	Високий	Середній	Низький
Приклади реального використання	Голосові дзвінки, відеоконференції	Браузинг, хмарні сервіси, API	Резервне копіювання, обмін документами

Опис досліджуваної корпоративної мережі

У даній роботі розглядається модель корпоративної локальної мережі, побудована на основі трирівневої ієрархічної архітектури Cisco. Згідно з цією концепцією, мережа поділяється на функціональні рівні, кожен з яких оптимізований для конкретних завдань:

- Рівень розподілу (Distribution Layer): місце впровадження політик безпеки, інтелектуальної маршрутизації та агрегації каналів перед передачею трафіку на магістраль.
- Рівень ядра (Core Layer): відповідає за максимально швидку та безперебійну трансляцію масивних потоків даних без затримок на складну обробку пакетів.
- Рівень доступу (Access Layer): виступає безпосереднім інтерфейсом для кінцевих пристроїв, забезпечуючи їхнє входження в мережу та контроль доступу.

Топологія досліджуваної локальної корпоративної мережі

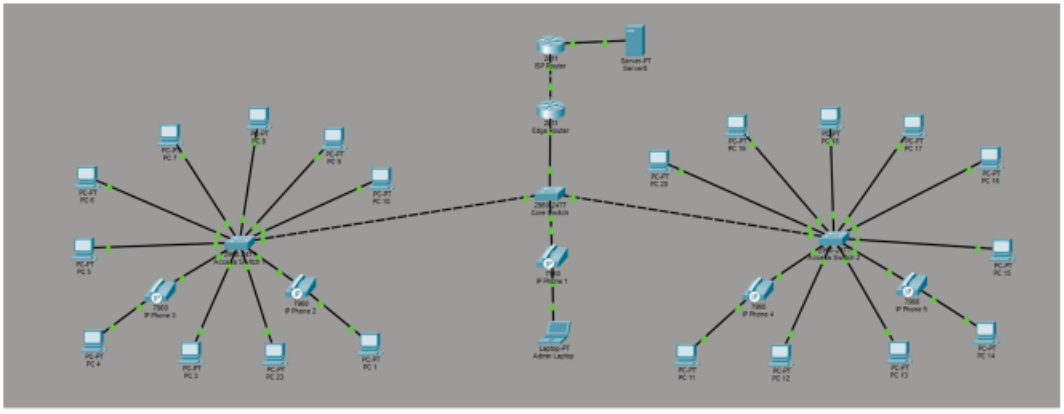


Рисунок 2.2 – Топологія локальної мережі підприємства

Розробка локальної корпоративної мережі



Рисунок 3.1 – Список налаштувань VLAN на Access Switch



Рисунок 3.6 – Список налаштувань Policing та ACL

Тестування мережі

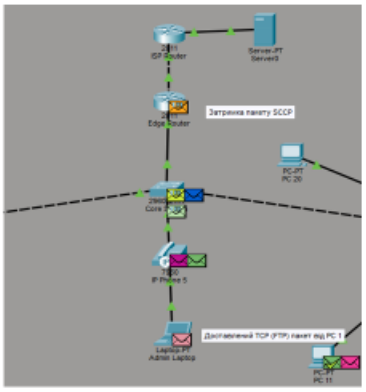


Рисунок 3.9 – Затримка службового пакету SCCP без налаштувань QoS

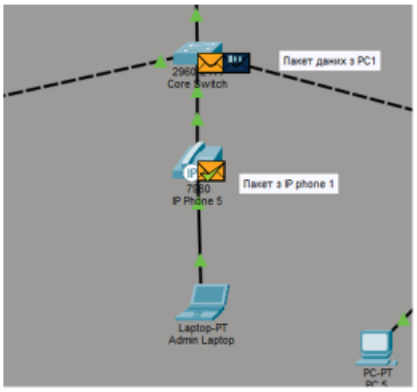
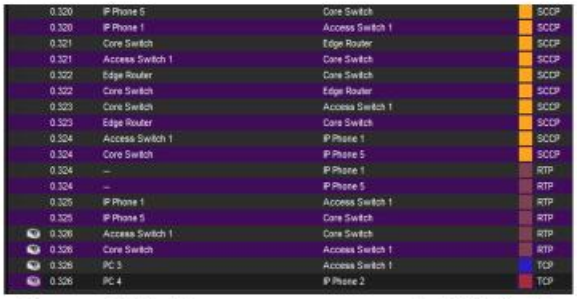


Рисунок 3.11 – Порядок надходження пакетів з даними

Різниця між затримками



0.320	IP Phone 5	Core Switch	SCCP
0.320	IP Phone 1	Access Switch 1	SCCP
0.321	Core Switch	Edge Router	SCCP
0.321	Access Switch 1	Core Switch	SCCP
0.322	Edge Router	Core Switch	SCCP
0.322	Core Switch	Edge Router	SCCP
0.323	Core Switch	Access Switch 1	SCCP
0.323	Edge Router	Core Switch	SCCP
0.324	Access Switch 1	IP Phone 1	SCCP
0.324	Core Switch	IP Phone 5	SCCP
0.324	--	IP Phone 1	RTP
0.324	--	IP Phone 5	RTP
0.325	IP Phone 1	Access Switch 1	RTP
0.325	IP Phone 5	Core Switch	RTP
0.326	Access Switch 1	Core Switch	RTP
0.326	Core Switch	Access Switch 1	RTP
0.326	PC 3	Access Switch 1	TCP
0.326	PC 4	IP Phone 2	TCP

Рисунок 3.10 – Час надходження пакетів RTP з VoIP-даними



Рисунок 3.12 – Час проходження пакетів

Інформація з пакетів з даними

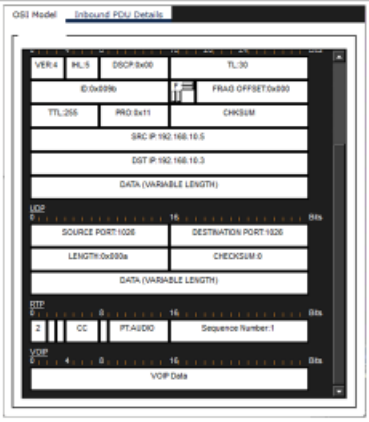


Рисунок 3.13 - Переданий RTP пакет з даними голосу



Рисунок 3.15 – Скинутий пакет з даними про доступ до HTTP

Висновки

Для дослідження QoS, в середовищі Cisco Packet Tracer була розроблена локальна корпоративна мережа, з використанням методів пріоретизації, класифікування та маркування пакетів що, дозволило зменшити затримки у проходження пакетів VoIP у мережі більш ніж у 10 разів порівняно з варіантом мережі без забезпечення QoS. Зокрема в ній була реалізована сегментація та були введені списки доступу, які також підвищили ефективність та загальний рівень безпеки мережі.

Використання комплексного підходу до поєднання QoS і механізмів безпеки дозволило забезпечити стабільну роботу таких критично важливих сервісів, таких як VoIP, та HTTPS, тому, впроваджене рішення відповідає сучасним вимогам до рівня якості обслуговування в корпоративних мережах, забезпечує гнучкість, масштабованість і надійність їх функціонування.