

Принципи роботи комп'ютерних мереж

Шевченко Максим, студент ¹ (ORCID: 0009-0004-2000-0777)

¹ Київський національний університет будівництва і архітектури, 03037, м. Київ, проспект Повітряних Сил, 31, Україна

АНОТАЦІЯ

Ця робота присвячена вивченню основних принципів роботи комп'ютерних мереж, які є фундаментом сучасних інформаційних технологій. У роботі розглянуто моделі OSI та TCP/IP, класифікацію мереж за територіальним охопленням, основні протоколи передачі даних, принципи маршрутизації та адресації, а також питання безпеки в комп'ютерних мережах. Розуміння цих аспектів є важливим для ефективного використання та розвитку комп'ютерних систем.

Ключові слова: комп'ютерні мережі, модель OSI, TCP/IP, LAN, WAN, протоколи, маршрутизація, IP-адресація, безпека мереж.

1. ВСТУП

Комп'ютерні мережі відіграють ключову роль у сучасному суспільстві, забезпечуючи комунікацію між різними пристроями та дозволяючи обмінюватися даними по всьому світу. З моменту створення першої мережі ARPANET в 1969 році комп'ютерні мережі стали основою для розвитку глобальних інформаційних систем, що включають в себе Інтернет, корпоративні мережі та локальні мережі. Завдяки комп'ютерним мережам стало можливим миттєве передавання інформації на великі відстані, що значно підвищило ефективність бізнесу, науки та освіти. Знання принципів роботи комп'ютерних мереж є важливим для розуміння того, як функціонують інтернет, локальні мережі та різні сервіси, які ми використовуємо щодня.

2. МЕТА РОБОТИ

Ознайомлення з основними принципами та концепціями роботи комп'ютерних мереж, що дозволить поглибити свої знання в цій галузі та розвинути навички, необхідні для подальшого навчання і професійного зростання в сфері комп'ютерної інженерії.

3. МОДЕЛЬ OSI ТА TCP/IP

Мережеві протоколи організовані у вигляді моделей, серед яких найпоширенішими є модель OSI (Open Systems Interconnection) та модель TCP/IP. Модель OSI складається з семи рівнів: фізичний, каналний, мережевий, транспортний, сеансовий, представницький і прикладний. Кожен рівень відповідає за певну функціональність, що дозволяє даним переміщуватися від одного комп'ютера до іншого через мережу.

Фізичний рівень відповідає за передачу сирих даних через фізичні носії, такі як кабелі або оптоволокно. Канальний рівень забезпечує надійність передачі даних між двома вузлами мережі, включаючи контроль помилок і управління доступом до середовища передачі. Мережевий рівень займається маршрутизацією даних, визначаючи оптимальні маршрути між джерелом і одержувачем.

Транспортний рівень відповідає за забезпечення надійної передачі даних між кінцевими точками зв'язку, контролюючи поділ даних на сегменти та їх пересилання.

Сеансовий рівень підтримує і управляє діалогом (сеансом) між двома вузлами, дозволяючи їм встановлювати, підтримувати і закривати зв'язок. Представницький рівень відповідає за перетворення даних у формат, зрозумілий для прикладного рівня, і може включати в себе шифрування або стиснення даних. Нарешті, прикладний рівень надає мережеві сервіси безпосередньо користувачам, такі як електронна пошта, передача файлів та веб-доступ.

Модель TCP/IP є спрощеною версією OSI і використовується у більшості сучасних мереж, зокрема в інтернеті. Вона включає в себе чотири рівні: мережевий доступ, інтернет, транспортний і прикладний. TCP/IP забезпечує надійність передачі даних і їх адресацію в глобальній мережі Інтернет.

4. ТИПИ КОМП'ЮТЕРНИХ МЕРЕЖ

Комп'ютерні мережі класифікуються за різними критеріями, зокрема за територіальним охопленням:

LAN (Local Area Network) — локальна мережа, яка об'єднує комп'ютери в межах невеликої географічної зони, наприклад, в одному офісі або будівлі. LAN зазвичай забезпечують високу швидкість передачі даних і використовуються для з'єднання персональних комп'ютерів, серверів, принтерів та інших пристроїв.

WAN (Wide Area Network) — глобальна мережа, яка охоплює великі географічні райони, наприклад, мережі, що з'єднують офіси в різних містах або країнах. WAN зазвичай використовують для об'єднання кількох локальних мереж та забезпечення зв'язку між ними через інтернет або інші глобальні мережі.

MAN (Metropolitan Area Network) — мережа, яка охоплює місто або великий регіон. MAN є проміжним рівнем між LAN та WAN і зазвичай використовується для забезпечення зв'язку між офісами, що розташовані в різних частинах міста. PAN (Personal Area Network) — персональна мережа, яка використовується для зв'язку між пристроями, що належать одній особі, наприклад, комп'ютерами, смартфонами, планшетами та іншими гаджетами. Зазвичай PAN охоплює невелику територію, наприклад, кімнату або автомобіль.

5. ПРОТОКОЛИ ПЕРЕДАЧІ ДАНИХ

Протоколи — це набори правил, що визначають, як дані передаються через мережу. Найпоширенішими протоколами

є TCP (Transmission Control Protocol) та IP (Internet Protocol). TCP забезпечує надійність передачі даних, розбиваючи інформацію на пакети, перевіряючи їх доставку і пересилаючи втрачені пакети. Завдяки TCP користувачі можуть бути впевнені, що їхні дані будуть доставлені без помилок і в правильному порядку.

IP відповідає за адресацію та маршрутизацію пакетів даних у мережі. Кожен пристрій у мережі має унікальну IP-адресу, що дозволяє ідентифікувати його серед інших пристроїв. Протокол IP розрізняє два основних типи адрес: IPv4, що складається з чотирьох октетів, і IPv6, що використовує шістнадцяткову систему числення і дозволяє значно розширити кількість доступних адрес.

Серед інших важливих протоколів можна виділити UDP (User Datagram Protocol), який, на відміну від TCP, не забезпечує надійності передачі даних, але є більш швидким, що робить його корисним для застосувань, де швидкість важливіша за надійність, таких як онлайн-ігри або потокове відео.

6. ПРИНЦИПИ МАРШРУТИЗАЦІЇ ТА АДРЕСАЦІЇ

Маршрутизація — це процес визначення шляху, яким дані рухаються від відправника до отримувача через мережу. Для цього використовуються маршрутизатори, які аналізують IP-адреси і вибирають найоптимальніший маршрут для передачі даних. Маршрутизатори взаємодіють між собою, обмінюючись інформацією про мережу, і будують таблиці маршрутизації, які використовуються для прийняття рішень щодо того, яким шляхом передавати дані.

IP-адресація дозволяє кожному пристрою в мережі мати унікальний ідентифікатор, що необхідно для доставки пакетів до правильного отримувача. Існують два основні типи адресації: статична, коли IP-адреса задається вручну і не змінюється з часом, і динамічна, коли адреса присвоюється автоматично за допомогою протоколу DHCP (Dynamic Host Configuration Protocol) і може змінюватися при кожному підключенні пристрою до мережі.

7. БЕЗПЕКА В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Безпека є критично важливою складовою роботи мереж. Вона включає в себе методи шифрування даних, аутентифікації користувачів, використання міжмережових екранів (фаєрволів) та антивірусних програм для захисту від несанкціонованого доступу та атак.

Шифрування даних забезпечує конфіденційність інформації, яка передається через мережу, перетворюючи її в зашифрований формат, що може бути розшифрований лише авторизованими користувачами. Аутентифікація користувачів дозволяє переконатися в тому, що доступ до мережі мають лише ті користувачі, які мають на це право.

Фаєрволи контролюють трафік між внутрішніми і зовнішніми мережами, блокуючи небезпечні або несанкціоновані з

8. ВИСНОВКИ

Принципи функціонування комп'ютерних мереж лежать в основі розвитку інформаційних технологій та є важливими для всіх сфер сучасного суспільства, від побутових пристроїв до глобальних систем управління. Вивчення мережових технологій, таких як LAN, MAN, WAN, PAN, а також протоколів передачі даних, дозволяє зрозуміти, як різні пристрої комунікують і взаємодіють один з одним.

Зокрема, надійна передача даних завдяки протоколам TCP/IP є фундаментом Інтернету. Проте сьогоденні вимоги, зокрема збільшення кількості підключених пристроїв, зростання трафіку та постійне збільшення кількості загроз кібербезпеці, вимагають інновацій у підходах до маршрутизації та захисту даних. Розвиток нових протоколів, таких як QUIC, та технологій, таких як SD-WAN, SDN і IPv6, створюють можливості для вирішення сучасних викликів.

Особливо важливу роль відіграє безпека мереж, адже з кожним роком збільшується кількість кіберзагроз, які можуть завдати шкоди як індивідуальним користувачам, так і великим організаціям. Застосування методів шифрування, аутентифікації, використання фаєрволів, VPN, та інтеграція систем виявлення загроз (IDS/IPS) стали критичними елементами захисту інформації. Крім того, в умовах масової цифровізації з'являються нові потреби в захисті віддаленого доступу та управлінні гібридними мережевими інфраструктурами.

Отже, сучасний фахівець у галузі комп'ютерної інженерії повинен не лише володіти знаннями про класичні концепції роботи мереж, але й бути в курсі сучасних технологій та тенденцій.

Список літератури

- [1] Tanenbaum, Andrew S. Computer networks / Andrew S. Tanenbaum, David J. Wetherall. – 5th ed. [2011]. – 938 p.
- [2] Kurose J. F. Computer Networking. A Top-Down Approach, 7th Ed / James F. Kurose, Keith W. Ross. – Pearson Education, Inc., 2017. – 864 p.
- [3] A. Behrouz, Forouzan. Data Communications and Networking, 4th ed., New York: McGraw-Hill Companies. Inc.; 2007. – 1171 p.
- [4] Comer, D. Internetworking with TCP/IP. Volume One (6th Edition). – Pearson, 2013. – 733 p.

¹ Робота виконана під керівництвом к. т. н., доц. Євгенії Шабали