Київський національний університет будівництва і архітектури

Кваліфікаційна робота на здобуття ОР «магістр»
на тему: «**Система захищеного доступу на основі Open VPN**»

Керівник КР: д.т.н., проф. Терентьєв О.О.
Розробив: студент спеціальності
125 «Кібербезпека», ОР «магістр»
Чуб Р.А..

Мета роботи – дослідження технології Open VPN, аналіз протоколів і розробка захищеного доступу на основі даної технології.

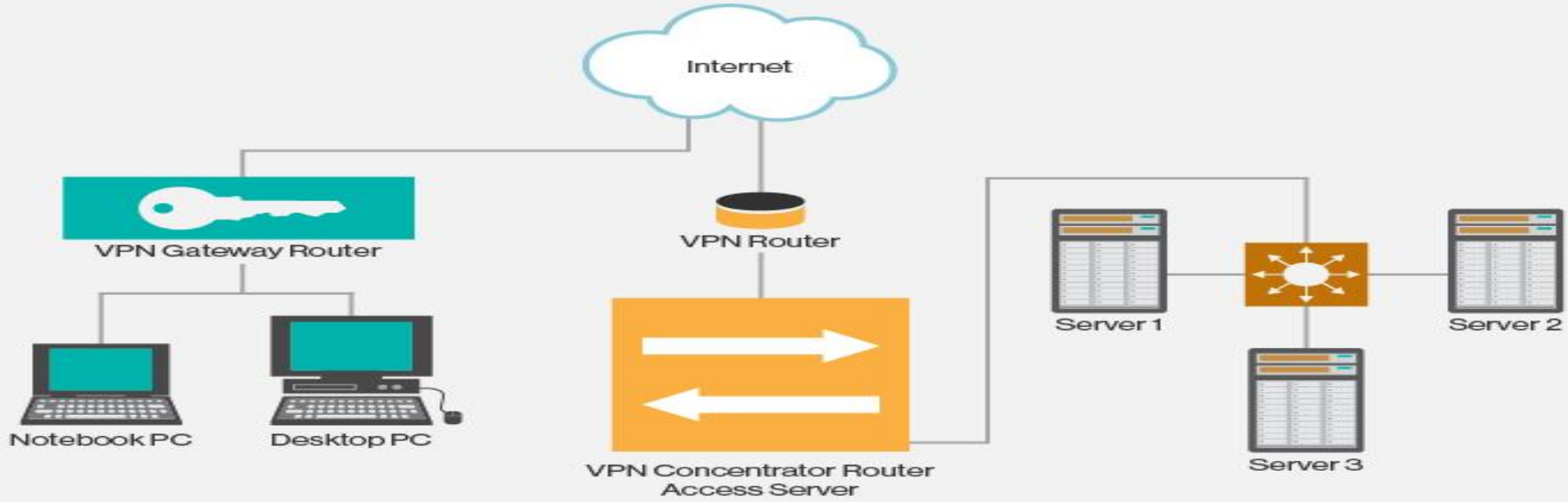
Основні завдання роботи:

1. Дослідження побудови та використання Open VPN
2. Аналіз протоколів VPN
3. Розробка захищеного доступу на основі технології Open VPN

Актуальність - в даний час віртуальні приватні мережі Open VPN (Open Virtual Private Network) широко використовуються в сучасних інформаційних системах. У найближчому майбутньому можна очікувати подальше зростання використання даної технології і появи нових рішень.

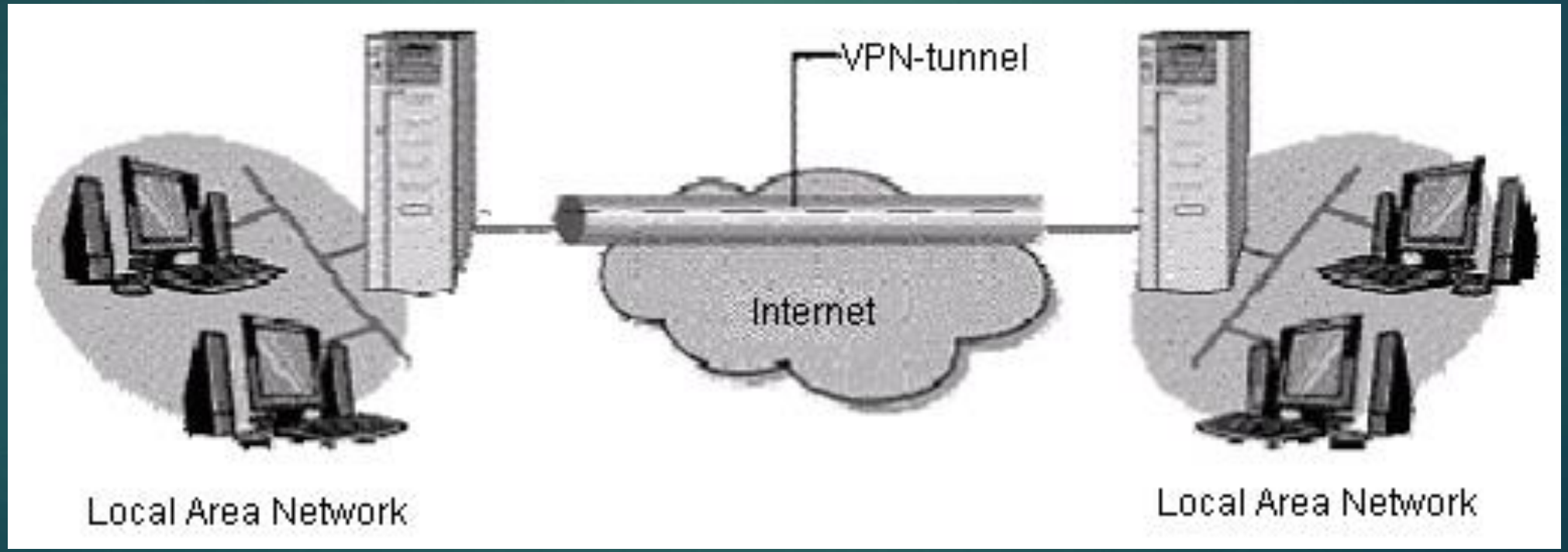
ПОНЯТТЯ ТА МЕТА МЕРЕЖІ VPN

VPN (скорочення від англ. *Virtual Private Network* — віртуальна приватна мережа) — узагальнююча назва мереж, що створюються поверх інших мереж, які мають менший рівень довіри. *Мета VPN-технологій* полягає в максимальному ступені відокремлення потоків даних одного підприємства від потоків даних всіх інших користувачів мережі загального користування.

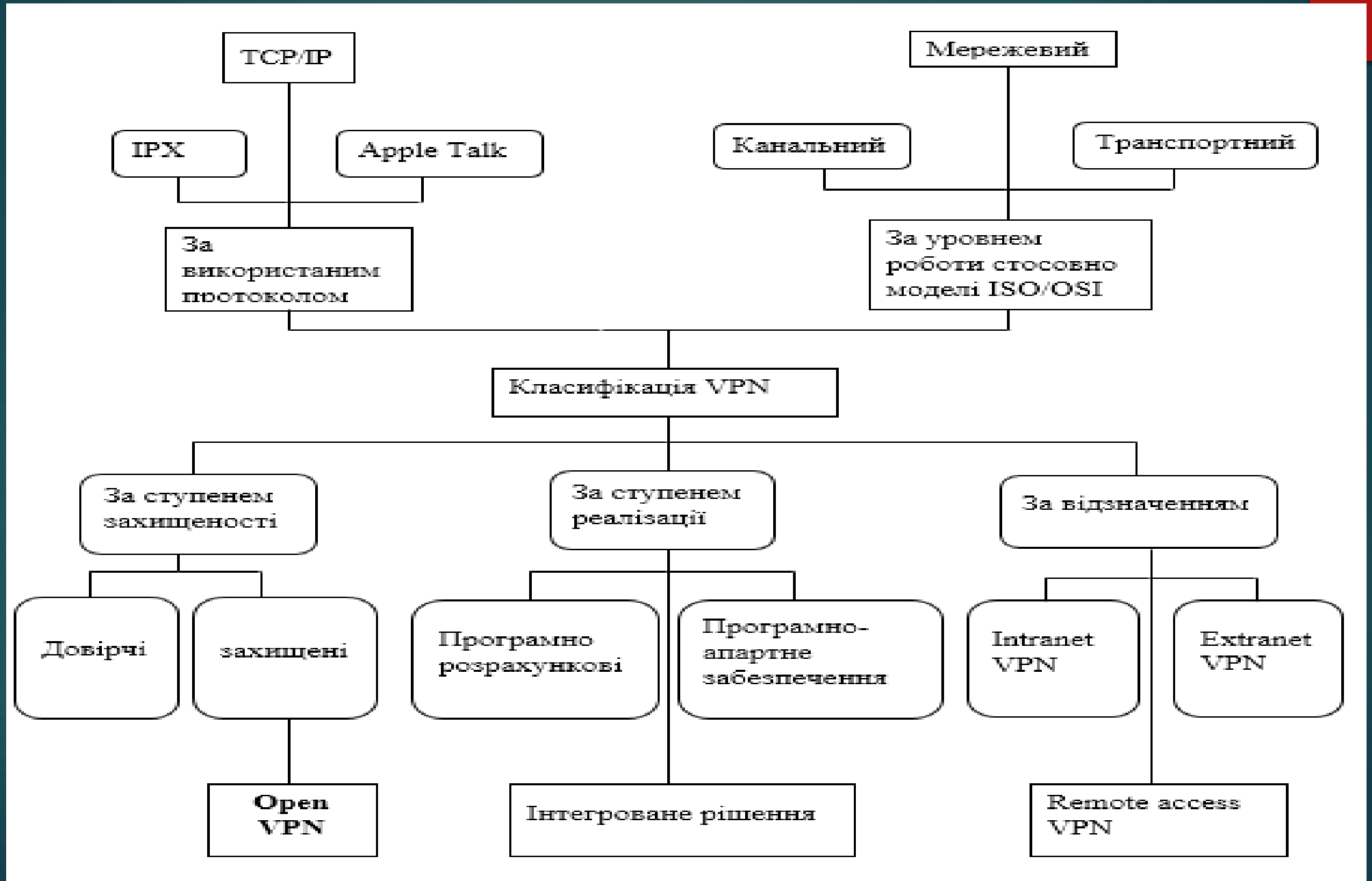


Структурна схема VPN

VPN складається з двох частин: «внутрішня» (підконтрольна) мережа, яких може бути декілька, і «зовнішня» мережа, через яку проходять інкапсульовані з'єднання (зазвичай використовується Інтернет).

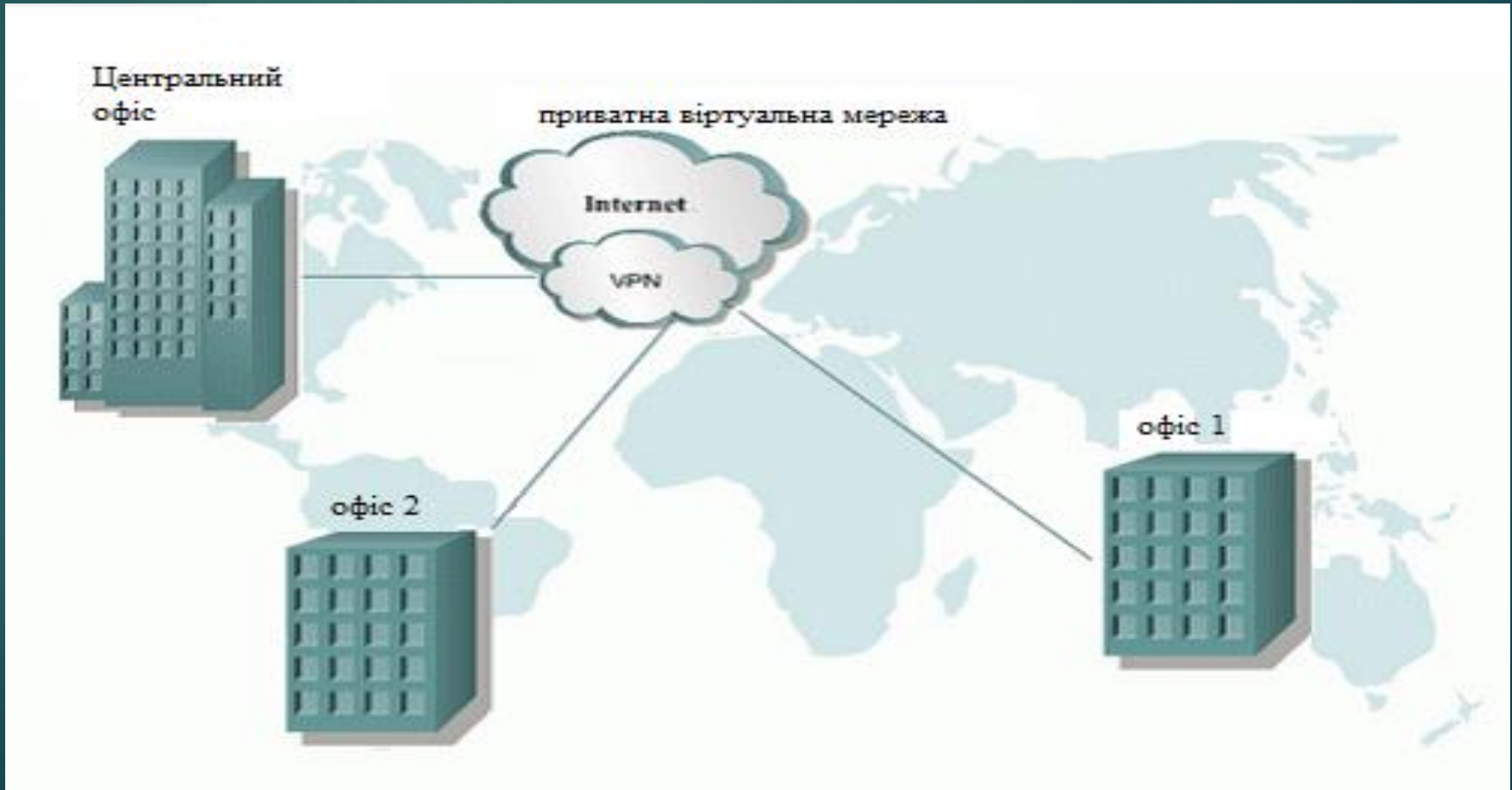


КЛАСИФІКАЦІЯ VPN-МЕРЕЖ



Open VPN

OpenVPN — вільна реалізація технології віртуальної приватної мережі (VPN) з відкритим сирцевим кодом для створення шифрованих з'єднань між двома клієнтськими машинами або забезпечення роботи централізованого VPN-сервера для одночасної роботи декількох клієнтів.



АНАЛІЗ ПРОТОКОЛІВ VPN МЕРЕЖ

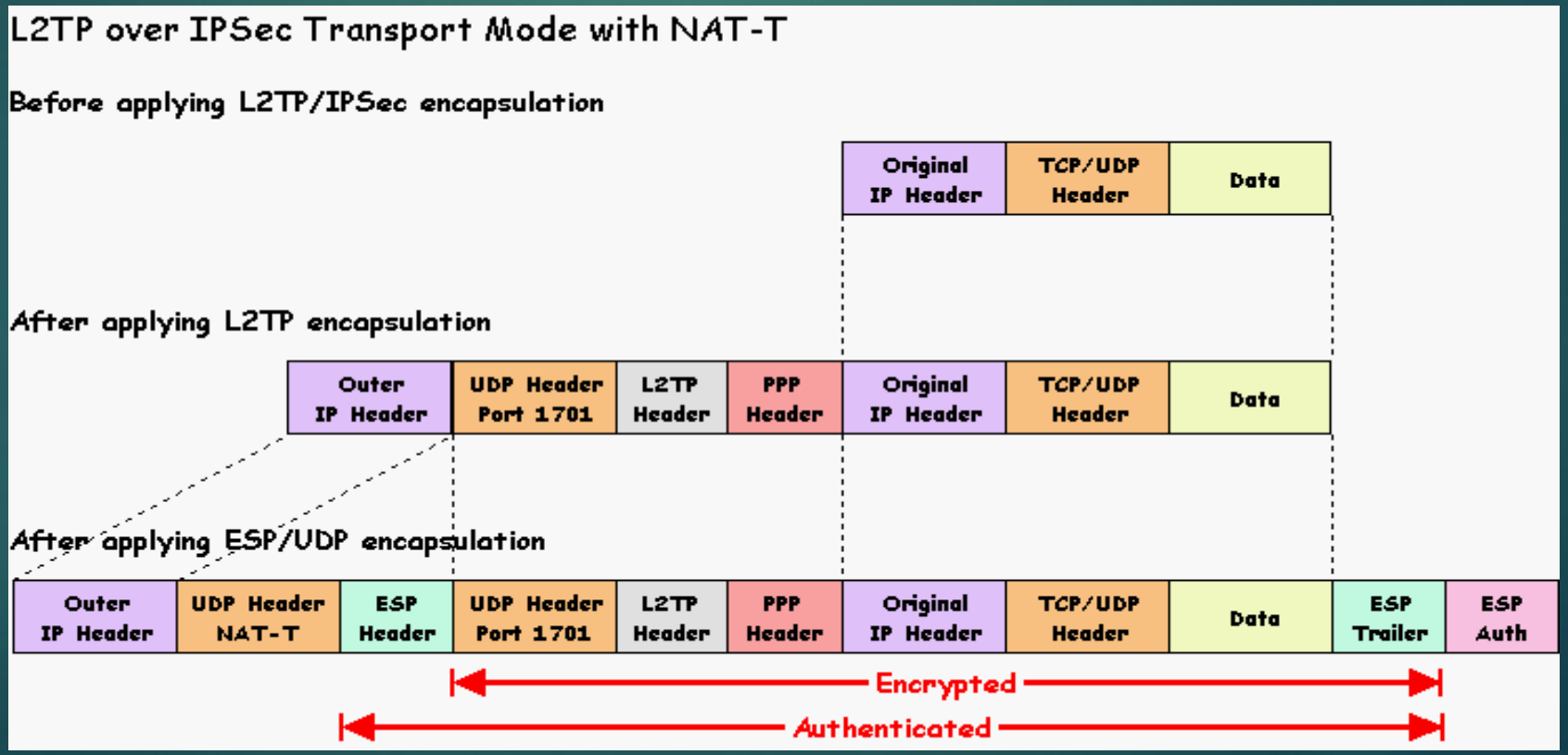
Захищений канал можна побудувати за допомогою системних засобів, реалізованих на різних рівнях моделі взаємодії відкритих систем OSI. Такі протоколи як: L2TP, PPTP, IPSec, і т.д.

Протоколи захищеного доступу	Прикладний	Впливають на додатки
	Представницький	
	Сеансовий	
	Транспортний	Не впливають на додатки
	Мережевий	
	Канальний	
	Фізичний	

Рівні протоколів захищеного каналу

ПРОТОКОЛ L2TP

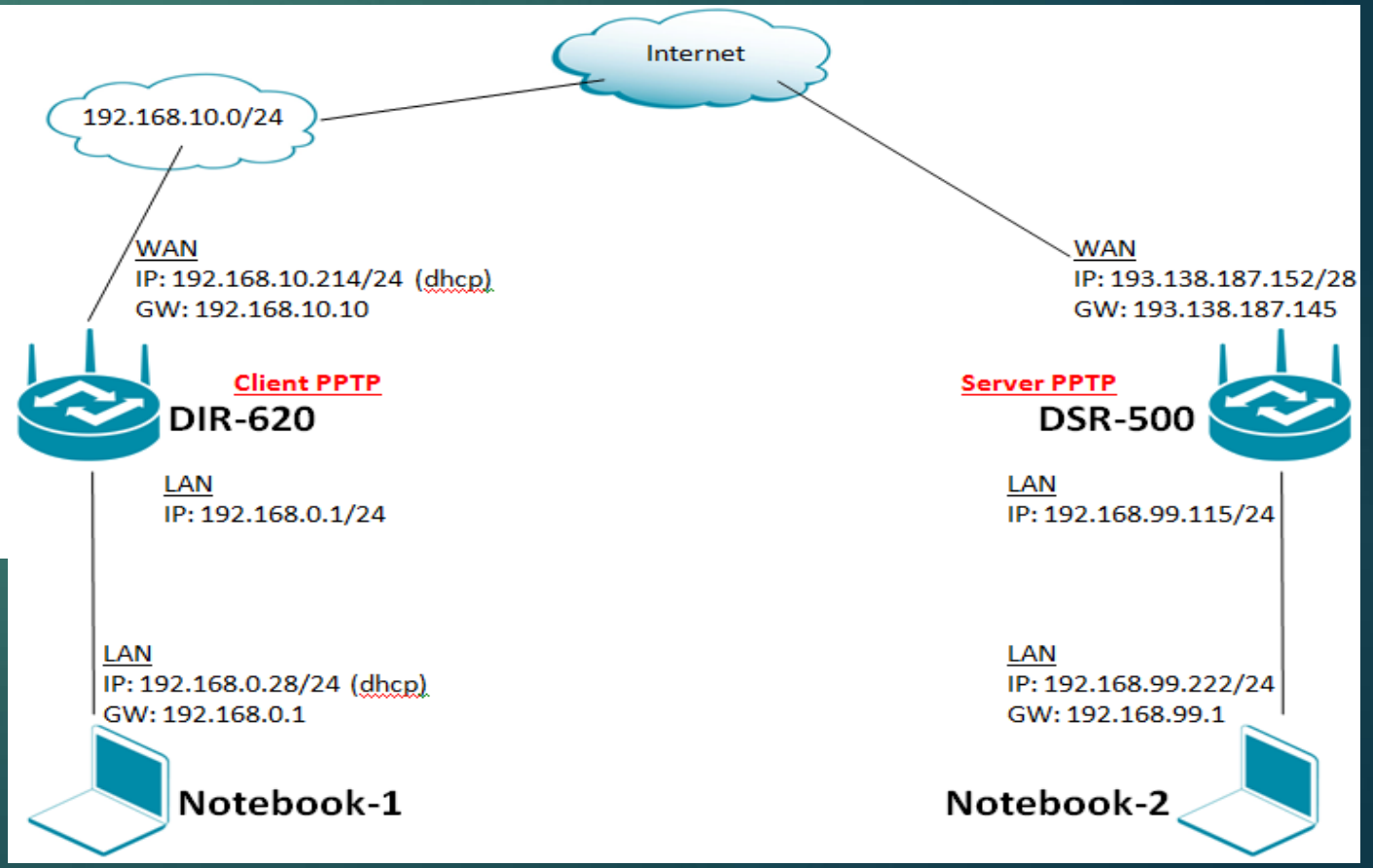
Протокол L2TP (Layer-2 Tunneling Protocol - L2TP) розроблений в організації Internet Engineering Task Force (IETF) за підтримки компаній Microsoft і Cisco Systems як протокол захищеного тунелювання PPP-трафіку через мережі загального призначення з довільним середовищем.



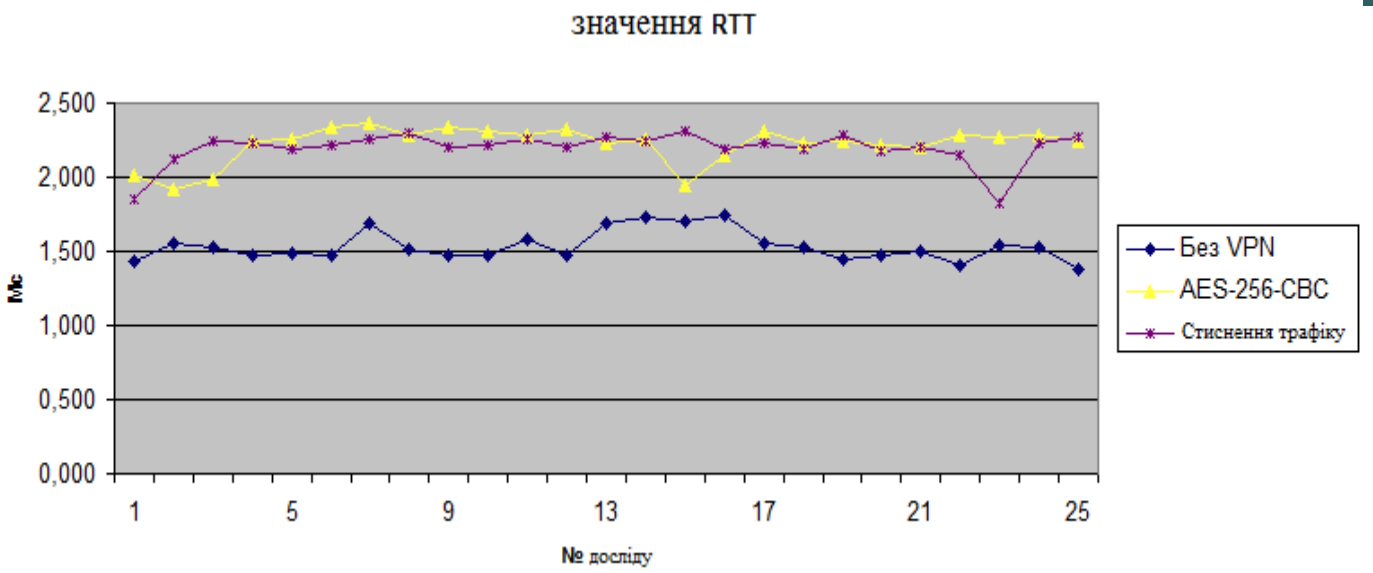
ПРОТОКОЛ PPTP

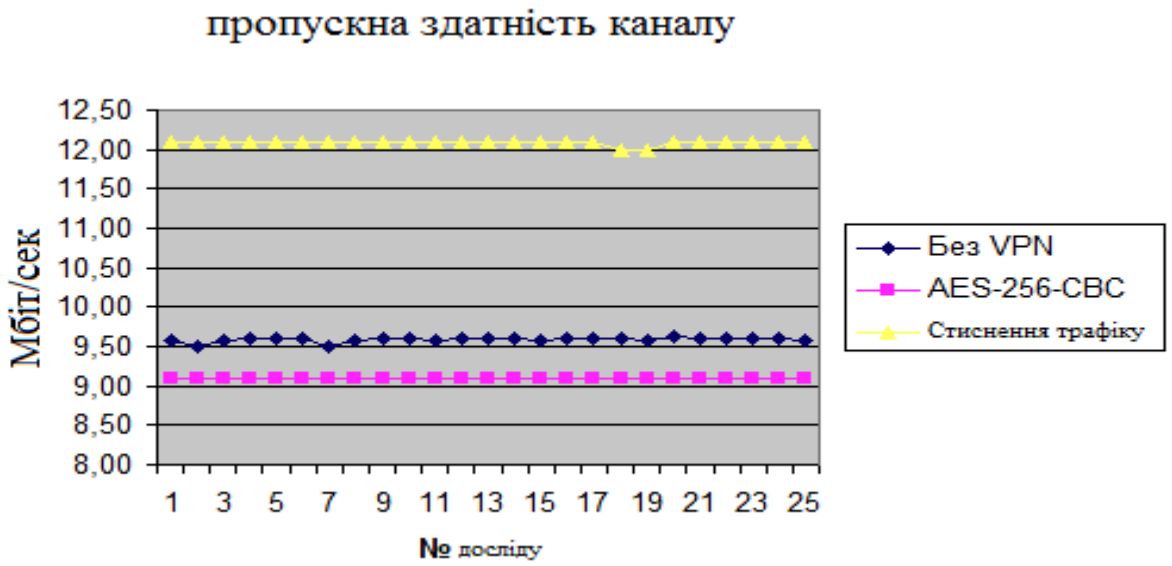
Протокол PPTP (Point-to-Point-Tunneling Protocol), розроблений Microsoft за підтримки інших компаній, є розширенням протоколу PPP (Point-to-Point Protocol) для створення захищених віртуальних каналів при доступі віддалених користувачів до локальних мереж через Internet.

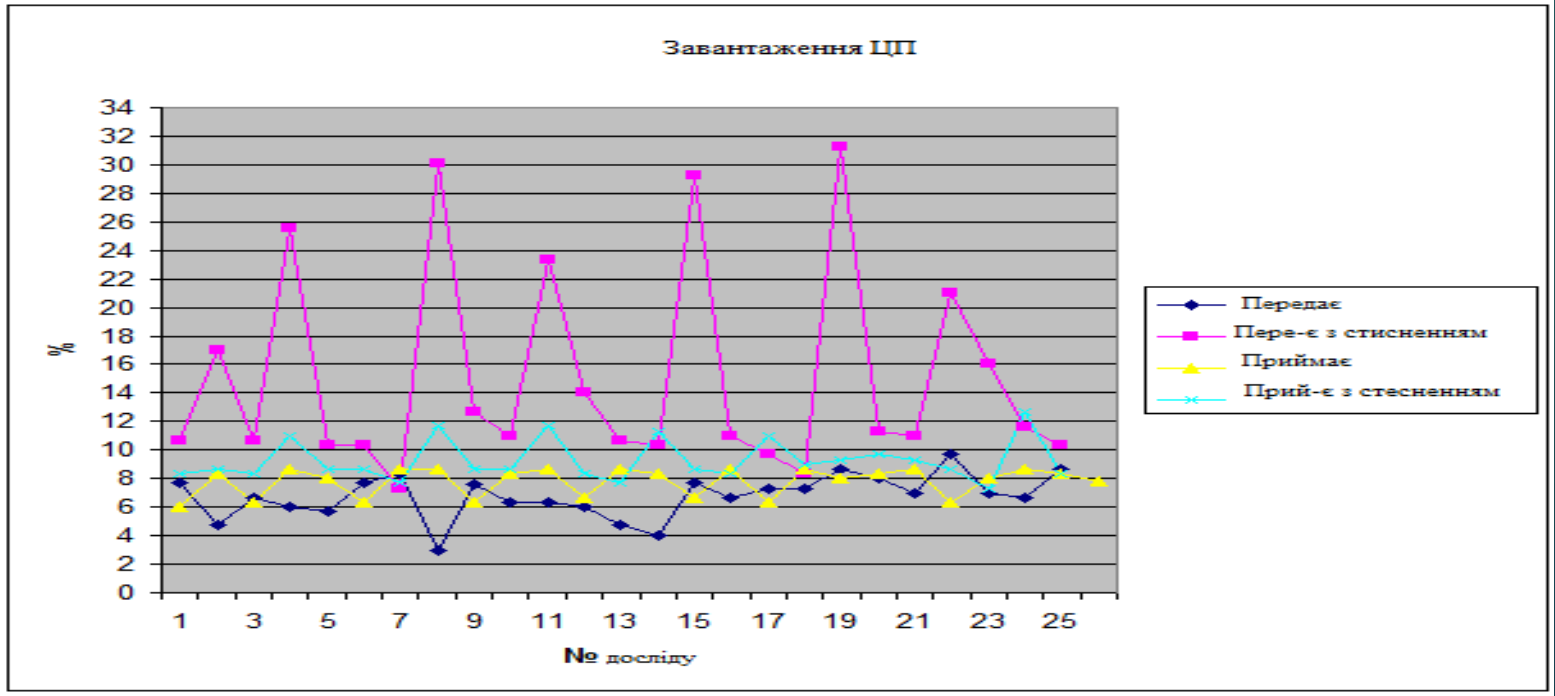
Заголовок кадру передачі	IP Заголовок	GRE заголовок	PPP заголовок	Зашифровані дані PPP	Закінчення кадру передачі



ОЦІНКА ПРОДУКТИВНОСТІ ПІД ЧАС ВИКОРИСТАННЯ OPEN VPN







ВИСНОВКИ

- проведено ретельне теоретичне ознайомлення з технологією OPEN VPN, можливостями її реалізації, тенденціями розвитку;
- розглянуто протоколи і методи реалізації віртуальних мереж. При аналізі протоколів VPN мереж робиться акцент на еталонній багаторівневій моделі OSI;
- було розроблено захищений доступ на основі Open VPN за допомогою побудови захищених каналів – тунелів;
- представлена оцінка продуктивності під час використання Open VPN;
- створюючи захищену мережу на основі технології OpenVPN, отримуємо одну загальну мережу на кілька офісів з шифрацією переданих даних і зростанням швидкості за рахунок стиснення трафіку.
- у загальному вигляді технологія OpenVPN повністю виправдовує себе.