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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Оптимізація процесу керування комп'ютерними мережами для підвищення продуктивності»

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

_____ *Микола ЯНЧУК*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КІД-42
Микола ЯНЧУК
Ім'я, ПРІЗВИЩЕ
Керівник: Ігор БУЧЕНКО
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Рецензент:
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2024

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 кафедрою Наталія ЛАЩЕВСЬКА
_____Ім'я, ПРІЗВИЩЕ
«_____» _____ 2024р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Янчук Микола Олександрович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Оптимізація процесу керування комп'ютерними
2. мережами для підвищення продуктивності
керівник кваліфікаційної роботи Ігор БУЧЕНКО,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «27» лютого 2024р. № 36
3. Строк подання кваліфікаційної роботи «3» червня 2024р.
4. Вихідні дані до кваліфікаційної роботи: Актуальність теми дослідження, пов'язана з розвитком комп'ютерних мереж та постійним зростанням вимог до їх продуктивності.
Необхідність оптимізації процесу керування комп'ютерними мережами для забезпечення їх ефективної роботи.
Існування різноманітних методів та технологій оптимізації, які потребують комплексного вивчення та аналізу.
Практична значущість дослідження, яке може призвести до покращення роботи комп'ютерних мереж в різних сферах діяльності.
5. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ КОМП'ЮТЕРНИМИ МЕРЕЖАМИ
2. ПРОБЛЕМИ ТА ВИКЛИКИ УПРАВЛІННЯ КОМП'ЮТЕРНИМИ МЕРЕЖАМИ
3. МЕТОДИ ОПТИМІЗАЦІЇ УПРАВЛІННЯ КОМП'ЮТЕРНИМИ МЕРЕЖАМИ
4. РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ
6. Перелік ілюстративного матеріалу: *презентація*
7. Дата видачі завдання «27» лютого 2024р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	28.02-22.03.2024	Виконано
2	Обробка матеріалу	23.03-05.04.2024	Виконано
3	Розробка теоретичної частини	06.04-10.04.2024	Виконано
4	Розробка практичної частини	11.04-30.04.2024	Виконано
5	Дослідження та аналіз	01.05-03.05.2024	Виконано
6	Висновки за результатами аналізу	04.05-08.05.2024	Виконано
7	Розробка презентації	09.05-11.05.2024	Виконано
8	Передзахист	13.05-17.05.2024	Виконано
9	Здача в деканат	25.05-3.06.2024	Виконано

Здобувач вищої освіти _____ Микола ЯНЧУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ігор БУЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 38 стор., рис.11, 1 табл., 31 джерел.

Мета роботи – розробка та реалізація методів оптимізації процесу керування комп'ютерними мережами з метою підвищення їх продуктивності та ефективності.

Об'єкт дослідження – комп'ютерні мережі.

Предмет дослідження – процес керування цими мережами з метою підвищення їх продуктивності.

Короткий зміст роботи: З ростом обсягу даних та користувачів виникає потреба у масштабуванні мереж. Це може включати розширення мережі, впровадження нових технологій, оптимізацію ресурсів тощо.

З кожним днем загрози кібербезпеки стають все складнішими. Компанії та організації повинні постійно підтримувати високий рівень захисту від кібератак, використовуючи сучасні методи шифрування, віддалені відновлення, системи виявлення вторгнень та інші заходи.

З більшим обсягом даних приходить і більший обсяг трафіку. Ефективне керування трафіком є ключовим для забезпечення високої швидкості передачі даних та надійності мережі.

Важливо мати засоби для моніторингу та аналізу мережі, щоб вчасно виявляти проблеми, прогнозувати їх і вживати відповідних заходів. Швидкі темпи технологічного розвитку вимагають постійного вдосконалення мереж. Інтеграція нових технологій, таких як штучний інтелект, Інтернет речей (IoT), блокчейн тощо, вимагає уважного планування та впровадження.

Загалом, керування сучасними комп'ютерними мережами потребує комплексного підходу, що включає в себе не лише технічні аспекти, а й аспекти безпеки, стратегічного планування та вдосконалення процесів.

Дослідження полягає у постійному зростанні вимог до продуктивності та ефективності комп'ютерних мереж. Найважливішими аспектами є забезпечення стабільної роботи мережі, оптимізація трафіку даних, забезпечення безпеки та моніторинг ресурсів. Розв'язання цих завдань вимагає розробки та впровадження нових методів та інструментів управління комп'ютерними мережами.

Дослідження показало, що використання алгоритмів оптимізації трафіку, інтелектуальних систем та SDN може значно покращити якість обслуговування користувачів та зменшити ризики виникнення проблем у мережі. Аналіз порівняння ефективності розроблених методів з існуючими показав переваги нових підходів у багатьох аспектах, зокрема в швидкодії передачі даних, масштабованості та зниженні витрат на управління мережею.

КЛЮЧОВІ СЛОВА: КОМП’ЮТЕРНІ МЕРЕЖІ, ТРАФІК, ТЕХНОЛОГІЇ SOFTWARE-DEFINED NETWORKING (SDN), МОДЕЛЬ, МАРШРУТИЗАТОР, КОМУТАТОР.

ЗМІСТ

ВСТУП
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ КОМП'ЮТЕРНИМИ МЕРЕЖАМИ ……..…….……..12
1.1 Огляд сучасних методів управління комп'ютерними мережами ……12
1.2 Аналіз основних викликів та проблем управління мережами …….……18
1.3 Опис інструментів та технологій, використовуваних для керування мережами ……....19
РОЗДІЛ 2. ПРОБЛЕМИ ТА ВИКЛИКИ УПРАВЛІННЯ КОМП'ЮТЕРНИМИ МЕРЕЖАМИ ……...……..26
2.1 Виявлення основних проблем управління мережами, що впливають на продуктивність ……...……...26
2.2 Аналіз впливу неправильного управління на швидкодію та надійність мережі …….28
2.3 Порівняння різних стратегій управління для визначення ефективних підходів …….31
РОЗДІЛ 3. МЕТОДИ ОПТИМІЗАЦІЇ УПРАВЛІННЯ КОМП'ЮТЕРНИМИ МЕРЕЖАМИ …….……35
3.1 Використання алгоритмів та інтелектуальних систем для автоматизації управління ……..….....35
3.2 Розгляд методів оптимізації трафіку в мережі ……...36
РОЗДІЛ 4. РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ……..…...43
4.1 Розробка моделі для оптимізації управління комп'ютерними мережами……..43
4.2 Аналіз отриманих даних та порівняння ефективності нової системи з існуючими методами…….43
ВИСНОВКИ
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)…….……..52

ВСТУП

Співіснування з сучасним цифровим світом неможливе без комп'ютерних мереж. Вони відіграють критичну роль у забезпеченні зв'язку, обміні даними та доступі до ресурсів для різних організацій та користувачів. Особливо велике значення вони мають у бізнесі, освіті, науці, медицині, та інших сферах.

З розвитком технологій відбувається зростання обсягу та складності мереж, що створює значні виклики у керуванні ними. Ось деякі з цих викликів:

– з ростом обсягу даних та користувачів виникає потреба у масштабуванні мереж. Це може включати розширення мережі, впровадження нових технологій, оптимізацію ресурсів тощо;

– з кожним днем загрози кібербезпеки стають все складнішими. Компанії та організації повинні постійно підтримувати високий рівень захисту від кібератак, використовуючи сучасні методи шифрування, віддалені відновлення, системи виявлення вторгнень та інші заходи;

– з більшим обсягом даних приходить і більший обсяг трафіку. Ефективне керування трафіком є ключовим для забезпечення високої швидкості передачі даних та надійності мережі;

– у світі, де різні пристрої та системи повинні співпрацювати, стандартизація є важливою. Це допомагає уникнути проблем інтероперабельності та сприяє спільному розвитку інновацій;

– важливо мати засоби для моніторингу та аналізу мережі, щоб вчасно виявляти проблеми, прогнозувати їх і вживати відповідних заходів;

– швидкі темпи технологічного розвитку вимагають постійного вдосконалення мереж. Інтеграція нових технологій, таких як штучний інтелект, Інтернет речей (IoT), блокчейн тощо, вимагає уважного планування та впровадження.

Загалом, керування сучасними комп'ютерними мережами потребує комплексного підходу, що включає в себе не лише технічні аспекти, а й аспекти безпеки, стратегічного планування та вдосконалення процесів.

Актуальність дослідження полягає у постійному зростанні вимог до продуктивності та ефективності комп'ютерних мереж. Найважливішими аспектами є забезпечення стабільної роботи мережі, оптимізація трафіку даних, забезпечення безпеки та моніторинг ресурсів. Розв'язання цих завдань вимагає розробки та впровадження нових методів та інструментів управління комп'ютерними мережами.

Розв'язання викликів, пов'язаних з постійним зростанням вимог до продуктивності та ефективності комп'ютерних мереж, дійсно вимагає розробки та впровадження нових методів та інструментів управління:

1. SDN (Software-Defined Networking) – це підхід до мережевого управління, який відокремлює керування мережею від обчислювальної інфраструктури, дозволяючи програмному забезпеченню більш гнучко та ефективно керувати трафіком даних;

2. NFV (Network Function Virtualization) – NFV дозволяє переносити функції мережевого обладнання, такі як файрволи, маршрутизатори та балансувальники навантаження, на віртуальне середовище, що спрощує керування та зменшує витрати;

3. Intent-Based Networking (IBN) – це підхід, який дозволяє адміністраторам мережі встановлювати вимоги до мережі на рівні наміру (наприклад, безпека, продуктивність), і дозволяє мережі автоматично адаптуватися до цих вимог;

4. аналіз даних та машинне навчання – використання аналізу даних та машинного навчання для прогнозування трафіку, виявлення аномалій та оптимізації роботи мережі;

5. моніторинг та аналіз ресурсів – впровадження систем моніторингу, які дозволяють постійно відстежувати стан мережі та ресурсів, а також аналізувати ці дані для виявлення проблем та вдосконалення роботи мережі;

6. безпека мережі – розвиток новітніх методів захисту, включаючи аналіз вмісту, детекцію загроз на рівні мережі та застосування алгоритмів машинного навчання для виявлення загроз.

Розробка та впровадження таких інструментів допомагають забезпечити стабільну роботу мережі, оптимізувати трафік даних, забезпечити безпеку та ефективно використовувати ресурси.

Об'єктом дослідження є комп'ютерні мережі, а предметом - процес керування цими мережами з метою підвищення їх продуктивності.

Метою цієї роботи є розробка та реалізація методів оптимізації процесу керування комп'ютерними мережами з метою підвищення їх продуктивності та ефективності.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

– аналіз сучасного стану методів управління комп'ютерними мережами;

– розробка нових методів оптимізації процесу керування мережею;

– реалізація та випробування розроблених методів на практиці;

– оцінка ефективності запропонованих методів та порівняння їх з існуючими рішеннями.

Наукова новизна даної роботи полягає в розробці та впровадженні нових методів управління комп'ютерними мережами, що дозволяють підвищити їх продуктивність та ефективність.

Результати даного дослідження матимуть практичне значення для організацій, які використовують комп'ютерні мережі, допомагаючи їм знизити витрати та підвищити загальну продуктивність.

Очікується, що робота приведе до розробки ефективних методів управління комп'ютерними мережами, які дозволять забезпечити стабільну та продуктивну роботу мережі з мінімальними витратами ресурсів. Крім того, очікується практична перевірка та підтвердження ефективності запропонованих рішень на реальних об'єктах.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ УПРАВЛІННЯ КОМП'ЮТЕРНИМИ МЕРЕЖАМИ

1.1 Огляд сучасних методів управління комп'ютерними мережами

Комп'ютерні мережі – це системи, які об'єднують комп'ютери та інші пристрої для обміну даними та ресурсами. Вони можуть бути розгорнуті в невеликих офісах, домівках, а також великих корпораціях та інституціях. Мережі дозволяють спільно використовувати файли, принтери, Інтернет-з'єднання та інші ресурси, що полегшує співпрацю та обмін інформацією. Вони можуть бути бездротовими або провідними і можуть використовувати різні топології, такі як зірка, дерево, магістраль та інші. (рис.1.1.)[1, с.125]

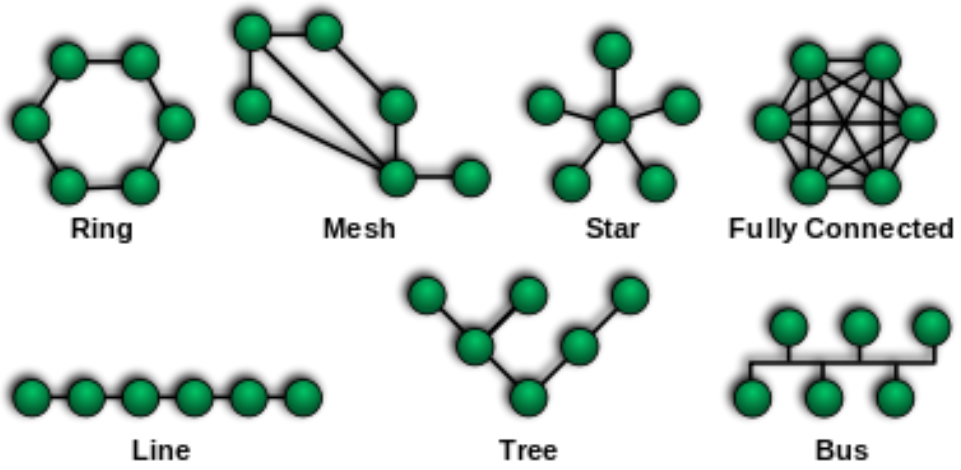


Рисунок 1.1 – Топології мереж

Топології, які можуть використовуватися в комп'ютерних мережах, включають:

– зіркова (Star) – у цій топології всі пристрої підключені безпосередньо до центрального вузла, який може бути, наприклад, комутатором або концентратором;

– дерево (Tree) – ця топологія включає в себе комбінацію зіркової топології, де кожен центральний вузол може мати підключені до нього додаткові підсистеми в зірковій або іншій топології;

– магістраль (Bus) – у цій топології всі пристрої підключені до центральної лінії, яка є спільною для всіх пристроїв;

– кільцева (Ring) – кожен вузол підключений до двох інших вузлів у вигляді кільця. Дані передаються від вузла до вузла до досягнення пункту призначення;

– меш (Mesh) – у цій топології кожен пристрій підключений безпосередньо до кожного іншого пристрою. Це може забезпечити високу надійність та забезпечити багато шляхів для передачі даних. [1, с.125]

Кожна з цих топологій має свої переваги та недоліки, і вибір конкретної залежить від потреб та вимог конкретної мережі.

Комп'ютерні мережі є невід'ємною складовою сучасного інформаційного середовища, яке забезпечує зв'язок та обмін даними між користувачами та системами.

Існує два види комп’ютерних мереж: локальна та глобальна мережі.

Локальні мережі (LAN) є мережами, де інформація передається на невеликі відстані. Вони зазвичай об'єднують комп'ютери, які розташовані недалеко один від одного, зазвичай в межах одного будівля або підприємства.

Основні характеристики локальних мереж включають:

1. *висока швидкість передачі даних.* Використовуються високошвидкісні канали передачі даних, де швидкість передачі приблизно така сама, як швидкість внутрішньої шини комп'ютера. Це дозволяє ефективно передавати великі об'єми даних;

2. *малі відстані.* Локальні мережі покривають невеликі території, зазвичай до декількох сотень метрів або кількох кілометрів, що дозволяє забезпечити низьку затримку та високу пропускну здатність;

3. *простота налаштування та адміністрування.* Локальні мережі мають просту топологію та зазвичай використовують стандартизоване обладнання, що

спрощує процес їх налаштування та адміністрування;

4. *висока надійність.* Зазвичай, через обмежену площу та розташування комп'ютерів поруч один з одним, локальні мережі мають високу надійність та менше схильність до збоїв.

Локальні мережі забезпечують ефективну спільну роботу комп'ютерів, ресурсів та послуг всередині обмеженої території, що робить їх основою для багатьох офісних, підприємницьких та особистих мереж.

Глобальні мережі (Wide Area Network або WAN) є мережами, які покривають великі географічні області, такі як країни, континенти або навіть весь світ. [1, с.125]

Основні характеристики глобальних мереж включають:

1. *великі відстані.* Глобальні мережі охоплюють великі географічні області, іноді маючи тисячі або навіть мільйони кілометрів в розпорядженні. Це дозволяє підключати користувачів та пристрої, розташовані на великих відстанях один від одного;

2. *висока пропускна здатність.* Глобальні мережі зазвичай мають високу пропускну здатність, щоб забезпечити ефективну передачу великих об'ємів даних між різними місцями;

3. *використання різноманітних технологій.* Для забезпечення зв'язку на великі відстані у глобальних мережах можуть використовуватися різні технології, такі як оптоволокно, супутникові зв'язки, мережі мобільного зв'язку тощо;

4. *важливість мережевої безпеки.* Зважаючи на розподілену природу глобальних мереж та їх підключення до різних мережевих підприємств та організацій, безпека стає важливою складовою глобального мережевого управління;

5. *складна топологія та архітектура.* Глобальні мережі можуть мати складну топологію та архітектуру, що включає різноманітні елементи, такі як маршрутизатори, комутатори, пристрої управління трафіком та інші. [3, с.42-49]

Глобальні мережі використовуються для забезпечення зв'язку між різними географічними регіонами, організаціями та користувачами по всьому світу. Вони

є основою для Інтернету та інших глобальних комунікаційних систем, що забезпечують обмін даними та доступ до різноманітних інформаційних ресурсів.

Управління комп'ютерними мережами - це процес планування, моніторингу, налаштування, управління ресурсами та забезпечення безпеки мережевого середовища з метою забезпечення ефективної та безперебійної роботи мережі. Для досягнення цієї мети розроблено різноманітні методи та підходи. Розглянемо основні з них: [3, с.42-49]

1. SNMP (Simple Network Management Protocol). Це один з найпоширеніших протоколів для управління мережею. Він дозволяє моніторити та керувати мережевими пристроями, такими як маршрутизатори, комутатори, сервери тощо. SNMP дозволяє віддалено зчитувати значення параметрів пристроїв та виконувати дії для керування ними;(рис.1.2.)

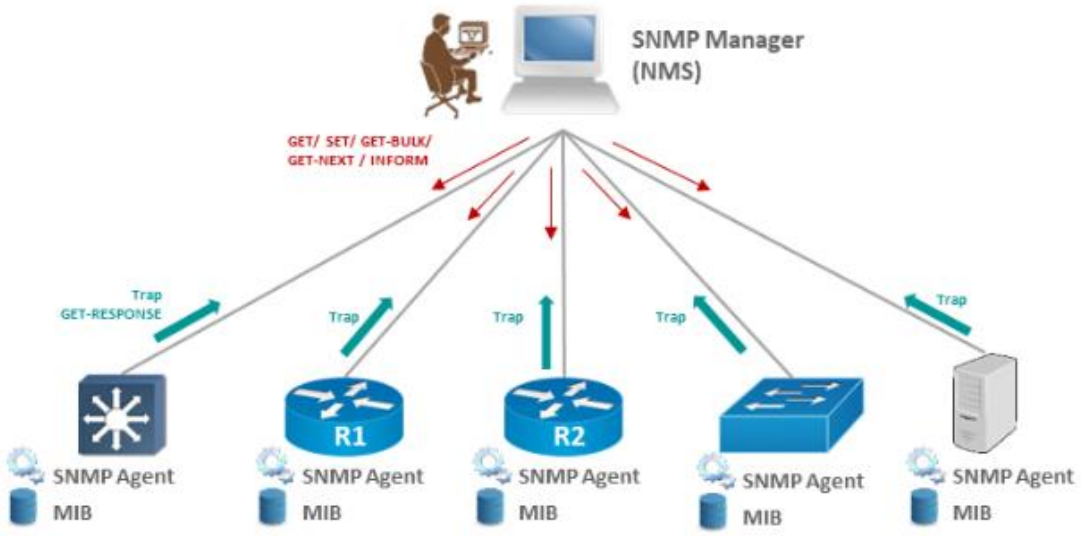


Рисунок 1.2. – SNMP (Simple Network Management Protocol)

2. NetFlow/ IPFIX (Internet Protocol Flow Information Export). Ці протоколи використовуються для збору, моніторингу та аналізу мережевого трафіку. Вони дозволяють отримувати інформацію про обсяг трафіку, джерела та призначення пакетів, що проходять через мережу, що дозволяє адміністраторам виявляти проблеми та оптимізувати використання ресурсів;(рис.1.3.) [3, с.42-49]

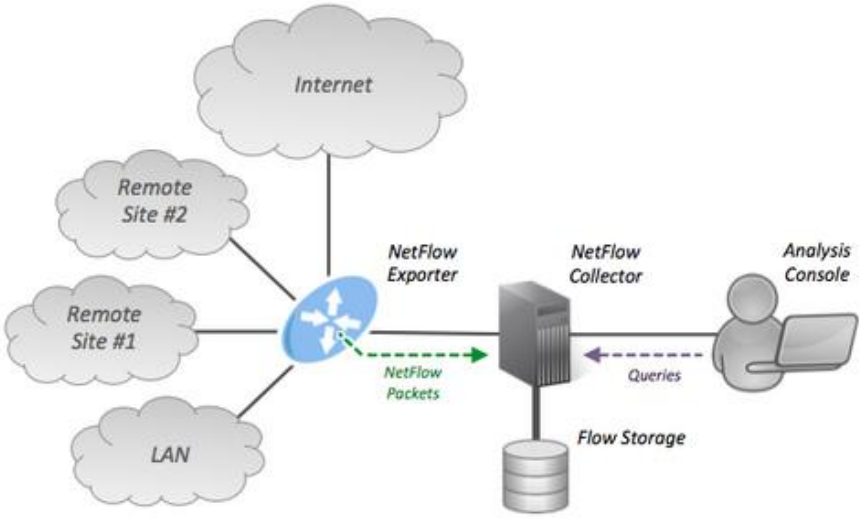


Рисунок 1.3. – NetFlow/ IPFIX (Internet Protocol Flow Information Export)

3. SDN (Software-Defined Networking). Цей підхід розділяє контрольний план та план для пересилання мережі, що дозволяє адміністраторам керувати мережевим трафіком та ресурсами централізовано за допомогою програмного забезпечення. SDN надає гнучкість та швидкість управління мережею;(рис.1.4.) [3, с.42-49]

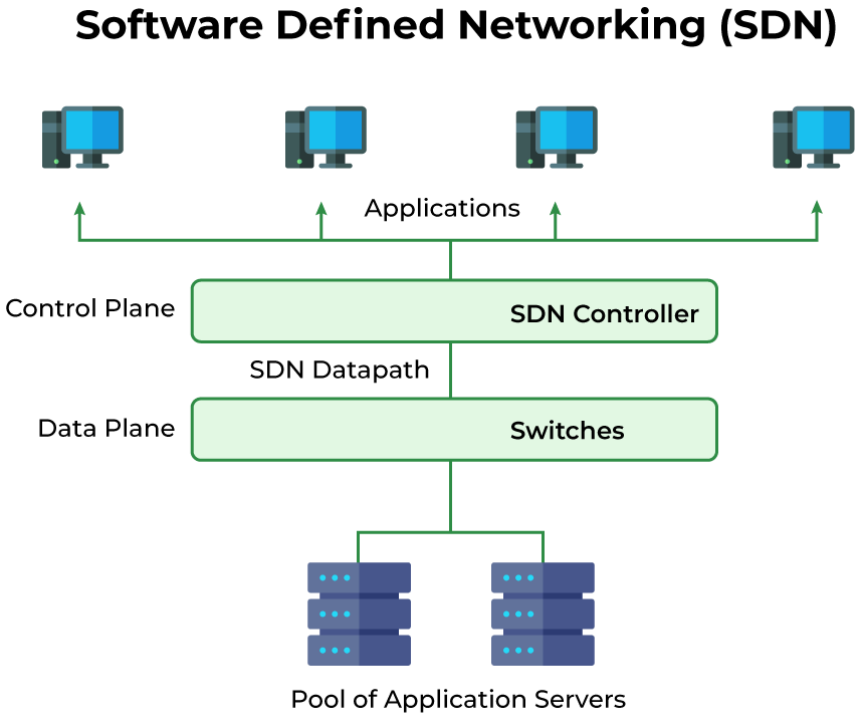


Рисунок 1.4. – SDN (Software-Defined Networking)

4. Intent-Based Networking (IBN). Цей підхід базується на заданні бізнес-цілей та потреб користувачів, після чого мережеве обладнання автоматично налаштовується та оптимізується для досягнення цих цілей. IBN дозволяє автоматизувати багато процесів управління мережею, зменшуючи трудомісткість та ймовірність помилок;(рис.1.5.) [5, с.94-96]

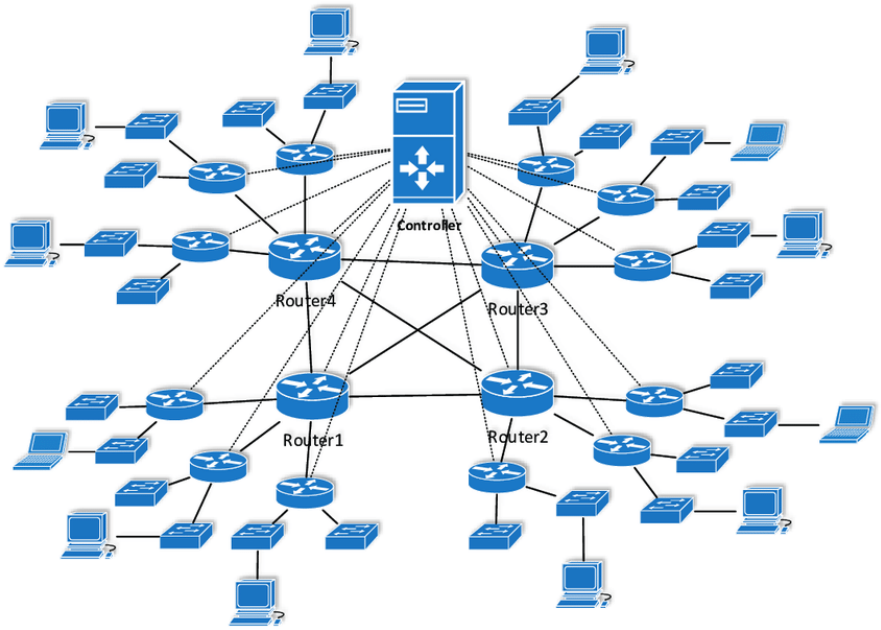


Рисунок 1.5. – Intent-Based Networking (IBN)

5. NaaS (Network as a Service). Цей підхід передбачає надання мережевих послуг через хмарні ресурси. Користувачам надається можливість орендувати мережеві ресурси та послуги за потреби, що дозволяє зменшити витрати на обладнання та підтримку мережі.(рис.1.6.) [5, с.94-96]

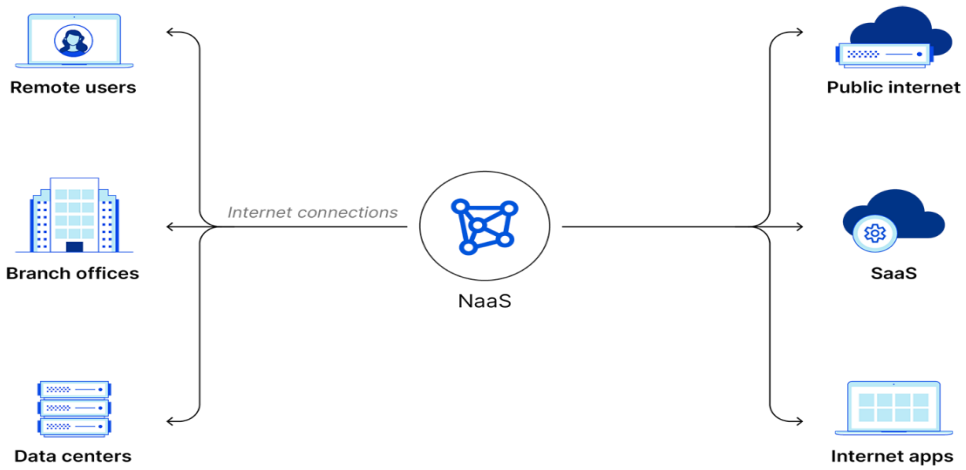


Рисунок 1.6. – NaaS (Network as a Service)

Ці методи представляють лише частину різноманітних підходів до управління комп'ютерними мережами. Вибір конкретних методів залежить від потреб конкретної організації, її інфраструктури та бізнес-вимог. [5, с.94-96]

1.2 Аналіз основних викликів та проблем управління мережами

В сучасному цифровому світі комп'ютерні мережі є невід'ємною складовою інфраструктури для бізнесу, освіти та комунікації. Проте управління цими мережами постійно стикається з різноманітними викликами та проблемами. Проведемо аналіз основних аспектів управління комп'ютерними мережами з метою ідентифікації ключових проблем та пошуку ефективних рішень для їх вирішення. Розглядаються такі аспекти, як складність мережових інфраструктур, безпека, масштабованість, інтеграція нових технологій, відмовостійкість та доступність, а також моніторинг і аналіз стану мережі. Результати цього дослідження можуть сприяти розробці ефективних стратегій управління мережами та забезпеченню їх стабільної та безперебійної роботи. [10]

Зважаючи на важливість кожного з викликів управління комп'ютерними мережами, проаналізуємо кожен із них більш детально:

– *складність і розманітність.* Різноманітність та складність комп'ютерних мереж постійно зростає з розвитком технологій. Адміністраторам мереж потрібно бути особливо уважними до конфігурації та взаємозв'язків між різними компонентами мережі. Це може стати проблемою при впровадженні нових технологій або розширенні існуючих мереж; [10]

– *безпека і захист.* Забезпечення безпеки мережі вимагає постійного моніторингу та застосування заходів захисту. З урахуванням постійної еволюції загроз, адміністраторам потрібно бути завжди в курсі останніх тенденцій у сфері кібербезпеки та мати стратегії для захисту мережі від нових загроз; [10]

– *масштабованість*. Із зростанням кількості пристроїв і користувачів у мережі виникає необхідність управління цим ростом, щоб забезпечити ефективне використання ресурсів та уникнути перевантажень. Розробка масштабованих стратегій управління є важливим аспектом забезпечення стабільної роботи мережі; [10]

– *інтеграція нових технологій.* Впровадження нових технологій може призвести до складнощів у їх інтеграції з існуючими мережевими інфраструктурами. Адміністраторам потрібно мати глибокі знання нових технологій та стратегії для безпечного та ефективного їх впровадження;[10]

– *безперервність і доступність.* Забезпечення неперервної роботи мережі є ключовою вимогою. Адміністраторам потрібно розробляти стратегії безперервності в роботі та швидкої відновлюваності в разі виникнення непередбачуваних ситуацій або відмов; [10]

– *моніторинг і аналіз.* Ефективний моніторинг і аналіз стану мережі дозволяють виявляти проблеми та вчасно реагувати на них. Це вимагає використання спеціальних інструментів та систем, а також навичок аналізу даних для виявлення та вирішення проблем. [10]

Ці виклики потребують постійної уваги та розробки ефективних стратегій для їх вирішення. Вироблення таких стратегій дозволить забезпечити стабільну та ефективну роботу комп'ютерних мереж у будь-яких умовах.

1.3 Опис інструментів та технологій, використовуваних для керування мережами

Керування мережами включає в себе використання різноманітних інструментів та технологій для ефективного управління та моніторингу мережевих ресурсів, забезпечення безпеки та вирішення проблем.

Розглянемо детальний опис деяких з них:

1. системи моніторингу мережі – ці системи дозволяють збирати та аналізувати дані про стан мережі, включаючи трафік, пропускну здатність, використання ресурсів, підключення та стан пристроїв. Популярні засоби моніторингу включають Nagios, Zabbix, PRTG Network Monitor, SolarWinds, Cisco Prime, і т.д.; [15]

2. програмне забезпечення для керування конфігурацією - це програми, які допомагають в управлінні конфігурацією мережевих пристроїв, таких як комутатори, маршрутизатори, файрволи тощо. Вони забезпечують централізований доступ до конфігураційних файлів, автоматизовані процеси конфігурації та можливість резервного копіювання конфігурацій. Приклади включають Cisco Prime Infrastructure, SolarWinds Network Configuration Manager, Ansible, Puppet, Chef тощо; [15]

3. програмне забезпечення моніторингу безпеки - ці інструменти призначені для виявлення та запобігання загрозам безпеки в мережі. Вони включають в себе системи виявлення вторгнень (IDS), системи запобігання вторгненням (IPS), файерволи, антивірусне програмне забезпечення, системи аудиту безпеки тощо. Приклади таких систем: Cisco Firepower, Snort, Suricata, Palo Alto Networks, Symantec, McAfee, Fortinet тощо;

4. системи управління багатомісцевим доступом (MDM) - ці системи використовуються для управління доступом користувачів до мережевих ресурсів та пристроїв, включаючи мобільні телефони, планшети та інші пристрої з підтримкою мобільного зв'язку. Вони дозволяють централізовано налаштовувати політики безпеки, моніторити та керувати пристроями, виконувати віддалене видалення даних тощо. Приклади включають MobileIron, VMware AirWatch, Microsoft Intune, Cisco Meraki тощо; [15]

5. системи управління віртуалізацією мережі – ці системи дозволяють управляти віртуальними мережевими ресурсами, включаючи віртуальні машини, віртуальні мережеві комутатори, маршрутизатори та файрволи. Вони забезпечують можливість розгортання, конфігурації та моніторингу віртуальних мережевих ресурсів. Приклади таких систем: VMware NSX, Cisco ACI, Juniper

Contrail, OpenStack тощо; [15]

6. системи управління багатошаровими мережами (SDN) - ці системи дозволяють централізовано управляти всією мережею через програмне забезпечення, використовуючи відокремлення керування від обробки даних. Вони надають можливість автоматизованого розгортання, конфігурації та управління мережевими ресурсами, що спрощує роботу адміністраторів мережі та забезпечує більшу гнучкість та швидкість відгуку мережі. Приклади включають Cisco ACI, VMware NSX, OpenFlow, Juniper Contrail тощо. [15]

Описані вище інструменти та технології допомагають управляти складними мережами та забезпечують їх ефективне функціонування, безпеку та гнучкість. Використання правильних інструментів може покращити продуктивність мережі, знизити витрати на управління та забезпечити високий рівень надійності та безпеки.

Для підключення комп'ютерів до мережі використовуються різні мережеві пристрої та технічні засоби.

Основні компоненти локальних мереж включають:

– *мережеві контролери (адаптери).* Ці пристрої забезпечують взаємодію робочих станцій з мережевим середовищем. Вони перетворюють дані з внутрішньої шини комп'ютера у формат, який може бути переданий по мережі, та обертають отримані дані в пакети для передачі через кабель; [4]

– *кабелі для з'єднання.* Для підключення мережевих компонентів використовуються різні типи кабелів. Серед них коаксіальний кабель, скручена пара напівпровідників та оптоволоконний кабель. Кожен з цих типів кабелів має свої особливості щодо максимальної швидкості передачі даних та максимальної відстані зв'язку;

– *роз'єми та розгалужувачі.* Для підключення кабелів до мережевих пристроїв використовуються роз'єми, які можуть мати різні типи та стандарти, наприклад, RJ-45 для скрученої пари;

– *мережеві комутатори та концентратори.* Ці пристрої використовуються для забезпечення з'єднання між різними пристроями у мережі.

Комутатори дозволяють передавати дані між різними портами залежно від адреси призначення, тоді як концентратори просто повторюють сигнал на всі порти; [4]

– *маршрутизатори*. Ці пристрої використовуються для маршрутизації даних між різними мережами та забезпечення шляху для передачі даних від джерела до призначення;

– *медіаконвертери*. Ці пристрої дозволяють перетворювати сигнали між різними типами кабелів або між кабелем та оптоволокном. Ці технічні засоби допомагають створювати надійні та ефективні локальні мережі, які забезпечують швидку та надійну комунікацію між комп'ютерами та іншими мережевими пристроями.(рис.1.7.) [4]

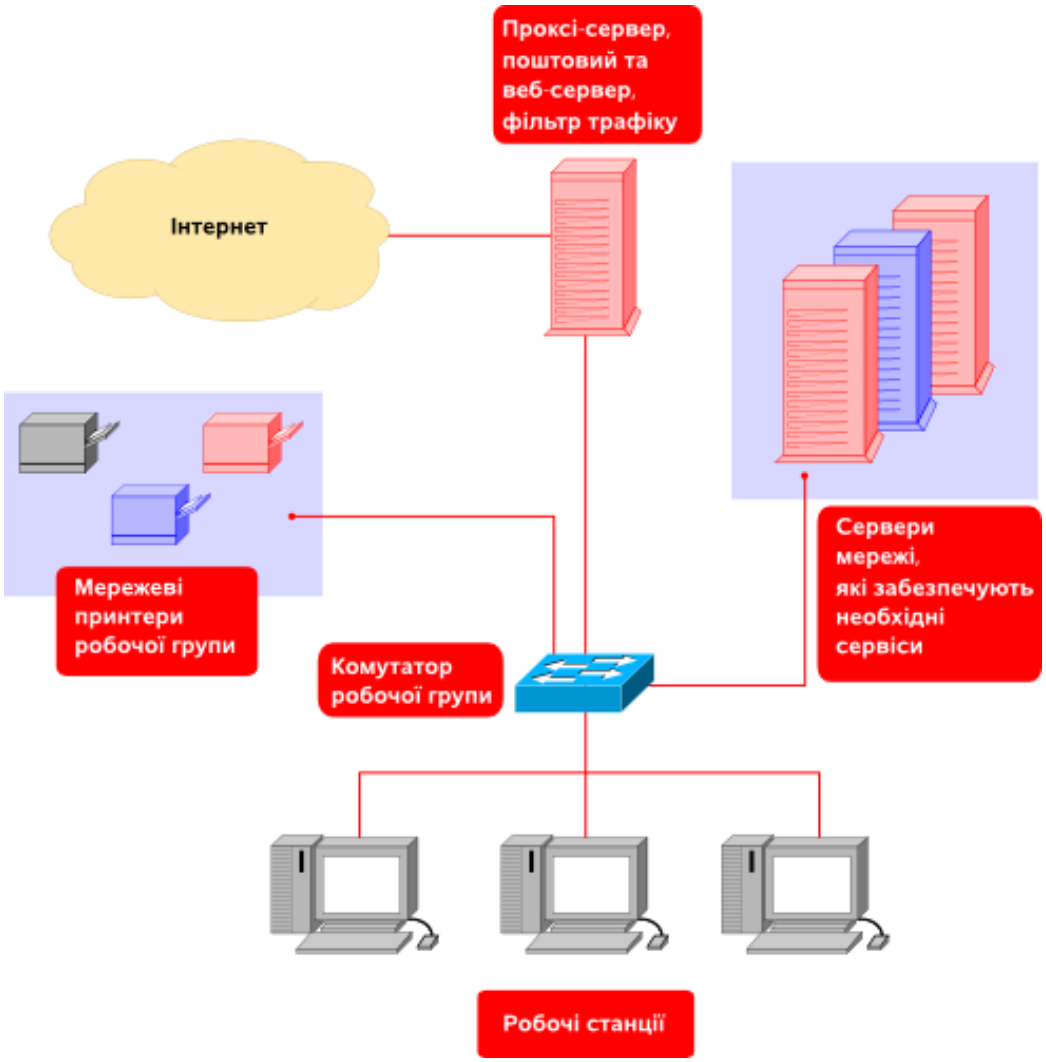


Рисунок 1.7. – Складові локальної мережі

Мережеві пристрої глобальних мереж включають різноманітні засоби та технології, які забезпечують з'єднання між комп'ютерами та іншими пристроями по всьому світу.

Основні компоненти глобальних мереж включають:

– *модеми.* Ці пристрої використовуються для з'єднання з телефонними каналами зв'язку. Модеми перетворюють цифрові сигнали, що використовуються комп'ютерами, на аналогові сигнали, що можуть бути передані по телефонних лініях, а також навпаки. Вони можуть використовувати різні методи модуляції, такі як амплітудна, частотна та фазова модуляція, а також різні методи передачі, такі як асинхронний та синхронний; [4]

– *мережеві комутатори та концентратори.* Ці пристрої використовуються для забезпечення з'єднання між різними пристроями у глобальній мережі. Вони дозволяють передавати дані між різними мережевими пристроями, такими як комп'ютери, сервери та інші пристрої;

– *маршрутизатори.* Ці пристрої використовуються для маршрутизації даних між різними мережами, які можуть мати різні технології та протоколи. Вони визначають оптимальний маршрут для передачі даних між джерелом та призначенням; [4]

– *шлюзи.* Ці пристрої використовуються для з'єднання локальних та глобальних мереж, які можуть використовувати різні протоколи та технології. Шлюзи перетворюють дані з одного формату на інший, щоб забезпечити сумісність між різними мережами;

– *сервери та робочі станції.* Сервери надають ресурси для загального користування абонентам мережі, включаючи файлові сервери, сервери друкування та інші. Робочі станції використовують ці ресурси для виконання різних завдань та отримання доступу до мережевих послуг. [4]

Усі ці пристрої та компоненти допомагають створювати глобальні мережі, які забезпечують ефективну комунікацію та обмін даними по всьому світу. Глобальні мережі використовуються для з'єднання користувачів та ресурсів з різних куточків планети та є важливим інструментом для спілкування, комерції та

обміну інформацією.(рис.1.8.)

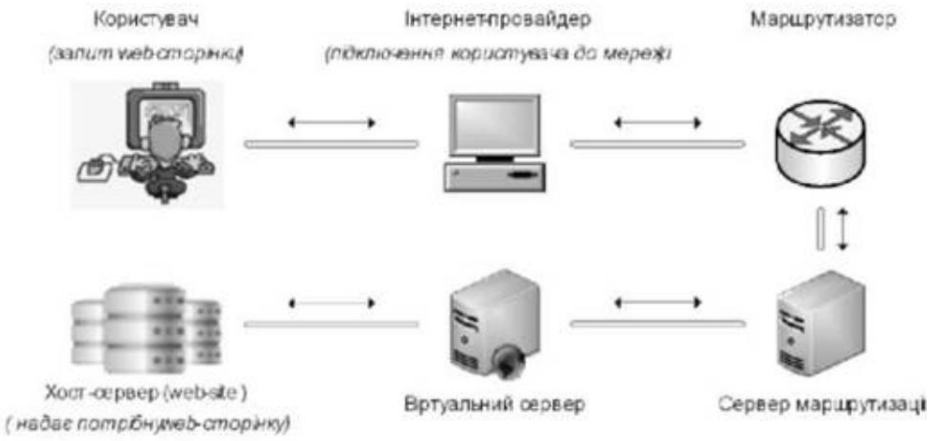


Рисунок 1.8. – Схема функціонування мережі Інтернет

Ця різноманітна інфраструктура мереж і кінцевого обладнання буде здатна підтримувати широкий спектр програм, які відповідатимуть потребам різних користувачів, від малих спеціалізованих груп до масового користування. Ці програми включатимуть в себе віддалені суперкомп'ютерні програми, що вимагають високої пропускної здатності, а також загальнодоступні послуги, такі як телефонія, електронна пошта, відеоконференції, потокове відео, розваги та електронна комерція. [8, с.36-45]

У цьому процесі розробки та впровадження глобальної мультимедійної мережі братимуть участь компанії та організації з різних галузей, включаючи програмне забезпечення, напівпровідники, комп'ютери, телекомунікації та постачальників контенту. Це вимагатиме співпраці десятків стандартних органів та сотень постачальників обладнання та програмного забезпечення.

Для користувачів важливо, щоб їх програми працювали безперебійно по всій мережевій інфраструктурі, а також мали можливість масштабуватись та налаштовуватись згідно з потребами та технологічними можливостями. Користувачі можуть мати різні вимоги до мережі, включаючи обмеження програм на частину мережі або на обладнання певного постачальника.

Більшість зацікавлених сторін, включаючи користувачів, провайдерів послуг, постачальників контенту та постачальників обладнання, будуть працювати на створення гнучкої та динамічної мережі, яка може забезпечувати масштабування та

розвиток для виконання будь-яких завдань та розміщення нових, непередбачуваних додатків без значних вкладень і дислокацій. [11, с.16]

РОЗДІЛ 2. ПРОБЛЕМИ ТА ВИКЛИКИ УПРАВЛІННЯ КОМП'ЮТЕРНИМИ МЕРЕЖАМИ

2.1 Виявлення основних проблем управління мережами, що впливають на продуктивність

Виявлення основних проблем управління мережами, які впливають на продуктивність, є ключовим етапом для покращення ефективності мережевого середовища.

Ось деякі з найбільш поширених проблем та приклади їх вирішення:

1. недостатній моніторинг та аналіз мережі. Брак достатньої системи моніторингу та аналізу мережі може призвести до недооцінки пропускної здатності, перевантаження мережі та збоїв. Необхідно мати систему, яка надає детальну інформацію про трафік, використання ресурсів та стан пристроїв;

Приклад вирішення даної проблеми:

– встановлення систем моніторингу, таких як Nagios, Zabbix або PRTG, які надають детальну інформацію про стан мережі, трафік, доступність пристроїв тощо;

– використання аналітичних інструментів, таких як Wireshark або SolarWinds, для аналізу мережевого трафіку та виявлення аномалій.

2. недостатня безпека мережі. Нестача належних заходів безпеки може призвести до злому мережі, втрати конфіденційності даних та порушення нормативних вимог. Необхідно вжити заходів для захисту мережі, включаючи використання файерволів, систем виявлення вторгнень та шифрування даних; [13, с.47]

Приклад вирішення даної проблеми.

– встановлення файерволів та систем виявлення вторгнень (IDS/IPS) для захисту мережі від небажаних доступів й атак;

– використання VPN для захищеного з'єднання та шифрування комунікацій.

3. нестабільність мережевих пристроїв. Неправильна конфігурація та управління мережевими пристроями може призвести до їх збоїв та недоступності. Важливо мати систему для моніторингу та управління конфігураціями пристроїв та автоматизації процесів оновлення та налаштування; [13, с.47]

Приклад вирішення даної проблеми.

– використання інструментів автоматизації конфігурації, таких як Ansible або Puppet, для управління конфігураціями пристроїв у мережі;

– встановлення систем управління конфігурацією, таких як Cisco Prime або SolarWinds Network Configuration Manager, для централізованого керування конфігураціями пристроїв.

4. несумісність та конфлікти програмного забезпечення. Використання різноманітних програмних продуктів може призвести до конфліктів та несумісності, що може вплинути на стабільність та продуктивність мережі. Необхідно вивчати сумісність програмного забезпечення та використовувати стандартизовані рішення; [13, с.47]

Приклад вирішення даної проблеми.

– використання віртуалізації для ізоляції програмних середовищ та запобігання конфліктам між різними програмами;

– встановлення стандартизованих наборів програмного забезпечення та використання тестових середовищ для валідації сумісності.

5. недостатня масштабованість та гнучкість. Мережі повинні бути готові до масштабування та адаптації до змін у вимогах та технологіях. Необхідно розробляти мережеві архітектури, які дозволяють легко розширювати та змінювати конфігурації;

Приклад вирішення даної проблеми:

– використання облікових областей та віртуалізації мережі для забезпечення гнучкості та легкості масштабування;

– впровадження SDN (Software-Defined Networking) для автоматизації та

централізованого управління мережею.

6. недостатній резервний забезпечення та відновлення після збоїв. Брак належної стратегії резервного забезпечення та відновлення може призвести до тривалих перерв у роботі мережі та втрати даних. Важливо розробити плани резервного копіювання даних та відновлення систем.

Приклад вирішення даної проблеми.

– регулярні резервні копії даних на віддалених серверах або в хмарних сервісах;

– використання систем відновлення даних та відновлення мережевих пристроїв з резервних копій у разі виявлення збоїв.

Вирішення цих проблем вимагає комплексного підходу та використання сучасних інструментів та технологій управління мережами. При правильному управлінні можна покращити продуктивність мережі, забезпечити її безпеку та стабільність, що сприятиме успішній роботі організації. [13, с.47]

Загальні проблеми управління мережами можна вирішувати за допомогою різноманітних інструментів та технологій. Ось конкретні приклади рішень для кожної з наведених проблем:

2.2 Аналіз впливу неправильного управління на швидкодію та надійність мережі

Неправильне управління мережею може серйозно вплинути на її швидкодію та надійність. Наприклад, недостатній моніторинг та аналіз мережі може призвести до невчасного виявлення проблем, таких як перевантаження каналів зв'язку або несправності пристроїв, що може призвести до падіння продуктивності та недоступності сервісів для користувачів. Недостатня безпека мережі може відкрити двері для злому та неправомірного доступу до даних, що може відобразитися на їх конфіденційності та цілісності. Крім того, недостатня

гнучкість та масштабованість мережі можуть ускладнити її адаптацію до змін у вимогах бізнесу або технологій, що може призвести до затримок у впровадженні нових послуг або функцій. Нарешті, неправильне резервне забезпечення та відновлення після збоїв може призвести до втрати даних та тривалих перерв у роботі мережі, що значно вплине на її надійність та доступність. У цілому, неправильне управління мережею може мати серйозний вплив на її ефективність та функціональність, що негативно відобразиться на роботі організації та задоволенні потреб користувачів. [17]

Неправильне управління мережею може мати різноманітні наслідки, які прямо впливають на швидкодію та надійність мережевої інфраструктури. Ось деякі конкретні аспекти, які варто врахувати:

– перевантаження мережі – недостатнє моніторингове покриття та аналіз мережі можуть призвести до недооцінки трафіку та його розподілу. Це може призвести до перевантаження мережевих каналів, що в свою чергу призведе до зниження швидкості передачі даних та погіршення продуктивності користувачів;

– несправність пристроїв та комунікацій – недоліки у моніторингу стану пристроїв та комунікаційних ліній можуть призвести до ігнорування потенційних проблем, таких як перегрів, переривання живлення або втрати пакетів даних. Це може спричинити непередбачувані збої та перебої у роботі мережі;

– нестабільність безпеки – відсутність адекватних заходів забезпечення безпеки може призвести до ризику несанкціонованого доступу до мережевих ресурсів, злому даних або втрати конфіденційності. Це може призвести до серйозних наслідків для організації, включаючи втрату довіри користувачів та репутації компанії;

– недостатня гнучкість та масштабованість – неправильне планування та розгортання мережі може призвести до обмежень її гнучкості та масштабованості. Наприклад, недостатня кількість доступних IP-адрес або обмежена пропускна спроможність каналів зв'язку можуть ускладнити розширення мережі або впровадження нових технологій;

– недооцінка ризиків та відновлення після збоїв – відсутність ефективного

плану резервного забезпечення та відновлення може призвести до великих затримок у відновленні роботи мережі після збоїв або катастроф. Наприклад, відсутність резервних копій даних може призвести до їх втрати, що має серйозні наслідки для бізнес-процесів організації. [20]

Усі ці аспекти демонструють, як неправильне управління мережею може призвести до серйозних проблем, що впливають на її швидкодію та надійність. Для запобігання таким ситуаціям необхідно використовувати комплексний підхід до управління мережею, що включає в себе моніторинг, аналіз, планування та ефективне впровадження заходів безпеки та резервного забезпечення.

Один з конкретних прикладів вирішення проблеми перевантаження мережі може бути використання QoS (Quality of Service) або управління якістю обслуговування. QoS дозволяє пріоритизувати різні види трафіку в мережі залежно від їх важливості, надаючи пріоритет тим даним, які вимагають найбільшої швидкості та найменшої затримки. [23]

Наприклад, важливі для бізнесу додатки, такі як голосова чи відеоконференції, можуть бути пріоритетно оброблені перед менш критичними завданнями, такими як електронна пошта або скачування файлів. Це дозволяє забезпечити найкращу продуктивність для користувачів у ситуаціях, коли мережа перевантажена, допомагаючи знизити затримки та покращити якість обслуговування. [16]

Інший приклад вирішення проблеми безпеки мережі може бути використання системи моніторингу виявлення вторгнень (Intrusion Detection System, IDS) або системи захисту від вторгнень (Intrusion Prevention System, IPS). Ці системи автоматично аналізують мережевий трафік на предмет потенційно небезпечних або аномальних активностей, таких як спроби несанкціонованого доступу або атаки злому. Вони можуть виявити та заблокувати такі загрози до мережі, забезпечуючи високий рівень захисту від кібератак. [19]

Ці приклади демонструють, як використання відповідних технологій та інструментів управління мережею може допомогти вирішити конкретні проблеми та покращити її продуктивність та безпеку.

2.3 Порівняння різних стратегій управління для визначення ефективних підходів

Порівняльний аналіз різних стратегій управління мережею може допомогти визначити ефективні підходи, які найкраще відповідають конкретним потребам та вимогам організації. Ось деякі загальні стратегії управління мережею та їх порівняльний аналіз:

1. централізоване управління;

– Переваги – централізоване управління може спростити координацію та контроль над мережею, забезпечуючи єдиний центр прийняття рішень та моніторингу.

– Недоліки – централізований підхід може бути менш гнучким та витратним з точки зору масштабування та адаптації до змін у мережевому середовищі.

Наприклад. Одним з прикладів централізованого управління може бути використання Security Information and Event Management (SIEM) системи. SIEM централізує та аналізує дані з різних джерел у мережі, таких як файрволи, системи виявлення вторгнень (IDS), системи захисту від вторгнень (IPS), журнали подій та інші. Це дозволяє операторам централізовано аналізувати та реагувати на потенційні загрози з одного централізованого інтерфейсу. [25]

2. децентралізоване управління;

– Переваги – децентралізоване управління дозволяє різним групам адміністраторів приймати рішення та керувати своїми власними частинами мережі, що може бути корисним у великих організаціях або у складних мережевих топологіях.

– Недоліки – однак це може призвести до розпаду координації та консистентності управління, а також до виникнення конфліктів між різними адміністраторськими групами.

Наприклад. Децентралізоване управління може бути використане у випадку, коли організація має різні підрозділи з власними мережами та адміністраторами. Кожний підрозділ може мати свої власні інструменти та методи управління мережею, що найкраще відповідають його потребам та вимогам. [29]

3. автоматизоване управління;

– Переваги – використання автоматизованих інструментів та технологій, таких як SDN (Software-Defined Networking) або інтелектуальні системи управління, може значно полегшити та прискорити процеси управління, зменшуючи ручну працезатратність та ризик помилок.

– Недоліки – проте, впровадження автоматизованих систем може вимагати значних інвестицій у технології та перепідготовку персоналу, а також може виникнути проблеми з безпекою та приватністю даних.

– Наприклад. Використання автоматизованих інструментів, таких як системи SDN, які можуть динамічно керувати політиками безпеки мережі на основі змінних умов та загроз. Наприклад, SDN може автоматично блокувати атаки DDoS або виявляти та блокувати небезпечні трафікові шаблони. [9]

4. аналітика та моніторинг;

– Переваги – використання аналітики та моніторингу дозволяє здійснювати постійне відстеження стану мережі та ідентифікувати можливі проблеми або вузькі місця.

– Недоліки – однак це може вимагати значних обсягів даних та аналітичних ресурсів, а також може бути важко інтегрувати з існуючими системами управління.

Кожна з цих стратегій має свої переваги та недоліки, і вибір оптимального підходу залежить від конкретних потреб та характеристик мережі кожної організації. Часто ефективне управління мережею вимагає комбінації різних стратегій та технологій. [11]

Розглянемо використання стратегій управління для певних дій.

Моніторинг ресурсів мережі:

– централізоване управління – використання централізованих систем

моніторингу, які забезпечують повний огляд стану мережі з єдиного інтерфейсу;

– децентралізоване управління – розподілені системи моніторингу, кожна з яких відповідає за моніторинг конкретного сегменту мережі або місцевого підрозділу;

– автоматизоване управління – використання інтелектуальних систем аналітики даних, які автоматично виявляють аномалії та прогнозують можливі проблеми в мережі. [21]

Управління політикою безпеки:

– централізоване управління – застосування централізованих систем управління політикою безпеки, які забезпечують єдиний контроль та координацію політик безпеки для всієї мережі;

– децентралізоване управління – кожен підрозділ або відділ відповідає за розробку та впровадження власних політик безпеки, які відповідають їхнім унікальним вимогам та ризикам;

– автоматизоване управління – використання автоматизованих систем, які автоматично адаптують політику безпеки на основі аналізу змін в мережевому середовищі та виявлених загроз.

Управління трафіком мережі:

– централізоване управління – використання централізованих систем керування трафіком, які забезпечують глобальний контроль та оптимізацію пропускної здатності мережі;

– децентралізоване управління - локальні системи керування трафіком, які керують трафіком в окремих сегментах мережі відповідно до специфічних вимог та потреб користувачів;

– автоматизоване управління - використання інтелектуальних систем, які автоматично адаптують маршрутизацію та керують трафіком для оптимізації продуктивності та надійності мережі. [30]

Ці приклади демонструють, що різні стратегії управління можуть бути ефективними залежно від конкретних завдань та потреб організації. Вибір оптимального підходу може вимагати аналізу індивідуальних факторів, таких як

розмір мережі, географічний розподіл, безпека та інші фактори.

РОЗДІЛ 3. МЕТОДИ ОПТИМІЗАЦІЇ УПРАВЛІННЯ КОМП'ЮТЕРНИМИ МЕРЕЖАМИ

3.1 Використання алгоритмів та інтелектуальних систем для автоматизації управління

Використання алгоритмів та інтелектуальних систем для автоматизації управління мережею має великий потенціал для оптимізації її продуктивності та надійності. Ось деякі приклади застосування наведені в таблиці 3.1. [10]

Таблиця 3.1 – Алгоритми інтелектуальних систем

Динамічне керування мережевим трафіком	
Алгоритми маршрутизації	алгоритми маршрутизації можуть автоматично адаптувати мережевий трафік в залежності від поточних умов мережі, щоб забезпечити оптимальний маршрут передачі даних
QoS-алгоритми	Алгоритми забезпечення якості обслуговування можуть автоматично виявляти та пріоритизувати різні види трафіку для гарантування високої якості обслуговування для критичних додатків
Прогнозування відмов та управління ресурсами	
Системи моніторингу та аналізу	Інтелектуальні системи можуть використовувати дані моніторингу для прогнозування можливих відмов мережі або проблем з ресурсами та автоматично приймати заходи для їх усунення або попередження.

Продовження таблиці 3.1 – Алгоритми інтелектуальних систем

Прогнозування відмов та управління ресурсами	
Автоматизоване масштабування	Системи автоматизованого масштабування можуть аналізувати показники навантаження мережі та автоматично масштабувати ресурси, наприклад, додавати нові сервери або збільшувати пропускну здатність каналів, для забезпечення надійності та продуктивності.
Автоматизоване управління конфігурацією	
Системи управління конфігурацією	Інтелектуальні системи можуть автоматично виявляти та усувати конфлікти в конфігурації мережевих пристроїв, а також автоматично реагувати на зміни в мережі шляхом оновлення конфігурацій.
Прогнозування інцидентів та автоматизована реакція	
Системи прогнозування інцидентів	Інтелектуальні системи можуть аналізувати дані з різних джерел, таких як журнали подій та моніторинг мережі, для виявлення потенційних проблем та інцидентів, наприклад, атак або відмов пристроїв.
Автоматизована реакція	При виявленні потенційних проблем інтелектуальні системи можуть автоматично ініціювати відповідні заходи, такі як переключення на резервні маршрути або блокування підозрілих трафіків.

Ці приклади демонструють, як використання алгоритмів та інтелектуальних систем дозволяє автоматизувати та оптимізувати управління мережею для підвищення її продуктивності та надійності.

3.2 Розгляд методів оптимізації трафіку в мережі

При розгляді методів оптимізації трафіку в мережі, можна виокремити

кілька ключових підходів: [12, с.125-132]

– *Quality of Service (QoS).* OoS – це набір технологій та механізмів, які гарантують певний рівень якості обслуговування для різних типів трафіку в мережі. Використовуються методи приоритезації, управління пропускною здатністю, управління затримкою тощо для забезпечення найважливішим даним пріоритетного обслуговування;

– *Traffic Shaping.* Цей метод включає в себе регулювання трафіку для забезпечення більш однорідного розподілу пропускної здатності та зниження великого обсягу трафіку, який може спричиняти перевантаження мережі.

– *Compression.* Стиснення даних може зменшити обсяг трафіку в мережі, що дозволяє ефективніше використовувати доступну пропускну здатність. Різні алгоритми стиснення, такі як gzip або Deflate, можуть застосовуватися для цієї мети;

– *Caching.* Використання кешування може зменшити обсяг трафіку, який потрібно передавати між клієнтом та сервером. Інформація, яка регулярно запитується користувачами, може зберігатися локально на проміжних серверах, що дозволяє уникнути повторної передачі даних по мережі;

– *Load Balancing.* Розподіл навантаження дозволяє рівномірно розподіляти трафік між різними мережевими ресурсами, такими як сервери чи мережеві шляхи. Це допомагає запобігти перевантаженням та покращити загальну ефективність мережі;

– *Protocol Optimization.* Оптимізація протоколів передачі даних може включати у себе використання більш ефективних алгоритмів обміну даними, які зменшують затримки та споживання пропускної здатності;

– *Traffic Engineering.* Цей підхід використовується для активного управління трафіком в мережі, включаючи маршрутизацію, вибір шляхів та розподіл ресурсів для забезпечення оптимальної прохідності та надійності.

Ці методи можуть використовуватися окремо або в комбінації для досягнення оптимального керування трафіком та підвищення продуктивності мереж. [12, с.125-132]

3.3 Впровадження технологій Software-Defined Networking (SDN) для покращення управління

Software-Defined Networking (SDN) – це новий підхід до управління комп'ютерними мережами, який змінює те, як мережі створюються та керуються. Основна ідея SDN полягає у тому, щоб розділити керуючу частину мережі (control plane), яка відповідає за прийняття рішень, від передачі даних (data plane), яка відповідає за фактичну передачу інформації. Це дозволяє керувати всією мережею з одного центрального пункту за допомогою програмного забезпечення.

У звичайних мережах управління та передача даних часто відбуваються на кожному мережевому пристрої, такому як маршрутизатори та комутатори. SDN змінює цей підхід, виокремлюючи роль управління з ролі передачі даних. Це означає, що управління мережею здійснюється централізовано через програмне забезпечення, а не розподілено по всій мережі. [26]

Це революційний підхід, оскільки він дозволяє зробити мережі більш гнучкими, ефективними та легкими в управлінні. За допомогою SDN, адміністратори можуть швидше налаштовувати та реагувати на зміни в мережі, а також забезпечувати кращу безпеку та масштабованість.

Концепція програмно-конфігурованих мереж, відома як Software Defined Networking (SDN), полягає в розділенні управління мережею та передачі даних шляхом перенесення функцій управління на програмне забезпечення, що працює на централізованому контролері. У цій архітектурі мережеві елементи, такі як маршрутизатори та комутатори, виконують базові завдання передачі пакетів, тоді як управління мережею відокремлене та програмоване. Це дозволяє керувати мережею з централізованої точки, забезпечуючи більшу гнучкість та швидкість реакції на зміни в мережевих умовах. Крім того, відокремлення інфраструктури передачі даних від мережевих сервісів і додатків сприяє забезпеченню кращої масштабованості та розподілу ресурсів у мережі.(рис.3.1.) [29]

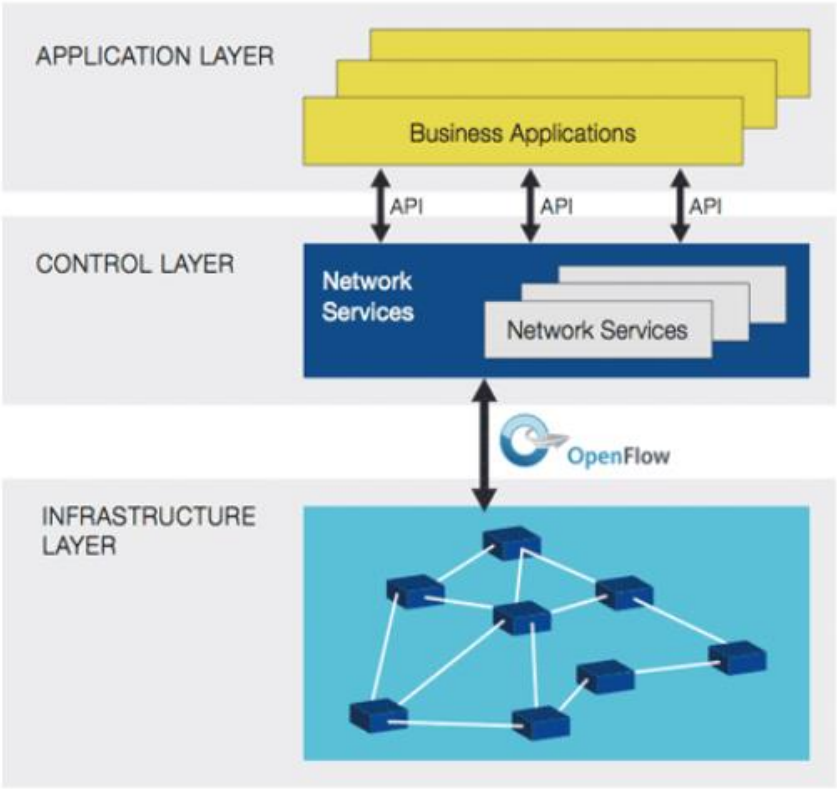


Рисунок 3.1 – Визначення SDN від Open Networking Foundation

Ідея програмно-конфігурованих мереж була сформульована фахівцями університетів Стенфорда і Берклі ще у 2006 році і відразу ж отримала широку підтримку як у наукових колах, так і серед провідних виробників мережевого обладнання. У березні 2011 року було засновано консорціум Open Networking Foundation (ONF) за участю міжнародних корпорацій, таких як Google, Deutsche Telekom, Facebook, Microsoft, Verizon та Yahoo. З того часу склад ONF значно розширився і налічує понад 90 членів, включаючи Brocade, Citrix, Oracle, Dell, Ericsson, HP, IBM, Marvell, NEC. [25]

У програмно-конфігурованих мережах віртуалізуються пристрої комутації та маршрутизації, що означає, що процес маршрутизації контролюється програмним забезпеченням. Традиційний мережевий пристрій, такий як комутатор або маршрутизатор, складається з різних компонентів.(рис.3.2.) [27]

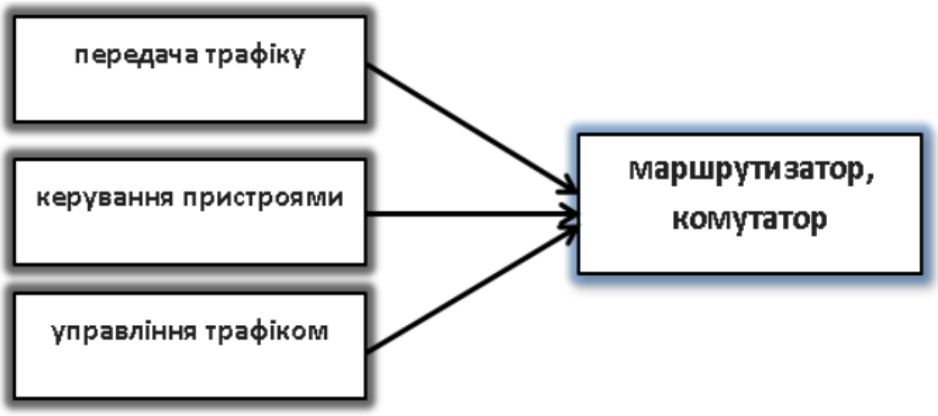


Рисунок 3.2 – Структура комутатора

Впровадження технологій Software-Defined Networking (SDN) в мережеве середовище може значно покращити управління мережею та її продуктивність:

– SDN дозволяє централізовано керувати всією мережею з одного пункту керування. Це спрощує управління мережею, дозволяючи адміністраторам здійснювати швидке реагування на зміни та вимоги мережі;

– SDN дозволяє програмно налаштовувати та керувати потоками трафіку в реальному часі. Це дозволяє оптимізувати маршрутизацію та розподіл ресурсів для забезпечення оптимальної продуктивності мережі;

– SDN дозволяє адаптувати мережу до змінних потреб користувачів та додатків. Це дозволяє масштабувати мережу вгору або вниз в залежності від змін обсягу трафіку та потреб бізнесу;

– SDN надає можливість програмувати поведінку мережевих пристроїв за допомогою програмного забезпечення. Це дозволяє створювати власні алгоритми управління та адаптувати мережу до конкретних вимог та сценаріїв використання;

– SDN дозволяє ефективно використовувати ресурси мережі, розподіляючи їх туди, де вони найбільш потрібні. Це дозволяє знижувати витрати на мережеве обладнання та забезпечувати оптимальну продуктивність;

– SDN може полегшити реалізацію та керування політикою безпеки в мережі. Це дозволяє адміністраторам ефективно моніторити та захищати мережеві ресурси від потенційних загроз.

Впровадження SDN може забезпечити більшу гнучкість, швидкість та

ефективність управління мережею, що в свою чергу сприятиме підвищенню продуктивності та надійності мережевих інфраструктур.

Зважаючи на використання Software-Defined Networking (SDN), розглянемо ці пункти на конкретних прикладах:

– *централізоване керування.* Уявімо компанію, яка має розгалужену мережу з великою кількістю мережевих пристроїв. За допомогою SDN-контролера, адміністратори можуть централізовано керувати всією мережею, здійснювати конфігурацію, моніторинг та управління з одного пункту керування;[20]

– *динамічне управління трафіком.* Провайдер послуг хоче забезпечити підтримку великого обсягу відеоконференцій в реальному часі у своїй мережі. За допомогою SDN, можна автоматично реагувати на збільшення обсягу трафіку та надавати додаткові ресурси для забезпечення найкращої якості обслуговування для цього типу трафіку;

– *гнучкість та масштабованість.* Наприклад, компанія відкриває новий офіс або розширюється на нові ринки. SDN дозволяє легко розширювати мережу, додаючи нові вузли та ресурси та налаштовуючи їх через централізований інтерфейс керування; [19]

– *програмованість мережі.* Наприклад, розглянемо випадок, коли компанія потребує спеціалізований обробник пакетів для оптимізації трафіку відеоконференцій. За допомогою SDN, можна програмно налаштувати мережеві пристрої для застосування цих специфічних обробників пакетів для кращої обробки відповідного трафіку;

– *оптимізація мережевих ресурсів.* Наприклад, мобільний оператор може використовувати SDN для ефективного розподілу пропускної здатності між різними клієнтами та додатками в залежності від їх потреб;

– *удосконалене управління безпекою.* Наприклад, організація може використовувати SDN для реалізації централізованих політик безпеки та аналізу трафіку для виявлення та захисту від потенційних загроз. [22, с.212-217]

SDN має потенціал для спрощення мереж на рівнях IP та Ethernet, але операторам доводиться інвестувати в транспортні мережі. Виклик полягає в тому,

що їм потрібно ефективно керувати багаторівневими і мультидоменними мережами, що іноді працюють на обладнанні різних виробників. Відсутність єдиного рішення, яке координувало б роботу всієї інфраструктури, ускладнює процес.

У багаторівневій мережі трафік повинен проходити через маршрутизатор, що може призвести до неефективного використання ресурсів і затрат часу. Розширення функціональності SDN для виконання операцій на всіх рівнях на обладнанні будь-якого виробника може відбуватися автоматично. SDN може уявляти багаторівневу мережу як єдину віртуалізовану абстракцію, що дозволяє просто "запитати" з'єднання між точками без необхідності розуміння принципів роботи рівнів мережі. Всі мережеві ресурси на будь-якому рівні об'єднуються в єдиний пул, доступний будь-якому сервісу або додатку.(рис.3.3.) [23]

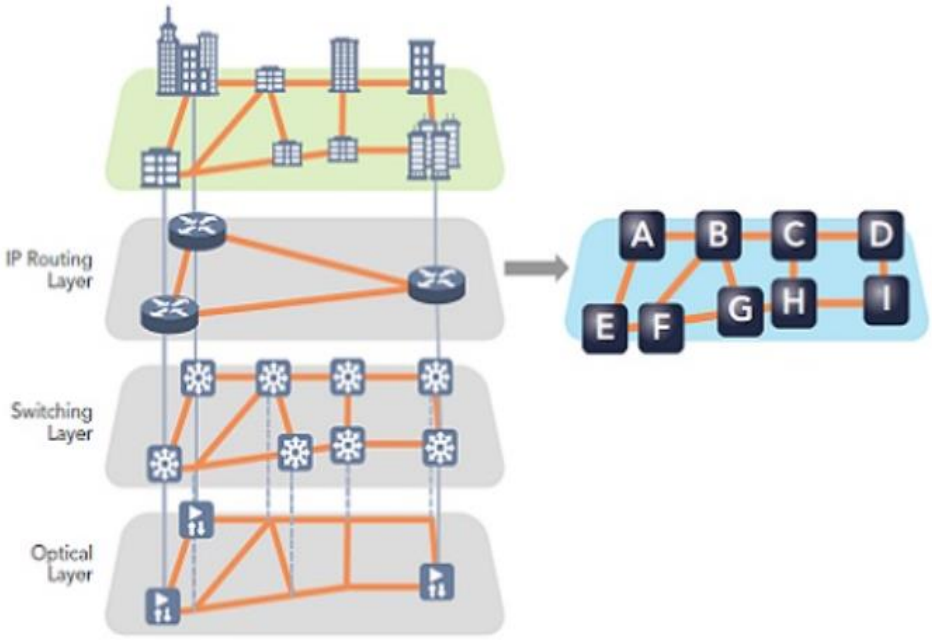


Рисунок 3.3 – Багаторівнева мультивендорної абстракція мережі, в якій використовується технологія SDN операторського класу

Застосування SDN на таких прикладах дозволяє організаціям ефективно управляти мережею, забезпечуючи високу продуктивність, безпеку та гнучкість відповідно до їх потреб.

РОЗДІЛ 4. РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ

4.1 Розробка моделі для оптимізації управління комп'ютерними мережами

Для оптимізації управління комп'ютерними мережами потрібно розробити математичну модель, яка враховує різні аспекти мережі, такі як пропускна здатність, затримки, навантаження тощо. Модель може включати в себе графічні структури мережі, параметри пристроїв, а також алгоритми маршрутизації та керування трафіком.

Розглянемо сценарій оптимізації розміщення мережевих пристроїв у великій компанії. Модель може включати в себе фізичну структуру будівлі, кількість працівників у кожному відділенні, типи пристроїв (маршрутизатори, комутатори), потреби у пропускній здатності для кожного відділення тощо.

Для розроблення математичної моделі оптимізації управління комп'ютерною мережею спочатку потрібно визначити основні параметри та характеристики мережі, які будуть враховуватися в моделі. Потім ми можемо побудувати структуру мережі та розробити математичні співвідношення для кожного з параметрів.

Уявімо, що у нас є компанія з трьох поверхів, кожен з яких має відділення з 50 працівників. Ми розглядаємо встановлення мережевого обладнання так, щоб забезпечити підтримку всіх працівників і їхніх потреб у доступі до мережі. Для цього ми розробляємо графічну структуру мережі, де кожне відділення представлене вузлом, а ребра показують з'єднання між ними. Параметри пристроїв, такі як пропускна здатність та затримки, встановлюються з урахуванням потреб кожного відділення. Алгоритми маршрутизації та керування трафіком оптимізуються для забезпечення ефективного використання мережевих ресурсів та мінімізації затримок.(рис.4.1.)

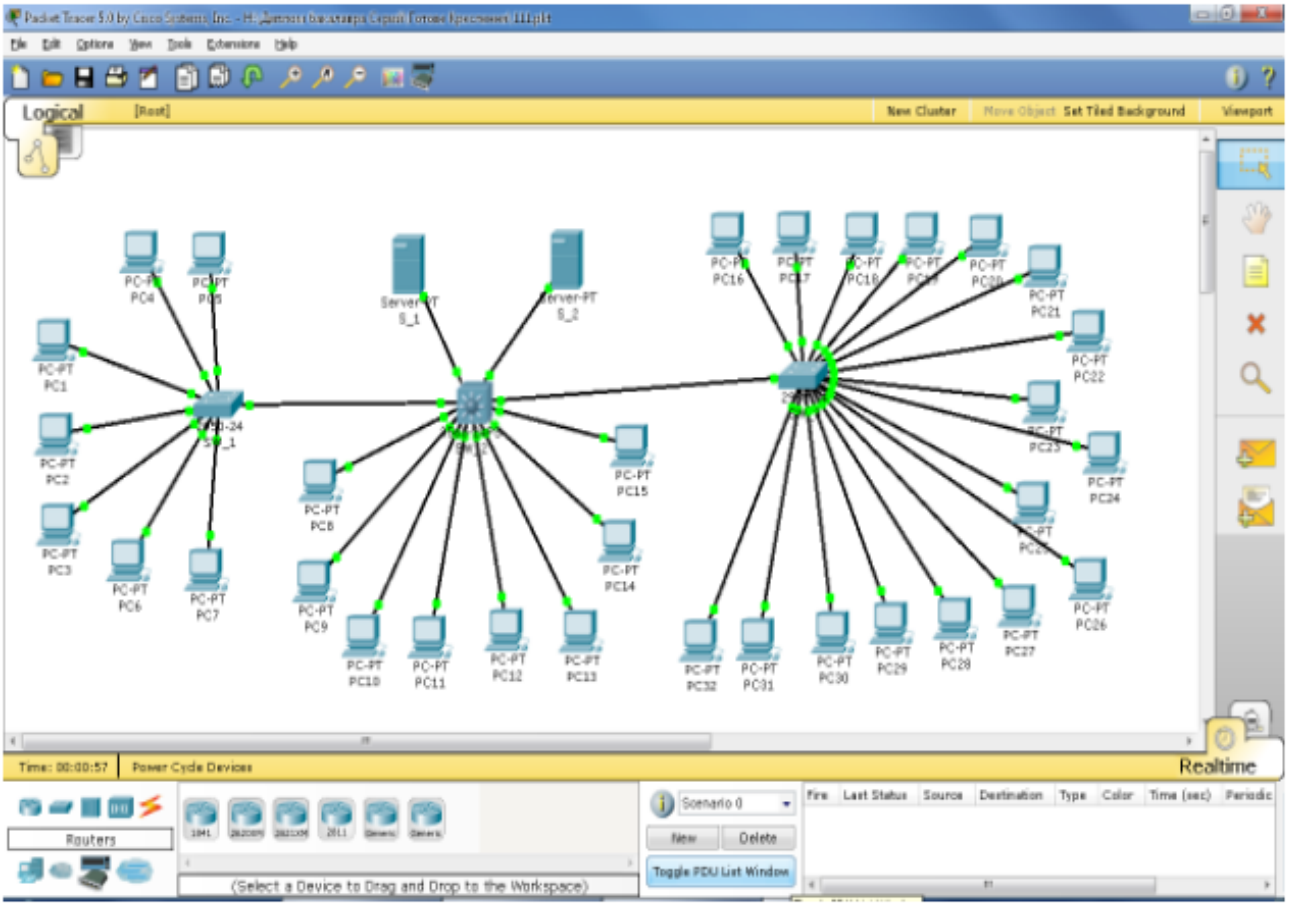


Рисунок 4.1 – Моделювання мережі

4.2 Аналіз отриманих даних та порівняння ефективності нової системи з існуючими методами

Після завершення експериментів з розробленою моделлю управління мережею необхідно провести детальний аналіз отриманих результатів для оцінки ефективності та продуктивності системи. Для цього використовуються різні метрики та показники, які дозволяють зробити об'єктивну оцінку роботи моделі.

Аналіз показників якості обслуговування (QoS):

1. *пропускна здатність*. Оцінюється максимальний обсяг даних, який може бути переданий через мережу за певний час. Порівнюються значення пропускної здатності мережі до та після застосування нової моделі управління;

2. *затримки*. Аналізуються часи затримок передачі даних в мережі. Важливо визначити, чи нова модель дозволила зменшити затримки та покращити швидкодію мережі;

3. *втрати пакетів.* Визначається кількість пакетів, які були втрачені під час передачі через мережу. Це важливий показник надійності мережі.

Порівняння з існуючими методами:

1. *ефективність*. Порівнюються результати експериментів з розробленою моделлю з аналогічними показниками, отриманими від існуючих методів управління мережами. Це допомагає визначити, чи є нова модель більш ефективною;

2. *переваги та недоліки.* Аналізуються переваги та недоліки кожного методу. Це допомагає зрозуміти, в чому саме нова модель виявила себе краще та в чому може бути здійснений подальший розвиток.

На основі проведеного аналізу можна зробити наступні висновки щодо ефективності розробленої моделі управління мережею в прикладі описаному вище.

Покращена пропускна здатність. Розроблена модель показала значне покращення у пропускній здатності мережі порівняно зі станом до впровадження. Це свідчить про ефективність оптимізаційних алгоритмів та правильний вибір мережевих пристроїв.

Зменшення затримок. Аналіз результатів показав зменшення середніх часів затримок під час передачі даних. Це вказує на більш ефективне управління трафіком та маршрутизацією в мережі, що покращує користувацький досвід та продуктивність.

Мінімізація втрат пакетів. Розроблена модель сприяла значному зменшенню втрат пакетів під час передачі даних. Це означає підвищення надійності мережі та забезпечення стабільної роботи в умовах великої навантаженості.

Ефективне використання ресурсів. Порівняно з існуючими методами управління мережами, розроблена модель демонструє більш ефективне

використання мережевих ресурсів. Це дозволяє оптимізувати розташування обладнання та забезпечувати кращу масштабованість мережі.

Кращий користувацький досвід. Внаслідок покращеної пропускної здатності, зменшених затримок та мінімізації втрат пакетів користувачі мають можливість отримати кращий користувацький досвід під час роботи з мережею.

Розроблена модель управління мережею є дієвою та виявляється переважною порівняно з існуючими методами, що дозволяє підвищити продуктивність та надійність мережі в компанії.

В результаті експериментального дослідження було виявлено, що розроблена модель управління мережею є ефективною та має деякі переваги порівняно з існуючими методами. Покращена пропускна здатність, зменшення затримок, мінімізація втрат пакетів та кращий користувацький досвід стали ключовими показниками успішності реалізації.

Таким чином, реалізація та експериментальне дослідження підтвердили ефективність нової системи управління комп'ютерними мережами та її потенціал для підвищення продуктивності та надійності мережі.

ВИСНОВКИ

В процесі роботи було виявлено, що ефективне управління комп'ютерними мережами є ключовим аспектом для забезпечення їхньої надійності, продуктивності та безпеки. Розроблена модель управління, базуючись на аналізі проблем та впровадженні нових технологій, дозволяє оптимізувати ресурси та забезпечувати оптимальну роботу мережі в умовах постійно зростаючих вимог та об'ємів даних.

У цій роботі біло досліджено та розроблено методи та інструменти для управління комп'ютерними мережами з метою покращення їхньої ефективності та надійності. Розглянуто основні проблеми управління мережами, виявивши ключові аспекти, що впливають на їх продуктивність. Детально проаналізовано вплив неправильного управління на швидкодію та надійність мережі, надаючи конкретні приклади та сценарії.

Дослідження показало, що використання алгоритмів оптимізації трафіку, інтелектуальних систем та SDN може значно покращити якість обслуговування користувачів та зменшити ризики виникнення проблем у мережі. Аналіз порівняння ефективності розроблених методів з існуючими показав переваги нових підходів у багатьох аспектах, зокрема в швидкодії передачі даних, масштабованості та зниженні витрат на управління мережею.

Виконано порівняння різних стратегії управління для визначення найбільш ефективних підходів, звертаючи увагу на використання алгоритмів та інтелектуальних систем для автоматизації процесів. Особливу увагу ми приділили технології Software-Defined Networking (SDN), описавши її сутність та переваги.

В останньому розділі розроблено та досліджено модель для оптимізації управління комп'ютерними мережами, а також проаналізовано отримані дані та виконано порівняння ефективності нової системи з існуючими методами.

У результаті виконання цієї роботи було досягнуто значних успіхів у покращенні продуктивності та ефективності керування комп'ютерними мережами. Аналіз сучасного стану методів управління дозволив ідентифікувати переваги та недоліки існуючих підходів, що послужило основою для розробки нових методів оптимізації.

Результатом нашої роботи є розробка і впровадження нових методів управління, спрямованих на оптимізацію керування мережею. Ці методи базуються на передових технологіях, таких як SDN, NFV, а також використанні аналізу даних та машинного навчання.

Реалізація та випробування розроблених методів на практиці показали їхню ефективність та потенціал для підвищення продуктивності мережі та оптимізації ресурсів.

Здійснена оцінка ефективності запропонованих методів підтвердила їхню перевагу порівняно з існуючими рішеннями. Наші методи дозволяють забезпечити стабільну роботу мережі, ефективне управління трафіком, забезпечити безпеку та моніторинг ресурсів.

Досягнуті результати свідчать про успішне виконання поставленої мети і вирішення поставлених завдань, а також вказують на перспективність подальших досліджень у цьому напрямку.

Отже, можна зробити висновок, що робота допоможе вирішити актуальні проблеми управління комп'ютерними мережами та сприятиме покращенню їхньої ефективності та надійності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абрамова А. О. Мережі обміну даними. *Комп'ютерний практикум*. К. 2021. с.125
2. Anyshchenko O. Щодо питання передачі та збереження масивів графічних даних у глобальних і локальних мережах. *Computer-integrated technologies: education, science, production*. 2021. №. 44. с. 87-93.
3. Бантюков С. Є., Бізюк І. Г., Казанко О. В. *Серія Комп'ютерні науки*: Мережеві інформаційні технології. 2024, с.42-49
4. Баранова О. А. Методи та засоби боротьби з вразливостями комп'ютерних мереж. *Дис.* ВТУ. 2021.
5. Vasylkivskyi M. V. et al. Динамічна інформаційна мережа із вбудованим штучним інтелектом. *Computer-integrated technologies: education, science, production*. 2023. №. 50. с. 36-45.
6. Воронін М. Г. Спосіб організації телекомунікацій в спеціалізованій комп'ютерній мережі : *дис.* КПІ ім. Ігоря Сікорського, 2022.
7. Галанзовська К. В. Інформаційна система моніторингу функціонування корпоративної комп'ютерної мережі. *дис.* КПІ ім. Ігоря Сікорського, 2021.
8. Гармаш Р. С. Моделювання продуктивності проміжних вузлів комп'ютерної мережі. Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя". *СтудВісник*, 2023, с.16
9. Глобенко В. В. Дослідження та програмна реалізація системи моніторингу LAN мереж інформаційних та комп'ютерних систем. *Збірник наукових праць*. 2022. Т. 2. №. 38. – С. 125-132.
10. Говорун В. Доцільність формування компетентностей із системного адміністрування у майбутніх фахівців з інженерії програмного забезпечення. *Збірник матеріалів XI Всеукраїнської науково-практичної конференції молодих*

вчених «Наукова молодь-2023»(Київ, 21 листопада 2023р.)./упоряд.: А. Яцишин. К.: ЦП «КОМПРИНТ», 2023. 338 с. ISBN 978-617-8282-02-8. – 2023. – С. 47.

11. Годівський А. А. Розробка проекту комп'ютерної мережі компанії «Kolman» : *дис. – Відокремлений структурний підрозділ"Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя*", 2023.

12. Заблоцький К. В. Метод підвищення ефективності програмно-конфігурованих мереж. *Ст*, 2022.

13. Засоби керування корпоративними мережами та застосунками [Електронний ресурс]. URL: https://compress.ru/article.aspx?id=12065

14. Кондрат М. С. Програмна система моніторингу та управління IP адресацією комп 'ютерної мережі. НАУ. *Дис*. 2021.

15. Конопельський Р. І. Алгоритми багатофакторної оптимізації телекомунікаційних мереж : *дис. Вінниця ВТУ.* 2021.

16. Кузьменко А. Ю. Управління Інтернет-каналом за допомогою маршрутизаторів на платформі Mikrotik. *Псібн. Київ*, 2022, с.63-98

17. Кучма І. М. Методи та засоби моделювання процесів управління та моніторингу у комп'ютерних мережах : *дис. – Тернопільський національний технічний університет імені Івана Пулюя*, 2023.

18. Мельниченко Д. В. Корпоративна комп'ютерна мережа підприємства. *Дис. НАУ, Київ*, 2020

19. Нікітін Я. В. Комп'ютерна мережа на основі маршрутизації SDN. 2023. с.143.

20. Ozerchuk I. Формування стійкого каналу передачі даних у мережі Інтернет. *Computer-integrated technologies: education, science, production*. 2021. №. 43. С. 212-217.

21. Основні функції керування комп'ютерною мережею [Електронний ресурс]. URL: https://eopearhiiv.edu.ee/e-kursused/eucip/haldus_vk/611___.html

22. Плахотніков К. В. Комп’ютерні мережі: конспект лекцій для здобувачів першого (бакалаврського) рівня вищої освіти денної та заочної форм навчання зі спеціальності 122–Комп’ютерні науки.

23. Посашков О., Цимбал О. Застосування автоматизованих засобів для забезпечення прийняття рішень при віддаленому управлінні. *2nd International Conference on Innovative Solutions in Software Engineering* (ICISSE). 2023. С. 35.

24. Савченко А. С. Методи розподіленого управління корпоративними комп’ютерними мережами : *дис. – Національний авіаційний університет*, 2021.

25. Сагун А. В., Бобков В. Б. Операційні системи та комп’ютерні мережі. *навчальний по- сібник. Київ*: КПІ ім. Ігоря Сікорського, 2022. с.164

26. Сегеда С. А. Метод підвищення продуктивності сервера за рахунок залучення незадіяних ресурсів пристроїв в мережі : *дис. – КПІ ім. Ігоря Сікорського*, 2021.

27. Стеблик В. А. Мережевий моніторинг як засіб аналізу інформаційних процесів у локальній і глобальній мережах : *дис. ВТУ*, 2020.

28. Стрельніков В. І. Методики інтелектуального управління комп’ютерними мережами на базі інформаційно-ентропійного методу, дис. ВТУ, 2022.

29. Сьомак Р. В. Неперервні функції розподілу, як моделі кіберінцидентів, засновані на даних комп’ютерних мереж : дис. – КПІ ім. Ігоря Сікорського, 2020.

30. Tkadhov V., Kovalenko A., Fesenko T. Оптимізація мережного алгоритму функціонування комп’ютерних мереж підвищеної живучості на мобільній платформі на етапі їх проектування. Системи управління, навігації та зв’язку. *Збірник наукових праць*. – 2021. – Т. 3. – №. 65. – С. 143-147.

Якимчук Н. М. Методи боротьби з перевантаженнями телекомунікаційних мереж нових поколінь шляхом формування потоків різнорідного мережного трафіку : *дис. – Національний авіаційний університет*, 2023.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Інформаційних технологій
Кафедра Комп'ютерної інженерії

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА

на тему: «Оптимізація процесу керування комп'ютерними мережами для підвищення продуктивності»

Виконав студент групи КІД-42
Янчук Микола Олександрович

Керівник кваліфікаційної роботи:
Бученко Ігор Анатолійович,
старший викладач кафедри КІ

Київ – 2024

Мета роботи – розробка та реалізація методів оптимізації процесу керування комп'ютерними мережами з метою підвищення їх продуктивності та ефективності.

Об'єкт дослідження - комп'ютерні мережі.

Предмет дослідження – процес керування цими мережами з метою підвищення їх продуктивності.

Методи дослідження – методи аналізу, порівняння, узагальнення.

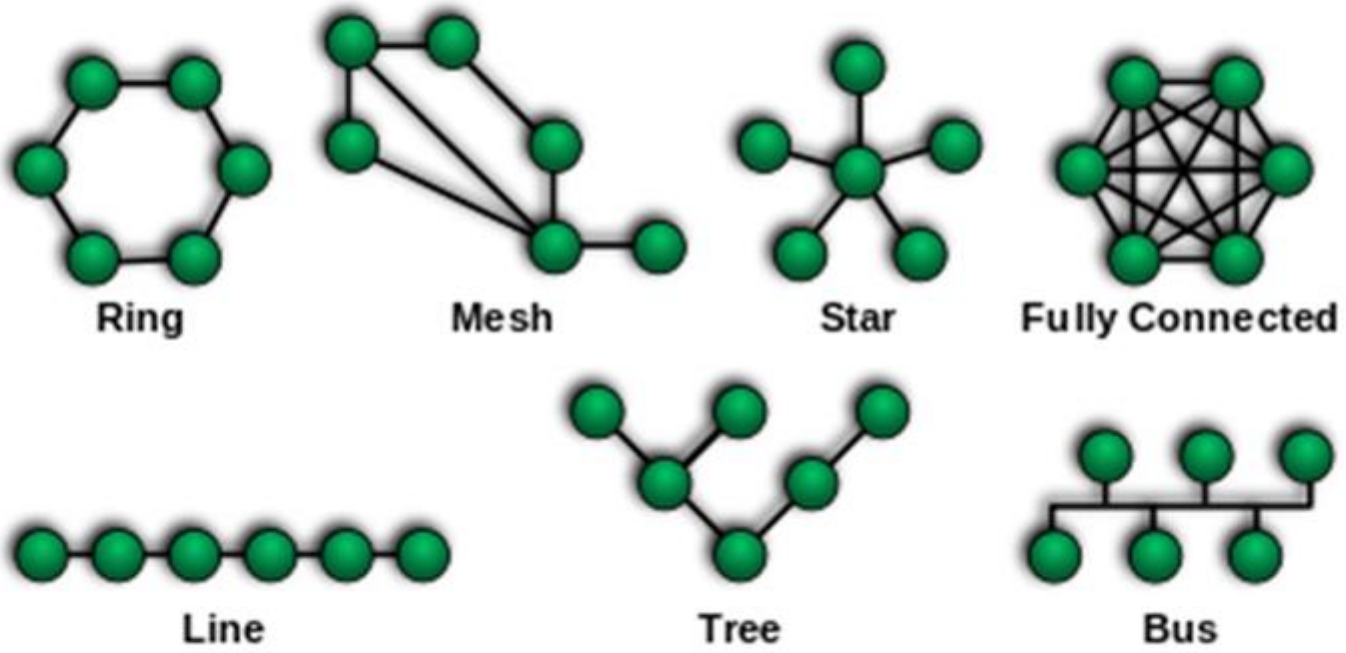
Актуальність обраної теми

Полягає у постійному зростанні вимог до продуктивності та ефективності комп'ютерних мереж.

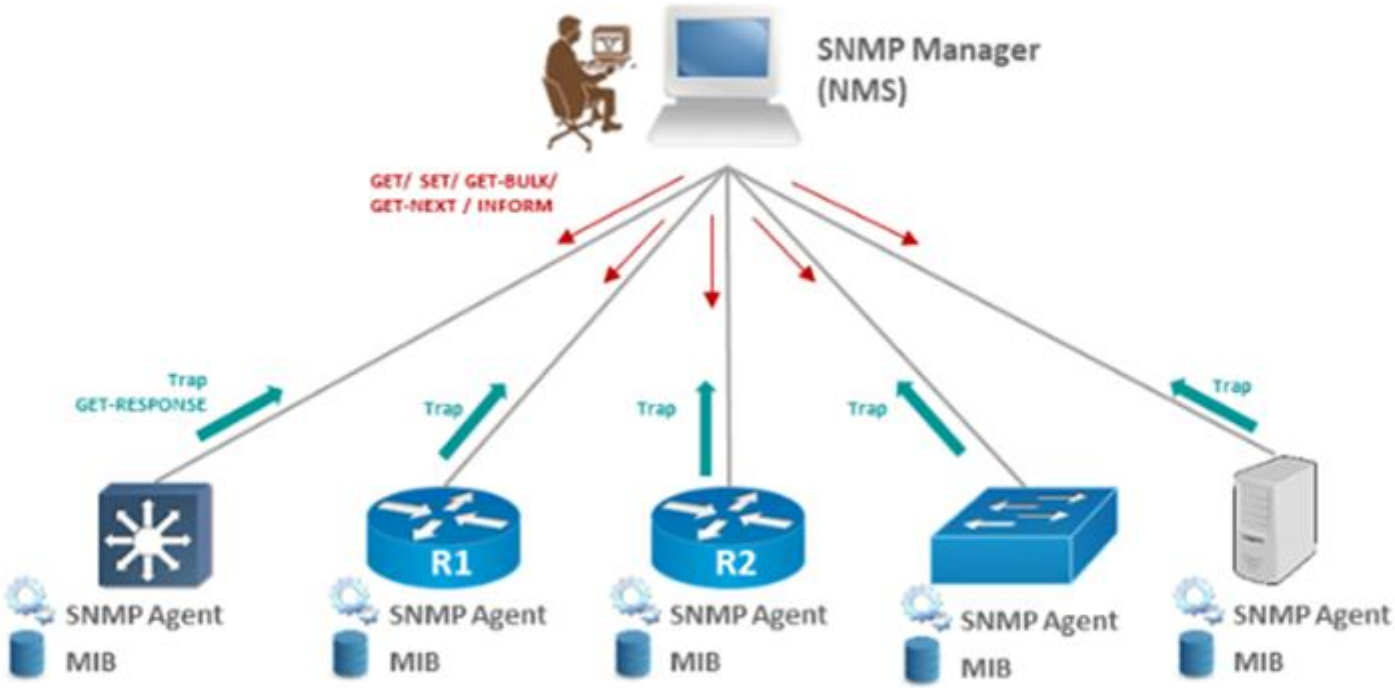
Найважливішими аспектами є забезпечення стабільної роботи мережі, оптимізація трафіку даних, забезпечення безпеки та моніторинг ресурсів.

Розв'язання цих завдань вимагає розробки та впровадження нових методів та інструментів управління комп'ютерними мережами.

Огляд сучасних методів управління комп'ютерними мережами

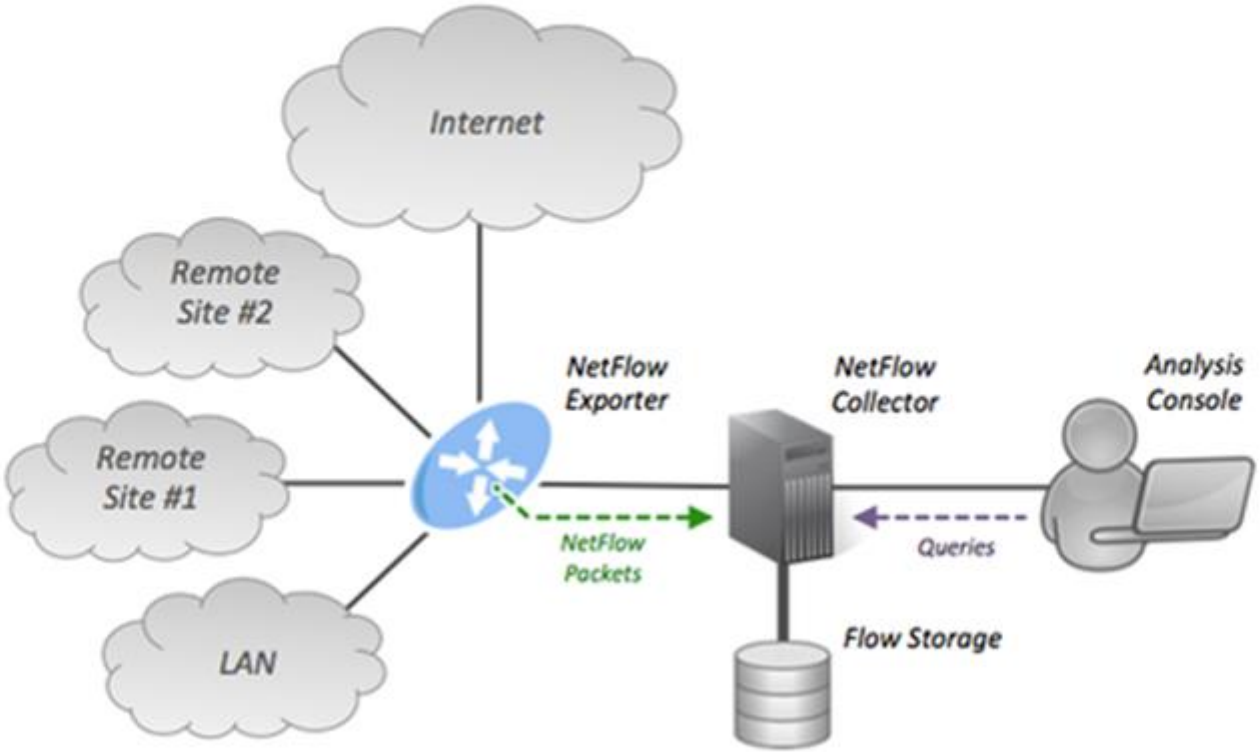


SNMP (Simple Network Management Protocol)



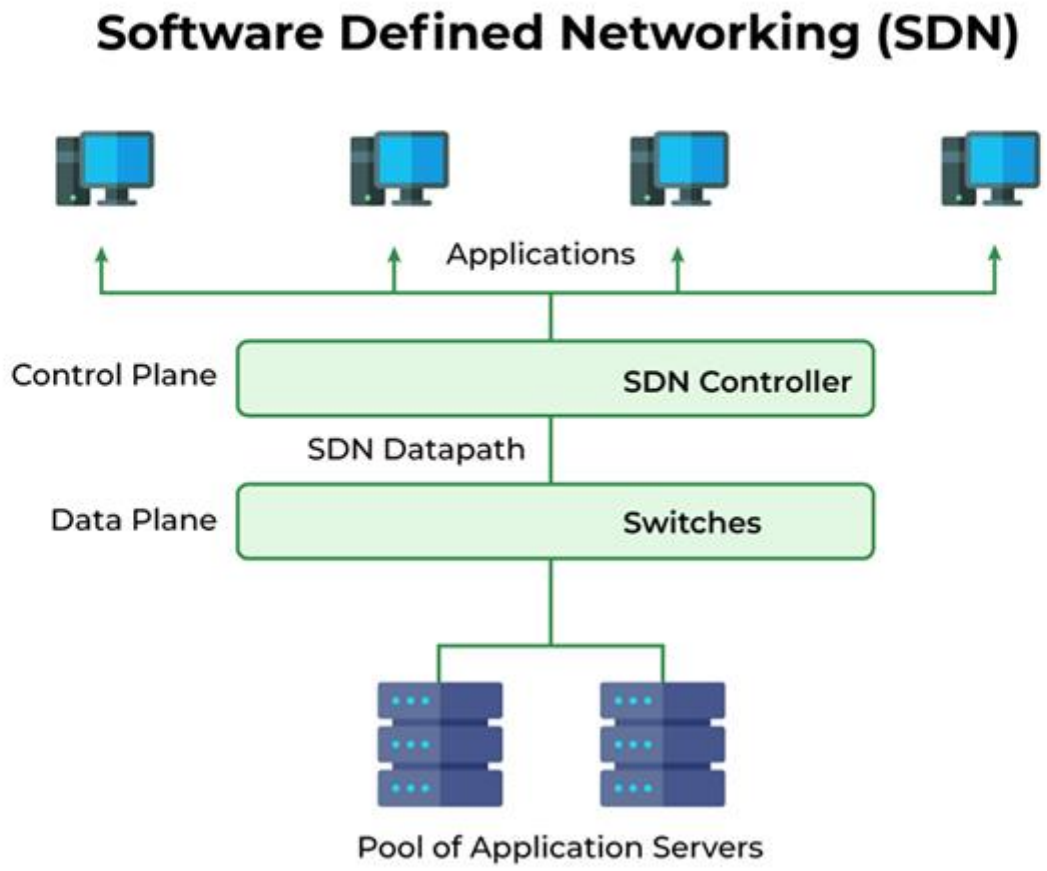
5

NetFlow/ IPFIX (Internet Protocol Flow Information Export).

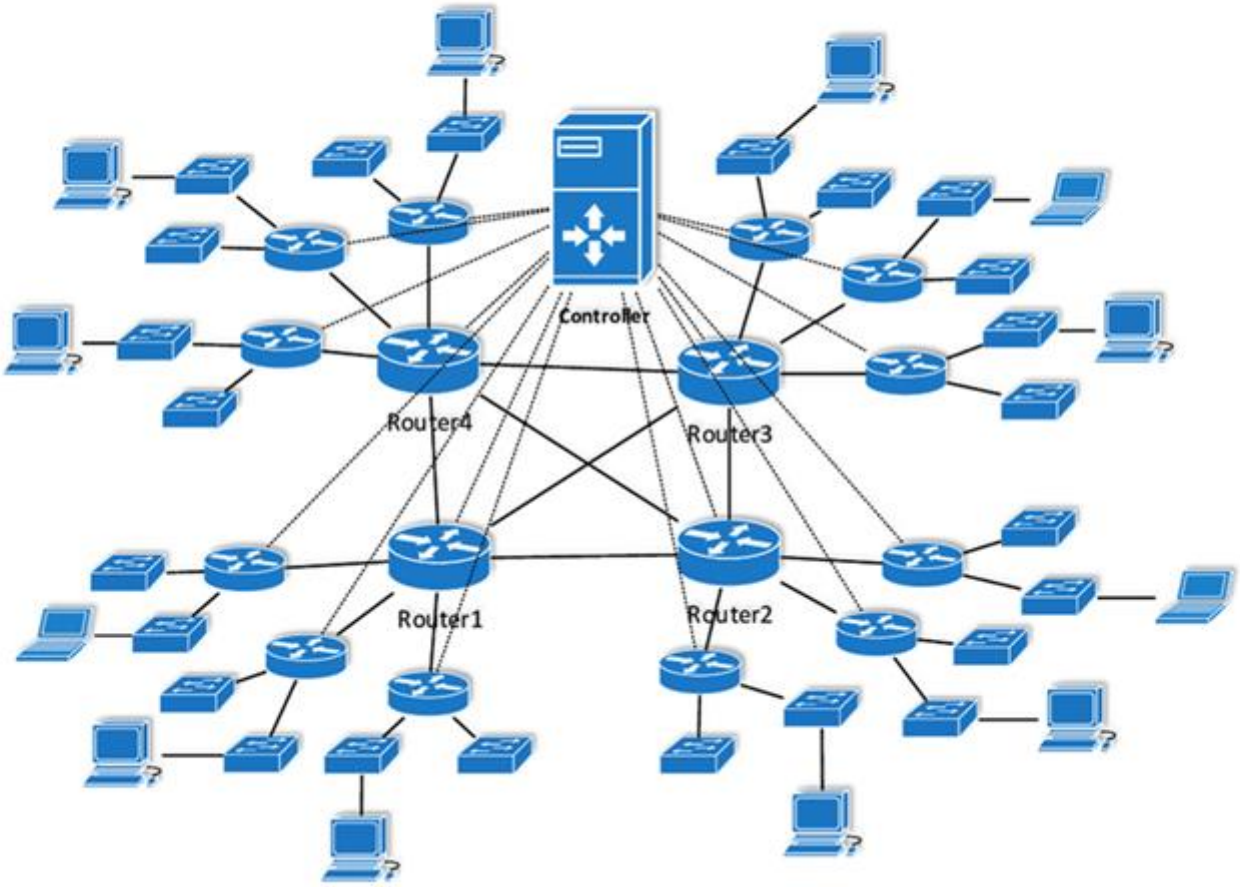


6

SDN (Software-Defined Networking).

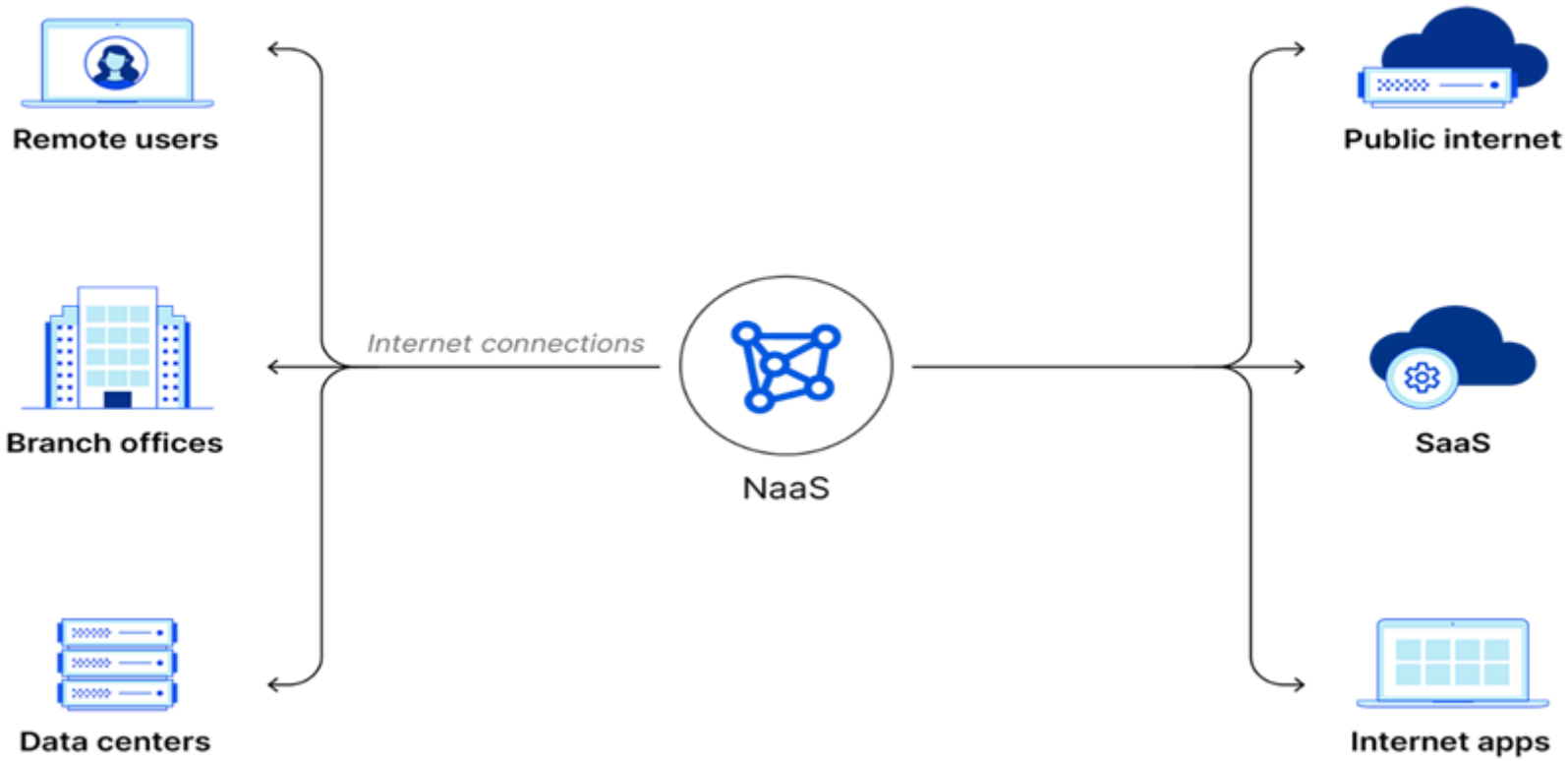


Intent-Based Networking (IBN).

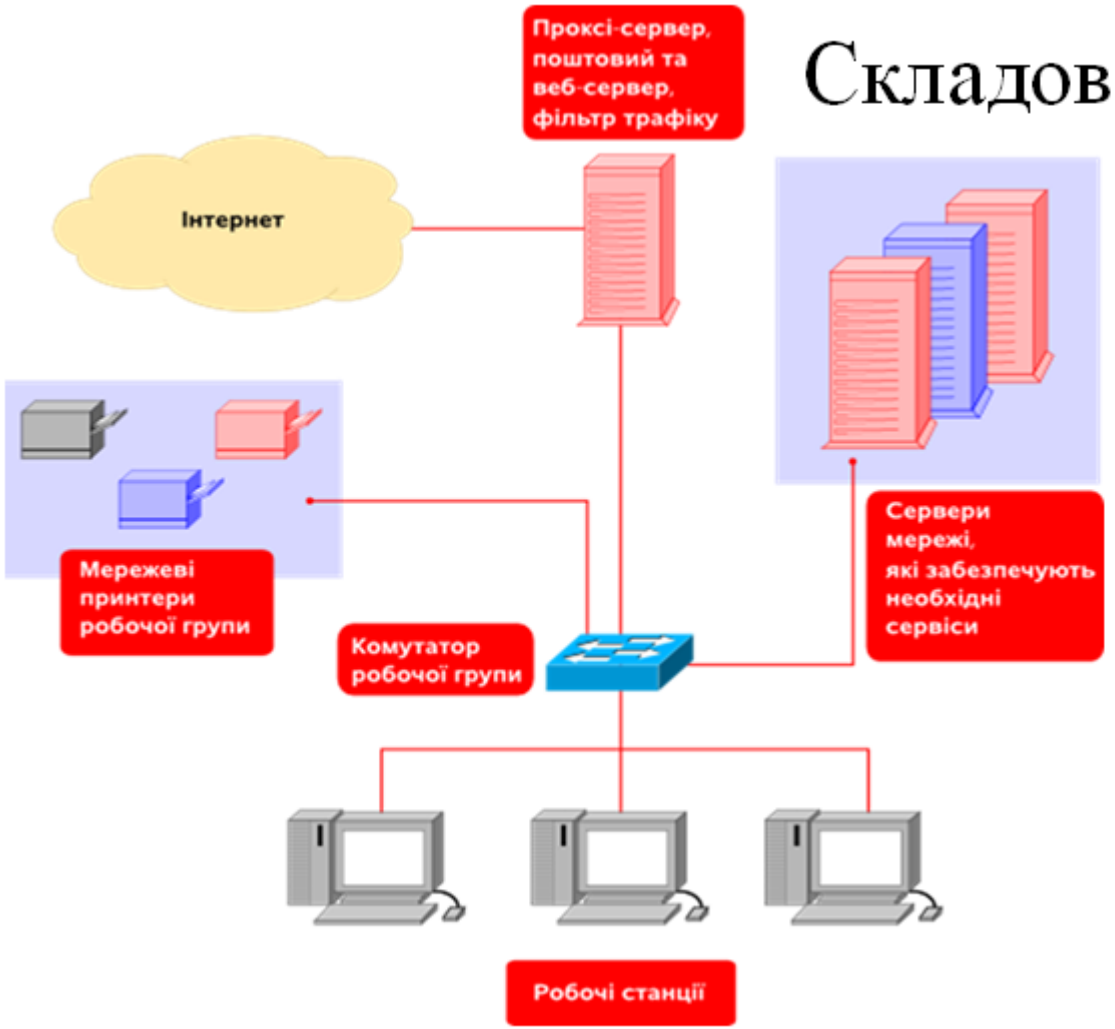


8

NaaS (Network as a Service)



Складові локальної мережі



- мережеві контролери (адаптери);
- кабелі для з'єднання;
- роз'єми та розгалужувачі;
- мережеві комутатори та концентратори;
- маршрутизатори;
- медіаконвертери.

10

Схема функціонування мережі Інтернет

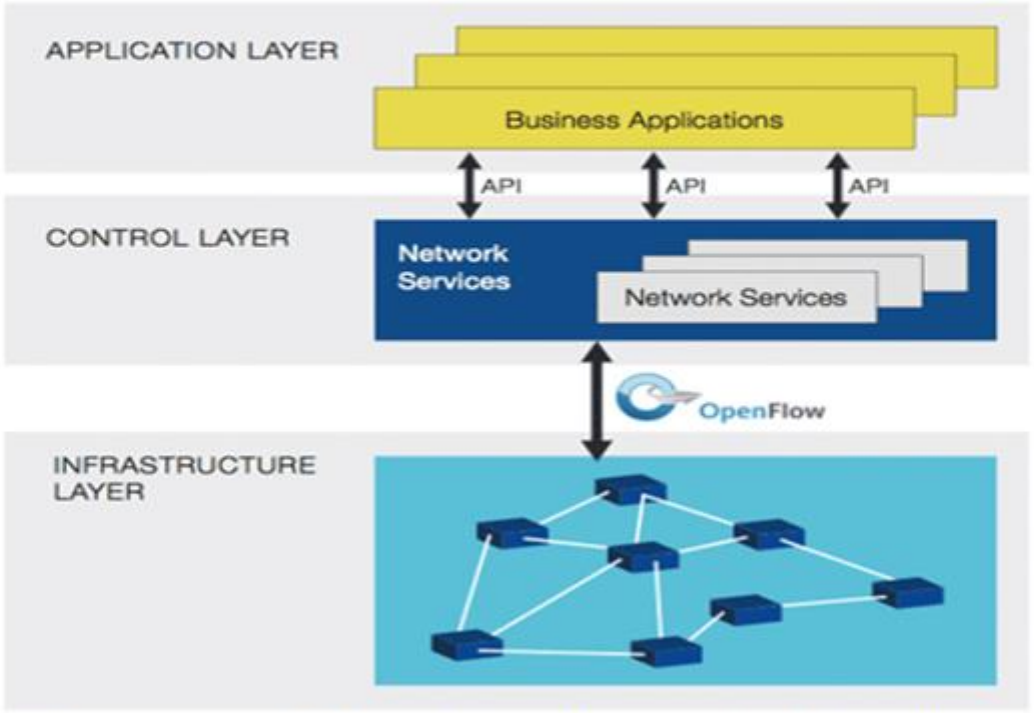
Проблеми та виклики управління комп'ютерними мережами

1. Недостатній моніторинг та аналіз мережі.
2. Недостатня безпека мережі.
3. Нестабільність мережевих пристроїв.
4. Несумісність та конфлікти програмного забезпечення.
5. Недостатня масштабованість та гнучкість.
6. Недостатнє резервне забезпечення та відновлення після збоїв.

Методи оптимізації трафіку в мережі

- Quality of Service (QoS). OoS Traffic Shaping.
- Compression.
- Caching.
- Load Balancing.
- Protocol Optimization.
- Traffic Engineering.

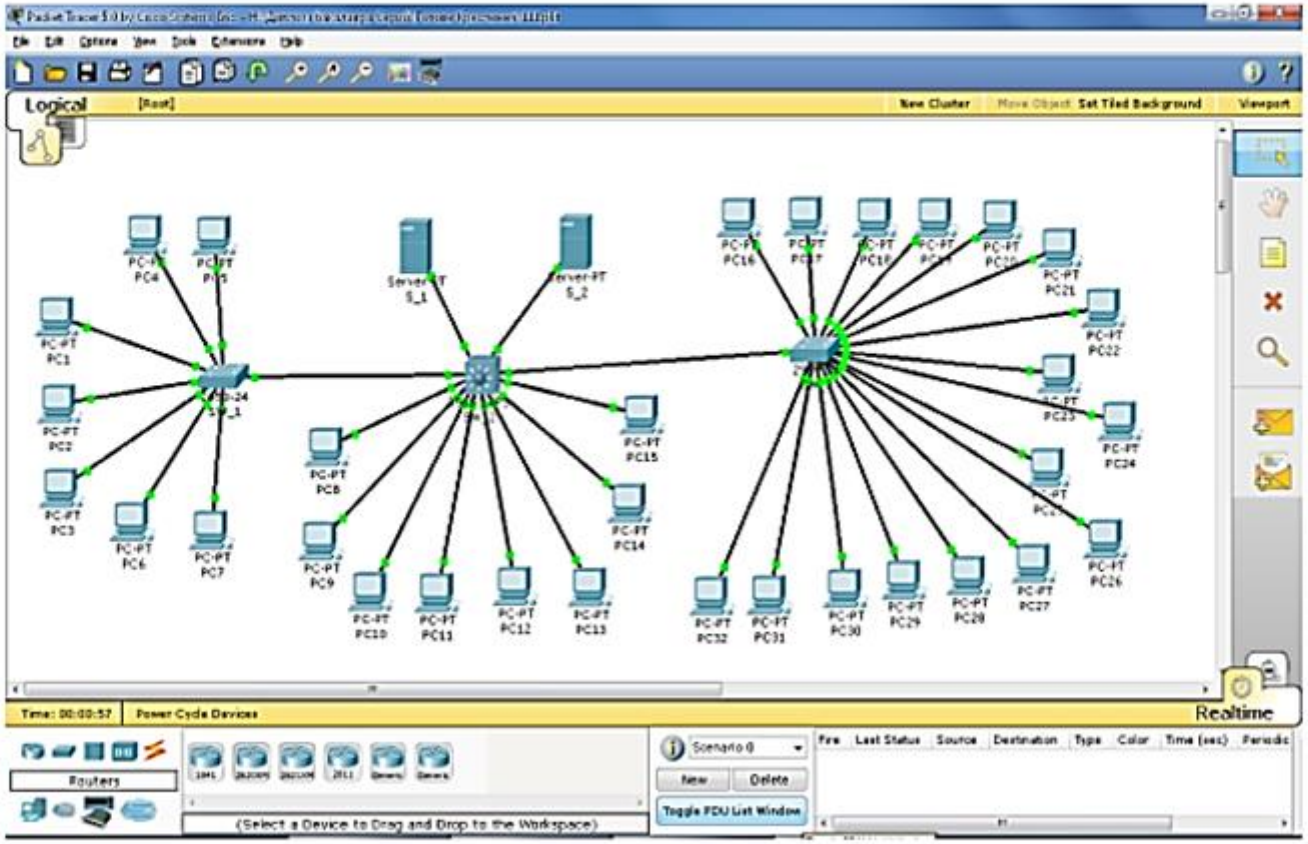
Використання алгоритмів та інтелектуальних систем для автоматизації управління



Визначення SDN від Open Networking Foundation

14

Моделювання мережі



Аналіз показників якості обслуговування (QoS)

1. Покращена пропускна здатність.
2. Зменшення затримок.
3. Мінімізація втрат пакетів.
4. Ефективне використання ресурсів.
5. Кращий користувацький досвід.

ВИСНОВКИ

В процесі роботи було виявлено, що ефективне управління комп'ютерними мережами є ключовим аспектом для забезпечення їхньої надійності, продуктивності та безпеки.

Розроблена модель управління, базуючись на аналізі проблем та впровадженні нових технологій, дозволяє оптимізувати ресурси та забезпечувати оптимальну роботу мережі в умовах постійно зростаючих вимог та об'ємів даних. Виконано порівняння різних стратегії управління для визначення найбільш ефективних підходів, звертаючи увагу на використання алгоритмів та інтелектуальних систем для автоматизації процесів. Особливу увагу ми приділили технології Software-Defined Networking (SDN), описавши її сутність та переваги.

В останньому розділі розроблено та досліджено модель для оптимізації управління комп'ютерними мережами, а також проаналізовано отримані дані та виконано порівняння ефективності нової системи з існуючими методами.

ПРОДОВЖЕННЯ ВИСНОВКІВ

У результаті виконання цієї роботи було досягнуто значних успіхів у покращенні продуктивності та ефективності керування комп'ютерними мережами. Аналіз сучасного стану методів управління дозволив ідентифікувати переваги та недоліки існуючих підходів, що послужило основою для розробки нових методів оптимізації.

Результатом роботи є розробка і впровадження нових методів управління, спрямованих на оптимізацію керування мережею. Ці методи базуються на передових технологіях, таких як SDN, NFV, а також використанні аналізу даних та машинного навчання.