ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Удосконалення та оптимізація алгоритмів балансування навантаження у розподілених комп'ютерних мережах»

на здобуття освітнього ступеня магістра
зі спеціальності 123 Комп'ютерна інженерія
(код, найменування спеціальності)
освітньо-професійної програми комп'ютерні системи та мережі
(назва)

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

_____ *Божко М.В.*
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти групи КСДМ-62
Божко М.В.
Ім'я, ПРІЗВИЩЕ

Керівник: к.т.н., доцент Лащевська Н.О.
науковий ступінь, вчене звання
Ім'я, ПРІЗВИЩЕ

Рецензент: _____
науковий ступінь, вчене звання
Ім'я, ПРІЗВИЩЕ

Київ 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра Комп'ютерної інженерії

Ступінь вищої освіти магістр

Спеціальність 123 Комп'ютерна інженерія

Освітньо-професійна програма комп'ютерні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою к.т.н., доцент
Лащевська Н.О.
«___» _____ 20__ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Божко Максиму Володимировичу

(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Удосконалення та оптимізація алгоритмів балансування навантаження у розподілених комп'ютерних мережах

керівник кваліфікаційної роботи к.т.н., доцент Лащевська Н.О.,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 20_ р. № ___

2. Строк подання кваліфікаційної роботи «___» _____ 20__ р.

3. Вихідні дані до кваліфікаційної роботи:
3.1 Технології балансування навантаження в розподілених комп'ютерних мережах
3.2. Побудова мережі та її удосконалення
3.3. Науково-технічна література по обраній темі

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Поняття, характеристики, алгоритми та приклади пристроїв балансування навантаження в розподілених комп'ютерних мережах
2. Труднощі балансування навантаження в розподілених комп'ютерних мережах
3. Побудова та удосконалення мережі з використанням балансування навантаження у розподілених комп'ютерних мережах

5. Перелік ілюстративного матеріалу: *презентація*

6. Дата видачі завдання «___» _____ 20__ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Визначення напрямку дослідження та вибір об’єкта		Виконано
2	Отримання завдання і складання змісту дипломної роботи		Виконано
3	Написання першого розділу роботи		Виконано
4	Написання другого розділу роботи		Виконано
5	Написання третього розділу роботи		Виконано
6	Написання висновків по роботі		Виконано
7	Підготовка до захисту: доповідь, ілюстративний (роздатковий) матеріал		Виконано
8	Рецензування дипломної роботи		Виконано
	Захист дипломної роботи		

Здобувач вищої освіти _____ Божко М.В.
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Лащевська Н.О.
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Божко М.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 123 Комп'ютерна інженерія
(код, найменування спеціальності)
освітньо-професійної програми комп'ютерні системи та мережі
(назва)
на тему: «Удосконалення та оптимізація алгоритмів балансування навантаження у розподілених комп'ютерних мережах».

Кваліфікаційна робота і рецензія додаються.

Директор ННІ _____ _____
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Божко Максим Володимирович підготував роботу на тему «Удосконалення та оптимізація алгоритмів балансування навантаження у розподілених комп'ютерних мережах», яка є завершеною, виконаною у відповідності з календарним планом самостійною розробкою автора, націленою на вирішення актуального завдання – оптимізації алгоритмів балансування навантаження у розподілених комп'ютерних мережах.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Божко М.В.
на оцінку «відмінно» та присвоїти йому кваліфікацію магістр.

Керівник кваліфікаційної роботи _____ Лащевська Н.О.
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач *Божко М.В.* допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою комп'ютерної інженерії _____ Лащевська Н.О.
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

Реферат

Текстова частина магістерської роботи: 91 сторінка, 28 рисунків, 10 джерел.

Об’єкт роботи – балансування навантаження у розподілених комп’ютерних мережах.

Предмет роботи – удосконалення існуючої мережі та її оптимізація алгоритмів балансування навантаження у розподілених комп’ютерних мережах

Мета роботи – є розробка та оптимізація стратегії балансування навантаження у розподілених комп'ютерних мережах за допомогою міжмережевих екранів та комутаторів. Основними завданнями є виявлення переваг та можливостей, які надають ці пристрої, і розробка алгоритмів, спрямованих на підвищення ефективності обробки даних та використання ресурсів мережі.

Короткий зміст роботи:

Поняття, характеристики, алгоритми та приклади пристроїв балансування навантаження, роль в зменшенні затримки трафіку, побудова та удосконалення мережі.

Ключові слова: балансування навантаження, міжмережевий екран, кумутатор, VLAN, мережа.

Зміст

Перелік умовних позначень

OSI - Open System Interconnection
ARP - Address Resolution Protocol
MAC - Media Access Control
IP - Internet Protocol
ПК - персональный компьютер
UDP - User Datagram Protocol
TCP - Transmission Control Protocol
ПЗ – програмне забеспечення
DNS- Domain Name System
FTP- File Transfer Protocol
BOOTP - bootstrap protocol
NFS - Network File System
RTP - Real-time Transport Protocol)
SMTP - Simple Mail Transfer Protocol
HTTPS - HyperText Transfer Protocol Secure
БД – база даних
URL - Uniform Resource Locator
GSLB - global server load balancing
TCP - Transmission Control Protocol
IT - Information Technology
HTTP - HyperText Transfer Protocol
CGI - Common Gateway Interfac
ПО – програмне забеспечення
ACL - Access Control List
ICMP - Internet Control Message Protocol
SSH - Secure Shell
NAT - Network Address Translation
NGFW - Next Generation Firewall
SQL - Structured Query Language
DDoS - denial-of-service attack
XSS - Cross Site Scripting
NIC - Network interface controller
HIPAA - Health Insurance Portability and Accountability Act
DSS - Data Security Standard
VPN - virtual private network
ICS - Internet Connection Sharing
LAN - local area network
QoS - Quality of service
VLAN - Virtual Local Area Network
PoE - Power over Ethernet

DPI - Deep Packet Inspection
IX - Extreme Networks
IDS - intrusion detection system
IPS - Network-based Intrusion
TLD - top-level domain
IETF - Internet Engineering Task Force
RFC - Request for Comments
ICANN - . Internet Corporation for Assigned Names and Numbers
IPv4 - nternet Protocol version 4
IPv6 - nternet Protocol version 6
TTL - Time To Live
ОС – операційна система
NS - Network Service
PCI - Peripheral component interconnect
FC - fibre channel
SFP - Small Form-factor Pluggable
QSFP - Quad Small Form-factor Pluggable
LC - Lucent Connector
SC - Subscriber Connector
MPO - multi-fiber push
RJ45 - Registered Jack
HSSDC - (High Scalability Data Center
SAN - Storage Area Network,
NAS - Network Attached Storage
iSCSI - Internet Small Computer System Interface
RDMA - remote direct memory access
G - gigabit
GBIC - GigaBit Interface Converter
ЦП – центральний процесор
ISA - Industry Standard Architecture
IBM - International Business Machines
USB - Universal Serial Bus
DSL - Digital subscriber line
APM - Advanced Power Management
CDN - Content Delivery Network
UX - User experience
SSL - Secure Sockets Layer
IoT - Internet of Things
ISL - Inter-Switch link

Вступ

У світі безмежних можливостей розподілених комп'ютерних мереж, де обчислювальні ресурси стають дорогоцінним активом для ефективної обробки величезних обсягів даних, проблема балансування навантаження виникає як важливе завдання для забезпечення високої продуктивності та надійності систем.

Сучасний цифровий епоха визначається неабияким зростанням об'ємів обробки даних, що вимагає ефективного використання розподілених мереж для забезпечення ресурсів, необхідних для подолання викликів сучасного інформаційного суспільства. Балансування навантаження стає стратегічним рішенням для забезпечення оптимального розподілу завдань та уникнення перевантажень в розподілених обчислювальних середовищах.

Мета цього дослідження полягає в глибокому розумінні, розробці та оптимізації стратегій балансування навантаження у розподілених комп'ютерних мережах. Звертаючись до цього питання, ми сподіваємося внести інновації у сучасні підходи до управління ресурсами, поліпшити продуктивність та забезпечити стабільну роботу систем в умовах зростаючих обчислювальних потреб.

У світі, де величезні обсяги даних генеруються в режимі реального часу, а хмарні та розподілені технології стають неодмінною частиною інфраструктури, вирішення проблем балансування навантаження є не лише актуальним завданням, але і ключовою умовою для подальшого технологічного розвитку.

Ми сподіваємося, що результати нашого дослідження не лише розкриють сутність проблеми балансування навантаження, а й визначать нові шляхи для створення більш ефективних, стійких та продуктивних розподілених комп'ютерних мереж. Ця робота може внести суттєвий внесок у вдосконалення обчислювальних систем, що стане важливою ланкою для майбутнього розвитку інформаційних технологій.

Розділ 1. Поняття, характеристики, алгоритми та приклади пристоїв балансування навантаження в розподілених комп'ютерних мережах

1.1 Поняття балансування навантаження в розподілених комп'ютерних мережах

У термінології комп'ютерних мереж балансування навантаження або вирівнювання навантаження (англ. load balancing) — метод розподілу завдань між кількома). резервування (відмовостійкості (динамічний додавання/видалення пристроїв), а також забезпечення кластерагоризонтального масштабування) з метою оптимізації використання ресурсів, скорочення часу обслуговування запитів, серверами (наприклад, мережевими пристроями).

У комп'ютерах балансування навантаження розподіляє навантаження між кількома обчислювальними ресурсами, такими як комп'ютери, комп'ютерні кластери, мережі, центральні процесори або диски. Мета балансування навантаження — оптимізація використання ресурсів, максимізація пропускної спроможності, зменшення часу відгуку та запобігання перевантаженню будь-якого одного ресурсу. Використання декількох компонентів балансування навантаження замість одного компонента може підвищити надійність та доступність за рахунок резервування. Балансування навантаження зазвичай передбачає наявність спеціального програмного забезпечення або апаратних засобів, таких як багаторівневий комутатор або система доменних імен, як серверний процес.

Балансування навантаження відрізняється від фізичного з'єднання тим, що балансування навантаження ділить трафік між мережевими інтерфейсами на мережевий сокет (модель OSI рівень 4) основі, у той час як з'єднання каналу передбачає поділ трафіку між фізичними інтерфейсами на нижчому рівні, або пакет (модель OSI рівень 3) або каналом зв'язку (модель OSI рівень 2).

Балансування навантаження може бути використане для розширення можливостей ферми серверів, що складається з більш ніж одного сервера. Вона також може дозволити продовжувати роботу навіть за умов, коли кілька виконавчих пристроїв (серверів) вийшли з ладу. Завдяки цьому зростає стійкість до відмов, і

з'являється можливість динамічно регулювати використовувані обчислювальні ресурси за рахунок додавання/видалення виконавчих пристроїв в кластері.

1.2 Характеристики балансування навантаження в розподілених комп'ютерних мережах

Рівні балансування

Процедура балансування здійснюється за допомогою цілого комплексу алгоритмів і методів, що відповідають наступним рівням моделі OSI

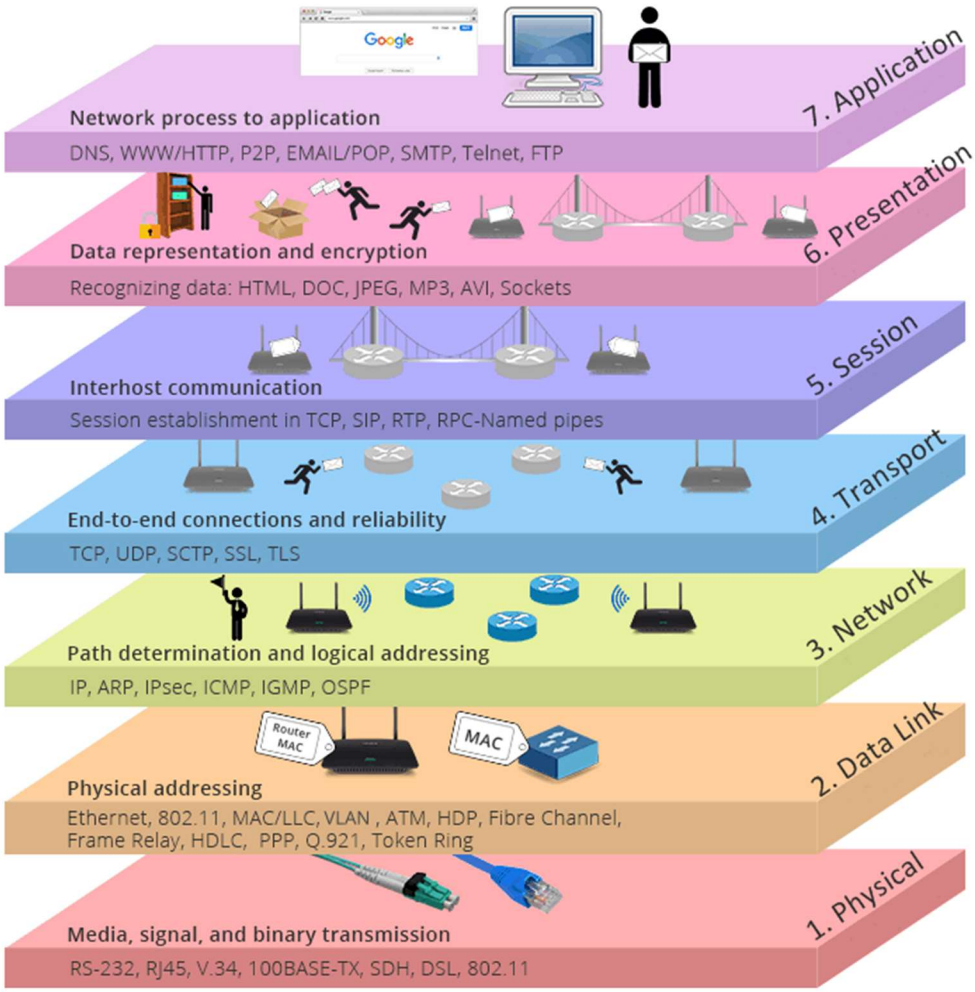


Рис. 1 Семирівнева модель OSI

Розглянемо певні рівні докладніше, а саме:

- мережевому;

- транспортному;

- прикладному.

- Мережевий рівень - на цьому етапі визначається шлях передачі та вводиться нове поняття маршрутизації. На L3 використовується 2 типи протоколів: з встановленням та без встановлення з'єднання. Перший тип протоколів надсилає дані, що містять повну інформацію про відправника та одержувача. Це потрібно для того, щоб мережні пристрої отримали повну адресну інформацію та правильно визначили шлях для маршрутизації даних. Пакет передаватиметься від одного маршрутизатора (роутера) до іншого, доки не потрапить одержувачу.

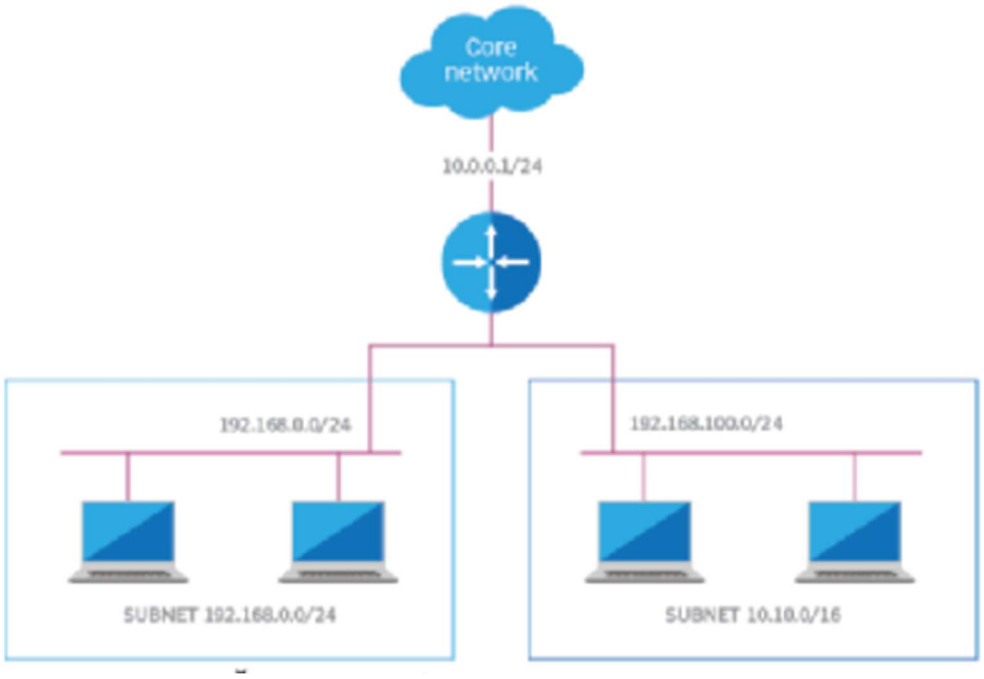


Рис. 2 Схема роботи мережевого рівня моделі OSI

Але протоколи, які працюють без встановлення з'єднання, мають один істотний мінус – не дотримання порядку передачі даних. Користувач отримає повідомлення від відправника не так, як він їх надсилав, тому що різні пакети можуть бути надіслані різними маршрутами. У цьому випадку, перш ніж інформація потрапить до користувача, вона обробляється L4 транспортними протоколами.

При використанні протоколів із встановленням з'єднання дані надходять користувачеві в тому порядку, в якому вони були надіслані. Але при їх використанні

сам процес надсилання інформації займає більше часу. Найактивніше на L3 використовується протокол ARP для визначення MAC-адреси по IP. Він також здійснює зворотнє перетворення унікального ідентифікатора мережного обладнання IP.

L1, L2, L3 відносяться до рівнів середовища. Вони відповідають за переміщення даних бездротовими мережами, кабелями, мережевим обладнанням. Вищі рівні (з L4 по L7) називають рівнями хоста. Вони взаємодіють з пристроями користувача (ПК, смартфонами, планшетами) і відповідають за подання даних.

- Транспортний рівень - Надсилання даних від відправника до одержувача регулюється окремо. За цей процес відповідає транспортний рівень. Під час передачі інформації завжди втрачається частина даних. Для деяких видів файлів (аудіо, відео, фотографії) малі втрати не критичні. Для передачі даних застосовується протокол UDP. Він забезпечує відправлення пакетів без встановлення з'єднання.

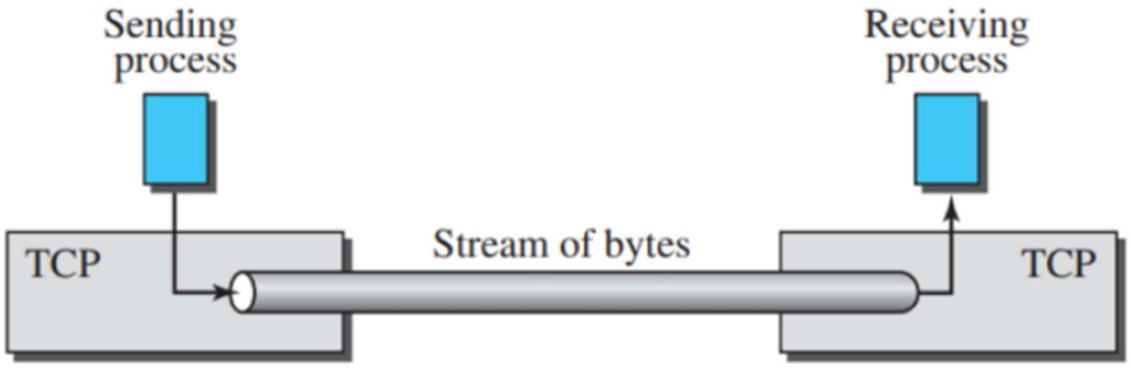


Рис.3 Схема роботи транспортного рівня моделі OSI

У разі використання UDP файл ділиться на датаграми. Вона містить заголовки, необхідні для доставки до одержувача. З цієї причини датаграми можуть надсилатися користувачеві різними маршрутами та у довільному порядку. Якщо датаграма загубиться, у файлі з'являється биті дані.

Якщо користувач надсилає файли, чутливі до втрат даних, застосовується TCP.

Він перевіряє цілісність інформації, що передається. У разі його використання файл сегментується. Але це відбувається не завжди, а лише з тими пакетами даних, розмір яких перевищує пропускну спроможність мереж. Сегментація також потрібна, коли відбувається відправлення файлів нестабільними мережами.

У повсякденній роботі інженери взаємодіють лише з першими чотирма рівнями. Знати їх особливості потрібно для проектування мереж та налаштування обладнання. З іншими рівнями взаємодіють розробники ПЗ.

- Прикладний рівень – рівень додатків. Він відповідає за взаємодію користувачів додатків з працюючою мережею. Цей рівень забезпечує використання програмами мережевих служб, відправлення e-mail, обмін даними через торренти, надання ПЗ інформації про збої тощо. До протоколів прикладного рівня відносять:

- DNS;
- FTP;
- BOOTP;
- BitTorrent;
- NFS;
- RTP;
- SMTP і т.д.

У разі HTTPS його приналежність до L7 або L6 визначається способом використання. Якщо користувач займається веб-серфінгом, протокол відносять до прикладного рівня. Якщо здійснюється передача фінансових даних, то низькорівневий HTTPS розглядають як L6.

Сьомий рівень відповідає за подання даних у зрозумілому користувачеві вигляді. На цьому етапі не відбувається доставка чи маршрутизація інформації. Протоколи просто конвертують дані для візуалізації. Крім перетворення даних, вони також забезпечують доступ до віддалених БД, пересилають службову інформацію.

Алгоритми балансування навантаження

Round Robin (круговий обхід) - це простий алгоритм балансування

навантаження, який розподіляє запити або завдання між серверами у порядку чергового обходу. Кожен сервер отримує запит у відповідності до свого порядку у черзі, і після того, як останній сервер отримає запит, обхід починається спочатку.

Основна ідея Round Robin полягає в тому, щоб рівномірно розподілити навантаження між серверами, уникнути перевантаження одного сервера, і забезпечити велику доступність та рівномірну використаність ресурсів.

Наприклад, якщо є три сервери (A, B, C), то запити будуть розподілятися в такому порядку: A, B, C, A, B, C, і так далі

Існують різні варіації Round Robin. Наприклад, можливе використання вагових коефіцієнтів для серверів, де кожен сервер отримує кількість запитів пропорційно його ваговому коефіцієнту. Це може бути корисно, коли сервери мають різну продуктивність або ресурси.

Round Robin - це простий і легко реалізований алгоритм, але він може бути не оптимальним у випадку, коли сервери мають різний обсяг ресурсів або великі розбіжності в продуктивності. У таких випадках можуть бути застосовані інші алгоритми балансування, які беруть до уваги додаткові параметри.

Least Connections **(**з сервером, у якого найменше з'єднань**)** - це алгоритм балансування навантаження, який спрямований на розподіл нових запитів між серверами таким чином, щоб кожен новий запит надсилався на сервер з найменшою кількістю активних з'єднань або клієнтів.

Основна ідея полягає в тому, щоб уникнути перевантаження серверів, розподіляючи навантаження пропорційно їхній поточній зайнятості. Якщо сервер має менше активних з'єднань, то йому буде присвоєний новий запит. Це дозволяє досягти рівномірного розподілу навантаження між серверами.

Процес роботи алгоритму можна описати наступним чином:

- Кожен сервер підтримує лічильник активних з'єднань;
- Коли надходить новий запит, алгоритм вибирає сервер, який має найменшу кількість активних з'єднань;
- Новий запит направляється на обраний сервер;

- Лічильник активних з'єднань для обраного сервера збільшується.

Цей підхід дозволяє ефективно використовувати ресурси серверів і розподіляти навантаження відповідно до їхньої поточної зайнятості. Однак важливо враховувати, що у деяких сценаріях, де час обробки кожного запиту може значно відрізнятися, цей метод може не завжди забезпечувати ідеальний баланс між серверами. У таких випадках може бути використано більш складні алгоритми балансування.

Weighted Round Robin (ваговий круговий обхід) - це модифікація алгоритму Round Robin, в якій кожному серверу надається ваговий коефіцієнт, що визначає його спроможність обробляти запити. Сервери з більшими ваговими коефіцієнтами отримують більше запитів у порівнянні з серверами, у яких ваговий коефіцієнт менший.

Основна ідея вагового кругового обходу полягає в тому, що він дозволяє надавати пріоритет серверам з великими ресурсами або вищою продуктивністю, забезпечуючи їм більше запитів для обробки. Це особливо корисно, коли сервери в мережі мають різний обсяг ресурсів або продуктивність.

Процес роботи вагового кругового обходу:

- Кожен сервер має свій ваговий коефіцієнт, який визначається його продуктивністю або ресурсами;
- Запити розподіляються між серверами у порядку чергового обходу, але кожен сервер отримує кількість запитів, пропорційну його ваговому коефіцієнту;
- Коли досягається кінець списку серверів, обхід починається спочатку;
- Процес повторюється, а вагові коефіцієнти визначають розподіл навантаження між серверами.

Цей підхід дозволяє адаптувати розподіл трафіку до особливостей кожного сервера в мережі і ефективно використовувати його ресурси.

Least Response Time (з найменшим часом відповіді) - це метод балансування навантаження, в якому нові запити направляються на сервер, який має найменший час відповіді або найшвидший відгук на попередні запити.

Основна ідея полягає в тому, щоб оптимізувати час відповіді на запити,

направляючи їх на сервери з найшвидшою реакцією. Це може допомогти покращити продуктивність та знизити час очікування для клієнтів.

Процес роботи алгоритму може виглядати наступним чином:

- Кожен сервер підтримує внутрішній механізм вимірювання часу відповіді на запити;
- Коли приходить новий запит, алгоритм вибирає сервер, який має найменший час відповіді;
- Новий запит направляється на обраний сервер;
- Алгоритм оновлює час відповіді для обраного сервера.

Цей метод може бути особливо ефективним у сценаріях, де час обробки кожного запиту може варіюватися і важливо вибрати сервер з найшвидшою реакцією. Однак важливо враховувати, що точність вимірювання часу відповіді і розподіл навантаження може бути чутливим до змін в мережі та навантаження.

Adaptive Load Balancing (адаптивне балансування навантаження) - це підхід до балансування навантаження, який використовує динамічні стратегії на основі аналізу поточного стану системи та серверів. Основна ідея полягає в тому, щоб система адаптувалася до змін в навантаженні, стані серверів та інших факторах для оптимізації розподілу трафіку.

Основні принципи адаптивного балансування навантаження включають:

- Моніторинг стану системи: Система в реальному часі відстежує параметри, такі як завантаження серверів, час відповіді, кількість активних з'єднань та інші метрики продуктивності;
- Аналіз і вивчення тенденцій: На основі зібраних даних алгоритм аналізує тенденції та прогнозує можливі зміни в навантаженні або стані серверів;
- Прийняття рішень: На основі аналізу система вирішує, як змінити розподіл трафіку. Це може включати зміну вагових коефіцієнтів для серверів, перерозподіл запитів або використання інших стратегій балансування;
- Динамічне адаптування: Система в реальному часі впроваджує зміни в розподіл трафіку відповідно до прийнятих рішень;

- Зворотний зв'язок: Система продовжує відстежувати результати внесених змін та вносить корективи в стратегію балансування в залежності від ефективності.

Переваги адаптивного балансування навантаження включають здатність адаптуватися до змін у навантаженні та стані серверів, що робить його ефективним у змінливих умовах. Однак впровадження таких стратегій може вимагати складніших механізмів та алгоритмів для аналізу та вирішення завдань балансування.

Content-based routing (маршрутизація на основі вмісту) - це метод балансування навантаження, при якому розподіл трафіку визначається характеристиками або вмістом запитів. Вміст може бути аналізований для визначення, на який сервер направити запит, з урахуванням конкретних властивостей чи характеристик.

Основні ідеї та принципи content-based routing

- Аналіз вмісту запиту: Система аналізує вміст запитів, такі як заголовки HTTP, параметри URL або інші атрибути запиту;
- Визначення критеріїв маршрутизації: Задаються правила чи умови, які визначають, які типи запитів направлятимуться на які сервери. Наприклад, запити на статичний контент можуть бути направлені на один сервер, а запити на динамічний контент - на інший;
- Маршрутизація відповідно до правил: Запити автоматично маршрутизуються на сервери відповідно до визначених критеріїв;
- Динамічна адаптація: Система може динамічно змінювати правила маршрутизації в залежності від змін у навантаженні, стані серверів чи інших факторів.

Цей підхід дозволяє ефективно маршрутизувати різні типи запитів на різні сервери в залежності від їхнього вмісту чи характеристик. Content-based routing особливо корисний у сценаріях, де сервери мають різні здатності обробки або служать різним типам вмісту (наприклад, статичний та динамічний контент).

Global Server Load Balancing (глобальне балансування навантаження) - це стратегія балансування навантаження, яка працює на рівні глобальної мережі та використовує розподілені сервери для керування трафіком між різними дата-центрами або серверами в різних географічних областях. Основна мета - забезпечити

високу доступність, оптимізувати шляхи передачі даних та надавати користувачам швидкий доступ до ресурсів.

Основні характеристики та принципи GSLB:

- Географічний розподіл: Сервери або дата-центри розміщені в різних регіонах чи країнах з метою наближення до користувачів та оптимізації шляхів передачі даних;
- DNS-запити: GSLB використовує DNS для визначення, який сервер повинен обслуговувати конкретний запит. DNS-запити використовуються для маршрутизації користувачів на найближчий або оптимальний сервер;
- Моніторинг стану серверів: Система GSLB в реальному часі моніторить стан серверів, перевіряючи їх доступність та продуктивність;
- Врахування навантаження: GSLB може враховувати навантаження на кожному сервері та маршрутизувати трафік для забезпечення рівномірного розподілу ресурсів;
- Адаптивні стратегії: Здатність адаптувати стратегії маршрутизації в залежності від змін у стані серверів, навантаженні та інших факторах.
- Гарантія доступності: GSLB може надавати можливості для автоматичного переадресації трафіку в разі виявлення проблем або неполадок на серверах.

Все це дозволяє GSLB оптимізувати розподіл трафіку, забезпечувати високу доступність та покращувати продуктивність в мережах з розподіленими серверами або дата-центрами.

1.3 **Приклади пристроїв, до яких застосовується балансування навантаження**

Кластер серверів - це група серверів, що працюють разом в одній системі, щоб забезпечити користувачам більш високу доступність. Ці кластери використовуються для скорочення часу простою, дозволяючи іншому серверу продовжувати роботу у разі збою. Група серверів підключена до однієї системи. У той момент, коли один із цих серверів стає недоступним, робоче навантаження перерозподіляється на інший

сервер до того, як клієнт переживає якийсь час простою.

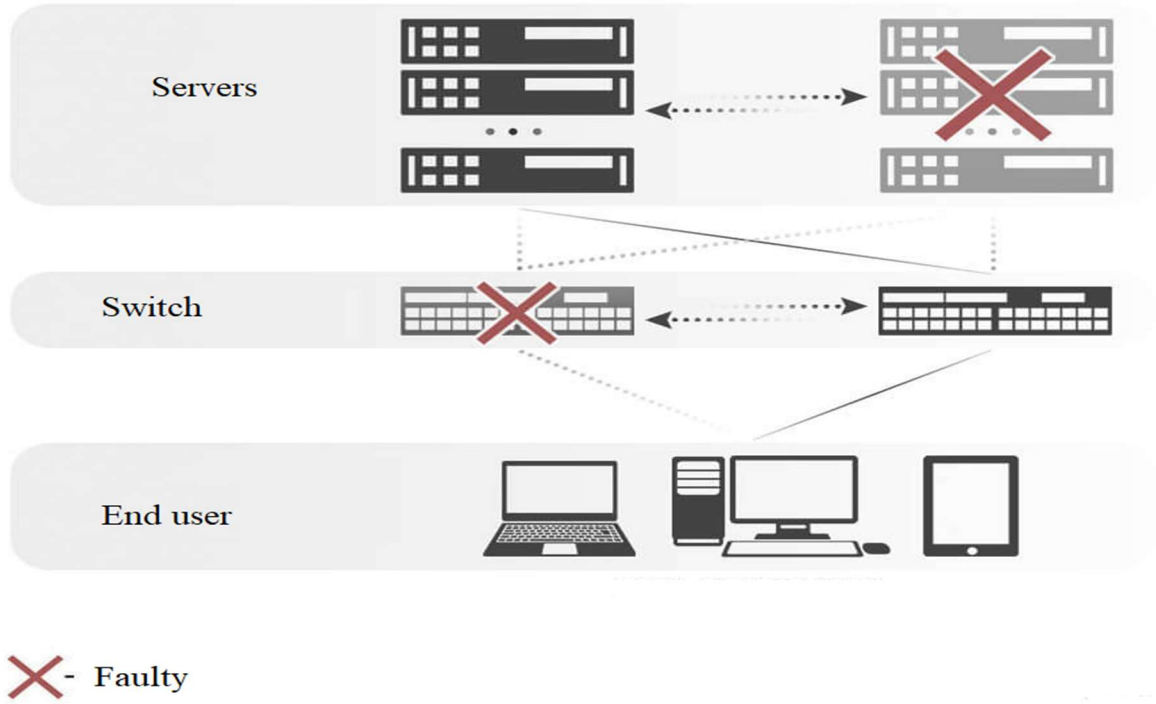


Рис. 4 Схемае роботи кластерів сервірів

Види кластерів:

- Відказостійкі. Кілька серверів об'єднуються з метою дублювання один одного.
- Високопродуктивні. На групу машин надсилаються дані для обробки - кластер розподіляє завдання по всіх учасників для прискорення обробки.
- Балансувальники. Усі запити на сервери розподіляються у випадковому порядку між нодами кластера.

Вважають, що кластери серверів діляться на дві моделі:

1) Перша — це використання єдиного масиву зберігання інформації, що дає можливість швидшого перепідключення при збої. Однак у випадку з об'ємною базою даних та великою кількістю апаратних одиниць у системі можливе падіння продуктивності.

2) Друга — це модель, за якої сервери незалежні, як і їхня периферія. У разі відмови перерозподіл відбувається між серверами. Тут ситуація зворотна — трафік у

системі більш вільний, однак ускладнюється та обмежується користування загальною базою даних.

Основним обґрунтуванням для кластерів серверів є захист від простоїв та збоїв. Як згадано вище, кластерні сервери забезпечують підвищений захист від повного відключення мережі під час збою живлення та призначені для захисту від трьох основних типів збоїв:

- Збій програми/служби: збій, який впливає на критично важливі програми та служби в мережі;
- Системний/апаратний збій: виходи з ладу, які впливають на такі компоненти, як процесори, пам'ять, адаптери, диски та джерела живлення;
- Збій датацентру: збої датацентрів, які зачіпають кілька місць, зазвичай викликані стихійними лихами, які призводять до масових відключень електроенергії.

Основні можливості кластера серверів:

- кластер серверів може функціонувати одному чи кількох комп'ютерах (робочих серверах);
- на кожному робочому сервері може функціонувати один або кілька робочих процесів, які обслуговують клієнтські з'єднання в рамках кластера;
- підключення нових клієнтів до робочих процесів кластера виконується з урахуванням аналізу довгострокової статистики завантаженості робочих процесів
- взаємодія процесів кластера з клієнтськими додатками, між собою та з сервером баз даних здійснюється за протоколом TCP/IP;
- процеси кластера сервера можуть бути запущені як додаток або як сервіс.
- загальна схема клієнт-серверного варіанта роботи
- у клієнт-серверному варіанті роботи клієнтська програма взаємодіє з кластером серверів, який, у свою чергу, здійснює взаємодію з сервером баз даних.

У клієнт-серверному варіанті роботи клієнтська програма взаємодіє з кластером серверів, який, у свою чергу, здійснює взаємодію з сервером баз даних.

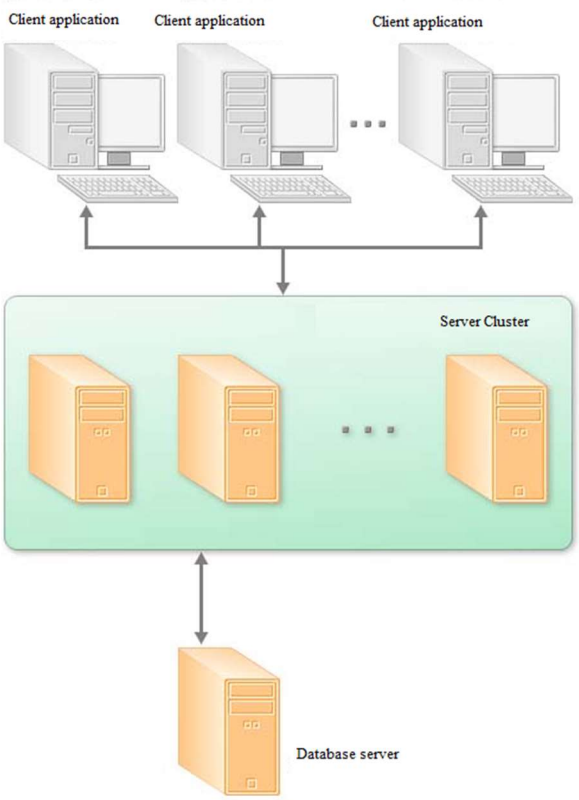


Рис.5 Загальна схема клієнт-серверного варіанта роботи

Один із комп'ютерів, що входять до складу кластера серверів, є центральним сервером кластера. Центральний сервер, крім обслуговування клієнтських з'єднань, керує роботою всього кластера та зберігає реєстр кластера.

Для клієнтського з'єднання кластер адресується на ім'я центрального сервера та номер IP порту. Якщо використовується стандартний IP порт, достатньо вказівки одного імені центрального сервера.

Під час встановлення з'єднання клієнтська програма звертається до центрального сервера кластера. Центральний сервер, на основі аналізу статистики завантаженості робочих процесів, направляє клієнтський додаток до конкретного робочого процесу, який його обслуговуватиме. Цей процес може бути як на центральному сервері, так і на будь-якому робочому сервері кластера.

Робочий процес виконує аутентифікацію користувача та обслуговує з'єднання до закінчення сеансу роботи клієнта з цією інформаційною базою.

Існує три основні причини кластеризації серверів. Це доступність, масштабованість та надійність. Ключ до захищеної IT-інфраструктури лежить у надмірності. Створення кластера серверів в одній мережі забезпечує максимальну

надмірність і гарантує, що одна помилка не спричинить відключення всієї мережі.

Проксі-сервер - це посередник між користувачем і цільовим сервером, на якому безпосередньо розміщується сайт. Фактично він являє собою проміжний сервер, що виконує роль шлюзу і одночасно фільтра для ефективного, але безпечного зв'язку комп'ютера або мобільного пристрою з великим світом інтернету. У тому числі для забезпечення анонімності та конфіденційності користувача, вкрай важливих при роботі в мережі.

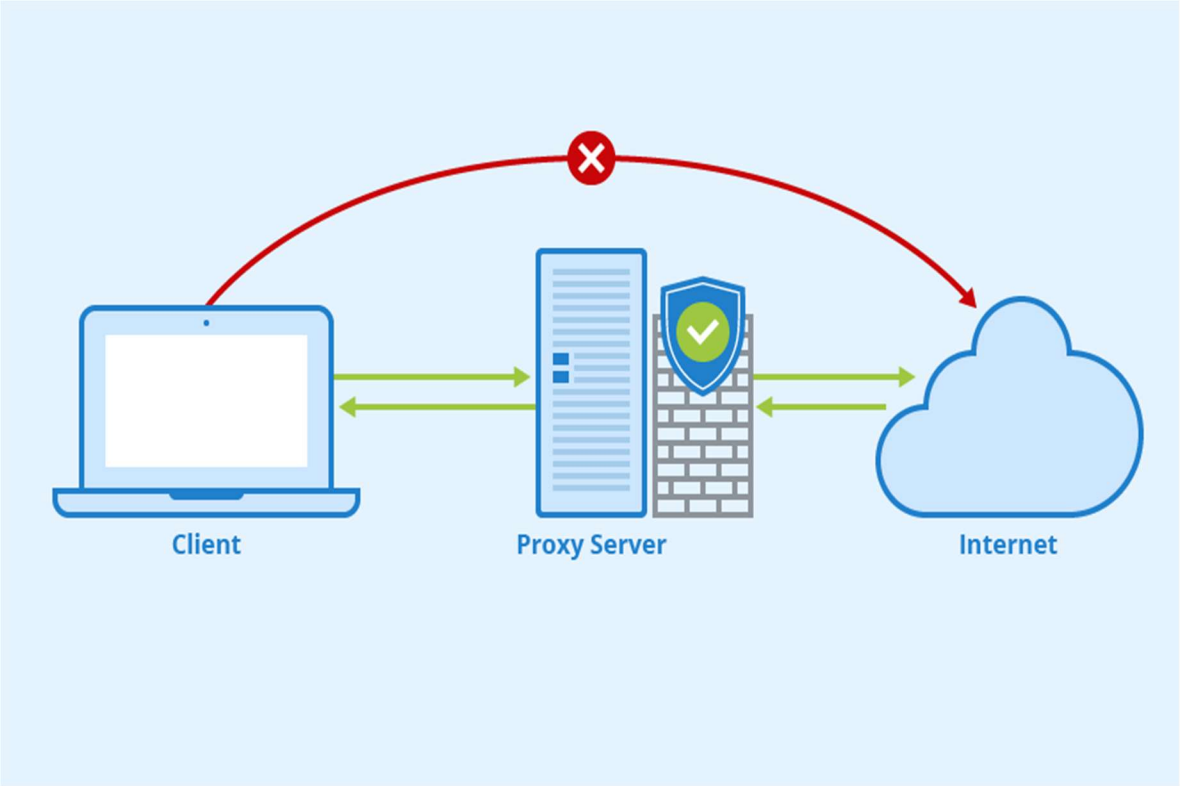


Рис. 5 Схема роботи сучасних проксі-серверів

Розглянемо докладніше, що це таке звичайними словами, необхідність і принципи роботи сучасних проксі-серверів, а також їх основні плюси і мінуси.

Назва «проксі-сервер» традиційно має англомовне коріння і відбулося від слова proxy, яке перекладається як «уповноважений» або «посередник». Друга частина терміну — «сервер» — означає місце для зберігання даних, важливою функцією якого виступає надання користувачам доступу до інформації на підставі запитів, що надходять. Якщо узагальнити сказане, можна отримати на виході досить просте визначення, яке виглядає наступним чином.

Під проксі-сервером розуміється сервер проміжного рівня, що виконує функції посередника між користувачем і кінцевим сервером і одночасно забезпечує безпеку встановленого зв'язку разом з конфіденційністю даних людини. Хоча на практиці він здатний вирішити набагато більше завдань. Тут ж необхідно виділити його головне завдання — роль посередника чи сполучної ланки між користувачем та інтернетом в цілом/цільовим сервером в части.

Як працює проксі сервер

Принцип функціонування проксі-сервера досить простий. Спочатку відбувається отримання запиту, надісланого користувачем. Далі він обробляється і пересилається на цільовий сервер. Отримана від останньої відповідь перевіряється на безпеку і переправляється користувачу. При необхідності він також піддається обробці та коригуванні з урахуванням функціонального призначення проксі.Паралельно формується профіль користувача у виді історії запитів, основних інтересів та характерних особливостей поведінки в інтернеті. Зібрана інформація використовується по-різному, що залежить від типу, призначення та налаштувань проксі-сервера.

Паралельно формується профіль користувача у виді історії запитів, основних інтересів та характерних особливостей поведінки в інтернеті. Зібрана інформація використовується по-різному, що залежить від типу, призначення та налаштувань проксі-сервер.

Типи проксі-серверів

Схема роботи з використанням проксі-серверів широко поширена, що стало причиною розробки декількох різних типів подібних посередників. Тому має сенс детальніше описати найзатребуваніші з них на сьогоднішній день. Вони класифікуються за двома ознаками: принцип роботи (прямий або зворотний) і ступень анонімності користувача (прозорий, анонімний, спотворює і високоанонімний).

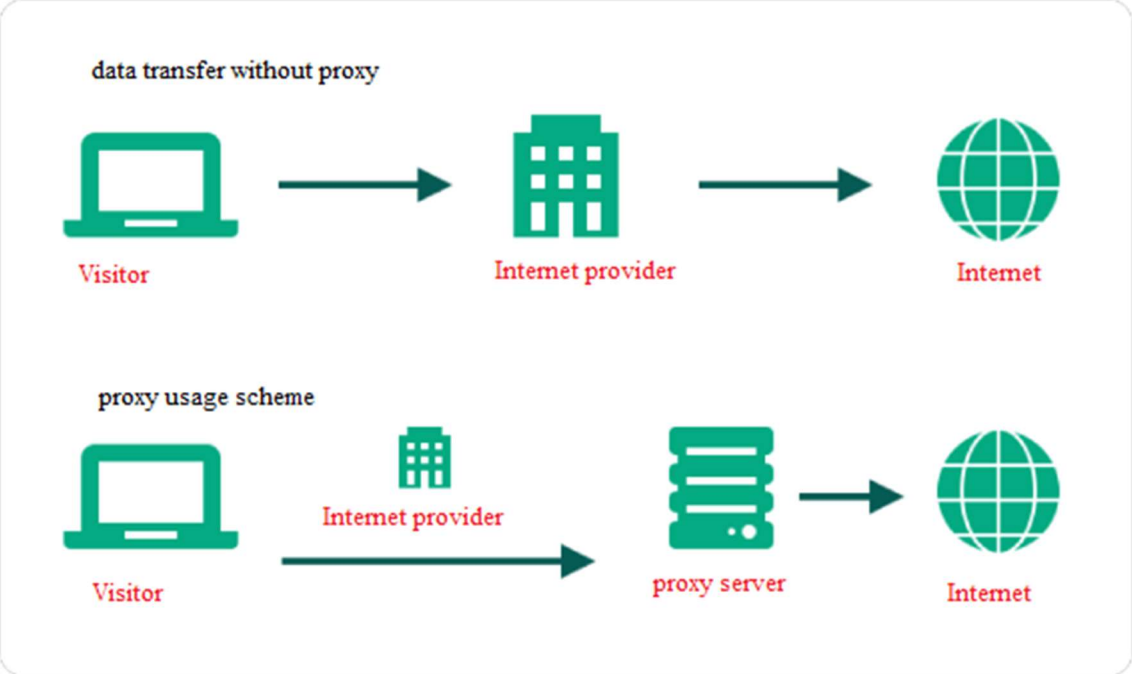


Рис. 6 Прямий, або Forward Proxy

Класичний варіант проксі. Сервер розміщується безпосередньо між відвідувачем інтернету та сайтами. Принцип його дії описано вище. Задіяння посередника розширює можливості користувача в частині відвідування заблокованих ресурсів, збереження конфіденційності персональних даних і захисту ПК/смартфону від потенційно небезпечної інформації ззовні. Саме прямий проксі-сервер використовується на практиці найчастіше.

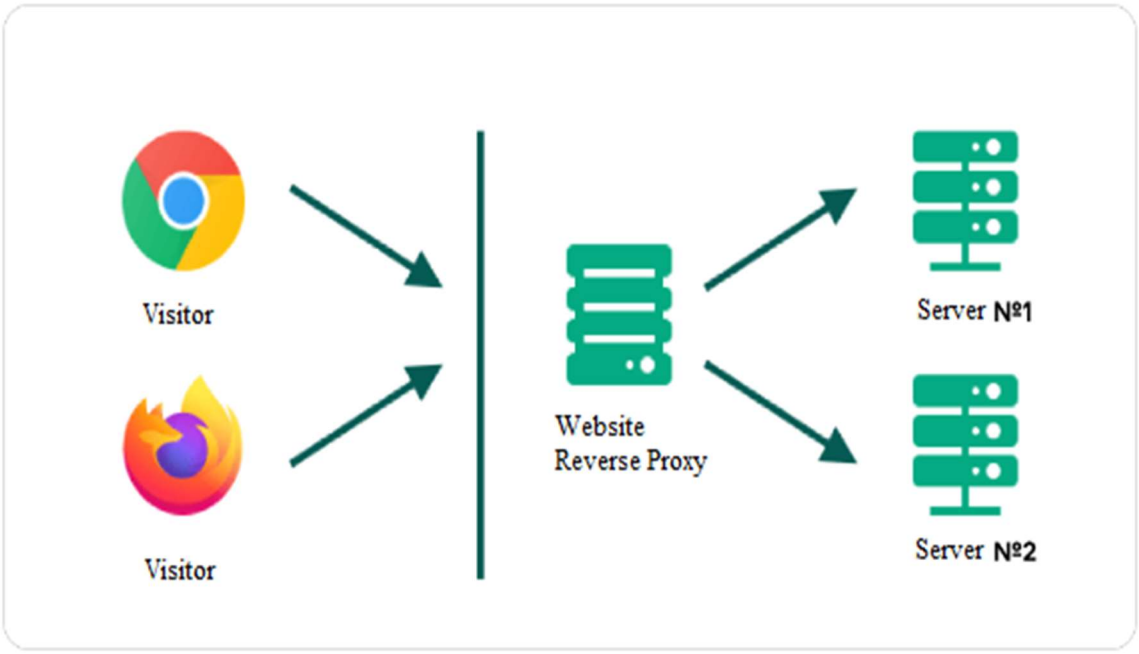


Рис. 7 Зворотній, або Reverse Proxy

Цей тип проксі має дещо іншим функціоналом. Основним завданням посередника стає розподіл потоку запитів між серверами, на яких розміщується вміст сайту. Справа в тому, що нерідко для зберігання інформації одного інтернет-ресурсу використовуються різні сервери. Що передбачає необхідність регулювати навантаження на кожен з них. Саме цим займаються проксі, які визначають, на який саме із серверів сайту буде направлений той чи інший запит. Іншими словами, грамотне використання Reverse Proxy підвищує ефективність роботи як користувача, так і інтернет-ресурсу.

Прозорий

Цей тип проксі не приховує інформацію про користувача. Веб-сайт отримує дані про реальну IP-адресу. Основним завданням прозорих Proxy виступає кешування даних і фільтрація контенту, який надходить або походить від користувачів, підключених до цього сервера. Як приклад практичного використання подібних ресурсів можна навести комп'ютерні мережі освітніх установ, які блокують доступ студентів або школярів до YouTube, соціальних мереж або інших сайтів з розважальним вмістом. Мета подібних дій очевидна — створення оптимальних умов

для ефективного ведення навчального процесу.

Анонімний

У цьому випадку на цільовий сайт не надходить даних про реальну IP-адресу як самого проксі-сервера, так і користувача, що надіслав запит. Що забезпечує конфіденційність особистих даних і надає можливість обходити блокування, пов'язане з географічною приналежністю. Єдиним недоліком такого проксі стає неможливість приховати його використання. Іншими словами, на стороні сайту є розуміння, що робота з відвідувачем ведеться через посередника.

Змінний

Проксі змінює IP-адресу і HTTP-заголовки в автоматичному режимі. Результатом стає не тільки досить ефективний захист особистої інформації користувача, але й неможливість встановити факт роботи із задіянням посередника.

Високоанонімний

Класифікація використовуваних на практиці проксі-серверів була неповною без опису основних різновидів з точки зору функціоналу. Загальна кількість таких ресурсів дуже велика. Нижче наводяться найпоширеніші на сьогоднішній день.

HTTP

Це найпопулярніший вид Proxy. Застосовується майже повсюдно. Дозволяє вирішити кілька актуальних завдань:

- кешування (стиснення) даних, що прискорює обмін інформацією;
- фільтрація контенту за допомогою блокування сайтів певної спрямованості;
- відключення реклами та рекламних повідомлень.

HTTPS

Проксі захищає персональні дані користувача за допомогою шифрування

вихідного трафіку. Сервер такого виду особливо часто застосовується, якщо потрібно зберегти конфіденційну інформацію, наприклад, про реквізити банківських карток або електронних гаманців. Важливо розуміти, що HTTPS-сервер не є повноцінною захисною системою з точки зору професійного хакера, хоча вирішує деякі питання безпеки на досить успішному рівні.

CGI

Найпростіший варіант сайту або розширення, який виступає в якості посередника між відвідувачем і веб-ресурсом. Його основним суттєвим завданням зазвичай стає отримання надлімітного доступу. Наприклад, якщо правилами сайту допускається певна кількість безкоштовних відвідувань. Враховуючи обмежений функціонал, CGI важко назвати повноцінним проксі-сервером.

Socks (SOCKS)

Найсучасніший і прогресивний проксі. Перша версія мережевого протоколу розроблена досить давно в 1992 році. Сьогодні застосовується четверта та п'ята. Socks-проксі вважається найкращим засобом забезпечення конфіденційності користувача під час відвідування інтернету. Веб-ресурс не тільки не отримує IP-адреси відвідувача, але і не бачить, що контакт відбувається з задіянням Proxy.

Навіщо потрібний Proxy Server

Наведені вище класифікації наочно демонструють широке коло завдань, які здатні вирішувати різні типи та види проксі-серверів. До найбільш актуальних в даний час функцій, що успішно виконуються ними, можна віднести такі:

- Захист конфіденційних даних користувача від збирання пошуковими системами. Причому йдеться не стільки про дії хакерів, скільки про проведення різних рекламних кампаній, розроблених з урахуванням персональної інформації про потенційного покупця;

- Отримання доступу до заблокованих ресурсів. Що стало особливо актуальним після введення антиросійських санкцій і дій вітчизняної влади. Тим більше, що значна частина подібних заходів серйозно зав'язана на інтернет та численні веб-ресурси;
- Збільшення швидкості обміну даними. Відбувається за рахунок кешування файлів, що дозволяє прискорити завантаження інформації і ефективніше використовувати ресурси всіх зацікавлених сторін: як серверів сайту, так і ПК або мобільного пристрою користувача;
- Обмеження доступу до контенту. Завдання, фактично зворотне описаним двома пунктами вище. Полягає в блокуванні інтернет-ресурсів певної спрямованості, наприклад, розважальної;
- Забезпечення безпеки. У цьому випадку наявність посередника між ПК/смартфоном приватної особи або локальною корпоративною мережею та інтернетом дозволяє створити ще один рубіж захисту від дій хакерів або проникнення шкідливих вірусів. Важливо використовувати для цього перевірені (ще краще платні та ліцензовані) файрволи (від англійського firewall брандмауер або міжмережевий захист);
- Тестування ПО. Приватна функція проксі, яка використовується спеціалізованими компаніями - розробниками сайтів. Дозволяє зібрати дані про специфіку роботи в географічному регіоні, де цей веб-ресурс заблокований.
-

Плюси та мінуси проксі

Практичне використання Proxy-сервера супроводжується як плюсами, так і мінусами. До найбільш важливих переваг цього інструменту слід віднести такі:

- Різноманітний функціонал, який визначається типом проксі, що застосовується;
- Опція зміни IP-адреси як одна з найбільш затребуваних функцій сервера;
- Поєднання продуктивності та порівняно високої ефективності;

- Мінімальні вимоги в частини фінансових витрат та використання апаратних ресурсів із сторони користувача;
- Широкий вибір доступних проксі-серверів, включаючи безкоштовні та платні варіанти (приклади найпопулярніших наводяться нижче);
- Універсальність, яка виражається в можливості використання як для забезпечення анонімності користувача, так і для ведення.

Як найпомітніших недоліків застосування проксі-сервера потрібно відзначити три:

- Суттєвий ризик втрати конфіденційних даних, який пов'язаний з автоматичним збором у кеш-пам'яті Proxy і далеко не завжди високим рівнем захисту від несанкціонованого злому;
- Можливість несумісності протоколів локальної мережі та проксі-сервера, яка стає особливо актуальною, якщо останній є безкоштовним або пропонується ненадійним провайдером;
- Низький рівень більшої частини Proxy, які функціонують у безкоштовному режимі, що призводить до необхідності звертатися на платні ресурси та нести супутні витрати.

Ризики проксі

Застосування Proxy неминуче супроводжується певними ризиками. Крім недоліків, описаних вище, необхідно пам'ятати ще про кілька можливих проблем. Перша з них—широкий вибір доступних на сьогодні проксі-серверів. Тому вибір потрібного вимагає вивчення питання і, як наслідок, витрачання часу

Другий істотний ризик полягає в зборі персональних даних користувача, який здійснюється переважно проксі автоматично. Отримана таким чином інформація може використовуватися далі, наприклад для організації та проведення контекстної рекламної кампанії. Причому без будь-якої згоди користувача.

Фактично звідси випливає ще один дуже серйозний ризик. Користувач сам передає конфіденційні відомості про себе третій особі (на додаток до власників сайтів

та інтернет-провайдеру). Ним стає адміністратор Proxy, від рівня професіоналізму якого залежить ступінь безпеки особистої інформації. Що робить проблему вибору відповідного проксі-сервера ще більш актуальною.

Міжмережевий екран (Firewall в перекладі з англійського) - це апаратний або програмний пристрій безпеки мережі, який відстежує весь вхідний і вихідний трафік і на основі визначеного набору правил безпеки приймає, відхиляє або скидає певний трафік. Прийняти : дозволити трафік Відхилити : заблокувати трафік, але відповісти з «помилкою недоступності» Відкинути : заблокувати трафік без відповіді Брандмауер встановлює бар'єр між захищеними внутрішніми мережами та зовнішньою ненадійною мережею, такою як Інтернет.

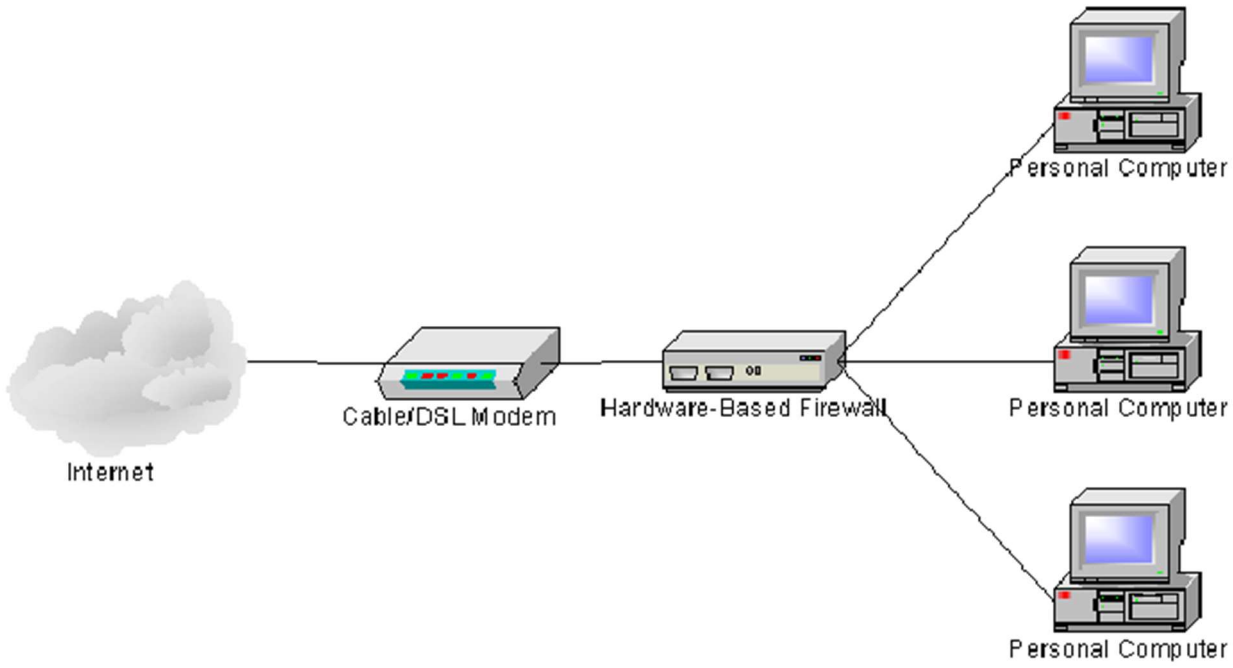


Рис. 7 Схема роботи міжмережевого екрану

До брандмауерів безпека мережі забезпечувалася списками контролю доступу (ACL), які розміщувалися на маршрутизаторах. ACL – це правила, які визначають, чи потрібно надавати або забороняти доступ до мережі для певної IP-адреси. Але ACL не може визначити характер пакета, який він блокує. Крім того, сам по собі ACL не може захистити мережу від загроз. Таким чином, був представлений брандмауер. Підключення до Інтернету більше не є необов'язковим для організацій. Однак доступ

до Інтернету приносить користь організації; це також дозволяє зовнішньому світу взаємодіяти з внутрішньою мережею організації. Це створює загрозу для організації. Щоб захистити внутрішню мережу від несанкціонованого трафіку, нам потрібен брандмауер.

Як працює брандмауер

Брандмауер зіставляє мережевий трафік із набором правил, визначеним у його таблиці. Коли правило збігається, до мережевого трафіку застосовується асоційована дія. Наприклад, правила визначаються так, що будь-який співробітник відділу кадрів не може отримати доступ до даних із сервера кодів, і в той же час визначається інше правило, згідно з яким системний адміністратор може отримати доступ до даних як відділу кадрів, так і технічного відділу. Правила можна визначити на брандмауері на основі необхідності та політики безпеки організації. З точки зору сервера мережевий трафік може бути вихідним або вхідним. Брандмауер підтримує окремий набір правил для обох випадків. Здебільшого пропускається вихідний трафік, що надходить із самого сервера. Тим не менш, установити правило для вихідного трафіку завжди краще, щоб досягти більшої безпеки та запобігти небажаному спілкуванню. Вхідний трафік обробляється інакше. Більшість трафіку, який досягає брандмауера, є одним із цих трьох основних протоколів транспортного рівня - TCP, UDP або ICMP. Усі ці типи мають адресу джерела та адресу призначення. Також TCP і UDP мають номери портів. ICMP використовує код типу замість номера порту, який визначає мету цього пакета. Політика за замовчуванням: дуже важко чітко охопити всі можливі правила брандмауера. З цієї причини брандмауер завжди повинен мати політику за замовчуванням. Політика за умовчанням складається лише з дій (прийняти, відхилити або видалити). Припустімо, що на брандмауері не визначено правило щодо підключення SSH до сервера. Отже, він дотримуватиметься політики за умовчанням. Якщо політика брандмауера за замовчуванням налаштована на приймання , будь-який комп’ютер за межами вашого офісу може встановити з’єднання SSH із сервером. Таким чином, встановлення політики за замовчуванням як видалення (або

відхилення) завжди є хорошою практикою.

Генерація брандмауера

Брандмауери можна класифікувати на основі їхнього покоління.

Брандмауер із фільтрацією пакетів першого покоління: брандмауер із фільтрацією пакетів використовується для керування доступом до мережі шляхом моніторингу вихідних і вхідних пакетів і дозволу їм пропускати або зупиняти на основі IP-адрес джерела й призначення, протоколів і портів. Він аналізує трафік на рівні транспортного протоколу (але в основному використовує перші 3 рівні). Пакетні брандмауери обробляють кожен пакет ізольовано. Вони не можуть визначити, чи є пакет частиною існуючого потоку трафіку. Тільки він може дозволити або заборонити пакети на основі унікальних заголовків пакетів. Брандмауер фільтрації пакетів підтримує таблицю фільтрації, яка вирішує, чи буде пакет переслано чи відхилено.

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Рис. 8 Зразок правила брандмауера фільтра пакетів

З наведеної таблиці фільтрації пакети будуть фільтруватися за такими правилами:

1. Вхідні пакети з мережі 192.168.21.0 заблоковані;
2. Вхідні пакети, призначені для внутрішнього сервера TELNET (порт 23), блокуються;
3. Вхідні пакети, призначені для хосту 192.168.21.3, блокуються;
4. Дозволені всі відомі служби мережі 192.168.21.0;

5. Друге покоління — брандмауер з перевіркою стану: брандмауери з контролем стану (виконує перевірку пакетів із визначенням стану) здатні визначати стан з'єднання пакета, на відміну від брандмауера з фільтрацією пакетів, що робить його ефективнішим. Він відстежує стан мережевого з'єднання, яке проходить через нього, наприклад потоки TCP. Таким чином, рішення щодо фільтрації базуватимуться не лише на визначених правилах, а й на історії пакетів у таблиці стану;

6. Брандмауер рівня додатків третього покоління: брандмауер рівня додатків може перевіряти та фільтрувати пакети на будь-якому рівні OSI, аж до рівня додатків. Він має можливість блокувати певний вміст, а також розпізнавати випадки неправильного використання певних програм і протоколів (наприклад, HTTP, FTP). Іншими словами, брандмауери прикладного рівня — це хости, які запускають проксі-сервери. Брандмауер проксі запобігає прямому з'єднанню між будь-якою стороною брандмауера, кожен пакет має проходити через проксі. Він може дозволяти або блокувати трафік на основі попередньо визначених правил. Примітка. Брандмауери прикладного рівня також можна використовувати як транслятор мережевих адрес (NAT);

7. Брандмауери наступного покоління (NGFW): брандмауери наступного покоління розгортаються сьогодні, щоб зупинити сучасні порушення безпеки, такі як завчасні атаки зловмисного програмного забезпечення та атаки на рівні додатків. NGFW складається з глибокої перевірки пакетів, перевірки додатків, перевірки SSL/SSH і багатьох функцій для захисту мережі від цих сучасних загроз.

Magic Firewall

«Чарівний брандмауер» — це термін, який використовується для опису функції безпеки, наданої компанією з веб-хостингу та безпеки Cloudflare. Це хмарний брандмауер, який забезпечує захист від широкого спектру загроз безпеці, включаючи DDoS-атаки, впровадження SQL, міжсайтовий сценарій (XSS) та інші типи атак, спрямованих на веб-додатки.

Magic Firewall працює, аналізуючи трафік до веб-сайту та використовуючи

набір попередньо визначених правил для виявлення та блокування зловмисного трафіку. Правила базуються на аналізі загроз із різних джерел, у тому числі з власної мережі аналізу загроз компанії, і можуть бути налаштовані власниками веб-сайтів відповідно до їхніх конкретних потреб безпеки.

Magic Firewall вважається «чарівним», тому що він розроблений для безперебійної та непомітної роботи для відвідувачів веб-сайту, без будь-якого помітного впливу на продуктивність веб-сайту. Його також легко налаштувати та керувати, і до нього можна отримати доступ через веб-панель керування Cloudflare.

Загалом, Magic Firewall — це потужний інструмент безпеки, який надає власникам веб-сайтів додатковий рівень захисту від різноманітних загроз безпеці.

Типи брандмауера

Брандмауери зазвичай бувають двох типів: на основі хоста та на основі мережі.

1.Брандмауери на основі хосту: брандмауер на основі хоста встановлюється на кожному вузлі мережі, який контролює кожен вхідний і вихідний пакет. Це програмне забезпечення або набір програм, які є частиною операційної системи. Брандмауери на основі хостів потрібні, оскільки мережеві брандмауери не можуть забезпечити захист у надійній мережі. Брандмауер хоста захищає кожен хост від атак і несанкціонованого доступу.

2.Мережеві брандмауери: функція мережевого брандмауера на рівні мережі. Іншими словами, ці брандмауери фільтрують весь вхідний і вихідний трафік по мережі. Він захищає внутрішню мережу, фільтруючи трафік за правилами, визначеними на брандмауері. Мережевий брандмауер може мати дві або більше карт мережевого інтерфейсу (NIC). Мережевий брандмауер зазвичай є спеціальною системою з інстальованим пропрієтарним програмним забезпеченням.

Переваги використання Firewall

1.Захист від несанкціонованого доступу: можна налаштувати брандмауери для обмеження вхідного трафіку з певних IP-адрес або мереж, запобігаючи легкому

доступу хакерів або інших зловмисників до мережі чи системи. Захист від небажаного доступу.

2.Запобігання зловмисному програмному забезпеченню та іншим загрозам: запобігання зловмисному програмному забезпеченню та іншим загрозам: брандмауери можна налаштувати для блокування трафіку, пов’язаного з відомим зловмисним програмним забезпеченням або іншими проблемами безпеки, допомагаючи в захисті від таких атак.

3.Контроль доступу до мережі: обмежуючи доступ до певних осіб або груп для певних серверів або програм, брандмауери можна використовувати для обмеження доступу до певних мережевих ресурсів або послуг.

4.Моніторинг мережевої активності: брандмауери можна налаштувати для запису та відстеження всієї мережевої активності. Ця інформація має важливе значення для виявлення та вивчення проблем безпеки та інших видів тіньової поведінки.

5.Відповідність нормам: багато галузей зв’язані правилами, які вимагають використання брандмауерів або інших заходів безпеки. Організації можуть дотримуватися цих правил і запобігти будь-яким штрафам за допомогою брандмауера.

6.Сегментація мережі: використання брандмауерів для поділу більшої мережі на менші підмережі зменшує поверхню атаки та підвищує рівень безпеки.

Недоліки використання Firewall

1.Корпоративні мережі: багато підприємств використовують брандмауери для захисту від небажаного доступу та інших ризиків безпеці своїх корпоративних мереж. Ці брандмауери можна налаштувати так, щоб дозволяти лише авторизованим користувачам отримувати доступ до певних ресурсів або послуг і запобігати трафіку з певних IP-адрес або мереж.

2.Урядові організації: Урядові організації часто використовують брандмауери для захисту конфіденційних даних і дотримання таких правил, як HIPAA або PCI-

DSS. Вони можуть використовувати найсучасніші брандмауери, такі як брандмауери наступного покоління (NGFW), які можуть виявляти та зупиняти вторгнення, а також керувати доступом до певних даних і програм.

3.Постачальники послуг: брандмауери використовуються постачальниками послуг для захисту своїх мереж і даних своїх клієнтів, зокрема провайдерів, постачальників хмарних послуг і хостингових компаній. Вони можуть використовувати брандмауери, які приймають величезні обсяги трафіку та підтримують розширені функції, такі як VPN і балансування навантаження.

4.Малі підприємства: малі фірми можуть використовувати брандмауери для відокремлення своїх внутрішніх мереж, обмеження доступу до певних ресурсів або програм і захисту своїх мереж від зовнішніх загроз.

5.Домашні мережі. Для захисту від небажаного доступу та інших загроз безпеці багато домашніх користувачів використовують брандмауери. Брандмауер, вбудований у багато маршрутизаторів, можна налаштувати для блокування вхідного трафіку та обмеження доступу до мережі.

6.Системи промислового контролю (ICS): брандмауери використовуються для захисту систем промислового контролю від незаконного доступу та кібератак у багатьох життєво важливих інфраструктурах, включаючи електростанції, водоочисні споруди та транспортні системи.

Комутатори (Switch з англійського)- е мережевий пристрій, який використовується для з’єднання пристроїв у комп’ютерній мережі. Це важливий компонент будь-якої локальної мережі (LAN), оскільки він дозволяє пристроям спілкуватися один з одним і спільно використовувати такі ресурси, як файли, принтери та доступ до Інтернету.

Він працює на рівні 2 моделі OSI або на рівні каналу даних. Вони з’єднують пристрої в мережу та використовують комутацію пакетів для надсилання, отримання або пересилання пакетів даних або кадрів даних через мережу.

Комутатор у комп’ютерній мережі має багато портів, до яких можна підключати комп’ютери. Коли кадр даних надходить на будь-який порт мережевого

комутатора, він перевіряє адресу призначення, виконує необхідні перевірки та надсилає кадр до відповідного пристрою (пристроїв). Він підтримує одноадресну, багатоадресну та широкомовну передачу.

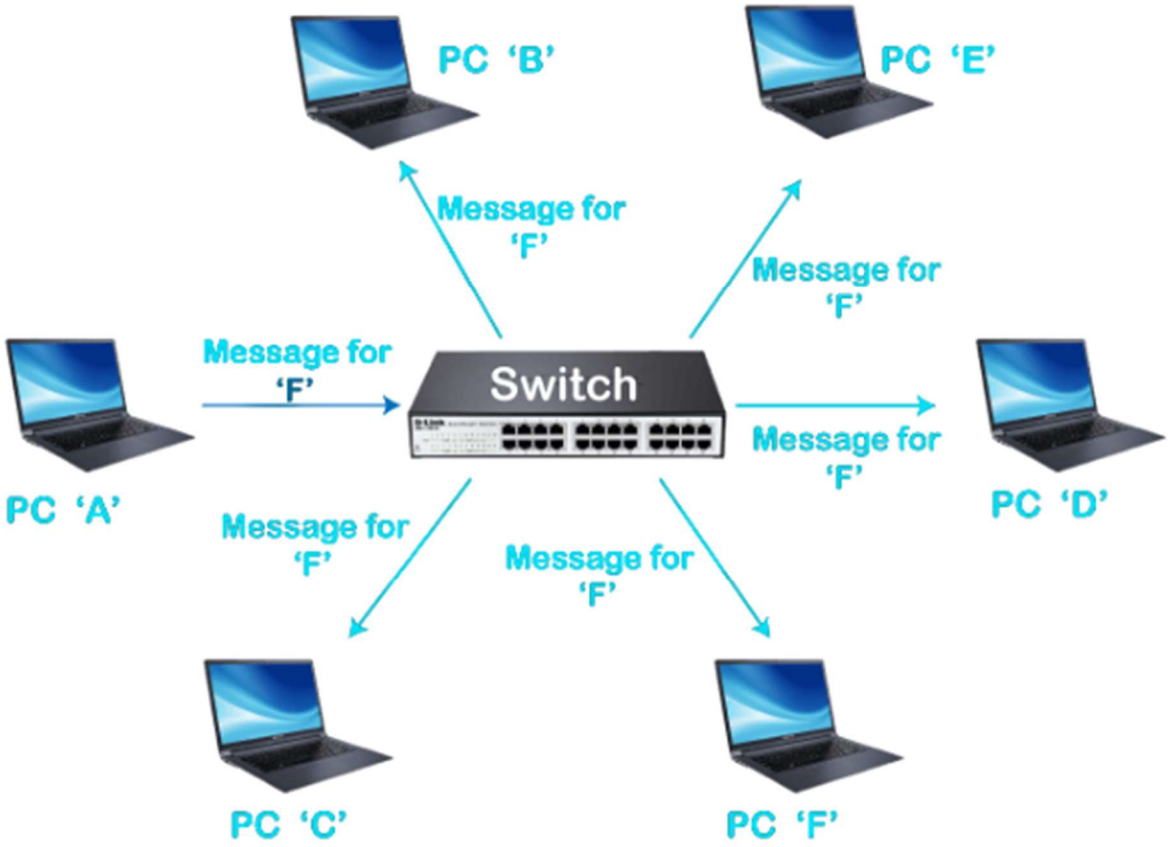


Рис. 9 Робота комутатора в комп'ютерній мережі

Коли джерело хоче надіслати пакет даних до пункту призначення, пакет спочатку потрапляє в комутатор, де його зчитує комутатор, а MAC-адреса адресата знаходить для ідентифікації пристрою перед відправленням через відповідні порти, які привести до пристроїв призначення.

Комутатор створює тимчасове з'єднання між джерелом і одержувачем для зв'язку, а потім розриває з'єднання, коли розмова буде завершена. Крім того, він забезпечує повну пропускну здатність для мережевого трафіку, що одночасно йде до пристрою та від нього, зменшуючи конфлікти.

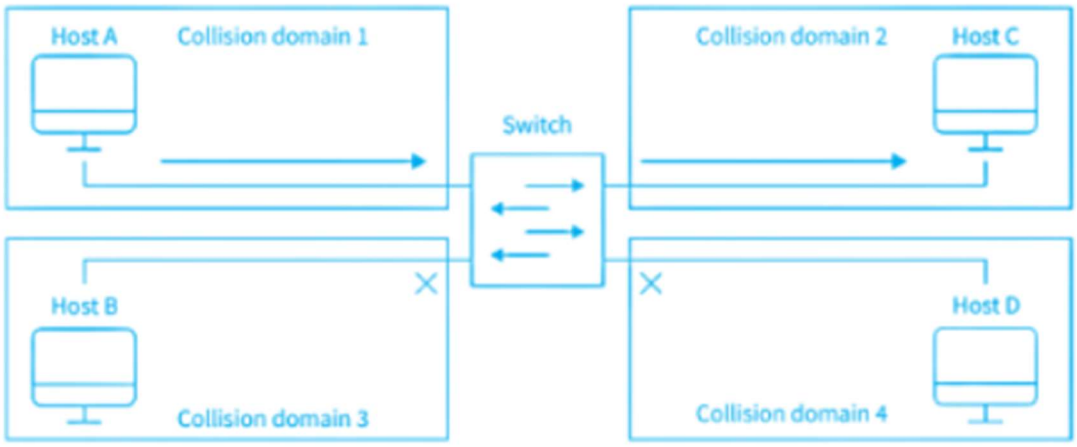


Рис. 10 Типи комутаторів у комп'ютерній мережі

- **Некерований комутатор:** некеровані комутатори є найпростішим типом комутаторів, які не потребують налаштування. Вони зазвичай використовуються в невеликих мережах, де потрібне просте підключення. Ці комутатори мають фіксований набір функцій і не пропонують розширених функцій, таких як якість обслуговування (QoS) або VLAN. Це пристрої, що підключаються та працюють, які просто з'єднують мережеві пристрої.
- **Керований комутатор:** керовані комутатори пропонують розширені функції та параметри конфігурації, такі як VLAN, QoS і віддзеркалення портів. Вони дозволяють мережевим адміністраторам налаштовувати, керувати та контролювати параметри мережі, що робить їх ідеальними для великих мереж, які потребують детальнішого контролю. Керовані комутатори можна додатково класифікувати на два типи: розумні комутатори та повністю керовані комутатори.
- **Комутатор локальної мережі:** комутатор локальної мережі підключає пристрої до внутрішньої локальної мережі компанії. Інші назви — комутатори Ethernet і комутатори даних. Ці комутатори особливо корисні для зменшення перевантаження мережі або вузьких місць. Вони розподіляють смугу пропускання так, щоб пакети даних у мережі не накладалися.

- **Комутатор PoE:** комутатори Power over Ethernet (PoE) використовуються в мережах PoE Gigabit Ethernet. Завдяки технології PoE, яка поєднує передачу даних і електроенергії через одне з'єднання, підключені до неї пристрої можуть отримувати енергію та дані по одній лінії.

Переваги комутатора в комп'ютерній мережі:

- **Підвищення продуктивності мережі:** комутатори допомагають підвищити продуктивність мережі, зменшуючи перевантаження мережі та покращуючи швидкість передачі даних. Це пов'язано з тим, що вони використовують комутацію пакетів, яка дозволяє передавати дані безпосередньо до місця призначення.
- **Покращена безпека:** комутатори підвищують безпеку мережі, дозволяючи адміністраторам створювати VLAN (віртуальні локальні мережі) для сегментації мережі та контролю доступу до конфіденційних даних. Це допомагає запобігти несанкціонованому доступу та захищає від загроз безпеці, таких як порушення даних.
- **Просте керування мережею:** комутатори пропонують централізовану точку контролю для керування мережею, що дозволяє адміністраторам налаштовувати та контролювати налаштування мережі з єдиного місця. Це зменшує потребу в ручному налаштуванні окремих пристроїв і економить час.
- **Масштабованість:** комутатори можна легко додавати або видаляти з мережі, що робить їх масштабованими та адаптованими до мінливих вимог мережі. Це дозволяє легко розширювати мережу в міру зростання організації.

Недоліки комутатора в комп'ютерній мережі:

- **Вартість:** комутатори можуть бути дорожчими за інші мережеві пристрої, такі як концентратори або повторювачі. Це може бути недоліком для невеликих організацій або тих, хто має обмежений бюджет.
- **Складність:** керовані комутатори можуть бути складними та вимагати спеціальних знань для налаштування та керування. Це може бути недоліком для організацій без досвідчених мережевих адміністраторів.

- **Єдина точка відмови:** комутатор може бути єдиною точкою відмови в мережі. Якщо комутатор виходить з ладу, це може призвести до виходу з ладу всієї мережі, що призведе до простою та втрати продуктивності.
- **Обмежена сумісність:** комутатори можуть бути несумісними з усіма мережевими пристроями, особливо зі старими або нестандартними пристроями. Це може обмежити гнучкість мережі та вимагати придбання додаткового обладнання.

Висновок

Комутатори є важливим компонентом сучасних комп'ютерних мереж, що забезпечує ефективний зв'язок між пристроями. Вони пропонують численні переваги, зокрема підвищену швидкість мережі, зменшення перевантажень мережі, покращену безпеку та більшу масштабованість.

Однак комутатори також можуть бути дорогими, складними для налаштування та створювати єдину точку збою. Розуміючи різні типи комутаторів, а також їхні переваги та недоліки, мережеві адміністратори можуть приймати обґрунтовані рішення щодо найкращого комутатора для потреб своєї організації.

Deep packet inspection (Сервери інспектування вмісту) – це глибока перевірка пакетів , яка також відома як DPI, витяг інформації, IX або повна перевірка пакетів, є типом фільтрації мережевих пакетів. Глибока перевірка пакетів оцінює частину даних і заголовок пакета, який передається через точку перевірки, відсіваючи будь-яку невідповідність протоколу, спам, віруси, вторгнення та будь-які інші визначені критерії для блокування проходження пакета через перевірку. точка.

Глибока перевірка пакетів також використовується для визначення того, чи перенаправляється конкретний пакет до іншого пункту призначення. Коротше кажучи, глибока перевірка пакетів здатна знаходити, виявляти, класифікувати, блокувати або перенаправляти пакети, які містять певний код або дані, які не виявляються, не класифікуються, блокуються або не перенаправляються за допомогою звичайної фільтрації пакетів. На відміну від звичайної фільтрації пакетів, глибока перевірка пакетів виходить за рамки перевірки заголовків пакетів.

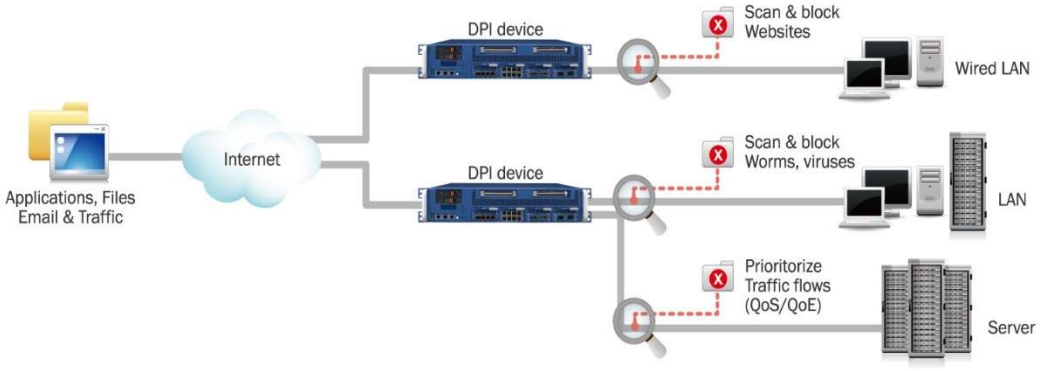


Рис. 11 Схема роботи глибокої перевірки пакетів

Як працює глибока перевірка пакетів

Глибока перевірка пакетів — це форма фільтрації пакетів, яка зазвичай виконується як функція брандмауера. Він застосовується на прикладному рівні взаємодії відкритих систем.

Глибока перевірка пакетів оцінює вміст пакета, який проходить через контрольну точку. Використовуючи правила, призначені вами, вашим постачальником Інтернет-послуг або мережевим чи системним адміністратором, глибока перевірка пакетів визначає, що робити з цими пакетами в реальному часі.

Глибока перевірка пакетів може перевірити вміст цих пакетів, а потім з’ясувати, звідки він надійшов, наприклад служба чи програма, яка його надіслала. Крім того, він може працювати з фільтрами, щоб знаходити та перенаправляти мережевий трафік із онлайн-сервісів, таких як Twitter чи Facebook, або з певної IP-адреси.

Глибока перевірка пакетів проти традиційної фільтрації пакетів

Звичайна фільтрація пакетів зчитує лише інформацію заголовка кожного пакета. Це був базовий підхід, який був менш складним, ніж сучасний підхід до фільтрації пакетів, головним чином через технологічні обмеження на той час. Брандмауери мали дуже низьку обчислювальну потужність, і її було недостатньо для

обробки великих обсягів пакетів. Іншими словами, звичайна фільтрація пакетів була схожа на читання назви книги без усвідомлення чи оцінки вмісту обкладинки.

З появою нових технологій глибока перевірка пакетів стала можливою. У міру того, як він став більш ретельним і повним, це стало більше порівняти з тим, щоб взяти книгу, відкрити її та прочитати від палітурки до палітурки.

Випадки використання для глибокої перевірки пакетів

Існує кілька способів використання глибокої перевірки пакетів. Він може діяти як як система виявлення вторгнень, так і як комбінація запобігання та виявлення вторгнень. Він може ідентифікувати конкретні атаки, які ваш брандмауер, системи запобігання та виявлення вторгнень не можуть адекватно виявити.

Якщо у вашій організації є користувачі, які використовують свої ноутбуки для роботи, глибока перевірка пакетів є життєво важливою для запобігання проникненню хробаків, шпигунського програмного забезпечення та вірусів у вашу корпоративну мережу. Крім того, використання глибокої перевірки пакетів базується на правилах і політиках, визначених вами, що дозволяє вашій мережі виявляти, чи є заборонені використання схвалених програм.

Глибока перевірка пакетів також використовується адміністраторами мереж, щоб полегшити потік мережевого трафіку. Наприклад, якщо у вас є повідомлення з високим пріоритетом, ви можете використовувати глибоку перевірку пакетів, щоб увімкнути високопріоритетну інформацію для негайного проходження, перед іншими повідомленнями з нижчим пріоритетом. Ви також можете визначити пріоритетність критично важливих пакетів перед звичайними пакетами перегляду. Якщо у вас виникають проблеми з одноранговими завантаженнями, ви можете використовувати глибоку перевірку пакетів, щоб зменшити або уповільнити швидкість передачі даних. DPI також можна використовувати для розширення можливостей провайдерів Інтернету речей, щоб запобігти використанню пристроїв Інтернету речей у DDOS-атаках шляхом блокування зловмисних запитів від пристроїв.

Оператори мобільного зв’язку та інші подібні постачальники послуг також використовують глибоку перевірку пакетів, щоб адаптувати свої пропозиції для окремих абонентів, дозволяючи їм диференціювати використання даних як «все, що ви можете з’їсти», стінний сад або додану вартість. Звукозаписні компанії та інші власники авторських прав також можуть вимагати від постачальників Інтернет-послуг заблокувати незаконне завантаження їхнього вмісту – процес досягається шляхом глибокої перевірки пакетів.

В інших випадках глибока перевірка пакетів використовується для показу цільової реклами користувачам, законного перехоплення та застосування політики. Глибока перевірка пакетів також може запобігти деяким типам атак переповнення буфера.

Нарешті, глибока перевірка пакетів може допомогти вам запобігти витоку інформації, наприклад, під час надсилання конфіденційного файлу електронною поштою. Замість того, щоб успішно надіслати файл, користувач натомість отримає інформацію про те, як отримати необхідний дозвіл і дозвіл на його надсилання.

Як і інші технології, глибоку перевірку пакетів також можна використовувати для менш ніж чудових цілей, таких як підслуховування та цензура. Насправді відомо, що уряд Китаю використовує глибоку перевірку пакетів для моніторингу мережевого трафіку країни та цензурує певний вміст і сайти, які завдають шкоди його інтересам. Ось як Китай зміг заблокувати порнографію, релігійну інформацію, матеріали, що стосуються політичного інакомислення, і навіть такі популярні веб-сайти, як Wikipedia, Google і Facebook.

Хоча DPI має багато потенційних варіантів використання, він може легко виявити одержувача або відправника вмісту, який він відстежує, тому є деякі занепокоєння щодо конфіденційності. Це насамперед викликає занепокоєння, коли DPI використовується в контексті маркетингу та реклами, шляхом моніторингу поведінки користувачів і продажу веб-перегляду та інших даних маркетинговим або рекламним компаніям.

Методи глибокої перевірки пакетів

Глибоку перевірку пакетів використовують два основні типи продуктів: брандмауери, у яких реалізовані такі функції IDS, як перевірка вмісту, і системи IDS, спрямовані на захист мережі, а не на виявлення атак. Деякі з основних методів , які використовуються для глибокої перевірки пакетів, включають:

- Зіставлення шаблону або підпису – один із підходів до використання брандмауерів, які використовують функції IDS, зіставлення шаблону чи підпису, аналізує кожен пакет із базою даних відомих мережевих атак. Недоліком цього підходу є те, що він ефективний лише для відомих атак, а не для атак, які ще не виявлені;
- Аномалія протоколу – ще один підхід до використання брандмауерів із функціями IDS, аномалія протоколу використовує підхід «відмови за замовчуванням», який є ключовим принципом безпеки. Використовуючи цю техніку, визначення протоколу використовуються для визначення того, який вміст слід дозволити. Це відрізняється від підходу простого дозволу всього вмісту, який не відповідає базі даних підписів, як це відбувається у випадку зіставлення шаблону або підпису. Основна перевага аномалії протоколу полягає в тому, що вона пропонує захист від невідомих атак;
- Рішення IPS – деякі рішення IPS використовують технології DPI. Ці рішення мають подібну функціональність до вбудованих IDS, хоча вони мають можливість блокувати виявлені атаки в режимі реального часу. Однією з найбільших проблем у використанні цієї методики є ризик помилкових спрацьовувань, який можна певною мірою зменшити шляхом створення консервативної політики.

Деякі обмеження існують для цих та інших методів DPI, хоча постачальники пропонують рішення, спрямовані на усунення практичних та архітектурних проблем за допомогою різних засобів. Крім того, рішення DPI тепер пропонують низку інших безкоштовних технологій, таких як VPN, аналіз зловмисного програмного забезпечення, фільтрація спаму, фільтрація URL-адрес та інші технології, забезпечуючи більш повний захист мережі.

Проблеми глибокої перевірки пакетів

Жодна технологія не є ідеальною, і глибока перевірка пакетів не є винятком. Він має три чіткі недоліки:

1. Глибока перевірка пакетів дуже ефективна для запобігання таким атакам, як атаки на відмову в обслуговуванні, атаки переповнення буфера та навіть деякі форми зловмисного програмного забезпечення. Але його також можна використовувати для створення подібних атак .

2. Глибока перевірка пакетів може зробити ваш поточний брандмауер та інше програмне забезпечення безпеки, яке ви використовуєте, складнішим і важчим для керування . Ви повинні бути впевнені, що ви постійно оновлюєте та переглядаєте політики глибокої перевірки пакетів, щоб забезпечити постійну ефективність.

3. Глибока перевірка пакетів може уповільнити вашу мережу , виділивши ресурси для брандмауера, щоб він міг справлятися з навантаженням обробки.

Крім проблем конфіденційності та властивих обмежень глибокої перевірки пакетів, деякі проблеми виникли через використання сертифікатів HTTPS і навіть VPN з тунелюванням конфіденційності. Деякі брандмауери тепер пропонують перевірку HTTPS, яка розшифровує трафік, захищений HTTPS, і визначає, чи дозволено проходження вмісту. Однак глибока перевірка пакетів продовжує залишатися цінною практикою для цілей, починаючи від управління продуктивністю до мережевої аналітики, криміналістики та безпеки підприємства.

Сервери DNS - система доменних імен (DNS) — це база даних імен, у якій розташовані імена доменів Інтернету та переведені в адреси Інтернет-протоколу (IP). Система доменних імен зіставляє ім’я, яке люди використовують для пошуку веб-сайту, на IP-адресу, яку комп’ютер використовує для пошуку цього веб-сайту.

Наприклад, якщо хтось вводить «example.com» у веб-браузер, сервер за кадром відображає це ім’я на відповідну IP-адресу. Структура IP-адреси схожа на 203.0.113.72.

Перегляд веб-сторінок і більшість інших дій в Інтернеті покладаються на DNS для швидкого надання інформації, необхідної для підключення користувачів до

віддалених хостів. Відображення DNS розподілено по всьому Інтернету в ієрархії повноважень. Постачальники доступу та підприємства, а також уряди, університети та інші організації зазвичай мають власні призначені діапазони IP-адрес і призначене доменне ім'я. Вони також зазвичай запускають DNS-сервери для керування відображенням цих імен на ці адреси. Більшість уніфікованих покажчиків ресурсів (URL) побудовано навколо імені домену веб-сервера, який приймає запити клієнтів.

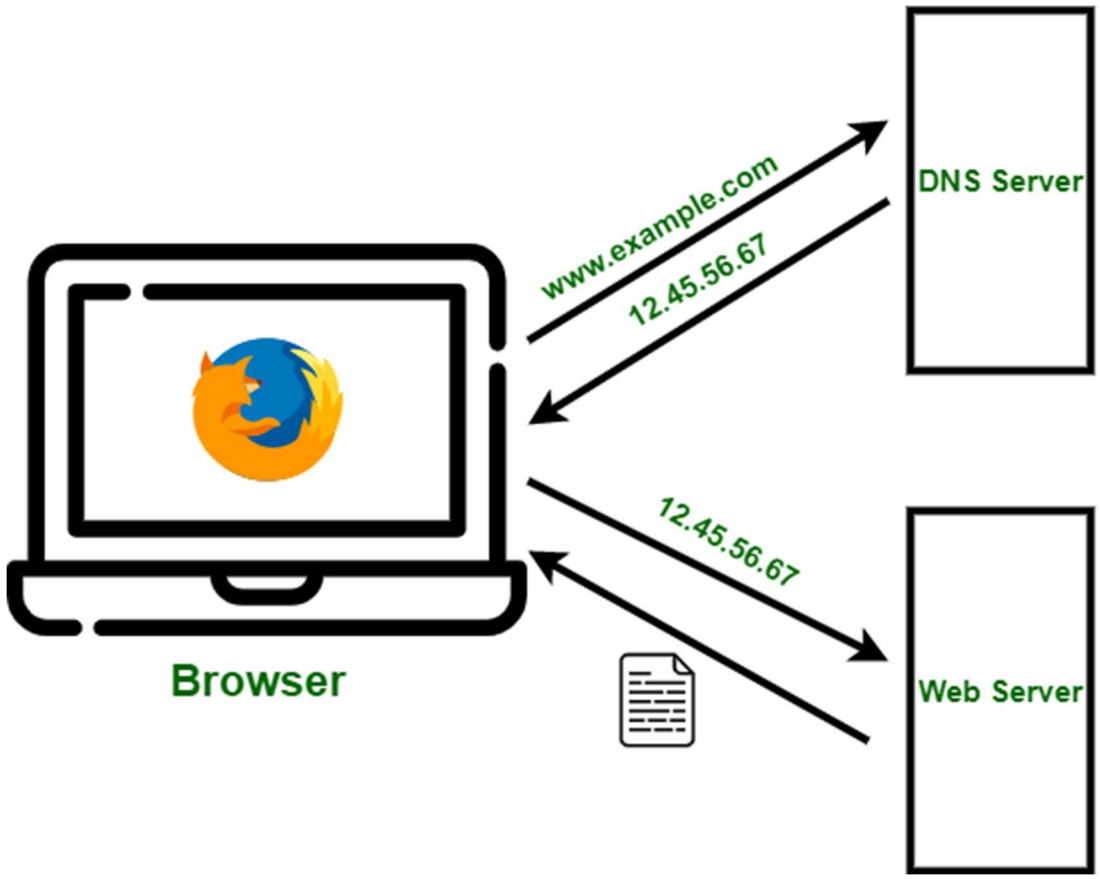


Рис. 12 Схема роботи DNS

Як працює DNS

DNS-сервери перетворюють URL-адреси та доменні імена в IP-адреси, які комп'ютери можуть розуміти та використовувати. Вони перетворюють те, що користувач вводить у браузері, у те, що машина може використати для пошуку веб-сторінки. Цей процес перекладу та пошуку називається розділенням DNS .

Основний процес вирішення DNS складається з таких кроків:

1. Користувач вводить веб-адресу або доменне ім’я в браузер;

2. Браузер надсилає в мережу повідомлення, яке називається рекурсивним DNS-запитом , щоб дізнатися, якій IP-адресі чи мережевій адресі відповідає домен;

3. Запит надсилається до рекурсивного DNS-сервера , який також називається рекурсивним розв’язувачем і зазвичай керується постачальником послуг Інтернету (ISP). Якщо рекурсивний розпізнавач має адресу, він поверне адресу користувачеві, і веб-сторінка завантажиться;

4. Якщо рекурсивний DNS-сервер не має відповіді, він надішле запит серії інших серверів у такому порядку: кореневі сервери імен DNS, сервери імен домену верхнього рівня (TLD) і авторитетні сервери імен;

5. Три типи серверів працюють разом і продовжують перенаправляти, доки не отримають запис DNS, який містить запитувану IP-адресу. Він надсилає цю інформацію на рекурсивний DNS-сервер, і завантажується веб-сторінка, яку шукає користувач. Кореневі сервери імен DNS і сервери верхнього рівня в основному перенаправляють запити та рідко самі забезпечують вирішення;

6. Рекурсивний сервер зберігає, або кешує , запис A для імені домену, який містить IP-адресу. Наступного разу, коли він отримає запит на це доменне ім’я, він зможе відповісти безпосередньо користувачеві замість того, щоб запитувати інші сервери;

7. Якщо запит досягає авторитетного сервера і він не може знайти інформацію, він повертає повідомлення про помилку.

Весь процес надсилання запитів до різних серверів займає частки секунди і зазвичай непомітний для користувача.

DNS-сервери відповідають на запитання як усередині, так і за межами власних доменів. Коли сервер отримує запит із-за меж домену щодо інформації про ім’я чи адресу всередині домену, він надає повноважну відповідь.

Коли сервер отримує запит із свого домену на ім’я чи адресу за межами цього домену, він пересилає запит на інший сервер, зазвичай той, яким керує його провайдер.

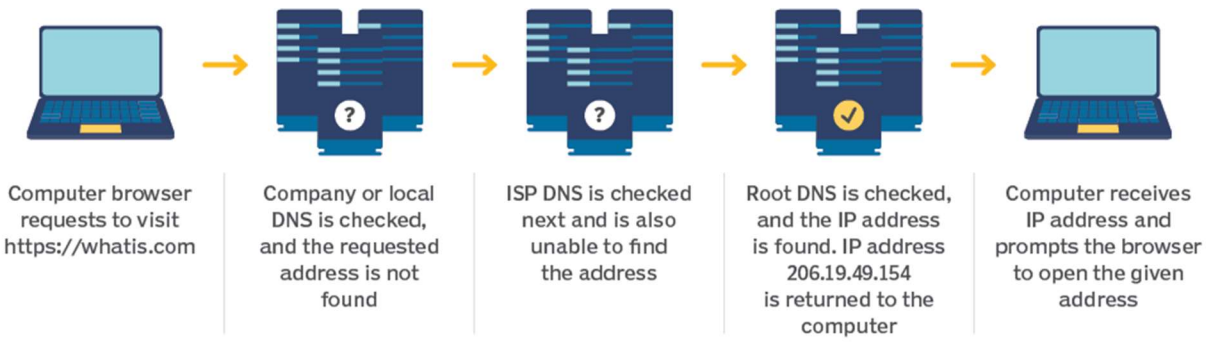


Рис. 13 Структура роботи DNS

Структура DNS

Доменне ім’я зазвичай міститься в URL-адресі. Доменне ім’я складається з кількох частин, які називаються мітками . Ієрархія домену читається справа наліво, кожен розділ позначає підрозділ.

ДВУ з’являється після крапки в доменному імені. Прикладами доменів верхнього рівня є .com, .org і .edu, але є багато інших. Деякі можуть позначати код країни або географічне розташування, наприклад .us для Сполучених Штатів або .ca для Канади.

Кожна мітка ліворуч від TLD позначає інший субдомен домену праворуч. Наприклад, в URL-адресі www.techtarget.com "techtarget" є субдоменом .com, а "www." є субдоменом techtarget.com.

Може бути до 127 рівнів субдоменів, а кожна мітка може містити до 63 символів. Загальна довжина домену може складати до 253 символів. Інші правила включають заборону починати або закінчувати мітки дефісами та не мати повністю цифрового імені TLD.

Інженерна робоча група Інтернету (IETF) визначила правила щодо впровадження доменних імен у запиті на коментарі (RFC) 1035.

Типи DNS-серверів

Існує кілька типів серверів , залучених до завершення вирішення DNS. У наведеному нижче списку описано чотири сервери імен у тому порядку, в якому через них проходить запит. Вони надають шукане доменне ім’я або перенаправлення на інші сервери імен.

- Рекурсивний сервер. Рекурсивний сервер приймає DNS-запити від програми, наприклад веб-браузера. Це перший ресурс, до якого користувач отримує доступ, і він або надає відповідь на запит, якщо він є в кеші, або звертається до сервера наступного рівня, якщо його немає. Цей сервер може пройти кілька ітерацій запитів, перш ніж повернути відповідь клієнту;
- Кореневий сервер імен. Цей сервер є першим місцем, куди рекурсивний сервер надсилає запит, якщо він не має кешованої відповіді. Кореневий сервер імен — це індекс усіх серверів, які матимуть запитувану інформацію. Ці сервери контролюються Інтернет-корпорацією з присвоєння імен і номерів, зокрема філією ICANN , що називається Управлінням з присвоєння номерів Інтернету;
- Сервер верхнього рівня. Кореневий сервер направляє запит на основі домену верхнього рівня – .com, .edu або .org в URL-адресі. Це більш конкретна частина пошуку;
- Авторитетний сервер імен. Авторитетний сервер імен є кінцевою контрольною точкою для запиту DNS. Ці сервери знають усе про даний домен і мають справу з субдоменною частиною доменного імені. Ці сервери містять записи ресурсів DNS із певною інформацією про домен, наприклад запис A. Вони повертають необхідний запис на рекурсивний сервер, щоб надіслати назад клієнту та кешувати його ближче до клієнта для майбутніх пошуків.

Простий спосіб поглянути на процес: рекурсивний сервер в основному запитує від імені користувача, а авторитетний сервер в першу чергу відповідає на запит користувача. Кореневий сервер і сервер верхнього рівня обробляють запит під час його переміщення від рекурсивного сервера до належного центру.

Типи DNS-запитів

Наступні типи DNS-запитів є основними, які мають місце в різних точках вирішення DNS:

- Рекурсивні DNS-запити – це запити, які виконуються між рекурсивним сервером і клієнтом. Надається відповідь або повне розпізнавання імені, або повідомлення про помилку про те, що ім’я не знайдено. Рекурсивні запити закінчуються або відповіддю, або помилкою;
- Ітераційні DNS-запити виконуються між рекурсивним резолвером, який є локальним DNS-сервером, і нелокальними серверами імен, такими як кореневий, TLD і авторитетні сервери імен. Ітераційні запити не вимагають вирішення імені; замість цього сервери імен можуть відповісти рефералом. Кореневий сервер посилає рекурсивний сервер на TLD, який направляє його на авторитетний сервер. Авторитетний сервер надає доменне ім’я рекурсивному серверу, якщо воно є. Ітераційні запити вирішуються як відповідь, так і реферал;
- Нерекурсивні запити – це ті, для яких рекурсивний розв’язувач уже знає, де отримати відповідь. Відповідь або кешується на рекурсивному сервері, або рекурсивний сервер знає, що потрібно пропустити кореневий сервер і сервери верхнього рівня та перейти безпосередньо до певного авторитетного сервера. Він нерекурсивний, тому що немає потреби — і, отже, немає запиту — у додаткових запитах. Нерекурсивні запити вирішуються у відповіді. Якщо рекурсивний розпізнавач кешує IP-адресу з попереднього сеансу та обслуговує цю адресу під час наступного запиту, це вважається нерекурсивним запитом.

У базовому процесі DNS клієнт робить рекурсивний запит до рекурсивного розв’язувача, який потім робить серію ітеративних запитів, які призводять до перенаправлення до наступного ітераційного запиту. Зрештою, запит надходить до авторитетного сервера, який, якщо рекурсивний розв’язувач знає, що знайде відповідь там, робить нерекурсивний запит для її отримання. Потім інформація зберігається в рекурсивному розв’язувачі (див. розділ «Кешування DNS»), щоб нерекурсивний запит міг отримати її в майбутньому.

Загальні записи DNS

Записи DNS — це інформація, яку шукає запит. Залежно від запиту, клієнта чи програми потрібна різна інформація. Деякі записи є обов'язковими, наприклад запис A.

Існує багато типів записів DNS, кожен із яких має власну мету вказувати, як слід обробляти запит. Загальні записи DNS:

- Запис. Це означає адресу та містить IP-адресу домену. Записи A застосовуються лише до адрес IPv4. Натомість адреси IPv6 мають записи AAAA, які використовують довший формат адрес IPv6. Більшість веб-сайтів мають лише один запис A, але деякі більші сайти мають кілька, що допомагає з балансуванням навантаження, обслуговуючи різні записи A різним користувачам у великому трафіку;
- Запис NS. Ці записи сервера імен вказують на те, який авторитетний сервер відповідає за всю інформацію про даний домен. Часто для підвищення надійності домени мають як основний, так і резервний сервери імен, а для спрямування запитів до них використовуються кілька записів NS;
- TXT запис . Записи TXT дозволяють адміністраторам вводити текст у DNS. Початкова мета полягала в тому, щоб розміщувати нотатки, які читаються людиною, у DNS, але сьогодні туди часто розміщують нотатки, які читаються машиною. Записи TXT використовуються для підтвердження права власності на домен, безпечної електронної пошти та боротьби зі спамом;
- Запис CNAME . Записи канонічного імені використовуються замість запису A, якщо є псевдонім. Вони використовуються для повторного запиту тієї самої IP-адреси з двома різними доменами. Прикладом може бути URL-адреса searchsecurity.techtarget.com, де CNAME надсилатиме запит techtarget.com.

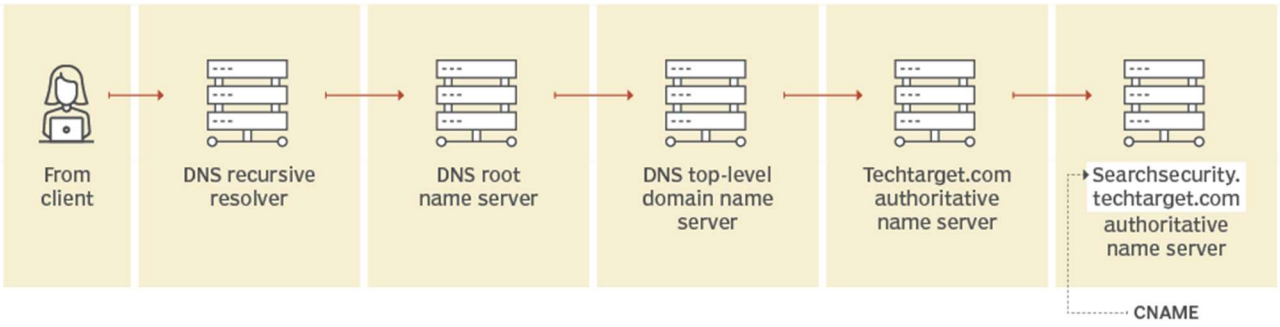


Рис. 14 Схема роботи запису CNAME

Як DNS підвищує продуктивність Інтернету

Сервери можуть кешувати записи A або IP-адреси, які вони отримують із запитів DNS протягом встановленого періоду часу. Кешування підвищує ефективність, дозволяючи серверам швидко відповідати наступного разу, коли надходить запит на ту саму IP-адресу.

Наприклад, якщо кожному в офісі потрібно отримати доступ до того самого навчального відео на певному веб-сайті в той самий день, локальний DNS-сервер повинен буде вирішити ім’я лише один раз, а потім він зможе обслуговувати всі інші запити зі свого кешу. Тривалість зберігання запису, також відома як час життя (TTL), встановлюється адміністраторами та залежить від різних факторів. Довші періоди часу зменшують навантаження на сервери, а коротші забезпечують найточніші відповіді.

Кешування DNS

Метою кешування DNS є скорочення часу, необхідного для отримання відповіді на запит DNS. Кешування дозволяє DNS зберігати попередні відповіді на запити ближче до клієнтів і швидше отримувати ту саму інформацію під час наступного запиту.

Дані DNS можна кешувати в кількох місцях. Деякі поширені включають наступне:

- Браузер. Більшість браузерів, як-от Apple Safari, Google Chrome і Mozilla Firefox, кешують дані DNS за замовчуванням протягом певного періоду часу. Браузер є першим кеш-пам’яттю, яке перевіряється під час надсилання запиту DNS, перш ніж запит залишить машину на локальний сервер розпізнавання DNS;
- Операційна система (ОС). Багато ОС мають вбудовані DNS-розпізначі, які називаються заглушками , які кешують дані DNS і обробляють запити перед їх надсиланням на зовнішній сервер. Зазвичай запит до ОС надсилається після браузера або іншої програми для запитів;
- Рекурсивний розв'язувач. Відповідь на DNS-запит також може бути кешована в рекурсивному резолвері DNS. Резолвери можуть мати деякі записи, необхідні для повернення відповіді, і мати можливість пропустити деякі кроки в процесі вирішення DNS. Наприклад, якщо резолвер має записи A, але не має записів NS, резолвер може пропустити кореневий сервер і запитати безпосередньо сервер TLD.

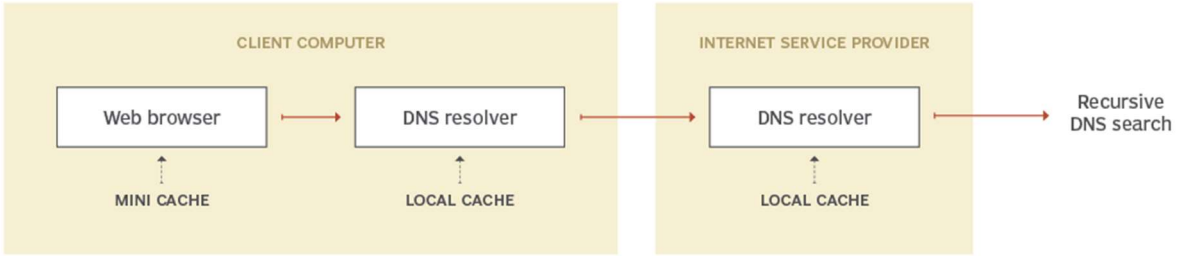


Рис. 15 Схема роботи кешування DNS

Безпека DNS

У DNS дійсно є кілька вразливостей, які були виявлені з часом. Отруєння кешу DNS є однією з таких вразливостей. У разі отруєння кешу DNS дані розподіляються

до кеш-резольверів, видаючи себе за авторитетний вихідний сервер. Тоді дані можуть представляти неправдиву інформацію та впливати на TTL. Фактичні запити програм також можуть бути перенаправлені до зловмисної хост-мережі.

Особа зі зловмисними намірами може створити небезпечний веб-сайт із оманливою назвою та спробувати переконати користувачів, що веб-сайт справжній, надаючи хакеру доступ до інформації користувача. Замінивши символ у доменному імені на схожий на вигляд символ, наприклад, замінивши цифру 1 на літеру l, яка може виглядати подібно, користувача можна ввести в оману, вибравши хибне посилання. Це зазвичай використовується під час фішингових атак.

Для безпеки окремі особи можуть використовувати розширення безпеки DNS. Вони підтримують криптографічно підписані відповіді.

Мережеві адаптери

NIC називається картою мережевого інтерфейсу, також відомою як контролер мережевого інтерфейсу. Мережева карта — це мережевий компонент, який працює на другому канальному рівні. Зазвичай це друкована плата, встановлена на комп’ютері для підключення до мережі та забезпечує приватне підключення до мережі для комп’ютера. Хоча мережевий адаптер є невеликою частиною підключення комп’ютера до мережі, він відіграє незамінну роль. Мережеві адаптери діють як перетворювачі, перетворюючи дані в цифрові сигнали, які передаються за допомогою кабелів або бездротових маршрутизаторів у серверній мережі. Як інтерфейс на рівні TCP/IP мережевий адаптер може передавати сигнали на фізичному рівні та пакети на мережевому рівні. Незалежно від рівня, він діє як посередник між комп’ютером/сервером і мережею даних. Коли користувач запитує веб-сторінку, локальна мережа отримує дані з пристрою користувача, надсилає їх на мережевий сервер, а потім отримує необхідні дані для представлення користувачеві.

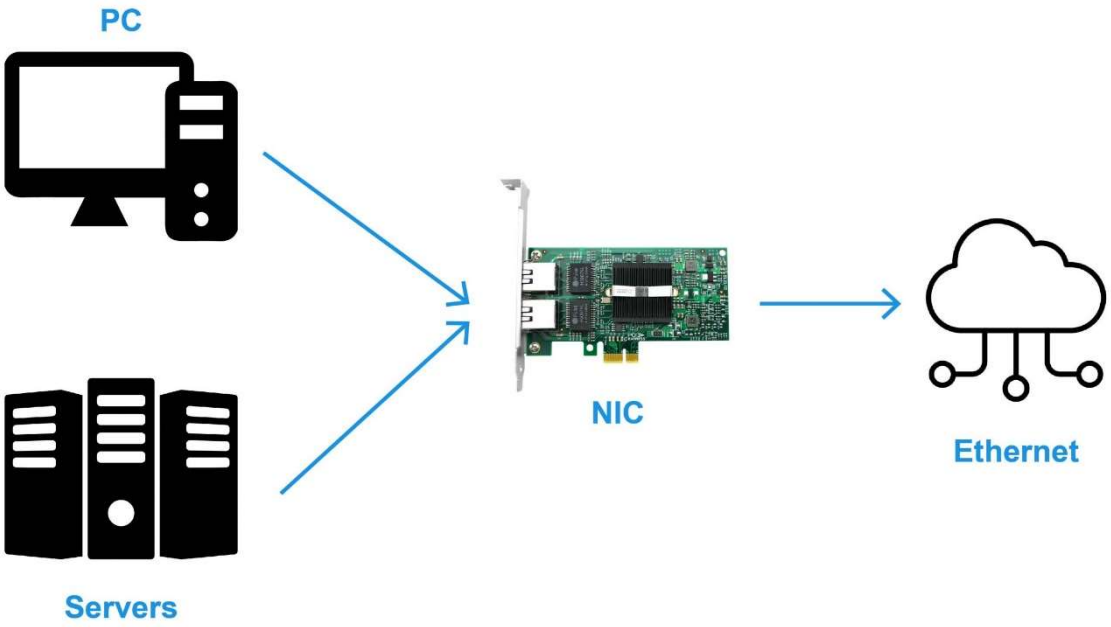


Рис. 16 Схема роботи мережевого адаптеру

Компоненти NI

Традиційно мережевий адаптер складається з контролера, слота Boot ROM, одного чи кількох портів NIC , порту материнської плати, світлодіодних індикаторів, кронштейна та деяких інших електронних компонентів. Кожен компонент виконує свою унікальну функцію:

- Контролер : як основна частина мережевої карти, контролер безпосередньо визначає продуктивність мережевої карти. Контролер діє як невеликий центральний процесор для обробки вхідних даних;
- Гніздо Boot ROM : це гніздо дозволяє активувати функцію Boot ROM, яка дозволяє бездисковим робочим станціям підключатися до мережі, тим самим підвищуючи безпеку та знижуючи витрати на обладнання;
- Порт NIC : Зазвичай цей порт безпосередньо підключається до кабелю Ethernet або оптичного модуля для генерування та отримання сигналів від мережевих кабелів або оптоволоконних перемичок;

- Інтерфейс шини : Цей інтерфейс розташований збоку від друкованої плати, інтерфейс шини, широко відомий як «Золотий палець», вставляється в слот розширення материнської плати комп’ютера та використовується для з’єднання між мережевою картою та комп’ютером або сервером;
- Світлодіодний індикатор : індикатор допомагає користувачам визначити робочий стан мережевого адаптера, чи підключено мережу та чи передаються дані. Наприклад, Link/Act вказує на активний стан підключення, Full вказує, чи є воно повним дуплексом, а Power є індикатором Power;
- Кронштейн : на ринку мережевих карт PCI є два типи кронштейнів: один — це кронштейн повної висоти висотою 120 мм, а інший — кронштейн половинної висоти висотою 80 мм. Кронштейн може допомогти користувачеві закріпити мережеву карту в слоті розширення комп'ютера або сервера.

Рис. 17 Контролер компонента NI

Типи

Мережевих адаптерів NIC можна класифікувати на такі типи відповідно до інтерфейсу шини, швидкості передачі та домену програми.

Класифікація за протоколом

Відповідно до протоколу передачі мережеві адаптери можна розділити на три типи: карта Ethernet, карта FC і карта IB.

- Ethernet-карта (Ethernet-адаптер) : використовується протокол IP як протокол передачі, зазвичай підключається до Ethernet-комутатора за допомогою оптоволоконного кабелю або кабелю витої пари. Оптичний порт використовує волоконно-оптичний кабель для передачі даних, а інтерфейсом відповідного модуля зазвичай є SFP, QSFP тощо. Відповідними волоконно-оптичними інтерфейсами є LC, SC, MPO тощо. Загальним типом інтерфейсу електричного порту є RJ45, який зазвичай підключається за допомогою кабелю вита пара, а також є невелика кількість інтерфейсів, підключених за допомогою коаксіального кабелю;
- Картка FC : наукова назва Fibre Channel. Він використовує протокол передачі Fibre Channel і підключається до комутатора Fibre Channel через оптичні кабелі. Існує два типи інтерфейсів: оптичний і електричний. Режими передачі та відповідні модулі оптичних портів подібні до плат Ethernet, але відповідними портами є лише SC і LC. Тип електричного інтерфейсу - DB9 або HSSDC;
- Картка IB : Infiniband використовується для підключення пристроїв FC/IP SAN, пристроїв NAS і серверів, а також використовується як протокол зберігання iSCSI RDMA. Карти InfiniBand забезпечують наднизьку затримку, надвисоку пропускну здатність та інноваційні мережеві обчислювальні механізми, які забезпечують прискорення, масштабованість і багатофункціональні технології, необхідні для сучасних сучасних робочих навантажень.

Класифікація за швидкістю передачі

Залежно від швидкості існують самоадаптивні карти 10/100 Мбіт/с, гігабітні карти 1000 Мбіт/с, 10G, 25G, 100G і навіть більш швидкісні карти.

Самоадаптивна карта 10 Мбіт/с/100 Мбіт/с: зараз це популярний тип мережевої карти. Він може автоматично адаптуватися до двох різних вимог до пропускної здатності мережі. Його можна підключати до старих мережевих пристроїв зі швидкістю 10 Мбіт/с, а також можна застосовувати для підключення нових мережевих пристроїв зі швидкістю 100 Мбіт/с, тому його широко визнали користувачі.

Мережевий адаптер 1000 Мбіт/с: забезпечує вищу пропускну здатність для швидкого Ethernet. Gigabit Ethernet — це високошвидкісна технологія локальної мережі, яка забезпечує пропускну здатність 1 Гбіт/с через мідні дроти. Відповідна мережева карта є гігабітною мережевою картою, яка також може досягати пропускної здатності 1 Гбіт/с. Існує два типи мережевих інтерфейсів для гігабітних мережевих адаптерів: один — це звичайна вита пара RJ45, а інший — гігабітний оптоволоконний інтерфейс SFP/GBIC.

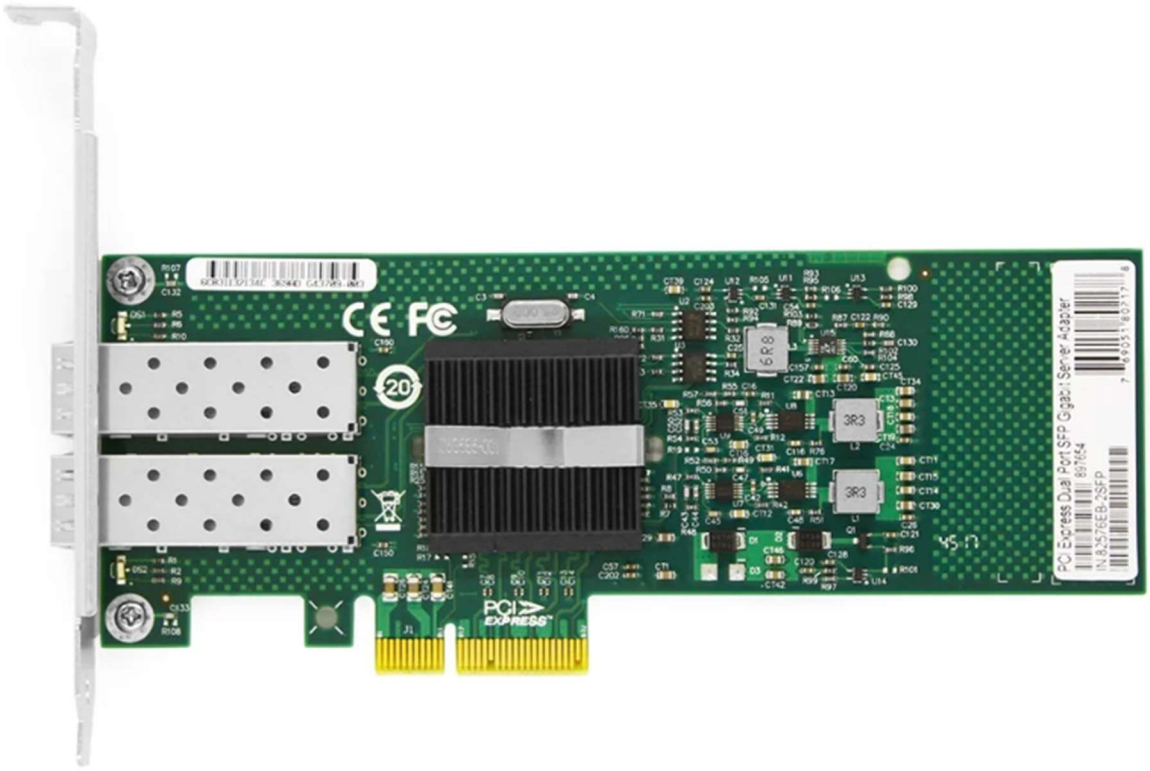


Рис. 18 Мережава картка 10G

Оптоволоконна мережева карта 10G : основною мережею є карта 10G Ethernet. Як і карти Gigabit Ethernet, карти 10G Ethernet підтримують одномодове або багатомодове оптоволокно. Використання карт 10G Ethernet дає мережевим операторам більше свободи для розміщення центрів обробки даних і підтримки кількох кампусних мереж у межах 80 кілометрів одна від одної одночасно. У центрах обробки даних недороге багатомодове оптоволокно може використовуватися як магістраль мережі 10G між комутаторами та комутаторами, а також між комутаторами та серверами.

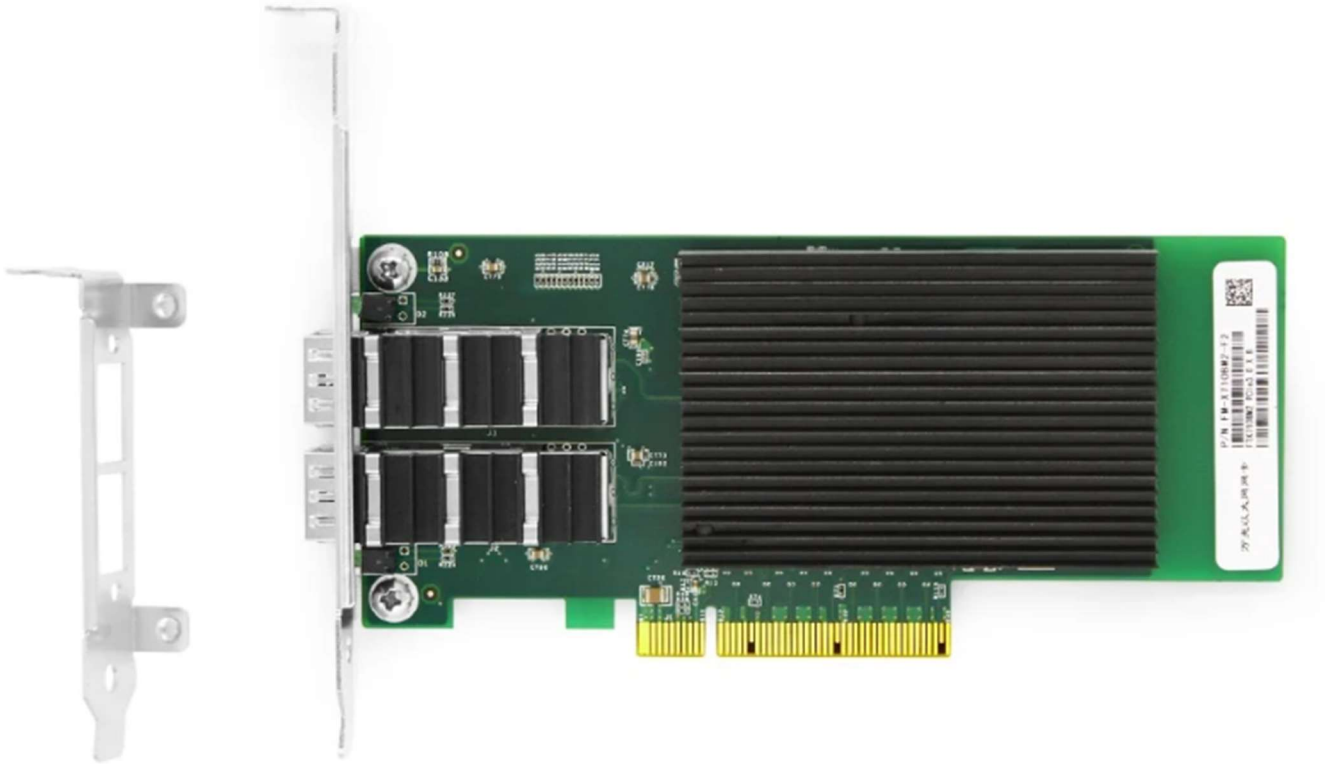


Рис. 19 Мережава картка 25G

Оптоволоконний мережевий адаптер 25G : порівняно з оптоволоконним мережевим адаптером 10G більша пропускна здатність адаптера оптоволоконної мережі 25G відповідає мережевим вимогам високопродуктивного обчислювального кластера. Під час оновлення мережі зі швидкістю 100G або вище волоконний мережевий адаптер 25G є однією з незамінних інфраструктур. У процесі оновлення центру обробки даних з 10G/40G до 25G/100G (інтерфейс сервера — 25G, інтерфейс з'єднання комутаторів — 100G), все більше людей підтримують 25GbE, включаючи Google, Microsoft та інших великих хмарних постачальників для абсолютного розпізнавання 25G.

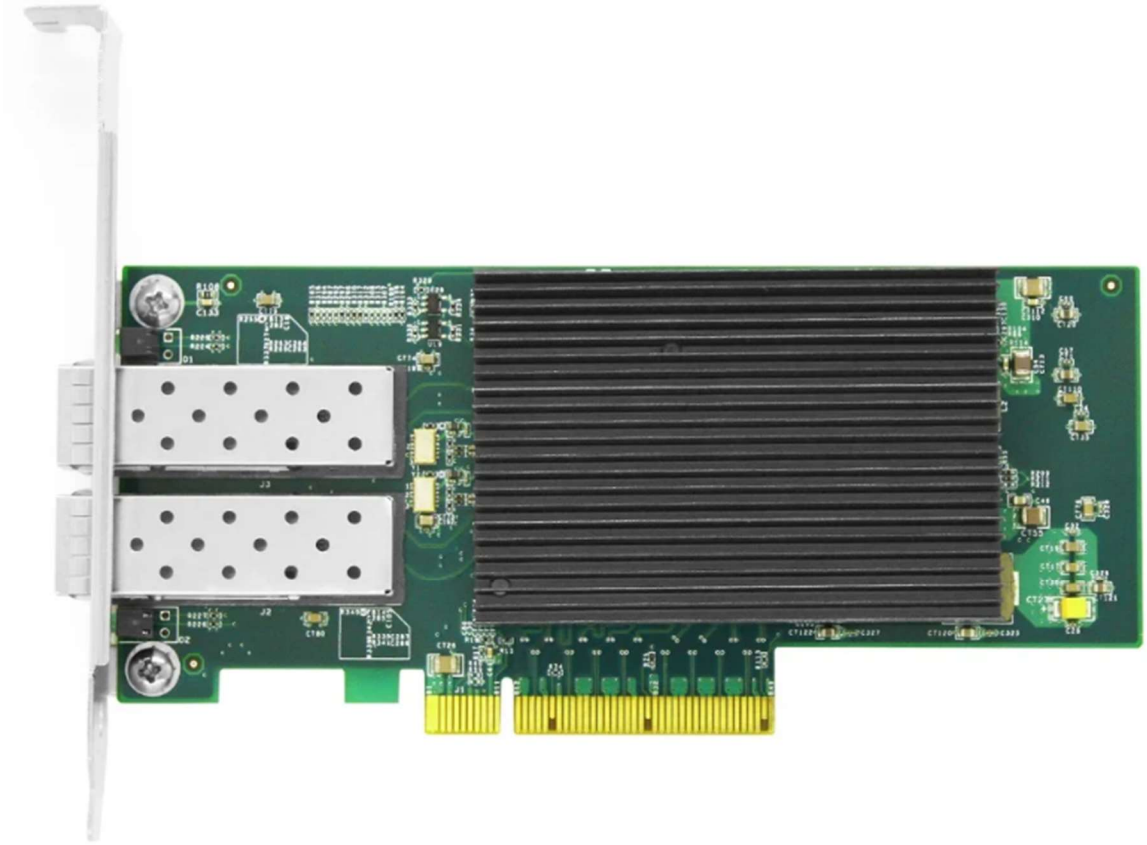


Рис. 20 Мережава картка 40G

Оптоволоконна мережева карта 40G : порт 40G QSFP+, який в основному використовується для серверів і пристроїв високого класу. Оптичний мережевий адаптер 40G оптичного порту QSFP забезпечує просту інтеграцію в будь-який PCI Express X8 з оптимізованою продуктивністю мережі 40Gigabit таким чином, щоб системний вхід/вихід не був вузьким місцем у високопродуктивних мережевих програмах. Він може підтримувати пропускну здатність 40 Гбіт/с і стандартний слот PCI-E X8, забезпечуючи ефективну та стабільну роботу мережевої карти. Крім того, мережевий адаптер підтримує такі функції, як VLAN, політика QOS і контроль трафіку, що підходить для середніх і великих додатків локальної мережі.

Рис.21 Мережава картка 100G

Адаптер волоконно-оптичної мережі 100G : Зі збільшенням попиту на масову передачу даних серверам зазвичай потрібно встановлювати кілька мережевих адаптерів, щоб задовольнити високий попит на обробку даних. Завдяки цій функції мережа центру обробки даних поступово оновлюється з мережевих адаптерів 10G до 100G або навіть вищих тарифів. Мережевий адаптер 100G має високу пропускну здатність, низьку затримку мережевої обробки та здатність допомагати ЦП розвантажувати мережеві функції, заощаджуючи обчислювальну потужність ЦП і максимально знижуючи енергоспоживання.

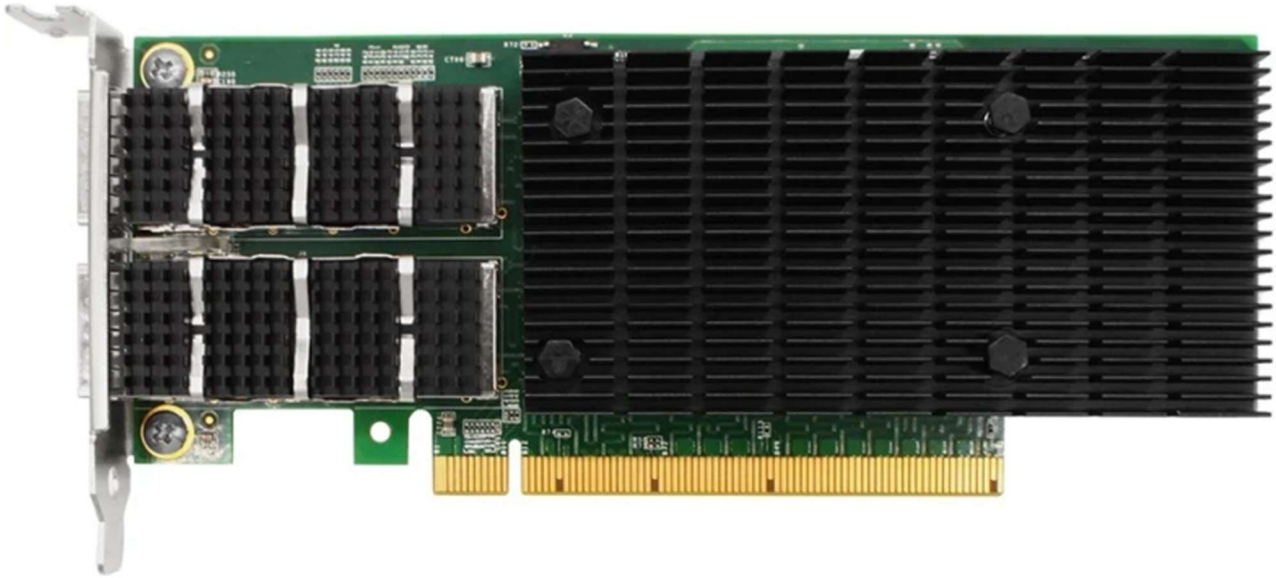


Рис.22 Мережава картка ISA

Класифікація за типами шинного інтерфейсу:

- Мережева карта ISA : архітектура промислового стандарту була випущена в 1981 році, яка є структурою шини, сумісною зі стандартами IBM. Через низьку швидкість вводу-виводу інтерфейсу шини ISA він був поступово виведений із появою технології шини PCI на початку 1990-х років і тепер рідко зустрічається на ринку.
- Мережева карта PCI : вона називається Peripheral Component Interconnect. Це стандарт локальної шини ПК, представлений у 1993 році. Оскільки його швидкість вводу-виводу набагато вища, ніж у мережевої карти шини ISA (найвища швидкість ISA становить лише 33 МБ/с, тоді як поточна швидкість передачі даних PCI 64-бітна). становить 266 МБ/с), він поступово замінив колишній стандарт ISA. Цей тип мережевої карти спочатку використовується на сервері, пізніше також широко використовується в настільному комп'ютері, є основним типом інтерфейсу мережевої карти. Більшість сучасних комп'ютерів не мають плат розширення, але використовують вбудовані мережеві карти. Тому мережеві карти PCI були замінені іншими інтерфейсами шини, такими як інтерфейси PCI-X або USB.
- Мережева карта PCI-X : PCI-X — це вдосконалена технологія шини PCI. У порівнянні з оригінальним PCI, швидкість вводу-виводу подвоєна, а швидкість передачі даних також вища, ніж інтерфейс PCI. Плата інтерфейсу шини PCI-X

зазвичай має 32-розрядну шину, але також підтримує 64-розрядну роботу зі швидкістю до 1064 МБ/с. У більшості випадків слоти PCI-X зворотно сумісні з PCI NIC.

- Мережева карта PCIe : карта PCIe — це мережева карта з портом PCIe, яка використовується як порт розширення для підключення материнської плати. Зокрема, карти розширення на основі PCI можна вставляти в слоти PCIe на системній платі пристроїв, таких як хости, сервери та мережеві комутатори. Більшість материнських плат комп’ютерів тепер мають спеціальні слоти PCIe для карт PCIe. Як правило, ширина слота буде такою ж, як ширина мережевої карти, або навіть ширше.

Розділ 2. Труднощі балансування навантаження в розподілених комп'ютерних мережах

2.1 Роль балансування мережевого навантаження в зменшенні затримки

Затримка визначається як час, потрібний пакету даних для проходження від джерела до місця призначення. Простіше кажучи, це затримка, яка виникає під час передачі даних через мережу.

Оскільки світ стає все більш взаємопов’язаним , а бізнес продовжує покладатися на цифрові технології, попит на швидкі та надійні мережі продовжує зростати.

Як затримка впливає на продуктивність мережі

Затримка може значно вплинути на продуктивність мережі, особливо для додатків у реальному часі, таких як онлайн-ігри, відеоконференції та хмарні служби. Висока затримка може призвести до повільного часу відповіді, затримки та тремтіння, що робить ці програми непридатними для використання.

Наприклад, в онлайн-іграх висока затримка може спричинити затримку дій гравця, що призведе до поганого досвіду гри. Подібним чином у відеоконференціях висока затримка може спричинити затримки передачі відео та аудіо, що призведе до поганого зв’язку.

У хмарних службах висока затримка може вплинути на швидкість і продуктивність програми. Наприклад, якщо користувач отримує доступ до хмарної програми з високою затримкою, завантаження даних або виконання операцій може зайняти більше часу.

Фактори, що впливають на затримку

Кілька факторів можуть впливати на затримку, зокрема швидкість з’єднання, пропускна здатність і перевантаження мережі:

- Швидкість з’єднання означає швидкість, з якою дані передаються через мережу. Вища швидкість з’єднання зазвичай призводить до меншої затримки;
- Пропускна здатність – це обсяг даних, який можна передати через мережу. Вища пропускна здатність зазвичай призводить до меншої затримки;
- Перевантаження мережі виникає, коли через мережу передається великий обсяг даних. Це може спричинити затримки та збільшити затримку.

Важливість швидкості з’єднання та пропускної здатності

Швидкість мережевого з’єднання та пропускна здатність є критичними факторами для визначення затримки. Вища швидкість з’єднання та вища пропускна здатність зазвичай призводять до меншої затримки. Наприклад, волоконно-оптичне з’єднання зазвичай має вищу пропускну здатність і вищу швидкість з’єднання, ніж інтернет-з’єднання DSL, що призводить до меншої затримки.

Крім того, відстань між вихідним і кінцевим пристроями також може впливати на затримку. Що стосується відстані, то чим далі відстань, тим більше часу потрібно для передачі даних, що призводить до вищої затримки.

Як виміряти мережеву затримку та продуктивність

Затримка вимірюється в мілісекундах (мс), і ви можете використовувати кілька інструментів діагностики для вимірювання продуктивності мережі та затримки, а також перевірити затримку, втрату пакетів і швидкість мережі.

Найбільш часто використовувані інструменти включають Ping, Traceroute і Speedtest:

- Тести Ping передбачають надсилання невеликого пакета даних від одного пристрою до іншого та вимірювання часу, необхідного для повернення пакета (тобто час зворотного зв’язку). Вони зазвичай використовуються для вимірювання часу затримки між двома пристроями в локальній мережі або між локальним пристроєм і інтернет-сервером;

- Інструмент traceroute передбачає надсилання пакета даних на віддалений пристрій і відстеження маршруту, яким він досягає IP-адреси призначення (одностороння затримка). Він надає інформацію про кожен стрибок на шляху, включаючи затримку кожного стрибка;
- Інструменти моніторингу продуктивності мережі (NPM) забезпечують комплексне уявлення про продуктивність мережі, включаючи використання пропускної здатності, затримку, втрату пакетів і продуктивність додатків. Вони можуть допомогти організаціям виявити та діагностувати проблеми продуктивності мережі в режимі реального часу;
- Інструменти тестування пропускної здатності вимірюють обсяг даних, які можна передати через мережу за певний проміжок часу. Їх можна використовувати для визначення обмежень пропускної здатності та планування модернізації мережі;
- Нарешті, інструменти моніторингу продуктивності додатків (APM) допомагають мережевому адміністратору контролювати продуктивність конкретних програм і служб, які працюють у мережі, допомагаючи організаціям виявляти та діагностувати проблеми, які впливають на продуктивність додатків.

Використовуючи ці інструменти та методи, організації можуть навчитися вимірювати затримку та продуктивність і визначати проблеми, які на них впливають. Маючи цю інформацію, вони можуть реалізувати ефективні стратегії для покращення продуктивності мережі та забезпечення оптимальної взаємодії з користувачем.

Інтерпретація результатів затримки

Інтерпретація результатів затримки є важливою частиною керування продуктивністю мережі. Результати затримки можуть надати уявлення про стан мережі та допомогти виявити проблеми, які впливають на продуктивність мережі.

Ось кілька вказівок щодо інтерпретації результатів затримки:

- Потрібно знати очікувану затримку . Різні типи мереж і програм мають різні очікувані діапазони затримок. Наприклад, додатки для онлайн-ігор вимагають низької затримки, як правило, менше 50 мс, тоді як програми для відеоконференцій

можуть допускати вищу затримку до 150 мс. Знання очікуваної затримки для конкретної програми чи мережі може допомогти вам точно інтерпретувати результати затримки програми;

- Подивитися на тенденцію з часом . Затримка може коливатися з часом через перевантаження мережі, зміни в топології мережі або інші фактори. Важливо дивитися на тенденцію результатів затримки з плином часу, щоб визначити закономірності чи аномалії;
- Порівняйте результати з базовою лінією . Встановлення базової лінії для затримки має вирішальне значення для визначення змін у продуктивності мережі. Порівняння поточних результатів затримки зі встановленою базовою лінією може допомогти вам визначити тенденції та визначити, збільшується чи зменшується затримка;
- Визначити потенційні причини . Результати затримки можуть вказувати на проблеми, пов’язані з пропускною здатністю, маршрутизацією, перевантаженням або іншими факторами. Виявлення потенційних причин проблем із затримкою може допомогти вам визначити правильний курс дій для покращення продуктивності мережі;
- Розглянемо вплив на досвід користувача . Затримка може вплинути на роботу мережевих програм і служб. Розуміння впливу затримки на взаємодію з користувачем може допомогти вам визначити пріоритетність проблем із затримкою та визначити належний рівень відповіді.

Результати затримки слід інтерпретувати в поєднанні з іншими показниками продуктивності, такими як втрата мережевих пакетів, швидкість мережі та використання пропускної здатності. Крім того, їх слід порівняти з галузевими еталонними показниками та найкращими практиками, щоб визначити, чи вони прийнятні.

Як покращити затримку мережі

Зменшення затримки є важливим для організацій, які залежать від

високопродуктивних мереж для підтримки своїх операцій. Низька продуктивність мережі може призвести до зниження продуктивності, зниження задоволеності користувачів і втрати прибутку.

На щастя, є кілька стратегій, які організації можуть використати для зменшення затримки.

Зрозуміти свої вимоги до мережі

Щоб ефективно керувати затримкою, важливо розуміти свої вимоги до мережі. Це передбачає визначення критичних програм і служб, які потребують низької затримки , наприклад відеоконференції, обробка даних у реальному часі та онлайн-ігри. Розуміючи свої вимоги до мережі, ви можете визначити пріоритетність трафіку та виділити достатню пропускну здатність для підтримки критичних програм.

Оптимізація конфігурації та інфраструктури мережі

Оптимізація всієї мережевої конфігурації передбачає налаштування мережевих пристроїв, таких як маршрутизатори та комутатори, для встановлення пріоритетів швидкості трафіку та зменшення затримки. Це може включати налаштування політики якості обслуговування (QoS) для визначення пріоритетності трафіку в реальному часі, наприклад відео- та голосового трафіку, і налаштування мережевих пристроїв для мінімізації втрати та затримки пакетів.

Крім того, оновлення карт мережі та інфраструктури може значно зменшити затримку та підвищити продуктивність мережі. Це може включати оновлення з DSL-з’єднання на волоконно-оптичний кабель, заміну застарілих мережевих пристроїв новими, швидшими пристроями або збільшення пропускної здатності для підтримки програм із високою пропускною здатністю.

Використовувати мережі доставки контенту (CDN)

CDN — це розподілені мережі серверів, які кешують і доставляють вміст ближче до кінцевого користувача, таким чином зменшуючи затримку та підвищуючи продуктивність. Це особливо корисно для організацій, у яких користувачі

знаходяться в різних частинах світу, оскільки це може зменшити відстань, яку дані повинні пройти, щоб досягти місця призначення.

Зменшити перевантаження мережі

Перевантаження мережі може спричинити затримки та збільшити затримку, особливо в періоди пікового використання. Організації можуть зменшити перевантаження мережі, запровадивши інструменти керування смугою пропускання, такі як формування трафіку та балансування навантаження, щоб більш рівномірно розподіляти мережевий трафік і запобігати вузьким місцям.

Балансування навантаження передбачає розподіл трафіку між декількома серверами для підвищення продуктивності та зменшення навантаження на окремі сервери.

Формування трафіку передбачає встановлення пріоритетів трафіку на основі вимог програми, наприклад надання вищого пріоритету трафіку в реальному часі, як-от голосовому та відеотрафіку, порівняно з іншими типами трафіку.

Відстежувати та вимірювати продуктивність мережі

Щоб ефективно керувати затримкою, слід регулярно контролювати та вимірювати продуктивність мережі за допомогою інструментів. Це дозволяє виявити проблеми із затримкою та відстежувати ефективність стратегій зменшення затримки.

Навчити персонал мережі

Ефективне керування затримкою вимагає командних зусиль. Мережевий персонал має пройти навчання щодо найкращих методів керування затримкою, моніторингу мережі та методів усунення несправностей. Це може допомогти переконатися, що вони володіють необхідними навичками для швидкого й ефективного виявлення та вирішення проблем затримки.

Проблеми в управлінні затримкою

Керування затримкою не позбавлене проблем. Незважаючи на прогрес у мережевих технологіях і доступність методів зменшення затримки, низка факторів все ще може впливати на затримку мережі.

Відстань

Відстань є значним фактором затримки мережі. Чим далі дані повинні подорожувати, тим більша затримка вводиться. Затримка може бути особливо проблематичною для програм, які потребують низької затримки, наприклад для обробки даних у реальному часі та онлайн-ігор. Щоб подолати цю проблему, вам, можливо, доведеться розглянути можливість розгортання периферійних обчислень, які можуть зменшити відстань, на яку передаються дані.

Обмеження пропускної здатності

Високе використання пропускної здатності може призвести до перевантаження та втрати пакетів, що може збільшити затримку. Організації можуть подолати цю проблему, запровадивши політику формування трафіку та якості обслуговування (QoS), щоб визначити пріоритет критичних програм і забезпечити їм необхідну пропускну здатність.

Складність мережі

Складність сучасних мереж може ускладнити виявлення та усунення проблем із затримкою. Оскільки бездротові мережі стають складнішими та перетворюються на більші мережі, виявлення основної причини затримки може стати складнішим, особливо коли проблеми із затримкою виникають періодично. Щоб подолати цю проблему, організації можуть запровадити інструменти моніторингу мережі та затримки, які можуть виявляти та діагностувати проблеми затримки в режимі реального часу.

Безпека

Методи зменшення затримки, такі як кешування вмісту, можуть викликати

проблеми з безпекою. Ось чому вкрай важливо збалансувати потребу у покращенні продуктивності та потребу в безпеці шляхом впровадження безпечних протоколів і моніторингу мережевого трафіку на наявність потенційних загроз безпеці. Оптимізація безпеки мережі може передбачати впровадження брандмауерів, систем виявлення вторгнень та інших заходів безпеки для захисту від потенційних загроз.

Вартість

Керування затримкою може бути дорогим, особливо для організацій, яким потрібен високий рівень продуктивності мережі. Розгортання високопродуктивного мережевого обладнання та впровадження методів зменшення затримки може бути дорогим, особливо для мереж малого та середнього бізнесу. Ми рекомендуємо ретельно оцінити співвідношення витрат і переваг методів зменшення затримки, щоб переконатися, що вони є економічно ефективними.

Масштабованість

У міру зростання організацій їхні вимоги до мережі можуть значно змінюватися. Забезпечити масштабованість стратегій керування затримкою може бути складно, особливо для організацій, які швидко розвиваються. Щоб подолати цю проблему, подумайте про розгортання масштабованої мережевої інфраструктури, яка може адаптуватися до мінливих вимог мережі.

2.2 Основні плюси та мінуси балансувальників наванатеження

Під час впровадження балансувальників навантаження у вашу комп’ютерну мережу важливо розуміти їхні плюси та мінуси. Тут перераховані різні переваги та недоліки балансувальників навантаження.

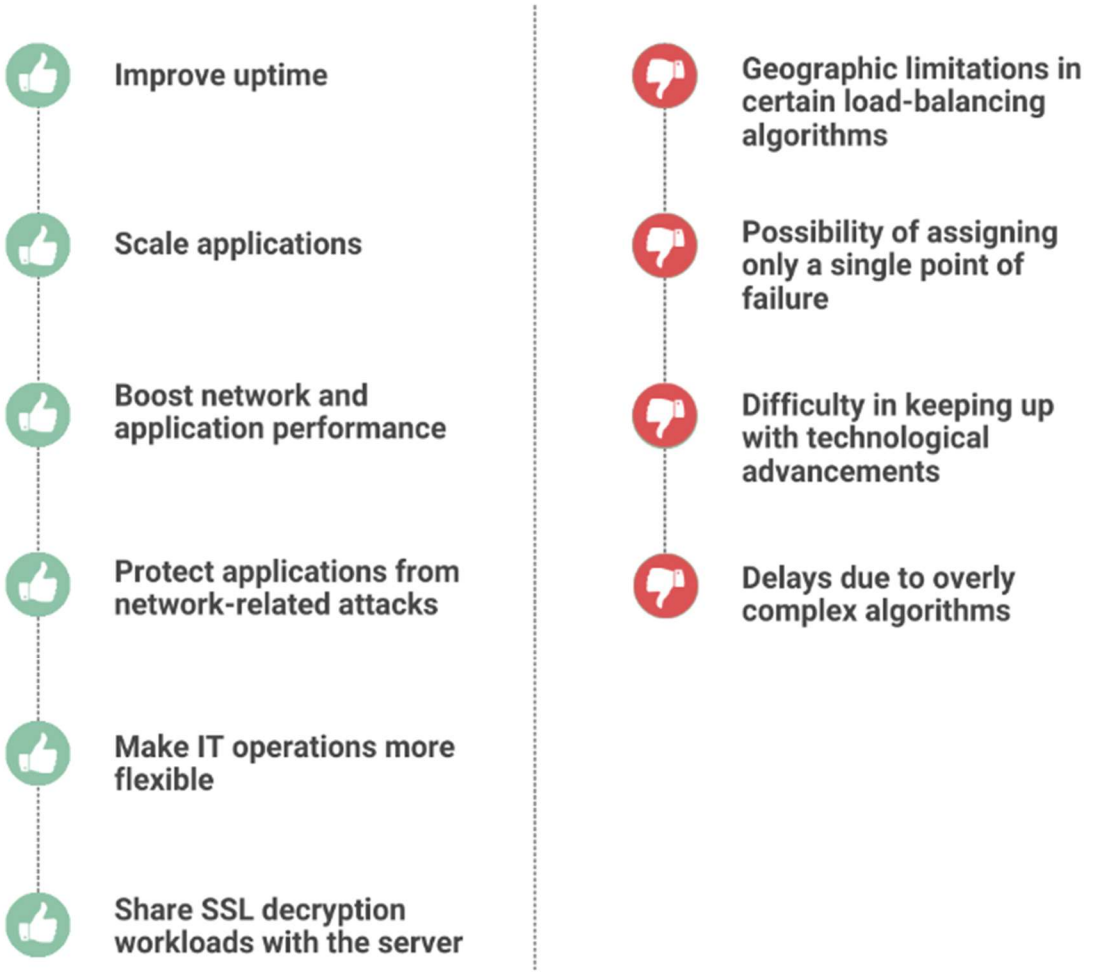


Рис.23 Схема переваг та недоліків балансування навантаження

Плюси балансувальників навантаження

Використовуючи пристрій або програмне забезпечення балансування навантаження, ми можемо: покращити час безвідмовної роботи.

Збій сервера або час простою обслуговування може призвести до серйознішого збою програми, що робить програму недоступною. Автоматично виявляючи проблеми з сервером і перенаправляючи клієнтський трафік на легкодоступні сервери, балансувальники навантаження покращують стійкість систем до збоїв.

Перенаправляючи трафік на альтернативний сервер, ремонт або оновлення сервера можна виконувати без збоїв. Це також корисно для аварійного відновлення, коли трафік можна завчасно скеровувати на резервні сайти.

Упевнено масштабувати програми

Балансувальники навантаження можуть розумно розподіляти мережевий трафік між кількома серверами. Балансування навантаження усуває перевантаження на окремих серверах, дозволяючи програмам безперешкодно обробляти сотні тисяч запитів клієнтів. Вони навіть можуть прогнозувати трафік за допомогою динамічних алгоритмів, дозволяючи додавати або видаляти сервери за потреби.

Підвищення продуктивності мережі та програм

Балансувальники навантаження підвищують ефективність додатків, зменшуючи затримку мережі та збільшуючи час відповіді. Вони пропорційно розподіляють робоче навантаження між серверами, щоб кожен сервер міг працювати з максимальною потужністю. Ви також можете налаштувати балансувальники навантаження, щоб перенаправляти клієнтські запити на географічно ближчий сервер, значно зменшуючи затримку програми.

Захист програм від мережевих атак

Сучасні балансувальники навантаження включають вбудовані протоколи безпеки мережі , пропонуючи додатковий рівень захисту для веб-додатків. Вони є корисним інструментом у боротьбі з розподіленими атаками на відмову в обслуговуванні (DDoS), коли зловмисники переповнюють додаток або систему незліченною кількістю одночасних запитів, що призводить до збою сервера. Навіть якщо ви не можете уникнути такої атаки, ви можете автономно перенаправити трафік зловмисника на різні внутрішні сервери, щоб пом’якшити її наслідки.

Балансувальники з належною конфігурацією спрямовуватимуть трафік через масив взаємопов’язаних брандмауерів для додаткової безпеки. Балансувальники навантаження можуть додатково контролювати трафік і миттєво блокувати шкідливий вміст.

Забезпечити кращий досвід користувача (UX)

Балансувальники навантаження можуть покращити UX, якщо компанія керує веб-сайтами з високим трафіком, програмами або наборами даних, які генерують багато запитів. Він оптимізує споживання ресурсів, передачу даних і час відповіді, щоб запропонувати кінцевим користувачам найкращий сервіс. У налаштуваннях із високим трафіком балансування навантаження забезпечує безперебійне й точне виконання запитів користувачів. Це гарантує, що користувачам не доведеться боротися з млявими або невідповідними програмами чи ресурсами.

Зробити IT-операції більш гнучкими

Використання кількох серверів із балансуванням навантаження дає IT-адміністраторам більшу гнучкість у управлінні трафіком веб-сайту. Наприклад, вони можуть виконувати технічне обслуговування сервера, не впливаючи на доступність сайту. Завдяки системі планового технічного обслуговування принаймні один сервер завжди буде доступний, щоб отримати навантаження, поки інші перебувають у стані простою на технічному обслуговуванні.

Робочі навантаження дешифрування SSL із сервером

Якщо ваш веб-сайт має сертифікат SSL, сервери беруть на себе додаткову відповідальність. Запити, а також будь-які пов’язані дані захищені шифруванням під час доставки на веб-сайт SSL. Сервери отримують цю зашифровану інформацію та мають завдання розшифрувати її перед тим, як почати її обробку. Це споживає дорогоцінний час, а також обчислювальну потужність.

Балансери навантаження мають вирішальне значення в такій ситуації. Вони декодують дані перед передачею на веб-сервер. Це дозволяє серверу повністю зосередитися на оцінці вхідних даних і передачі відповідних даних. Це зберігає обчислювальні ресурси хоста, які можна краще використовувати в іншому місці.

Мінуси балансувальників навантаження

Переваги балансувальників навантаження неймовірні. Без функції балансування навантаження у вашій мережі ви, ймовірно, станете свідком неефективного використання ресурсів і низької продуктивності програми. Тим не менш, важливо також звернути увагу на проблеми, з якими ви можете зіткнутися під час використання балансувальників навантаження.

Географічні обмеження в певних алгоритмах балансування навантаження

Деякі алгоритми балансування навантаження призначені для дуже малих областей. Переривання зв'язку, паузи мережі, простір між розподіленими об'єктами та роз'єднання між користувачем і запитуваними ресурсами не враховуються. Вузли у віддалених місцях становлять проблему, оскільки протоколи не призначені для роботи в таких середовищах.

Можливість призначення лише однієї точки відмови

Деякі протоколи балансування навантаження не можуть підтримувати розосереджені вузли, а натомість покладаються на централізований вузол для прийняття всіх рішень. У малоймовірному сценарії, коли центральний вузол виходить з ладу, кожна частина обчислювального середовища буде скомпрометована. Щоб подолати цю проблему, кілька вузлів у налаштуваннях балансування навантаження повинні бути налаштовані на обробку трафіку та прийняття рішень щодо маршрутизації.

Складно йти в ногу з технологічним прогресом

Доступність хмарних служб за запитом, Інтернет речей (IoT), мобільні програми з високою пропускною здатністю та блокчейн змінили очікування користувачів щодо онлайн-програм . Надійний балансир навантаження повинен відповідати мінливим вимогам споживачів, обчислювальній потужності, ємності накопичувача та функціям системи. Однак постійно оновлювати алгоритми

балансування навантаження може бути складно.

Затримки через надто складні алгоритми

Алгоритми для балансування навантаження часто є подвійним заголовком зі своїми плюсами та мінусами. Складність конкретних алгоритмів може вплинути на загальну ефективність системи. Це може призвести до незначних, але значних змін у часі міграції, допустимих дефектах і швидкості реагування. Незалежно від навантаження на сервер, алгоритми балансування навантаження повинні бути налаштовані для забезпечення найоптимальнішої продуктивності системи.

Розділ 3. Побудова та удосконалення мережі з використанням балансування навантаження у розподілених комп'ютерних мережах

3.1 Опис мережі з використання концентратора та Soho Router її недоліки.

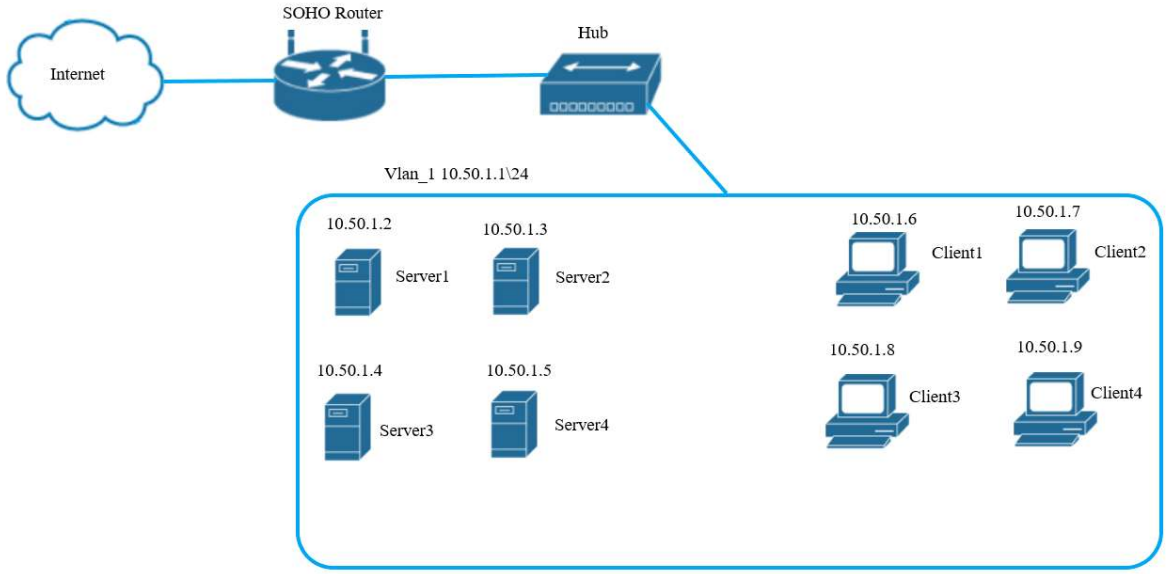


Рис. 24 Схема роботи мережі з використання концентратора та Soho Router її недоліки

Перелік обладнання та їхні задані параметри:

Мережа Internet – це наш провайдер з зовнішьою IP адресою яка дає змогу підключитися до глобальної мережі.

SOHO-роутер (Small Office/Home Office router) - це мережевий пристрій, призначений для використання в невеликих офісах або домашніх умовах. Його основна функція - забезпечення доступу до Інтернету та обміну даними між різними пристроями в локальній мережі. Вонизазвичай мають вбудований комутатор (switch) з декількома портами для підключення комп'ютерів, принтерів та інших пристроїв в мережі. Вони також часто включають в себе функції брандмауера (firewall) для захисту мережі від небезпечних зовнішніх впливів, а також можуть підтримувати бездротовий доступ (Wi-Fi).

SOHO-роутери легко налаштовуються та використовуються, і вони призначені для того, щоб забезпечити швидкий та надійний доступ до Інтернету для невеликих груп користувачів.Він має наступні налаштування:

Router IP Address:10.50.1.1
Subnet Mask: 255.255.255.0

Концентратор (хаб): Концентратор передає дані всім пристроям, які підключені до нього. Він не аналізує IP-адреси і не визначає шляхи маршрутизації.
Client (1-4) – це звичайні мережеві пристрої (комп'ютери, ноутбук, тощо). Вони мають наступні IP адреси:

Client1 – 10.50.1.2
Client2 - 10.50.1.3
Client3 - 10.50.1.4
Client4 - 10.50.1.5

Server (1-4) – це сервери які виконують різноманітні функції, такі як зберігання та управління даними, обробка веб-сторінок, обслуговування електронної пошти, управління доменами та інші задачі, спрямовані на забезпеченнянадійної роботи мережі та доступу до інформаційних ресурсів. Вони мають наступні IP адреси:

Server1 – 10.50.1.6
Server2 - 10.50.1.7
Server3 -10.50.1.8
Server4 -10.50.1.9

Недоліки мережі з використанням SOHO Router та Hub:

Хоча SOHO-роутери можуть бути досить ефективними для багатьох домашніх та малих офісних мереж, вони мають деякі обмеження, особливо щодо балансування навантаження:

- Обмежена потужність обробки:

SOHO-роутери часто мають обмежену обробку даних, що може призводити до обмежень у їхній здатності ефективно обробляти великі обсяги трафіку або виконувати балансування навантаження в разі значної кількості користувачів або пристроїв.

- Відсутність розширених функцій:

SOHO-роутери часто не мають таких розширених функцій балансування навантаження, які можуть бути доступні в більш продуктивних та дорогих маршрутизаторах. Це може обмежити їхню здатність ефективно розподіляти трафік.

- Обмежені можливості керування мережею:

SOHO-роутери зазвичай не надають такі розширені можливості керування мережею, які можуть бути необхідні для складних сценаріїв балансування навантаження.

- Відсутність резервних механізмів:

SOHO-роутери можуть не мати вбудованих механізмів резервування та відновлення в разі відмови. Це може призвести до втрати доступу до Інтернету, якщо роутер вийде з ладу.

- Низька масштабованість:

Зростання обсягу трафіку або кількості підключених пристроїв може призвести до перевантаження SOHO-роутера, що вплине на його продуктивність та здатність ефективно балансувати навантаження.

- Колізії даних:

Хаби працюють на фізичному рівні мережі і не мають здатності розділяти мережевий трафік між портами. Це може призводити до колізій даних, особливо в ситуаціях великої активності на мережі.

- Низька пропускна здатність:

Хаби розділяють доступ до мережі між всіма підключеними пристроями, що призводить до низької пропускної здатності. У порівнянні з більш сучасними комутаторами, які можуть розділяти трафік і вдосконалювати пропускну здатність, хаби недоцільні для використання в сучасних мережах.

- Відсутність інтелектуального керування:

Хаби не мають інтелектуального керування трафіком, що робить неможливим ефективне балансування навантаження. Кожен пакет даних, який надсилається через хаб, ретранслюється на всі порти, незалежно від його призначення.

- Брак безпеки:

Хаби не надають жодного рівня безпеки на мережевому рівні. У зв'язку з цим вони менше придатні для захисту від небажаного доступу та інших мережевих загроз.

- Обмежена гнучкість:

Хаби не здатні адаптуватися до змін в мережі та надмірно витрачають ресурси, ретранслюючи дані всім пристроям в мережі, навіть якщо це не є необхідним.

3.2 Модернізація мережі з використанням комутатора та міжмережевого екрану, розділення на окремі VLAN

В модернізації мережі буде використовуватись алгоритм - Source MAC Hashing.

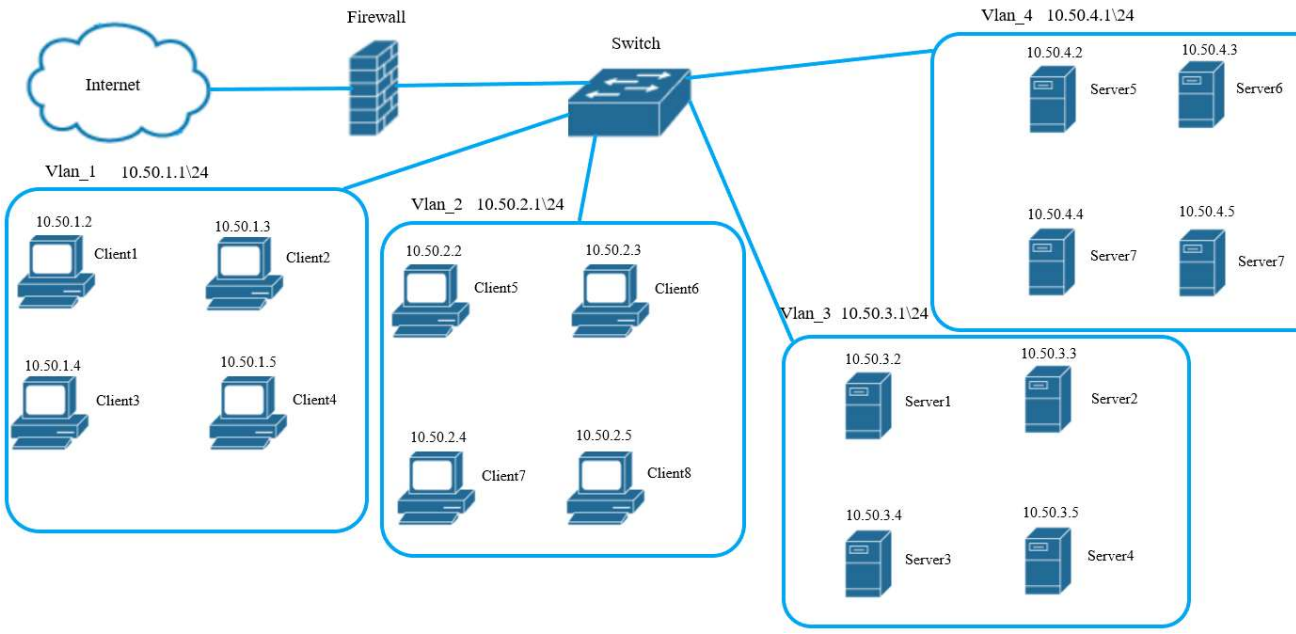


Рис. 25 Схема роботи мережі з використанням міжмережевого екрану та

керовонаго комутатора

Перелік обладнання та їхні задані параметри:

- Firewall – він виконує функції не лише захисту мережі від несанкціонованого доступу, але і керуванням трафіком та направленням даних між різними мережевими сегментами.
- Керований комутатор (Managed Switch) - надає можливості адміністрування та конфігурування через інтерфейс керування. У відміну від некерованих комутаторів, які працюють автономно без можливостей вдалого конфігурування, керовані комутатори дозволяють адміністраторам мережі налаштовувати різноманітні параметри для оптимізації роботи мережі та забезпечення безпеки.

Мережі та пристрої з наступними параметрами:

Vlan_1 10.50.1.1\24 (Vlan_1 назва нашої мережі, 10.50.1.1\24 – шлюз, 24 - маска підмережі)

Client1 – 10.50.1.2

Client2 – 10.50.1.3

Client3 – 10.50.1.4

Client4 – 10.50.1.5

Vlan_2 10.50.2.1\24 (Vlan_2 назва нашої мережі, 10.50.2.1\24 – шлюз, 24 - маска підмережі)

Client6 – 10.50.2.2

Client7 – 10.50.2.3

Client8 – 10.50.2.4

Client9 – 10.50.2.5

Vlan_3 10.50.3.1\24 (Vlan_3 - назва нашої мережі, 10.50.3.1\24 – шлюз, 24 - маска

підмережі)

Server1 – 10.50.3.2

Server2 – 10.50.3.3

Server3 – 10.50.3.4

Server4 – 10.50.3.5

Vlan_4 10.50.4.1\24 (Vlan_4 - назва нашої мережі, 10.50.4.1\24 – шлюз, 24 - маска підмережі)

Server5 – 10.50.4.2

Server6 – 10.50.4.3

Server7 – 10.50.4.4

Server8 – 10.50.4.5

Опис процесу удосконалення мережі за допомогою VLAN Trunking на Firewall.

В першу чергу потрібно налаштувани VLAN Trunking на Firewall для оптимізації використання мережевих ресурсів та розподілу трафіку між різними частинами мережі для підвищення ефективності та доступності.

VLAN Trunking - це техніка використання VLAN для передачі трафіку між різними мережевими пристроями, такими як комутатори чи маршрутизатори. Коли вам потрібно передавати трафік для кількох VLAN через одне фізичне з'єднання, ви використовуєте VLAN trunk.

Основні характеристики VLAN Trunking:

- Тегування пакетів:

У системах VLAN Trunking, кожен пакет має додатковий тег, який вказує, до якого VLAN він належить. Це тегування дозволяє обладнанню розрізняти трафік різних VLAN і правильно направляти його відповідно.

- Стандарти тегування:

Для тегування пакетів зазвичай використовують стандарти IEEE 802.1Q або ISL

(Inter-Switch Link). Протокол IEEE 802.1Q широко поширений і є стандартом для більшості сучасних мережевих обладнань.

- Транкінгові порти:

Порти на комутаторах чи маршрутизаторах, які налаштовані для підтримки VLAN trunking, називаються транкінговими портами. Ці порти можуть передавати трафік для різних VLAN і взаємодіяти з іншими транкінговими портами на інших пристроях.

Процедура навантаження тегування:

У системах 802.1Q, тег вставляється у заголовок Ethernet-фрейму і містить інформацію про VLAN ID, контрольні біти, та іншу необхідну інформацію. Це дозволяє обладнанню відрізняти різні VLAN і ефективно передавати трафік.

Ідентифікація натяків на протоколи:

VLAN Trunking також дозволяє передавати різні типи трафіку (наприклад, голосовий, даних, керівництва) для різних VLAN, що полегшує обробку та управління мережевим трафіком.

Загальний приклад налаштування мереж на Firawall

```
interface GigabitEthernet0/0
ip address 10.50.1.1 255.255.255.0
no shutdown
exit

interface GigabitEthernet0/1
ip address 10.50.2.1 255.255.255.0
no shutdown
exit

interface GigabitEthernet0/2
ip address 10.50.3.1 255.255.255.0
no shutdown
exit

interface GigabitEthernet0/3
ip address 10.50.4.1 255.255.255.0
no shutdown
exit
```

Рис. 26 Створення мережі на Firewall

```
arp type inet 10.50.1.2 0000.0c12.3456 ARPA  # Client1
arp type inet 10.50.1.3 0000.0c12.3457 ARPA  # Client2
arp type inet 10.50.1.4 0000.0c12.3458 ARPA  # Client3
arp type inet 10.50.1.5 0000.0c12.3459 ARPA  # Client4

arp type inet 10.50.2.2 0000.0c12.3460 ARPA  # Client1
arp type inet 10.50.2.3 0000.0c12.3461 ARPA  # Client2
arp type inet 10.50.2.4 0000.0c12.3462 ARPA  # Client3
arp type inet 10.50.2.5 0000.0c12.3463 ARPA  # Client4

arp type inet 10.50.3.2 0000.0c12.3464 ARPA  # Server1
arp type inet 10.50.3.3 0000.0c12.3465 ARPA  # Server2
arp type inet 10.50.3.4 0000.0c12.3466 ARPA  # Server3
arp type inet 10.50.3.5 0000.0c12.3467 ARPA  # Server4

arp type inet 10.50.4.2 0000.0c12.3468 ARPA  # Server1
arp type inet 10.50.4.3 0000.0c12.3469 ARPA  # Server2
arp type inet 10.50.4.4 0000.0c12.3470 ARPA  # Server3
arp type inet 10.50.4.5 0000.0c12.3471 ARPA  # Server4
```

Рис. 27 Призначення IP-адрес на Firewall

Наступним кроком потрібно налаштувати на комутаторі окремі VLAN для мережевих пристроїв.

Налаштування окремих VLAN на керованому комутаторі має кілька важливих переваг і застосувань у мережевому середовищі:

- Ізоляція трафіку:

Безпека: Використання VLAN дозволяє фізично і логічно ізолювати трафік між різними групами користувачів чи пристроями. Це може бути корисним для запобігання несанкціонованого доступу та захисту конфіденційної інформації.

Менше бродкаст-трафіку: Розділення мережі на VLAN допомагає обмежити розповсюдження бродкаст-трафіку, що може виникнути в одній VLAN, не впливаючи на інші.

- Оптимізація пропускної здатності:

Балансування навантаження: Розподіліть користувачів та пристрої між різними VLAN для ефективного використання пропускної здатності мережі та покращення продуктивності.

Керування трафіком: Можливість визначити пріоритети та обмеження ширини смуги для кожного VLAN, що сприяє кращому керуванню трафіком.

- Флексібільність конфігурації:

Віртуалізація мережі: VLAN дозволяють створювати віртуальні локальні мережі, незалежно від фізичної топології. Це особливо корисно в складних мережах або в середовищах, де змінюється розташування пристроїв.

Робота з різними службами: Окремі VLAN можуть використовуватися для різних служб, таких як голосова та даних, що дозволяє оптимізувати роботу різних типів трафіку.

- Керування багатокористувацькою мережею:

Керування багатокористувацькою мережею: В середовищах, де існують різні групи користувачів (наприклад, велика корпоративна мережа), VLAN дозволяють вам легко керувати доступом та ресурсами для кожної групи.

Загальне налаштування VLAN на комутаторі.

```
Switch> enable
Switch# configure terminal

Switch(config)# vlan 1
Switch(config-vlan)# name Vlan_1

Switch(config)# vlan 2
Switch(config-vlan)# name Vlan_2

Switch(config)# vlan 3
Switch(config-vlan)# name Vlan_3

Switch(config)# vlan 4
Switch(config-vlan)# name Vlan_4

Switch(config)# interface GigabitEthernet0/0
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1

Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2

Switch(config)# interface GigabitEthernet0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 3

Switch(config)# interface GigabitEthernet0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 4

Switch(config-if)# exit
Switch(config)# write memory
Switch(config)# exit
```

Рис. 28 Налаштування VLAN на комутаторі

За підсумком, видно що: було встановлено нове та сучасне обалдання для балансування наванатаження в розподілених комп’ютерних мережах, а саме:

Використали метод балансування навантаження VLAN Trunking для передачі даних різних VLAN через один фізичний з'єднаний інтерфейс (такий як Ethernet-з'єднання). Це дозволяє оптимізувати використання доступних ресурсів та розподіляти трафік різних VLAN.

Використали метод балансування навантаження по алгоритму - Source MAC Hashing за допомогою керованого комутатора, він може використовуватися для розподілу трафіку між різними портами чи шляхами (наприклад, у мережах Ethernet)

на основі даних (Source MAC address) кожного пакета. Цей метод сприяє рівномірному використанню доступних ресурсів та підвищенню ефективності мережі.

Висновок

У ході цього дослідження ми ретельно вивчили проблематику балансування навантаження в розподілених комп'ютерних мережах та дослідили можливості використання міжмереживих екранів та комутаторів для оптимізації цього процесу. Отримані результати та висновки вказують на важливість використання цих пристроїв у практиці для досягнення оптимальної продуктивності та стійкості в розподілених середовищах.

Однією з ключових переваг використання міжмереживих екранів є їхня здатність до ефективного розподілу мережевого трафіку між вузлами системи. Це дозволяє уникнути перевантажень та забезпечити рівномірне розподілення завдань, що в свою чергу підвищує ефективність використання обчислювальних ресурсів.

Дослідження також підтвердило, що використання комутаторів в розподілених мережах дозволяє оптимізувати шляхи передачі даних та зменшує час відповіді системи. Інтелігентне управління мережевим трафіком та ресурсами стає ключовим елементом для забезпечення високої швидкодії та продуктивності.

Однак важливо відзначити, що ефективність міжмереживих екранів та комутаторів значно залежить від ретельно розроблених алгоритмів балансування навантаження. Оптимальний вибір стратегій та їх узгодженість з характером роботи системи може суттєво підняти ефективність балансування.

У висновку, можна стверджувати, що використання міжмереживих екранів та комутаторів є перспективним напрямком для оптимізації балансування навантаження в розподілених комп'ютерних мережах. Дані пристрої відкривають шлях до створення більш продуктивних, стійких та високофункціональних розподілених систем, що відповідають вимогам сучасних інформаційних технологій.

ПЕРЕЛІК ПОСИЛАНЬ

1. Балансування навантаження в комп'ютерних мережах [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Load_balancing_(computing)
2. Комп'ютерні мережі [Електронний ресурс] – Режим доступу до ресурсу: https://km.ptngu.com/lections/7.html
3. Міжмережеві екрани [Електронний ресурс] – Режим доступу до ресурсу: https://mail.google.com/mail/u/0/?pli=1#inbox?projector=1
4. Комутатор [Електронний ресурс] – Режим доступу до ресурсу: https://www.techtarget.com/searchnetworking/definition/switch
5. Мережеві адаптери [Електронний ресурс] – Режим доступу до ресурсу: https://www.techopedia.com/definition/8546/network-adapter
6. Алгоритми балансування навантаження [Електронний ресурс] – Режим доступу до ресурсу: https://www.enjoyalgorithms.com/blog/types-of-load-balancing-algorithms
7. Розгортання мережі за допомогою міжмережевого екрану [Електронний ресурс] – Режим доступу до ресурсу: https://www.lumen.com/help/en-us/edge-private-cloud/creating-a-firewall-rule-to-allow-internet-access-for-networks.html
8. Розгортання VLAN за допомогою мережевого комутатора [Електронний ресурс] – Режим доступу до ресурсу: https://petri.com/csc_setup_a_vlan_on_a_cisco_switch/
9. Характерисики роботи VLAN Trunking [Електронний ресурс] – Режим доступу до ресурсу:https://www.networkacademy.io/ccna/ethernet/vlan-trunking
10. Принципи роботи алгоритму [Електронний ресурс] – Режим доступу до ресурсу: https://documentation.extremenetworks.com/slxos/sw/20xx/20.4.1/l2config/GUID-68B60232-D88B-4B59-AF04-A0D2283B95F6.shtml

ПРЕЗЕНТАЦІЯ

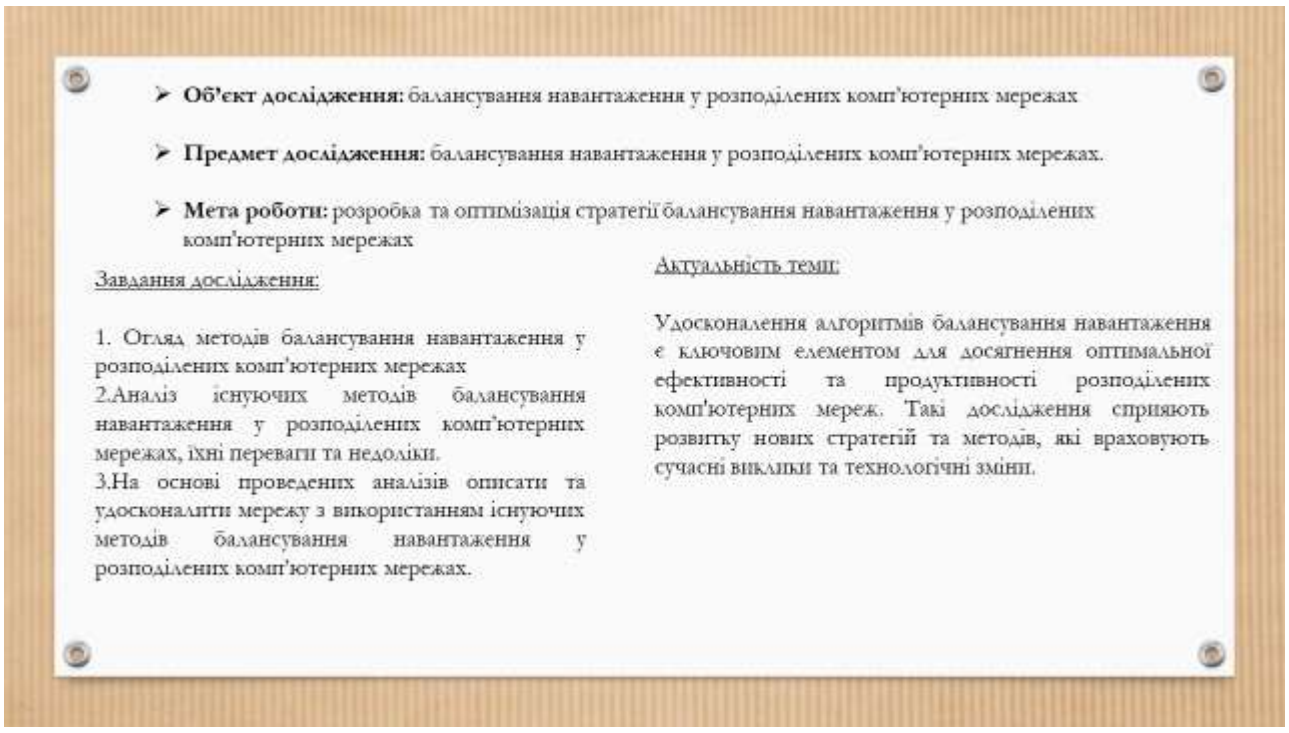
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

Презентація до дипломної роботи на тему:

«Удосконалення та оптимізація алгоритмів балансування навантаження у розподілених комп'ютерних мережах»

Виконав: Божко М.В.
Науковий керівник: Лащевська Н.О.



- **Об'єкт дослідження:** балансування навантаження у розподілених комп'ютерних мережах
- **Предмет дослідження:** балансування навантаження у розподілених комп'ютерних мережах.
- **Мета роботи:** розробка та оптимізація стратегії балансування навантаження у розподілених комп'ютерних мережах

Завдання дослідження:

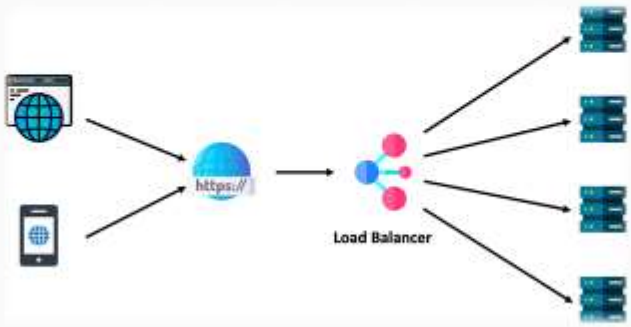
1. Огляд методів балансування навантаження у розподілених комп'ютерних мережах
2. Аналіз існуючих методів балансування навантаження у розподілених комп'ютерних мережах, їхні переваги та недоліки.
3. На основі проведених аналізів описати та удосконалити мережу з використанням існуючих методів балансування навантаження у розподілених комп'ютерних мережах.

Актуальність теми:

Удосконалення алгоритмів балансування навантаження є ключовим елементом для досягнення оптимальної ефективності та продуктивності розподілених комп'ютерних мереж. Такі дослідження сприяють розвитку нових стратегій та методів, які враховують сучасні виклики та технологічні зміни.

Поняття балансування навантаження у розподілених комп'ютерних мережах

Балансування навантаження у розподілених комп'ютерних мережах — це процес розподілу робочих завдань, обчислювального або мережевого навантаження між різними вузлами або комп'ютерами в мережі з метою оптимізації використання ресурсів та підвищення продуктивності системи. Основна ідея полягає в тому, щоб рівномірно розподілити завдання серед різних вузлів так, щоб уникнути перевантаження деяких ресурсів та забезпечити ефективне використання доступних потужностей.



Основні аспекти балансування

Динамічний розподіл завдань: Система балансування повинна бути здатна враховувати зміни в обсязі робочого навантаження і динамічно перерозподілювати завдання для оптимізації використання ресурсів.

Моніторинг ресурсів: Ефективне балансування передбачає систему моніторингу, яка слідкує за станом ресурсів, таких як потужність процесора, обсяг пам'яті, пропускна здатність мережі тощо.

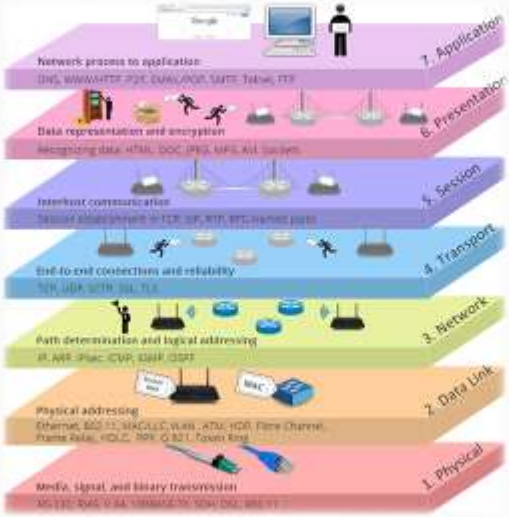
Методи прийняття рішень: Балансування може базуватися на різних методах прийняття рішень, таких як найменший обсяг навантаження, пропускна спроможність, вартість, та інші критерії, залежно від конкретних вимог та характеристик системи.

Гнучкість та адаптивність: Балансування повинно бути гнучким, здатним адаптуватися до змін в обсязі роботи, конфігурації мережі або стану вузлів.

Мінімізація затримок: При балансуванні навантаження важливо уникати затримок у виконанні завдань шляхом ефективного розподілу ресурсів.

Стійкість до відмов: Балансування має бути стійким до відмов, тобто здатним враховувати та компенсувати непередбачувані ситуації, такі як виходження з ладу певних вузлів.

Рівні балансування



Розглянемо певні рівні докладніше, а саме:

Мережевий рівень (англ. Network Layer) – здійснює зв'язок між вузлами (абонентами), тобто надсилає пакети даних до адресата, встановлює мережу. Мережевий рівень відповідає за адресацію і маршрутизацію (управління потоками даних). Ним здійснюється також обробка помилок і мультиплексування. На цьому рівні працюють маршрутизатори і функціонують протоколи IP, ICMP, IGMP, ARP, OSPF.

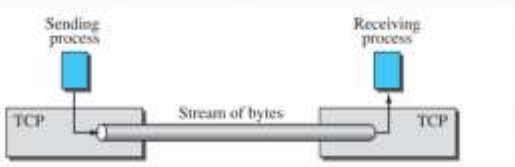
Транспортний рівень (англ. Transport Layer) – забезпечує передачу даних між програмними компонентами (сервісами, додатками, сеансами, процесами), здійснює управління рухом цих пакетів. Підтримує сегментацію та мультиплексування. Протоколи транспортного рівня: TCP/UDP, SST, FCP, SPX, SCTP, RUDP, NBF, IL, DCCP, CUDP, ATP.

Прикладний рівень (англ. Application Layer) – самий верхній, сьомий рівень OSI-моделі. Забезпечує взаємодію мережі і користувача. Рівень дозволяє програмам отримувати доступ до мережевих служб, здійснювати запити до баз даних, мати доступ до файлів, пересилати електронну пошту. На цьому рівні працюють веб-сайти, програми, застосунки, різні додатки. Протоколи рівня: HTTP, SSH, FTP, Telnet, DNS, IMAP/POP/SMTP та ін.

Мережевий

Прикладний

Транспортний



Алгоритми балансування навантаження

- Round Robin
- Least Loaded
- Content-Based Routing
- Least Connection
- Source MAC Hashing
- Adaptive Load Balancing
- Weighted Round Robin
- Proportional Share Scheduling

Round Robin: Це простий алгоритм, при якому завдання розподіляються між вузлами в порядку черговості. Кожен вузол обробляє завдання, поки він не стане знову на черзі.

Least Connection: Цей метод призначає завдання вузлу з найменшою кількістю активних з'єднань.

Weighted Round Robin: Такий алгоритм подібний до звичайного Round Robin, але кожному вузлу призначається вага в залежності від його потужності або характеристик, і завдання розподіляються відповідно до цих ваг.

Least Loaded: Завдання призначаються вузлам з найменшим навантаженням. Цей підхід може враховувати різні метрики, такі як завантаження процесора, обсяг вільної пам'яті тощо.

Adaptive Load Balancing: Цей метод використовує алгоритми машинного навчання для передбачення навантаження та адаптації до змін у робочих умовах.

Content-Based Routing: Завдання розподіляються відповідно до вмісту чи характеристик завдань. Наприклад, завдання із схожим типом обробляються вузлами, які спеціалізуються на цьому типі завдань.

Proportional Share Scheduling: Використовує пропорції або квоти для розподілу ресурсів між вузлами відповідно до їхніх можливостей та ваг.

Source MAC Hashing: використовується в мережевих пристроях, таких як комутатори або маршрутизатори, для розподілу трафіку між різними шляхами або портами.

Приклади пристроїв балансування навантаження

- Серверні кластери
- Проксі-сервери
- Міжмережні екрани
- Комутатори
- Сервери інспектування вмісту
- Мережеві адаптери
- Сервери DNS

Роль балансування мережевого навантаження в зменшенні затримки

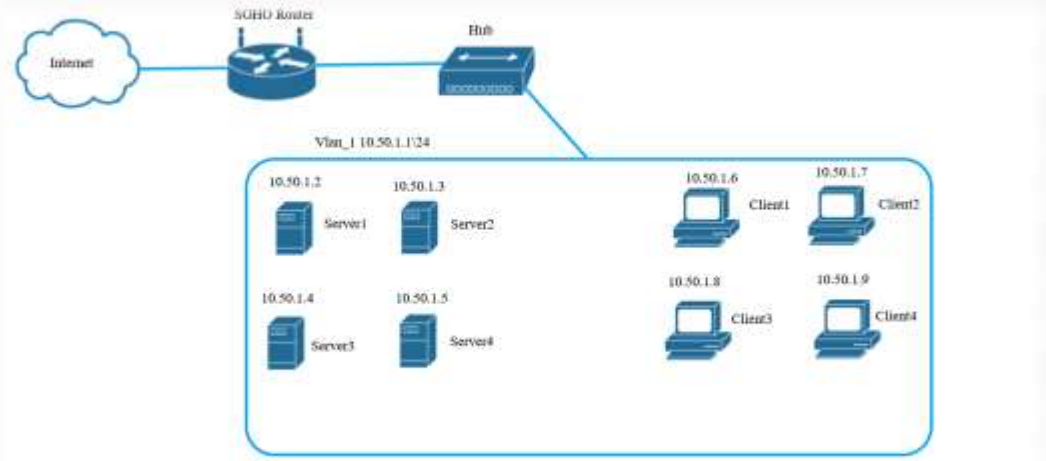
Затримка визначається як час, потрібний пакету даних для проходження від джерела до місця призначення. Простіше кажучи, це затримка, яка виникає під час передачі даних через мережу.
Оскільки світ стає все більш взаємопов'язаним , а бізнес продовжує покладатися на цифрові технології, попит на швидкі та надійні мережі продовжує зростати.

Затримка може значно вплинути на продуктивність мережі, особливо для додатків у реальному часі, таких як онлайн-ігри, відеоконференції та хмарні служби. Висока затримка може призвести до повільного часу відповіді, затримки та тремтіння, що робить ці програми непридатними для використання.
Кілька факторів можуть впливати на затримку, зокрема швидкість з'єднання, пропускна здатність і перевантаження мережі:

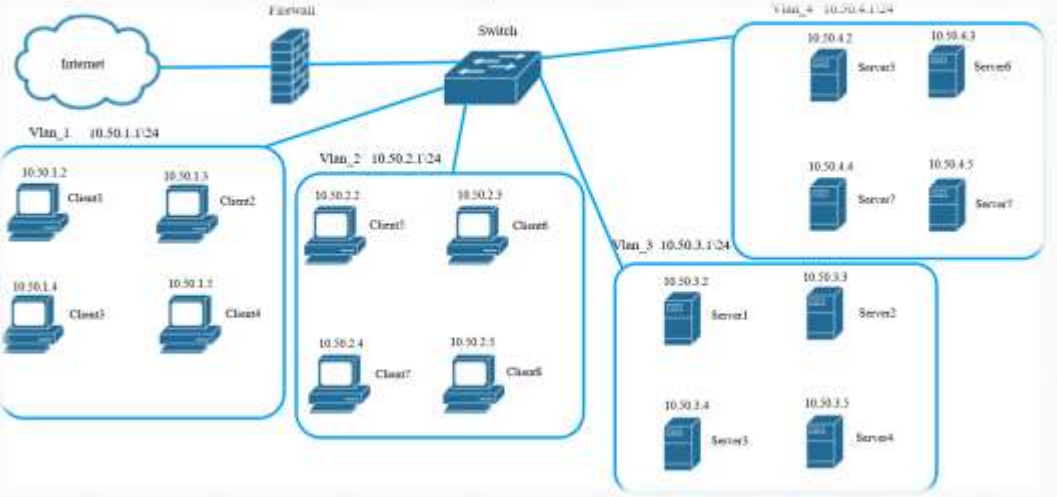
- Швидкість з'єднання означає швидкість, з якою дані передаються через мережу. Вища швидкість з'єднання зазвичай призводить до меншої затримки;
- Пропускна здатність – це обсяг даних, який можна передати через мережу. Вища пропускна здатність зазвичай призводить до меншої затримки;
- Перевантаження мережі виникає, коли через мережу передається великий обсяг даних. Це може спричинити затримки та збільшити затримку.

Плюси балансування навантаження в розподілених комп'ютерних мережах

Схема мережі з використання Hub та Soho Router для балансування навантаження



Модернізація мережі з використанням комутатора та міжмережевого екрану, розділення на окремі VLAN



Дякую за Увагу!

Висновок

У ході цього дослідження ми ретельно вивчили проблематику балансування навантаження в розподілених комп'ютерних мережах та дослідили можливості використання міжмережевих екранів та комутаторів для оптимізації цього процесу. Отримані результати та висновки вказують на важливість використання цих пристроїв у практиці для досягнення оптимальної продуктивності та стійкості в розподілених середовищах.

Однією з ключових переваг використання міжмережевих екранів є їхня здатність до ефективного розподілу мережевого трафіку між вузлами системи. Це дозволяє уникнути перевантажень та забезпечити рівномірне розподілення завдань, що в свою чергу підвищує ефективність використання обчислювальних ресурсів.

Дослідження також підтвердило, що використання комутаторів в розподілених мережах дозволяє оптимізувати шляхи передачі даних та зменшує час відповіді системи. Інтелігентне управління мережевим трафіком та ресурсами стає ключовим елементом для забезпечення високої швидкодії та продуктивності.

Однак важливо відзначити, що ефективність міжмережевих екранів та комутаторів значно залежить від ретельно розроблених алгоритмів балансування навантаження. Оптимальний вибір стратегій та їх узгодженість з характером роботи системи може суттєво підняти ефективність балансування.

У висновку, можна стверджувати, що використання міжмережевих екранів та комутаторів є перспективним напрямком для оптимізації балансування навантаження в розподілених комп'ютерних мережах. Дані пристрої відкривають шлях до створення більш продуктивних, стійких та високофункціональних розподілених систем, що відповідають вимогам сучасних інформаційних технологій.