Національний університет «Полтавська політехніка імені Юрія Кондратюка»

(повне найменування закладу вищої освіти)

Навчально-науковий інститут інформаційних технологій і робототехніки

(повне найменування інституту, назва факультету (відділення))

Кафедра автоматики, електроніки та телекомунікацій

(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи

бакалавр

(ступінь вищої освіти)

на тему «Дослідження протоколів транспортного рівня мереж наступного покоління NGN»

Виконав: студент 4 курсу, групи 401ТТ

спеціальності 172 «Електронні комунікації та радіотехніка

(шифр і назва напряму підготовки, спеціальності)

Гольонко М.С.

(прізвище та ініціали)

Керівник Жученко О.С.

(прізвище та ініціали)

Рецензент Штомпель М.А.

(прізвище та ініціали)

Полтава - 2023 рік

Реферат

Робота містить 50 сторінок, 23 ілюстрації, 7 використаних джерел.

Ключові слова: Протоколи транспортного рівня, Мережі наступного покоління (NGN), TCP/IP, UDP, SCTP, Ретрансляція, Контрольні біти.

Актуальність роботи:

- З'ясування ефективності та надійності протоколів транспортного рівня NGN є важливим завданням у сучасному світі, де швидкість передачі даних, безпека та надійність є вирішальними факторами.

- Дослідження протоколів транспортного рівня NGN також може сприяти розвитку мереж з великою місткістю та покращенню якості обслуговування для користувачів.

Мета роботи:

- Ознайомлення з основними протоколами транспортного рівня NGN, їх функціями та особливостями.

- Аналіз та порівняння протоколів з метою виявлення їх переваг та недоліків.

- Визначення ефективних стратегій використання протоколів транспортного рівня NGN для покращення продуктивності та надійності мережі.

- Висунення рекомендацій щодо використання та оптимізації протоколів транспортного рівня NGN.

Abstract

The work contains 50 pages, 23 illustrations, 7 used sources.

Keywords: Transport layer protocols, Next generation networks (NGN), TCP/IP, UDP, SCTP, Relay, Control bits

Relevance of work:

- Finding out the effectiveness and reliability of NGN transport layer protocols is an important task in today's world, where data transfer speed, security and reliability are crucial factors.

- Research on NGN transport layer protocols can also contribute to the development of high-capacity networks and improve the quality of service for users.

Purpose of work:

- Familiarization with the main protocols of the NGN transport layer, their functions and features.

- Analysis and comparison of protocols in order to identify their advantages and disadvantages.

- Identify effective strategies to use NGN transport layer protocols to improve network performance and reliability.

- Making recommendations for the use and optimization of NGN transport layer protocols.

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Інститут Навчально-науковий інститут інформаційних технологій та робототехніки
Кафедра Автоматики, електроніки та телекомунікацій
Ступінь вищої освіти Бакалавр
Спеціальність 172 «Телекомунікації та радіотехніка»

ЗАТВЕРДЖУЮ
Завідувач кафедри автоматики, електроніки та телекомунікацій

_____О.В. Шефер

“ 01 ” квітня 2023 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРУ СТУДЕНТУ

Гольонко Максиму Сергійовичу

1. Тема роботи «Дослідження протоколів транспортного рівня мереж наступного покоління NGN» керівник роботи Жученко О.С, к.т.н., доцент

затверджена наказом вищого навчального закладу від 20.03.2023 року № 236

2. Строк подання студентом проекту (роботи) 14.06.2023 р.

3. Вихідні дані до проекту (роботи)

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Теоретичний огляд протоколів транспортного рівня мереж наступного покоління NGN та їх властивостей. Аналіз протоколів транспортного рівня мереж наступного покоління NGN на основі вибраних критеріїв. Дослідження виконання деяких протоколів транспортного рівня мереж наступного покоління NGN, зокрема TCP, SCTP та DCCP, в умовах зміни рівня навантаження та втрат пакетів на каналі зв'язку. Опис результатів досліджень та їх аналіз. Висновки про ефективність протоколів транспортного рівня мереж наступного покоління NGN та їх внесок у розвиток мереж наступного покоління. Рекомендації щодо використання певних протоколів транспортного рівня мереж наступного покоління NGN у певних умовах.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів):

презентація обсягом не менше 5 слайдів.

1) Теоретичний огляд протоколів транспортного рівня мереж наступного покоління NGN та їх властивостей.;

2) Данні для дослідження протоколів (рівні навантаження);
3) Короткий опис результатів досліджень та їх аналіз;

6. Дата видачі завдання 01.04.2023 р.

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів кваліфікаційної роботи бакалавра	Термін виконання етапів роботи			Примітка (плакати)
1	Підготовка матеріалів до оглядово-аналітичної частини.	26.04.23	I	20%	Пл. 1
2	Розробка розділу оглядово-аналітичної частини.	10.05.23		40%	Пл. 2
3	Розробка розділів спеціальної частини	24.05.23	II	60%	Пл. 3
4	Аналіз отриманих результатів роботи	07.06.23		80 %	Пл. 4,5
5	Оформлення кваліфікаційної роботи бакалавра, підготовка демонстраційного матеріалу	14.06.23		100%	Пл. 6

Студент _____ Гольонко М.С.

Керівник роботи_____ Жученко О.С.

Зміст

Вступ

Протягом останніх років, мережі наступного покоління NGN (Next Generation Networks) виявилися дуже популярними і важливими для передачі інформації у сучасному світі. Завдяки широкому спектру послуг, які вони надають, вони стали невід'ємною частиною нашого повсякденного життя. Однак, для забезпечення ефективного та надійного передавання даних в мережах наступного покоління, важливо мати ефективні та надійні протоколи транспортного рівня.

Ця кваліфікаційна робота присвячена дослідженню протоколів транспортного рівня мереж наступного покоління NGN та їх властивостей. Головною метою цього дослідження є розуміння різних протоколів транспортного рівня, зокрема TCP, SCTP та DCCP, їх взаємодії з іншими протоколами та відмінностей в їхньому використанні. Додатково, будуть проведені дослідження виконання деяких протоколів в різних умовах, таких як зміна рівня навантаження та втрат пакетів на каналі зв'язку.

Результати цього дослідження мають велике значення для визначення ефективності та надійності різних протоколів транспортного рівня мереж наступного покоління. Ці дані також допоможуть розробити рекомендації щодо використання цих протоколів в різних умовах. Це може сприяти подальшому розвитку мереж наступного покоління та підвищенню якості послуг, що надаються користувачам.

Дослідження надійності передачі даних, керування потоком та перевантаженням, мультиплексування, підтримки безпеки, швидкості передачі даних та сумісності з існуючими протоколами є ключовими критеріями, які будуть розглянуті в цьому дослідженні. Порівнюючи характеристики та особливості протоколів TCP, SCTP та DCCP на основі цих критеріїв, ми зможемо отримати глибоке розуміння їхніх переваг та обмежень у контексті мереж наступного покоління NGN.

На основі результатів цього дослідження, розробники мереж та інженери зможуть приймати кращі рішення щодо вибору протоколів транспортного рівня в залежності від конкретних вимог і умов використання.

1. Теоретичний огляд

Протоколи транспортного рівня – це протоколи мережі, що забезпечують передачу даних між програмами, які працюють на різних комп'ютерах або пристроях. У мережах наступного покоління NGN, протоколи транспортного рівня відіграють важливу роль у забезпеченні ефективного та надійного передавання даних.

Основними протоколами транспортного рівня мереж наступного покоління NGN є TCP (Transmission Control Protocol), SCTP (Stream Control Transmission Protocol) та DCCP (Datagram Congestion Control Protocol).

TCP (Transmission Control Protocol) - це протокол транспортного рівня мережі, що забезпечує надійну доставку даних між програмами, які працюють на різних комп'ютерах або пристроях. TCP використовується в різних мережевих архітектурах, включаючи мережі наступного покоління NGN (Next Generation Networks).

TCP забезпечує послідовну передачу даних, що дозволяє відновлювати дані, що були втрачені під час передачі. Для цього TCP використовує механізм нумерації послідовних пакетів, який дозволяє визначити, які дані були передані успішно, а які були втрачені. Якщо дані були втрачені, TCP відправляє запит на повторну передачу цих даних.

TCP також використовує механізми контролю навантаження на мережу, такі як механізм перегляду вікна та контролю потоку. Механізм перегляду вікна дозволяє контролювати кількість пакетів, які можна відправити до отримувача, не очікуючи підтвердження доставки попередніх пакетів. Це дозволяє підтримувати високу швидкість передачі даних та уникнути перевантаження мережі.

Механізм контролю потоку дозволяє регулювати швидкість передачі даних залежно від здатності отримувача обробляти дані. Це дозволяє уникнути перевантаження отримувача та забезпечує надійну доставку даних.

Також TCP підтримує механізм контролю припинення з'єднання, який дозволяє закрити з'єднання між двома пристроями після завершення передачі даних. Це забезпечує ефективне використання ресурсів.

SCTP (Stream Control Transmission Protocol) - це протокол транспортного рівня, розроблений для надійної транспортної послуги з підтримкою потоків даних та декількох з'єднань. SCTP є протоколом наступного покоління, який може бути використаний в різних мережевих архітектурах, включаючи мережі наступного покоління NGN (Next Generation Networks).

Одна з основних відмінностей SCTP від TCP полягає у підтримці мультиплексування потоків даних та декількох з'єднань. SCTP використовує концепцію асоціації, що дозволяє використовувати більше одного з'єднання між двома пристроями одночасно. Кожне з'єднання містить набір потоків даних, які можуть бути мультиплексовані на одному з'єднанні. Це дозволяє ефективно використовувати ресурси мережі та забезпечує більш високу швидкість передачі даних.

SCTP також забезпечує надійну доставку даних, подібно до TCP, з використанням механізму контролю потоку та механізму перегляду вікна. Однак, SCTP має додаткові механізми контролю навантаження на мережу, такі як механізм конгестійного керування та механізм керування ресурсами. Механізм конгестійного керування дозволяє контролювати швидкість передачі даних на мережі та уникнути перевантаження мережі. Механізм керування ресурсами дозволяє контролювати використання ресурсів на мережевих пристроях та уникнути перевантаження ресурсів.

SCTP також підтримує механізм контролю припинення з'єднання, який дозволяє забезпечити безпечне припинення з'єднання між пристроями та уникнути втрати даних або підриву безпеки мережі. SCTP також має додаткові функції, такі як підтримка багатодотичних мереж, механізм перевірки доставки та підтримка механізмів захисту від DDoS-атак.

Одним з головних застосувань SCTP є транспортування SIP (Session Initiation Protocol), який використовується для управління сеансами зв'язку в

мережах наступного покоління. SCTP забезпечує надійну транспортну послугу для SIP, що дозволяє забезпечити високу якість обслуговування для клієнтів та забезпечити ефективність мережі.

Узагальнюючи, SCTP є протоколом транспортного рівня, який забезпечує надійну транспортну послугу з підтримкою потоків даних та декількох з'єднань. Він підтримує мультиплексування потоків даних, механізми контролю навантаження на мережу та припинення з'єднання, а також має додаткові функції для підтримки багатодотичних мереж та захисту від DDoS-атак. SCTP використовується в різних мережевих архітектурах, включаючи мережі наступного покоління NGN, та є одним з головних протоколів для транспортування SIP.

DCCP (Datagram Congestion Control Protocol) - це протокол транспортного рівня, призначений для передачі даних у мережах з високим рівнем забруднення (congestion), таких як Інтернет. DCCP розроблений як альтернатива TCP та UDP, що дозволяє забезпечити ефективнішу передачу даних для додатків, які вимагають надійності та контролю навантаження на мережу.

Одна з головних властивостей DCCP - це підтримка різних профілів перенесення даних (transport service profiles), що відповідають різним типам додатків. Ці профілі визначають рівень надійності, максимальну пропускну здатність та інші характеристики транспортної послуги. Таким чином, DCCP забезпечує можливість налаштування протоколу відповідно до вимог конкретного додатку.

DCCP також має механізми контролю навантаження на мережу та підтримки мультиплексування потоків даних, що дозволяє ефективно використовувати ресурси мережі. Крім того, DCCP має механізм контролю забруднення мережі (congestion control), що забезпечує стабільність та надійність передачі даних в умовах змінного навантаження на мережу.

Однією з особливостей DCCP є можливість використовувати різні кодеки для передачі аудіо- та відеоданих. Кодеки відповідають за стиснення

та розкодування даних і дозволяють ефективно передавати медіадані в мережі з обмеженою пропускною здатністю.

DCCP може бути використаний для різних додатків, таких як потокове відео, відеоконференції.

До переваг DCCP належить можливість використання різноманітних методів управління переповненням та контролю за потоком даних. Зокрема, протокол надає можливість використання двох методів управління переповненням: роздільне та інтегроване управління. Роздільне управління передбачає використання окремого каналу для передачі повідомлень про стан мережі, в той час як при інтегрованому управлінні повідомлення про стан мережі передаються в тому ж самому каналі, що й дані.

До додаткових можливостей DCCP належить підтримка з'єднань з багатьма потоками, що дає можливість одночасно передавати та отримувати різні потоки даних. Крім того, протокол забезпечує можливість використання не тільки з'єднань з надійним передаванням даних, але й з'єднань з ненадійним передаванням даних.

DCCP може бути використаний для передачі даних у різноманітних застосунках, де важливо забезпечити високу ефективність передачі даних при використанні мереж наступного покоління. Зокрема, протокол може бути використаний для передачі аудіо та відео потоків, онлайн ігор, а також в інших застосунках, які потребують швидкої передачі даних з високим рівнем надійності.

Для порівняння характеристик, особливостей та ефективності протоколів транспортного рівня мереж наступного покоління NGN проведемо аналіз трьох таких протоколів: TCP, SCTP та DCCP.

TCP (Transmission Control Protocol) - це протокол, який забезпечує надійний транспорт даних у мережах. Він використовується для передачі даних, що вимагають надійності, таких як веб-сторінки, електронні листи та файли.

Основні характеристики TCP:

- Надійна доставка даних: TCP забезпечує доставку даних без втрат та дублювань.
- Контроль потоку: TCP контролює потік даних, щоб уникнути переповнення буфера на приймачі.
- Контроль перевірки цілісності: TCP використовує механізм перевірки цілісності, який гарантує, що дані не змінювались під час передачі.
- З'єднання на рівні протоколу: TCP встановлює з'єднання між відправником та приймачем на рівні протоколу.
- Керування перенавантаженням: TCP має механізми, які дозволяють йому зменшувати швидкість передачі даних, якщо мережа перенавантажена.

SCTP (Stream Control Transmission Protocol) - це протокол, який забезпечує передачу даних в мережах. Він був створений з метою забезпечення підтримки додатків з високим рівнем надійності, таких як VoIP, відеоконференції та трансляції мультимедіа.

Далі порівняємо особливості та ефективність SCTP та DCCP протоколів.

SCTP та DCCP були розроблені для різних цілей, і відповідно мають свої особливості та застосування.

SCTP є багатоканальним протоколом з можливістю передачі даних в багатьох потоках, які можуть бути використані для різних цілей, таких як підтримка мультикасту, забезпечення резервного каналу передачі даних, та підтримка функцій безпеки. SCTP також має механізми для уникнення заторів на мережевому рівні та механізми відновлення після втрати пакетів. Одним з головних недоліків SCTP є його складність, яка може збільшувати накладні витрати на обробку пакетів.

DCCP забезпечує забезпечену передачу даних з контролем перевантаження, що робить його ідеальним для мультимедійних додатків, таких як трансляції відео та аудіо. Він також підтримує різні режими передачі, такі як потокова передача та передача без забезпечення доставки. DCCP є

менш складним за SCTP, що дозволяє зменшити накладні витрати на обробку пакетів. Однак, на відміну від SCTP, DCCP не підтримує мультикаст.

Загалом, якщо потрібна забезпечена передача даних у багатьох потоках, з підтримкою безпеки та механізмами відновлення після втрати пакетів, то SCTP може бути кращим вибором. У разі, якщо важливішим є забезпечення контролю перевантаження та меншої складності, то DCCP може бути кращим варіантом.

Крім того, SCTP має підтримку механізму мультиплексування, який дозволяє передавати різні потоки даних через один SCTP з'єднання. Це зменшує навантаження на мережу і збільшує ефективність передачі даних.

Нарешті, DCCP є протоколом, який підтримує найбільшу кількість типів потоків даних, таких як надійні, ненадійні та стрімінгові. Він також має механізм контролю навантаження, який дозволяє регулювати швидкість передачі даних в залежності від стану мережі.

Основні відмінності між протоколами полягають у їх підтримці функцій, швидкості передачі даних та надійності. TCP є найбільш поширеним протоколом і має високу надійність, але його швидкість може бути обмеженою. SCTP є менш популярним, але він має вбудовану підтримку мультиплексування та є більш ефективним для передачі даних в деяких випадках. DCCP є дуже гнучким і може підтримувати різні типи потоків даних, а також має механізм контролю навантаження.

Отже, вибір протоколу транспортного рівня залежить від конкретних вимог до мережі та потреб користувачів. Для додатків, які потребують високої надійності передачі даних, TCP може бути найкращим варіантом. Для додатків, які потребують більшої ефективності, SCTP або DCCP можуть бути кращими варіантами, залежно від потреб користувачів та характеру передаваних даних.

2. Аналіз протоколів транспортного рівня NGN за вибраними критеріями:

1. Надійність передачі даних
    1.1. TCP
    1.2. SCTP
    1.3. DCCP
2. Керування потоком та перевантаженням
    2.1. TCP
    2.2. SCTP
    2.3. DCCP
3. Мультиплексування
    3.1. TCP
    3.2. SCTP
    3.3. DCCP
4. Підтримка безпеки
    4.1. TCP
    4.2. SCTP
    4.3. DCCP
5. Швидкість передачі даних
    5.1. TCP
    5.2. SCTP
    5.3. DCCP
6. Сумісність з існуючими протоколами
    6.1. TCP
    6.2. SCTP
    6.3. DCCP

Аналіз протоколів транспортного рівня NGN за вибраними критеріями:

1. Надійність передачі даних:
    1.1. TCP:

TCP (Transmission Control Protocol)(Рис.1) є надійним протоколом передачі даних, який забезпечує впорядковану та доставку без втрат пакетів. Він використовує механізми підтвердження та повторної передачі для гарантованої доставки даних до отримувача. TCP також підтримує контроль цілісності даних та управління потоком, що дозволяє регулювати швидкість передачі відповідно до можливостей мережі. Протокол TCP є дуже надійним, але може страждати від затримок та втрат пакетів у мережах з великими затримками або втратами.

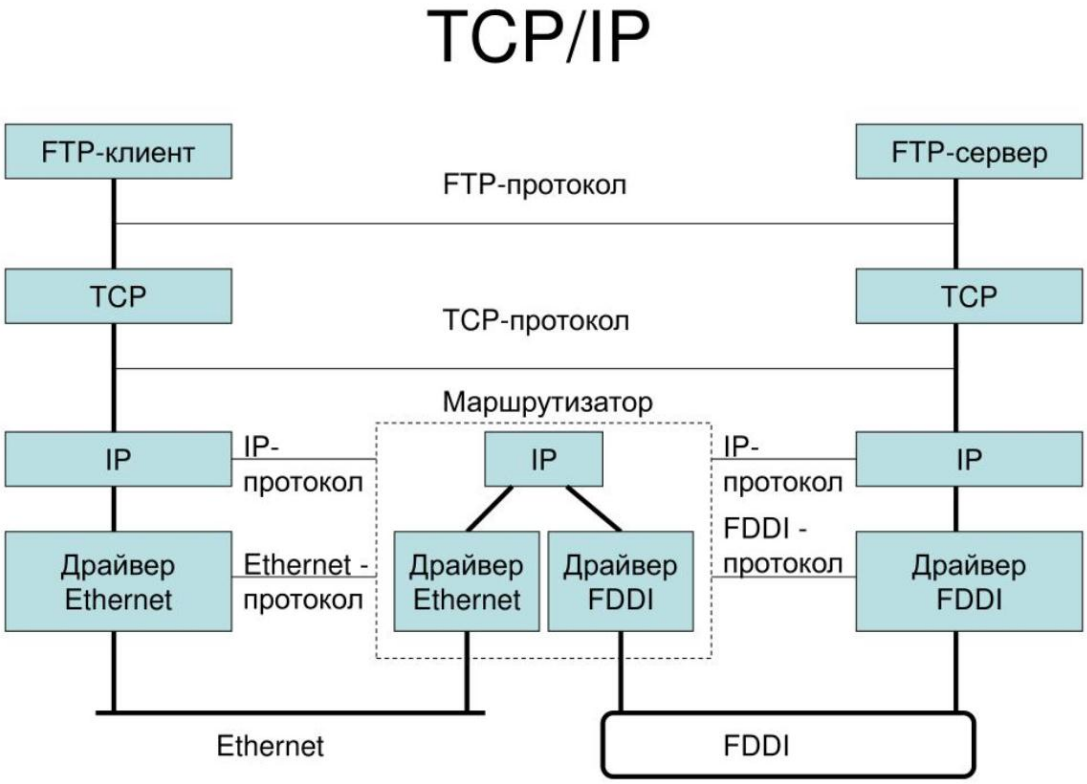

Рисунок 1.1 – TCP протокол.

1.2. SCTP:

SCTP (Stream Control Transmission Protocol)(Рис. 2) також є надійним протоколом передачі даних, але він має додаткові механізми, що роблять його більш гнучким для додатків з особливими вимогами. SCTP використовує концепцію асоційованих потоків, яка дозволяє передавати кілька потоків даних через одне з'єднання. Це забезпечує краще використання ресурсів мережі та підвищує ефективність передачі даних. SCTP також має механізми реакції на втрати пакетів та регулювання швидкості передачі даних. В

порівнянні з TCP, SCTP може бути менш вразливим до затримок та втрат у мережі.

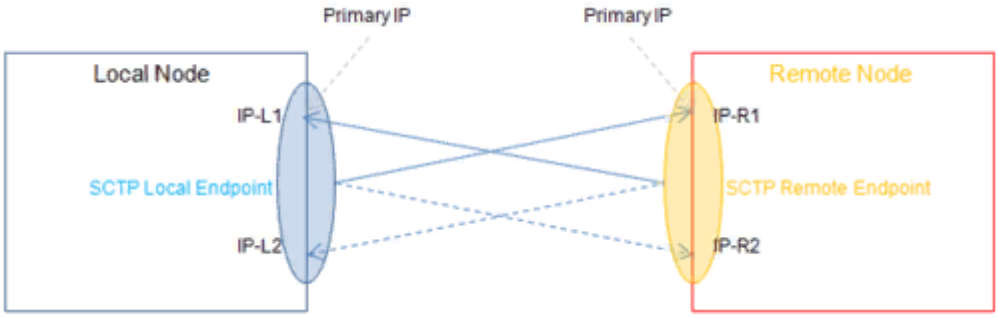

Рисунок 1.2 – SCTP протокол.

1.3. DCCP:

DCCP (Datagram Congestion Control Protocol)(Рис. 3) забезпечує надійну передачу даних, але з меншою гарантією доставки порівняно з TCP або SCTP. DCCP використовує механізм керування припливом, який дозволяє регулювати швидкість передачі даних, але не забезпечує повну гарантію доставки та впорядкування. Цей протокол підходить для додатків, які припускають певну втрату даних або не вимагають строгого порядку доставки.

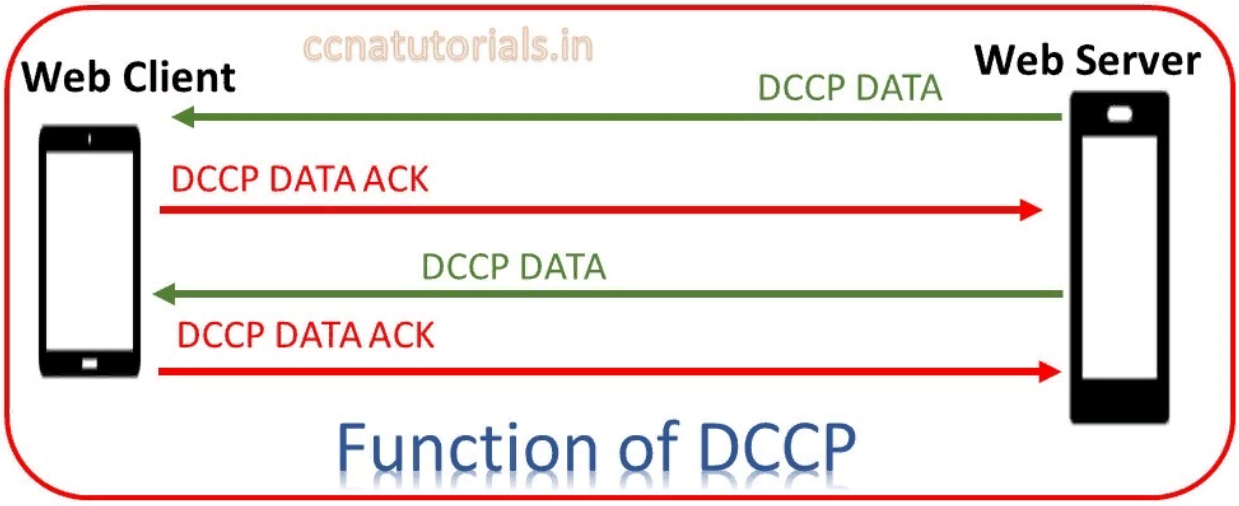

Рисунок 1.3 – DCCP протокол.

2. Керування потоком та перевантаженням:

2.1. TCP:

TCP має потужні механізми керування потоком, такі як вікно власне масштабування, механізм виявлення заторів та алгоритми пригнічення передачі даних. Це дозволяє TCP реагувати на перевантаження мережі та

регулювати швидкість передачі відповідно до її можливостей. TCP також використовує механізм контролю витоку, що дозволяє обмежити швидкість передачі даних до сприйнятливого рівня отримувача.

2.2. SCTP:

SCTP також має механізми керування потоком, але використовує інші алгоритми порівняно з TCP. SCTP використовує механізми розділення трафіку на потоки та обмеження швидкості передачі для кожного потоку окремо. Це дозволяє SCTP більш гнучко реагувати на перевантаження та забезпечити краще розподіл ресурсів мережі.

2.3. DCCP:

DCCP також має механізми керування потоком, але менш складні порівняно з TCP або SCTP. DCCP використовує власний алгоритм керування припливом, що дозволяє обмежувати швидкість передачі даних. Проте, DCCP може бути менш ефективним у розподілі ресурсів мережі під час перевантаження.

3. Мультиплексування:

3.1. TCP:

TCP не підтримує пряме мультиплексування декількох потоків через одне з'єднання. Кожне з'єднання TCP призначене для одного потоку даних. Проте, TCP може використовувати порти для ідентифікації різних додатків або сервісів.

3.2. SCTP:

SCTP підтримує мультиплексування декількох потоків даних через одне з'єднання. Кожен потік має свій ідентифікатор, що дозволяє відновлювати відповідність між пакетами і потоками на отримувачі. Це дозволяє більш ефективно використовувати ресурси мережі та підвищує пропускну здатність.

3.3. DCCP:

DCCP також підтримує мультиплексування декількох потоків через одне з'єднання. Кожен потік має свій ідентифікатор, що дозволяє розрізняти

пакети і потоки на отримувачі. Це дає можливість передавати різні потоки даних через одне з'єднання.

4. Підтримка безпеки:

4.1. TCP:

TCP не надає вбудованих механізмів шифрування або автентифікації даних. Для забезпечення безпеки з'єднання, необхідно використовувати додаткові протоколи, такі як TLS (Transport Layer Security), що забезпечує шифрування та ідентифікацію сторін.

4.2. SCTP:

SCTP має вбудовану підтримку безпеки через механізми, такі як аутентифікація, шифрування та захист від атак. SCTP може використовувати TLS для забезпечення безпеки з'єднання та захисту від перехоплення або модифікації даних.

4.3. DCCP:

DCCP не має вбудованої підтримки безпеки. Аналогічно до TCP, для забезпечення безпеки з'єднання необхідно використовувати додаткові механізми, такі як TLS.

5. Швидкість передачі даних:

5.1. TCP:

TCP має добре розроблені алгоритми керування перевантаженням, які дозволяють регулювати швидкість передачі даних в залежності від стану мережі. TCP може пристосовуватись до різних швидкостей мережі, знижуючи швидкість у разі перевантаження та збільшуючи її відповідно до можливостей мережі та отримувача.

5.2. SCTP:

SCTP також має механізми для регулювання швидкості передачі даних. Він може пристосовуватись до швидкості мережі та забезпечувати оптимальну пропускну здатність. SCTP може бути особливо ефективним у мережах з високою затримкою та втратами.

5.3. DCCP:

DCCP має менш розвинуті механізми регулювання швидкості порівняно з TCP або SCTP. Він може обмежувати швидкість передачі даних, але не має такої деталізації та гнучкості, як у TCP або SCTP.

6. Сумісність з існуючими протоколами:

6.1. TCP:

TCP є широко підтримуваним і використовуваним протоколом у сучасних мережах. Він є стандартом для багатьох додатків та протоколів, таких як HTTP, FTP, SMTP і т.д. TCP здатний співпрацювати з різними мережевими пристроями та оперативними системами.

6.2. SCTP:

SCTP, хоча менш поширений порівняно з TCP, все ж є стандартом для деяких протоколів, зокрема у сфері телекомунікаційних мереж. Він підтримується в деяких оперативних системах та мережевих пристроях.

6.3. DCCP:

DCCP є менш поширеним протоколом у порівнянні з TCP та SCTP. Його використання обмежене, і він не є стандартом для багатьох додатків чи протоколів.

Це загальний аналіз протоколів транспортного рівня NGN за вибраними критеріями. Варто враховувати, що кожен протокол має свої особливості та відмінності, і вибір протоколу залежить від конкретних вимог та сценаріїв використання.

3. Для дослідження виконання протоколів транспортного рівня мереж наступного покоління NGN, зокрема TCP, SCTP та DCCP, в умовах зміни рівня навантаження та втрат пакетів на каналі зв'язку, можна виконати наступні кроки:

1. Підготовка тестового середовища:

- Встановлення необхідного програмного забезпечення та налаштування потрібних протоколів.
- Створення симуляційної мережі для відтворення зміни рівня навантаження та втрат пакетів.

Цей процес дослідження виконання протоколів транспортного рівня NGN може бути реалізований за допомогою програмного забезпечення для симуляції мережі, такого як NS-3(Рис.4), та інших інструментів для аналізу мережі. Деталізація та результати аналізу будуть залежати від конкретних умов дослідження та налаштувань тестового середовища.

Рисунок 1.4 – NS-3 симулятор.

NS-3 (Network Simulator 3) - це вільно поширюване програмне забезпечення для симуляції мережевих протоколів та алгоритмів. Воно надає зручне та потужне середовище для вивчення та аналізу різних аспектів мережевих систем.

NS-3 побудована на мові програмування C++ і заснована на дискретно-подієвій моделі, що дозволяє точно моделювати поведінку мережевих протоколів у відповідь на різні події. Вона пропонує широкий набір модулів і компонентів, які дозволяють користувачам створювати складні моделі мереж та проводити різноманітні дослідження.

Основні особливості NS-3 включають:

- Реалістична моделювання: NS-3 намагається максимально точно відтворити реальні умови мережі. Це означає, що користувачі можуть

враховувати різні параметри, такі як пропускна здатність, затримки, помилки передачі, шум, втрати пакетів тощо.

- Розширюваність: NS-3 надає гнучкий механізм для додавання власних модулів і розширення функціональності. Користувачі можуть створювати власні моделі протоколів, алгоритми маршрутизації та інші компоненти для виконання своїх конкретних досліджень.
- Багатомодульна архітектура: NS-3 складається з різних модулів, які відповідають за різні аспекти мережевого стеку та функціональності. Це дозволяє користувачам вибирати лише необхідні модулі для своїх експериментів, що сприяє ефективності та оптимізації ресурсів.
- Підтримка реального часу: NS-3 може працювати у реальному часі, що дозволяє виконувати симуляції з врахуванням реальних швидкостей передачі даних та затримок, що є важливим для деяких досліджень та додатків.

NS-3 використовується в наукових дослідженнях, академічних проектах та розробці мережевих протоколів. Воно дозволяє користувачам вивчати та аналізувати різні аспекти мережевих систем, від простих до складних сценаріїв. NS-3 є потужним інструментом для моделювання та дослідження мереж, що сприяє розвитку та вдосконаленню мережевих технологій.

Крім NS-3, ще одним популярним інструментом для моделювання мереж є Cisco Packet Tracer. Cisco Packet Tracer - це програмне забезпечення, розроблене компанією Cisco Systems з метою навчання та вивчення мережевих технологій.

Cisco Packet Tracer надає інтерактивне середовище для створення віртуальних мереж, де користувачі можуть створювати, налаштовувати та тестувати мережеві сценарії. Він має графічний інтерфейс, що дозволяє візуалізувати мережеві компоненти, такі як маршрутизатори, комутатори, сервери тощо, і з'єднувати їх за допомогою різних типів з'єднань.

Cisco Packet Tracer має певні особливості, що роблять його корисним для навчання мережевих технологій.

Крім NS-3 та Cisco Packet Tracer, існує також багато інших програм та інструментів для моделювання та симуляції мереж.

Один з них - OMNeT++ (Objective Modular Network Testbed in C++). OMNeT++ є відкритим інструментом для моделювання та симуляції мережевих систем, що дозволяє створювати складні моделі мереж з різними протоколами та компонентами. Він підтримує різні рівні моделювання, включаючи моделювання каналів передачі даних, мережевого роутингу, протоколів транспортного рівня та багато іншого.

Іншим прикладом є OPNET (Optimized Network Engineering Tools), що надає можливості моделювання, аналізу та симуляції мережевих систем. OPNET має широкий набір функцій для дослідження різних аспектів мереж, включаючи пропускну здатність, затримки, рівень обслуговування, роутинг, протоколи транспортного рівня та інше.

Інші відомі програми для моделювання мереж включають QualNet, NetSim, GNS3, MiniNet та багато інших. Кожна з цих програм має свої особливості та переваги і може бути використана для різних цілей, включаючи навчання, дослідження та розробку мережевих протоколів.

2. Збір початкових даних:

- Вимірювання базових характеристик протоколів, таких як пропускна здатність, затримка, втрати пакетів тощо в умовах без навантаження та стабільної мережі.

3. Зміна рівня навантаження:

- Налаштування симуляційної мережі для відтворення зміни рівня навантаження, наприклад, збільшення кількості одночасних з'єднань або розміру передаваних даних.
- Запуск тестових сценаріїв, які відтворюють різні рівні навантаження на кожен з протоколів.

4. Вимірювання та аналіз результатів:

- Збір даних про характеристики протоколів під час зміни рівня навантаження, таких як пропускна здатність, затримка, втрати пакетів тощо.

- Аналіз отриманих результатів для кожного протоколу та порівняння їх.

5. Зміна умов каналу зв'язку:

- Налаштування симуляційної мережі для відтворення втрат пакетів на каналі зв'язку, наприклад, зміна рівня шуму, імітація перешкод або зниження якості з'єднання.

- Запуск тестових сценаріїв для кожного протоколу, щоб дослідити їхню ефективність та стійкість в умовах втрат пакетів.

6. Вимірювання та аналіз результатів:

- Збір даних про характеристики протоколів під час зміни умов каналу зв'язку, таких як пропускна здатність, затримка, втрати пакетів тощо.

- Аналіз отриманих результатів для кожного протоколу та порівняння їх.

7. Висновки:

- Формулювання висновків на основі отриманих результатів дослідження протоколів.

- Визначення, які протоколи виявилися найефективнішими та стійкими в умовах зміни рівня навантаження та втрат пакетів на каналі зв'язку.

2. Дослідження протоколів

Щоб перевірити як працюють протоколи, потрібно спочатку зібрати певну мережу для подальшого розгляду цих протоколів. Збір мережі та подальше її налаштування й дослідження буде проходити в спеціалізованій програмі під назвою Cisco Pocket Traker.

Cisco Packet Tracer - це інтерактивна програма, розроблена компанією Cisco Systems, яка використовується для моделювання, налаштування та тестування мережевих схем. Вона є потужним інструментом для вивчення мережевих технологій і дозволяє студентам, викладачам і мережевим інженерам ефективно вивчати та впроваджувати різні аспекти мережевого дизайну та конфігурації.

Основні особливості Cisco Packet Tracer:

- Моделювання мережі: Ви можете створювати власні мережеві схеми шляхом перетягування й розміщення пристроїв, таких як маршрутизатори, комутатори, комп'ютери та інші, на віртуальну дошку.
- Конфігурація пристроїв: Ви можете налаштовувати різні параметри пристроїв, включаючи IP-адреси, маршрутизацію, VLAN, бездротові мережі тощо. Це дозволяє вам експериментувати з налаштуванням різних мережевих протоколів та сервісів.
- Симуляція мережі: Packet Tracer надає можливість запускати симуляцію створених мереж для перевірки їх роботи та взаємодії пристроїв. Ви можете спостерігати за передачею даних, виявляти помилки та відлагоджувати проблеми в мережі.
- Програмування мережевих пристроїв: Cisco Packet Tracer підтримує мови програмування, такі як Python, для автоматизації та програмування мережевих пристроїв. Це дозволяє створювати скрипти для автоматизованої настройки та керування мережевими пристроями.
- Віртуальні лабораторії: Packet Tracer містить набір попередньо сконфігурованих віртуальних лабораторій, що дозволяють студентам

вивчати та вирішувати реальні мережеві задачі без необхідності фізичного обладнання.

Cisco Packet Tracer широко використовується в навчальних закладах для вивчення мережевих технологій, а також в мережевих компаніях для моделювання та тестування мережевих конфігурацій перед їх реалізацією.

2.1 Створення мережі.

Першим кроком у збірці мережі є визначення елементів, які будуть наявні в ній. Такими елементами є 4 ПК, один сервер та один свіч. Всі вони потрібні для подальшого дослідження протоколів.

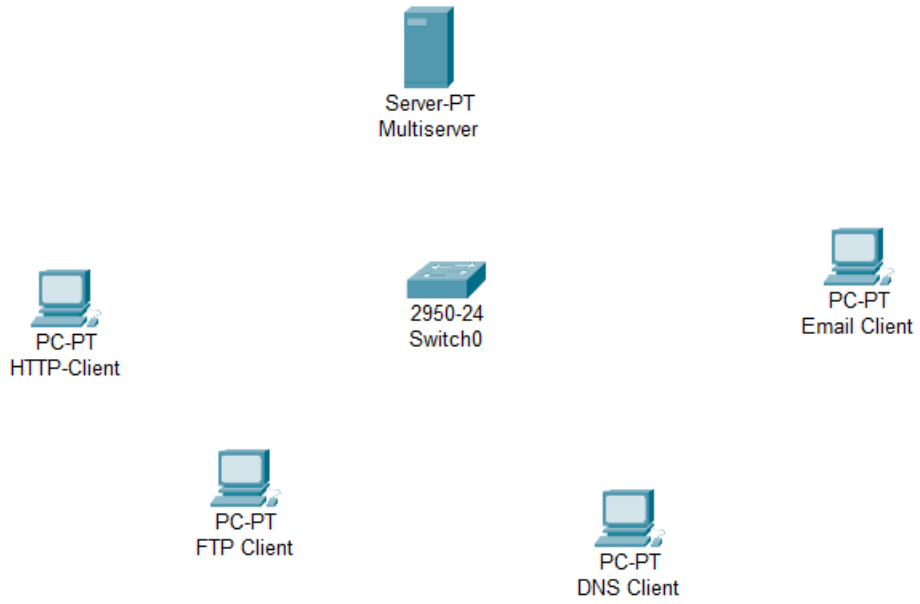

Рисунок 2.1 – елементи майбутньої мережі.

Наступним кроком є підключення всіх пристроїв в єдину мережу. Для цього потрібно в програмі зліва в низу обрати розділ підключення, а потім обрати тип підключення, яке буде застосовано.

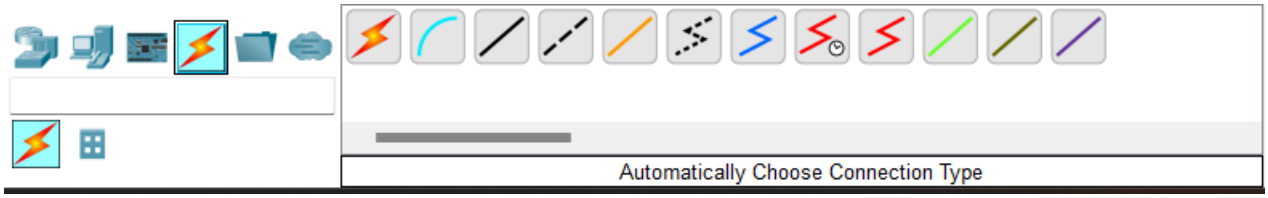

Рисунок 2.2 – Вибір типу підключення.

В даному випадку буде обрано автоматичний тип підключення. І програма сама, автоматично вибере найкращий спосіб.

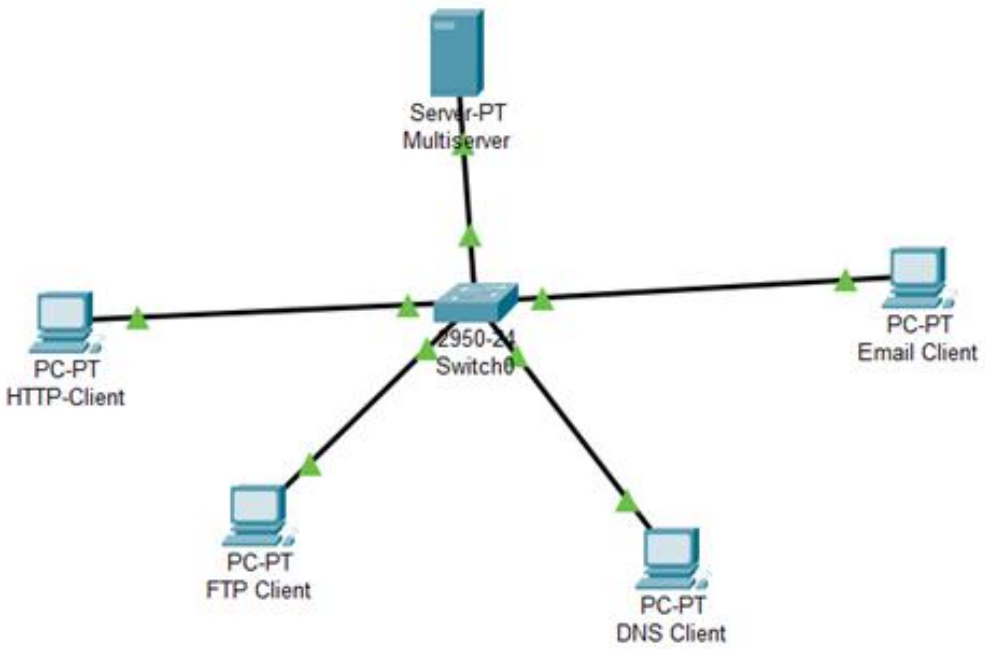

Рисунок 2.3 – Підключена мережа.

Після закінчення підключення, мережа вже має змогу в деякій мірі функціонувати. Та для коректного і правильного функціонування, її потрібно ще налаштувати.

2.2 Налаштування мережі

Першим та найважливішим елементом, який буде налаштовано є сервер. Натиснувши на його ярличок в мережі, відкриються різноманітні його налаштування. Для початку потрібно обрати розділ desktop де відкриються різноманітні доступні програми для використання. Далі знайти програму під назвою ip configuration, та відкрити її. В цій програмі потрібно провести айпі конфігурацію для пристрою. А саме:

IPv4 – 192.168.0.2

Subnet Mask – 255.255.255.0

Default Gateway –192.168.0.1

DNS Server – 192.168.0.2

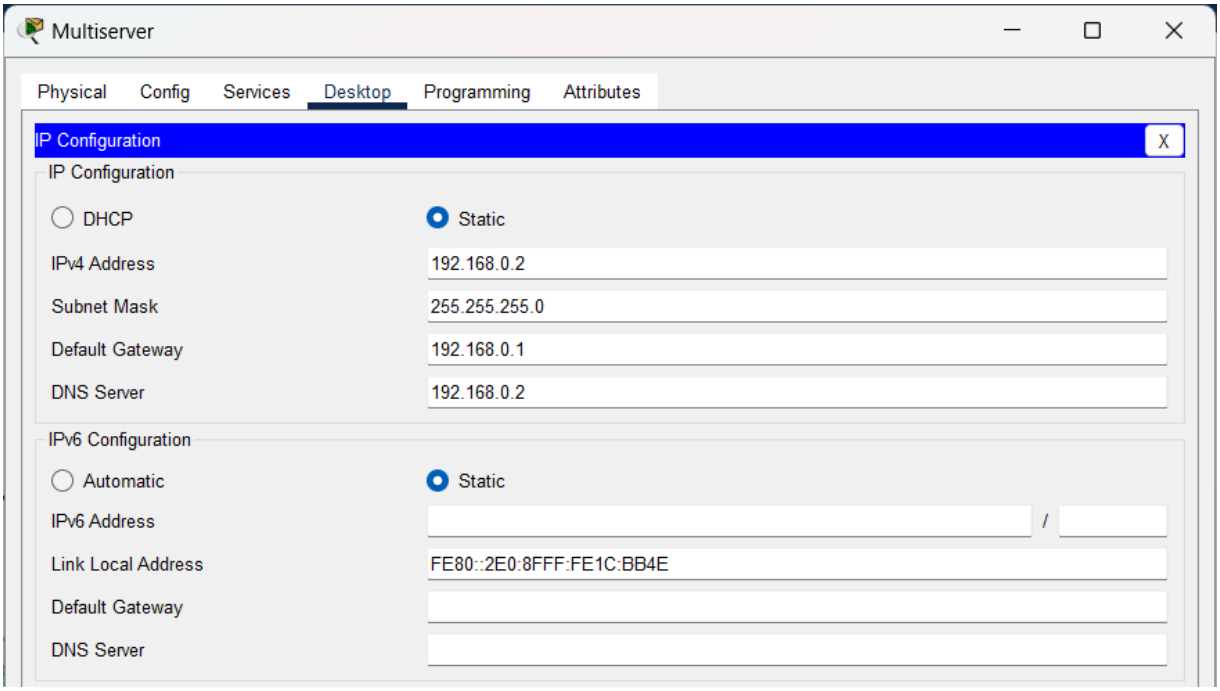

Рисунок 2.4 – Конфігурація айпі.

Тепер процес конфігурації айпі завершений, і можна переходити до наступного етапу налаштування, а саме до глобального налаштування сервера.

Повернувшись назад до розділу desktop, потрібного перемкнути його на розділ Serwices. В даному розділі відбудеться подальший процес налаштування.

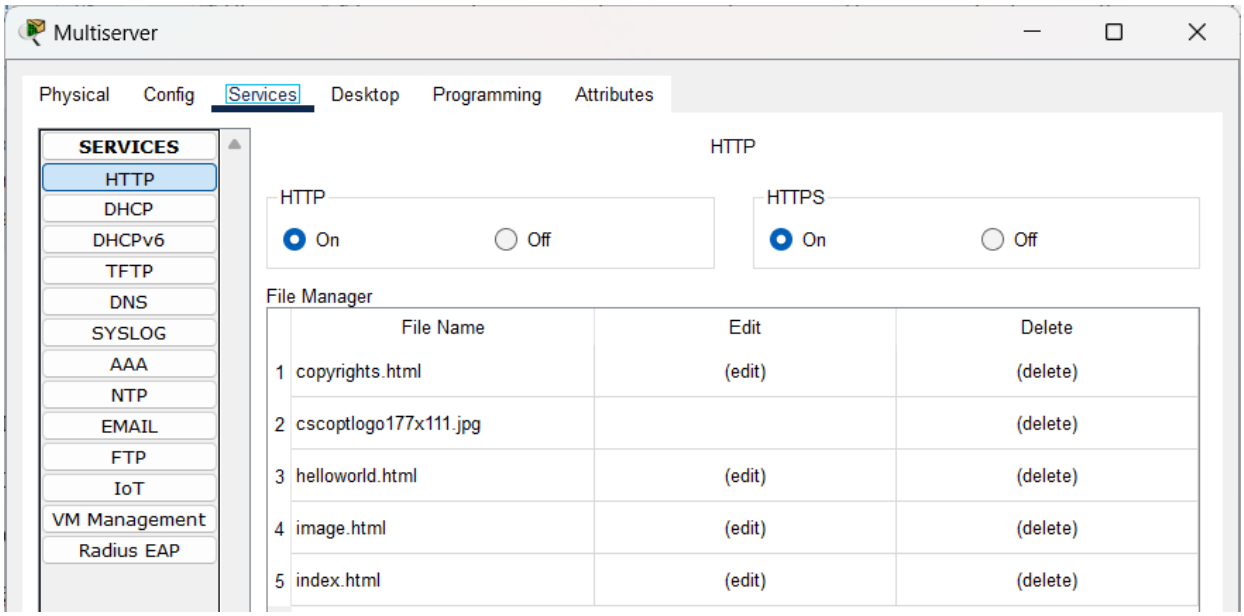

Рисунок 2.5 – Вигляд меню Serwices.

Обравши вкладку HTTP відкриється список наявних файлів. В ньому потрібно обрати index.html в якому провести подальші зміни. А саме, написати наступний текст:

```
<html>
<body>
    <h1> Interet technology</h1>
    <hr/>
    <h3> By Poltava 12345</h3>
</body>
</html>
```

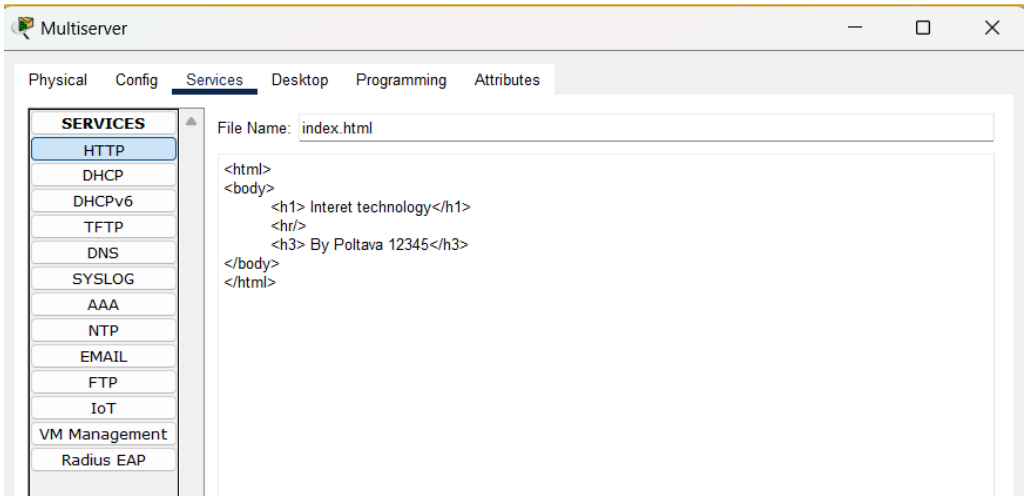

Рисунок 2.6 – Змінений файл index.html.

Написавши цей код потрібно зберегти зміни у файлі та вийти. Наступним кроком є налаштування самого DNS сервера. Для цього потрібно перейти до наступного однойменного розділу – DNS. Першим кроком тут є вмикання самого DNS серверу. Далі в полі Resource Records: Name потрібно назвати наш DNS сервер. Обране ім’я для нього – це pvg.edu.in. Саме це в подальшому користувачі повинні будуть вводити, для можливості відправки повідомлення іншому користувачу. І заключним етапом є введення айпі цього DNS сервера, яке вже було задано в попередньому етапі налаштування, а саме

- 192.168.0.2. Після чого потрібно додати обраний DNS в однойменну базу серверів, натиснувши кнопку Add.

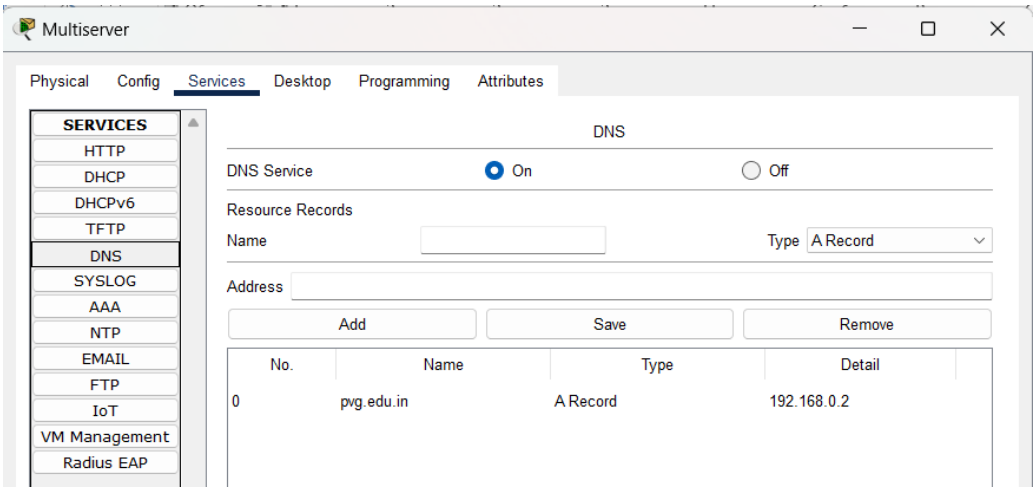

Рисунок 2.7 – Результат налаштування DNS.

Наступним етапом є реєстрація емейлів користувачів за цим доменом. Для цього спочатку потрібно перейти до розділу EMAIL. В ньому, в першу чергу, потрібно ввімкнути STM Service та POP3 Service, для коректної роботи системи.

Далі в полі Domain Name потрібно написати ім’я домену яке було обране у попередньому розділі, це - pvg.edu.in. Після чого потрібно зареєструвати користувачів, яким буде в подальшому наданий доступ відправки та прийому повідомлень. Для цього потрібно в полях нижче написати ім’я облікового запису, та пароль, завдяки якому до цього облікового запису можна буде потім зайти.

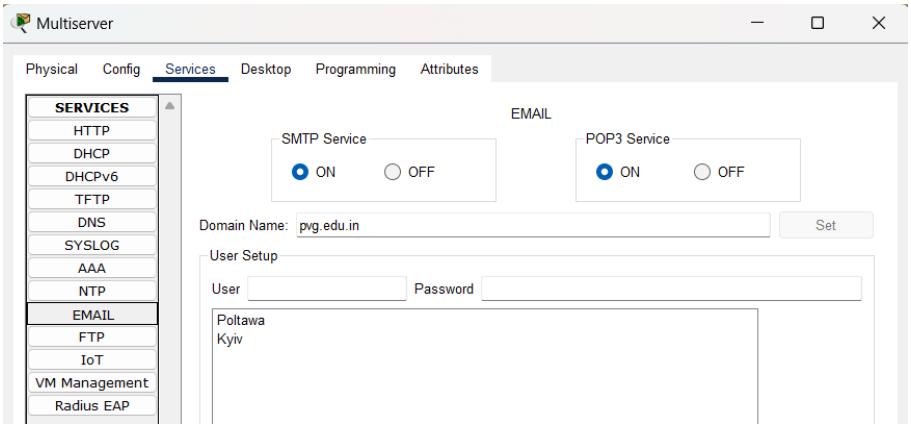

Рисунок 2.8 – Результат налаштування EMAIL.

Облікові записи для користувачів, які були додані мають назву Poltava та Kyiv. До кожного з яких паролем є послідовність цифр від одного до п’яти, а саме – 12345. На рисунку 6, можна бачити результат додавання цих облікових записів в систему, для їх подальшої можливості використання.

Наступним кроком є процес налаштування FTP. FTP (File Transfer Protocol) - це протокол передачі файлів, який використовується для обміну файлами між комп'ютерами у мережі Інтернет. Він є одним з найпоширеніших протоколів для передачі файлів і надає можливість керувати, завантажувати і вивантажувати файли з віддалених серверів.

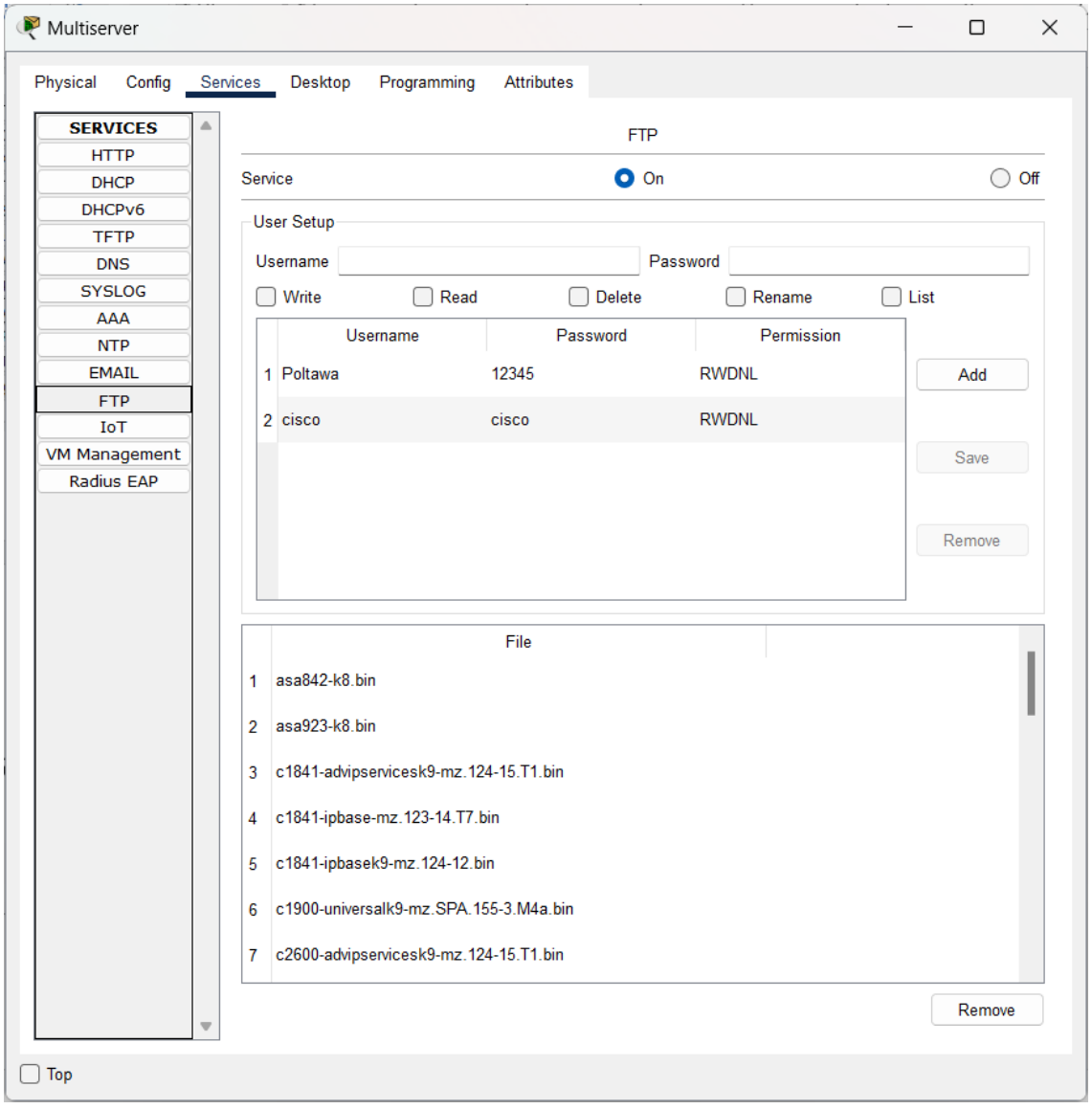

Рисунок 2.9 – Процес налаштування FTP.

Першим кроком є активування даного протоколу. Для цього в розділі Service потрібно обрати функцію on. Після чого FTP протокол буде активовано. Далі потрібно по черзі в полі User Name ввести дані облікових записів, які були створені на попередньому етапі. Після чого нижче поставити всі можливі голочки для них, та додати за допомогою кнопки Add. Це дасть певні права для користувачів відповідно до галочок, які були поставлені перед додаванням користувача. Це є фінальним етапом налаштування сервера.

Наступним етапом є налаштування айпі конфігурацій для наявних ПК. Для цього потрібно натиснути на один з ПК, перейти в розділ desktop та обрати програму ip configuration. Саме в ній для даного ПК потрібно й провести айпі конфігурацію за даним прикладом:

IPv4 – 192.168.0.3

Subnet Mask – 255.255.255.0

Default Gateway –192.168.0.1

DNS Server – 192.168.0.2

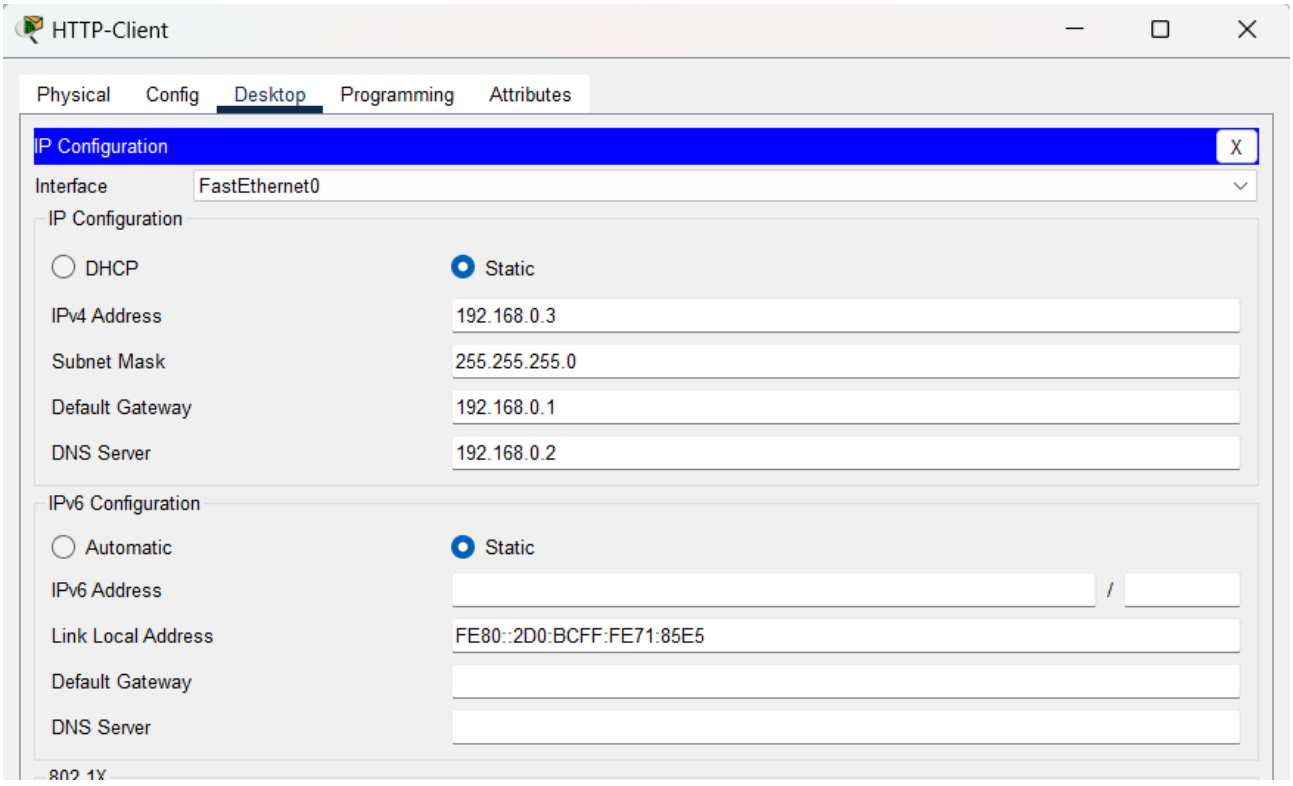

Рисунок 2.10 – Налаштування ПК.

Дане налаштування відбувалося для ПК під назвою HTTP-Client. За цим же принципом потрібно налаштувати наступні ПК. Дані за якими будуть налаштовані інші ПК:

- ПК FTP Client
    - IPv4 – 192.168.0.4
    - Subnet Mask – 255.255.255.0
    - Default Gateway –192.168.0.1
    - DNS Server – 192.168.0.2
- ПК DNS Client
    - IPv4 – 192.168.0.5
    - Subnet Mask – 255.255.255.0
    - Default Gateway –192.168.0.1
    - DNS Server – 192.168.0.2
- ПК Email Client
    - IPv4 – 192.168.0.6
    - Subnet Mask – 255.255.255.0
    - Default Gateway –192.168.0.1
    - DNS Server – 192.168.0.2

Після цього налаштування ПК завершено, і залишається фінальний етап налаштування мережі – налаштування емейлів на самих ПК. Для цього потрібно натиснути на ПК Email Client, в розділі desktop знайти застосунок Email та увійти до облікового запису, який був створений. Після заходження в застосунок Email відбудеться налаштування безпосередньо вже пошти користувача. Тут потрібно ввести інформацію про користувача - ім’я користувача, емейл адрес за яким його зможуть знайти інши користувачі. Далі потрібно ввести інформацію про сервер, який буде використано. І останнім це ввести інформацію про обліковий запис користувача. Де буде зазначатися його

логін та пароль. Після чого слід зберегти зміни і налаштування буде завершено.

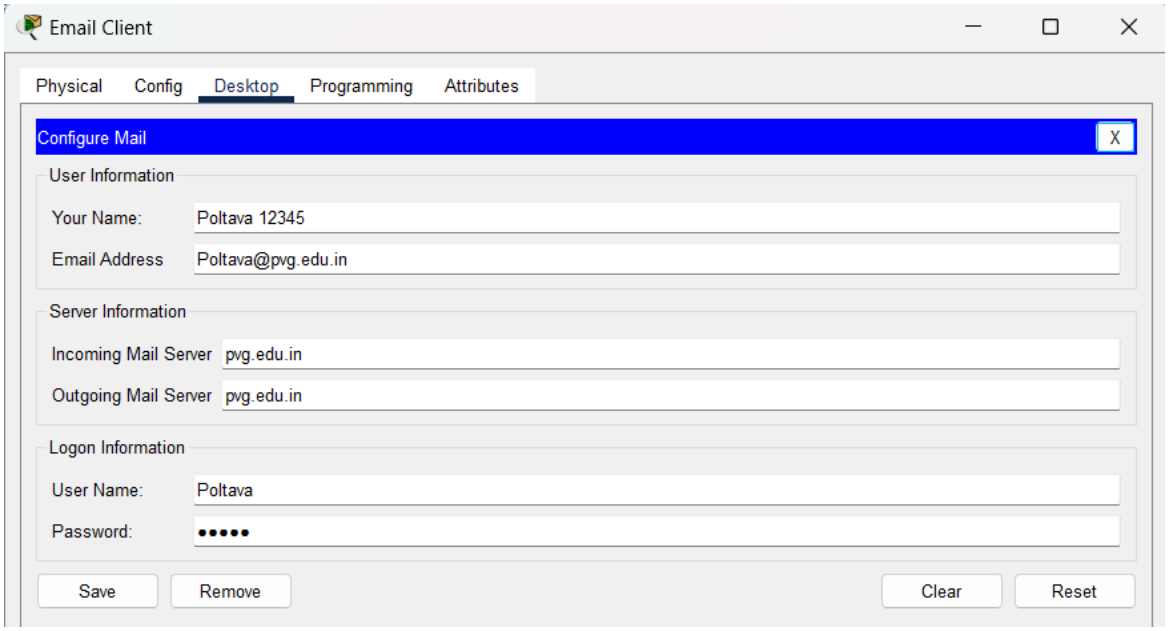

Рисунок 2.11 – Налаштування першого облікового запису.

Аналогічне налаштування потрібно провести й для ПК HTTP-Client. Але слід обрати вже інший обліковий запис.

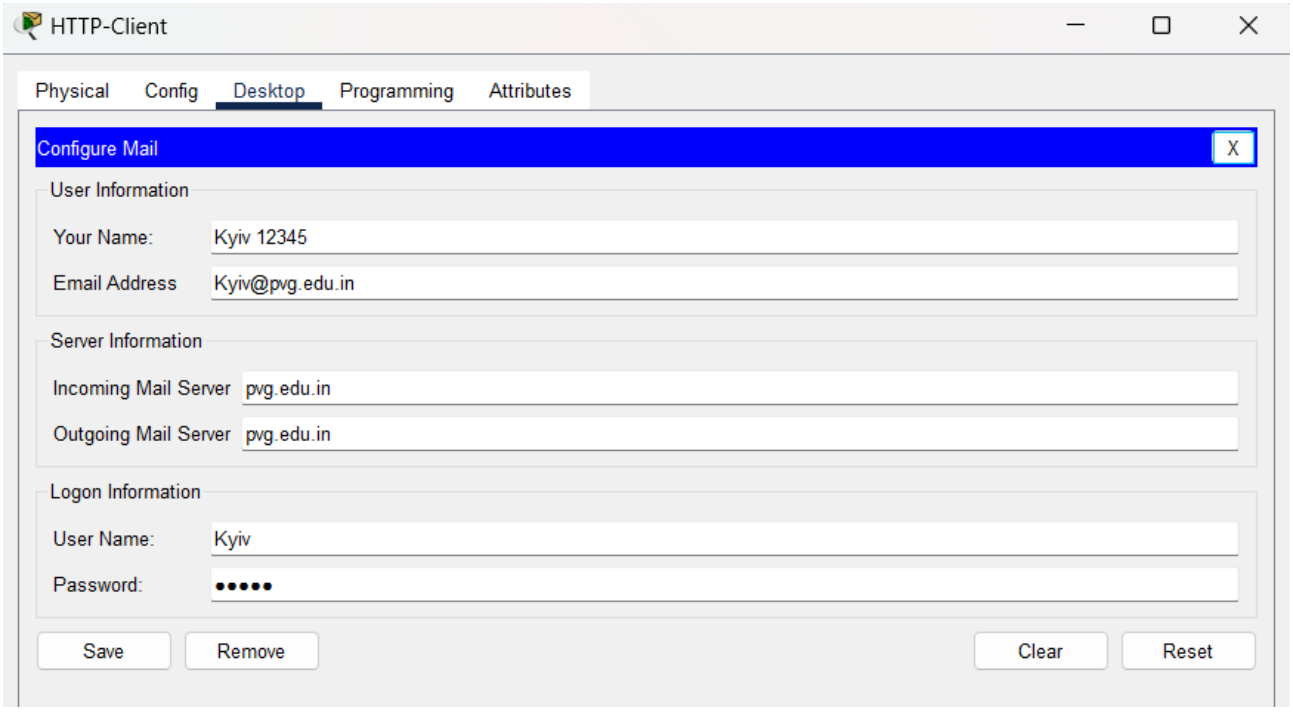

Рисунок 2.12 – Налаштування другого облікового запису.

Після всіх дій, які були проведені, процес налаштування мережі є завершеним. Тепер ми маємо змогу провести її подальше дослідження, а також впевнитись в її функціонуванні.

2.3 Дослідження протоколів.

Першим кроком є перевірка з’єднання та можливість передачі пакетів даних між пристроями. Для цього потрібно натиснути на MultiServer, в ньому відкрити розділ desktop, в якому знайти програму Command Prompt. В даній програмі ввести команду *ping 192.168.1.255*. Через декілька секунд буде результат від кожного під’єднаного пристрою.

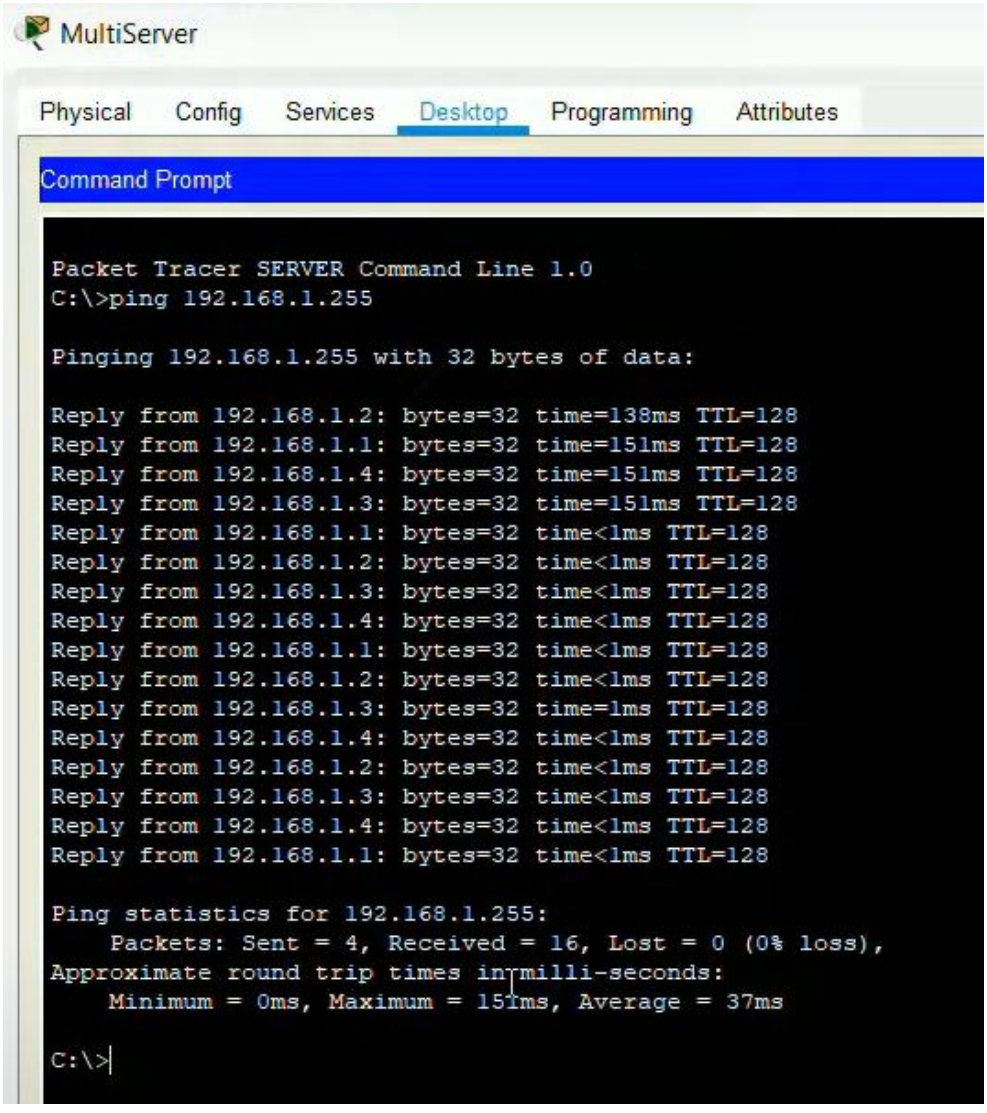

Рисунок 2.13 – Результат виконання команди.

Received = 16 свідчить, що всі пакети даних успішно повертаються назад. Sent = 4 свідчить про те, що було відправлено чотири пакета. Тільки 4 тому, що в схемі наявно лише чотири пристрої (ПК). Це все свідчить про те, що мережа працює належним чином.

Далі потрібно згенерувати трафіки, а саме веб-трафік(HTTP), FTP-трафік, DNS-трафік та трафік електронної пошти. Для цього потрібно перейти в режим моделювання. Потім відкрити HTTP Client та в розділі desktop знайти програму Web Browser. У відкритому браузері потрібно ввести айпі сервера та запустити його. Тепер веб-трафік є згенерованим. В підтвердження цього, на схемі з’явиться запечатаний конверт, який являє собою пакет даних HTTP.

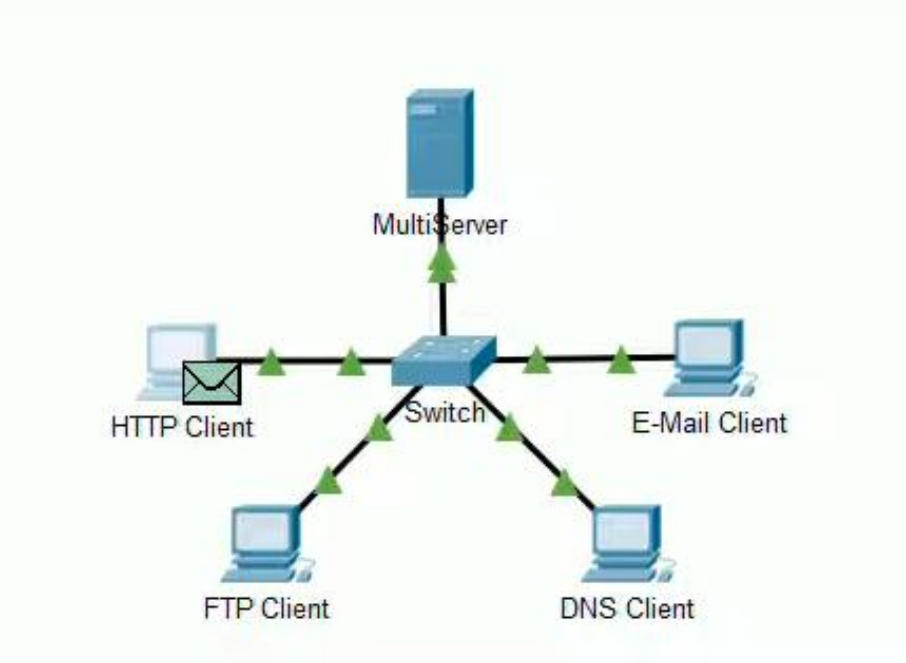

Рисунок 2.14 – Створений HTTP-пакет даних.

Наступним кроком є генерація FTP-трафіка. Для цього потрібно відкрити FTP Client і в розділі desktop відкрити програму Command Promp. В даній програмі потрібно ввести команду для генерації FTP-трафіка. Ця команда – це *ftp 192.168.1.254*, після введення якої відбудеться генерування трафіка.

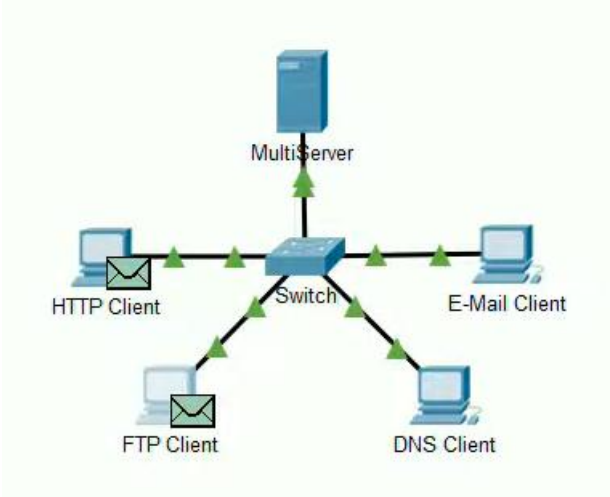

Рисунок 2.15 – Створений FTP-пакет даних.

Після цього потрібно згенерувати DNS-трафік. Аналогічно з генерацією попереднього трафіку, потрібно відкрити однойменний клієнт в якому в програмі Command Promp виконати команду *nslookup multiserver.pvg.edu.in*. Як і з попередньою генерацією, DNS-трафік буде створено. Переконатися в цьому можна аналогічно з попередніми трафіками.

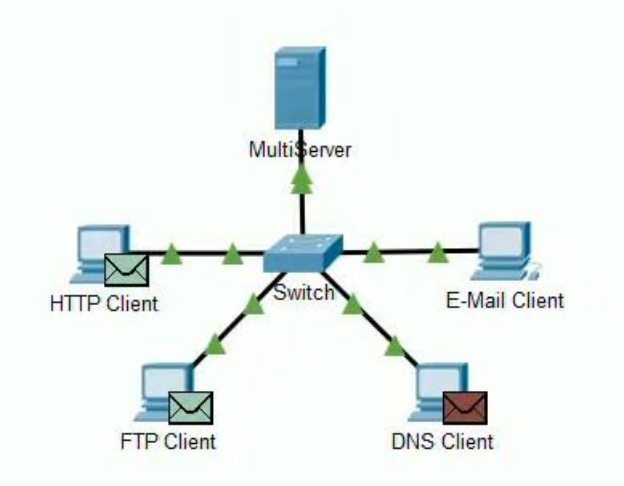

Рисунок 2.16 – Створений DNS-трафік даних.

Фінальним етапом генерації трафіку, є створення трафіку електронної пошти. Для цього з E-Mail Client потрібно відправити листа на іншу пошту. В даному випадку на пошту, яка була створена на етапі створення мережі. Після відправки листа з’явиться наступне:

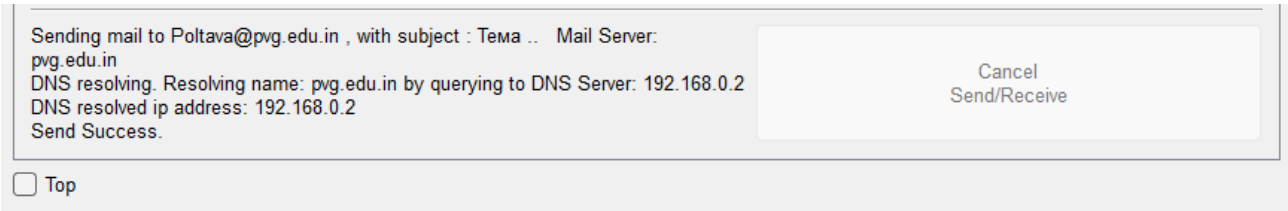

Рисунок 2.17 – Результат відправки листа.

Результатом виконання цих дій буде створення трафіку електронної пошти. Який є останнім з типів трафіку, які будуть створені. Після цього з’явиться відповідний символ листа проти E-Mail Client на схемі.

Щоб впевнитися, що все працює потрібно спробувати передати пакети даних до мультисервера. У вікні симуляції, яке з’явилося після переходу в режим моделювання, яке було здійснено перед початком генерації трафіку, потрібно запустити передачу пакетів даних.

Після запуску можна спостерігати як всі пакети одночасно відправляються до свіча (комутатора), а потім по черзі до мультисервера. Фінальним етапом передачі даних є почергове отримання відповіді для кожного пристрою

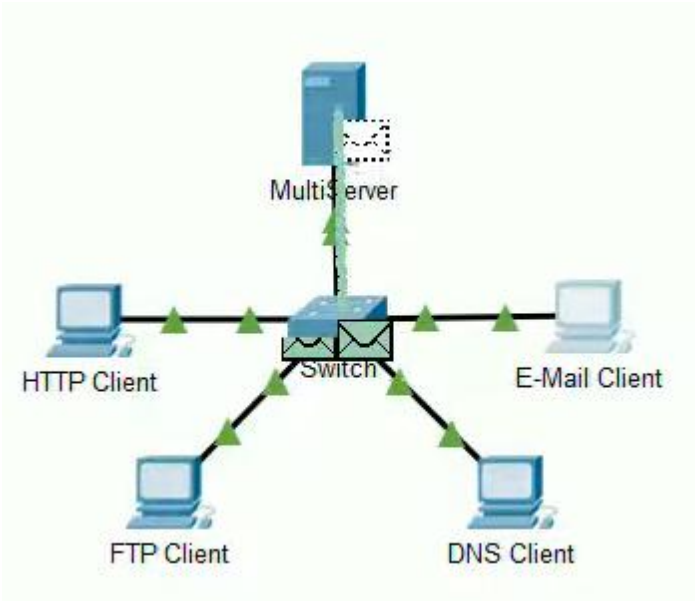

Рисунок 2.18 – Процес передачі пакетів даних.

Всі кроки передачі пакетів даних можна спостерігати на наступному рисунку:

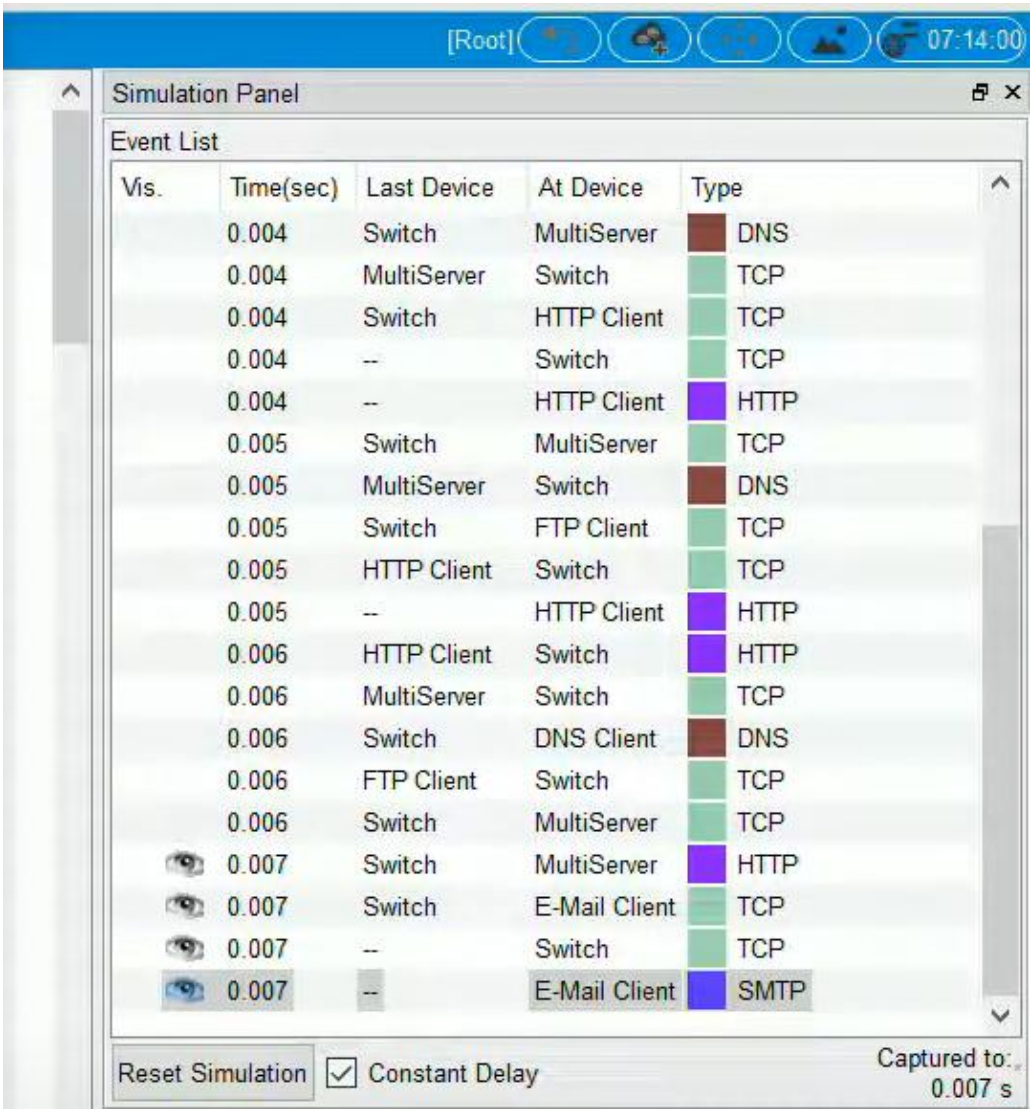

Рисунок 2.19 – Етапи передачі пакетів даних.

Це загальний вигляд передачі всього масиву даних. Для дослідження конкретного з протоколів потрібно скористатися фільтром та обрати потрібні. В даному випадку буде проводитись дослідження TCP та HTTP протоколів. Використавши фільтри потрібно натиснути на один з пакетів даних, щоб подивитися детальну інформацію про нього.

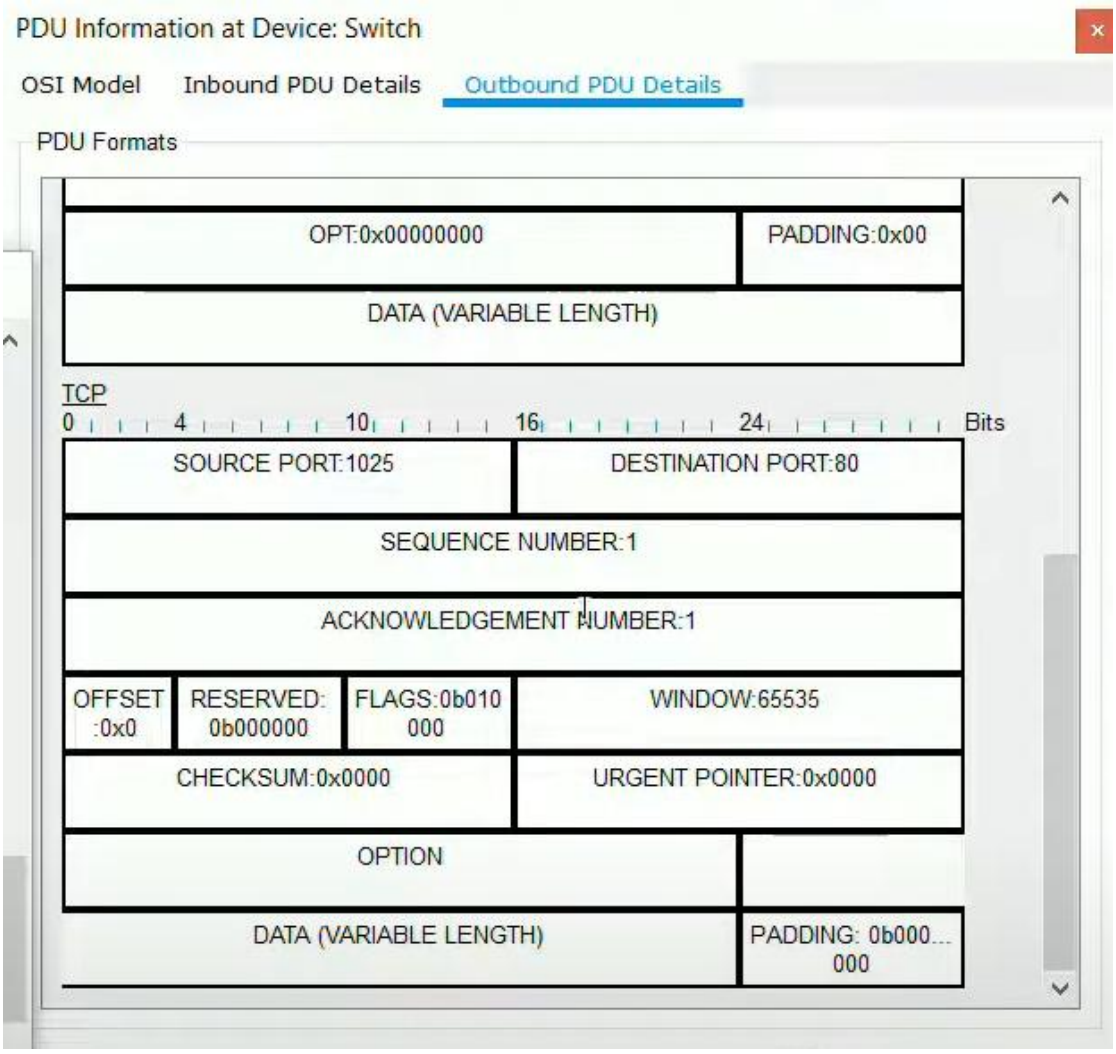

Рисунок 2.20– Дослідження TCP.

Відкривши один з пакетів даних, можна подивитися детальну інформацію про нього та стан в якому знаходиться процес передачі даного пакету. Переглянувши дані можна зробити висновки, звідки й куди передаються дані, проглянути детальну інформацію про пакет даних, переглянути стан передачі.

За таким же принципом можна переглянути й пакети даних інших протоколів. Інформація, яка наявна свідчить про те, що за допомогою протоколу TCP пакети даних передаються нормально й без перешкод, а самий стан передачі інформації має певну стійкість до втрати частини пакетів даних.

2.4 Висновок до розділу.

Після проведення дослідження протоколу TCP (Transmission Control Protocol) в середовищі Cisco Packet Tracer можна зробити наступні висновки:

- Надійність передачі даних: Протокол TCP забезпечує надійну передачу даних шляхом впровадження механізмів підтвердження доставки, перевірки цілісності даних та управління потоком. Це дозволяє гарантувати, що дані будуть доставлені у правильному порядку та без втрат.
- Управління потоком: TCP використовує механізми віконного керування та алгоритми контролю переповнення, щоб регулювати швидкість передачі даних між відправником і отримувачем. Це дозволяє пристосовувати швидкість передачі до поточних умов мережі та запобігає перевантаженням.
- Розбиття даних на пакети: TCP розбиває дані на пакети перед відправкою, а потім збирає їх у правильному порядку відповідно до номерів послідовності. Це дозволяє передавати великі об'єми даних через мережу та забезпечує їх правильну реконструкцію на отримувачі.
- Відправка підтверджень: TCP використовує підтвердження для підтвердження успішної доставки даних. Отримуючи підтвердження від отримувача, відправник може бути впевнений, що дані були доставлені правильно. У разі невдалої доставки або втрати пакетів, TCP автоматично відправляє знову тільки втрачені пакети.
- Контроль цілісності даних: TCP використовує контрольну суму для перевірки цілісності даних. Це дозволяє виявляти будь-які зміни або пошкодження даних під час передачі.

Загалом, дослідження протоколу TCP в середовищі Cisco Packet Tracer підтвердило його ефективність та надійність в передачі даних через мережу. TCP є одним з найпоширеніших протоколів у Інтернеті і використовується для передачі різних типів даних, включаючи веб-сторінки, електронну пошту та файлові передачі.

Висновки

Дослідження протоколів транспортного рівня мереж наступного покоління (Next Generation Networks, NGN) відкриває широкі можливості для подальшого розвитку та вдосконалення телекомунікаційних систем. NGN є перехідним етапом в еволюції мереж, спрямованим на забезпечення інтеграції традиційних телекомунікаційних служб з інтернет-протоколами та розширеними сервісами.

Протоколи транспортного рівня в NGN мають вирішувати ряд викликів, пов'язаних з високою швидкістю передачі даних, надійністю, безпекою і якістю обслуговування. Дослідження цих протоколів спрямовані на розробку ефективних рішень, які враховують особливості NGN-середовища.

У даній роботі було проведено дослідження протоколів транспортного рівня мереж наступного покоління (Next Generation Networks, NGN), зокрема було змодельовано мережу і досліджено передачу пакетів даних за допомогою протоколу TCP.

Протокол TCP (Transmission Control Protocol) є одним з основних протоколів транспортного рівня, що використовується в Інтернеті. Він забезпечує надійну та послідовну передачу даних між вузлами мережі. В рамках дослідження було вивчено принципи роботи TCP та його взаємодію з іншими компонентами мережі NGN.

Під час моделювання мережі та передачі пакетів даних була приділена значна увага вивченню основних характеристик та параметрів протоколу TCP, таких як розмір вікна, механізми керування перевантаженням, алгоритм контролю перетину часових меж (Congestion Control), та інші.

Результати дослідження показали, що протокол TCP є ефективним і надійним рішенням для передачі даних в мережах NGN. Він забезпечує керування потоком даних, корекцію помилок, відновлення втрачених пакетів та управління перевантаженням. Протокол TCP також дозволяє досягти високої швидкості передачі даних та забезпечує стабільну роботу мережі при змінних умовах передачі.

Однак, в ході дослідження також було виявлено деякі обмеження протоколу TCP, зокрема пов'язані зі збільшенням затримок передачі даних у великих мережах та нездатністю ефективно працювати з високими рівнями втрати пакетів. Такі обмеження можуть вплинути на якість обслуговування та продуктивність мережі.

Отже, висновок з дослідження протоколів транспортного рівня мереж NGN, з фокусом на протокол TCP, полягає в тому, що TCP є потужним та ефективним протоколом для надійної передачі даних у мережах наступного покоління. Однак, при розробці мереж NGN необхідно враховувати його обмеження та шукати рішення для оптимізації та покращення його продуктивності, зокрема в умовах великих розмірів мереж та високих рівнів втрати пакетів. Такі дослідження допоможуть розробити ефективніші та вдосконалені протоколи транспортного рівня для майбутніх мереж NGN, що забезпечать ще більшу продуктивність, надійність та якість обслуговування.

Список використаних джерел

1. Cisco Networking Acade. [Електронний ресурс] – Режим доступу: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiakIue0L3_AhXQpIsKHZwvCEwQFnoECA4QAQ&url=https%3A%2F%2Fwww.netacad.com%2Fru&usg=AOvVaw2F0ygc7Fm4Hep_YFparxuu
2. Протоколи мереж NGN. [Електронний ресурс] – Режим доступу: https://studfile.net/preview/2918681/page:9/

   Transmission Control Protocol. [Електронний ресурс] – Режим доступу: https://ua.wikipedia.org/wiki/TCP
3. Протокол TCP [Електронний ресурс] – Режим доступу: https://docstore.mik.ua/manuals/ru/linux_base/node350.html
4. Cisco Packet Tracer [Електронний ресурс] – Режим доступу: https://www.netacad.com/courses/packet-tracer
5. Моделі OSI [Електронний ресурс] – Режим доступу: https://lanmarket.ua/ua/stats/modeli-OSI---posobie-dlya-nachinayushchih/
6. Network Protocols [Електронний ресурс] – Режим доступу: https://www.comptia.org/content/guides/what-is-a-network-protocol
7. Types of Networking Protocol [Електронний ресурс] – Режим доступу: https://www.manageengine.com/network-monitoring/network-protocols.html

Додаток А

Theoretical review

Transport layer protocols are network protocols that enable data transfer between programs running on different computers or devices. In next-generation NGN networks, transport layer protocols play an important role in ensuring efficient and reliable data transmission.

The main transport layer protocols of next-generation NGN networks are TCP (Transmission Control Protocol), SCTP (Stream Control Transmission Protocol) and DCCP (Datagram Congestion Control Protocol).

TCP (Transmission Control Protocol) is a network transport layer protocol that ensures reliable data delivery between programs running on different computers or devices. TCP is used in various network architectures, including NGN (Next Generation Networks).

TCP provides serial data transmission, which allows recovery of data that was lost during transmission. To do this, TCP uses a sequential packet numbering mechanism that allows you to determine which data was transmitted successfully and which was lost. If data has been lost, TCP sends a request to retransmit that data.

TCP also uses network load control mechanisms, such as window view and flow control. The window view mechanism allows you to control the number of packets that can be sent to the recipient without waiting for confirmation of the delivery of previous packets. This allows you to maintain a high data transfer rate and avoid network congestion.The flow control mechanism allows you to adjust the data transfer rate depending on the ability of the recipient to process the data. This avoids overloading the recipient and ensures reliable data delivery.

TCP also supports a connection termination control mechanism that allows you to close the connection between two devices after the data transfer is complete. This ensures efficient use of resources.

SCTP (Stream Control Transmission Protocol) is a transport layer protocol designed for a reliable transport service with support for data streams and multiple

connections. SCTP is a next-generation protocol that can be used in various network architectures, including NGN (Next Generation Networks).

One of the main differences between SCTP and TCP is the support for multiplexing data streams and multiple connections. SCTP uses the concept of association, which allows more than one connection between two devices to be used at the same time. Each connection contains a set of data streams that can be multiplexed on a single connection. This allows efficient use of network resources and provides a higher data transfer rate.

SCTP also provides reliable data delivery, similar to TCP, using a flow control mechanism and a windowing mechanism. However, SCTP has additional network load control mechanisms, such as congestion control mechanism and resource control mechanism. The congestion control mechanism allows you to control the speed of data transmission on the network and avoid network congestion.The resource management mechanism allows you to control the use of resources on network devices and avoid resource overload.

SCTP also supports a connection termination control mechanism that allows for safe termination of connections between devices and avoids data loss or network security compromise. SCTP also has additional features such as support for multi-touch networks, a delivery verification mechanism, and support for DDoS protection mechanisms.

One of the main applications of SCTP is the transport of SIP (Session Initiation Protocol), which is used to manage communication sessions in next-generation networks. SCTP provides a reliable transport service for SIP, enabling high quality of service for customers and ensuring network efficiency.

In summary, SCTP is a transport layer protocol that provides a reliable transport service with support for data streams and multiple connections. It supports data flow multiplexing, network load control and connection termination mechanisms, and has additional features to support multi-touch networks and protect against DDoS attacks. SCTP is used in various network architectures, including next-generation NGN networks, and is one of the main protocols for SIP transport.

DCCP (Datagram Congestion Control Protocol) is a transport layer protocol designed for data transmission in highly congested networks such as the Internet.

DCCP is designed as an alternative to TCP and UDP, allowing for more efficient data transfer for applications that require reliability and network load control.

One of the main properties of DCCP is the support of different data transfer profiles (transport service profiles) corresponding to different types of applications. These profiles define the level of reliability, maximum throughput and other characteristics of the transport service. Thus, DCCP provides the ability to configure the protocol according to the requirements of a specific application.

DCCP also has mechanisms to control network load and support multiplexing of data flows, which allows efficient use of network resources. In addition, DCCP has a mechanism for controlling network pollution (congestion control), which ensures stability and reliability of data transmission in conditions of variable network load.

One of the features of DCCP is the ability to use different codecs to transmit audio and video data. Codecs are responsible for the compression and decoding of data and allow efficient transmission of media data over networks with limited bandwidth.

DCCP can be used for various applications such as video streaming, video conferencing.

The advantages of DCCP include the ability to use various methods of overflow control and data flow control.In particular, the protocol provides the possibility of using two methods of overflow management: separate and integrated management.

Separate control involves using a separate channel to transmit network status messages, while integrated control uses network status messages on the same channel as data.

Additional features of DCCP include support for multi-stream connections, which enables simultaneous transmission and reception of different data streams. In

addition, the protocol provides the ability to use not only connections with reliable data transmission, but also connections with unreliable data transmission.

DCCP can be used for data transmission in a variety of applications where it is important to ensure high data transmission efficiency when using next-generation networks. In particular, the protocol can be used to transmit audio and video streams, online games, as well as in other applications that require fast data transmission with a high level of reliability.

To compare the characteristics, features and efficiency of the transport layer protocols of the next generation NGN networks, we will analyze three such protocols: TCP, SCTP and DCCP.

TCP (Transmission Control Protocol) is a protocol that ensures reliable data transport in networks. It is used to transfer data that requires reliability, such as web pages, emails and files.

The main characteristics of TCP:

• Reliable data delivery: TCP ensures data delivery without loss or duplication.

• Flow control: TCP controls the flow of data to avoid buffer overflows at the receiver.

• Integrity check control: TCP uses an integrity check mechanism to ensure that data has not been altered during transmission.

• Protocol Layer Connection: TCP establishes a protocol layer connection between sender and receiver.

• Congestion management: TCP has mechanisms that allow it to reduce data rates if the network is congested.

SCTP (Stream Control Transmission Protocol) is a protocol that provides data transmission in networks. It was designed to support high-reliability applications such as VoIP, video conferencing, and streaming media.

Next, we will compare the features and effectiveness of SCTP and DCCP protocols.

SCTP and DCCP were developed for different purposes and have their own characteristics and applications accordingly.

SCTP is a multi-stream protocol that can be used for various purposes, such as supporting multicast, providing a redundant data link, and supporting security features. SCTP also has mechanisms to avoid congestion at the network layer and mechanisms to recover from packet loss. One of the main disadvantages of SCTP is its complexity, which can increase the overhead of packet processing.DCCP provides secure data transfer with congestion control, making it ideal for multimedia applications such as streaming video and audio. It also supports various transfer modes such as streaming and delivery without delivery assurance. DCCP is less complex than SCTP, allowing for reduced packet processing overhead. However, unlike SCTP, DCCP does not support multicast.

In general, if secure multi-threaded data transfer is required, with support for security and packet loss recovery mechanisms, then SCTP may be the better choice. If providing congestion control and less complexity is more important, then DCCP may be a better option.

In addition, SCTP supports a multiplexing mechanism that allows different data streams to be transmitted over a single SCTP connection. This reduces the load on the network and increases the efficiency of data transmission.

Finally, DCCP is the protocol that supports the largest number of data flow types, such as reliable, unreliable, and streaming. It also has a load control mechanism that allows you to adjust the data transfer rate depending on the state of the network.

The main differences between the protocols are their support of functions, data transfer speed and reliability. TCP is the most common protocol and has high reliability, but its speed can be limited. SCTP is less popular, but it has built-in support for multiplexing and is more efficient for data transfer in some cases.DCCP is very flexible and can support different types of data flows and has a load control mechanism.

Therefore, the choice of transport layer protocol depends on specific network requirements and user needs. For applications that require high data transmission reliability, TCP may be the best option. For applications that require higher

performance, SCTP or DCCP may be better options, depending on user needs and the nature of the data being transmitted.