МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ
Факультет кібербезпеки, програмної інженерії та комп'ютерних наук
Кафедра інформаційних технологій

Пояснювальна записка

до кваліфікаційної роботи
другого (магістерського) рівня

на тему МЕТОДИ ОЦІНКИ ЕФЕКТИВНОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ

Виконав: студент 2 курсу, групи ІКК 2.1
спеціальності
121 Інженерія програмного забезпечення

Смокін Павло Олександрович

Керівник Розенвассер Д.М.

Рецензент Педяш В.В.

Одеса – 2023

ДОВІДКА

кафедри ІТ про виконану магістерську роботу

студента 2 курсу ФКПІ та КН групи ІКК 2.1

Смокіна Павла Олександровича

на тему Методи оцінки ефективності комп'ютерної мережі

Висновок нормоконтролера каск. роботи до кваліфік. роботи викона-
на з незначними порушеннями ДСТУ, оформл. дипло
положення МПУ

Нормоконтролер викл. каф. ІТ. 15.12.2023 Кальніцька І.В.
(науковий ступінь, вчене звання, посада) (підпис, дата) (і. б. прізвище)

Висновок відповідального за наявність плагіату згідно з сертифікатом
ID унікальність роботи підтверджено.

Відповідальна особа викл.-каф. ІТП 15.12.2023 Кальніцька І.В.
(науковий ступінь, вчене звання, посада) (підпис, дата) (і. б. прізвище)

Попередня експертиза (захист) магістерської роботи
(бакалаврської роботи чи магістерської роботи)

студ. Семокін П. О. проведена "12" 12. 2023 р.
(прізвище і.б.)

Висновки кваліфікаційна робота виконана у
повному обсязі. В роботі розглядаються комп'ютерні
мережі, показники їхньої ефективності, методи
оцінки ефективності комп'ютерних мереж.
Здобувач має достатню теоретичну підготов-
ку. Виконана магістерська робота відповідає
діючим стандартам та рекомендується
до захисту

Члени комісії (підпис) д.т.н., проф. Стрелковська І.В.
(науковий ступінь, вчене звання, посада, прізвище і.б.)

(підпис) к.т.н., доц. Григор'єва Т.Г.
(науковий ступінь, вчене звання, посада, прізвище і.б.)

(підпис) к.т.н., доц. Горбалов В.Е.
(науковий ступінь, вчене звання, посада, прізвище і.б.)

МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, програмної інженерії та комп'ютерних наук
Кафедра інформаційних технологій
Освітній ступінь магістр
Галузь знань 12 Інформаційні технології
Спеціальність 121 Інженерія програмного забезпечення

ЗАТВЕРДЖУЮ
Завідувач кафедри ІТ
к.т.н., доц.
_____ Т.І.Григор'єва
"25" 09 2023 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ

Смокіну Павлу Олександровичу

1. Тема роботи: Методи оцінки ефективності комп'ютерної мережі
керівник роботи Розенвассер Денис Михайлович
затверджені наказом закладу вищої освіти від 25.09.2023 р. № 1957

2. Строк подання студентом роботи 11.12.2023

3. Вихідні дані до роботи: зробити огляд комп'ютерних мереж та методів оцінки їхньої ефективності. Розробити алгоритм оцінки ефективності комп'ютерної мережі за допомогою різних методів.

4. Зміст розрахунково-пояснювальної записки
Розділ 1: Огляд комп'ютерних мереж
Розділ 2: Показники ефективності комп'ютерної мережі
Розділ 3: Порівняння методів оцінки ефективності комп'ютерної мережі

5. Перелік графічного матеріалу (з зазначенням обов'язкових креслень)
Слайд 1 – Порівняня типів комп'ютерних мереж

Слайд 2 – Ефективність комп'ютерної мережі
Слайд 3 – Показники ефективності комп'ютерної мережі
Слайд 4 – Порівняння методів оцінки ефективності комп'ютерної мережі
Слайд 5 – Висновки та рекомендації

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Завдання видав	Завдання прийняв

7. Дата видачі завдання 25.09.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Вступ	25.09.2023-5.10.2023	вик
2	Огляд комп'ютерних мереж	6.10.2023-19.10.2023	вик
3	Показники ефективності комп'ютерної мережі	20.10.2023-5.11.2023	вик
4	Порівняння методів оцінки ефективності комп'ютерної мережі	6.11.2023-20.11.2023	вик
5	Висновки та рекомендації	21.11.2023-28.11.2023	вик
6	Перелік джерел та посилань	29.11.2023-5.12.2023	вик
7	Оформлення презентації	6.12.2023-11.12.2023	вик

Студент _____ П.О. Смокін
(підпис)

Керівник роботи _____ Д.М. Розенвассер
(підпис)

ВІДГУК КЕРІВНИКА

магістерської роботи студента Смокіна П.О.
на тему: «Методи оцінки ефективності комп'ютерної мережі»

Завдання оцінки ефективності комп'ютерної мережі полягає в тому, щоб визначити, наскільки добре мережа виконує свої функції. Оцінка ефективності мережі може бути використана для вирішення таких завдань, як: підвищення продуктивності мережі, покращення надійності мережі, поліпшення безпеки мережі, зменшення витрат на володіння та експлуатацію мережі. Аналіз та оцінка ефективності комп'ютерних мереж є дуже актуальною задачею.

У роботі розглядаються комп'ютерні мережі, показники їхньої ефективності, методи оцінки ефективності комп'ютерних мереж.

Студент Смокін С.О. добре розібрався з усіма проблемами і основну увагу приділив докладному аналізу ефективності комп'ютерної мережі та розробці алгоритму оцінки ефективності комп'ютерної мережі.

Робота проводилася значною мірою самостійно. Графік консультацій не порушувався.

Завдання на ВКР виконано. При оформленні пояснювальної записки та демонстраційних слайдів використовувались комп'ютерні технології.

Під час виконання магістерської роботи студент Смокін С.О. глибоко вивчив питання ефективності комп'ютерної мережі, показав уміння користуватись навчальною та технічною літературою, ставити та розв'язувати інженерні задачі.

Магістерська робота відповідає вимогам до випускних магістерських робіт. Робота студента Смокіна П.О. заслуговує оцінки «добре».

Студент Смокін П.О. заслуговує присвоєння кваліфікації магістр з інженерії програмного забезпечення за заявленою спеціальністю 121 «Інженерія програмного забезпечення».

Керівник
к.т.н., доцент кафедри КН  Д.М. Розенвассер

РЕЦЕНЗІЯ

на магістерську роботу студента Смокіна П.О.
на тему: «Методи оцінки ефективності комп'ютерної мережі»

Магістерська робота містить 3 розділи текстової частини, демонстраційні слайди, виконана згідно з завданням на магістерську роботу.

У роботі розглядаються різні типи комп'ютерних мереж та методи оцінки їхньої ефективності.

Тема оцінки ефективності комп'ютерних мереж є дуже актуальною і важливою в сучасному світі інформаційних технологій. Велика частина бізнес-процесів, освітніх установ, наукових досліджень та повсякденного життя залежить від надійності, продуктивності та безпеки комп'ютерних мереж. Зі зростанням обсягів мережевого трафіку та вимог до швидкості передачі даних важливо вдосконалювати і оцінювати ефективність мережі.

Магістерська робота виконана відповідно до завдання. Демонстраційні матеріали й пояснювальна записка виконані охайно й відповідно до вимог ЄСКД. Прийняті рішення обґрунтовано.

Автором показана достатня теоретична підготовка. Робота виконана грамотно, текст її послідовний та зрозумілий, оформлення роботи та демонстраційних слайдів якісне.

До недоліків роботи варто віднести:

- у роботі відсутні чисельні оцінки ефективності окремих компонентів комп'ютерної мережі;

- у роботі не вказано вичерпну послідовність дій для оцінки ефективності комп'ютерної мережі.

Зазначені недоліки суттєво не знижують якості виконаної роботи.

Магістерська робота відповідає вимогам до випускних кваліфікаційних робіт магістрів. Робота студента Смокіна П.О. заслуговує оцінки «добре».

Студент Смокін П.О. заслуговує присвоєння кваліфікації магістр з інженерії програмного забезпечення за заявленою спеціальністю 121 «Інженерія програмного забезпечення».

Рецензент
к.т.н., доцент кафедри КІ та ІТ Педяш В.В.

UNICHECK
by Turnitin

Ім'я користувача:
Анна Серединко

ID перевірки:
1016014349

Дата перевірки:
17.12.2023 19:10:37 MSK

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
17.12.2023 19:14:15 MSK

ID користувача:
100001433

Назва документа: Смокін_Методи_оцінки_ефективності_комп'ютерної_мережі

Кількість сторінок: 35 Кількість слів: 5393 Кількість символів: 42595 Розмір файлу: 1.44 MB ID файлу: 1015701007

2.56%
Схожість

Найбільша схожість: 0.63% з Інтернет-джерелом (https://uk.unionpedia.org/i/Java)

2.56% Джерела з Інтернету | 108 ..... Сторінка 37

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

РЕФЕРАТ

Текстова частина магістерської роботи: 50 с., 11 рисунків, 2 таблиці, 1 додаток, 24 джерела.

КОМП'ЮТЕРНА МЕРЕЖА, ЕФЕКТИВНІСТЬ, НАДІЙНІСТЬ, ПРОДУКТИВНІСТЬ, ТЕСТУВАННЯ, ЗАТРИМКА, БЕЗПЕКА

Об'єкт дослідження – комп'ютерні мережі та їхні компоненти.

Мета роботи – зробити огляд комп'ютерних мереж та методів оцінки їхньої ефективності. Розробити алгоритм оцінки ефективності комп'ютерної мережі за допомогою різних методів.

Метод дослідження – аналітичний з використання комп'ютерних технологій.

У магістерській роботі проведено аналіз комп'ютерних мереж та методів оцінки ефективності. Розроблено алгоритм оцінки ефективності комп'ютерної мережі за допомогою різних методів. Зроблено висновки та рекомендації щодо застосування приведеного алгоритму.

ABSTRACT

The text part of the master paper: 50 pp., 11 figures, 2 tables, 1 appendix, 24 references.

COMPUTER NETWORK, EFFICIENCY, RELIABILITY, PRODUCTIVITY, TESTING, LATENCY, SECURITY

Object of research are computer networks and their components.

The purpose of the work is review computer networks and methods of evaluating their effectiveness. Develop an algorithm for evaluating the effectiveness of a computer network using various methods.

The research method is analytical with the use of computer technologies.

In the master's work, an analysis of computer networks and efficiency assessment methods was carried out. An algorithm for evaluating the effectiveness of a computer network using various methods has been developed. Conclusions and recommendations regarding the application of the given algorithm have been made.

ЗМІСТ

1 ОГЛЯД КОМП’ЮТЕРНИХ МЕРЕЖ

1.1 Типи комп’ютерних мереж

Комп'ютерна мережа - це сукупність комп'ютерів і інших пристроїв, з'єднаних між собою каналами передачі даних. Комп'ютерні мережі використовуються для обміну даними, спільного використання ресурсів і доступу до Інтернету.

Комп’ютерні мережі дозволяють обмінюватися даними між різними комп’ютерами. Це може бути текстова інформація, зображення, відео, звук або будь-які інші дані. Вони дозволяють спільно використовувати ресурси, такі як принтери, сканери, накопичувачі інформації та програмне забезпечення, а також дозволяють людям спілкуватися між собою, незалежно від їхнього місцезнаходження.

Головними застосуваннями комп’ютерних мереж можна назвати доступ до ресурсів комп’ютерів, розташованих в інших місцях, спільну роботу над проектами, електронну комерцію для електронних платежів та купівлі-продажу товарів і послуг та, звичайно, доступ до Інтернету, перегляду відео та прослуховування музики.

Існує багато різних типів комп'ютерних мереж.

За областю дії комп'ютерні мережі поділяються на:

- персональні мережі (PAN) - це локальні мережі, які об'єднують комп'ютери та інші пристрої в межах однієї кімнати або невеликого приміщення. PAN зазвичай використовують для спільного використання файлів, принтерів та інших ресурсів;
- локальні мережі (LAN) - це локальні мережі, які об'єднують комп'ютери та інші пристрої в межах одного будівлі або невеликого комплексу будівель. LAN зазвичай використовують для спільного використання файлів, принтерів, баз даних та інших ресурсів;

- кампусні мережі (CAN) - це локальні мережі, які об'єднують комп'ютери та інші пристрої в межах одного університету або іншого великого комплексу будівель. CAN зазвичай використовують для спільного використання файлів, принтерів, баз даних, додатків та інших ресурсів;
- мережі міської зони (MAN) - це тип комп'ютерної мережі, яка покриває велику територію, наприклад, місто чи мегаполіс. MAN-мережі зазвичай використовуються для надання доступу до Інтернету, а також для надання інших послуг, таких як відеоконференції та інтегрована передача голосу і тексту;
- глобальні мережі (WAN) - це мережі, які об'єднують комп'ютери та інші пристрої в різних місцях, наприклад, в різних містах або країнах. WAN зазвичай використовують для спільного використання файлів, принтерів, баз даних, додатків та інших ресурсів, а також для надання доступу до Інтернету.

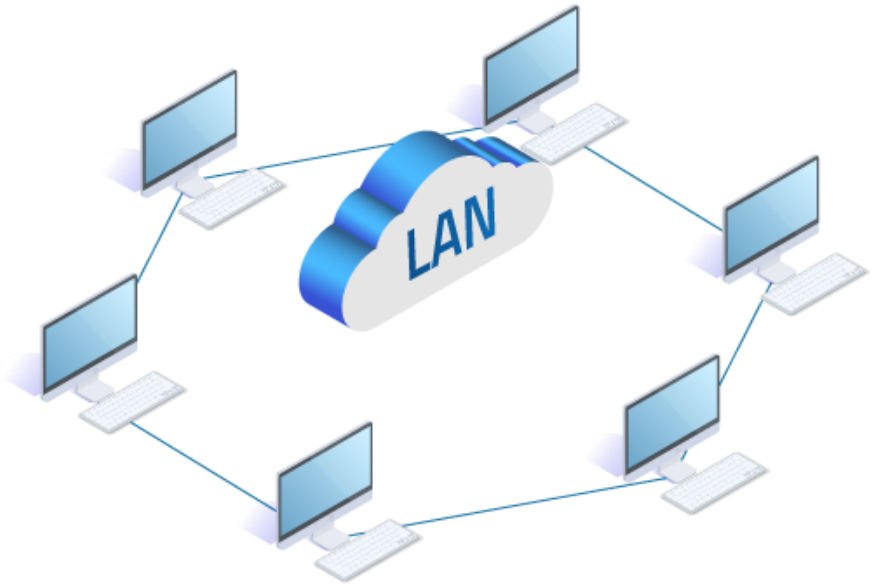

Рисунок 1.1 – Приклад мережі MAN

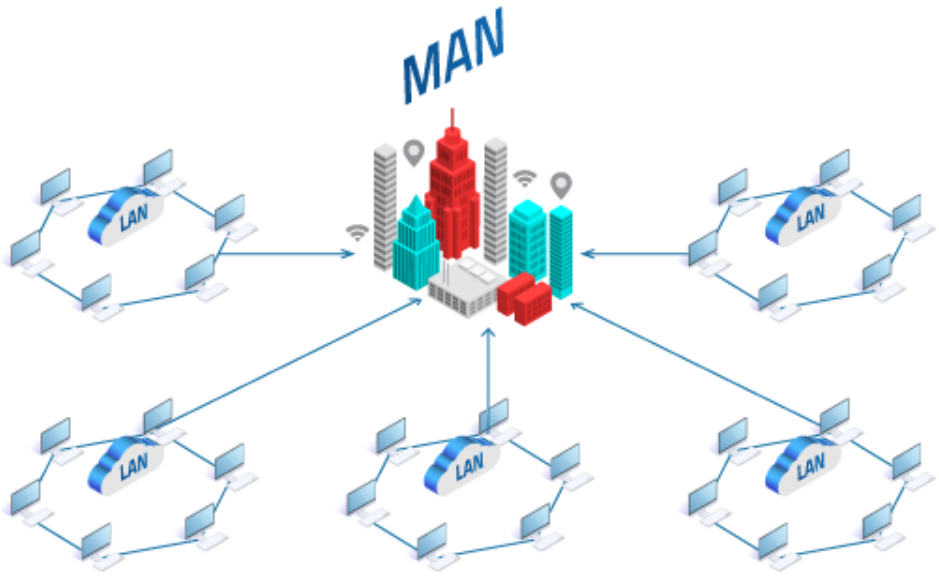

Рисунок 1.2 – Приклад мережі MAN

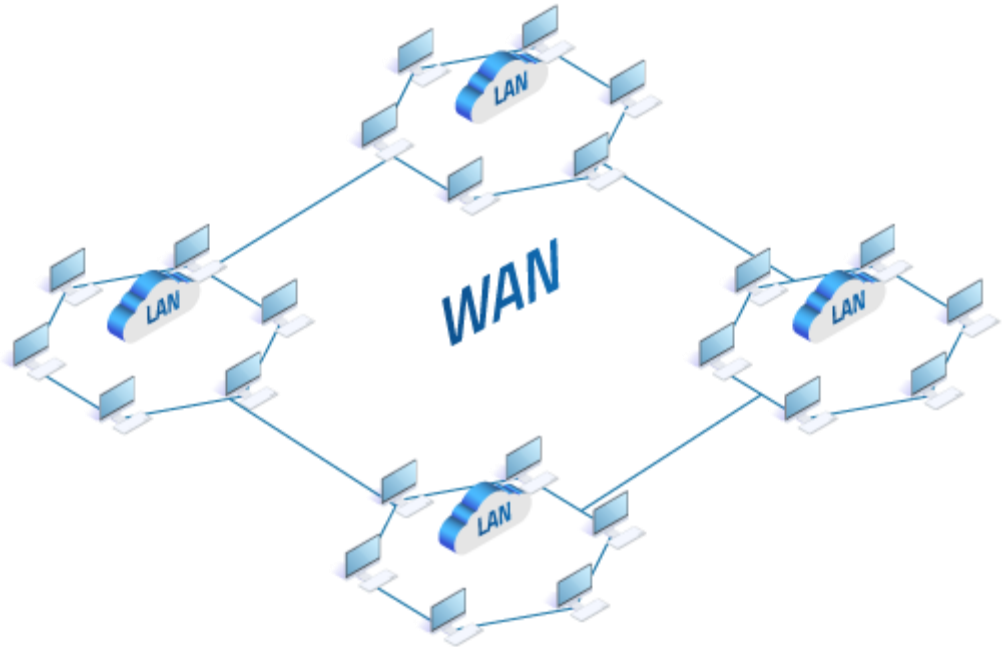

Рисунок 1.3 – Приклад мережі WAN

Топологія - це конфігурація фізичних зв'язків між вузлами мережі. За типом топології комп'ютерні мережі поділяються на:

- кільцева топологія - мережа, в якій комп'ютери з'єднані в кільце. Дані передаються по колу від одного комп'ютера до іншого;
- топологія шина - мережа, в якій комп'ютери з'єднані в одну лінію. Дані передаються по лінії від одного комп'ютера до іншого;

- топологія зірка - мережа, в якій комп'ютери з'єднані з центральним пристроєм, наприклад, з маршрутизатором. Дані передаються від одного комп'ютера до іншого через центральний пристрій;

- мережа з розгалуженим деревом - мережа, яка є комбінацією зіркової та шинної топології;

- мережа з повною зв'язністю - мережа, в якій кожен комп'ютер з'єднаний з кожним іншим комп'ютером.

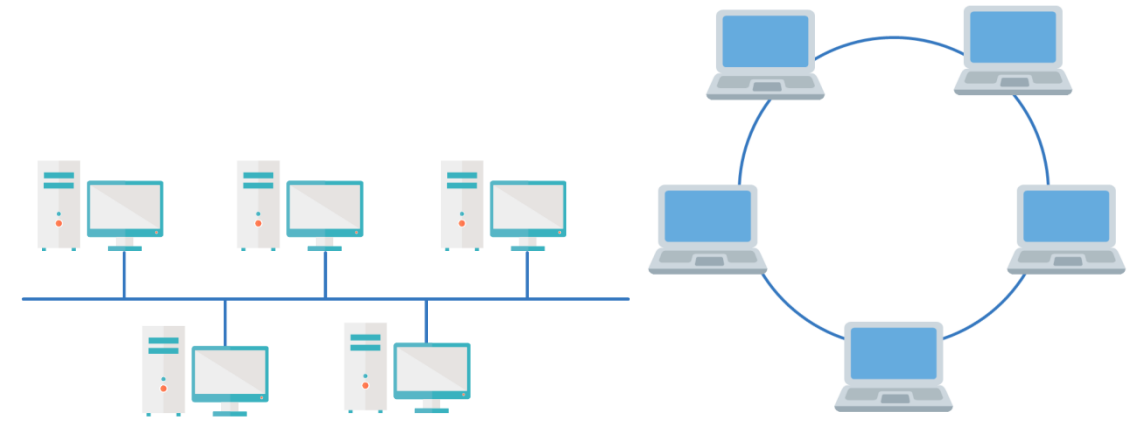

Рисунок 1.4 – Приклади мереж з топологією шина та кільце

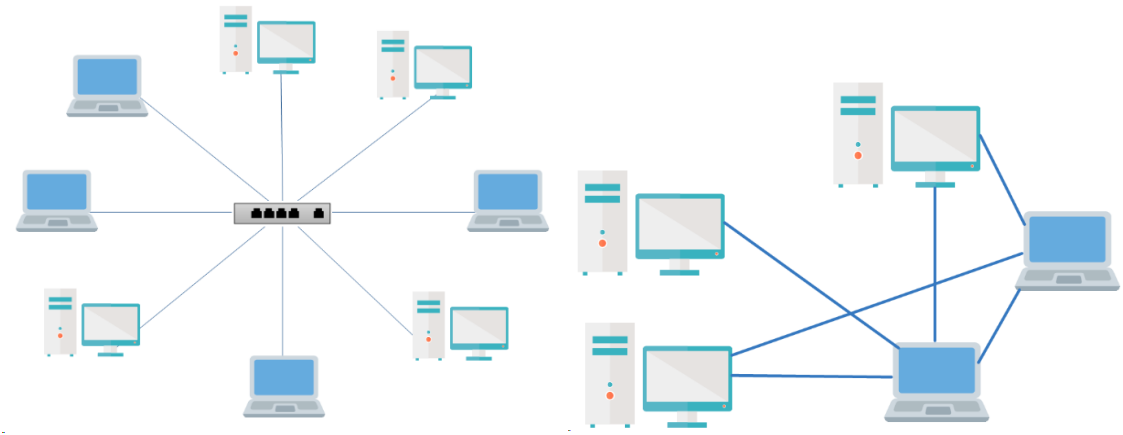

Рисунок 1.5 – Приклади мереж з топологією зірка та зв’язаною

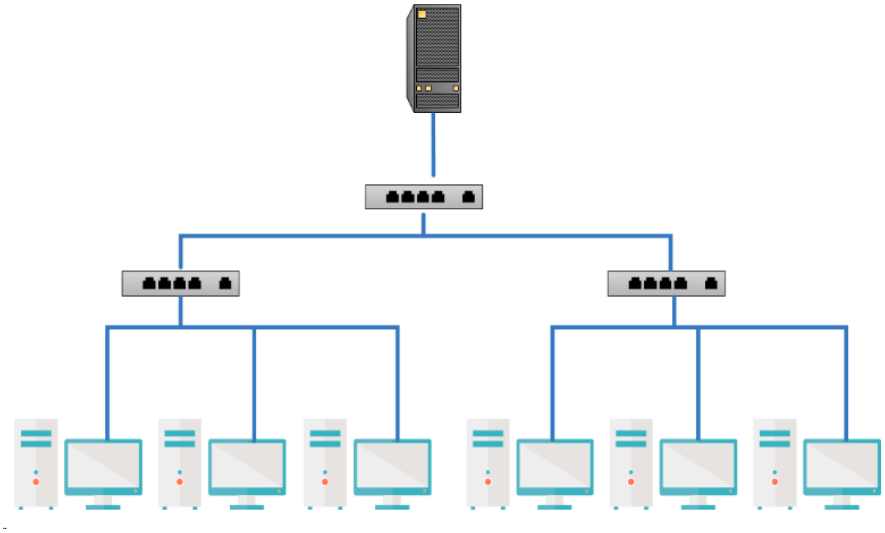

Рисунок 1.6 – Приклад мережі з топологією дерево

За типом протоколу комп'ютерні мережі поділяються на:

- мережі Ethernet - це мережі, які використовують протокол Ethernet для передачі даних. Ethernet є найпоширенішим протоколом для локальних мереж;
- мережі Wi-Fi - це мережі, які використовують протокол Wi-Fi для передачі даних по бездротовому зв'язку. Wi-Fi використовується для створення локальних мереж, а також для доступу до Інтернету;
- мережі Bluetooth - це мережі, які використовують протокол Bluetooth для передачі даних на коротких відстанях. Bluetooth використовується для підключення таких пристроїв, як смартфони, планшети та ноутбуки.

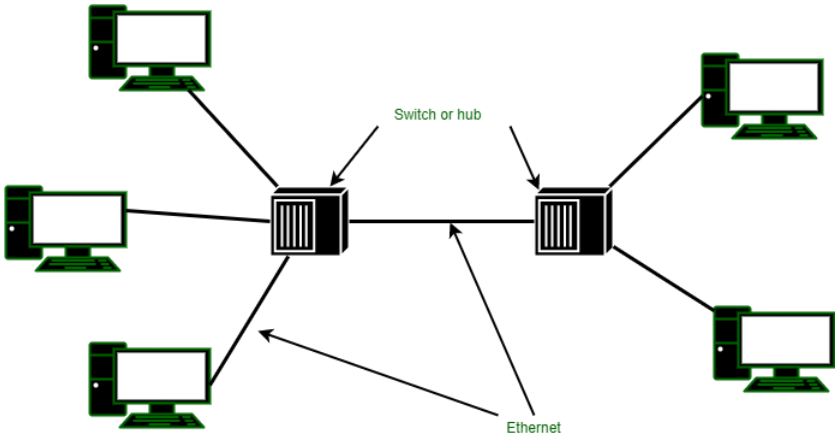

Рисунок 1.7 – Приклад мережі Ethernet

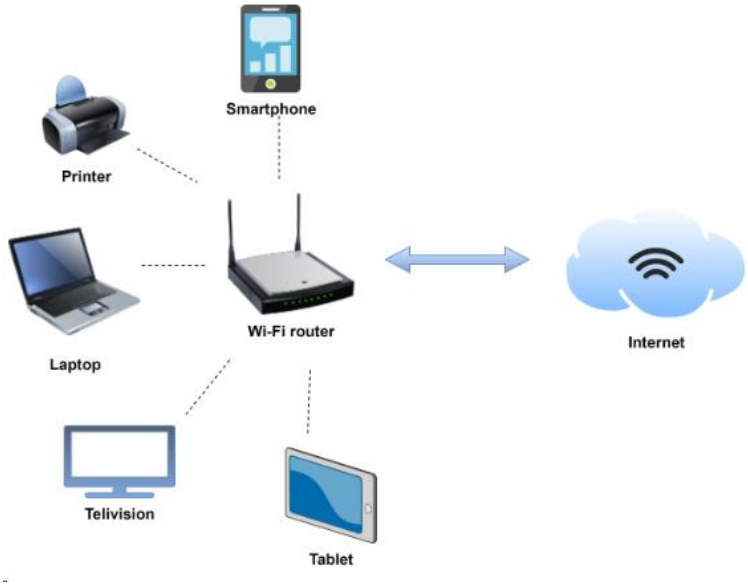

Рисунок 1.8 – Приклад мережі Wi-Fi

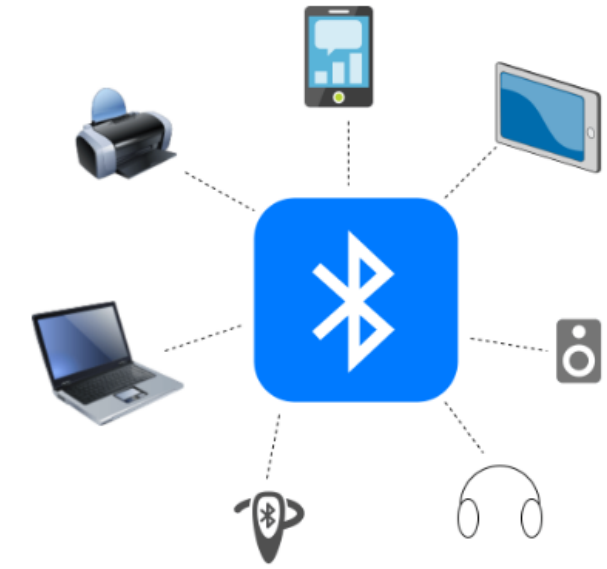

Рисунок 1.9 – Приклад мережі Bluetooth

За типом доступу до мережі комп'ютерні мережі поділяються на:

- публічні мережі - це мережі, до яких може мати доступ будь-хто. Публічні мережі часто використовуються для доступу до Інтернету;
- приватні мережі - це мережі, доступ до яких обмежений певною групою людей. Приватні мережі часто використовуються в бізнесі та освіті.

Віртуальні приватні мережі (VPN) - це технологія, яка дозволяє створювати надійний і захищений зв'язок між комп'ютерами, розташованими в різних мережах. VPN створюється шляхом створення віртуального каналу зв'язку між

комп'ютерами. Цей канал зв'язку захищений за допомогою шифрування, що забезпечує конфіденційність даних, що передаються.

VPN можна використовувати для різних цілей, таких як: віддалений доступ до корпоративних ресурсів, безпека передачі даних, забезпечення конфіденційності.

Рисунок 1.10 – Приклад мережі VPN

Тобто комп’ютерні мережі можна порівнювати за областю дії, за типом топології, за типом протоколу та за типом доступу.

1.2 Компоненти комп’ютерних мереж

Комп'ютерні мережі складаються з різних компонентів, включаючи:

- апаратне забезпечення - це фізичні пристрої, які використовуються для створення мережі, наприклад, комп'ютери, кабелі та маршрутизатори;
- програмне забезпечення - це програми, які керують мережею, наприклад, операційні системи та протоколи мережі.

Комп'ютери є основними пристроями, які використовуються для доступу до мережі. Комп'ютери можуть бути різними, наприклад, настільні комп'ютери, ноутбуки, смартфони та планшети.

Мережеві адаптери - це пристрої, які дозволяють комп'ютерам з'єднуватися з мережею. Мережеві адаптери можуть бути вбудовані в комп'ютери або встановлюватися окремо.

Мережеве обладнання допомагає керувати мережею. Мережеве обладнання включає в себе такі пристрої, як маршрутизатори, комутатори та точки доступу.

Маршрутизатори - це пристрої, які направляють дані по мережі. Маршрутизатори використовуються для з'єднання різних мереж, наприклад, локальних мереж і Інтернету.

Комутатори - це пристрої, які з'єднують комп'ютери в локальній мережі. Комутатори допомагають підвищити швидкість і ефективність передачі даних по локальній мережі.

Точки доступу - це пристрої, які дозволяють комп'ютерам підключатися до мережі по бездротовому зв'язку. Точки доступу використовуються для створення бездротових локальних мереж (WLAN).

Мережеві кабелі забезпечують фізичний зв’язок між комп’ютерами та іншими пристроями. До них відносяться коаксіальні кабелі, виті пари та оптоволоконні кабелі.

Коаксіальні кабелі мають круглий переріз і складаються з двох шарів ізоляції, між якими розташований провідник. Коаксіальні кабелі можуть бути одножильними або багатожильними. Одножильні коаксіальні кабелі мають один провідник, а багатожильні - кілька.

Вити пари складаються з двох ізольованих проводів, які скручені між собою. Виті пари можуть бути неекрановані або екрановані. Неекрановані витої пари не мають додаткової ізоляції, а екрановані - мають додатковий шар ізоляції, який захищає їх від перешкод.

Оптоволоконні кабелі складаються з скляного або пластикового волокна, по якому поширюється світло. Оптоволоконні кабелі забезпечують найвищу швидкість передачі даних, але вони також є найдорожчими.

Операційні системи керують комп'ютерами. Операційні системи забезпечують доступ до мережі, а також управляють мережевими ресурсами, такими як файли, принтери та сервери.

Протоколи мережі визначають, як дані передаються по мережі. Протоколи мережі забезпечують, щоб дані передавалися правильно і без помилок.

Віртуальні приватні мережі VPN працюють за допомогою наступного принципу:

1. клієнтський комп'ютер підключається до VPN-сервера;
2. VPN-сервер шифрує дані, що передаються від клієнтського комп'ютера;
3. шифровані дані передаються через Інтернет;
4. VPN-сервер на іншому кінці каналу зв'язку розшифрує дані.

VPN захищає дані, що передаються, за допомогою шифрування. Для шифрування даних в VPN використовуються різні алгоритми шифрування, такі як AES, RSA та 3DES.

Крім шифрування, для забезпечення безпеки VPN використовуються аутентифікації, яка дозволяє VPN-серверу перевірити, що комп'ютер, який підключається до VPN-з'єднання, є дійсним та ідентифікація, яка дозволяє VPN-серверу визначити, хто підключається до VPN-з'єднання.

Для створення VPN-з'єднання необхідні такі компоненти: VPN-сервер - це комп'ютер, який забезпечує створення і підтримку VPN-з'єднання; VPN-клієнт - це програмне забезпечення, яке встановлюється на комп'ютері, який підключається до VPN-з'єднання; VPN-тунель - це віртуальний канал зв'язку між VPN-сервером і VPN-клієнтом.

Комп'ютерні мережі складаються з різних компонентів, які працюють разом, щоб забезпечити обмін даними між комп'ютерами.

1.3 Порівняння комп’ютерних мереж

Комп'ютерні мережі забезпечують ряд переваг, включаючи зручність, безпеку та доступність.

Зручність означає, що комп'ютерні мережі дозволяють користувачам обмінюватися даними та ресурсами швидко і легко.

Безпека означає, що комп'ютерні мережі можуть використовуватися для захисту даних від несанкціонованого доступу.

Доступність комп'ютерної мережі дозволяє користувачам отримувати доступ до інформації та ресурсів, які знаходяться в інших місцях. Наприклад, користувачі можуть отримати доступ до файлів, які зберігаються на сервері, який знаходиться в іншому місті або навіть в іншій країні.

Комп'ютерні мережі також мають деякі недоліки, включаючи вартість, проблеми з безпекою та складність.

Створення і обслуговування комп'ютерної мережі може бути дорогим. Комп'ютерні мережі можуть бути вразливими до атак. Управління комп'ютерною мережею може бути складним завданням.

Незважаючи на ці недоліки, комп'ютерні мережі є важливим компонентом сучасного суспільства.

Основні відмінності між комп'ютерними мережами:

- область дії - персональні мережі мають найменшу область дії, а глобальні мережі - найбільшу.
- розмір - персональні мережі мають найменший розмір, а глобальні мережі - найбільший.
- швидкість передачі даних - глобальні мережі зазвичай мають найвищу швидкість передачі даних, а персональні мережі - найнижчу.
- безпека - глобальні мережі зазвичай є найбільш вразливими до атак зловмисників, а персональні мережі - найменш вразливими.
- вартість - глобальні мережі зазвичай є найбільш дорогими, а персональні мережі - найдешевшими.
- складність - глобальні мережі зазвичай є найбільш складними в використанні та адмініструванні, а персональні мережі - найпростішими.

У таблиці 1.1 подано порівняння комп'ютерних мереж за різними параметрами.

Таблиця 1.1 - Порівняння комп'ютерних мереж за різними параметрами

Параметр	Персональні мережі (PAN)	Локальні мережі (LAN)	Кампусні мережі (CAN)	Глобальні мережі (WAN)
Область дії	В межах однієї кімнати або невеликого приміщення	В межах одного будівлі або невеликого комплексу будівель	В межах одного університету або іншого великого комплексу будівель	Між різними місцями, наприклад, в різних містах або країнах
Розмір	Невеликий	Середній	Великий	Дуже великий
Швидкість передачі даних	Середня	Висока	Дуже висока	Висока
Безпека	Низька	Середня	Висока	Висока
Вартість	Низька	Середня	Висока	Дуже висока
Складність	Проста	Складна	Дуже складна	Дуже складна
Приклади	Домашня мережа, мережа для спільного використання файлів і принтерів	Корпоративна мережа, мережа для спільного використання ресурсів і додатків	Університетська мережа, мережа для надання доступу до ресурсів і додатків	Інтернет, глобальна мережа для надання доступу до інформації і ресурсів

Вибір типу комп’ютерної мережі залежить від таких факторів, як масштаб мережі, топологія мережі, тип передавання даних, протоколи мережі та інші.

Для локальних мереж, які об’єднують комп’ютери, розташовані в одному місці, зазвичай використовуються зв’язні топології, такі як зіркова або шинна. Для глобальних мереж, які об’єднують комп’ютери, розташовані в різних місцях, зазвичай використовуються зв’язні топології, такі як зіркова або кільцева. Для віртуальних приватних мереж (VPN) можна використовувати будь-яку топологію.

Для локальних мереж, які мають невелику кількість комп’ютерів, зазвичай використовуються протоколи Ethernet або Token Ring. Для локальних мереж, які мають велику кількість комп’ютерів, зазвичай використовуються протоколи Ethernet або Wi-Fi. Для глобальних мереж зазвичай використовуються протоколи Ethernet або Wi-Fi.

При виборі типу комп’ютерної мережі необхідно враховувати всі фактори, які впливають на роботу мережі.

1.4 Конфігурація мережі

Конфігурація мережі - це набір параметрів, які визначають, як мережа працює. Конфігурація мережі включає в себе такі параметри, як:

- тип мережі - локальна мережа (LAN), мережа широкомасштабного доступу (WAN) або інший тип мережі.
- топологія мережі - кільцева топологія, шина, зірка або інша топологія.
- протоколи мережі - протоколи, які використовуються для передачі даних по мережі.
- адресація мережі - система адресації, яка використовується для ідентифікації пристроїв у мережі.
- безпека мережі - заходи безпеки, які використовуються для захисту мережі від несанкціонованого доступу.

Конфігурація мережі може бути налаштована вручну або автоматично. Ручне налаштування мережі дозволяє більш точно налаштувати мережу відповідно до конкретних потреб. Автоматичне налаштування мережі спрощує процес налаштування мережі, але може не забезпечити такий високий рівень контролю, як ручне налаштування.

Конфігурація мережі може бути змінена в будь-який час. Наприклад, якщо мережа росте або змінюються потреби користувачів, може знадобитися змінити конфігурацію мережі.

До основних завдань, які можуть виконуватися в рамках конфігурації мережі можна віднести:

- підключення пристроїв до мережі - це завдання включає в себе підключення пристроїв до мережі за допомогою кабелів або бездротового зв'язку.
- налаштування адресації мережі - це завдання включає в себе призначення IP-адрес, MAC-адрес та інших адрес пристроям у мережі.
- налаштування протоколів мережі - це завдання включає в себе налаштування протоколів, які використовуються для передачі даних по мережі.
- налаштування безпеки мережі - це завдання включає в себе налаштування заходів безпеки, які використовуються для захисту мережі від несанкціонованого доступу.

Конфігурація мережі є важливим завданням для будь-якої мережі. Правильна конфігурація мережі забезпечує ефективну роботу мережі та захист даних.

Конфігурацію мережі необхідно оптимізувати. Це включає в себе вибір оптимальних параметрів для мережевих пристроїв, таких як маршрутизатори, комутатори та точки доступу.

1.5 Обслуговування мережі

Обслуговування мережі - це комплекс заходів, які виконуються для забезпечення безперебійної роботи мережі та захисту даних. Обслуговування мережі включає в себе такі завдання, як:

- конфігурація мережі - це завдання включає в себе налаштування параметрів мережі, таких як тип мережі, топологія мережі, протоколи мережі та адресація мережі.
- підтримка обладнання мережі - це завдання включає в себе перевірку стану обладнання мережі, усунення неполадок та заміну несправного обладнання.
- безпека мережі - це завдання включає в себе налаштування заходів

безпеки, які використовуються для захисту мережі від несанкціонованого доступу.

- резервне копіювання даних - це завдання включає в себе створення резервних копій даних для захисту від втрати даних.

Обслуговування мережі є важливим завданням для будь-якої мережі. Правильне обслуговування мережі забезпечує ефективну роботу мережі та захист даних.

Перелічимо деякі конкретні завдання, які можуть виконуватися в рамках обслуговування мережі:

- щоденне обслуговування - це завдання включає в себе перевірку стану мережі та усунення дрібних неполадок.
- щотижневе обслуговування - це завдання включає в себе більш ретельну перевірку стану мережі та усунення більш серйозних неполадок.
- щомісячне обслуговування - це завдання включає в себе оновлення програмного забезпечення та драйверів, а також проведення тестових випробувань мережі.
- річна перевірка - це завдання включає в себе повний огляд мережі та усунення будь-яких проблем, які можуть бути виявлені.

Частота виконання цих завдань залежить від розміру мережі та її складності. Для невеликих мереж може бути достатньо щоденного обслуговування. Для великих мереж може знадобитися щоденне, щотижневе, щомісячне та щорічне обслуговування.

Обслуговування мережі може виконуватися штатними співробітниками або аутсорсинговою компанією. Вибір методу обслуговування залежить від розміру мережі, її складності та бюджету.

Необхідно забезпечити належне обслуговування мережі. Це включає в себе регулярне оновлення програмного та апаратного забезпечення, а також усунення неполадок.

2 ПОКАЗНИКИ ЕФЕКТИВНОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Ефективність комп'ютерної мережі

Ефективність комп'ютерної мережі — це міра того, наскільки добре мережа виконує свої функції. Ефективність залежить від багатьох факторів, насамперед продуктивності, надійності, безпеки мережі. Ефективність мережі визначається тим, як швидко, надійно і безпечно вона може передавати дані, забезпечувати доступ до ресурсів і захищати дані від несанкціонованого доступу.

Продуктивність мережі визначається її здатністю передавати дані за одиницю часу. Продуктивність мережі залежить від таких факторів, як тип мережі, пропускна здатність мережі, типи використовуваних протоколів та інші.

Надійність мережі визначається її здатністю забезпечувати безперервність роботи. Надійність мережі залежить від таких факторів, як якість обладнання, надійність мережевих протоколів, наявність резервних систем та інші.

Безпека мережі визначається її здатністю захищати дані від несанкціонованого доступу. Безпека мережі залежить від таких факторів, як тип використовуваних протоколів, наявність засобів захисту, політика безпеки та інші.

Додатково можна виділити такі фактори як затримка та втрати даних.

Затримка мережі — це час, який потрібен для передачі даних від одного пристрою до іншого в мережі. Затримка визначається відстанню між пристроями, типом мережі, типом обладнання, навантаженням на мережу та іншими.

Втрати даних — це неможливість отримати доступ до даних у їх звичайному місцерозташуванні та за допомогою звичайних програмних засобів внаслідок помилок у програмному/апаратному забезпеченні або необачних дій користувача.

Для підвищення ефективності комп'ютерної мережі необхідно враховувати всі фактори, які впливають на її роботу. Вибір оптимальних рішень для кожного з цих факторів дозволить створити ефективну комп'ютерну мережу, яка буде

відповідати поставленим завданням. Надалі розглянемо кожен з цих факторів докладніше.

2.2 Продуктивність

Продуктивність - це міра того, як ефективно мережа може передавати дані.

На продуктивність мережі впливають такі фактори:

- тип мережі - локальні мережі (LAN) зазвичай мають більш високу продуктивність, ніж мережі широкомасштабного доступу (WAN).
- топологія мережі - мережі з повною зв'язністю мають більш високу продуктивність, ніж мережі з іншою топологією.
- протоколи мережі - деякі протоколи мережі, такі як Ethernet, мають більш високу продуктивність, ніж інші протоколи.
- обладнання мережі - використання високоякісного обладнання мережі може підвищити продуктивність мережі.
- завантаженість мережі - чим більше пристроїв підключено до мережі, тим нижче продуктивність мережі.
- відстань між відправником і одержувачем - чим далі знаходяться відправник і одержувач, тим більше часу буде потрібно для передачі даних.
- якість каналу – чим гірше канал, тим менше продуктивність мережі.
- пропускна здатність мережі, яка визначається максимальним обсягом даних, що може бути передано мережею за одиницю часу.

Продуктивність мережі можна покращити за допомогою таких заходів:

1) використання високоякісного обладнання мережі - використання високоякісного обладнання мережі, такого як маршрутизатори та комутатори, може підвищити продуктивність мережі.

2) усунення неполадок - усунення неполадок в мережі, таких як перевантажені пристрої або несправні кабелі, може підвищити продуктивність мережі.

3) зменшення навантаження на мережу - зменшення навантаження на мережу, наприклад, шляхом використання бездротових мереж або хмарних технологій, може підвищити продуктивність мережі.

Продуктивність мережі визначається її здатністю передавати дані, обробляти запити і забезпечувати надійний доступ до ресурсів. Вона може бути виміряна за допомогою таких показників, як пропускна здатність, завантаження мережі, час відповіді на запити, швидкість передачі даних і т.д. Збільшення продуктивності мережі може бути досягнуто шляхом оптимізації конфігурації обладнання, використання більш швидких комунікаційних протоколів, впровадження технологій віртуалізації та удосконаленням програмного забезпечення для управління мережею.

Продуктивність мережі є важливою характеристикою для будь-якої мережі. Продуктивна мережа забезпечує швидкий і надійний доступ до даних і ресурсів.

2.3 Затримка

Затримка - це час, який потрібен даним для проходження по мережі. Затримка може бути виміряна в мілісекундах або мікросекундах.

Затримка мережі може бути викликана такими факторами:

- розмір пакета - чим більший пакет, тим довше він буде передаватися по мережі.
- тип мережі - локальні мережі (LAN) зазвичай мають більш низьку затримку, ніж мережі широкомасштабного доступу (WAN).
- топологія мережі - мережі з повною зв'язністю мають більш низьку затримку, ніж мережі з іншою топологією.
- протоколи мережі - деякі протоколи мережі, такі як Ethernet, мають більш низьку затримку, ніж інші протоколи.
- обладнання мережі - використання високоякісного обладнання мережі може зменшити затримку мережі.
- завантаженість мережі - чим більше пристроїв підключено до мережі,

тим вища затримка мережі.

Затримка мережі може впливати на відчуття часу (затримка мережі може призвести до відчуття затримки в часі, наприклад, при відтворенні відео або геймінгу) та якість обслуговування (затримка мережі може призвести до зниження якості обслуговування (QoS), наприклад, при передачі чутливих до часу даних).

Затримку мережі можна зменшити за допомогою таких заходів:

1) використання високоякісного обладнання мережі - використання високоякісного обладнання мережі, такого як маршрутизатори та комутатори, може зменшити затримку мережі.

2) усунення неполадок - усунення неполадок в мережі, таких як перевантажені пристрої або несправні кабелі, може зменшити затримку мережі.

3) зменшення навантаження на мережу - зменшення навантаження на мережу, наприклад, шляхом використання бездротових мереж або хмарних технологій, може зменшити затримку мережі.

Затримка мережі є важливою характеристикою для будь-якої мережі. Затримка мережі може впливати на роботу мережевих додатків і сервісів., на продуктивність мережі та якість обслуговування користувачів, тому важливо аналізувати та оптимізувати її для забезпечення ефективної роботи мережі.

2.4 Втрати даних

Втрати даних - це кількість даних, які втрачаються під час передачі по мережі. Втрати даних вимірюються у відсотках.

Втрати даних мережі може бути викликана різними факторами, включаючи:

- пошкодження мережевого обладнання, такого як кабелі, маршрутизатори або комутатори, може призвести до втрати даних.
- несправність програмного забезпечення, яке використовується в мережі, може призвести до втрати даних.
- зловмисні дії, такі як хакерство або шкідливе програмне забезпечення, можуть призвести до втрати даних.

- природні явища, такі як повені, пожежі або грози, можуть призвести до втрати даних.

Втрати даних мережі може мати серйозні наслідки, включаючи:

- втрати даних можуть призвести до втрати важливої інформації, наприклад, фінансових даних, медичних записів або особистих файлів.
- втрати даних можуть призвести до переривання роботи бізнесу, наприклад, якщо дані, необхідні для роботи бізнесу, будуть втрачені.
- втрати даних можуть призвести до зниження продуктивності, наприклад, якщо співробітники будуть витрачати час на відновлення втрачених даних.

Щоб мінімізувати ризик втрати даних мережі, важливо вжити заходів для захисту мережі, таких як:

1) регулярне резервне копіювання даних є одним з найкращих способів захисту від втрати даних.

2) використання сучасного обладнання яке відповідає найостаннішим стандартам безпеки, може допомогти захистити мережу від втрат даних.

3) встановлення брандмауера може допомогти захистити мережу від зловмисних дій.

4) оновлення програмного забезпечення може допомогти усунути вразливості, які можуть бути використані для атаки на мережу.

Великі втрати даних можуть призвести до погіршення продуктивності та якості обслуговування в мережі. Для вимірювання втрат даних часто використовують такі параметри, як Packet Loss Rate (відсоток втрат пакетів) чи Bit Error Rate (відсоток помилок бітів).

Для вирішення проблем втрат даних можуть використовуватися різні методи та технології, такі як корекція помилок, використання буферів, оптимізація маршрутизації, використання протоколів, що контролюють потік, та інші.

2.5 Надійність

Надійність - це ймовірність того, що мережа буде працювати безперебійно. Надійність можна виміряти в відсотках. Надійність об'єкта є комплексною властивістю, її оцінюють за чотирма показниками – безвідмовністю, довговічністю, ремонтопридатністю і зберіганням або за поєднанням цих властивостей.

На надійність мережі впливають такі фактори:

- тип мережі - локальні мережі (LAN) зазвичай більш надійні, ніж мережі широкомасштабного доступу (WAN).
- топологія мережі - мережі з повною зв'язністю більш надійні, ніж мережі з іншою топологією.
- протоколи мережі - деякі протоколи мережі, такі як Ethernet, більш надійні, ніж інші протоколи.
- обладнання мережі - використання надійного обладнання мережі може підвищити надійність мережі.
- завантаженість мережі - чим менше пристроїв підключено до мережі, тим вища надійність мережі.

Надійність мережі можна підвищити за допомогою таких заходів:

- використання надійного обладнання мережі, такого як маршрутизатори та комутатори, може підвищити надійність мережі.
- регулярне обслуговування мережі, включаючи оновлення програмного забезпечення та усунення неполадок, може підвищити надійність мережі.
- забезпечення резервування, наприклад, шляхом використання резервних маршрутизаторів або комутаторів, може підвищити надійність мережі.

Надійність мережі є важливою характеристикою для будь-якої мережі. Надійна мережа забезпечує безперебійну роботу бізнесу та захист даних.

Для підвищення надійності мережі можна виконувати наступні дії:

1) використання джерела безперебійного живлення (ДБЖ) може забезпечити резервне живлення для мережевого обладнання в разі відключення електроенергії.

2) використання резервних каналів зв'язку може забезпечити альтернативний шлях для передачі даних у разі відмови основного каналу зв'язку.

3) використання протоколів виявлення відмов та відновлення можуть допомогти мережі відновитися після відмови пристрою або каналу зв'язку.

Вибір конкретних заходів для підвищення надійності мережі залежить від типу мережі, розміру мережі та конкретних потреб. Надійність мережі може бути підтримана за допомогою резервування обладнання, застосування технологій виявлення та усунення несправностей, а також правильного налаштування мережевих пристроїв. Надійність мережі є важливим аспектом її функціонування, оскільки вона впливає на безперебійну роботу бізнес-процесів та задоволення потреб користувачів.

2.6 Безпека

Безпека - це здатність мережі захистити дані від несанкціонованого доступу, випадкового або навмисного втручання в роботу мережі або спроб руйнування її компонентів. Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу.

Безпеку можна оцінити за допомогою таких показників, як кількість інцидентів безпеки, кількість виявлених загроз та кількість даних, які були захищені.

Основні загрози безпеці мережі:

- несанкціонований доступ - це ситуація, коли користувач отримує доступ до мережі без дозволу. Несанкціонований доступ може бути використаний для крадіжки даних, руйнування даних або перехоплення даних.
- зловмисне програмне забезпечення - це програмне забезпечення, яке розроблено з метою завдати шкоди мережі або її користувачам. Зловмисне програмне забезпечення може бути використано для крадіжки даних, руйнування даних або перехоплення даних.
- фішинг - це техніка соціальної інженерії, яка використовується для обману

користувачів і отримання їхніх конфіденційних даних, таких як паролі або номери кредитних карток.

- спам - це несанкціонована розсилка електронних листів, які часто містять шкідливе програмне забезпечення або інші загрози.
- атаки DDoS - це атаки, які спрямовані на перевантаження мережі або веб-сайту, щоб зробити їх недоступними.

Щоб захистити мережу від цих загроз, важливо вжити таких заходів:

- використання брандмауера - брандмауер є першою лінією захисту мережі від несанкціонованого доступу.
- використання антивірусного програмного забезпечення - антивірусне програмне забезпечення допомагає захистити мережу від зловмисного програмного забезпечення.
- використання фільтрів спаму - фільтри спаму допомагають захистити мережу від спаму.
- оновлення програмного забезпечення часто включають виправлення вразливостей, які можуть бути використані для атаки на мережу.
- обізнаність користувачів - важливо, щоб користувачі були обізнані про потенційні загрози безпеці мережі і знали, як захистити себе.

Важливо також регулярно проводити аудит безпеки мережі, щоб виявити будь-які потенційні проблеми. Аудит безпеки мережі включає в себе перевірку обладнання, програмного забезпечення, даних і персоналу.

До заходів, які можуть бути використані для захисту мережі, відносять:

1) використання складних паролів - складні паролі важче зламати.
2) використання двофакторної аутентифікації (2FA) - 2FA додає додатковий рівень безпеки, вимагаючи від користувача ввести код з мобільного телефону.
3) використання шифрування - шифрування даних допомагає захистити їх від несанкціонованого доступу.
4) використання фізичних заходів безпеки, таких як контроль доступу і камери відеоспостереження, також може допомогти захистити мережу.

Безпека мережі є постійною боротьбою, оскільки зловмисники постійно розробляють нові методи для атаки на мережі. Адміністратори мереж повинні постійно переглядати свої заходи безпеки, щоб забезпечити захист мережі від останніх загроз.

3 ПОРІВНЯННЯ МЕТОДІВ ОЦІНКИ ЕФЕКТИВНОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Тестування продуктивності

Для оцінки ефективності комп'ютерної мережі можна використовувати різні інструменти та методики.

Тестування продуктивності - це метод оцінки продуктивності мережі шляхом генерації штучного навантаження на мережу.

Тестування продуктивності мережі проводиться для визначення того, чи може мережа підтримувати необхідне навантаження.

Тестування продуктивності мережі може проводитися для різних цілей, таких як:

- оцінка продуктивності мережі після внесення змін - наприклад, після встановлення нового обладнання або оновлення програмного забезпечення.
- планування майбутніх потреб - наприклад, для визначення того, чи потрібно буде збільшити пропускну здатність мережі.
- виявлення проблем із продуктивністю - наприклад, для виявлення вузьких місць у мережі.

Тестування продуктивності мережі може проводитися за допомогою різних методів, таких як:

- синтетичні тести - це метод, при якому на мережу навмисно навантажується штучне навантаження для оцінки продуктивності мережі.
- функціональні тести - це метод, при якому вимірюється пропускна здатність мережі під час реального використання.

Тестування дозволяє виявити проблеми з продуктивністю мережі на ранніх етапах, допомагає визначити, які зміни можна внести в мережу для підвищення продуктивності, покращує якість обслуговування користувачів.

Тестування продуктивності мережі може бути складним завданням, і для його проведення часто використовуються спеціальні інструменти.

У процесі тестування можуть використовуватися різноманітні інструменти для вимірювання різних параметрів мережі, такі як iperf, Wireshark, та інші.

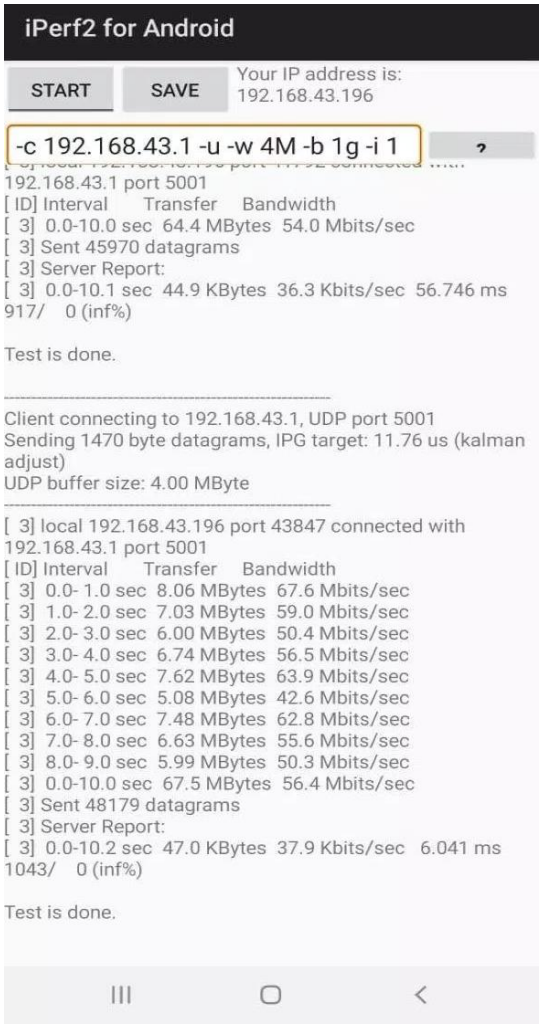

Рисунок 3.1 – Інтерфейс додатка iperf

```
Connecting to host localhost, port 5201
[  5] local ::1 port 44422 connected to ::1 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  46.7 MBytes   392 Mbits/sec    0    320 KBytes
[  5]   1.00-2.00   sec  42.7 MBytes   359 Mbits/sec    0    320 KBytes
[  5]   2.00-3.00   sec  41.8 MBytes   350 Mbits/sec    0    320 KBytes
[  5]   3.00-4.00   sec  41.1 MBytes   345 Mbits/sec    0    320 KBytes
[  5]   4.00-5.00   sec  40.3 MBytes   338 Mbits/sec    0    320 KBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-5.00   sec   213 MBytes   357 Mbits/sec    0             sender
[  5]   0.00-5.00   sec   211 MBytes   354 Mbits/sec                  receiver


iperf Done.
```

Рисунок 3.2 – Приклад роботи iperf (вимірювання продуктивності)

```
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  5]   0.00-10.04  sec   119 MBytes  99.8 Mbits/sec  0.000 ms  0/85789 (0%)
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
iperf3: interrupt - the server has terminated

C:\Users\ttiller\Downloads\iperf-3.1.3-win64>iperf3 -c 192.168.1.122 -b 100M -R -u
Connecting to host 192.168.1.122, port 5201
Reverse mode, remote host 192.168.1.122 is sending
[  4] local 192.168.1.111 port 52151 connected to 192.168.1.122 port 5201
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-1.00   sec  12.1 MBytes   102 Mbits/sec  0.059 ms  52/1604 (3.2%)
[  4]   1.00-2.00   sec  11.9 MBytes   100 Mbits/sec  0.059 ms  0/1527 (0%)
[  4]   2.00-3.00   sec  11.9 MBytes   100 Mbits/sec  0.059 ms  0/1525 (0%)
[  4]   3.00-4.00   sec  11.9 MBytes  99.9 Mbits/sec  0.072 ms  0/1525 (0%)
[  4]   4.00-5.00   sec  11.9 MBytes   100 Mbits/sec  0.093 ms  0/1526 (0%)
[  4]   5.00-6.00   sec  11.9 MBytes   100 Mbits/sec  0.091 ms  0/1527 (0%)
[  4]   6.00-7.00   sec  11.9 MBytes   100 Mbits/sec  0.058 ms  0/1525 (0%)
[  4]   7.00-8.00   sec  11.9 MBytes   100 Mbits/sec  0.052 ms  0/1526 (0%)
[  4]   8.00-9.00   sec  11.9 MBytes   100 Mbits/sec  0.047 ms  0/1526 (0%)
[  4]   9.00-10.00  sec  11.9 MBytes   100 Mbits/sec  0.057 ms  0/1526 (0%)
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-10.00  sec   120 MBytes   101 Mbits/sec  0.057 ms  52/15337 (0.34%)
[  4] Sent 15337 datagrams

iperf Done.

C:\Users\ttiller\Downloads\iperf-3.1.3-win64>
```

Рисунок 3.3 – Приклад роботи iperf (вимірювання смуги частот, джиттера та відсотка втрат)

В рамках тестування продуктивності мережі можуть бути оцінені пропускна здатність мережі, затримка мережі, втрати даних.

Результати тестування продуктивності мережі можуть бути використані для прийняття рішень про те, як покращити продуктивність мережі.

3.2 Аналіз трафіку

Методика аналізу трафіку - це метод оцінки ефективності мережі шляхом аналізу реального трафіку, що проходить по мережі.

Аналіз трафіку може використовуватися для різних цілей, таких як:

- виявлення проблем із мережею - наприклад, для виявлення атак, перевантаження мережі або інших проблем.
- планування мережі - наприклад, для визначення того, чи потрібно збільшити пропускну здатність мережі або додати нові ресурси.
- удосконалення мережі - наприклад, для підвищення продуктивності мережі або зменшення затримки.

Аналіз трафіку може бути розділений на два основних типи:

- сигнатурний аналіз - це метод аналізу трафіку, який використовує попередньо визначені шаблони (сигнатури) для виявлення атак або інших проблем.
- аномальний аналіз - це метод аналізу трафіку, який шукає відхилення від нормального поведінки мережі.

Сигнатурний аналіз є більш ефективним для виявлення відомих атак, але він може бути неефективним для виявлення нових або невідомо атак. Аномальний аналіз є більш ефективним для виявлення невідомих атак, але він може бути менш ефективним для виявлення відомих атак.

Аналіз трафіку може проводитися за допомогою різних інструментів, таких як:

- пакетні аналізатори - це інструменти, які дозволяють переглядати і аналізувати пакети даних, які передаються по мережі.
- аналізатори потоку - це інструменти, які дозволяють переглядати і аналізувати потоки даних, які передаються по мережі.
- системи виявлення вторгнень (IDS) - це системи, які автоматично виявляють атаки на мережу.

Методика аналізу трафіку залежить від цілей аналізу. Для виявлення відомих атак можна використовувати сигнатурний аналіз з використанням пакетних аналізаторів. Для виявлення невідомих атак можна використовувати аномальний аналіз з використанням аналізаторів потоку або систем виявлення вторгнень.

Основні етапи методики аналізу трафіку:

1) збір даних - на цьому етапі збираються дані для аналізу. Дані для аналізу трафіку можуть бути зібрані за допомогою різних методів, таких як:

   а) протоколювання - це метод, при якому записуються всі пакети даних, які передаються по мережі.

   б) спостереження - це метод, при якому використовується спеціальне обладнання для перехоплення трафіку.

2) фільтрація даних - на цьому етапі дані фільтруються, щоб видалити непотрібні або неважливі дані.

3) аналіз даних - на цьому етапі дані аналізуються для виявлення проблем або аномалій.

4) повідомлення про результати - на цьому етапі результати аналізу повідомляються користувачам.

Методика аналізу трафіку може включати в себе використання різноманітних інструментів, таких як:

- Wireshark: цей інструмент дозволяє перехоплювати та аналізувати пакети даних, що проходять через мережу. Він надає докладну інформацію про різні аспекти трафіку.
- NetFlow або IPFIX: ці протоколи забезпечують можливість збору та аналізу статистики трафіку на рівні роутерів та комутаторів.
- SNMP (Simple Network Management Protocol): використовується для моніторингу та управління мережевими пристроями, зокрема для отримання інформації про їхню використану пропускну здатність.
- апаратні монітори мережі: деякі мережеві пристрої та комутатори можуть надавати вбудовані інструменти для моніторингу трафіку.
- аналітика трафіку в реальному часі: включає в себе різні інструменти,

які дозволяють слідкувати за трафіком в реальному часі та виявляти аномалії.

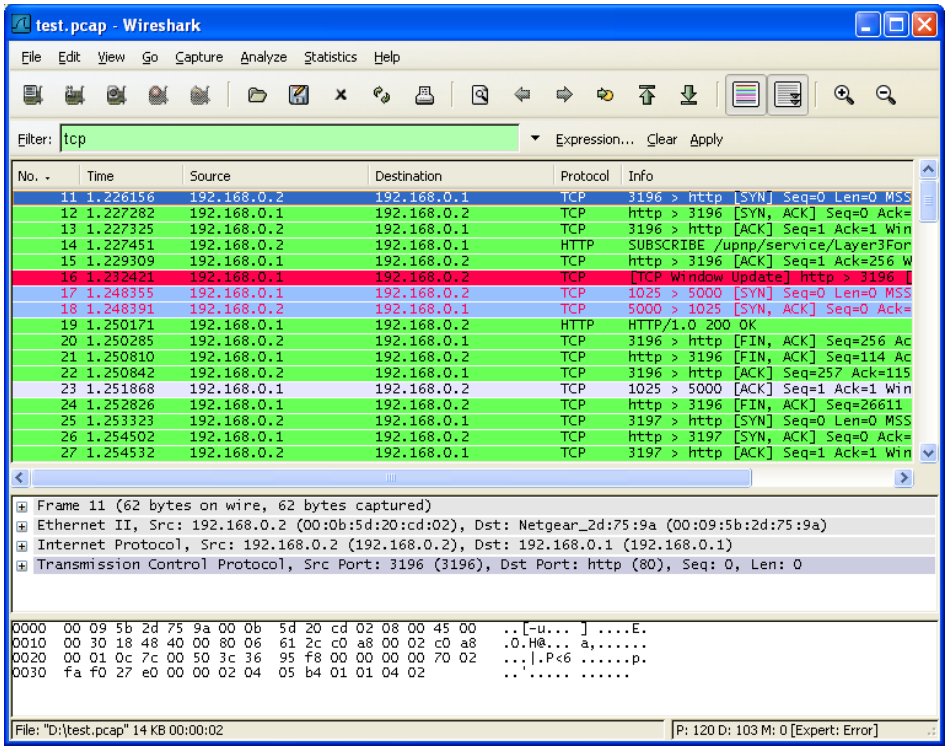

Рисунок 3.4 – Приклад роботи інструменту Wireshark

Використання цих інструментів дозволяє здійснювати глибокий аналіз мережевого трафіку, ідентифікувати проблеми, вдосконалювати конфігурацію та оптимізувати продуктивність мережі.

3.3 Моделювання мережі

Методика моделювання мережі - це метод оцінки ефективності мережі шляхом створення моделі мережі та симуляції її роботи.

Модель мережі - це абстрактне представлення реальної мережі, яке використовується для дослідження поведінки мережі.

Моделювання мережі може використовуватися для різних цілей, таких як:

- планування мережі - наприклад, для визначення того, чи потрібно збільшити пропускну здатність мережі або додати нові ресурси.
- удосконалення мережі - наприклад, для підвищення продуктивності мережі або зменшення затримки.

- дослідження нових технологій - наприклад, для дослідження впливу нових технологій на поведінку мережі.

Методика моделювання мережі може бути розділена на три основних типи:

- аналітичний метод - це метод моделювання мережі, який використовує математичні моделі для дослідження поведінки мережі.
- імітаційне моделювання - це метод моделювання мережі, який використовує комп'ютерну програму для відтворення поведінки мережі.
- емпіричний метод - це метод використовує дані про реальну мережу для створення моделі мережі.

Аналітичний метод є більш точним, ніж імітаційне моделювання, але він може бути менш практичним для складних мереж. Імітаційне моделювання є менш точним, ніж аналітичний метод, але воно може бути більш практичним для складних мереж.

Модель мережі може бути представлена на різних рівнях деталізації:

- фізичний рівень - це рівень, який представляє фізичні компоненти мережі, такі як кабелі, пристрої та канали зв'язку.
- логічний рівень - це рівень, який представляє логічну структуру мережі, наприклад, топологію мережі та протоколи мережі.
- прикладний рівень - це рівень, який представляє прикладні програми, які використовують мережу.

Вибір рівня деталізації залежить від цілей моделювання. Для планування мережі може бути достатньо моделі на фізичному або логічному рівні. Для дослідження нових технологій може знадобитися модель на прикладному рівні.

При моделюванні мережі виконують такі етапів:

1. вибір методу моделювання - на цьому етапі вибирається метод моделювання, який буде використовуватися.
2. розробка моделі - на цьому етапі розробляється модель мережі.
3. відпрацювання моделі - на цьому етапі модель мережі відпрацьовується для перевірки її точності.
4. аналіз результатів - на цьому етапі аналізуються результати

моделювання.

Методика моделювання мережі може бути складним завданням, і для її реалізації часто використовуються спеціальні інструменти і методи.

Для моделювання мережі зазвичай використовуються наступні інструменти:

- MATLAB - це програмне забезпечення для математичного моделювання, яке може використовуватися для аналітичного моделювання мережі.
- GNU Octave - система для виконання математичних розрахунків, що надає інтерпретовану мову, багато в чому сумісну з Matlab.
- SciLab - пакет наукових програм для чисельних обчислень, що надає потужне відкрите середовище для інженерних і наукових розрахунків.
- OMNET++ - це програмне забезпечення для імітаційної моделювання мережі, яке є популярним вибором для моделювання складних мереж.
- NS-3 - це ще один популярний інструмент для імітаційної моделювання мережі.
- Cisco Packet Tracer - це програма для моделювання мереж, розроблена компанією Cisco Systems. Вона призначена для вивчення, тестування та експериментів із конфігурацією мережевих пристроїв та розв'язанням завдань, пов'язаних із мережевими технологіями.
- GNS3 - це інструмент для віртуального моделювання та тестування мережевих конфігурацій. Він дозволяє користувачам створювати та експериментувати з мережевими топологіями, включаючи в себе різні маршрутизатори, комутатори та інші пристрої, які використовуються в сучасних комп'ютерних мережах.

Рисунок 3.5 - Інтерфейс програми OMNET++

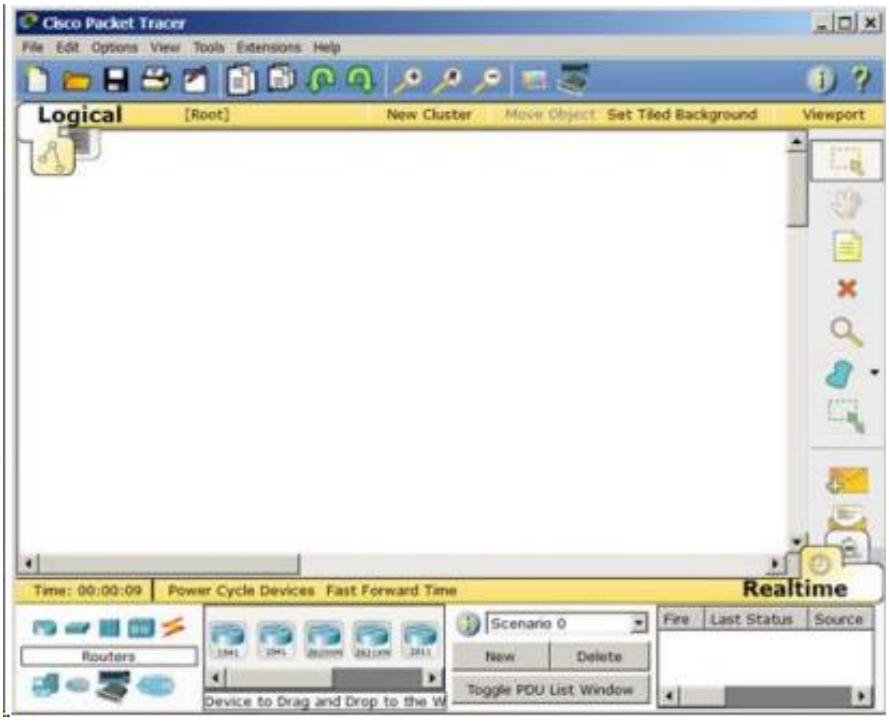

Рисунок 3.6 - Інтерфейс програми Cisco Packet Tracer

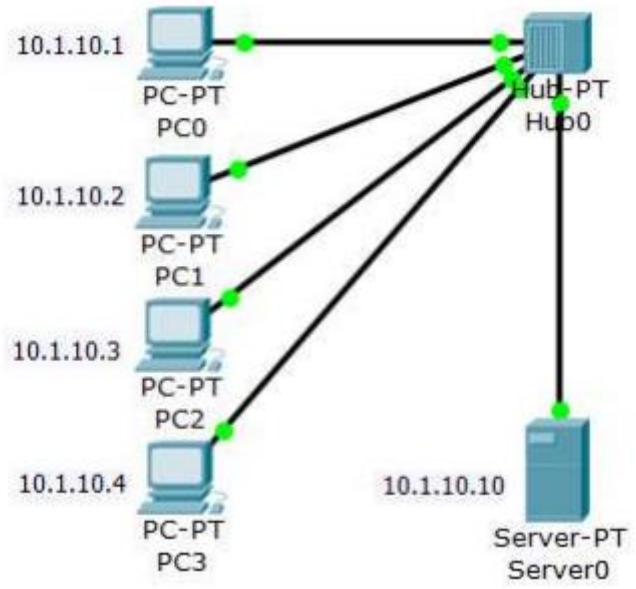

Рисунок 3.7 – Приклад моделі мережі у Cisco Packet Tracer

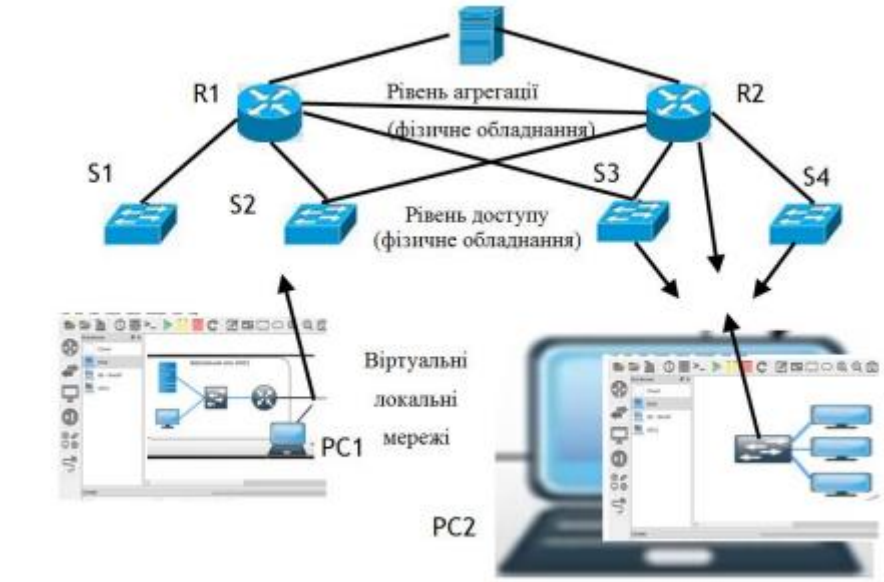

Рисунок 3.8 – Приклад моделі мережі у GNS3

Моделювання мережі дозволяє аналізувати, прогнозувати та оптимізувати різні аспекти мереж, такі як їхню продуктивність, надійність, ефективність та безпеку. Цей інструмент може бути використаний для проектування нових мереж, вдосконалення існуючих мереж, виявлення проблем та вирішення їх, а також для прийняття стратегічних рішень щодо розвитку мереж.

Моделювання мереж може бути проведене за допомогою різних методів, таких як математичне моделювання, симуляція, аналіз чергових систем, теорія графів та інші. В залежності від конкретних цілей та обставин, вибирається відповідний метод моделювання.

Застосування моделювання мереж допомагає покращити управління мережами, зменшити витрати на їхню експлуатацію, забезпечити високу якість обслуговування для користувачів та забезпечити стабільну роботу мереж у різних умовах. Таким чином, моделювання мереж є важливим інструментом для розвитку та оптимізації мережевих систем у сучасному світі.

3.4 Алгоритм оцінки ефективності комп’ютерної мережі

Отже, оцінка ефективності комп'ютерної мережі може виконуватися за допомогою різних методів та алгоритмів, які оцінюють різні аспекти мережі.

Алгоритм оцінки ефективності комп’ютерної мережі може включати такі кроки:

1) збір необхідних даних про мережу, таких як кількість комп'ютерів, тип та обсяг переданих даних, час роботи мережі тощо;
2) визначення основних показників ефективності мережі, таких як пропускна здатність, завадозахищеність, швидкодія тощо;
3) вибір методу оцінки ефективності, наприклад, аналітичний метод, симуляційне моделювання або експертна оцінка;
4) проведення розрахунків та/або моделювання для отримання показників ефективності мережі;
5) аналіз отриманих результатів і прийняття рішення щодо оптимізації роботи мережі.

На практиці цей алгоритм може реалізовуватись наступним чином.

Для оцінки пропускної здатності мережі для різних типів трафіку адміністратор мережі має виконати такі дії:

- вирішує використовувати метод пакетного аналізу;

- вимірює пропускну здатність мережі за допомогою тестів на передачу даних та час відправки-прийому (пінг) для визначення затримки;
- застосовує інтенсивний трафік для вимірювання, як мережа веде себе під високим навантаженням;
- вимірює затримки та джиттер для оцінки якості передачі даних у реальному часі, наприклад, для відтворення відео чи голосу;
- проводить тести на відновлення послуг та перевірку ефективності систем резервування в разі виходу з ладу основних компонентів;
- використовує інструмент моніторингу мережі для збору даних про трафік мережі;
- використовує статистичні методи для аналізу даних про трафік мережі;
- робить висновок, чи відповідає вимогам пропускна здатність мережі.