Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Навчально-науковий інститут інформаційних технологій і робототехніки
Кафедра автоматики, електроніки та телекомунікацій

Пояснювальна записка

до кваліфікаційної роботи

магістр

на тему: **Проєктування розподіленої корпоративної мережі**

Виконав: студент 6 курсу, групи 601-ТТ
спеціальності 172 «Електронні комунікації та радіотехніка»
Панич В.В.
Керівник Індик С.В.
Рецензент Шефер О.В.

Полтава – 2025 рік

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Інститут Навчально-науковий інститут інформаційних технологій і робототехніки
Кафедра Автоматики, електроніки та телекомунікацій
Ступінь вищої освіти Магістр
Спеціальність 172 «Електронні комунікації та радіотехніка»

ЗАТВЕРДЖУЮ
Завідувач кафедри автоматики, електроніки та телекомунікацій
_____ О.В. Шефер
"02" 09 2024 р.

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Паничу Владиславу Володимировичу

1. Тема проекту (роботи) «Проєктування розподіленої корпоративної мережі» керівник проекту (роботи) Індик Сергій Володимирович, к.т.н., доцент, затверджена наказом вищого навчального закладу від "09" 08 2024 року № 818-р.
2. Строк подання студентом проекту (роботи) 27.12.2024 р.
3. Вихідні дані до проекту (роботи) ВБН В.2.2-33-2007. Проєктування телекомунікацій; ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою; RFC 4301: "Security Architecture for the Internet Protocol"; Cisco Packet Tracer; технічна документація Cisco.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Огляд сучасних підходів до побудови розподілених корпоративних мереж. Розгляд стандартів і протоколів, що використовуються в розподілених мережах. Характеристика обладнання для розподіленої корпоративної мережі. Огляд заходів і методів організації інформаційної безпеки в розподілених корпоративних мережах. Розробка логічної структури корпоративної мережі. Оцінка результатів моделювання взаємодії мережевих компонентів та аналіз результатів моделювання.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів):
   1) Титульний слайд
   2) Актуальність роботи
   3) Ключові принципи проектування
   4) Топологія розподілених корпоративних мереж

5) Стандарти та протоколи
6) Апаратні та програмні засоби мультисервісної мережі
7) Організація безпеки в корпоративних мережах
8) Модель корпоративної розподіленої мережі
9) Аналіз результатів моделювання на основі протоколу IPSec
10) Аналіз переваг та недоліків
11) Висновки по роботі

6. Дата видачі завдання 26.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів магістерської роботи	Термін виконання етапів роботи			Прим (плака
1	Аналіз принципів побудови розподілених корпоративних мереж	13.10.24		15%	Пл. 4
2	Дослідження особливостей проєктування мультисервісної мереж. Характеристика обладнання мультисервісної мережі.	27.10.24	I	30%	Пл. 8
3	Організація безпеки в корпоративних мережах	10.11.24		40%	Пл. 9
4	Вибір програмного забезпечення для моделювання	17.11.24		50%	—
5	Розробка схеми мережі на базі емулятора Cisco Packet Tracer	24.11.24	II	60%	Пл. 10
6	Оцінка результатів моделювання взаємодії мережевих компонентів та аналіз результатів моделювання	08.12.24		70%	Пл. 11-
7	Оформлення магістерської роботи	27.12.24	III	100%	Пл. 15

Магістрант _____ Панич В.В.

Керівник роботи _____ Індик С.В.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

DDoS (Distributed Denial of Service) — розподілена атака на відмову в обслуговуванні, що спрямована на перевантаження серверів, щоб зробити їх недоступними для користувачів.

IDS (Intrusion Detection System) — система виявлення вторгнень, яка аналізує трафік і виявляє підозрілі активності в мережі.

КІС (Комп'ютерна інформаційна система) — система, яка забезпечує збереження, обробку та передачу інформації за допомогою комп'ютерних технологій.

VPN (Virtual Private Network) — віртуальна приватна мережа, що створює захищений тунель для передачі даних через публічні мережі, такі як Інтернет.

RJ-45 (Registered Jack-45) — стандартний роз'єм для підключення мережевих кабелів, використовується в Ethernet-мережах.

OSPF (Open Shortest Path First) — протокол маршрутизації, що використовується в IP-мережах для визначення найкоротшого маршруту між вузлами.

EIGRP (Enhanced Interior Gateway Routing Protocol) — удосконалений протокол внутрішньої маршрутизації, розроблений компанією Cisco для ефективного управління трафіком.

NAT (Network Address Translation) — технологія перетворення IP-адрес, що дозволяє локальним мережам взаємодіяти з глобальною мережею Інтернет.

DMZ (Demilitarized Zone) — демілітаризована зона в мережі, яка створюється для захисту внутрішньої мережі, надаючи доступ до зовнішніх ресурсів.

TCP/IP (Transmission Control Protocol/Internet Protocol) — набір протоколів для передачі даних в мережах, що є основою Інтернету.

QoS (Quality of Service) — механізм забезпечення якості обслуговування в мережах, який гарантує пріоритет для важливого трафіку.

LAN (Local Area Network) — локальна обчислювальна мережа, що об'єднує пристрої в межах однієї фізичної локації.

WAN (Wide Area Network) — глобальна обчислювальна мережа, що з'єднує локальні мережі на великих відстанях.

VLAN (Virtual Local Area Network) — віртуальна локальна мережа, яка дозволяє розділяти фізичну мережу на логічні сегменти для підвищення продуктивності та безпеки.

MPLS (Multiprotocol Label Switching) — технологія маршрутизації пакетів у мережах, яка прискорює передачу даних завдяки використанню міток замість традиційної IP-маршрутизації.

STP (Spanning Tree Protocol) — протокол, що запобігає утворенню петель у топології мережі.

IPSec (Internet Protocol Security) — набір протоколів для забезпечення безпеки передачі даних через IP-мережі.

DHCP (Dynamic Host Configuration Protocol) — протокол, що автоматично призначає IP-адреси пристроям у мережі.

HTTPS (HyperText Transfer Protocol Secure) — захищений протокол передачі гіпертексту, що забезпечує шифрування даних між веб-браузером і сервером.

DNS (Domain Name System) — система доменних імен, що перетворює доменні імена в IP-адреси.

SSH (Secure Shell) — протокол для захищеного доступу до віддалених серверів та адміністрування мережевих пристроїв.

WPA2 (Wi-Fi Protected Access 2) — стандарт шифрування для захисту бездротових мереж, що забезпечує високий рівень безпеки.

MAC (Media Access Control) — адреса мережевого інтерфейсу, унікальний ідентифікатор пристрою в локальній мережі

ВСТУП

У сучасному світі інформаційні технології відіграють ключову роль у розвитку та функціонуванні підприємств різних розмірів і сфер діяльності. З кожним роком зростає потреба в організації ефективної та безпечної комунікації між співробітниками, підрозділами та філіями компаній, розташованими в різних географічних регіонах. У цьому контексті особливого значення набуває проєктування корпоративних мереж, які здатні забезпечити надійну взаємодію між різними елементами організаційної інфраструктури.

Корпоративна мережа — це основа для обміну інформацією всередині компанії, а також засіб забезпечення доступу до ресурсів, необхідних для виконання бізнес-завдань. З розвитком глобалізації, масштабуванням компаній та появою нових бізнес-моделей, особливо важливими стають розподілені корпоративні мережі, які об'єднують віддалені офіси, підрозділи, партнерів та клієнтів у єдину інформаційну екосистему. Такі мережі дозволяють забезпечити безперервний обмін даними між всіма учасниками бізнес-процесів, що підвищує оперативність прийняття рішень, оптимізує роботу компанії та зменшує затрати на комунікацію.

Актуальність теми. У зв'язку з безперервним зростанням обсягів даних, які передаються через мережі, а також із збільшенням кількості віддалених співробітників та офісів, компанії стикаються з новими викликами у сфері проєктування та впровадження розподілених мереж. Забезпечення надійності, безпеки, продуктивності та масштабованості таких мереж є пріоритетним завданням для IT-підрозділів організацій. Особливої важливості набувають питання захисту даних та запобігання несанкціонованому доступу, оскільки сучасні корпоративні мережі все частіше стають об'єктами кібератак.

Питання проєктування розподілених корпоративних мереж є актуальним як для великих компаній з глобальною присутністю, так і для середніх підприємств, що прагнуть розширити свої можливості та інтегруватися у цифрову економіку.

Таким чином, дослідження сучасних підходів до проєктування та впровадження таких мереж є важливим і актуальним завданням для забезпечення ефективної роботи підприємств у нових умовах.

Мета і завдання дослідження. Мета магістерської роботи полягає у розробці комплексного підходу до проєктування розподіленої корпоративної мережі, яка забезпечуватиме високу надійність, безпеку, масштабованість та продуктивність мережевої інфраструктури.

Завдання, що в рамках магістерської роботи, включають:

1. Проаналізувати сучасні тенденції у сфері проєктування корпоративних мереж, зокрема розподілених інфраструктур.
2. Дослідити основні вимоги до побудови розподілених корпоративних мереж з точки зору продуктивності, безпеки, масштабованості та надійності.
3. Визначити та порівняти існуючі архітектури корпоративних мереж, що використовуються в середніх та великих підприємствах.
4. Розробити концепцію проєктування розподіленої корпоративної мережі для конкретного підприємства, що відповідає сучасним вимогам до інформаційної безпеки та продуктивності.
5. Провести моделювання запропонованого мережевого рішення та проаналізувати його ефективність з використанням сучасних програмних засобів.
6. Оцінити можливості масштабування та адаптації розробленої мережі до зростаючих потреб компанії в умовах динамічного розвитку IT-середовища.

Об'єкт дослідження.

Об'єктом дослідження є розподілена корпоративна мережа. Це мережа, яка використовується для обміну даними між різними відділами компанії, які знаходяться в різних місцях. У роботі розглядається, як такі мережі будуються, які технології для цього використовуються і як забезпечити їхню безпеку. Особлива увага приділяється дослідженню методів забезпечення захищеності даних та оптимізації продуктивності мережі. Крім того, аналізуються сучасні підходи до управління трафіком і масштабованості мережевої інфраструктури.

Предмет дослідження.

Предметом дослідження є способи і підходи до проєктування розподілених корпоративних мереж. Зокрема, досліджується, як вибрати архітектуру мережі, які протоколи використовувати для обміну даними, як налаштувати безпеку і оптимізувати роботу мережі. Особливу увагу приділено забезпеченню безпеки переданих даних за допомогою протоколу IPSec, що дозволяє створити захищені канали зв'язку та забезпечити цілісність і конфіденційність інформації.

Практичне значення дослідження.

Результати магістерської роботи можна використовувати для створення або покращення корпоративних мереж на підприємствах. Запропоновані рекомендації допоможуть спроєктувати мережі, які будуть більш гнучкими, продуктивними і безпечними. Ці рішення можна застосувати в реальних умовах для забезпечення стабільної роботи мережі.

1. АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ РОЗПОДІЛЕНИХ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Вибір концепції мережі

Вибір концепції мережі є одним із найважливіших етапів у процесі проєктування розподіленої корпоративної мережі. Цей процес вимагає всебічного аналізу потреб у передачі даних, технічних характеристик та умов експлуатації. Правильно обрана концепція має забезпечувати надійне та безпечне функціонування телекомунікаційних послуг та ефективний обмін інформацією між різними підрозділами компанії.

Сьогодні корпоративні мережі повинні бути здатні адаптуватися до швидко змінюваного середовища, враховуючи фактори, такі як зростаюча мобільність співробітників, необхідність в віддаленому доступі до корпоративних ресурсів і використання хмарних технологій. Вибір концепції мережі також повинен враховувати потенційні загрози кібербезпеці, які можуть вплинути на цілісність та конфіденційність даних.

При виборі концепції мережі важливо визначити основні вимоги, які вона повинна задовольняти, зокрема:

- Безпека: Забезпечення надійного захисту даних і доступу до мережі.
- Продуктивність: Гарантування швидкості та надійності зв'язку між усіма підрозділами.
- Масштабованість: Можливість легкого розширення мережі у відповідь на зростаючі потреби.
- Економічність: Вибір рішень, що відповідають бюджетним обмеженням організації, без втрати якості.

Вибір концепції мережі має бути результатом ретельного аналізу і повинно базуватися на інтеграції різних аспектів, таких як технологічні інновації, вимоги

бізнесу і майбутні тенденції розвитку. Це дозволить забезпечити не лише стабільність і ефективність роботи корпоративної мережі, але й її здатність до адаптації в умовах змін.

Локальна мережа (LAN)

LAN (Local Area Network) — це мережа, яка з'єднує комп'ютери та інші пристрої в межах обмеженої географічної території, такої як будівля, офіс або кампус. LAN дозволяє користувачам обмінюватися файлами, доступати ресурси (наприклад, принтери, сервери) та спільно використовувати мережеві пристрої (Рисунок 1.1). Мережа LAN може бути побудована з використанням різних типів з'єднань, включаючи Ethernet, Wi-Fi та інші технології, що забезпечують зв'язок на малих відстанях [1].

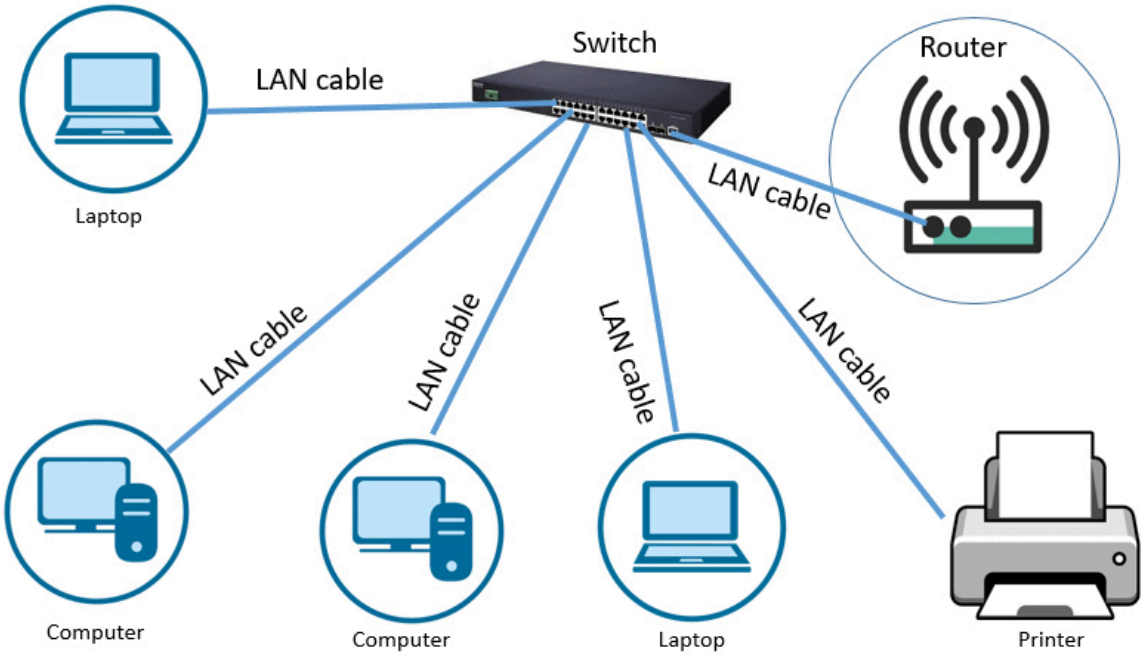


Рисунок 1.1 — Локальна мережа

LAN є основою для організації внутрішньої мережі в компанії, школі, університеті або в будь-якому іншому середовищі, де необхідно забезпечити обмін інформацією між пристроями в межах однієї будівлі або кампусу. Вона дозволяє

підключати комп'ютери до мережі для доступу до спільних ресурсів, таких як принтери, файли та бази даних. Також LAN може використовуватися для створення внутрішніх веб-сайтів або для забезпечення внутрішнього зв'язку, що дозволяє спрощувати роботу організації.

Переваги LAN:

- Швидкість і ефективність: LAN забезпечує швидке з'єднання та високошвидкісну передачу даних між пристроями на коротких відстанях.
- Низька вартість: Порівняно з WAN, LAN має низькі витрати на обладнання та установку, оскільки використовує доступні технології зв'язку.
- Зручність в управлінні: Локальна мережа зазвичай має меншу кількість пристроїв і простіший для налаштування та підтримки, що зменшує складність управління мережевою інфраструктурою.
- Широкі можливості для спільного використання ресурсів: Всі пристрої в мережі можуть ділити доступ до файлів, принтерів та інших ресурсів, що значно підвищує ефективність роботи.

Недоліки LAN:

- Обмежене покриття: LAN працює лише на обмежених відстанях, що обмежує її використання в великих або віддалених приміщеннях.
- Залежність від фізичної інфраструктури: Для надійного функціонування LAN необхідно прокладати кабелі (Ethernet) або забезпечувати стабільне Wi-Fi покриття, що може бути проблемою для великих будівель або застарілих мереж.
- Уразливість до збоїв: Якщо є фізичні пошкодження в мережевій інфраструктурі або проблеми з обладнанням, це може вплинути на роботу всієї мережі.

LAN є основною технологією для організації мережі в межах однієї будівлі або кампусу. Вона забезпечує високу швидкість передачі даних, ефективне використання ресурсів і зручність в управлінні, однак її покриття обмежене лише кількома десятками чи сотнями метрів. Зважаючи на невеликі витрати та простоту

налаштування, LAN є ідеальним рішенням для більшості малих і середніх організацій.

Глобальна комп'ютерна мережа (WAN)

WAN (Wide Area Network) — це мережа, яка охоплює великі географічні території, з'єднуючи різні локальні мережі (LAN) та дозволяючи їм обмінюватися даними на великі відстані (Рисунок 1.2). WAN може з'єднувати філії компаній в різних містах, країнах чи континентах. Ці мережі використовуються для обміну інформацією між офісами та надання доступу до централізованих ресурсів компанії, таких як сервери або бази даних.

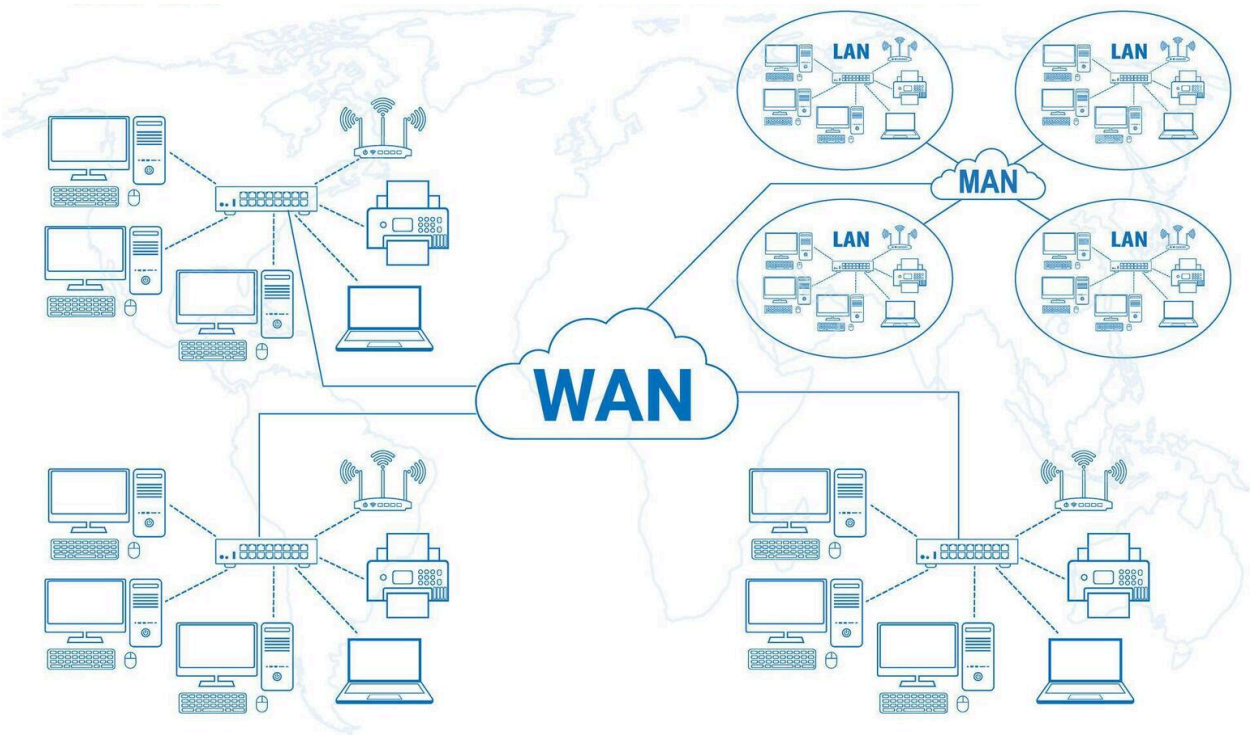


Рисунок 1.2 — Глобальна комп'ютерна мережа

WAN дає можливість організаціям ефективно об'єднувати віддалені офіси, працюючи з ними як з єдиною мережею. Це може включати віддалений доступ до корпоративних систем, передачу великих обсягів даних або забезпечення з'єднання між кількома офісами. WAN також дозволяє компаніям використовувати

централізовані сервери для зберігання даних, що дозволяє знижувати витрати на локальні ресурси [2].

Переваги WAN:

- Покриття великих територій: WAN дає змогу з'єднувати офіси або філії, розташовані на значних відстанях.
- Економія на інфраструктурі: Усі віддалені філії можуть підключатися до одного центрального сервера або бази даних, що зменшує необхідність у локальних системах.
- Масштабованість: WAN легко розширюється на нові географічні регіони, що є важливим фактором для міжнародних компаній.

Неадоліки WAN:

- Вартість: Зв'язок на великі відстані, особливо між континентами, може бути дорогим, особливо при використанні спеціалізованих каналів зв'язку.
- Низька пропускна здатність: WAN може мати обмежену пропускну здатність, що спричиняє більшу затримку і сповільнює передачу даних.
- Проблеми з надійністю: Оскільки WAN залежить від багатьох підключень та провайдерів, будь-які збої в одному з елементів можуть спричинити проблеми з підключенням.

WAN є незамінним інструментом для організацій, що мають кілька офісів або філій по всьому світу. Проте висока вартість і можливі проблеми з пропускною здатністю або надійністю потребують ретельного планування та вибору оптимальних рішень для з'єднань.

Віртуальні локальні мережі (VLAN)

VLAN (Virtual Local Area Network) — це технологія, яка дозволяє логічно розділяти одну фізичну мережу на кілька ізольованих сегментів (Рисунок 1.3). Кожен сегмент VLAN поводиться як окрема мережа, навіть якщо пристрої, що належать до різних VLAN, фізично знаходяться в одній точці мережі. Це дозволяє адміністраторам розділяти мережі для різних відділів, служб чи проектів без необхідності прокладати додаткові кабелі. VLAN також дозволяє ефективно управляти трафіком, оптимізуючи використання ресурсів і забезпечуючи безпеку .

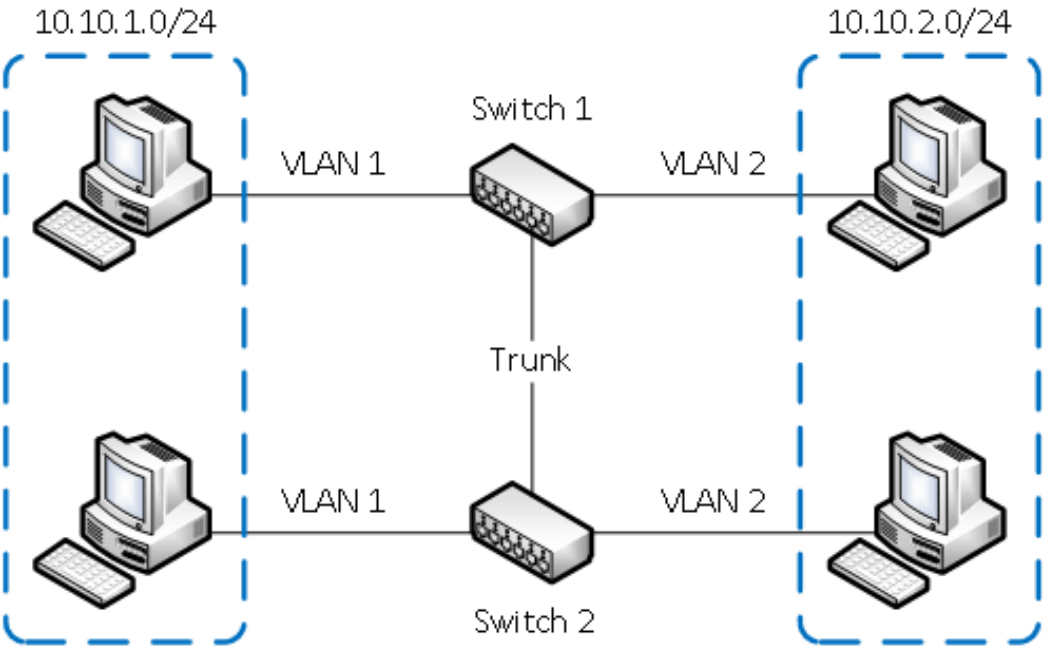


Рисунок 1.3 — Приклад реалізації VLAN

VLAN використовуються для зменшення навантаження на мережу, покращення її продуктивності, безпеки та управління. Це дозволяє створювати логічні підмережі для різних функцій організації, таких як відділи, без необхідності змінювати фізичну інфраструктуру. Наприклад, адміністративний відділ може мати окремий VLAN, який не буде мати прямого доступу до VLAN фінансового або виробничого відділів [3].

Переваги VLAN:

- Сегментація трафіку: VLAN допомагає розділити мережу на різні логічні сегменти, що покращує управління трафіком і підвищує продуктивність, зменшуючи колізії.
- Покращена безпека: Ізоляція мереж дозволяє обмежити доступ до чутливих даних або систем лише для користувачів чи пристроїв, що належать до конкретного VLAN.
- Менше мережевого трафіку: VLAN зменшує кількість широкомовних пакетів, обмежуючи їх лише певними сегментами мережі, що знижує навантаження.

- Гнучкість і масштабованість: VLAN дає можливість змінювати топологію без фізичної реконфігурації мережі. Це дозволяє більш ефективно використовувати існуючу інфраструктуру.
- Краще управління: Логічне розподілення трафіку допомагає краще керувати мережевими ресурсами, зокрема при налаштуванні пріоритетів для певних видів трафіку.

Недоліки VLAN:

- Складність налаштування: Налаштування VLAN може бути складним, особливо в великих мережах, де потрібно ретельно продумувати логіку сегментації.
- Обмеження на управління: Якщо неправильне управління VLAN може призвести до проблем з доступом, наприклад, до створення некоректних маршрутів між VLAN.
- Необхідність у додаткових пристроях: Для реалізації VLAN часто потрібні спеціальні комутатори, що підтримують цю технологію, що може додатково збільшити витрати на обладнання.
- Безпека на рівні елементів: Хоча VLAN підвищує безпеку, вона не є абсолютно захищеною, оскільки за допомогою спеціалізованих атак (наприклад, VLAN hopping) зловмисники можуть отримати доступ до даних.

VLAN є важливим інструментом для сегментації мережі, який дозволяє підвищити безпеку, зменшити навантаження та покращити управління мережею. Однак для досягнення максимальних результатів необхідне правильне налаштування та технічна підтримка, що може бути складним завданням для великих або складних інфраструктур.

Віртуальні приватні мережі (VPN)

VPN (Virtual Private Network) — це технології, які забезпечують безпечний доступ до приватних мереж через публічні інтернет-з'єднання (Рисунок 1.4). VPN дозволяє створювати захищене з'єднання через публічну мережу (наприклад, Інтернет), що дає змогу користувачам працювати з корпоративними ресурсами, як у локальній мережі. VPN використовує шифрування для забезпечення

конфіденційності переданих даних і забезпечує анонімність, що є важливим при доступі до чутливих або конфіденційних інформаційних систем [4].

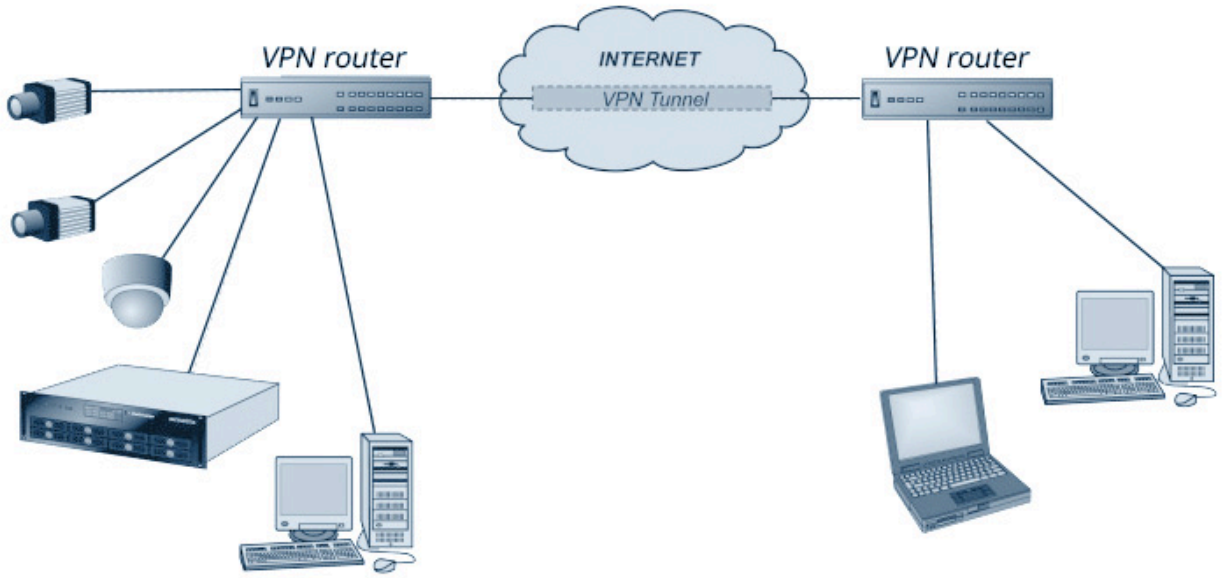


Рисунок 1.4 — Схема VPN з’єднання

VPN часто використовується для забезпечення безпечного віддаленого доступу до корпоративних мереж, особливо для працівників, які працюють із дому або з інших віддалених локацій. VPN також дозволяє безпечно передавати дані між двома віддаленими мережами, що важливо для захисту інформації від перехоплення, коли користувачі підключаються до публічних Wi-Fi мереж.

Переваги VPN:

- Безпека даних: VPN шифрує весь трафік, що забезпечує захист від перехоплення та атак.
- Віддалений доступ: VPN дозволяє віддаленим працівникам або філіям отримувати доступ до корпоративних ресурсів, як якщо б вони знаходилися в локальній мережі.

Недоліки VPN:

- Затримки в передачі даних: Використання VPN може призвести до збільшення затримок через шифрування та маршрутизацію трафіку через додаткові сервери.
- Складність налаштування: Налаштування VPN потребує спеціальних знань, що може бути перешкодою для деяких організацій.

VPN є важливим інструментом для забезпечення безпеки та конфіденційності при віддаленому доступі до мережі. Хоча він може уповільнити інтернет-з'єднання, його переваги для захисту даних значно перевищують ці недоліки.

Мультипротокольне маркування (MPLS)

MPLS (Multiprotocol Label Switching) — це потужна технологія, яка забезпечує ефективну маршрутизацію даних у великих та складних мережах (Рисунок 1.5). Завдяки своїй здатності підтримувати різні типи трафіку та протоколів, MPLS стає важливим інструментом для оптимізації мережевих ресурсів та забезпечення високої якості обслуговування. Технологія дозволяє забезпечити швидшу та більш ефективну передачу даних, особливо в складних мережах з великими обсягами трафіку.

MPLS підтримує різноманітні протоколи та дозволяє створювати приватні віртуальні мережі (VPN), а також забезпечує високий рівень якості обслуговування (QoS), що є важливим для підприємств, які потребують гарантованої пропускної здатності та мінімізації затримок [5].

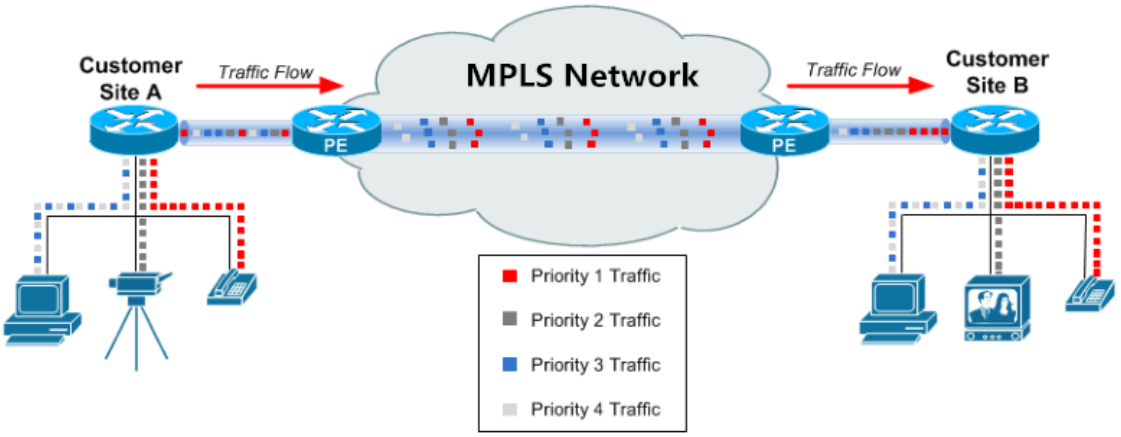


Рисунок 1.5 — Схема MPLS мережі

MPLS використовується для оптимізації маршрутизації та управління мережевим трафіком у великих корпоративних або операторських мережах. Вона дозволяє створювати приватні віртуальні мережі (VPN) для віддалених офісів та підрозділів, забезпечувати високоякісну передачу даних для критичних додатків, таких як голосові чи відео-трансмісії, де важлива мала затримка та стабільність з'єднання та оптимізувати використання мережевих ресурсів, зменшуючи необхідність у постійній маршрутизації IP-пакетів.

Переваги MPLS:

- Швидкість та продуктивність: Однією з головних переваг MPLS є його здатність забезпечувати високу швидкість та продуктивність у маршрутизації даних.
- Гнучкість: MPLS пропонує велику гнучкість у використанні різних протоколів, що робить його універсальним рішенням для корпоративних мереж.
- Простота в управлінні і масштабованість: MPLS дозволяє легко масштабувати мережу, додаючи нові лінії або маршрути для обробки більшого трафіку без великих змін у топології.

Недоліки MPLS:

- Високі витрати: Одним з найбільших недоліків MPLS є висока вартість впровадження та експлуатації. Провайдери послуг часто стягують значні

плати за підключення та щомісячні послуги, що може стати перешкодою для малих і середніх підприємств.

- Складність налаштування та управління: Налаштування та управління мережами MPLS може бути складним і вимагати спеціалізованих знань.
- Відсутність шифрування: Хоча MPLS забезпечує певний рівень безпеки, відсутність вбудованих механізмів шифрування означає, що організації повинні додатково впроваджувати шифрування для захисту даних у випадках, коли це необхідно.

MPLS є потужним і ефективним інструментом для забезпечення високої продуктивності та надійності в великих корпоративних та операторських мережах. Вона ідеально підходить для організацій, які потребують високої пропускної здатності, мінімальних затримок і стабільної роботи критичних додатків. Однак технологія вимагає високих інвестицій у налаштування та обслуговування, що може бути невигідно для малих компаній.

Після ретельного аналізу переваг і недоліків таких технологій, як VLAN, VPN і MPLS, можна зробити обґрунтований висновок про вибір оптимальної концепції для розподілених корпоративних мереж. Хоча кожна з цих технологій має свої переваги, VPN, незважаючи на деякі недоліки, виявляється найбільш ефективним рішенням для організацій, які потребують безпечного і надійного доступу до корпоративних ресурсів.

Однією з основних переваг VPN є її здатність забезпечити високий рівень безпеки. Використовуючи шифрування даних, VPN захищає конфіденційну інформацію від можливих загроз, таких як перехоплення або атаки зловмисників. Це особливо важливо в умовах зростаючих кіберзагроз, коли компанії стикаються з ризиками витоку даних та втрати конфіденційності. VPN дозволяє співробітникам, які працюють з віддалених локацій, впевнено отримувати доступ до важливих ресурсів, знаючи, що їх дані захищені.

Крім безпеки, VPN також пропонує високу гнучкість. Сучасний бізнес вимагає можливості швидко адаптуватися до змін у середовищі, таких як віддалена робота або розширення на нові ринки. VPN дозволяє компаніям легко

налаштовувати доступ до ресурсів для нових користувачів та пристроїв, що спрощує процес адміністрування. В умовах, коли багато компаній переходять на моделі гібридної або віддаленої роботи, важливо мати технологію, яка забезпечує зручний доступ до корпоративних систем з будь-якої точки світу.

Ще одним важливим аспектом є економічна ефективність. Використання VPN може знизити витрати на інфраструктуру зв’язку. На відміну від MPLS, який вимагає значних інвестицій у приватні лінії зв’язку, VPN дозволяє використовувати вже існуючі інтернет-з'єднання для забезпечення доступу до ресурсів компанії. Це робить VPN більш доступним варіантом для малих і середніх підприємств, які прагнуть зберегти бюджет, але при цьому не хочуть жертвувати безпекою.

Незважаючи на наявні недоліки VPN, такі як можливі затримки в передачі даних і складність налаштування, переваги, які вона надає, перевищують ці недоліки в контексті сучасних вимог до бізнесу. Тому, при проектуванні розподіленої корпоративної мережі, рекомендується обирати VPN як основний інструмент для забезпечення безпечного зв’язку. Це не тільки відповідає потребам в безпеці та доступності, але й сприяє формуванню ефективної і гнучкої мережевої інфраструктури, яка може швидко реагувати на виклики сучасного бізнес-середовища.

1.2 Визначення структури розподіленої корпоративної мережі

Визначення структури розподіленої корпоративної мережі є важливим етапом, оскільки вона визначає, як будуть організовані та взаємодіятимуть усі елементи системи. Правильна структура мережі забезпечує високий рівень продуктивності, надійності, масштабованості та безпеки, що, в свою чергу, сприяє ефективності бізнес-процесів.

Структура розподіленої корпоративної мережі зазвичай складається з кількох ключових компонентів, які виконують свої специфічні функції. У її основі лежить клієнт-серверна архітектура, де клієнти, такі як комп'ютери або мобільні пристрої, звертаються до серверів для отримання доступу до ресурсів і послуг. Сервери в цій архітектурі відіграють важливу роль, оскільки вони зберігають дані, обробляють запити та виконують бізнес-логіку, що є критично важливим для функціонування організації.

Додатково, мережа включає в себе різноманітні мережеві пристрої, такі як маршрутизатори, комутатори та кінцеві пристрої. Маршрутизатори відповідають за пересилання даних між різними сегментами мережі, забезпечуючи зв'язок між локальними мережами та глобальним Інтернетом. Комутатори, в свою чергу, оптимізують трафік усередині локальної мережі, зменшуючи затримки при передачі даних.

Ще однією важливою складовою структури розподіленої корпоративної мережі є системи зберігання даних. Це можуть бути мережеві сховища, які дозволяють централізовано зберігати інформацію, що робить її доступною для всіх користувачів організації. Такі системи підвищують ефективність роботи з даними і забезпечують простий доступ до важливої інформації.

Безпека є критично важливим аспектом у структурі розподіленої мережі. Використання брандмауерів, систем виявлення та запобігання вторгненням (IDS/IPS) та віртуальних приватних мереж (VPN) забезпечує захист даних і запобігає несанкціонованому доступу. Це особливо важливо для організацій, які обробляють конфіденційну інформацію.

При визначенні структури мережі важливо враховувати не лише її компоненти, а й рівні, на яких ці компоненти взаємодіють. Зазвичай розподілені корпоративні мережі діляться на три основних рівня: доступний, агрегаційний та ядровий. Доступний рівень є найнижчим, де користувачі підключаються до мережі через робочі станції, ноутбуки та мобільні пристрої. Агрегаційний рівень відповідає за управління трафіком, що проходить від кількох доступних рівнів, включаючи комутатори, які забезпечують з’єднання між підключеними

пристроями. Ядровий рівень є серцем мережі, який забезпечує високу пропускну здатність та швидкість передачі даних через маршрутизатори та комутатори, що забезпечують пересилання інформації між різними сегментами.

Коли мова йде про вибір структури розподіленої корпоративної мережі, важливо враховувати кілька факторів. По-перше, розмір і географічне розташування організації визначають, як мережа буде розподілена. Для великих компаній з численними філіями важливо, щоб мережа підтримувала різні локації, забезпечуючи при цьому зручний доступ до ресурсів. По-друге, типи даних, які будуть оброблятися, також повинні враховуватися при проектуванні мережі, оскільки це вплине на налаштування безпеки та управління даними. Кількість користувачів, які одночасно використовують мережу, має вирішальне значення для визначення необхідної пропускної здатності, що допоможе уникнути перевантаження мережі.

Визначення структури розподіленої корпоративної мережі є критично важливим процесом, що забезпечує ефективність та надійність роботи підприємства. Правильна організація елементів мережі та їх взаємозв'язок дозволяють забезпечити стабільну роботу у швидко змінюваному технологічному середовищі, що, в свою чергу, впливає на успішність бізнесу.

1.3 Стандарти та протоколи

Стандарти та протоколи є критично важливими елементами розподілених корпоративних мереж, оскільки вони визначають правила, за якими відбувається обмін даними між різними пристроями та системами. У сучасному інформаційному середовищі, де використовуються різноманітні технології та платформи, дотримання стандартів забезпечує сумісність, надійність та безпеку мережі.

Стандарти відіграють ключову роль у забезпеченні правильного функціонування корпоративних мереж, оскільки вони визначають технічні вимоги та норми для різних компонентів мережі, таких як обладнання, програмне забезпечення та протоколи зв'язку. Завдяки цим стандартам знижуються ризики несумісності між пристроями від різних виробників, а також полегшується інтеграція нових технологій, що забезпечує стабільність і надійність мережі. Ось деякі з основних стандартів, що використовуються в корпоративних мережах:

1. **IEEE 802** — це сімейство стандартів, що визначає вимоги до різних типів мереж, включаючи локальні (LAN) і широкомасштабні (WAN). Ці стандарти забезпечують узгодженість у роботі мереж і пристроїв різних виробників. Наприклад:
    - IEEE 802.3 — стандарт, який визначає технологію Ethernet для проводових локальних мереж. Ethernet є основною технологією для передачі даних в корпоративних мережах завдяки своїй надійності та швидкості.
    - IEEE 802.11 — стандарт для бездротових мереж Wi-Fi. Він описує методи і технічні вимоги для створення та підтримки бездротових з'єднань у місцях, де використання проводів неможливе або непрактичне. Цей стандарт є основою для більшості корпоративних бездротових мереж.
2. **ISO/IEC 27001** — це міжнародний стандарт для систем управління безпекою інформації (ISMS). Цей стандарт допомагає організаціям визначити, впровадити, підтримувати та покращувати політики безпеки, що охоплюють всі аспекти захисту інформації. Відповідно до цього стандарту, організації повинні забезпечити конфіденційність, цілісність та доступність даних, а також управлінську і технічну безпеку їх обробки та зберігання. Цей стандарт є критично важливим для захисту корпоративних даних від загроз та несанкціонованого доступу [6].
3. **ITU-T** — це сектор міжнародного союзу електрозв'язку (ITU), який розробляє глобальні стандарти для телекомунікаційних технологій. Стандарти ITU-T забезпечують сумісність і взаємодію між різними мережами та системами

по всьому світу. Вони охоплюють широкий спектр технологій, таких як маршрутизація, передача даних, шифрування та інші аспекти комунікацій. Протоколи, розроблені в рамках ITU-T, гарантують, що пристрої та системи, що використовують різні технології, можуть ефективно взаємодіяти між собою [7].

Протоколи — це формальні правила, які регулюють, як дані передаються та обробляються в мережі. Вони забезпечують узгодженість у зв'язках між мережевими пристроями та дозволяють їм правильно інтерпретувати отримані дані. Основні протоколи, що використовуються в корпоративних мережах, включають:

1. **TCP/IP (Transmission Control Protocol/Internet Protocol)**: Це набір протоколів, що є основою для більшості мереж, включаючи Інтернет. Він складається з двох основних частин: протоколу TCP, який відповідає за надійність передачі даних, і протоколу IP, що забезпечує маршрутизацію пакетів даних між пристроями в мережі. TCP гарантує, що передані дані не будуть втрачені або пошкоджені, шляхом їх розбиття на пакети і контролю їхнього отримання. Протокол IP забезпечує адресацію і направлення пакетів від джерела до призначення. Завдяки цим двом протоколам забезпечується надійна і ефективна комунікація в розподілених мережах [8].

2. **IPSec (Internet Protocol Security)**: Це набір протоколів для забезпечення безпеки передачі даних через IP-мережі. Він використовує методи шифрування та автентифікації, щоб захистити конфіденційність, цілісність і автентичність даних, що передаються. IPSec може працювати на рівні пакета, забезпечуючи безпеку для всієї мережі або для конкретних з’єднань. Це особливо корисно для створення віртуальних приватних мереж (VPN), де дані передаються через публічні канали, але залишаються захищеними від несанкціонованого доступу [9].

3. **PPP (Point-to-Point Protocol)**: Це протокол, який використовується для встановлення прямого з'єднання між двома мережевими вузлами. PPP забезпечує передачу даних через послідовні з'єднання, такі як телефонні лінії, мобільні мережі чи інші канали зв'язку. PPP підтримує функції автентифікації,

шифрування і стиснення, що дозволяє підвищити безпеку і ефективність передачі даних. Цей протокол часто використовується в сценаріях, де потрібно забезпечити з’єднання між віддаленими точками, наприклад, у широкосмугових мережах або при використанні модемів [10].

4. **HTTP/HTTPS (Hypertext Transfer Protocol/Secure)**: Ці протоколи використовуються для передачі даних в Інтернеті. HTTPS, що є захищеною версією HTTP, шифрує дані для захисту конфіденційності під час передачі інформації між браузером і веб-сервером [11].

5. **FTP (File Transfer Protocol)**: Це протокол для передачі файлів між клієнтом і сервером у мережі. Він дозволяє завантажувати або вивантажувати файли, а також переглядати їх структуру на віддаленому сервері. FTP забезпечує швидкий доступ до файлів і можливість їх передачі по мережі. Існують варіанти FTP, які забезпечують безпечну передачу даних, такі як FTPS (FTP Secure) і SFTP (SSH File Transfer Protocol), що використовують шифрування для захисту даних під час передачі.

6. **OSPF (Open Shortest Path First)**: Це протокол внутрішньої маршрутизації, який використовує алгоритм стану ліній для визначення найкращих шляхів передачі даних в IP-мережах. Оскільки OSPF працює на рівні маршрутизаторів, він дозволяє зберігати ефективність маршрутизації в мережах з великою кількістю пристроїв і складною топологією. OSPF також підтримує автоматичне оновлення маршрутів, що дозволяє адаптувати мережу до змін у реальному часі, наприклад, при виході з ладу маршрутизаторів або зміні мережевих з'єднань [12].

7. **DHCP (Dynamic Host Configuration Protocol)**: Це протокол, який автоматично призначає IP-адреси та інші мережеві налаштування (наприклад, маски підмереж, шлюзи за замовчуванням) пристроям у мережі. Це значно спрощує адміністрування мереж, оскільки не потрібно вручну конфігурувати кожен пристрій. DHCP використовується в більшості корпоративних мереж, де кількість підключених пристроїв може бути великою і змінюватися часто.

8. **GRE (Generic Routing Encapsulation)**: Це протокол тунелювання, який дозволяє інкапсулювати пакети одного протоколу всередині іншого для передачі через мережу. Це дає змогу створювати віртуальні тунелі для передавання даних між віддаленими точками, наприклад, між двома офісами корпоративної мережі через Інтернет. GRE часто використовується для підключення віддалених локацій або для створення VPN-мереж. Цей протокол не забезпечує шифрування, тому його часто використовують разом з іншими технологіями для захисту переданих даних.

Дотримання встановлених стандартів і протоколів є необхідною умовою для забезпечення ефективної та безпечної роботи розподіленої корпоративної мережі. Вони допомагають у створенні зручних умов для інтеграції нових технологій і систем, а також забезпечують високий рівень безпеки і захисту даних. В умовах швидкого розвитку технологій і постійних загроз кібербезпеки дотримання стандартів стає ще більш важливим.

Стандарти та протоколи формують основу, на якій будуються розподілені корпоративні мережі. Їх правильне застосування забезпечує сумісність, надійність та безпеку інформаційних систем, що, в свою чергу, впливає на ефективність бізнес-процесів. Розуміння і дотримання цих стандартів є ключовими для успішного функціонування сучасної корпоративної мережі.

1.4 Топологія розподілених корпоративних мереж

Топологія розподіленої корпоративної мережі визначає фізичну і логічну організацію її елементів, а також спосіб, яким пристрої з'єднані один з одним. Правильний вибір топології впливає на продуктивність, надійність та безпеку мережі, а також на її здатність до масштабування. Залежно від специфіки бізнес-процесів і технологічних вимог, організації можуть вибирати різні типи топологій, кожна з яких має свої переваги і недоліки [13].

Існує кілька основних типів топологій, які використовуються в розподілених корпоративних мережах:

1. **Топологія зірка**: Топологія "зірка" передбачає, що всі пристрої в мережі підключаються до центрального вузла, яким може бути комутатор або маршрутизатор (Рисунок 1.6). Уся передача даних здійснюється через цей центральний пристрій, який відповідає за управління трафіком. Основною перевагою є простота в налаштуванні та масштабуванні мережі, а також швидке виявлення несправностей. Однак, залежність від центрального вузла є її головним недоліком, оскільки вихід з ладу цього пристрою паралізує всю мережу. У корпоративних мережах зіркову топологію часто використовують для локальних мереж офісів, де важливі стабільність і простота управління.

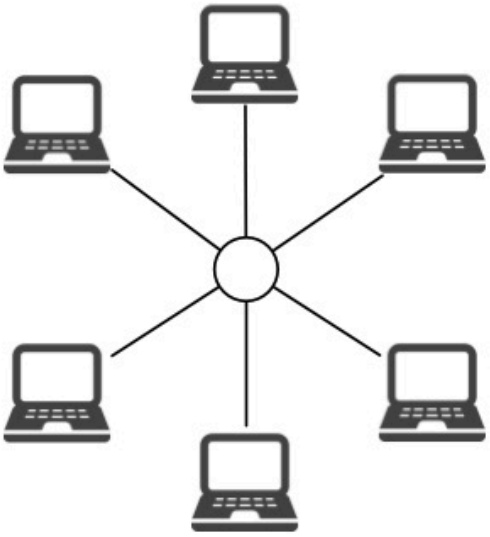


Рисунок 1.6 — Топологія "зірка"

2. **Топологія шина**: Топологія "шина" базується на використанні єдиного кабелю, до якого підключені всі пристрої (Рисунок 1.7). Передача даних здійснюється вздовж кабелю, і кожен пристрій перевіряє, чи адресований йому поточний кадр. Ця топологія вирізняється низькими витратами на кабелі та обладнання, але є надзвичайно вразливою до пошкодження магістралі, що зупиняє

роботу всієї мережі. Хоча її простота була корисною на ранніх етапах розвитку мереж, сучасні корпоративні мережі використовують її рідко через обмежену масштабованість і складність в управлінні трафіком.

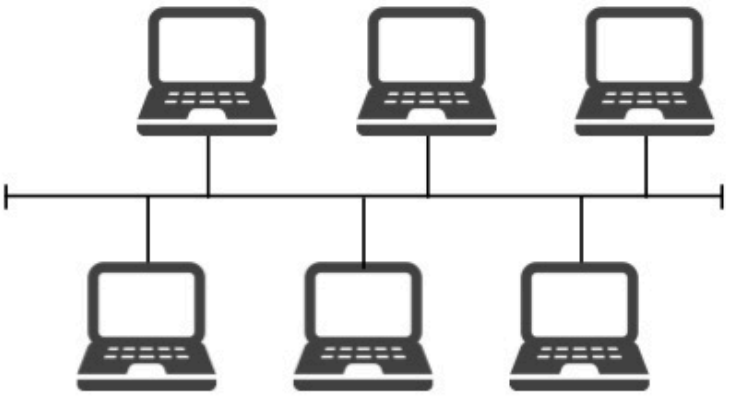


Рисунок 1.7 — Топологія "шина"

3. **Топологія кільце**: У топології "кільце" пристрої підключені в замкнене кільце, де дані передаються від одного вузла до іншого у певному напрямку (Рисунок 1.8). Цей підхід дозволяє забезпечити впорядковану передачу даних та ефективне використання пропускної здатності. Однак, вихід з ладу одного пристрою або кабелю порушує роботу всієї мережі. Топологія "кільце" має обмежене використання в сучасних корпоративних мережах, проте може застосовуватися в системах автоматизації чи спеціалізованих промислових мережах.

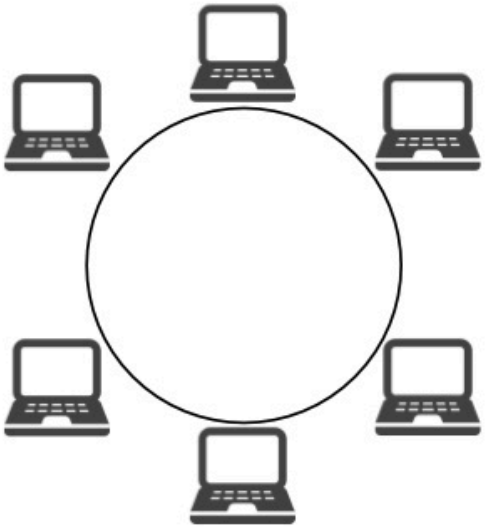


Рисунок 1.8 — Топологія “кільце”

4. **Деревоподібна топологія**: Деревоподібна топологія є ієрархічною структурою, яка поєднує кілька зіркових топологій (Рисунок 1.9). Вона забезпечує організоване підключення пристроїв у підмережах, де є центральний кореневий вузол і підлеглі вузли, які можуть розширюватися далі. Ця топологія добре підходить для масштабування великих мереж, оскільки нові пристрої можна додати без значного впливу на інші сегменти. Основний недолік полягає в залежності від центрального вузла та складності прокладання кабелів. Деревоподібна топологія ідеально підходить для великих корпоративних мереж із чіткою структурою, де важлива масштабованість.

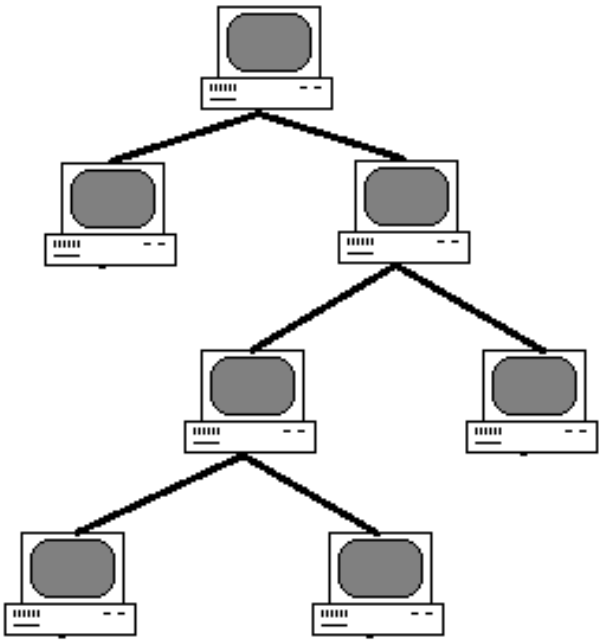


Рисунок 1.9 — Деревоподібна топологія

5. **Гібридна топологія**: Гібридна топологія комбінує елементи кількох різних топологій, таких як "зірка", "кільце" та "шина", для створення мережі, що відповідає потребам організації (Рисунок 1.10). Такий підхід забезпечує високу гнучкість і надійність, оскільки вихід з ладу одного сегмента не впливає на всю мережу. Проте розробка та впровадження гібридної топології потребують значних ресурсів і складного управління. У корпоративних розподілених мережах гібридна топологія є найпоширенішим рішенням, оскільки дозволяє інтегрувати різні сегменти для досягнення балансу між продуктивністю, масштабованістю та надійністю.

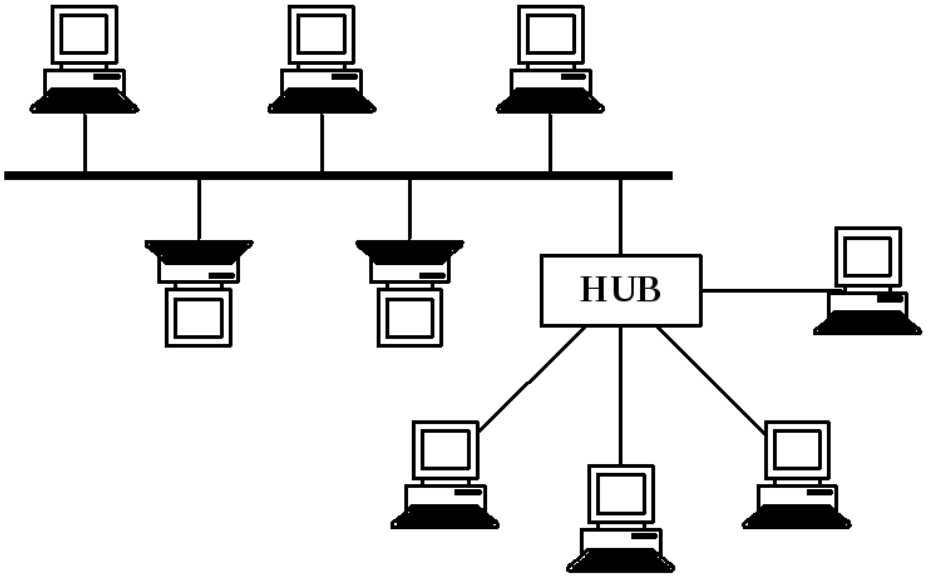


Рисунок 1.10 — Гібридна топологія

Топологія розподіленої корпоративної мережі є важливим аспектом її проєктування. Вибір топології мережі залежить від кількох важливих факторів. Одним з основних є розмір організації: для великих підприємств з численними відділеннями та великою кількістю користувачів найкраще підходять топологія зірка або деревоподібна, оскільки вони забезпечують зручне управління та легкість масштабування. Важливим також є типи даних, що обробляються: для підприємств, які працюють з великими обсягами даних, оптимальним вибором буде топологія, що мінімізує затримки і забезпечує високу пропускну здатність, такі як зірка або мішана. Бюджет також відіграє роль, адже деякі топології, наприклад, шинна, можуть бути дешевшими в реалізації, але потребують ретельного планування для запобігання можливим проблемам при виході з ладу. Крім того, важливим фактором є масштабованість: якщо підприємство планує рости, варто обирати топологію, яка дозволяє легко додавати нові пристрої без значних витрат часу та ресурсів.

2. ПЛАНУВАННЯ РОЗПОДІЛЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Особливості проєктування мультисервісної мережі

Мультисервісна мережа (МСМ) – це інфраструктура, здатна обслуговувати різні типи трафіку: дані, голос, відео і сигнальний (керуючий) трафік. Це рішення дозволяє підтримувати широке різноманіття послуг на єдиній платформі, що важливо для сучасних організацій, яким необхідно інтегрувати комунікації, обмін інформацією, управління процесами та інші бізнес-функції. МСМ створює можливості для зниження витрат на підтримку інфраструктури, підвищення гнучкості і забезпечення масштабованості для бізнесів та провайдерів послуг. У цьому розділі розглянемо ключові особливості мультисервісних мереж, їхні переваги, виклики впровадження та майбутні тенденції.

Мультисервісні мережі забезпечують передачу різнорідного трафіку завдяки використанню декількох мережевих технологій і протоколів, серед яких основними є IP/MPLS, Ethernet, ATM та Frame Relay. Основними принципами МСМ є:

1. Підтримка різних типів трафіку. Основною особливістю є можливість одночасної підтримки голосового, відео- та інформаційного трафіку, що вимагають різних стандартів і характеристик. Наприклад, для голосового трафіку важливі мінімальні затримки, а для відео — висока пропускна здатність.

2. Якість обслуговування (QoS). Якість обслуговування є ключовим аспектом у мультисервісних мережах. Мережа повинна гарантувати певний рівень надійності та продуктивності для кожного типу трафіку. Наприклад, голосові та відео-з’єднання вимагають низької затримки та мінімальної втрати пакетів, а для передавання даних (зокрема, файлів) затримка не є настільки критичною.

3. Маршрутизація та пріоритезація трафіку. Завдяки застосуванню протоколів маршрутизації і механізмів пріоритезації мультисервісні мережі

можуть спрямовувати трафік таким чином, щоб важливі дані отримували необхідні ресурси для надійної передачі.

4. Безпека. МСМ, обслуговуючи різні типи трафіку, повинні мати надійні механізми безпеки, щоб захищати чутливі дані. Це досягається шляхом використання засобів шифрування, аутентифікації та моніторингу мережевого трафіку.

5. Гнучкість і масштабованість. Мультисервісні мережі мають бути легко адаптованими до змін у кількості підключень, трафіку та вимог користувачів. Це досягається завдяки використанню гнучкої архітектури, яка підтримує розширення мережевих ресурсів без значних перебудов.

Мультисервісні мережі мають низку важливих переваг, які роблять їх ефективними і привабливими для сучасних організацій. Вони дозволяють об'єднати різні типи трафіку в єдиній мережевій інфраструктурі, що не лише знижує витрати на її підтримку, але й підвищує гнучкість та масштабованість. Такі мережі здатні забезпечити високу якість обслуговування, що критично важливо для голосових і відео-комунікацій. Ось деякі з основних переваг, що надають мультисервісні мережі:

1. Зменшення витрат на інфраструктуру. Об’єднання різних видів трафіку в одній мережі дозволяє значно знизити вартість створення та обслуговування інфраструктури. Відсутність необхідності утримувати окремі мережі для голосу, відео та даних допомагає зекономити як на обладнанні, так і на управлінні.

2. Поліпшення якості обслуговування. МСМ дозволяє забезпечити високий рівень якості обслуговування для критично важливих типів трафіку, таких як голос та відео, завдяки застосуванню технологій QoS. Це дає змогу надавати послуги з мінімальною затримкою і втратою даних, що покращує загальний користувацький досвід.

3. Підвищення продуктивності. Оскільки мультисервісні мережі є централізованими, то процеси маршрутизації та обробки даних стають більш

ефективними. Це дозволяє прискорити передачу даних і покращити загальну продуктивність мережі.

4. Спрощене управління та контроль. Замість управління кількома окремими мережами, адміністратори мають доступ до централізованого управління, яке полегшує моніторинг і налаштування мережі. Це дозволяє ефективніше виявляти та усувати проблеми, а також знижує навантаження на IT-персонал.

5. Масштабованість і гнучкість. МСМ легко адаптуються до змін у кількості користувачів та трафіку. Мережа може бути масштабована за рахунок додавання нових вузлів та підвищення пропускної здатності, що дозволяє підлаштовувати її під зростання бізнесу або збільшення навантаження.

6. Конвергенція послуг. Однією з головних переваг МСМ є можливість об’єднання різних видів послуг в одну мережу. Це дозволяє надавати комплексні послуги, такі як уніфіковані комунікації, інтеграція відеоконференцій, голосових дзвінків та обміну файлами на єдиній платформі.

Впровадження мультисервісної мережі також стикається з рядом викликів, які можуть ускладнити процес її інтеграції та експлуатації. Компанії повинні враховувати не лише технічні, але й організаційні аспекти, щоб забезпечити безперебійну роботу мережі. До того ж, налаштування та управління такою мережею потребує висококваліфікованих фахівців, а також може вимагати значних фінансових витрат на інфраструктуру та модернізацію. Ось деякі з основних викликів, з якими стикаються організації при впровадженні мультисервісних мереж:

1. Складність конфігурації. Інтеграція різних видів трафіку потребує високої кваліфікації IT-персоналу, оскільки потрібно налаштовувати QoS, маршрутизацію та безпеку для кожного типу трафіку.

2. Забезпечення якості обслуговування. Незважаючи на вбудовані механізми QoS, балансування якості обслуговування для різних видів трафіку може бути складним завданням, особливо під час високих навантажень. Неправильно налаштована QoS може призвести до затримок або втрати даних.

3. Безпека. Високий рівень інтеграції різних видів трафіку в одній мережі означає, що компрометація одного виду трафіку може вплинути на всю систему. Потрібне комплексне забезпечення безпеки, що може ускладнювати керування мережею.

4. Масштабованість при зростанні трафіку. Збільшення трафіку, зокрема через підвищення використання відеоконтенту та IoT, може викликати проблеми з масштабованістю. Мережа повинна бути здатна швидко адаптуватися до змін у навантаженні, що потребує модернізації обладнання та використання більш складних алгоритмів маршрутизації.

5. Вартість впровадження. Незважаючи на потенційну економію, початкові витрати на створення мультисервісної мережі можуть бути значними. Потрібно закупити сучасне обладнання, налаштувати протоколи та провести навчання персоналу, що може призвести до значних витрат на першому етапі.

Основні технології, що забезпечують роботу мультисервісних мереж, грають ключову роль у їх ефективності та здатності обробляти різноманітний трафік. Вони включають різноманітні протоколи та інфраструктурні рішення, що дозволяють оптимізувати маршрутизацію, забезпечувати якість обслуговування та інтегрувати різні види даних. Завдяки цим технологіям, мережі можуть одночасно підтримувати голос, відео та інші сервіси, гарантуючи їх стабільну і надійну роботу. Ось деякі з ключових технологій, що забезпечують ефективність мультисервісних мереж:

1. IP/MPLS (Multi-Protocol Label Switching). Це технологія, що дозволяє прискорити маршрутизацію, зменшуючи затримки при передачі пакетів і забезпечуючи якість обслуговування. MPLS маркує пакети, що дозволяє їм швидше проходити через мережу.

2. Ethernet. Ethernet залишається основною технологією для локальних мереж і забезпечує простоту інтеграції та високу пропускну здатність.

3. Технології забезпечення QoS. Протоколи, що забезпечують якість обслуговування, як-от DiffServ, RSVP, дозволяють налаштовувати параметри мережі для різних видів трафіку, забезпечуючи їхню стабільну роботу.

4. Системи безпеки (Firewall, VPN, IDS/IPS). Щоб захистити різні типи трафіку в одній мережі, використовуються різні технології безпеки, що забезпечують аутентифікацію користувачів, шифрування даних і моніторинг трафіку [14].

Мультисервісні мережі широко використовуються у корпоративних середовищах, державних установах і провайдерах зв’язку. Наприклад:

- Корпорації використовують мультисервісні мережі для об'єднання офісів і забезпечення уніфікованих комунікацій (голосових дзвінків, відеоконференцій і передачі даних).
- Освітні заклади застосовують МСМ для створення цифрових освітніх платформ, що об'єднують доступ до навчальних матеріалів, відеоуроків і інтерактивних занять.
- Медичні установи впроваджують мультисервісні мережі для обміну медичними даними, проведення телеконсультацій і моніторингу пацієнтів в реальному часі.

З поширенням хмарних технологій, IoT і зростанням попиту на високоякісні мультимедійні послуги майбутнє мультисервісних мереж виглядає перспективно. Тенденції включають:

1. Інтеграція з хмарними платформами. МСМ все частіше будуть інтегруватися з хмарними сервісами для забезпечення масштабованих рішень, доступних з будь-якої точки світу.
2. Розвиток SD-WAN (Software-Defined WAN). Ця технологія дозволяє гнучко налаштовувати МСМ для оптимізації передачі трафіку, зокрема в умовах глобальної мережі.
3. Покращення алгоритмів маршрутизації. Нові алгоритми, що забезпечують балансування навантаження і кращу маршрутизацію, допоможуть забезпечувати якість обслуговування навіть в умовах високого трафіку.
4. Інтеграція IoT. З поширенням інтернету речей мультисервісні мережі повинні будуть адаптуватися для підтримки різних видів підключених пристроїв та обробки великих обсягів даних, що поступають від них.

Мультисервісні мережі є невід'ємною частиною сучасної комунікаційної інфраструктури, яка дозволяє інтегрувати різні типи трафіку, такі як голос, відео та дані, в єдину мережу. Це надає організаціям значні переваги, включаючи зниження витрат на підтримку та обслуговування окремих мереж для кожного виду трафіку. Замість того, щоб використовувати кілька різних платформ для різних типів послуг, підприємства можуть централізувати свою мережеву інфраструктуру, що істотно спрощує керування та обслуговування.

Завдяки мультисервісним мережам стає можливим забезпечити високу якість послуг, оскільки ці мережі підтримують механізми управління трафіком, зокрема за допомогою технологій Quality of Service, які дозволяють забезпечувати пріоритетність важливих даних, таких як голосові дзвінки або відеоконференції. Це дозволяє гарантовано знижувати затримки та втрати даних, що критично для таких послуг, як реальний час передачі голосу чи відео. Окрім того, завдяки впровадженню механізмів моніторингу та оптимізації трафіку, забезпечується стабільність роботи навіть при високих навантаженнях.

Також мультисервісні мережі надають високий рівень гнучкості та масштабованості. Вони можуть адаптуватися до змін в обсягах трафіку та потребах бізнесу, що дозволяє організаціям швидко реагувати на нові вимоги. Це забезпечує зростаючу ефективність, оскільки мережа може бути масштабована для підтримки додаткових користувачів або нових технологій без значних витрат на перепланування інфраструктури. Крім того, мультисервісні мережі дозволяють інтегрувати різні види послуг в єдину платформу, що спрощує управління та знижує витрати на підтримку різноманітних систем.

Отже, мультисервісні мережі є важливим елементом для підприємств і організацій, що прагнуть до оптимізації витрат, підвищення продуктивності та забезпечення стабільної, високоякісної комунікації. Вони створюють потужну, адаптивну та безпечну основу для розвитку інфраструктури у сучасному світі комунікацій, забезпечуючи не лише ефективність, але й здатність до швидкої адаптації в умовах швидко змінюваних технологічних вимог.

2.2 Характеристика обладнання мультисервісної мережі

Мультисервісні мережі стали невід'ємною частиною сучасної корпоративної інфраструктури, оскільки вони дозволяють інтегрувати різноманітні сервіси та технології, такі як передача даних, голосу, відео та мультимедійних файлів. Такі мережі об'єднують різні типи трафіку, що надходять від користувачів, пристроїв та додатків, що функціонують у бізнес-середовищах. Їх проектування та впровадження потребують використання спеціалізованого обладнання, яке має забезпечити високу швидкість, надійність, безпеку та масштабованість.

Основними елементами мультисервісної мережі є маршрутизатори, комутатори, брандмауери (фаєрволи), системи захисту від загроз і телекомунікаційні сервери. Кожен із цих компонентів відіграє критичну роль у функціонуванні мережі, забезпечуючи її ефективність, надійність і безпеку. У цьому контексті важливо розглядати не тільки базові функції кожного елементу, але й специфічні характеристики та можливості, які ці компоненти надають для розв'язання конкретних завдань у корпоративних мережах. Для досягнення оптимальної ефективності, ці елементи повинні працювати в тісній взаємодії, забезпечуючи комплексний захист і стабільну передачу даних при високих навантаженнях.

Мультисервісні мережі повинні бути здатні до інтеграції різних технологій, а також забезпечувати надійний захист від потенційних кіберзагроз. Вибір правильного обладнання та його налаштування мають прямий вплив на ефективність роботи та безпеку таких мереж. У цьому розділі ми детально розглянемо обладнання, яке використовується в корпоративних мультисервісних мережах, а також його роль у загальній архітектурі.

2.2.1 Маршрутизатори

Маршрутизатори є важливими пристроями, які забезпечують передачу даних між різними сегментами мережі та підмережами (Рисунок 2.1). Вони працюють на третьому рівні моделі OSI — рівні мережі, та відповідають за маршрутизацію IP-пакетів, що дозволяє вибрати оптимальний шлях для передачі даних від джерела до отримувача. Завдяки маршрутизаторам забезпечується стабільна робота мережі, а також налаштовується з'єднання між локальними мережами та глобальними мережами, включаючи Інтернет.

У корпоративних мультисервісних мережах маршрутизатори мають особливе значення, оскільки вони не тільки забезпечують управління трафіком, але й виконують роль фільтрації та безпеки, вибираючи найкращі маршрути для передачі даних. Вони можуть також підтримувати протоколи для реалізації VPN, що дозволяє забезпечити захищений доступ до корпоративної мережі через Інтернет або інші глобальні мережі.

Маршрутизатори класифікуються за сферами застосування на кілька основних класів.

Магістральні маршрутизатори (backbone routers) призначені для побудови центральної мережі корпорацій, що об'єднує численні локальні мережі, розташовані в різних будівлях і побудовані на основі різних технологій. Ці маршрутизатори є найпотужнішими пристроями, здатними обробляти сотні тисяч або навіть мільйони пакетів на секунду, маючи велику кількість інтерфейсів для локальних і глобальних мереж. Вони підтримують як середньошвидкісні інтерфейси, так і високошвидкісні, такі як ATM і SDH зі швидкістю до 622 Мбіт/с і більше. Конструктивно магістральні маршрутизатори зазвичай виконані у вигляді модульної системи на базі шасі з великою кількістю слотів, що забезпечує надійність і відмовостійкість завдяки системам терморегуляції, резервним джерелам живлення і підтримці гарячої заміни модулів [15].

Маршрутизатори віддалених офісів з'єднують одну локальну мережу віддаленого офісу з центральною мережею або мережею регіонального відділення через глобальні канали зв’язку. Ці маршрутизатори можуть підтримувати резервний зв'язок за допомогою комутованої телефонної лінії. Різноманітність моделей таких пристроїв пояснюється їхньою спеціалізацією та орієнтацією на підтримку певного типу глобального зв’язку.

Маршрутизатори локальних мереж (комутатори 3-го рівня) виконують функцію поділу великих локальних мереж на підмережі, забезпечуючи високу швидкість маршрутизації. У таких маршрутизаторах усі порти працюють зі швидкістю не менше 10 Мбіт/с, багато з них підтримують швидкість 100 Мбіт/с або навіть більше. Основна вимога до цих пристроїв – висока продуктивність для оптимального функціонування всередині локальних мереж без використання низькошвидкісних інтерфейсів.

Маршрутизатори використовують різні протоколи маршрутизації для забезпечення ефективної передачі даних між мережами. Кожен протокол має свої особливості, які дозволяють адаптувати маршрутизацію до конкретних умов мережі. Вибір протоколу залежить від розміру мережі, її складності та вимог до швидкості та надійності обміну даними. Розглянемо три основних протоколи маршрутизації, які часто використовуються в корпоративних мережах:

- RIP (Routing Information Protocol) – один із найбільш поширених протоколів маршрутизації для невеликих комп’ютерних мереж, який дозволяє маршрутизаторам автоматично оновлювати інформацію про маршрути, отримуючи дані про напрямки і відстані в хопах (процес передачі мережевого пакету між вузлами) від своїх сусідів.
- OSPF (Open Shortest Path First) – протокол динамічної маршрутизації, що базується на технології відстеження стану каналу (link-state), і використовує алгоритм Дейкстри для визначення найкоротших шляхів у мережі.
- BGP (Border Gateway Protocol) – протокол маршрутизації, який застосовується для обміну трафіком між різними мережами в Інтернеті. Це протокол з вектором шляхів, що дозволяє мережам підключатися і обмінюватися

інформацією про доступність шляхів. BGP вибирає найкращий маршрут для трафіку, орієнтуючись на політики, налаштовані адміністраторами мереж.

У корпоративних мережах забезпечення високої доступності та надійності мережевої інфраструктури є критичним фактором для безперебійної роботи бізнес-процесів. Збої в мережі можуть призвести до значних фінансових втрат, втрати даних або навіть до порушення діяльності організації. Тому важливо, щоб мережа була максимально стійкою до непередбачених ситуацій, таких як апаратні відмови або проблеми з підключенням. Для досягнення цієї мети маршрутизатори застосовують різні технології, що дозволяють забезпечити безперервну роботу навіть у разі відмови одного з елементів мережі. Такі технології, як High Availability (HA) та VRRP (Virtual Router Redundancy Protocol), сприяють створенню резервних маршрутів і забезпечують автоматичне переключення на альтернативні шляхи або пристрої в разі збою, мінімізуючи час простою мережі.

Таким чином, маршрутизатори є одними з ключових елементів корпоративної інфраструктури, що забезпечують ефективну передачу даних між сегментами мережі, її безпеку, надійність і масштабованість. Правильне налаштування та використання маршрутизаторів дозволяє створити потужну і стабільну мережеву інфраструктуру, яка відповідає вимогам організації.

Рисунок 2.1 — Маршрутизатор Cisco RV345-K9-G5

2.2.2 Комутатори

Комутатори — це ключові пристрої для побудови корпоративних мереж (Рисунок 2.2), які забезпечують з'єднання між кінцевими пристроями (комп'ютери, сервери, принтери) і здійснюють передачу даних на рівні каналу передачі даних (Layer 2). Вони працюють на основі MAC-адрес і передають Ethernet-кадри між пристроями, визначаючи, куди направити дані залежно від адреси отримувача. Основною функцією комутатора є оптимізація трафіку всередині мережі, зменшуючи його розмір і підвищуючи ефективність передачі даних.

Комутатори поділяються на керовані та некеровані. Некеровані комутатори — це базові пристрої, які виконують лише основну функцію з'єднання пристроїв у мережі. Вони автоматично визначають, де передавати дані, на основі MAC-адрес, але не дозволяють налаштовувати додаткові функції або здійснювати управління трафіком. Ці комутатори зазвичай використовуються в малих або простих мережах, де немає потреби в складному керуванні мережею.

Керовані комутатори надають більше можливостей для управління та налаштування. Вони дозволяють адміністраторам мережі конфігурувати різні параметри, наприклад, створювати VLAN для розділення трафіку, налаштовувати пріоритети даних через QoS (Quality of Service) або застосовувати функції безпеки для обмеження доступу. Такі комутатори можуть працювати на Layer 2 (L2) для передачі даних на основі MAC-адрес або на Layer 3 (L3), що дає можливість маршрутизації за IP-адресами та підтримки маршрутизації між різними підмережами.

Важливим аспектом є те, що сучасні комутатори виконують не тільки функцію з'єднання пристроїв, але й надають ряд додаткових можливостей. Розглянемо функції, які часто використовуються в корпоративних мережах.

- PoE (Power over Ethernet): Функція, яка дозволяє комутатору передавати електричну енергію до підключених пристроїв, таких як IP-камери,

точки доступу Wi-Fi або IP-телефони, через Ethernet-кабелі. Це знижує потребу в додаткових джерелах живлення та спрощує встановлення мережевих пристроїв.

- Quality of Service (QoS): Ця функція дозволяє пріоритизувати трафік у мережі, що критично важливо для передачі голосових або відео-даних, щоб уникнути затримок і втрат при високому навантаженні на мережу. QoS гарантує, що важливі додатки, такі як відеоконференції або VoIP, отримують необхідну пропускну здатність і мають найвищий пріоритет.
- Link Aggregation: Технологія об'єднання кількох фізичних ліній зв'язку в одну логічну з більшою пропускною здатністю. Це дозволяє зменшити навантаження на окремі порти комутаторів і збільшити швидкість передачі даних між пристроями мережі.

Комутатори є основними елементами мережевої інфраструктури в корпоративних мережах. Вони забезпечують ефективну передачу даних між пристроями, знижуючи навантаження на мережу і підвищуючи її продуктивність. Різні типи комутаторів, такі як L2 та L3, дозволяють задовольнити вимоги як простих локальних мереж, так і складних корпоративних систем. Завдяки підтримці додаткових функцій, таких як PoE, QoS, VLAN та інших, комутатори можуть значно покращити ефективність і безпеку мережі, що робить їх незамінними в побудові надійних і масштабованих інфраструктур.

Рисунок 2.2 — Коммутатор Cisco WS-C2960RX-24TS-L

2.2.3 Міжмережевий екран

Міжмережевий екран — це система, яка контролює і фільтрує мережевий трафік на основі заданих правил безпеки. Він виконує роль бар’єра між внутрішньою мережею організації та зовнішнім середовищем, таким як Інтернет, і захищає мережу від кібератак, несанкціонованого доступу та інших загроз (Рисунок 2.3).

Для забезпечення потреб різних користувачів існує три основні типи фаєрволів: мережного рівня, прикладного рівня та рівня з'єднання. Кожен із них застосовує власний підхід до захисту мережі.

Фаєрволи мережного рівня, часто представлені екрануючими маршрутизаторами, контролюють службову інформацію пакетів лише на мережевому і транспортному рівнях моделі OSI. Їхнім недоліком є відсутність контролю даних на інших рівнях, а також недостатні механізми аудиту й сповіщення про загрози, що може залишати адміністраторів не проінформованими про атаки.

Фаєрволи прикладного рівня, також відомі як проксі-сервери, забезпечують високий рівень безпеки, оскільки створюють фізичний поділ між локальною мережею та Інтернетом. Однак їхня робота вимагає аналізу трафіку і ухвалення рішень про доступ, що може знижувати продуктивність мережі.

Фаєрволи рівня з'єднання, подібно до прикладних фаєрволів, працюють як сервери-посередники. Основна їхня перевага в універсальності: вони обслуговують широкий спектр протоколів без потреби в спеціалізованому програмному забезпеченні для кожної мережевої служби [16].

Окрім базового функціоналу, сучасні міжмережеві екрани мають розширені можливості:

- Віртуальні приватні мережі (VPN): забезпечують захищені канали зв’язку для віддалених користувачів або офісів.

- Фільтрація контенту: блокує доступ до небажаних вебсайтів або додатків.
- Виявлення і запобігання вторгнень (IDS/IPS): аналізують мережеву активність для виявлення та запобігання аномаліям.
- Пріоритезація трафіку (QoS): оптимізують розподіл ресурсів, забезпечуючи високу якість роботи для критично важливих сервісів.

Міжмережеві екрани є ключовими елементами безпеки в корпоративних мережах. Вони забезпечують першу лінію оборони від зовнішніх загроз, дозволяють мінімізувати ризик атак і забезпечують збереження конфіденційної інформації. Крім того, вони допомагають компаніям відповідати стандартам безпеки, таким як ISO/IEC 27001, PCI DSS та інші.

Міжмережеві екрани відіграють важливу роль у забезпеченні безпеки корпоративних мереж. Їхнє впровадження дозволяє не лише захистити організацію від кібератак, але й забезпечити стабільну роботу мережевої інфраструктури. Сучасні міжмережеві екрани, завдяки своїм розширеним функціям, є невід'ємним компонентом захисту у світі, де цифрові загрози постійно зростають

Рисунок 2.3 — Міжмережевий екран Cisco ASA 5506

2.2.4 Телекомунікаційні сервери

Телекомунікаційні сервери — це спеціалізовані сервери, які обробляють голосові, відео- та інші мультимедійні дані в межах корпоративних мереж (Рисунок 2.4). Вони забезпечують передачу даних для різноманітних мультимедійних додатків і є основними елементами для реалізації сервісів VoIP (Voice over IP), відеоконференцій, а також для передачі інших мультимедійних файлів. Телекомунікаційні сервери можуть бути як окремими фізичними пристроями, так і віртуальними сервісами, що працюють на загальних серверних платформах.

Телекомунікаційні сервери можуть підтримувати різні протоколи та стандарти, які використовуються для забезпечення ефективної передачі та обробки мультимедійних даних. Ось деякі з найпоширеніших протоколів:

- SIP (Session Initiation Protocol): використовується для встановлення, зміни та завершення сеансів зв'язку, таких як голосові дзвінки або відеоконференції. SIP дозволяє організувати виклик, підтримку сесій і контроль їх стану між користувачами або пристроями.
- RTP (Real-Time Protocol): призначений для передачі голосових і відео даних в реальному часі. RTP є критично важливим для передачі мультимедійного контенту, оскільки він забезпечує низьку затримку та високу швидкість передачі.
- RTCP (Real-Time Control Protocol): протокол, який працює разом з RTP і використовується для моніторингу якості передачі мультимедійних даних. RTCP допомагає контролювати такі параметри, як затримка, втрата пакетів та ширина каналу.
- H.323: протокол для голосового і відеозв'язку, який дозволяє створювати мультимедійні сесії в IP-мережах. Він використовується в корпоративних системах для забезпечення відеоконференцій і VoIP.
- MGCP (Media Gateway Control Protocol): протокол, який використовується для управління шлюзами медіа в телекомунікаційних системах.

Він дозволяє здійснювати передачу голосу через IP-мережі, а також здійснювати інтерфейс між традиційними телефонними мережами і IP-мережами.

Телекомунікаційні сервери є критичними для забезпечення ефективної комунікації в корпоративних мережах, оскільки вони дозволяють забезпечити передачу голосу та відео в режимі реального часу, що є основою для сучасних комунікаційних платформ. Вони дозволяють не лише здійснювати дзвінки та відеоконференції, але й інтегрувати різні служби і сервіси в єдину мережу, що важливо для великих організацій з розгалуженою інфраструктурою.

Завдяки застосуванню таких технологій, як VoIP і відеоконференції, підприємства можуть значно скоротити витрати на телефонний зв'язок і подорожі, а також підвищити ефективність комунікацій між співробітниками, незалежно від їхнього місцезнаходження. Важливо, що сучасні телекомунікаційні сервери можуть бути інтегровані з іншими мережевими пристроями, такими як маршрутизатори, комутатори, фаєрволи, що дозволяє створювати захищену і ефективну мережу для передачі мультимедійних даних.

Телекомунікаційні сервери є важливими компонентами корпоративних мереж, оскільки вони дозволяють організувати ефективну передачу голосових і відео даних у реальному часі. Використання сучасних протоколів, таких як SIP, RTP, H.323 та інших, забезпечує надійність і високоякісну комунікацію між співробітниками організації. Сучасні сервери не тільки підтримують різноманітні мультимедійні формати, але й інтегруються з іншими елементами мережі, створюючи надійну, масштабовану та безпечну інфраструктуру для корпоративних комунікацій.

Рисунок 2.4 — Сервер Cisco R210-BUN-5

2.3 Організація безпеки в корпоративних мережах

У сучасних умовах, коли інформація є важливим активом для будь-якої організації, забезпечення безпеки корпоративних мереж стає одним з найактуальніших завдань. Захист даних, мережевої інфраструктури та інформаційних систем необхідний для підтримки конфіденційності, цілісності та доступності інформації. Особливо важливою є захищеність при передачі даних між різними частинами корпоративної мережі та з зовнішніми користувачами чи іншими організаціями.

Технології безпеки в корпоративних мережах допомагають захистити мережеві ресурси від різноманітних загроз, таких як несанкціонований доступ, кіберзлочинність, витік конфіденційної інформації або атаки типу "відмова в обслуговуванні" (DDoS). Важливу роль у цьому відіграють як фізичні методи захисту, так і програмні технології, серед яких одним з основних є протокол IPSec (Internet Protocol Security), який забезпечує захищену передачу даних через Інтернет [17].

Актуальність питання безпеки корпоративних мереж зростає з кожним роком. З розвитком технологій і збільшенням кількості підключених пристроїв і користувачів мережа стає уразливою для атак. Використання протоколів захисту та методів забезпечення безпеки не є лише вимогою законодавства або внутрішніх політик організації, а необхідністю для збереження її репутації та економічної стабільності.

Такі загрози, як перехоплення даних, атаки на сервери, зловмисне втручання в мережевий трафік або навіть витік персональних даних користувачів, ставлять під загрозу нормальну роботу компаній. У зв'язку з цим вкрай важливим є створення стійкої системи захисту на всіх рівнях інфраструктури [18].

У загальному випадку для забезпечення безпеки в корпоративних мережах використовуються різноманітні методи захисту, зокрема:

1. Фізичний захист — це використання фізичних засобів для захисту серверів, комп'ютерних систем, мережевих пристроїв та інших компонентів інфраструктури. Це можуть бути замки, сейфи, системи відеоспостереження, охорона доступу до серверних кімнат.

2. Мережеве розмежування — це сегментація мережі для обмеження доступу між різними її частинами. Наприклад, використання внутрішніх та зовнішніх підмереж, щоб уникнути несанкціонованого доступу до важливих ресурсів.

3. Аутентифікація — забезпечення ідентифікації користувачів для перевірки їх прав доступу. Це може бути через логіни і паролі, а також використання двофакторної аутентифікації або біометричних даних.

4. Антивірусне програмне забезпечення — використання спеціальних програм для виявлення та ліквідації шкідливого програмного забезпечення, що може потрапити в мережу через заражені файли або вразливості в програмному забезпеченні.

5. Мережеві екрани (файрволи) — програмні або апаратні засоби, що обмежують або контролюють доступ до корпоративної мережі ззовні або

всередині. Вони дозволяють блокувати несанкціоновані підключення та попереджати атаки.

У контексті проектування розподілених корпоративних мереж безпека передавання даних є одним з основних аспектів, на яких слід зосередити увагу. Важливість забезпечення надійного захисту трафіку, що передається між різними частинами мережі або між віддаленими офісами та головним сервером, неможливо переоцінити. Розвиток Інтернету та глобальних корпоративних мереж створює умови для потужних кіберзагроз, які можуть привести до витоку конфіденційної інформації, несанкціонованого доступу або навіть до серйозних фінансових втрат. Одним із найефективніших методів для забезпечення безпеки передачі даних є використання протоколу IPSec (Internet Protocol Security) [19].

IPSec є стандартом, що забезпечує захищену передачу даних на рівні мережі, і це дає можливість ефективно побудувати безпечні з'єднання між різними елементами розподіленої корпоративної мережі, такими як віддалені офіси, філії або користувачі, підключені через Інтернет. Завдяки своїй універсальності та здатності працювати на рівні IP-протоколу, IPSec дозволяє створювати захищені VPN (віртуальні приватні мережі) і захищати дані в складних і великомасштабних корпоративних мережах. Важливість цього протоколу полягає в тому, що він забезпечує захист не лише від внутрішніх загроз, але й від зовнішніх атак, що робить його невід'ємною частиною стратегії кібербезпеки сучасних організацій.

IPSec (Internet Protocol Security) — це набір стандартів, розроблений для забезпечення безпеки на рівні Інтернет-протоколу (IP). Його основне призначення — забезпечити конфіденційність, автентичність і цілісність даних, що передаються через Інтернет або приватні мережі. IPSec застосовує різні криптографічні методи для захисту трафіку та забезпечення захищених з'єднань між двома або більше точками [20].

IPSec підтримує два основні режими роботи — транспортний режим та тунельний режим (Рисунок 2.5). Кожен з цих режимів має свої особливості і використовується залежно від вимог до безпеки і сценаріїв використання в мережі.

Розуміння різниці між ними є важливим для вибору найбільш підходящого методу захисту залежно від конкретних потреб мережі.

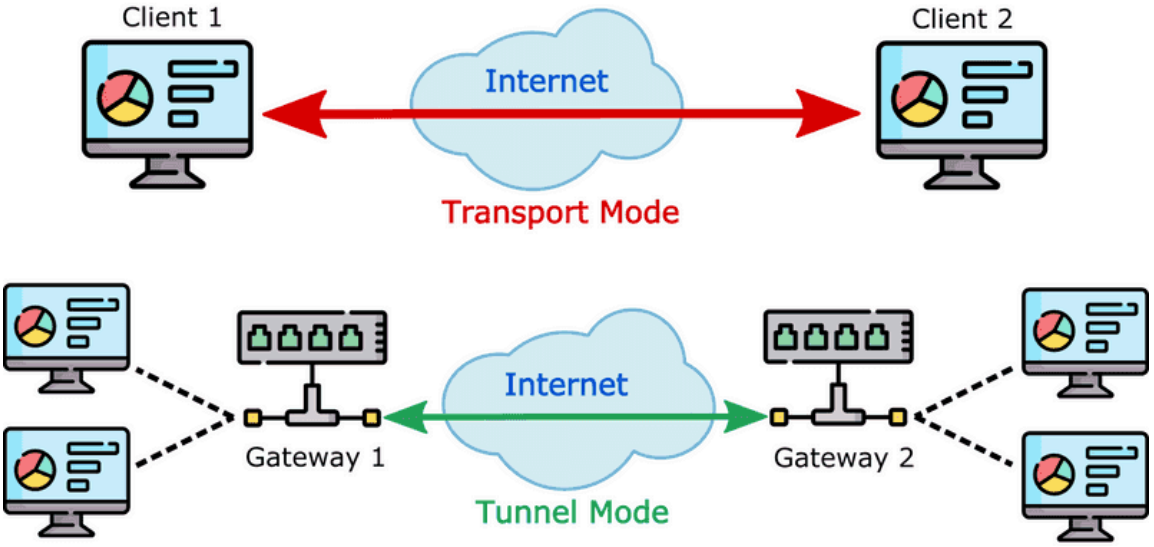


Рисунок 2.5 — Схема режимів роботи IPSec

Транспортний режим в IPSec шифрує тільки дані, що передаються в пакеті, залишаючи IP-заголовки незмінними. Це означає, що лише ті частини пакету, які містять корисне навантаження (payload), будуть захищені, а заголовки IP, які містять інформацію про адреси відправника і отримувача, залишаються відкритими.

Тунельний режим в IPSec шифрує весь IP-пакет, включаючи як заголовки, так і дані. Це дозволяє створювати захищені тунелі для передачі даних між різними мережами через ненадійні канали, такі як Інтернет. В результаті у тунельному режимі весь пакет (як заголовки, так і дані) шифрується і транспортується в новому IP-заголовку, що додається для маршрутизації.

Таблиця 2.1 — Порівняння транспортного та тунельного режимів

Характеристика	Транспортний режим (Transport Mode)	Тунельний режим (Tunnel Mode)
Шифрування	Шифруються тільки дані (корисне навантаження), а заголовки IP залишаються відкритими	Шифрується весь IP-пакет, включаючи як заголовки, так і дані
Тип застосування	Зазвичай використовується для точка-точка з'єднань в межах однієї мережі або між двома кінцевими точками	Використовується для створення VPN-з'єднань між різними мережами або для з'єднання віддалених точок через Інтернет або інші ненадійні канали
Накладні витрати	Нижчі накладні витрати на шифрування, оскільки шифрується тільки корисне навантаження, а заголовки не змінюються	Вищі накладні витрати, оскільки весь пакет шифрується і додається новий заголовок IP для маршрутизації, що збільшує розмір переданих даних
Безпека	Забезпечує конфіденційність та цілісність даних між двома кінцевими точками, але адреси та маршрути залишаються відкритими	Забезпечує більш високий рівень безпеки, оскільки приховує не тільки дані, а й маршрути та адреси. Захищає всю інформацію, що передається через мережу

Маршрут	Адреси відправника і отримувача залишаються відкритими, що дозволяє стороннім користувачам бачити шлях передавання	Весь маршрут і адреси приховуються завдяки додаванню нового заголовка IP, що робить маршрутизацію менш вразливою для атак
Мережі	Зазвичай застосовується в приватних або внутрішніх мережах, де не потрібно приховувати маршрути	Використовується для з'єднань між різними мережами, зокрема через Інтернет, де важливо приховувати дані маршрутизації
Продуктивність	Вищий рівень продуктивності, оскільки накладні витрати менші, а дані не шифруються на рівні маршрутизації	Зниження продуктивності через додаткові накладні витрати на шифрування заголовків та додавання нових заголовків
Простота налаштування	Просте налаштування для точка-точка з'єднань, оскільки шифруються тільки дані, без змін у заголовках маршрутизації	Складніше налаштування через необхідність додавання нового заголовка та шифрування всього пакету, що потребує більше часу для конфігурації
Приклад використання	Захист з'єднання між двома серверами або кінцевими пристроями в межах локальної мережі або внутрішньої VPN	Захищене з'єднання між двома віддаленими офісами через Інтернет або з'єднання віддаленого користувача з корпоративною мережею через VPN

І транспортний, і тунельний режими в IPSec є важливими для забезпечення безпеки в різних сценаріях використання. Транспортний режим є оптимальним для захисту зв'язку між двома точками в межах безпечної мережі, де важливо мінімізувати накладні витрати на шифрування, тоді як тунельний режим забезпечує високий рівень безпеки при захисті з'єднань через відкриті або ненадійні канали, такі як Інтернет. Оскільки тунельний режим шифрує як дані, так і заголовки, він є більш гнучким та ефективним рішенням для побудови корпоративних VPN і захисту міжмережевих з'єднань.

Основні компоненти IPSec — це два протоколи: AH (Authentication Header) та ESP (Encapsulating Security Payload). Ці протоколи дозволяють здійснювати різні рівні захисту залежно від вимог конкретного з'єднання. Важливо розуміти різницю між ними, оскільки кожен з цих протоколів виконує різні функції безпеки.

Протокол AH в IPSec відповідає за аутентифікацію пакета даних і перевірку його цілісності. Він додає в IP-пакет спеціальний заголовок, що містить хеш-код (MAC — Message Authentication Code), який використовується для перевірки того, чи не були дані змінені в процесі передачі.

Таблиця 2.2 – Структура AH-заголовка:

Поле	Розмір (біт)	Опис
Next Header	8	Тип заголовка протоколу, що йде після заголовка AH. Дозволяє приймальному IPSec-модулю визначити захищений протокол верхнього рівня
Payload Length	8	Загальний розмір AH-заголовка в 32-бітових словах мінус 2. Для IPv6 довжина повинна бути кратна 8 байтам.
Reserved	16	Зарезервоване поле, заповнюється нулями.
Security Parameters Index	32	Індекс параметрів безпеки. Разом із IP-адресою одержувача та протоколом безпеки

		однозначно визначає захищене з’єднання (SA). Значення 1–255 зарезервовані IANA.
Sequence Number	32	Послідовний номер для захисту від повторної передачі. Завжди зростає, використовується передавальним IPSec-модулем. Одержувач може обробляти чи ігнорувати це поле.
Integrity Check Value	Змінна	Контрольна сума для перевірки цілісності. Для IPv6 повинна бути кратна 8 байтам, а для IPv4 — 4 байтам.

Основні характеристики AH:

1. Аутентифікація: Протокол AH гарантує, що пакети даних надійшли від автентифікованого відправника і не були змінені в процесі передачі.

2. Цілісність: AH використовує хеш-функцію для створення контрольної суми, яка прикріплюється до пакету і дає змогу перевірити, чи не були змінені дані.

3. Без шифрування: AH не здійснює шифрування даних, тому він не забезпечує конфіденційність переданих даних, а лише їх цілісність і автентичність.

Протокол AH працює в транспортному і тунельному режимах IPSec (Рисунок 2.6), але в тунельному режимі AH може бути обмежений, оскільки деякі частини заголовка IP можуть змінюватися в процесі шифрування.

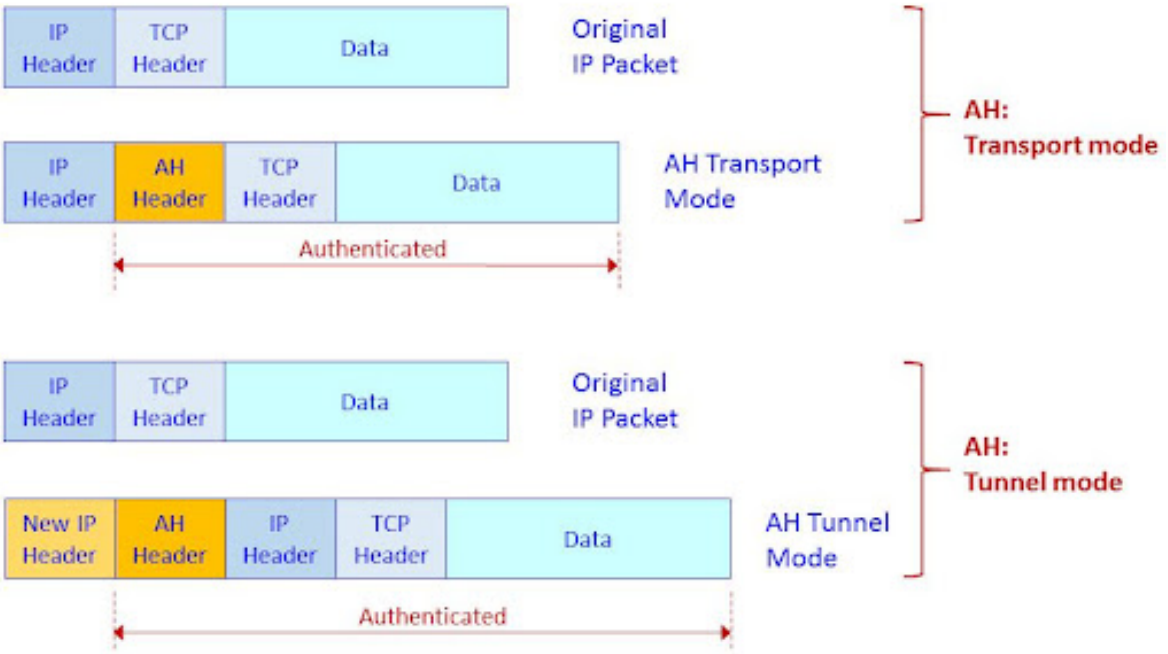


Рисунок 2.6 — Режими роботи протоколу Authentication Header в IPSec

Протокол ESP забезпечує не тільки автентичність і цілісність даних, як AH, але й шифрування самих даних, що дозволяє забезпечити конфіденційність переданої інформації. Це робить ESP більш потужним і універсальним інструментом для забезпечення безпеки в мережах.

Таблиця 2.2 – Структура ESP-заголовка:

Поле	Розмір (біт)	Опис
Security Parameters Index	32	Індекс параметрів безпеки. Разом із IP-адресою одержувача та ESP-протоколом визначає захищене з'єднання (SA). Значення 1–255 зарезервовані IANA для майбутнього використання.
Sequence Number	32	Послідовний номер для захисту від повторної передачі. Завжди присутній у пакеті ESP.
Payload Data	Змінна	Дані відповідно до типу, зазначеного в полі «Next Header». Може містити дані для синхронізації криптопроцесів (наприклад, вектор ініціалізації).
Padding	Змінна	Доповнення, необхідне для забезпечення кратності відкритого тексту певному числу байтів, залежно від алгоритму (наприклад, розмір блоку блочного шифру).
Pad Length	8	Довжина доповнення в байтах.
Next Header	8	Тип даних, що містяться у полі «Payload Data»
Integrity Check Value	Змінна	Контрольна сума для перевірки цілісності. Для IPv6 повинна бути кратна 8 байтам, а для IPv4 — 4 байтам.

Основні характеристики ESP:

1. Шифрування: ESP забезпечує шифрування даних, що дозволяє захистити їх від перехоплення. В результаті навіть якщо зловмисник отримає доступ до даних, він не зможе їх прочитати без відповідного ключа дешифрування.

2. Аутентифікація: ESP також включає в себе механізм аутентифікації, який дозволяє перевірити, що дані надійшли від авторизованого відправника.

3. Цілісність: Як і AH, ESP гарантує, що передані дані не були змінені під час транспортування.

ESP працює як в транспортному, так і в тунельному режимах (Рисунок 2.7). Однак, у разі тунельного режиму, ESP забезпечує не тільки шифрування і аутентифікацію даних, але й захист всього IP-пакету, що робить його ідеальним для створення VPN-з'єднань.

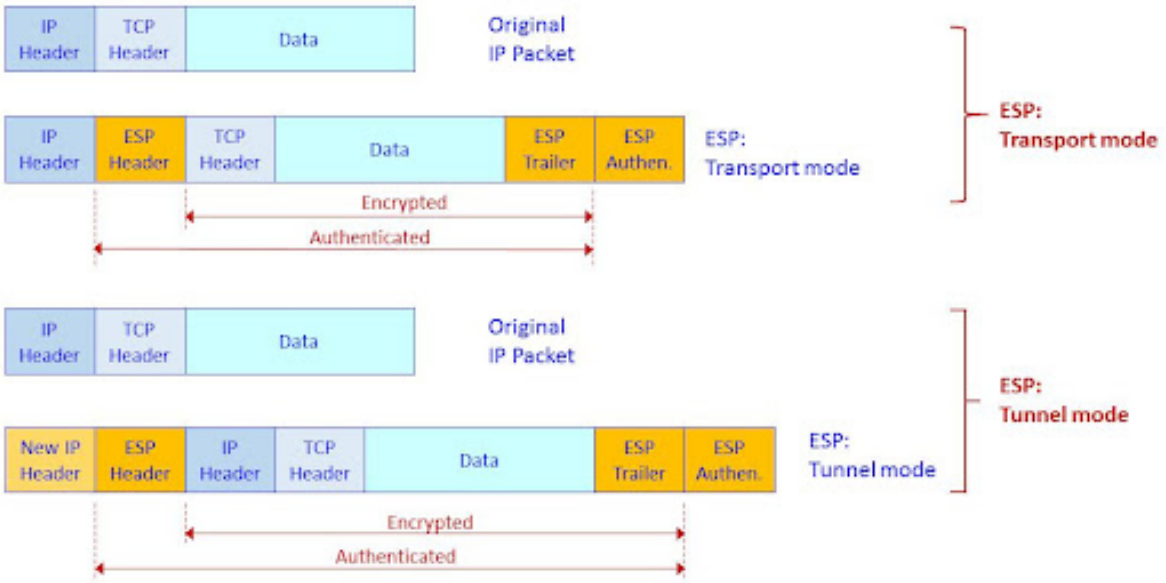


Рисунок 2.7 — Режими роботи протоколу Encapsulating Security Payload в IPSec

Механізм роботи IPSec базується на ряді криптографічних і аутентифікаційних процедур, що включають створення безпечного з'єднання між двома точками і захист даних, що передаються між ними. Ось як виглядає цей процес:

1. Ініціалізація безпечного з'єднання

Першим етапом роботи IPSec є ініціалізація з'єднання між двома пристроями або вузлами, що хочуть обмінюватися зашифрованими даними. Це здійснюється через використання протоколу IKE (Internet Key Exchange), який відповідає за встановлення безпечних параметрів з'єднання, таких як шифрувальні алгоритми та ключі.

Процес ініціалізації складається з двох основних етапів:

Етап 1 — Аутентифікація та обмін криптографічними параметрами: Під час цього етапу обидві сторони обмінюються своїми публічними ключами або сертифікатами для перевірки автентичності. Вони також домовляються про криптографічні алгоритми, які будуть використовуватися для шифрування та хешування даних (наприклад, AES для шифрування та SHA-256 для хешування).

Етап 2 — Генерація ключів для шифрування та аутентифікації: Ключі для шифрування даних генеруються за допомогою алгоритмів обміну ключами (наприклад, Diffie-Hellman), що дозволяє створити спільний секретний ключ для двох сторін, навіть якщо вони обмінюються лише публічними ключами.

2. Аутентифікація

На другому етапі встановленого з'єднання використовується метод аутентифікації, який гарантує, що обидві сторони дійсно є тим, за кого себе видають. Для цього використовуються різні методи:

Цифрові сертифікати: Сертифікати, видані авторитетними центрами сертифікації, підтверджують, що пристрій або користувач, який хоче підключитися до мережі, є автентичним і належить до конкретної організації.

Секретні ключі: В разі використання передавальних з'єднань, автентифікація може відбуватися через попередньо обміняні секретні ключі або використання паролів.

3. Шифрування та захист даних

Після того як з'єднання встановлено і аутентифікація пройшла успішно, переходять до процесу шифрування даних. Для цього використовуються криптографічні алгоритми, наприклад, AES (Advanced Encryption Standard) або 3DES (Triple DES). Пакет, що передається, шифрується за допомогою вибраного алгоритму, і лише обидві сторони, що мають правильний ключ, можуть розшифрувати його.

4. Передача та перевірка цілісності

Щоб переконатися, що дані не були змінені або пошкоджені під час передачі, IPSec використовує методи перевірки цілісності. Це досягається за допомогою механізмів хешування, таких як HMAC (Hashed Message Authentication Code). Кожен переданий пакет супроводжується спеціальним хешем, який обидві сторони використовують для перевірки, чи був пакет змінений.

5. Завершення сеансу

Після завершення передачі даних сеанс з'єднання може бути закритий, і обидві сторони видаляють тимчасові ключі, що були використані для шифрування та аутентифікації, щоб запобігти їх подальшому використанню. Якщо необхідно продовжити передавання даних, процедура ініціалізації знову запускається.

IPSec є комплексним і потужним протоколом для забезпечення безпеки даних на мережевому рівні. Завдяки своїм можливостям шифрування, аутентифікації та перевірки цілісності, IPSec є важливим інструментом для створення захищених VPN-з'єднань та мережевого трафіку, особливо в розподілених корпоративних мережах. Різноманітність режимів роботи (транспортний і тунельний) та підтримка різних криптографічних алгоритмів робить IPSec гнучким і ефективним рішенням для будь-яких вимог щодо безпеки в корпоративних мережах [21].

3. РОЗРОБКА ЛОГІЧНОЇ СТРУКТУРИ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Моделювання розподіленої корпоративної мережі

Сучасні корпоративні мережі стали важливою частиною інфраструктури будь-якої організації, оскільки вони забезпечують з'єднання між офісами, віддаленими працівниками, дата-центрами та хмарними сервісами. Така мережа повинна бути не тільки ефективною, але й безпечною, надійною та здатною витримувати високі навантаження. Враховуючи складність і масштаб сучасних корпоративних мереж, їх проектування та оптимізація вимагають застосування ефективних методів моделювання для забезпечення надійності та ефективності функціонування. Процес моделювання мереж дозволяє створювати віртуальні копії інфраструктури, що дає змогу тестувати нові рішення, прогнозувати поведінку системи в різних сценаріях і виявляти потенційні слабкі місця без ризику для реальних об'єктів.

У цьому контексті моделювання мереж набуває особливої значущості в рамках розробки корпоративних мереж для великих організацій, де навіть короткочасний збій може спричинити серйозні фінансові втрати або порушити ключові бізнес-процеси. Це особливо актуально для магістерських досліджень, де акцент робиться на глибокому аналізі та практичних рекомендаціях для розв'язання складних завдань проектування мереж. Методи моделювання мереж можна поділити на три основні категорії: аналітичне, емпіричне та симуляційне моделювання, кожне з яких має свої переваги і обмеження, що визначають їх застосування в залежності від специфіки задачі.

Аналітичне моделювання є ефективним інструментом для розрахунку основних параметрів мережі, таких як пропускна здатність, затримка, ймовірність втрати даних тощо, на основі математичних формул і теоретичних підходів. Однак, через складність врахування всіх можливих варіантів для великих і

розподілених мереж, цей метод має обмеження щодо точності в складних сценаріях.

Емпіричне моделювання ґрунтується на реальних даних з існуючих мереж і є чудовим методом для перевірки ефективності вже реалізованих рішень, проте потребує доступу до великої кількості даних і може бути менш корисним для проектування нових мереж або вивчення ще не впроваджених технологій.

Симуляційне моделювання є найпоширенішим і універсальним методом, який дозволяє створювати віртуальні моделі мереж і тестувати їх у різних сценаріях. Він забезпечує найбільшу гнучкість, даючи змогу не лише прогнозувати поведінку мережі, а й оптимізувати її. Саме цей метод є найбільш популярним у сучасному проектуванні корпоративних мереж, оскільки він дозволяє максимально точно відтворювати реальні умови роботи.

3.2 Вибір програмного забезпечення для моделювання

У рамках цієї магістерської роботи розглядаються два основні інструменти для моделювання корпоративних мереж: Cisco Packet Tracer та GNS3. Кожна з цих програм має свої особливості, переваги та недоліки, що впливають на вибір для різних типів задач. Ось детальний опис кожної з програм.

Cisco Packet Tracer

Cisco Packet Tracer — це програмне забезпечення, яке було спеціально розроблене компанією Cisco для навчальних цілей, а також для створення базових моделей мереж (Рисунок 3.1). Це популярний інструмент серед студентів і новачків у мережевих технологіях, оскільки він дозволяє швидко створювати віртуальні мережі та тестувати різні конфігурації мережевих пристроїв [22]. Cisco Packet Tracer має широкі можливості для вивчення основних принципів маршрутизації, налаштування VLAN, NAT і ACL, але не підтримує більш складні функціональності, які потрібні для моделювання великих корпоративних мереж.

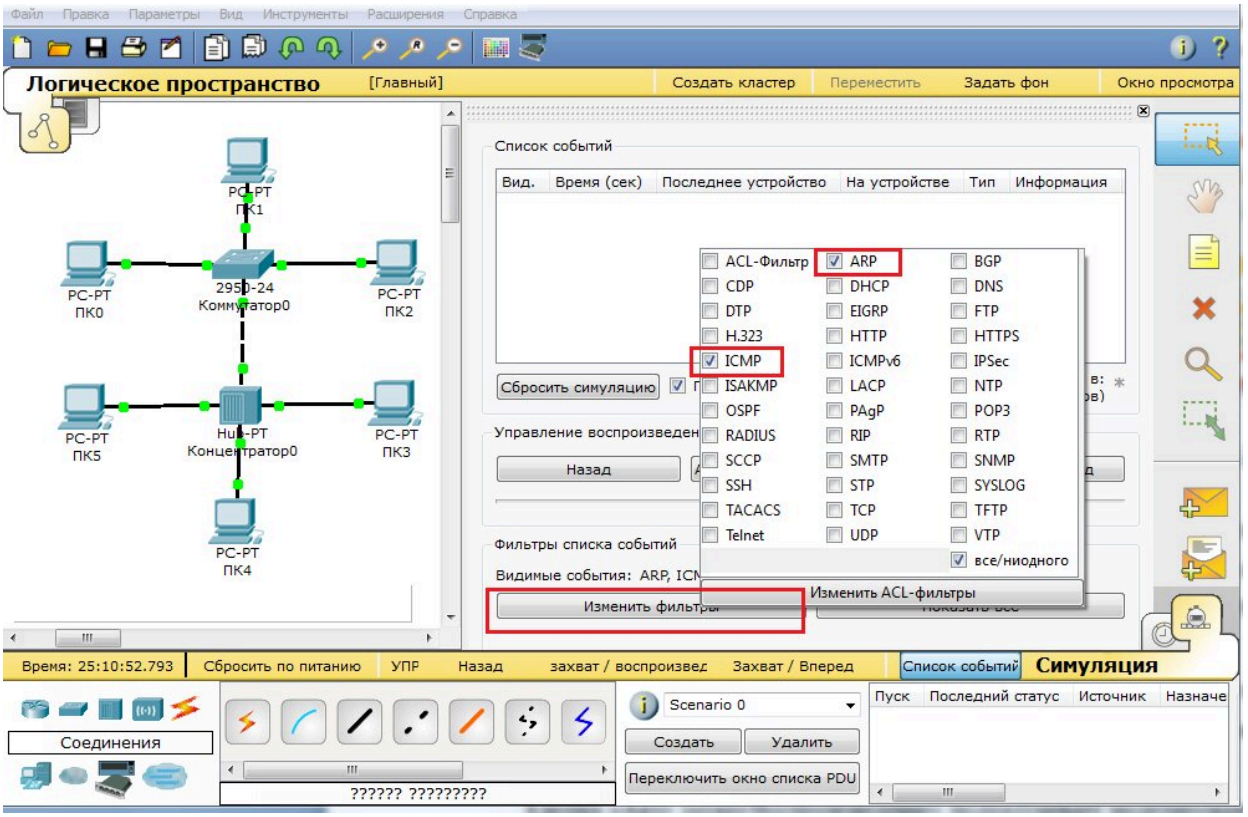


Рисунок 3.1 — Інтерфейс програми Cisco Packet Tracer

Переваги:

- Простота використання: Інтерфейс Cisco Packet Tracer є дуже інтуїтивно зрозумілим, що робить програму ідеальним інструментом для новачків у сфері мережевого адміністрування та проектування. Всі основні функції доступні через візуальне середовище, що дозволяє швидко освоїти роботу з програмою.
- Підтримка основних мережевих функцій: Програма підтримує налаштування базових мережевих функцій, таких як маршрутизація, VLAN, NAT (Network Address Translation), ACL (Access Control Lists), що дозволяє створювати різноманітні сценарії для середніх за складністю мереж.
- Широкий набір мережевих пристроїв Cisco: Cisco Packet Tracer дозволяє працювати з великою кількістю віртуальних пристроїв, таких як маршрутизатори, комутатори, точки доступу, що робить моделювання більш

реалістичним. Ці пристрої дозволяють відтворювати конфігурації, схожі на реальні мережі.

- Навчальні ресурси та інтерактивні сценарії: Cisco Packet Tracer включає вбудовані інтерактивні сценарії, завдяки чому студенти та початківці можуть наочно вивчати основи мережевих технологій і тестувати різні конфігурації без необхідності мати фізичне обладнання.
- Мультимедійні можливості: Програма дозволяє візуалізувати роботу мережі з використанням різних мультимедійних інструментів, таких як відео та аудіо потоки, що є корисним для демонстрації роботи мережі в реальних умовах.

Недоліки:

- Обмежена масштабованість: Для створення великих і складних мереж, що включають багато типів пристроїв і мережевих протоколів, можливості Packet Tracer можуть бути недостатніми.
- Не підтримує реальні образи операційних систем пристроїв: Це обмежує точність моделювання у порівнянні з іншими інструментами, які працюють з реальними образами.

GNS3 (Graphical Network Simulator-3)

GNS3 — це потужна платформа для емуляції та візуалізації мережевої інфраструктури, яка здобула популярність серед професіоналів завдяки своїй гнучкості та можливості інтеграції з реальними образами операційних систем пристроїв (Рисунок 3.2). Це означає, що GNS3 дозволяє створювати точніші моделі мереж, які базуються на реальних операційних системах, таких як Cisco IOS, Juniper JunOS, а також інші ОС для мережевих пристроїв. GNS3 також дозволяє інтегрувати фізичні пристрої в модель, що дає можливість створювати гібридні тестові середовища [23].

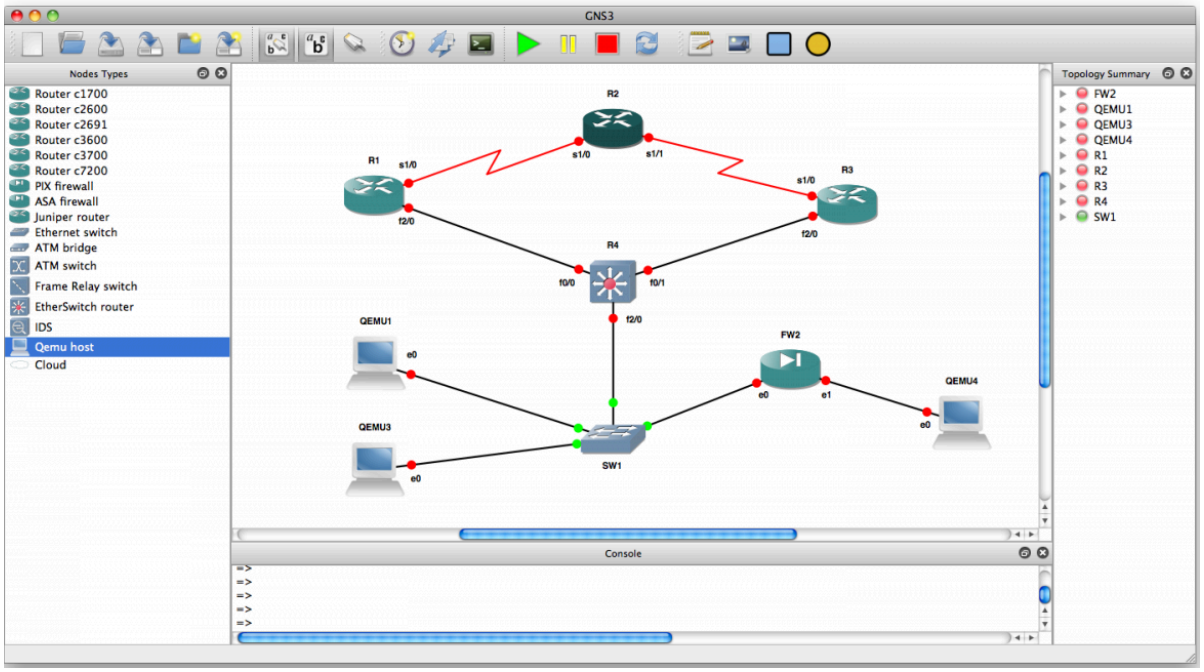


Рисунок 3.2 — Інтерфейс програми Graphical Network Simulator-3

Переваги:

- Емуляція реальних пристроїв: Одна з головних переваг GNS3 — це можливість працювати з реальними образами операційних систем пристроїв, таких як Cisco IOS, Juniper JunOS та інші. Це дозволяє створювати дуже точні моделі реальних мереж з використанням тих самих операційних систем, що й у реальному житті.
- Гнучкість і масштабованість: GNS3 дозволяє створювати дуже складні мережеві топології, в яких можна комбінувати різні типи мережевих пристроїв, підключати фізичні пристрої через серійні порти або інші методи інтеграції. Це робить GNS3 ідеальним інструментом для професійного проектування корпоративних мереж.
- Підтримка зовнішніх образів і плагінів: GNS3 підтримує інтеграцію з різними зовнішніми образами операційних систем, що дозволяє користувачам створювати моделі, що більш точно відображають реальні умови роботи мереж.
- Можливість інтеграції з фізичними пристроями: Важливою перевагою є можливість підключення фізичних пристроїв до віртуальних моделей для

створення гібридних тестових середовищ. Це дозволяє виконувати тестування в умовах, наближених до реальних.

- Можливості для професійного використання: GNS3 має всі необхідні інструменти для професійного проектування мереж і є потужним інструментом для глибокого тестування і налаштування корпоративних мереж.

Недоліки:

- Високі вимоги до ресурсів: GNS3 потребує значних обчислювальних ресурсів, оскільки для емуляції реальних операційних систем потрібна велика кількість пам'яті та потужний процесор.
- Складність в освоєнні: Інтерфейс програми може бути складним для початківців, оскільки для її ефективного використання необхідні знання мережевих технологій і конфігурацій.

Для моделювання мережі в межах нашої магістерської роботи був обраний Cisco Packet Tracer. Програма дозволяє ефективно створювати мережеві топології, налаштовувати мережеві пристрої та тестувати різні сценарії без значних витрат часу та ресурсів. Візуалізація процесів роботи мережі в Cisco Packet Tracer дає змогу краще розуміти взаємодію компонентів і знаходити оптимальні рішення для проектування мережі. Завдяки зручному інтерфейсу та широким можливостям налаштування, Cisco Packet Tracer забезпечує необхідний рівень деталізації, що дає змогу ефективно вирішувати завдання без необхідності використання складніших і важчих для реалізації інструментів.

Особливо важливим для нашої роботи є можливість налаштування IPsec, яке ми розглядаємо у рамках дослідження. Cisco Packet Tracer підтримує цей протокол для забезпечення безпеки та захищеного з'єднання між різними мережами, що дозволяє нам моделювати та тестувати різні сценарії використання VPN в межах корпоративної інфраструктури.

Всі ці чинники роблять Cisco Packet Tracer оптимальним вибором для проектування та тестування корпоративної мережі в межах нашої магістерської роботи, особливо з урахуванням необхідності інтеграції технологій безпеки, таких як IPsec.

3.3 Розробка схеми мережі на базі емулятора Cisco Packet Tracer

Для побудови розподіленої мережі в Cisco Packet Tracer було додано три маршрутизатори Cisco 1941: Router1, Router0 та Router2. Маршрутизатор Router1 виступає як маршрутизатор провайдера, Router0 — як маршрутизатор центрального офісу, а Router2 — як маршрутизатор філіалу (Рисунок 3.3).

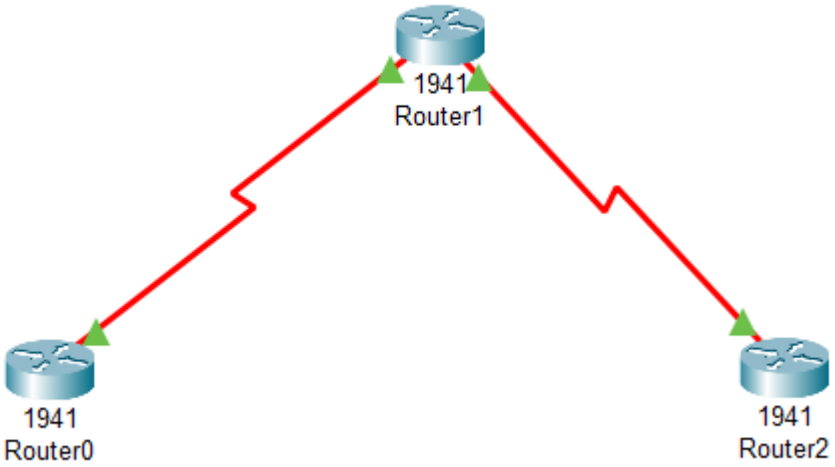


Рисунок 3.3 — Схема підключення маршрутизаторів

Для підключення маршрутизаторів Router1 та Router0, а також Router0 та Router2, були використані серійні порти. Для цього на маршрутизаторах Router1, Router0 та Router2 додано відповідні серійні модулі HWIC-2T, що забезпечують порти типу Serial 0/0/0-0/0/1 (Рисунок 3.4). Після цього було налаштовано з'єднання між маршрутизаторами через серійні кабелі DCE: порт Serial 0/0/0 на Router1 підключено до порту Serial 0/0/1 на Router0, а порт Serial 0/0/0 на Router0 підключено до порту Serial 0/0/0 на Router2. Це забезпечує з’єднання між маршрутизатором провайдера та центральним офісом, а також між центральним офісом і філіалом.

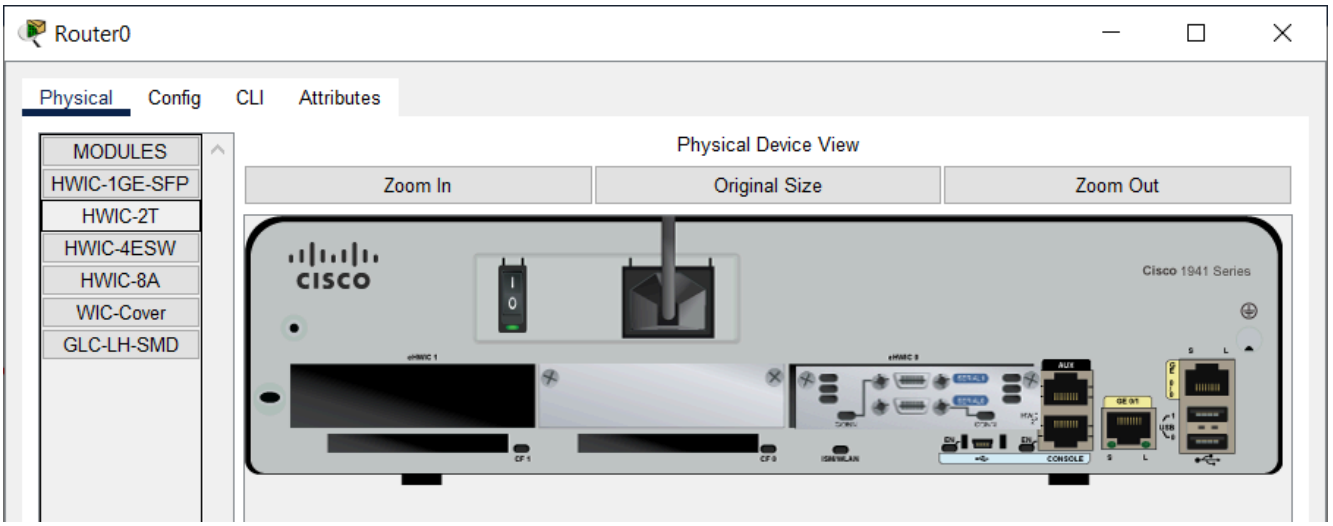


Рисунок 3.4 — Інтерфейси маршрутизатора Router0

Далі переходимо до налаштування маршрутизатора Router0. Зв'язок з локальною мережею центрального офісу буде виконуватися через інтерфейс GigabitEthernet0/0, якому призначаємо IP-адресу 192.168.10.1 з маскою підмережі 255.255.255.0. Команда "interface GigabitEthernet0/0" дозволяє нам зайти на необхідний інтерфейс, а за допомогою "ip address 192.168.10.1 255.255.255.0" встановити необхідну адресу. Також використовуємо команду "no shutdown", що дозволяє увімкнути вибраний нами інтерфейс (Рисунок 3.5).

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

Router(config-if)#exit
```

Рисунок 3.5 — Налаштування маршрутизатора Router0

Після налаштування локальної мережі необхідно налаштувати зв'язок з філіалом. Зв'язок з філіалом буде здійснюватися через ISP (Інтернет-провайдер). Заходимо на інтерфейс Serial0/0/0 і призначеємо IP-адресу 10.1.0.1 з маскою підмережі 255.255.255.252 для виходу в глобальну мережу (Рисунок 3.6).

```
Router(config)#interface Serial0/0/0
Router(config-if)#ip address 10.1.0.1 255.255.255.252
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#exit
```

Рисунок 3.6 — Налаштування зв'язку центрального офісу з Інтернет-провайдером

Встановимо адрес ISP для його взаємодії з центральним офісом. Використаємо інтерфейс Serial0/0/1 і IP-адресу 10.1.0.2 з маскою підмережі 255.255.255.252 (Рисунок 3.7).

```
Router(config)#int se0/0/1
Router(config-if)#ip ad
Router(config-if)#ip address 10.1.0.2 255.255.255.252
Router(config-if)#no sh

Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

Router(config-if)#ex
```

Рисунок 3.7 — Налаштування ISP

Тепер налаштуємо можливість проходу всього трафіку в ISP використовуючи адресу 10.1.0.2 встановлену на ISP в інтерфейсі Serial0/0/1. Команда “ip route 0.0.0.0 0.0.0.0 10.1.0.2” дає можливість трафіку з будь-якого джерела внутрішньої мережі безперешкодно проходити до ISP (Рисунок 3.8).

```
Router(config)#ip route 0.0.0.0 0.0.0.0 10.1.0.2
```

Рисунок 3.8 — Налаштування маршрутизації маршрутизатора Router0

Виконуємо аналогічні налаштування маршрутизатора Router2 для мережі філіалу. Для філіалу буде використовуватися адресний простір 10.2.0.0 з маскою 255.255.255.252.

У межах даного проекту здійснюється створення систематизованого розподіл адрес шляхом сегментації мережі за допомогою VLAN. Це передбачає виділення окремих діапазонів IP-адрес для кожного VLAN, що сприяє ефективному управлінню мережею та полегшує ідентифікацію вузлів. Такий підхід забезпечує узгодженість, логічність та прозорість у мережевому проектуванні, що полегшує масштабування мережі, покращує мережеву безпеку та сприяє швидкому вирішенню проблем мережі [24]. Детальний розподіл адрес для кожного VLAN центрального офісу подається в таблиці 3.1.

Таблиця 3.1 — Розподіл адрес для кожного VLAN центрального офісу

Назва	Мережа	Тип	Призначення	Адреса на комутаторі
Office	192.168.10.0/24	Статична		192.168.10.2
Admin	192.168.11.0/24	Динамічна	ПК адміністрації	192.168.11.1
IT	192.168.12.0/24	Динамічна	ПК IT-відділу	192.168.12.1
HR	192.168.13.0/24	Динамічна	ПК відділу кадрів	192.168.13.1
Finance	192.168.14.0/24	Динамічна	ПК фінансового відділу	192.168.14.1
Sales	192.168.15.0/24	Динамічна	ПК відділу продажів	192.168.15.1
Server	192.168.16.0/24	Статична	Сервери	192.168.16.1
Guest	192.168.17.0/24	Динамічна	Гостьова мережа	192.168.17.1

Проводимо аналогічні налаштування для мережі філіалу. Детальний розподіл адрес для кожного VLAN філіалу подається в таблиці 3.2.

Таблиця 3.2 — Розподіл адрес для кожного VLAN філіалу

Назва	Мережа	Тип	Призначення	Адреса на комутаторі
Office	172.16.10.0/24	Статична		172.16.10.2
Admin	172.16.11.0/24	Динамічна	ПК адміністрації	172.16.11.1
IT	172.16.12.0/24	Динамічна	ПК IT-відділу	172.16.12.1
HR	172.16.13.0/24	Динамічна	ПК відділу кадрів	172.16.13.1
Finance	172.16.14.0/24	Динамічна	ПК фінансового відділу	172.16.14.1
Sales	172.16.15.0/24	Динамічна	ПК відділу продажів	172.16.15.1
Server	172.16.16.0/24	Статична	Сервери	172.16.16.1
Guest	172.16.17.0/24	Динамічна	Гостьова мережа	172.16.17.1

Для маршрутизації трафіку в локальній мережі додаємо L3 комутатор (Layer 3 Switch). Використовуючи L3 комутатор для внутрішньої маршрутизації між VLAN-ами, ми знижуємо навантаження на центральний маршрутизатор, що дозволяє йому фокусуватися на маршрутизації трафіку між внутрішньою мережею і зовнішнім світом через ISP.

Для реалізації внутрішньої маршрутизації між VLAN-ами на L3 комутаторі необхідно налаштувати відповідні IP-адреси на його інтерфейсах, які будуть використовуватися для маршрутизації трафіку між різними сегментами мережі. Командою “interface vlan 11” заходимо на інтерфейс необхідного VLAN і призначеємо IP-адресу 192.168.11.1 з маскою підмережі 255.255.255.0. Командою “vlan 11” створюємо відповідну віртуальну локальну мережу з ідентифікатором 11 і командою ”name” назнаємо її назву (Рисунок 3.9).

```
Switch(config)#int vlan 11
Switch(config-if)#ip ad
Switch(config-if)#ip address 192.168.11.1 255.255.255.0
Switch(config-if)#ex

Switch(config)#vlan 11
Switch(config-vlan)#
%LINK-5-CHANGED: Interface Vlan11, changed state to up

Switch(config-vlan)#name Admin
Switch(config-vlan)#ex
```

Рисунок 3.9 — Налаштування Vlan 11 на L3 комутаторі

Проводимо аналогічні дії для налаштування інших VLAN-ів.

Перейдемо до налаштування транк портів на комутаторі Multilayer Switch0. Trunk port — це комутаційний порт, за допомогою якого може передаватися трафік із тегами від одного або декількох VLAN. Переходимо до налаштування інтерфейсу Gi1/0/2, створюємо статичний транк за допомогою команди “switchport mode trunk”. Після створення транку автоматично будуть дозволені всі VLAN. Командою “switchport trunk allowed vlan 11,12” дозволимо лише 11 і 12 VLAN. Проводимо аналогічні налаштування для портів Gi1/0/2-1/0/6 (Рисунок 3.10).

```
Switch(config)#int gi1/0/2
Switch(config-if)#sw
Switch(config-if)#switchport m
Switch(config-if)#switchport mode t
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan11, changed state to up

Switch(config-if)#sw
Switch(config-if)#switchport t
Switch(config-if)#switchport trunk a
Switch(config-if)#switchport trunk allowed v
Switch(config-if)#switchport trunk allowed vlan 11,12
Switch(config-if)#ex
```

Рисунок 3.10 — Налаштування trunk port на Multilayer Switch0

Далі переходимо до налаштування акцес портів на комутаторі Multilayer Switch0. Access port — це комутаційний порт, який належить до одного VLAN і передає лише нетегований інформаційний трафік. Заходимо на інтерфейс Gi1/0/1 і командою “switchport mode access” переходимо в access режим, а командою “switchport access vlan 10” дозволяємо vlan 10 на даному інтерфейсі (Рисунок 3.11).

```
Switch(config)#int gi1/0/1
Switch(config-if)#sw
Switch(config-if)#switchport m
Switch(config-if)#switchport mode a
Switch(config-if)#switchport mode access
Switch(config-if)#sw
Switch(config-if)#switchport a
Switch(config-if)#switchport access v
Switch(config-if)#switchport access vlan 10
Switch(config-if)#ex
```

Рисунок 3.11 — Налаштування access port на Multilayer Switch0

Налаштовуємо комутатор Switch1. Цей комутатор забезпечує підключення пристроїв співробітників компанії. Переходимо до інтерфейсів, які підключені до комутатора Multilayer Switch0, і створюємо trunk port для VLAN 11 і 12, що дозволить їхньому трафіку вільно проходити.

На комутаторі Switch1 також налаштовуємо access порти для підключення пристроїв співробітників компанії. Переходимо до налаштувань інтерфейсів, до яких будуть підключені пристрої користувачів. За допомогою команди “switchport mode access” переводимо порти в режим access. Далі командою “switchport access vlan 11” призначаємо порти до VLAN 11, що дозволить пристроям співробітників отримувати доступ до внутрішньої корпоративної мережі (Рисунок 3.12).

```
Switch(config)#int gi0/1
Switch(config-if)#sw
Switch(config-if)#switchport m
Switch(config-if)#switchport mode t
Switch(config-if)#switchport mode trunk
Switch(config-if)#sw
Switch(config-if)#switchport t
Switch(config-if)#switchport trunk a
Switch(config-if)#switchport trunk allowed v
Switch(config-if)#switchport trunk allowed vlan 11,12
Switch(config-if)#ex
Switch(config)#int ra fa0/1-3
Switch(config-if-range)#sw
Switch(config-if-range)#switchport m
Switch(config-if-range)#switchport mode a
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#sw
Switch(config-if-range)#switchport a
Switch(config-if-range)#switchport access v
Switch(config-if-range)#switchport access vlan 11
% Access VLAN does not exist. Creating vlan 11
Switch(config-if-range)#ex
```

Рисунок 3.12 — Налаштування портів на Switch1

Для налаштування автоматичної видачі IP-адрес в мережі використовується DHCP-сервер, що дозволяє пристроям отримувати всі необхідні налаштування без необхідності вручну вводити IP-адресу, шлюз або DNS-сервер. Це значно полегшує адміністрування мережі та знижує ймовірність виникнення помилок у налаштуваннях.

DHCP-сервер (Dynamic Host Configuration Protocol) — це сервер, який автоматично надає клієнтським пристроям в мережі IP-адреси і інші мережеві параметри. У нашому випадку, для видачі IP-адрес використовується сервер з IP-адресою 192.168.16.2. На цьому сервері налаштовуємо пул IP-адрес для VLAN. Для цього вказується діапазон IP-адрес, шлюз за замовчуванням та DNS-сервер (Рисунок 3.13).

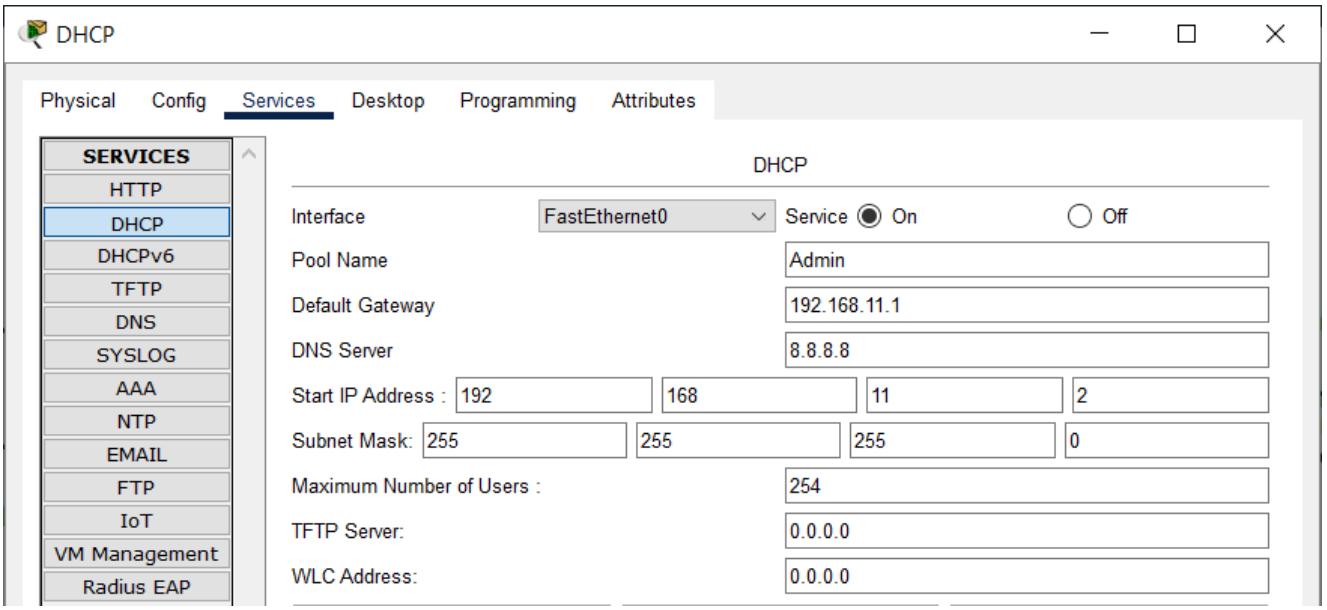


Рисунок 3.13 — Налаштування DHCP сервера центрального офісу

Оскільки DHCP-сервер знаходиться в іншій підмережі, потрібно налаштувати пересилання DHCP-запитів за допомогою IP Helper Address. Це налаштування дозволяє клієнтам VLAN 11 відправляти свої DHCP-запити на L3-комутатор, а він перенаправляє їх до серверу з IP-адресою 192.168.16.2. Для цього на інтерфейсі VLAN 11 на L3-комутаторі вводимо команду “ip helper-address 192.168.16.2”. Це дозволяє клієнтам в VLAN 11 отримувати IP-адреси та інші параметри автоматично, що спрощує налаштування та роботу в мережі (Рисунок 3.14).

```
Switch(config)#int vlan 11
Switch(config-if)#ip help
Switch(config-if)#ip helper-address 192.168.16.2
Switch(config-if)#ex
```

Рисунок 3.14 — Налаштування DHCP-Relay на Multilayer Switch0

Наступним етапом налаштуємо NAT. Network Address Translation дозволяє здійснювати трансляцію внутрішніх (приватних) IP-адрес в зовнішні (публічні) адреси для виходу в Інтернет. Це важливо для того, щоб пристрої в локальній мережі могли мати доступ до глобальної мережі Інтернет, використовуючи одну публічну IP-адресу.

Щоб налаштувати NAT, потрібно створити список дозволених IP-адрес для трансляції. Для цього командою “ip access-list extended FOR-NAT” створюємо access-list, в якому вказуємо діапазон IP-адрес, які будуть підлягати трансляції.

На маршрутизаторі вказуємо, який інтерфейс є внутрішнім, а який зовнішнім. Для цього заходимо на GigabitEthernet0/0 і командою “ip nat inside” назначаємо внутрішнім інтерфейсом, а інтерфейс Serial0/0/0 командою “ip nat outside” назначаємо зовнішнім (Рисунок 3.15).

```
Router(config)#ip access-list extended FOR-NAT
Router(config-ext-nacl)# deny ip 192.168.0.0 0.0.255.255 172.16.0.0 0.0.255.255
Router(config-ext-nacl)# permit ip 192.168.0.0 0.0.255.255 any
Router(config-ext-nacl)#ex
Router(config)#interface GigabitEthernet0/0
Router(config-if)# ip address 192.168.10.1 255.255.255.0
Router(config-if)# ip nat inside
Router(config-if)#ex
Router(config)#interface Serial0/0/0
Router(config-if)# ip address 10.1.0.1 255.255.255.252
Router(config-if)# ip nat outside
Router(config-if)#ex
Router(config)#ip nat inside source list FOR-NAT interface Serial0/0/0 overload
```

Рисунок 3.15 — Налаштування NAT

Тепер налаштуємо шифрування IPSec. Налаштування шифрування IPSec складається з двох етапів. На першому етапі визначаємо політику безпеки (ISAKMP IKE) для створення тунелю. На другому етапі налаштовуємо параметри тунелю (IPSec) для передачі даних.

Організуємо шифрування IPSec між маршрутизатором центрального офісу Router0 і маршрутизатором філіалу Router2. Командою “crypto isakmp policy 10” перейдемо до налаштування політик безпеки. Команда “encryption aes 256”

визначає метод шифрування AES. Далі створюємо метод аутентифікації pre-share командою “authentication pre-share”. Group 5 є методом обміну секретними ключами, а саме методом Диффі-Хеллмана.

Далі назначаємо спільний ключ (pre-shared key) для аутентифікації використовуючи команду “crypto isakmp key PJ2pc3T23n address 10.2.0.1”.

Тепер здійснюється налаштування transform-set визначаючи методи шифрування та хешування. Це налаштування здійснюється командою “crypto ipsec transform-set R1-R2 esp-aes 256 esp-sha-hmac” (Рисунок 3.16).

```
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#group 5
Router(config-isakmp)#ex
Router(config)#
Router(config)#crypto isakmp key PJ2pc3T23n address 10.2.0.1
Router(config)#crypto ipsec transform-set R1-R2 esp-aes 256 esp-sha-hmac
```

Рисунок 3.16 — Налаштування налаштування політик безпеки ISAKMP

Створимо список доступу, який визначає адреси, для яких буде застосовуватися шифруватися. Для цього використаємо команду “access-list 100 permit ip 192.168.0.0 0.0.255.255 172.16.0.0 0.0.255.255”.

Наступним етапом є створення об'єкта "crypto map", який об'єднує всі створені до цього елементи криптозахисту та вказуватиме кінцеві хости IPSec. Після створення цього об'єкта його конфігурація буде застосована до налаштувань інтерфейсу Serial 0/0/0. Для цього командою “interface serial 0/0/0” заходимо на відповідний інтерфейс і за допомогою “crypto map R1CrMAP” застосовуємо налаштування до даного інтерфейсу (Рисунок 3.17).

```
Router(config)#crypto map R1CrMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#set peer 10.2.0.1
Router(config-crypto-map)#set pfs group5
Router(config-crypto-map)#set security-association lifetime seconds 86400
Router(config-crypto-map)#set transform-set R1-R2
Router(config-crypto-map)#match address 100
Router(config-crypto-map)#ex
Router(config)#
Router(config)#interface serial 0/0/0
Router(config-if)#crypto map R1CrMAP
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#ex
```

Рисунок 3.17 — Налаштування crypto map Router0

Зробимо аналогічні налаштування на маршрутизаторі філіалу Router2. Відмінність полягатиме в адресі кінцевої точки тунелю, а саме в адресі Router0 (Рисунок 3.18).

```
Router#sh crypto map
Crypto Map R2CrMAP 10 ipsec-isakmp
        Peer = 10.1.0.1
        Extended IP access list 100
            access-list 100 permit ip 172.16.0.0 0.0.255.255 192.168.0.0 0.0.255.255
        Current peer: 10.1.0.1
        Security association lifetime: 4608000 kilobytes/86400 seconds
        PFS (Y/N): Y
        Transform sets={
                R2-R1,
        }
        Interfaces using crypto map R2CrMAP:
                Serial0/0/0
```

Рисунок 3.18 — Крипто карта Router2

Після налаштування IPSec шифрування тунелю можна перевірити статус ISAKMP сесії за допомогою команди «sh crypto isakmp sa». У відображеній конфігурації показано статус аутентифікації та інформацію про активні ISAKMP асоціації. Тут можна побачити IP-адреси кінцевих точок тунелю, стан аутентифікації та деталі щодо встановлення безпечного каналу для обміну ключами (Рисунок 3.19).

```
Router#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.2.0.1        10.1.0.1        QM_IDLE           1003    0 ACTIVE


IPv6 Crypto ISAKMP SA
```

Рисунок 3.19 — Виведення статусу ISAKMP асоціацій після налаштування IPSec

Отже, після моделювання мережі в Cisco Packet Tracer ми успішно створили робочу топологію, в якій реалізували різні протоколи та технології для забезпечення ефективної і безпечної передачі даних (Рисунок 3.20). У процесі моделювання були налаштовані такі протоколи, як IPSec для забезпечення захисту даних через шифрування та автентифікацію, NAT (Network Address Translation) для маскування приватних IP-адрес при доступі до зовнішніх мереж, а також DHCP (Dynamic Host Configuration Protocol) для автоматичного призначення IP-адрес пристроям у мережі.

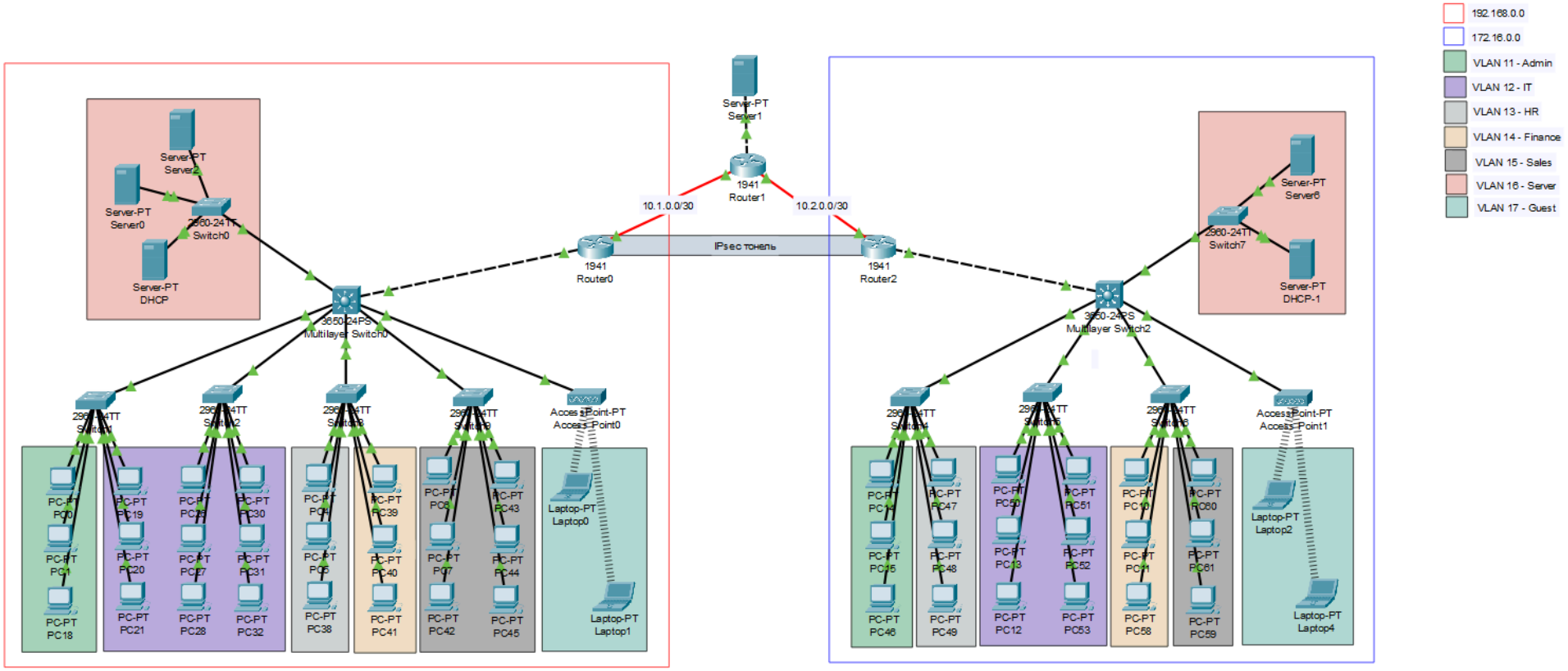


Рисунок 3.20 — Модель корпоративної розподіленої мережі

3.4 Аналіз результатів моделювання мережі на основі протоколу IPSec

Для перевірки коректної роботи IPSec тунелю в нашій мережевій моделі, ми ініціюємо передачу даних через тунель за допомогою ICMP запиту. Це дозволить нам переконатися в тому, що з'єднання між кінцевими пристроями працює належним чином, а механізми шифрування та автентифікації, реалізовані в IPSec, виконуються правильно (Рисунок 3.21).

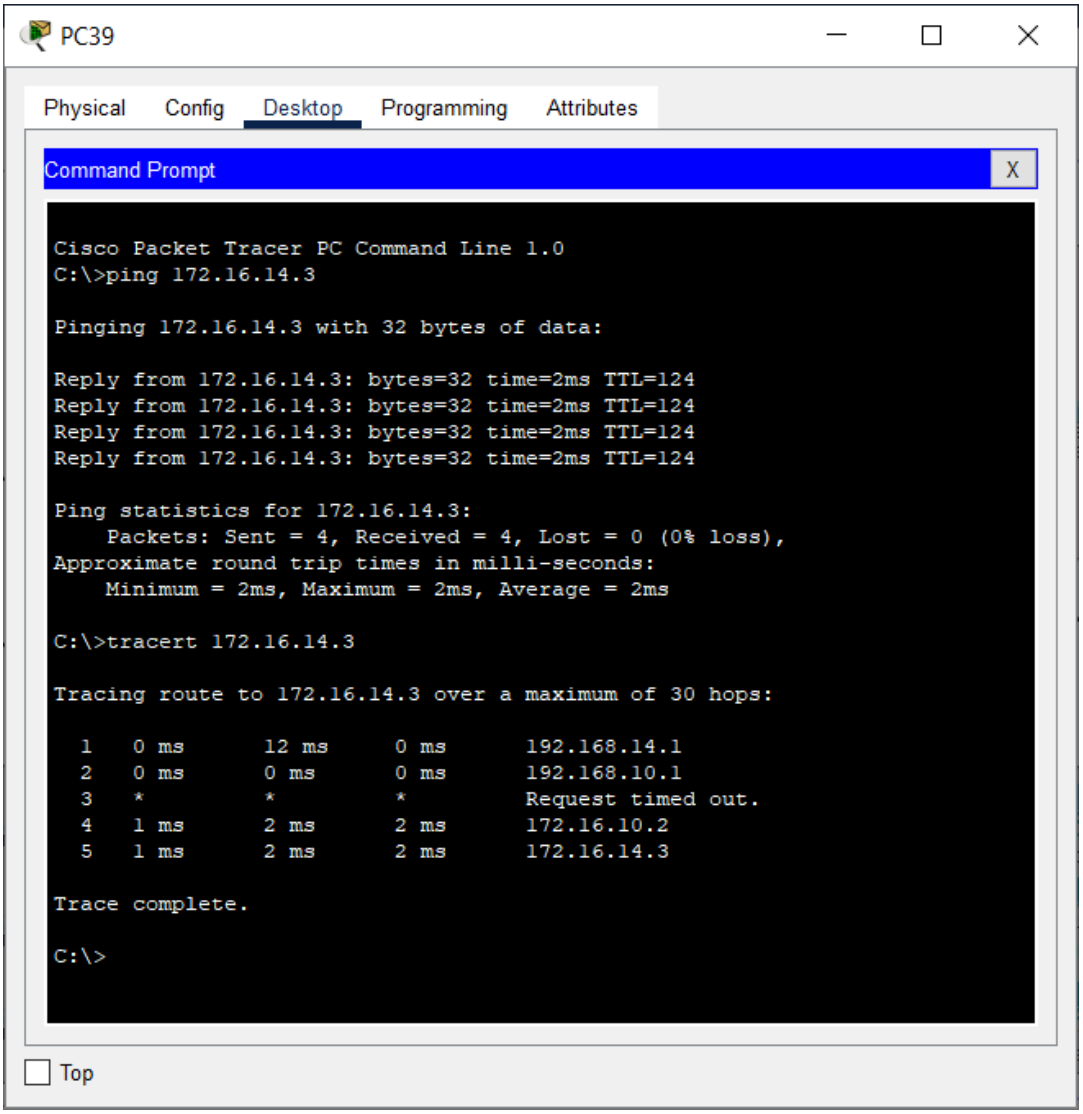


Рисунок 3.21 — Результат ICMP запитів між пристроями центрального офісу і філіалу

Ініціація exo запиту (ping) дозволяє перевірити працездатність тунелю, а також наочно продемонструвати, що IPSec забезпечує захист даних під час їх передачі. При цьому всі пакети, які проходять через IPSec тунель, можна відстежити за допомогою команди «sh crypto ipsec sa» на маршрутизаторі, який бере участь в з'єднанні. Ця команда виводить статистику щодо встановлених IPSec безпекових асоціацій (SA) і відображає важливі дані про обробку трафіку, що проходить через тунель (Рисунок 3.22).

```
Router#sh crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: R1CrMAP, local addr 10.1.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.0/255.255.0.0/0/0)
   remote  ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
   current_peer 10.2.0.1 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 0
   #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.0.1, remote crypto endpt.:10.2.0.1
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0xE935F977(3912628599)

     inbound esp sas:
      spi: 0x605DF4B9(1616770233)
        transform: esp-aes 256 esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2009, flow_id: FPGA:1, crypto map: R1CrMAP
        sa timing: remaining key lifetime (k/sec): (4525504/77321)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE
```

Рисунок 3.22 — Виведення статусу IPSec

Застосування команди «sh crypto ipsec sa» дозволяє побачити, як IPSec тунель обробляє пакети, зокрема, можна спостерігати за шифруванням, автентифікацією та іншими характеристиками трафіку. Виведена інформація

включає деталі про використовувані політики безпеки, ключі шифрування, а також індекси параметрів безпеки (SPI), які допомагають визначити, які саме налаштування застосовуються для обробки пакета.

Розглянемо процес роботи IPSec тунелю в нашій мережевій моделі більш детально, використовуючи режим симуляції. Симуляція в Cisco Packet Tracer дозволяє нам детально вивчити, як IPSec працює в реальному часі, забезпечуючи захист даних у нашій моделі. У ході перевірки ми проаналізуємо передані пакети та їх поля, щоб оцінити, чи виконуються необхідні функції безпеки, зокрема шифрування та автентифікація.

У симуляції ініціюємо процес передачі пакета з одного пристрою на інший (Рисунок 3.23).

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC39	ICMP
	0.001	PC39	Switch3	ICMP
	0.002	Switch3	Multilayer Switch0	ICMP
	0.003	Multilayer Switch0	Router0	ICMP
	0.004	Router0	Router1	ICMP
	0.005	Router1	Router2	ICMP
	0.006	Router2	Multilayer Switch2	ICMP
	0.007	Multilayer Switch2	Switch6	ICMP
	0.008	Switch6	PC10	ICMP
	0.009	PC10	Switch6	ICMP
	0.010	Switch6	Multilayer Switch2	ICMP
	0.011	Multilayer Switch2	Router2	ICMP
	0.012	Router2	Router1	ICMP
	0.013	Router1	Router0	ICMP
	0.014	Router0	Multilayer Switch0	ICMP
	0.015	Multilayer Switch0	Switch3	ICMP
	0.016	Switch3	PC39	ICMP

Reset Simulation | Constant Delay | Captured to: 0.016 s

Рисунок 3.23 — Івент-лист про передачу пакета через IPSec тунель.

Після успішної доставки пакета (Рисунок 3.24), ми можемо бути впевнені, що дані досягли своєї цілі без втрат або пошкоджень.

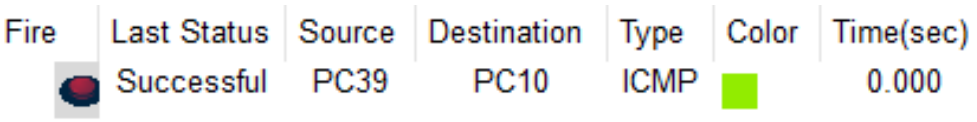


Рисунок 3.24 — Результат успішного обміну пакетами

Проводимо детальний аналіз структури пакета, зокрема перевіряємо наявність усіх необхідних полів, таких як ESP (Encapsulating Security Payload), які відповідають за шифрування та автентифікацію даних. Це дасть змогу оцінити, чи працюють механізми IPSec належним чином і чи відповідають вони встановленим вимогам безпеки [25].

Inbound PDU (Protocol Data Unit) описує пакет, що надходить до пристрою Router0. Він складається з кількох рівнів протоколів, зокрема Ethernet II, IP, та ICMP. Розглянемо детальніше структуру та призначення кожного елемента цього пакета (Рисунок 3.25).

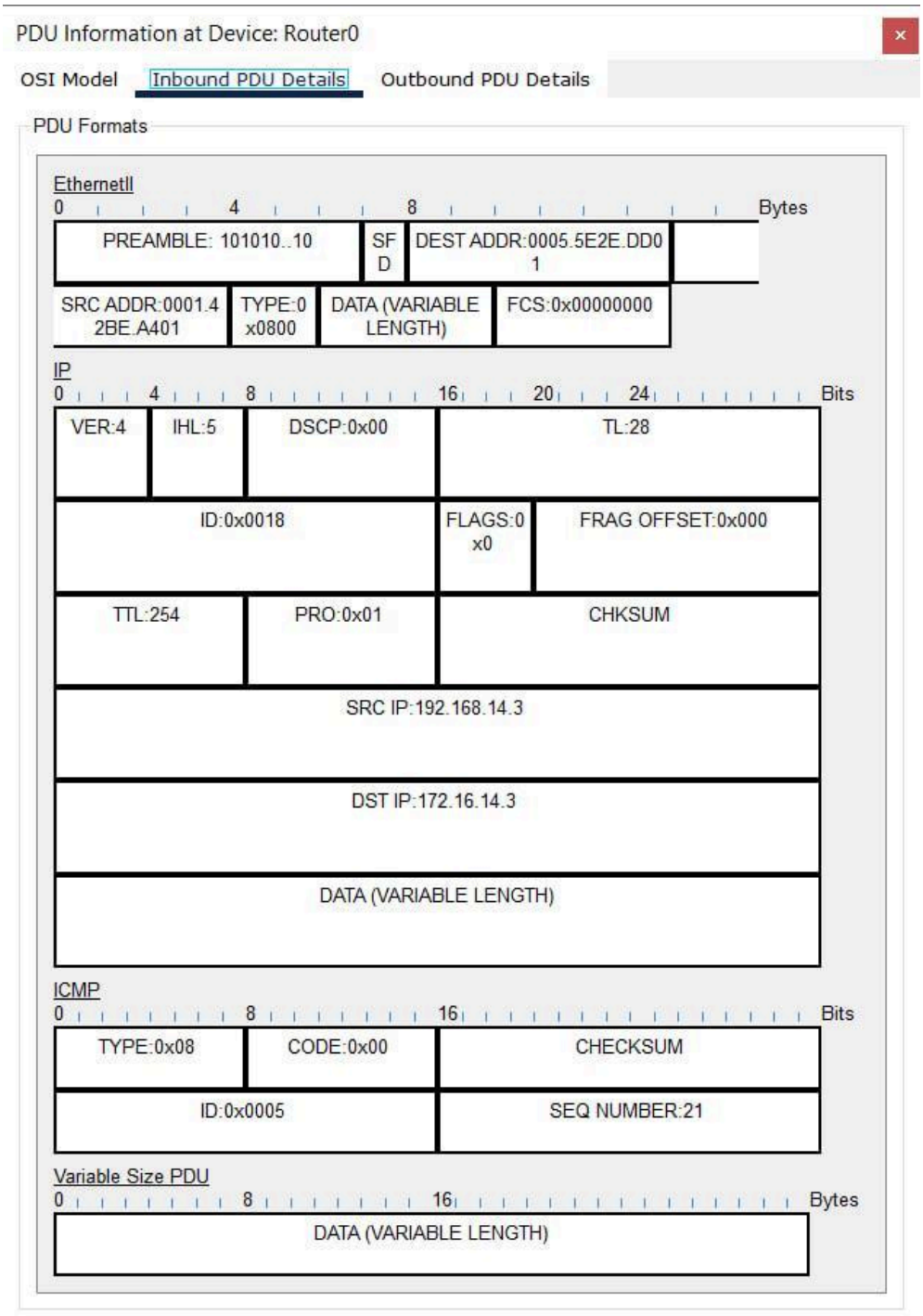


Рисунок 3.25 — Структура пакета Inbound PDU

Ethernet II є однією з найбільш поширених форматів кадрів для передачі даних у локальних мережах (LAN). Він є основою для багатьох сучасних мереж і включає в себе структуру, яка дозволяє ідентифікувати відправника та отримувача, а також визначати тип протоколу на наступному рівні.

Поля Ethernet II:

- Preamble (Преамбула): Початковий код для синхронізації приймача. Складається з 7 байт зі значенням "10101010" і 1 байта зі значенням "10101011". Використовується для підготовки приймача до прийняття пакета.
- DEST ADDR (MAC-адреса призначення): Фізична адреса отримувача пакета. MAC-адреса — унікальний ідентифікатор мережевого інтерфейсу для доставки пакетів між пристроями.
- SRC ADDR (MAC-адреса джерела): Містить MAC-адресу відправника для ідентифікації джерела пакета, важливо для зворотного зв'язку.
- TYPE: Поле визначає тип протоколу, який інкапсульований у кадрі Ethernet. Значення 0x0800 вказує, що в кадрі міститься протокол IPv4. Інші типи включають, наприклад, 0x86DD для IPv6, або 0x0806 для ARP (Address Resolution Protocol).

Поля IP-протоколу:

- SRC IP (IP-адреса джерела): Адреса відправника пакета (192.168.14.3). Ця адреса використовується для зворотного зв’язку або відповіді на запит.
- DST IP (IP-адреса призначення): Адреса отримувача пакета (172.16.14.3). Визначає кінцевий пункт призначення пакета в мережі.

ICMP (Internet Control Message Protocol) — це протокол для обміну діагностичними повідомленнями, що працює поверх IP. Він використовується для повідомлення про помилки і перевірки доступності пристроїв у мережі.

Поля ICMP-протоколу:

- TYPE (Тип повідомлення): Поле визначає тип ICMP повідомлення. Значення 0x08 означає Echo Request, тобто запит на відгук (ping), що використовується для перевірки доступності пристрою в мережі.
- SEQ NUMBER (Номер запиту): Поле містить порядковий номер конкретного запиту ICMP. Номер запиту використовується для того, щоб відрізняти різні запити один від одного та відслідковувати, на який саме запит було отримано відповідь. Це корисно для аналізу часу відповіді та виявлення можливих затримок або втрат пакетів у мережі.

Outbound PDU (Protocol Data Unit) — це структура даних, яка передається з вихідного пристрою (у цьому випадку Router0). Вона містить три основні рівні протоколів: HDLC, IP, та ESP Header. Нижче подано детальний розбір цих рівнів і їхніх полів із поясненнями термінів (Рисунок 3.26).

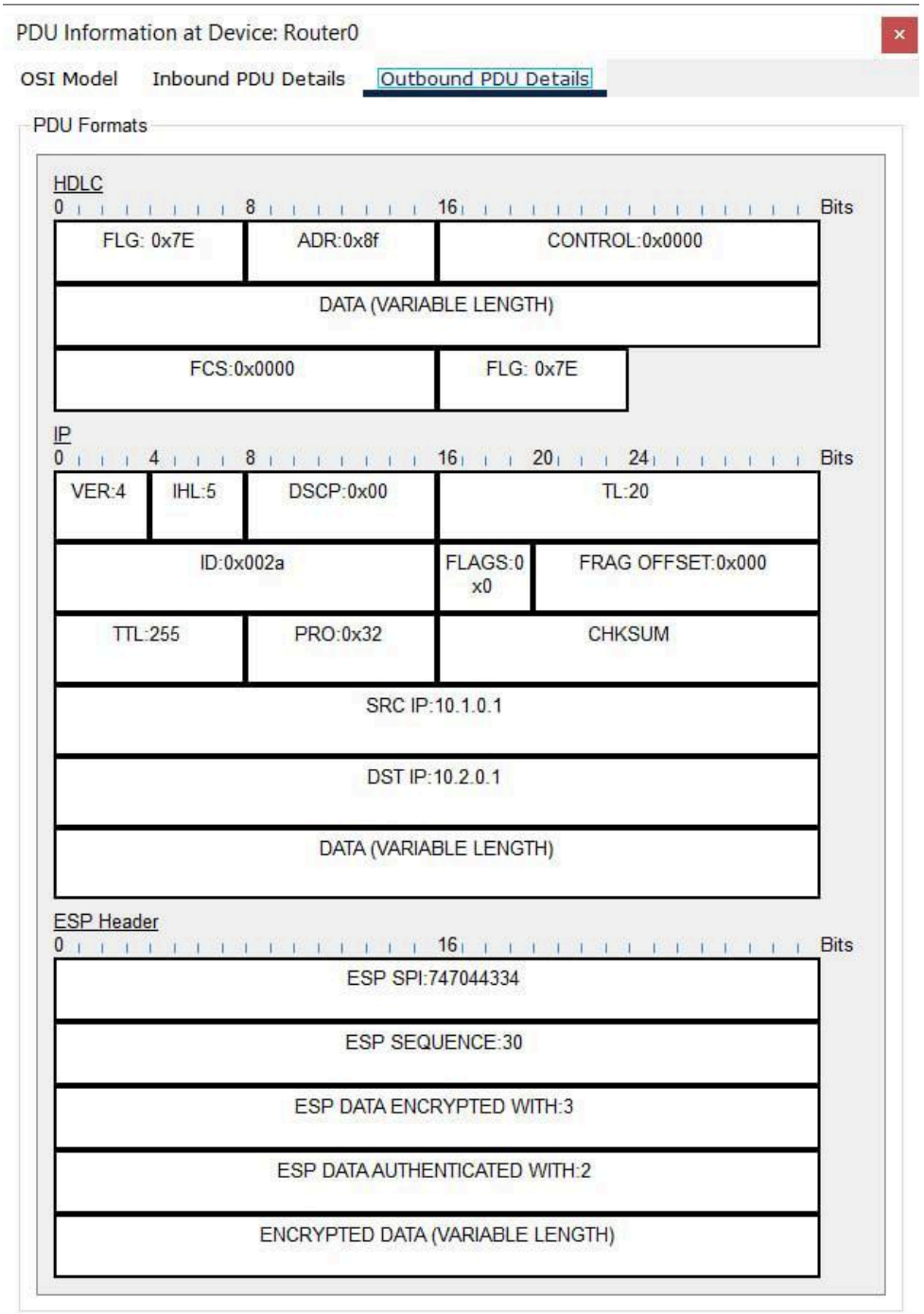


Рисунок 3.26 — Структура пакета Outbound PDU

HDLC (High-Level Data Link Control) — це протокол канального рівня (рівень 2 моделі OSI), який забезпечує надійну передачу даних між вузлами. Його основні функції — кадрування (організація даних у кадри), виявлення помилок і управління потоком даних.

Поля HDLC:

- FLG (Flag): Спеціальний символ, що позначає початок і кінець кадру в HDLC. Він є унікальним для протоколу, що дозволяє приймачу визначити межі кадру. Усі кадри HDLC починаються і закінчуються цим символом. Його наявність дозволяє уникнути непорозумінь в процесі прийому даних, оскільки флаг є унікальним та не використовується в інших частинах кадру.
- ADR (Address): Адреса відправника або одержувача. Це поле вказує, хто є кінцевим вузлом передачі даних (наприклад, комп'ютер або маршрутизатор). Значення в полі адреси дозволяє обчислити, куди повинні бути надіслані дані.
- CONTROL: Поле визначає тип кадру (наприклад, кадр запиту або підтвердження). Поле також визначає поведінку в процесі обміну даними: чи має місце запит на отримання підтвердження або чи передаються дані без зворотного зв'язку.
- DATA (Variable Length): Основне поле для передачі даних. Це місце, де надаються самі дані, які обробляються в межах протоколу. Довжина цього поля може варіюватися в залежності від розміру даних. В залежності від протоколу, вміст даного поля може мати різні формати (наприклад, текст, числа, або інші типи інформації).
- FCS (Frame Check Sequence): Використовується для перевірки цілісності кадру. FCS є результатом обчислення контрольної суми даних, що знаходяться в кадрі. Якщо FCS на приймальному боці не співпадає з очікуваним значенням, це вказує на помилку в передачі і кадр відкидається. Помилки можуть бути викликані різними факторами, такими як шум, неполадки в апаратному забезпеченні або інші проблеми в каналі передачі.

IP (Internet Protocol)— це протокол, що працює на мережевому рівні моделі OSI і відповідає за логічну адресацію, маршрутизацію та доставку даних між

різними мережами. IP визначає, як пакети передаються між різними пристроями в мережі, забезпечуючи безпечну доставку даних навіть через кілька проміжних мереж.

Поля IP-протоколу:

- VER (Version): Вказує на версію IP-протоколу. В даному випадку значення 4 означає, що це протокол IPv4, що є найбільш поширеним на сьогодні.
- IHL (Internet Header Length): Поле вказує на довжину заголовка IP. Оскільки заголовок може включати різні опції, поле IHL дозволяє визначити його фактичну довжину. Якщо в заголовку є додаткові опції, то довжина заголовка збільшується.
- DSCP (Differentiated Services Code Point): Поле використовується для маркування пакету з метою управління якістю обслуговування (QoS). Значення 0x00 вказує на стандартну обробку трафіку без пріоритетів. В залежності від значення DSCP пакети можуть мати пріоритет у мережі, що може впливати на швидкість і якість їх доставки.
- TL (Total Length): Загальна довжина пакету, що включає як заголовок, так і корисні дані. Поле визначає розмір пакету для коректної передачі та обробки. Важливо для коректної маршрутизації та для обмеження максимальної довжини пакету в мережі.
- ID (Identification): Унікальний ідентифікатор для кожного пакету, що дозволяє відновити фрагментовані пакети. Якщо IP-пакет фрагментується, кожен фрагмент має однакове значення в полі ID, що допомагає приймачу правильно зібрати фрагменти в один пакет.
- FLAGS: Керує фрагментацією пакета. В нашому випадку фрагментація вимкнена (0x0).
- TTL (Time-to-Live): Це поле визначає максимальну кількість хопів (маршрутизаторів), через які може пройти пакет. Кожен маршрутизатор зменшує TTL на 1. Якщо TTL досягає нуля, пакет відкидається. TTL допомагає запобігти нескінченним циклам у разі неправильного маршрутування пакетів.

- PRO (Protocol): Вказує, який протокол використовувався для транспортування даних. В нашому випадку 0x32 вказує на протокол ESP (Encapsulating Security Payload).
- SRC IP: Логічна адреса відправника пакета(10.1.0.1). Поле SRC IP визначає, звідки прийшов пакет. Воно використовується для зворотної маршрутизації і для з'ясування, якому пристрою потрібно відповісти.
- DST IP: Логічна адреса одержувача пакета (10.2.0.1). Це поле визначає, куди повинен бути доставлений пакет. У разі маршрутизації пакет передається через проміжні маршрутизатори до місця призначення.

ESP Header (Encapsulating Security Payload) є частиною протоколу IPsec, який забезпечує шифрування та аутентифікацію даних для захисту.

Поля ESP Header:

- ESP SPI (Security Parameters Index): Унікальний ідентифікатор параметрів безпеки для з'єднання, що дозволяє приймачу визначити використовувану криптографічну політику для шифрування та аутентифікації.
- ESP Sequence: Це поле вказує на порядковий номер пакета, що допомагає запобігти атакам повторного використання пакетів (30). При кожному новому пакеті його порядковий номер збільшується, що дозволяє однозначно ідентифікувати його місце в загальній послідовності. Це важливо для підтримки цілісності переданих даних.
- ESP DATA ENCRYPTED: Всі дані в межах IPSec тунелю шифруються, щоб запобігти їх доступу сторонніми особами. Це поле містить зашифровану частину пакета, де передаються корисні дані. Шифрування гарантує, що навіть якщо пакет перехопить третя сторона, вона не зможе прочитати його зміст без відповідного ключа дешифрування.
- ESP DATA AUTHENTICATED: Для забезпечення цілісності та автентичності даних використовуються спеціальні механізми автентифікації, такі як HMAC (Hash-based Message Authentication Code). Це поле містить контрольну суму або підпис, що дозволяє перевірити, чи не були дані змінені в процесі передачі (2).

- ENCRYPTED DATA (Variable Length): Це основна частина пакета, яка містить зашифровані дані, передані через IPSec тунель. Всі дані, що передаються в тунелі, захищаються від несанкціонованого доступу за допомогою криптографічних алгоритмів, що гарантує конфіденційність та цілісність.

Підсумовуючи, можна сказати, що налаштований IPSec тунель працює правильно і ефективно забезпечує захист переданих даних. Симуляція в Cisco Packet Tracer підтвердила, що всі необхідні поля присутні в пакеті і містять правильні значення. Це свідчить про те, що всі механізми шифрування та автентифікації працюють належним чином. Тунель шифрує дані, ідентифікує їх і забезпечує їх цілісність, що гарантує конфіденційність та безпеку переданої інформації. Отже, протокол IPSec в нашій моделі працює як і було передбачено.

3.5 Аналіз переваг та недоліків створеної системи

Після проведеного моделювання розподіленої корпоративної мережі за допомогою Cisco Packet Tracer, отримано результати, які дають змогу оцінити ефективність створеної системи. Аналіз результатів моделювання дозволяє визначити основні переваги та недоліки мережі, виявити можливі проблеми, що можуть виникнути під час експлуатації, а також спланувати заходи для покращення її роботи. Окрему увагу було приділено таким критичним аспектам, як затримки та втрати пакетів, що можуть значно вплинути на якість роботи мережі, а також рівень відмовостійкості системи, що є важливим для забезпечення її стабільності в умовах реальної експлуатації.

Під час моделювання було виявлено кілька ключових переваг створеної мережі. Однією з основних переваг є масштабованість мережі. Це означає, що можна легко додавати нові пристрої та сегменти, не впливаючи на стабільність роботи інших частин мережі. Завдяки правильно налаштованій маршрутизації, мережа здатна ефективно використовувати наявні ресурси, що забезпечує високу

пропускну здатність в межах локальних сегментів. Також варто відзначити централізоване управління мережею, яке дозволяє швидко реагувати на зміни та проводити моніторинг її роботи.

Однак, крім переваг, є й певні недоліки, які були виявлені під час тестування. По-перше, мережа має обмежену відмовостійкість. У разі виходу з ладу одного з ключових компонентів, таких як маршрутизатор чи канал зв'язку, є ризик, що частина мережі може вийти з ладу, що призведе до зупинки обміну даними між деякими підсистемами (Рисунок 3.27). Крім того, в умовах пікових навантажень спостерігаються деякі проблеми з затримкою передачі даних, а також з незначними втратами пакетів, що може негативно впливати на роботу критичних додатків.

```
Router#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.1.0.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.1.0.0/30 is directly connected, Serial0/0/0
L       10.1.0.1/32 is directly connected, Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
S    192.168.11.0/24 [1/0] via 192.168.10.2
S    192.168.12.0/24 [1/0] via 192.168.10.2
S    192.168.13.0/24 [1/0] via 192.168.10.2
S    192.168.14.0/24 [1/0] via 192.168.10.2
S    192.168.15.0/24 [1/0] via 192.168.10.2
S    192.168.16.0/24 [1/0] via 192.168.10.2
S    192.168.17.0/24 [1/0] via 192.168.10.2
S*   0.0.0.0/0 [1/0] via 10.1.0.2
```

Рисунок 3.27 — Поточна маршрутизація маршрутизатора Router0

Одним із важливих аспектів, який був оцінений під час моделювання, є затримка в мережі. Затримка — це час, необхідний для передачі даних від одного пристрою до іншого. У випадку локальних сегментів мережі затримка зазвичай не перевищує 10 мс, що є оптимальним значенням для більшості стандартних

додатків. Однак у випадку передачі даних через віддалені сегменти мережі, особливо через VPN, затримка може досягати 40-50 мс (Рисунок 3.28). Це вже значне значення, яке може вплинути на якість додатків, чутливих до затримок, таких як голосовий зв'язок або відеоконференції.

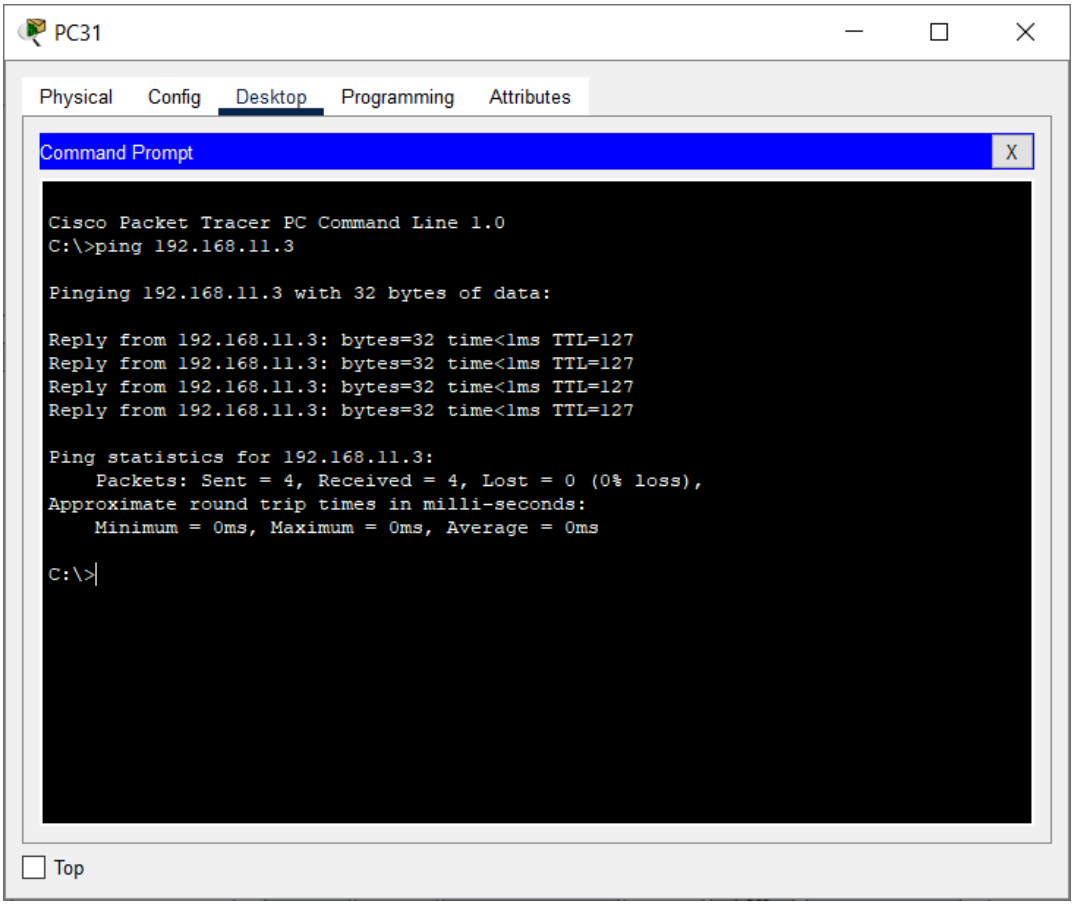


Рисунок 3.28 — Результат ICMP запитів між пристроями центрального офісу

Втрата пакетів — ще один важливий параметр, що безпосередньо впливає на ефективність роботи мережі. Під час тестування було зафіксовано невеликі втрати пакетів, які у найгіршому випадку становили до 2%. Ці втрати можуть бути незначними для більшості типів трафіку, однак для чутливих до втрат пакетів додатків, таких як VoIP або відео, це може створити проблеми. Найбільші втрати спостерігалися в періоди високих навантажень, коли мережа була завантажена великими обсягами даних.

Під час моделювання стало очевидно, що мережа працює досить стабільно в умовах середнього навантаження, однак для забезпечення високої відмовостійкості та стабільної роботи в реальних умовах необхідно вжити кілька заходів. Одним із таких заходів є створення резервних каналів зв'язку та маршрутизаторів. Якщо один із компонентів мережі виходить з ладу, система повинна мати можливість автоматично переключатися на резервні канали, що дозволить мінімізувати час простоя та забезпечити безперервність роботи.

На основі проведеного моделювання можна зробити кілька важливих висновків щодо ефективності та надійності розробленої мережі. Мережа в цілому працює стабільно та ефективно в умовах середнього навантаження, однак є кілька аспектів, які потребують вдосконалення. По-перше, для підвищення відмовостійкості необхідно передбачити резервні канали зв'язку та маршрутизатори. По-друге, для зменшення затримок та втрат пакетів потрібно впровадити механізми пріоритетизації трафіку та налаштувати маршрутизацію таким чином, щоб знизити навантаження на основні вузли мережі. Це дозволить забезпечити стабільну роботу мережі в умовах високих навантажень та мінімізувати ймовірність виникнення проблем з продуктивністю.

Загалом, результати моделювання показали, що розроблена мережа здатна ефективно виконувати свої функції при звичайних умовах експлуатації, але для покращення її роботи та забезпечення безперебійної роботи в реальних умовах слід вжити додаткових заходів для підвищення надійності та продуктивності.

ВИСНОВОК

У даній магістерській роботі було здійснено комплексне дослідження принципів побудови розподілених мереж з акцентом на використання сучасних протоколів безпеки, зокрема IPSec. У роботі було проаналізовано вибір концепції мережі, її структуру, стандарти та протоколи, а також розглянуті особливості планування та побудови мультисервісних мереж.

У першому розділі було детально розглянуто вибір концепції розподіленої корпоративної мережі та визначення її структури. Це стало основою для подальшого проектування мережі, зокрема для вибору топології та аналізу стандартів і протоколів. Важливим моментом було впровадження протоколу IPSec для забезпечення високого рівня захисту переданої інформації. Його використання дозволяє створювати безпечні VPN-з'єднання для віддалених філій підприємства, що гарантує цілісність та конфіденційність даних при передачі через Інтернет або інші ненадійні канали зв'язку.

Другий розділ роботи був присвячений особливостям проєктування мультисервісної мережі, яка дозволяє ефективно інтегрувати різні види трафіку, такі як голосовий, відео та дані, що значно підвищує функціональність мережі. Описувалося обладнання для створення мультисервісної мережі, включаючи маршрутизатори, комутатори, міжмережеві екрани та телекомунікаційні сервери. Ці компоненти дозволяють забезпечити високу швидкість передачі даних і надійність мережі, а також підтримку різних сервісів, які є важливими для роботи корпоративної мережі.

У третьому розділі було розроблено логічну структуру корпоративної мережі, включаючи моделювання розподіленої мережі за допомогою емулятора Cisco Packet Tracer. Використання цього програмного забезпечення дозволило візуалізувати взаємодію компонентів мережі, налаштувати маршрутизатори і комутатори, а також реалізувати захищені з'єднання з використанням IPSec. Модель мережі включала маршрутизатори для забезпечення з'єднання між

віддаленими офісами компанії, комутатори для налаштування локальних мереж, а також сервери для зберігання і обробки даних.

Моделювання мережі в Cisco Packet Tracer дозволило створити ефективну і безпечну корпоративну мережу, що відповідала вимогам сучасних технологій. Важливим аспектом стало використання IPSec для захищеного обміну даними між віддаленими філіями. Це рішення забезпечило конфіденційність і цілісність переданих даних, що є критично важливим для функціонування розподілених корпоративних мереж.

У результаті виконаної роботи було розроблено ефективну модель розподіленої корпоративної мережі, що враховує всі важливі аспекти проектування, включаючи вибір концепції мережі, структуру, стандарти та протоколи, а також методи забезпечення безпеки. Використання протоколу IPSec для захищених з'єднань між віддаленими офісами стало ключовим елементом для забезпечення конфіденційності та цілісності переданих даних, що є критично важливим у сучасних умовах. Моделювання мережі в Cisco Packet Tracer дозволило візуалізувати та тестувати усі етапи реалізації мережевої інфраструктури, що забезпечує її надійність і стабільність.

Отримані результати підтверджують, що за допомогою сучасних технологій і підходів можна створити надійну і безпечну корпоративну мережу, яка здатна ефективно функціонувати в умовах високих вимог до безпеки та масштабованості. Розроблена модель мережі може бути використана як основа для подальших практичних розробок і впровадження в реальних умовах, що дозволить значно підвищити ефективність управління та захисту корпоративних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Валецька Т. М. Комп'ютерні мережі. Апаратні засоби / Т. М. Валецька. – Київ : Центр навчальної літератури, 2004. – 208 с.

2. Forouzan B. Data Communications and Networking / Behrouz Forouzan, Behrouz A. Forouzan. – 3-тє вид. – [Б. м.] : McGraw-Hill Science/Engineering/Math, 2003. – 973 с.

3. Characterizing VLAN usage in an operational network / P. Garimella та ін. the 2007 SIGCOMM workshop, м. Kyoto, Japan, 27—31 серп. 2007 р. New York, New York, USA, 2007. URL: https://doi.org/10.1145/1321753.1321772

4. Virtual private network [Електронний ресурс] // cisco.com. – Режим доступу: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

5. MPLS fundamentals. Indianapolis, Ind : Cisco Press, 2007. 626 с.

6. Implementing the ISO / IEC 27001 ISMS standard. – [Б. м.] : Artech House, 2016. – 222 с.

7. ITU-T Recommendations [Електронний ресурс] // ITU. – Режим доступу: https://www.itu.int/en/ITU-T/publications/pages/recs.aspx

8. Pujolle G. Architecture TCP/IP [Електронний ресурс] / Guy Pujolle // Réseaux télécommunications. – 1997. – Режим доступу: https://doi.org/10.51257/a-v1-h2288

9. Dunbar N. IPsec networking standards – an overview [Електронний ресурс] / Neil Dunbar // Information security technical report. – 2001. – Т. 6, № 1. – С. 35–48. – Режим доступу: https://doi.org/10.1016/s1363-4127(01)00106-6

10. Point-to-Point tunneling protocol (PPTP) [Електронний ресурс] / K. Hamzeh [та ін.]. – [Б. м.] : RFC Editor, 1999. – Режим доступу: https://doi.org/10.17487/rfc2637

11. Silva A. L. d. S. Protocolo http x protocolo https [Електронний ресурс] / André Luis de Souza Silva, Regina Célia Marques Freitas Silva // Nucleus. – 2009. – Т. 6, № 1. – С. 85–92. – Режим доступу: https://doi.org/10.3738/1982.2278.146

12. Navarro M. Automatic OSPF Topology map generation using information of the OSPF database [Електронний ресурс] / Manuel Navarro, José Carlos Rangel, Edmanuel Cruz // KnE engineering. – 2018. – Т. 3, № 1. – С. 853. – Режим доступу: https://doi.org/10.18502/keg.v3i1.1506

13. Організація комп'ютерних мереж [Електронний ресурс]. – Режим доступу: https://kremenetskyy.blogspot.com/2017/10/blog-post.html

14. IDS/IPS [Електронний ресурс] // techukraine.net. – Режим доступу: https://techukraine.net/8-інструментів-ids-та-ips-для-кращого-аналізу

15. CCNA routing and switching portable command guide. – [Б. м.] : Cisco Press, 2016. – 364 с.

16. About Firewalls [Електронний ресурс] // checkpoint.com. – Режим доступу: https://www.checkpoint.com/cyber-hub/network-security/what-isfirewall/

17. DDoS-атака [Електронний ресурс] // eset.com.ua. – Режим доступу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/

18. Authentication [Електронний ресурс] // techtarget.com. – Режим доступу: https://www.techtarget.com/searchsecurity/definition/authentication

19. Поліщук А. В. Дослідження методів і засобів захисту інформації в корпоративних мережах [Електронний ресурс] : thesis / Поліщук Андрій Віталійович, Polishchuk Andrew. – [Б. м.], 2013. – Режим доступу: http://elartu.tntu.edu.ua/handle/123456789/2677

20. Doraswamy N., Harkins D. IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks. Prentice Hall PTR, 2003. 288 с.

21. Bollapragada V., Wainner S., Khalid M. IPSec VPN design. Cisco Press, 2005.

22. KAMİLOGLU M. E. Cisco Network Performance Evaluation Using Packet Tracer. International Journal of Electronics, Mechanical and Mechatronics

Engineering. 2015. T. 5, № 1. C. 905–911. URL: https://doi.org/10.17932/iau.ijemme.m.21460604.2015.5/1.905-911

23. Ramli A., Sriyono S., Ramza H. Analisa Kecepatan Lalu Lintas Data Jaringan Local Area Network Menggunakan Graphical Network Simulator 3 (GNS-3). Electrical Engineering Acta. 2021. T. 1, № 1. C. 13–19. URL: https://doi.org/10.22236/ate.v1i1.6946

24. Воропаєва К. А. Огляд способів організації VLAN : thesis. 2020. URL: http://openarchive.nure.ua/handle/document/13958

25. LAURENT-MAKNAVICIUS M. Protocole IPsec. Sécurité des systèmes d'information. 2003. URL: https://doi.org/10.51257/a-v1-te7545

ДОДАТОК А

1.1 Selection of the Network Concept

The selection of the network concept is one of the most critical stages in the design process of a distributed corporate network. This process requires a comprehensive analysis of data transmission needs, technical specifications, and operating conditions. A properly chosen concept should ensure reliable and secure functioning of telecommunication services and efficient information exchange between various company departments.

Today, corporate networks must be capable of adapting to a rapidly changing environment, taking into account factors such as the growing mobility of employees, the need for remote access to corporate resources, and the use of cloud technologies. The selection of the network concept must also address potential cybersecurity threats that could compromise data integrity and confidentiality.

When choosing a network concept, it is essential to define the primary requirements it must meet, including:

- Security: Ensuring reliable data protection and secure network access.
- Performance: Guaranteeing the speed and reliability of communication between all departments.
- Scalability: Providing the ability to easily expand the network in response to growing needs.
- Cost-effectiveness: Selecting solutions that meet the organization’s budget constraints without compromising quality.

The choice of a network concept should result from thorough analysis and be based on the integration of various aspects such as technological innovations, business requirements, and future development trends. This approach will ensure not only the

stability and efficiency of the corporate network but also its adaptability to changing conditions.

Local Area Network (LAN)

A LAN (Local Area Network) is a network that connects computers and other devices within a limited geographical area, such as a building, office, or campus. A LAN allows users to share files, access resources (e.g., printers, servers), and utilize network devices collectively (Figure 1.1). A LAN can be established using various types of connections, including Ethernet, Wi-Fi, and other technologies designed to enable communication over short distances [1].

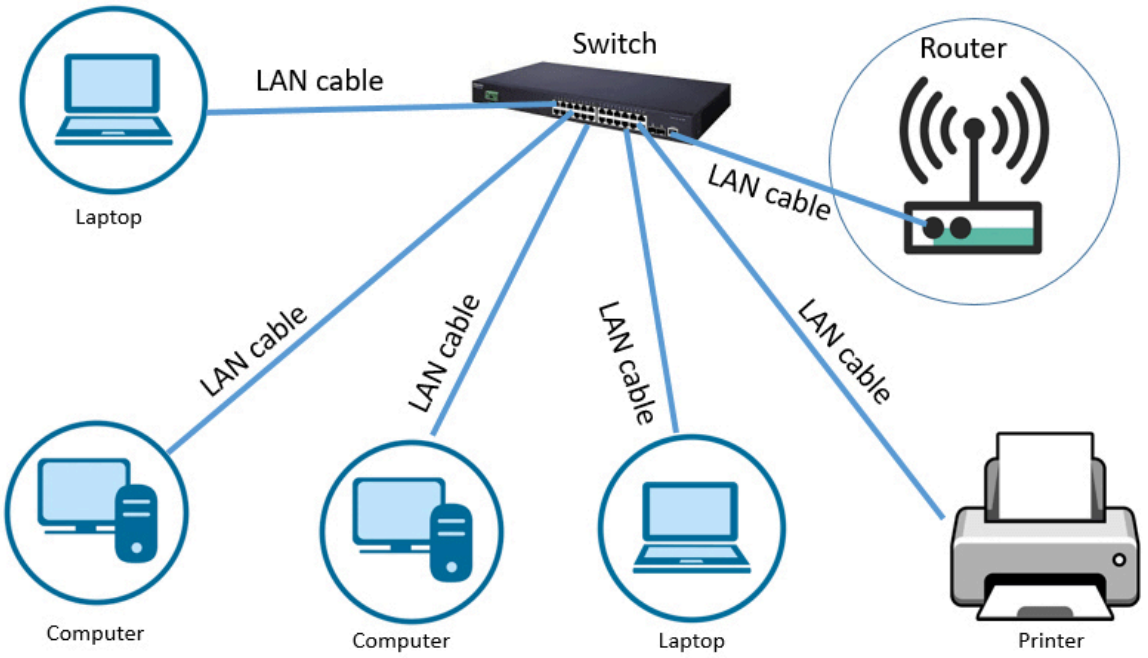


Figure 1.1 — Local Area Network

A LAN (Local Area Network) forms the foundation for organizing an internal network within a company, school, university, or any other environment where the exchange of information between devices within a single building or campus is required. It enables computers to connect to the network for access to shared resources,

such as printers, files, and databases. Additionally, a LAN can be used to create internal websites or facilitate internal communication, simplifying organizational workflows.

Advantages of LAN:

- Speed and Efficiency: A LAN provides fast connections and high-speed data transmission between devices over short distances.
- Low Cost: Compared to a WAN, a LAN has lower costs for equipment and installation, as it uses affordable communication technologies.
- Ease of Management: A local network typically involves fewer devices and is simpler to configure and maintain, reducing the complexity of network infrastructure management.
- Resource Sharing Capabilities: All devices within the network can share access to files, printers, and other resources, significantly improving operational efficiency.

Disadvantages of LAN:

- Limited Coverage: A LAN operates over limited distances, restricting its use in large or remote premises.
- Dependence on Physical Infrastructure: Reliable LAN operation requires the installation of cables (Ethernet) or stable Wi-Fi coverage, which can pose challenges in large buildings or outdated networks.
- Vulnerability to Failures: Physical damage to the network infrastructure or equipment malfunctions can impact the entire network's operation.

A LAN is a core technology for network organization within a single building or campus. It provides high data transmission speeds, efficient resource utilization, and ease of management. However, its coverage is typically limited to a few dozen or hundreds of meters. Considering its low cost and ease of setup, a LAN is an ideal solution for most small and medium-sized organizations.

Wide Area Network (WAN)

A WAN (Wide Area Network) is a network that spans large geographical areas, connecting various local area networks (LANs) and enabling them to exchange data over long distances (Figure 1.2). A WAN can connect company branches located in

different cities, countries, or continents. These networks are used for information exchange between offices and for providing access to centralized company resources, such as servers or databases.

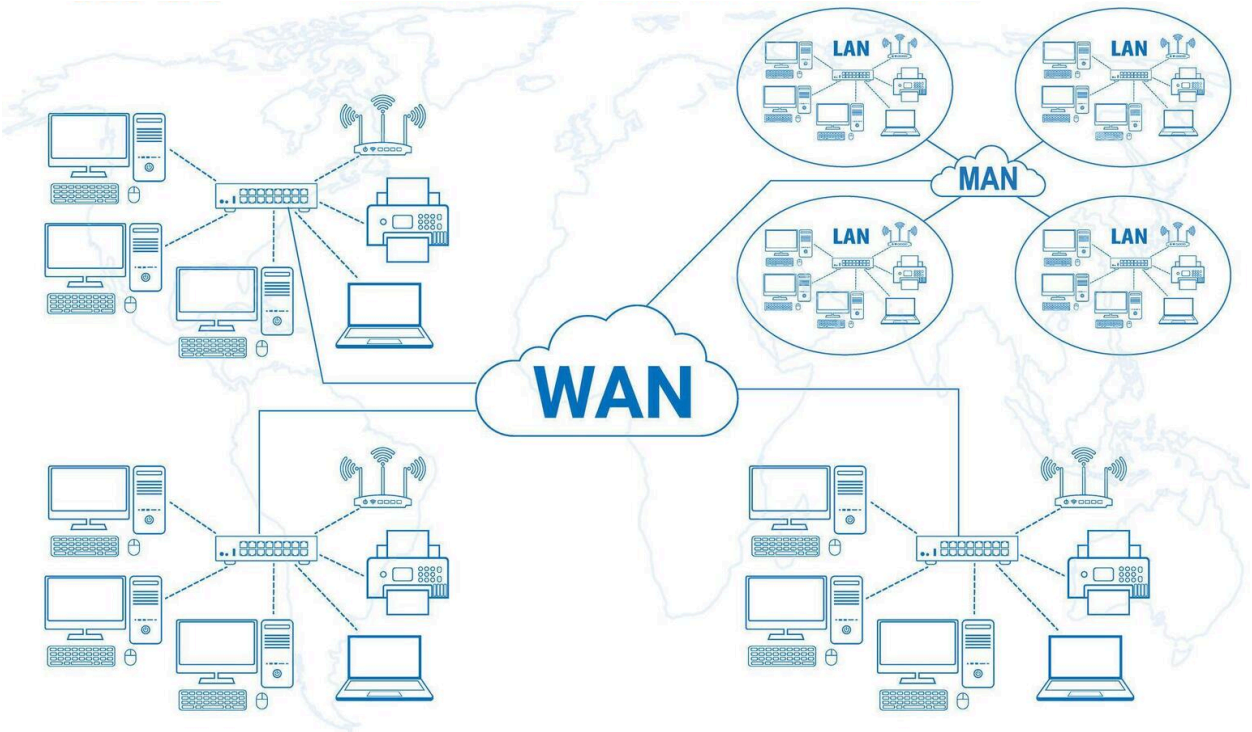


Figure 1.2 — Wide Area Network

WAN enables organizations to efficiently connect remote offices, operating them as a unified network. This can include remote access to corporate systems, the transfer of large volumes of data, or establishing connectivity between multiple offices. WAN also allows companies to use centralized servers for data storage, reducing the need for local resources [2].

Advantages of WAN:

- Wide Coverage: WAN allows the connection of offices or branches located across vast distances.
- Cost Savings on Infrastructure: All remote branches can connect to a single central server or database, reducing the need for local systems.

- Scalability: WAN can be easily expanded to cover new geographical regions, making it ideal for international companies.

Disadvantages of WAN:

- Cost: Long-distance connections, especially between continents, can be expensive, particularly when using dedicated communication channels.
- Low Bandwidth: WAN may have limited bandwidth, leading to higher latency and slower data transmission.
- Reliability Issues: Since WAN relies on multiple connections and providers, failures in any component can cause connectivity issues.

WAN is an indispensable tool for organizations with multiple offices or branches worldwide. However, its high cost and potential challenges with bandwidth or reliability require careful planning and the selection of optimal connectivity solutions.

Virtual Local Area Networks (VLAN)

VLAN (Virtual Local Area Network) is a technology that allows a single physical network to be logically divided into multiple isolated segments (Figure 1.3). Each VLAN segment functions as a separate network, even if devices belonging to different VLANs are physically located within the same network point. This enables administrators to segregate networks for different departments, services, or projects without the need to lay additional cables. VLANs also facilitate efficient traffic management, optimizing resource utilization and enhancing security.

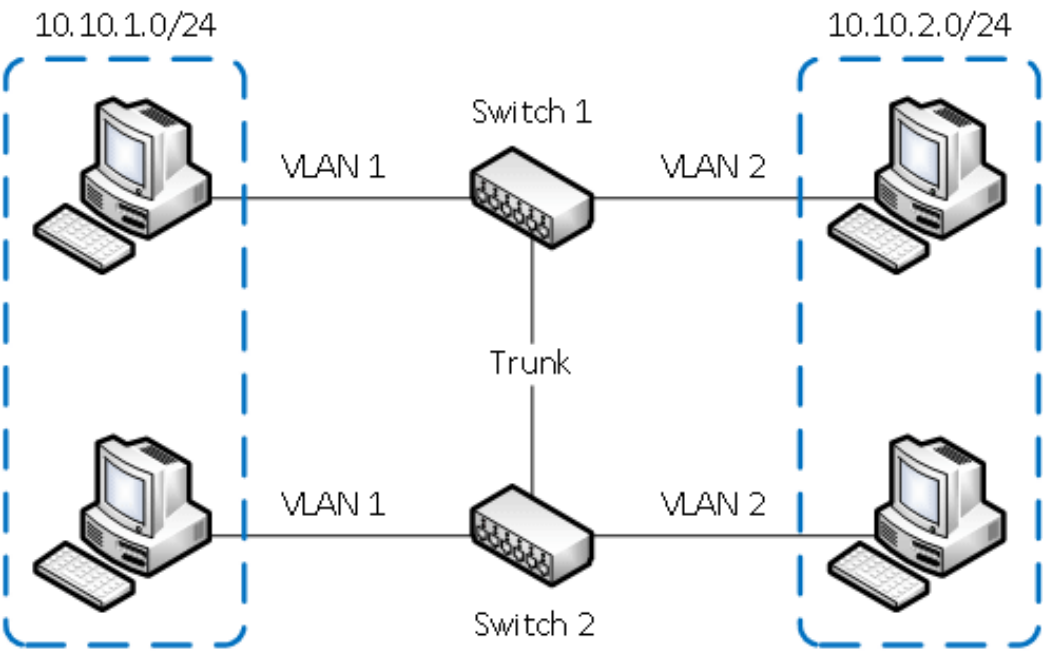


Figure 1.3 — Example of VLAN

VLANs are used to reduce network load, improve performance, enhance security, and simplify management. They allow the creation of logical subnets for various organizational functions, such as departments, without the need to modify the physical infrastructure. For instance, an administrative department can have its own VLAN, which is isolated from the VLANs of financial or production departments [3].

Advantages of VLAN:

- Traffic Segmentation: VLANs divide the network into different logical segments, improving traffic management and enhancing performance by reducing collisions.
- Enhanced Security: Network isolation restricts access to sensitive data or systems to users or devices within specific VLANs.
- Reduced Network Traffic: VLANs limit broadcast traffic to specific segments, reducing overall network load.
- Flexibility and Scalability: VLANs enable changes to network topology without requiring physical reconfiguration. This makes more efficient use of existing infrastructure.

- Improved Management: Logical traffic distribution helps manage network resources better, such as setting priorities for specific types of traffic.

Disadvantages of VLAN:

- Configuration Complexity: Setting up VLANs can be challenging, especially in large networks where segmentation logic needs careful planning.
- Management Limitations: Poor VLAN management may result in access issues, such as incorrect routing between VLANs.
- Need for Additional Devices: Implementing VLANs often requires switches that support this technology, increasing equipment costs.
- Element-Level Security Risks: While VLANs enhance security, they are not entirely foolproof. Specialized attacks, such as VLAN hopping, can allow attackers to access data across VLANs.

VLANs are a critical tool for network segmentation, providing enhanced security, reduced traffic load, and improved network management. However, achieving the best results requires proper configuration and technical support, which can be challenging in large or complex infrastructures.

Virtual Private Networks (VPN)

VPN (Virtual Private Network) refers to technologies that provide secure access to private networks over public internet connections (Figure 1.4). VPN enables the creation of secure connections through public networks (e.g., the Internet), allowing users to access corporate resources as if they were connected to a local network. VPN uses encryption to ensure the confidentiality of transmitted data and provides anonymity, which is crucial when accessing sensitive or confidential information systems [4].

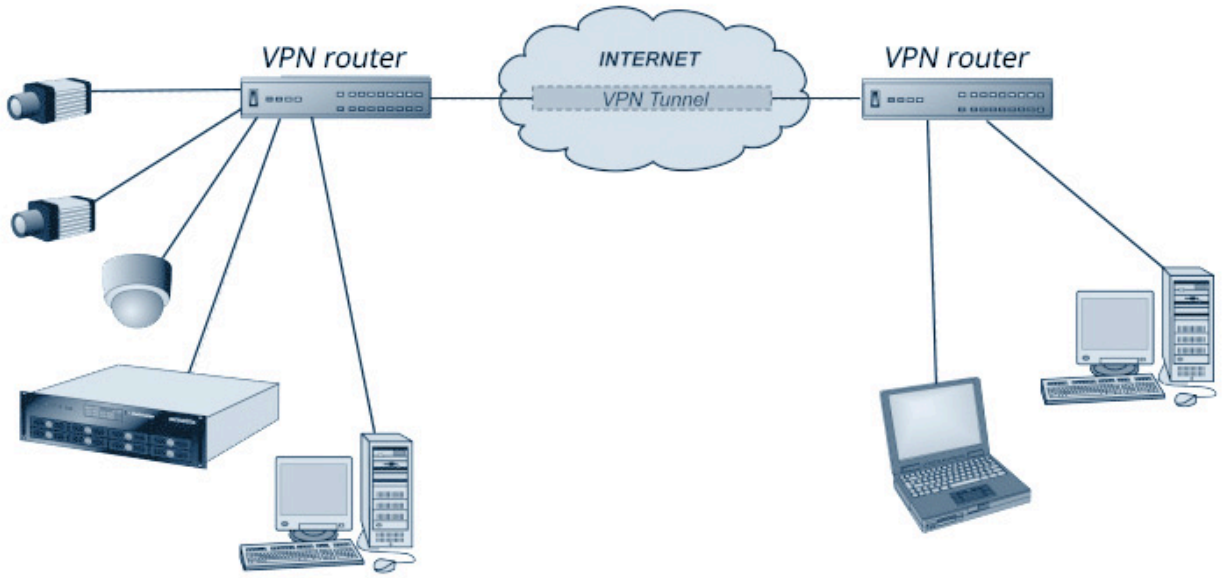


Figure 1.4 — VPN Connection Diagram

VPN is commonly used to provide secure remote access to corporate networks, especially for employees working from home or other remote locations. VPN also allows secure data transmission between two remote networks, which is crucial for protecting information from interception when users connect to public Wi-Fi networks.

Advantages of VPN:

- Data Security: VPN encrypts all traffic, providing protection against interception and attacks.
- Remote Access: VPN allows remote workers or branches to access corporate resources as if they were within the local network.

Disadvantages of VPN:

- Data Transfer Delays: Using a VPN can lead to increased latency due to encryption and traffic routing through additional servers.
- Configuration Complexity: Setting up a VPN requires specialized knowledge, which may be a barrier for some organizations.

VPN is an important tool for ensuring security and confidentiality when accessing networks remotely. Although it may slow down internet connections, its advantages in data protection far outweigh these drawbacks.

Multiprotocol Label Switching (MPLS)

MPLS (Multiprotocol Label Switching) is a powerful technology that enables efficient data routing in large and complex networks (Figure 1.5). Due to its ability to support different types of traffic and protocols, MPLS has become an essential tool for optimizing network resources and ensuring high-quality service. The technology allows for faster and more efficient data transmission, especially in complex networks with large volumes of traffic.

MPLS supports various protocols and enables the creation of private virtual networks (VPNs), as well as providing a high level of Quality of Service (QoS), which is crucial for businesses that require guaranteed bandwidth and minimal delays [5].

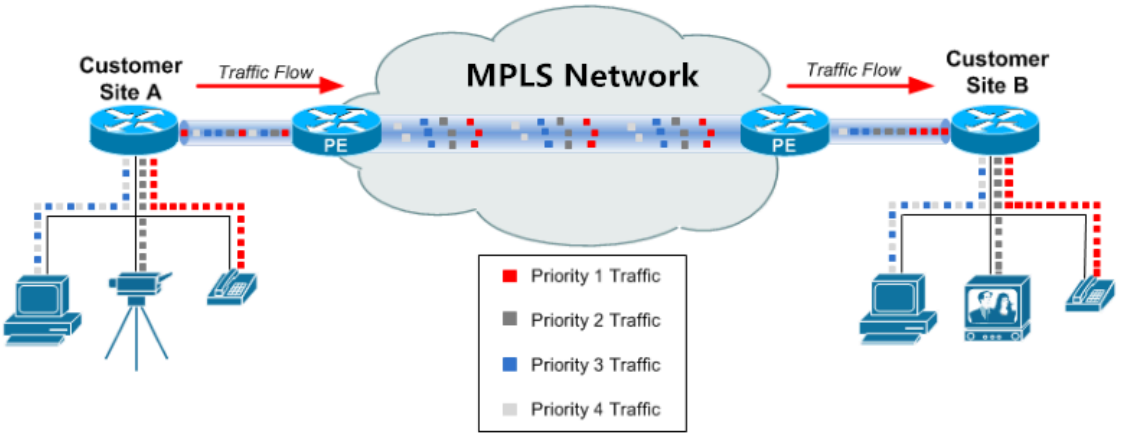


Figure 1.5 — MPLS Network Diagram

MPLS is used to optimize routing and manage network traffic in large corporate or service provider networks. It allows the creation of private virtual networks (VPNs) for remote offices and departments, ensures high-quality data transmission for critical applications such as voice or video transmissions, where low latency and connection stability are important, and optimizes the use of network resources by reducing the need for constant IP packet routing.

Advantages of MPLS:

- Speed and Performance: One of the main advantages of MPLS is its ability to provide high-speed and performance in data routing.
- Flexibility: MPLS offers great flexibility in using various protocols, making it a universal solution for corporate networks.
- Ease of Management and Scalability: MPLS allows for easy network scaling by adding new lines or routes to handle more traffic without major changes to the topology.

Disadvantages of MPLS:

- High Costs: One of the biggest drawbacks of MPLS is the high cost of implementation and operation. Service providers often charge significant fees for connection and monthly services, which can be a barrier for small and medium-sized businesses.
- Complex Setup and Management: Configuring and managing MPLS networks can be complex and require specialized knowledge.
- Lack of Encryption: Although MPLS provides a certain level of security, the absence of built-in encryption mechanisms means that organizations must implement additional encryption to protect data when needed.

MPLS is a powerful and effective tool for ensuring high performance and reliability in large corporate and service provider networks. It is ideal for organizations that require high bandwidth, minimal latency, and stable operation of critical applications. However, the technology requires significant investments in setup and maintenance, which may be impractical for smaller companies.

After a thorough analysis of the advantages and disadvantages of technologies such as VLAN, VPN, and MPLS, a well-founded conclusion can be made regarding the selection of the optimal concept for distributed corporate networks. Although each of these technologies has its own advantages, VPN, despite some drawbacks, proves to be the most effective solution for organizations requiring secure and reliable access to corporate resources.

One of the main advantages of VPN is its ability to provide a high level of security. By encrypting data, VPN protects confidential information from potential threats such as interception or attacks by malicious actors. This is especially important in the context of growing cyber threats, where companies face the risk of data breaches and loss of confidentiality. VPN allows remote workers to confidently access important resources, knowing that their data is protected.

In addition to security, VPN also offers high flexibility. Modern business demands the ability to quickly adapt to changes in the environment, such as remote work or expansion into new markets. VPN allows companies to easily configure access to resources for new users and devices, simplifying the administration process. In an era when many companies are transitioning to hybrid or remote work models, it is essential to have technology that provides convenient access to corporate systems from anywhere in the world.

Another important aspect is cost-effectiveness. The use of VPN can reduce costs associated with communication infrastructure. Unlike MPLS, which requires significant investments in private communication lines, VPN allows organizations to use existing internet connections to provide access to company resources. This makes VPN a more accessible option for small and medium-sized enterprises that aim to keep their budget under control while not compromising on security.

Despite the drawbacks of VPN, such as potential delays in data transmission and the complexity of configuration, the advantages it offers outweigh these disadvantages in the context of modern business requirements. Therefore, when designing a distributed corporate network, it is recommended to choose VPN as the primary tool for secure communication. This not only meets security and availability needs but also contributes to the creation of an effective and flexible network infrastructure that can quickly respond to the challenges of the modern business environment.

1.2 Defining the Structure of a Distributed Corporate Network

Defining the structure of a distributed corporate network is an important step, as it determines how all the system components will be organized and interact with each other. A proper network structure ensures high performance, reliability, scalability, and security, which in turn contributes to the efficiency of business processes.

The structure of a distributed corporate network typically consists of several key components, each performing its specific functions. At its core is the client-server architecture, where clients, such as computers or mobile devices, access servers to obtain resources and services. In this architecture, servers play a crucial role as they store data, process requests, and execute business logic, which is critical to the functioning of the organization.

Additionally, the network includes various network devices, such as routers, switches, and end devices. Routers are responsible for forwarding data between different segments of the network, providing communication between local networks and the global Internet. Switches, on the other hand, optimize traffic within the local network, reducing delays in data transmission.

Another important component of the structure of a distributed corporate network is data storage systems. These can be network-attached storage (NAS) devices that allow for centralized data storage, making it accessible to all users in the organization. Such systems improve data handling efficiency and ensure easy access to important information.

Security is a critical aspect of the structure of a distributed network. The use of firewalls, intrusion detection and prevention systems (IDS/IPS), and virtual private networks (VPNs) ensures data protection and prevents unauthorized access. This is especially important for organizations handling sensitive information.

When defining the structure of a network, it is essential to consider not only its components but also the levels at which these components interact. Typically, distributed corporate networks are divided into three main levels: access, aggregation,

and core. The access level is the lowest level where users connect to the network via workstations, laptops, and mobile devices. The aggregation level is responsible for managing the traffic passing from multiple access levels, including switches that provide connections between connected devices. The core level is the heart of the network, ensuring high bandwidth and data transfer speed through routers and switches that forward information between different segments.

When choosing the structure of a distributed corporate network, several factors must be considered. First, the size and geographic location of the organization determine how the network will be distributed. For large companies with multiple branches, it is important that the network supports various locations while providing convenient access to resources. Second, the types of data to be processed must also be taken into account when designing the network, as this will impact the configuration of security and data management. The number of users accessing the network simultaneously is crucial for determining the required bandwidth, which helps prevent network overload.

Defining the structure of a distributed corporate network is a critical process that ensures the efficiency and reliability of the business. Proper organization of network elements and their interaction ensures stable operation in a rapidly changing technological environment, which, in turn, affects the success of the business.

1.3 Standards and Protocols

Standards and protocols are critical elements of distributed corporate networks as they define the rules for data exchange between different devices and systems. In the modern information environment, where various technologies and platforms are used, adherence to standards ensures compatibility, reliability, and network security.

Standards play a key role in ensuring the proper functioning of corporate networks, as they define the technical requirements and norms for various network

components, such as hardware, software, and communication protocols. These standards reduce the risks of incompatibility between devices from different manufacturers and make it easier to integrate new technologies, ensuring the network's stability and reliability. Here are some of the main standards used in corporate networks:

1. **IEEE 802** is a family of standards that defines the requirements for various types of networks, including local area networks (LANs) and wide area networks (WANs). These standards ensure consistency in the operation of networks and devices from different manufacturers. For example:
    - IEEE 802.3 — A standard defining Ethernet technology for wired local area networks. Ethernet is the primary technology for data transmission in corporate networks due to its reliability and speed.
    - IEEE 802.11 — A standard for wireless Wi-Fi networks. It describes the methods and technical requirements for creating and maintaining wireless connections in locations where wired connections are impossible or impractical. This standard forms the basis for most corporate wireless networks.
2. **ISO/IEC 27001** is an international standard for information security management systems (ISMS). This standard helps organizations define, implement, maintain, and improve security policies covering all aspects of information protection. According to this standard, organizations must ensure the confidentiality, integrity, and availability of data, as well as managerial and technical security in its processing and storage. This standard is critical for protecting corporate data from threats and unauthorized access [6].
3. **ITU-T** is a sector of the International Telecommunication Union (ITU), which develops global standards for telecommunications technologies. ITU-T standards ensure compatibility and interoperability between different networks and systems worldwide. They cover a wide range of technologies such as routing, data transmission, encryption, and other communication aspects. The protocols developed under ITU-T ensure that devices and systems using different technologies can effectively interact with each other [7].

Protocols are formal rules that govern how data is transmitted and processed within a network. They ensure consistency in communication between network devices and allow them to correctly interpret the received data. The main protocols used in corporate networks include:

1. **TCP/IP (Transmission Control Protocol/Internet Protocol)**: This is a set of protocols that form the foundation for most networks, including the Internet. It consists of two main parts: the TCP protocol, which ensures reliable data transmission, and the IP protocol, which provides routing of data packets between devices on the network. TCP ensures that transmitted data is not lost or corrupted by breaking it into packets and controlling their receipt. The IP protocol handles addressing and routing of packets from the source to the destination. Together, these two protocols ensure reliable and efficient communication in distributed networks [8].

2. **IPSec (Internet Protocol Security)**: This is a set of protocols for ensuring secure data transmission over IP networks. It uses encryption and authentication methods to protect the confidentiality, integrity, and authenticity of transmitted data. IPSec can operate at the packet level, providing security for the entire network or specific connections. It is especially useful for creating virtual private networks (VPNs), where data is transmitted over public channels but remains protected from unauthorized access [9].

3. **PPP (Point-to-Point Protocol)**: This protocol is used to establish a direct connection between two network nodes. PPP allows data transmission over serial connections, such as phone lines, mobile networks, or other communication channels. PPP supports authentication, encryption, and compression features, improving data transmission security and efficiency. This protocol is often used in scenarios where a connection between remote points is required, such as in broadband networks or with modems [10].

4. **HTTP/HTTPS (Hypertext Transfer Protocol/Secure)**: These protocols are used for data transmission over the Internet. HTTPS, the secure version of HTTP, encrypts data to protect confidentiality when transmitting information between a browser and a web server [11].

5. **FTP (File Transfer Protocol)**: This protocol is used for transferring files between a client and a server in a network. It allows uploading or downloading files and viewing their structure on a remote server. FTP provides quick access to files and facilitates their transfer across the network. There are secure versions of FTP, such as FTPS (FTP Secure) and SFTP (SSH File Transfer Protocol), which use encryption to protect data during transmission.

6. **OSPF (Open Shortest Path First)**: This is an internal routing protocol that uses a link-state algorithm to determine the best paths for data transmission in IP networks. Since OSPF operates at the router level, it helps maintain routing efficiency in networks with many devices and complex topologies. OSPF also supports automatic route updates, allowing the network to adapt to real-time changes, such as router failures or changes in network connections [12].

7. **DHCP (Dynamic Host Configuration Protocol)**: This protocol automatically assigns IP addresses and other network settings (such as subnet masks, default gateways) to devices on the network. It greatly simplifies network administration, as manual configuration of each device is not required. DHCP is widely used in most corporate networks, where the number of connected devices can be large and frequently changing.

8. **GRE (Generic Routing Encapsulation)**: This is a tunneling protocol that allows encapsulating packets of one protocol within another for transmission over a network. This enables the creation of virtual tunnels for data transmission between remote points, such as between two corporate network offices over the Internet. GRE is often used for connecting remote locations or creating VPN networks. This protocol does not provide encryption, so it is frequently used in combination with other technologies for data protection during transmission.

Adhering to established standards and protocols is a necessary condition for ensuring the effective and secure operation of a distributed corporate network. They help create a favorable environment for integrating new technologies and systems while providing a high level of security and data protection. In an era of rapid technological

development and constant cybersecurity threats, adherence to standards is even more important.

Standards and protocols form the foundation upon which distributed corporate networks are built. Their proper implementation ensures compatibility, reliability, and security of information systems, which in turn affects the efficiency of business processes. Understanding and adhering to these standards is key to the successful operation of modern corporate networks.

1.4 Topology of Distributed Corporate Networks

The topology of a distributed corporate network defines the physical and logical organization of its components, as well as the manner in which devices are interconnected. The correct choice of topology affects the network's performance, reliability, security, and scalability. Depending on the specifics of business processes and technological requirements, organizations can choose different types of topologies, each with its own advantages and disadvantages [13].

There are several main types of topologies commonly used in distributed corporate networks:

1. **Star Topology:** The "star" topology assumes that all devices in the network are connected to a central node, which can be a switch or a router (Figure 1.6). All data transmission occurs through this central device, which is responsible for managing traffic. The main advantage of this topology is the ease of setup and network scalability, as well as the quick detection of faults. However, the dependence on the central node is its main disadvantage, as the failure of this device would paralyze the entire network. In corporate networks, star topology is often used for local networks in office settings, where stability and ease of management are critical.

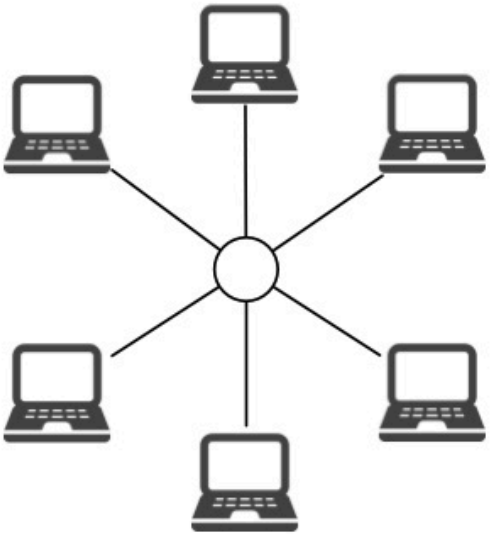


Figure 1.6 — Star Topology

2. **Bus Topology:** The "bus" topology is based on the use of a single cable to which all devices are connected (Figure 1.7). Data transmission occurs along the cable, and each device checks whether the current frame is addressed to it. This topology is characterized by low cable and equipment costs, but it is extremely vulnerable to damage to the backbone, which halts the operation of the entire network. Although its simplicity was useful in the early stages of network development, modern corporate networks rarely use it due to its limited scalability and difficulty in traffic management.

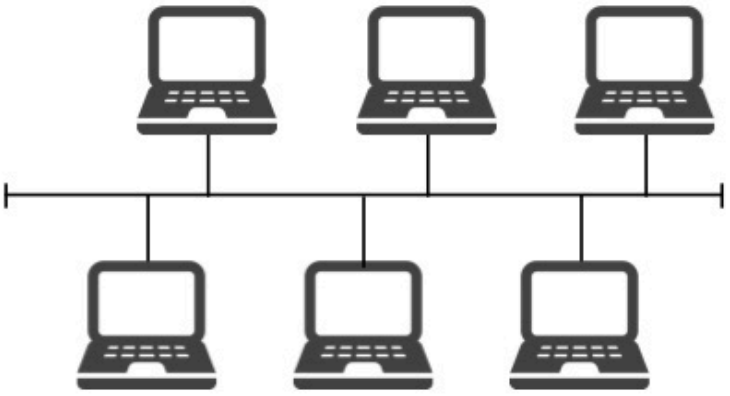


Figure 1.7 — Bus Topology

3. **Ring Topology:** In the "ring" topology, devices are connected in a closed loop, where data is transmitted from one node to another in a specific direction (Figure 1.8). This approach ensures orderly data transmission and efficient use of bandwidth. However, the failure of a single device or cable disrupts the operation of the entire network. The "ring" topology has limited use in modern corporate networks, but it can still be applied in automation systems or specialized industrial networks.

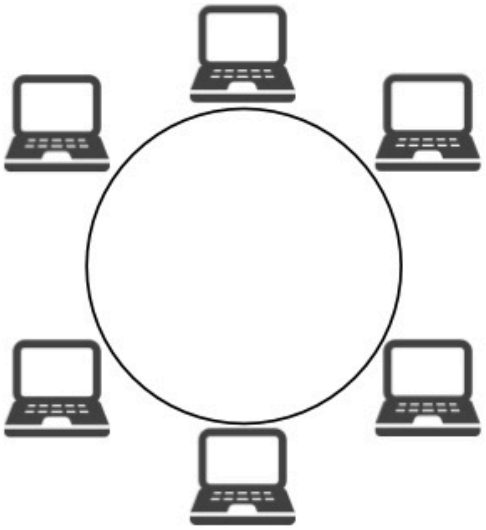


Figure 1.8 — Ring Topology

4. **Tree Topology:** Tree topology is a hierarchical structure that combines several star topologies (Figure 1.9). It provides organized device connections within subnets, where there is a central root node and subordinate nodes that can further expand. This topology is well-suited for scaling large networks, as new devices can be added without significantly impacting other segments. The main disadvantage lies in the dependency on the central node and the complexity of cable management. Tree topology is ideal for large corporate networks with a clear structure, where scalability is important.

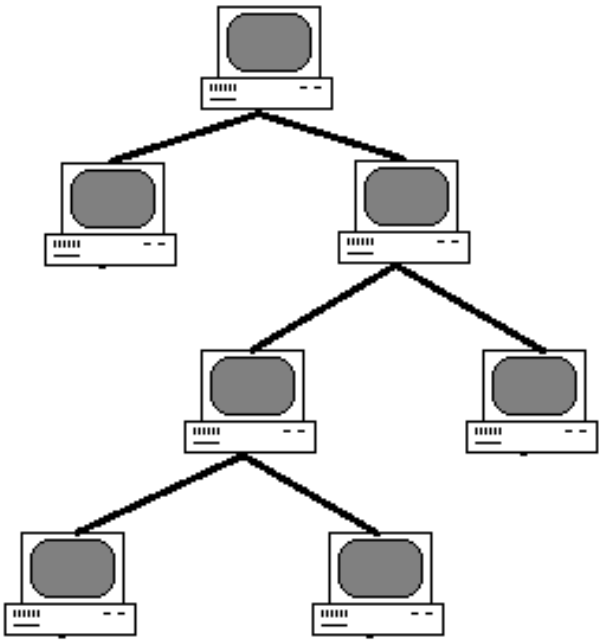


Figure 1.9 — Tree Topology

5. **Hybrid Topology:** Hybrid topology combines elements of several different topologies, such as "star", "ring", and "bus", to create a network that meets the needs of the organization (Figure 1.10). This approach provides high flexibility and reliability, as the failure of one segment does not affect the entire network. However, the design and implementation of hybrid topology require significant resources and complex management. In distributed corporate networks, hybrid topology is the most common solution, as it allows the integration of different segments to achieve a balance between performance, scalability, and reliability.

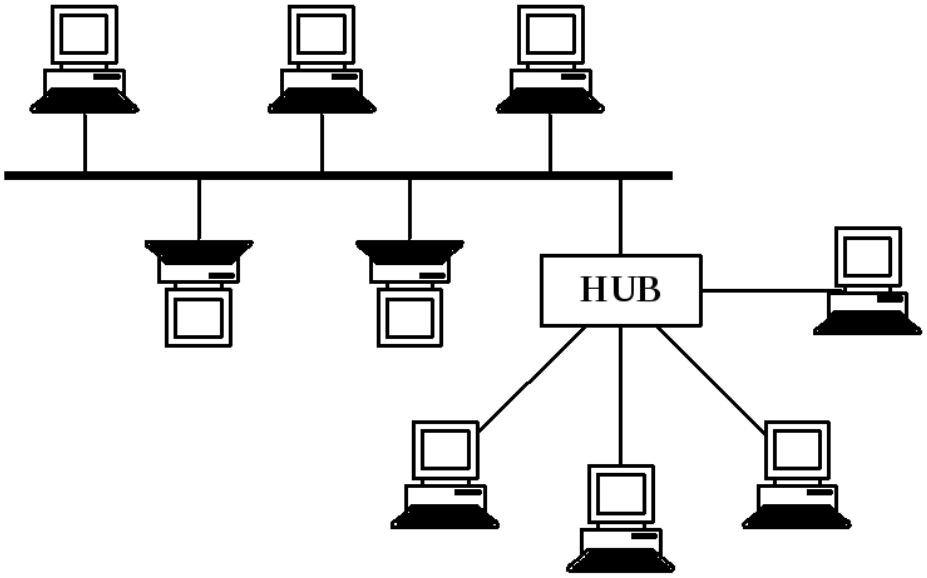


Figure 1.10 — Hybrid Topology

The topology of a distributed corporate network is an important aspect of its design. The choice of network topology depends on several key factors. One of the main factors is the size of the organization: for large enterprises with numerous branches and a large number of users, the star or tree topology is the most suitable, as they provide easy management and scalability. Another important factor is the types of data being processed: for businesses dealing with large volumes of data, the optimal choice would be a topology that minimizes delays and ensures high bandwidth, such as star or hybrid topology. The budget also plays a role, as some topologies, such as bus, may be cheaper to implement but require careful planning to prevent potential issues in the event of failure. Additionally, scalability is an important factor: if the company plans to grow, it is worth choosing a topology that allows easy addition of new devices without significant time and resource investment.

ДОДАТОК Б

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

ЗБІРНИК НАУКОВИХ ПРАЦЬ

за матеріалами X Всеукраїнської науково-практичної конференції

«ЕЛЕКТРОННІ ТА МЕХАТРОННІ СИСТЕМИ:
ТЕОРІЯ, ІННОВАЦІЇ, ПРАКТИКА»

20 грудня 2024 року

Полтава 2024

УДК 004.89 + 681.51

Збірник наукових праць за матеріалами X Всеукраїнської науково-практичної конференції «Електронні та мехатронні системи: теорія, інновації, практика», 20 грудня, 2024 р. / Національний університет «Полтавська політехніка імені Юрія Кондратюка».

Редколегія: О.В. Шефер (головний редактор) та ін. – Полтава: НУ «Полтавська політехніка імені Юрія Кондратюка», 2024. – 124 с.

У збірнику представлені результати наукових досліджень та розробок в області сучасних електромеханічних систем та автоматизації, електричних машини і апаратів, моделювання та методів оптимізації, енергозбереження в електромеханічних системах, управління складними технічними системами, проблем аварійності та діагностики в електромеханічних системах та електричних машинах, інформаційно-комунікаційних технологіях та засобах управління. Призначений для наукових й інженерно-технічних працівників, аспірантів і магістрів.

Матеріали відтворено з авторських оригіналів та рекомендовано до друку IX Всеукраїнської науково-практичної конференції «Електронні та мехатронні системи: теорія, інновації, практика». Редакція не обов'язково поділяє думку автора і не відповідає за фактичні помилки, яких він припустився.

Відповідальний за випуск - д.т.н., професор О.В. Шефер.

ЗМІСТ

УДК 621.39
***С.В. Індик**, к.т.н., доцент,*
***В.В. Панич**, магістрант*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ПРОЄКТУВАННЯ РОЗПОДІЛЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

Розподілені корпоративні мережі є основою для забезпечення ефективної роботи сучасних підприємств, які мають численні підрозділи та офіси в різних регіонах. Вони дозволяють забезпечити обмін даними, доступ до інформаційних ресурсів та забезпечити високий рівень безпеки при взаємодії віддалених користувачів. Оскільки вимоги до таких мереж постійно зростають у зв'язку з глобалізацією, мобільністю співробітників і збільшенням обсягів даних — питання їх проєктування та оптимізації набуває особливої актуальності. Об'єктами дослідження є корпоративні мережі, що охоплюють різні географічні локації та мають потребу в обміні даними між віддаленими офісами, філіями та віддаленими користувачами. Основними характеристиками таких мереж є: масштабованість, безпека, надійність і продуктивність. У дослідженні використано методи моделювання, аналізу топологій, а також технічні засоби моніторингу та оптимізації мережевих процесів. Для розв'язання завдань з підвищення продуктивності мережі застосовуються методи балансування навантаження, технології оптимізації трафіку та системи управління якістю обслуговування. Основним інструментом дослідження є аналіз різних архітектурних рішень та технічних засобів для забезпечення безпечного та ефективного обміну даними в умовах розподіленої мережі.

Результати дослідження показали, що для ефективного функціонування розподілених корпоративних мереж необхідно враховувати кілька основних аспектів. По-перше, вибір топології мережі, який залежить від розміру компанії та географічної поширеності її підрозділів, відіграє ключову роль у досягненні оптимальної продуктивності. Зокрема, топології "зірка", "дерево" та "кільце" демонструють різні переваги й недоліки в залежності від конкретних потреб бізнесу. Для малих та середніх компаній оптимальною є топологія зірка, яка забезпечує централізоване управління і простоту в налаштуванні, однак для великих корпорацій з численними підрозділами краще застосовувати деревоподібну топологію, що дозволяє покращити надійність і масштабованість мережі.

По-друге, для забезпечення безпеки в розподілених мережах необхідно застосовувати багатофакторну аутентифікацію, шифрування трафіку, а також використання віртуальних приватних мереж. Важливим компонентом є протокол IPsec (Internet Protocol Security), який забезпечує шифрування, цілісність і аутентифікацію даних, створюючи захищені тунелі для передачі між сегментами мережі. IPsec підтримує сучасні алгоритми шифрування, такі як Advanced Encryption Standard, і є надійним рішенням для захисту корпоративного трафіку. Впровадження систем моніторингу та засобів для

відстеження аномалій у мережевому трафіку також є важливим аспектом у забезпеченні безпеки.

По-третє, дослідження показали, що застосування технології Software-Defined WAN (SD-WAN) є перспективним методом для оптимізації використання каналів зв'язку та управління трафіком. Це дає змогу знижувати витрати на передачу даних між віддаленими офісами і при цьому підвищувати продуктивність за рахунок гнучкого налаштування маршрутизації. Застосування таких технологій дозволяє ефективно керувати мережею, знижуючи ризики відмов та забезпечуючи високу швидкість обміну інформацією в умовах великих навантажень.

Ще одним важливим результатом є те, що застосування методів балансування навантаження дає змогу збільшити ефективність роботи мережі, зменшуючи ймовірність перевантаження окремих елементів інфраструктури. Це дозволяє забезпечити стабільність і доступність мережевих ресурсів навіть у періоди пікового навантаження. Сучасні тенденції в проєктуванні корпоративних мереж орієнтовані на застосування новітніх технологій, таких як 5G, хмарні обчислення, штучний інтелект та Інтернет речей. Інтеграція цих технологій у розподілені мережі дозволяє значно збільшити швидкість обміну даними, забезпечити безпеку на новому рівні, а також оптимізувати використання ресурсів.

Дослідження вказують на важливість комплексного підходу до проєктування розподілених корпоративних мереж, що враховує як вимоги безпеки, так і ефективність використання ресурсів. Розробка оптимальних топологій, впровадження систем безпеки, а також технологій для управління трафіком і балансування навантаження дозволяє значно покращити продуктивність і надійність таких мереж. Отримані результати можуть бути використані для проєктування мереж у компаніях, що мають потребу в безпечному та ефективному обміні даними між віддаленими підрозділами, а також для подальших досліджень у сфері оптимізації мережевих архітектур у великих організаціях.

ЛІТЕРАТУРА:

1. Kent S., Seo K. Security Architecture for the Internet Protocol (RFC 4301) [Електронний ресурс] / Internet Engineering Task Force. – 2005. – Режим доступу: https://www.ietf.org/rfc/rfc4301.txt.

2. Kosiur D. IPSec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks. – Prentice Hall, 2000. – 320 с.

3. Cisco Systems. Cisco IPsec VPN Design Guide [Електронний ресурс] / Cisco Systems, Inc. – 2018. – Режим доступу: https://www.cisco.com.

DESIGN OF A DISTRIBUTED CORPORATE NETWORK

***S. Indyk**, PhD (Engineering), Associate Professor,*
***V. Panych**, Master's Student*
National University "Yuri Kondratyuk Poltava Polytechnic"

Міністерство освіти та науки України
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Кафедра автоматики, електроніки та телекомунікацій

Проєктування розподіленої корпоративної мережі

Кваліфікаційна робота магістра

Виконав: студент групи 601-ТТ Панич В.В.
Керівник: к.т.н., доцент Індик С.В.

Полтава 2025

ДОДАТОК В

Актуальність роботи

У зв'язку з безперервним зростанням обсягів даних, які передаються через мережі, а також із збільшенням кількості віддалених співробітників та офісів, компанії стикаються з новими викликами у сфері проєктування та впровадження розподілених мереж. Забезпечення надійності, безпеки, продуктивності та масштабованості таких мереж є пріоритетним завданням для IT-підрозділів організацій. Особливої важливості набувають питання захисту даних та запобігання несанкціонованому доступу, оскільки сучасні корпоративні мережі все частіше стають об'єктами кібератак.

Питання проєктування розподілених корпоративних мереж є актуальним як для великих компаній з глобальною присутністю, так і для середніх підприємств, що прагнуть розширити свої можливості та інтегруватися у цифрову економіку. Таким чином, дослідження сучасних підходів до проєктування та впровадження таких мереж є важливим і актуальним завданням для забезпечення ефективної роботи підприємств у нових умовах.

Мета роботи

Розробка комплексного підходу до проєктування розподіленої корпоративної мережі, яка забезпечуватиме високу надійність, безпеку, масштабованість та продуктивність мережевої інфраструктури.

Об'єкт дослідження

Розподілена корпоративна мережа як комплекс апаратного та програмного забезпечення, що забезпечує комунікацію між офісами організації, управління трафіком і захист корпоративних даних.

Предмет дослідження

Методи та технології проєктування, побудови і оптимізації розподілених корпоративних мереж, включаючи архітектурні рішення, моделі управління трафіком і засоби забезпечення інформаційної безпеки.

Завдання дослідження

1

Аналіз принципів побудови
Аналіз існуючих технологій та стандартів, що використовуються для побудови розподілених мереж.

2

Вибір апаратного забезпечення
Оцінка вимог до мережевого обладнання: маршрутизаторів, комутаторів, серверів тощо.

3

Організація безпеки
Розробка політик безпеки з використанням шифрування, ключової аутентифікації та методів захисту від несанкціонованого доступу.

4

Побудова моделі мережі
Створення структурної моделі корпоративної мережі з урахуванням вимог до трафіку, топології та безпеки.

5

Аналіз результатів моделювання
Аналіз мережевого трафіку з використанням інструментів моніторингу для перевірки шифрування, затримок і стабільності передачі даних через IPSec.

6

Аналіз переваг та недоліків
Оцінити можливості масштабування та адаптації розробленої мережі.Виявлення можливих обмежень або проблем, що потребують подальшого вдосконалення.

Ключові принципи проектування

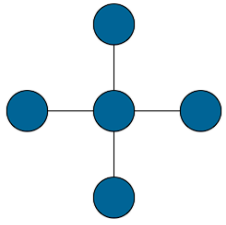
Масштабованість
Мережа має легко розширюватися за потреби, без необхідності значних змін в інфраструктурі.

Безпека
Захист даних та мережі від несанкціонованого доступу, хакерських атак та вірусів є надзвичайно важливим.

Ефективність
Мережа має забезпечувати високу пропускну здатність та швидкість передачі даних для підтримки ефективної роботи пристроїв.

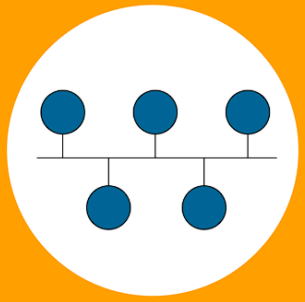
Надійність
Мережа повинна бути надійною та доступною, з мінімальним часом простою, щоб забезпечити безперебійну роботу компанії.

Топологія розподілених корпоративних мереж



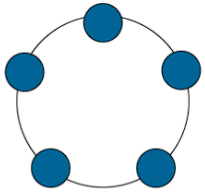
Зірка

Усі пристрої з'єднані через центральний вузол (комутатор або маршрутизатор). Забезпечує високу надійність, адже вихід з ладу одного вузла не впливає на інші.



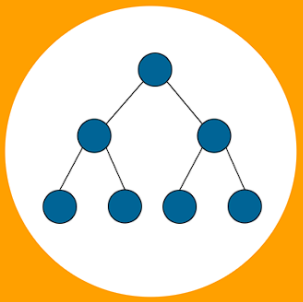
Шина

Всі пристрої підключені до однієї спільної магістралі. Простота установки, але вразливість до збоїв через єдиний канал зв'язку.



Кільце

Пристрої утворюють замкнуте кільце, де дані передаються від одного пристрою до іншого. Перевага – стабільна швидкість передачі, але вразливість до розриву кільця.



Дерево

Об'єднує елементи зіркової та шинної топологій, створюючи ієрархічну структуру. Зручна для масштабування великих мереж.

Стандарти та протоколи

Стандарти та протоколи є критично важливими елементами розподілених корпоративних мереж, оскільки вони визначають правила, за якими відбувається обмін даними між різними пристроями та системами. У сучасному інформаційному середовищі, де використовуються різноманітні технології та платформи, дотримання стандартів забезпечує сумісність, надійність та безпеку мережі.

Протоколи – це набір правил та інструкцій, які визначають, як пристрої обмінюються даними в мережі. Вони забезпечують уніфіковану взаємодію між різними пристроями, незалежно від їх виробника або операційної системи. Завдяки протоколам мережі стають керованими, ефективними та безпечними.

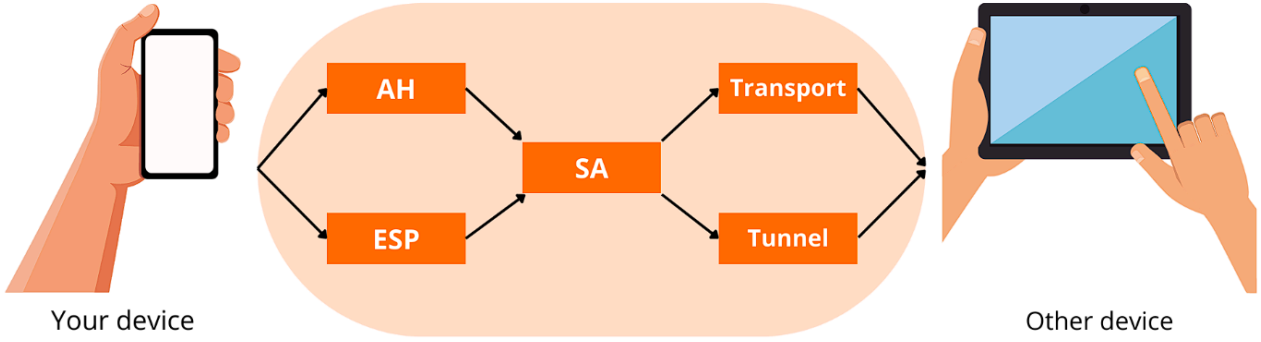
PPP (Point-to-Point Protocol)
Протокол канального рівня, який використовується для прямого з'єднання між двома пристроями. PPP підтримує автентифікацію, стиснення даних і багатопротокольну передачу, що робить його корисним у виділених каналах.

ISO/IEC 27001
Міжнародний стандарт для систем управління безпекою інформації (ISMS). Цей стандарт допомагає організаціям визначити, впровадити, підтримувати та покращувати політики безпеки, що охоплюють всі аспекти захисту інформації.

DHCP (Dynamic Host Configuration Protocol)
Протокол, що автоматично призначає IP-адреси пристроям у мережі, спрощуючи управління мережевими конфігураціями.DHCP забезпечує ефективний розподіл ресурсів та зменшує ризик конфліктів IP-адрес.

IPSec (Internet Protocol Security)

Критично важливий протокол для забезпечення захисту мережевих з'єднань у корпоративних мережах. Він гарантує високий рівень безпеки завдяки шифруванню, автентифікації та перевірці цілісності даних. IPSec дозволяє організаціям захищати конфіденційність інформації під час її передачі через незахищені мережі, такі як Інтернет, і є основою для створення надійних VPN-з'єднань.



Апаратні та програмні засоби мультисервісної мережі

Маршрутизатор

Пристрій, який забезпечує передачу даних між різними мережами, визначаючи оптимальний маршрут для їхнього руху.

Комутатор

Мережеве обладнання, що з'єднує пристрої в одній локальній мережі (LAN) і забезпечує ефективний розподіл даних між ними.

Сервер

Центральний комп'ютер у мережі, який надає ресурси, послуги та обчислювальні потужності іншим пристроям (клієнтам).

Міжмережевий екран

Захисний пристрій або програмний компонент, який контролює трафік, запобігаючи несанкціонованому доступу та забезпечуючи безпеку мережі.

Організація безпеки в корпоративних мережах

Актуальність питання безпеки корпоративних мереж зростає з кожним роком. З розвитком технологій і збільшенням кількості підключених пристроїв і користувачів мережа стає уразливою для атак. Використання протоколів захисту та методів забезпечення безпеки не є лише вимогою законодавства або внутрішніх політик організації, а необхідністю для збереження її репутації та економічної стабільності.

Такі загрози, як перехоплення даних, атаки на сервери, зловмисне втручання в мережевий трафік або навіть витік персональних даних користувачів, ставлять під загрозу нормальну роботу компаній. У зв'язку з цим вкрай важливим є створення стійкої системи захисту на всіх рівнях інфраструктури.

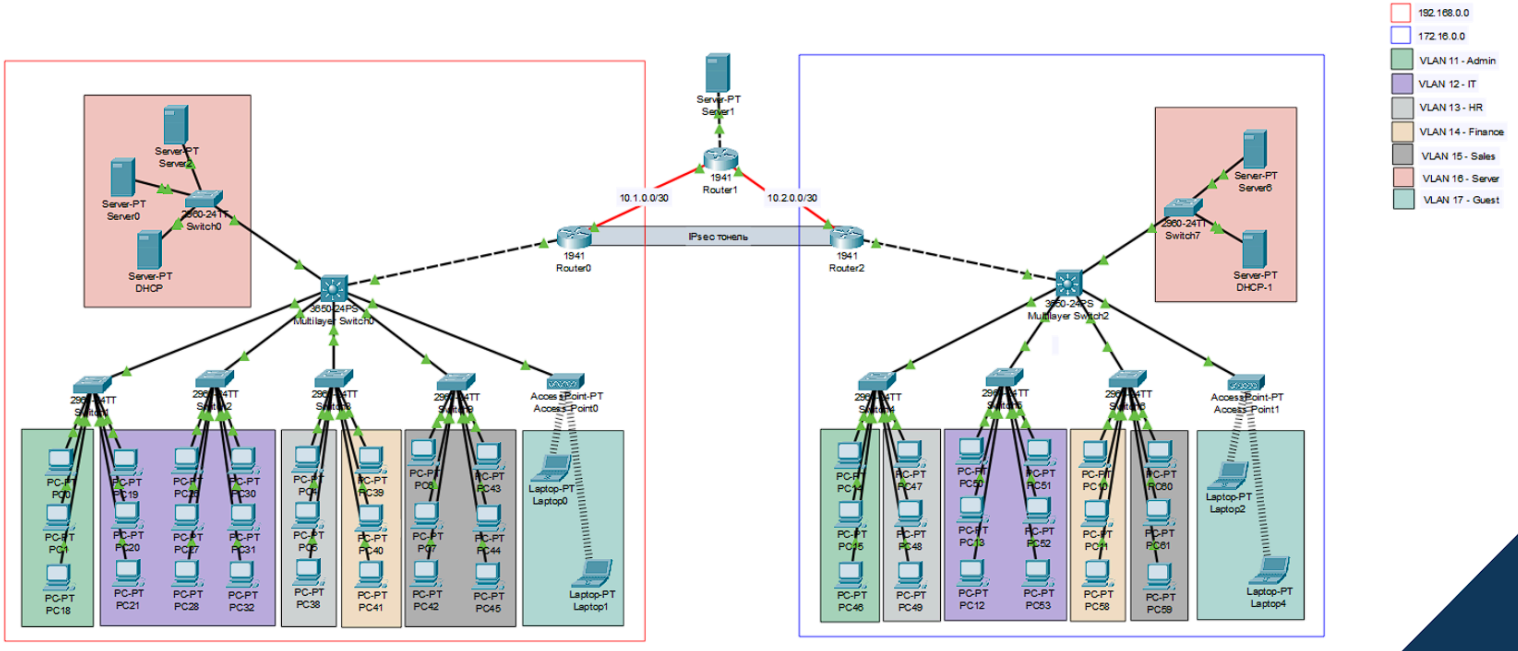
Мережеве розмежування
Сегментація мережі для обмеження доступу між різними її частинами. Наприклад, використання внутрішніх та зовнішніх підмереж, щоб уникнути несанкціонованого доступу до важливих ресурсів.

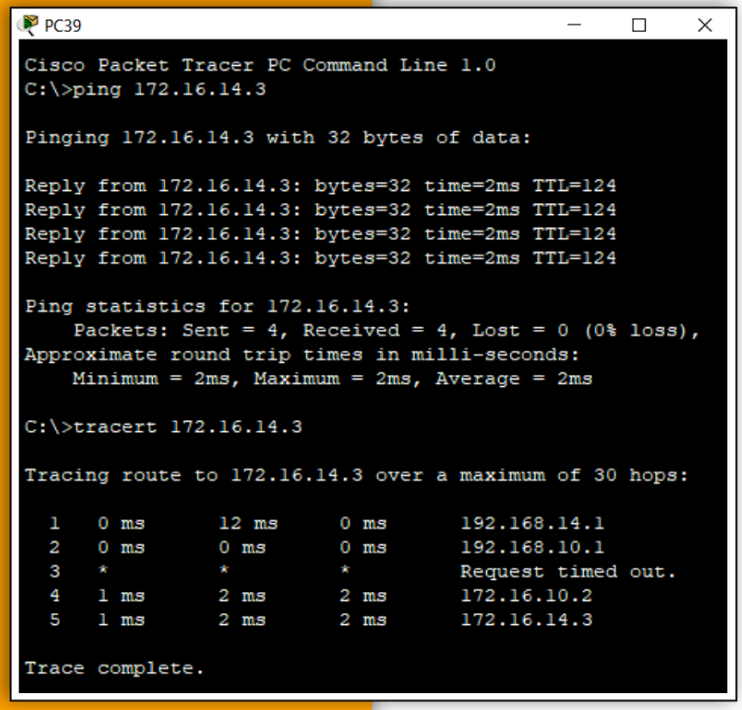
Мережеві екрани (файрволи)
Програмні або апаратні засоби, що обмежують або контролюють доступ до корпоративної мережі ззовні або всередині. Вони дозволяють блокувати несанкціоновані підключення та попереджати атаки.

Антивірусне програмне забезпечення
Використання спеціальних програм для виявлення та ліквідації шкідливого програмного забезпечення, що може потрапити в мережу через заражені файли або вразливості в програмному забезпеченні.

Модель корпоративної розподіленої мережі

В результаті виконаного моделювання корпоративної розподіленої мережі було створено ефективну і безпечну архітектуру, яка забезпечує надійне з'єднання між віддаленими офісами.





Аналіз результатів моделювання на основі протоколу IPSec

Для перевірки коректної роботи IPSec тунелю в нашій мережевій моделі, ми ініціюємо передачу даних через тунель за допомогою ICMP запиту.

Ініціація ехо запиту (ping) дозволяє перевірити працездатність тунелю, а також наочно продемонструвати, що IPSec забезпечує захист даних під час їх передачі.

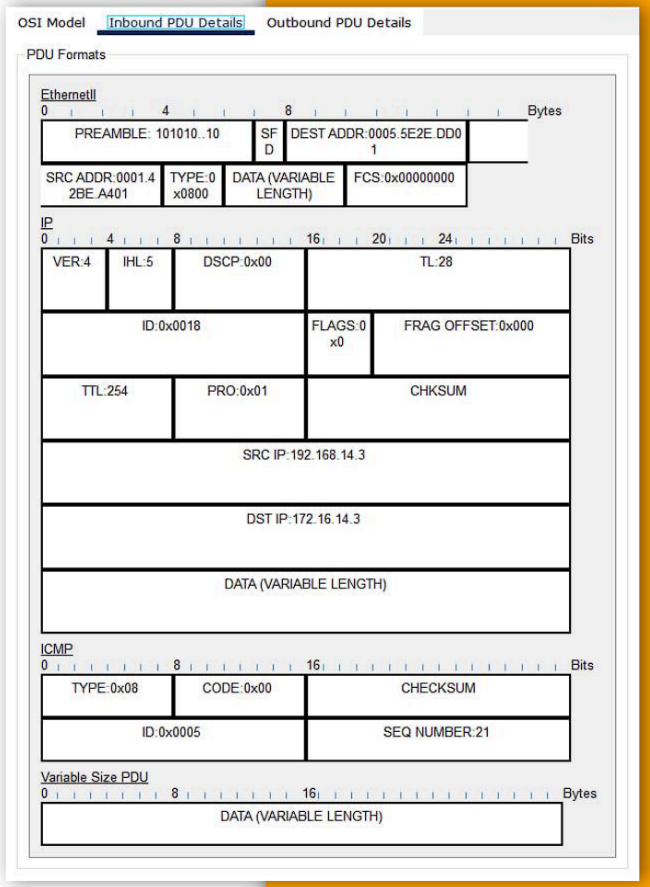
Inbound PDU (Protocol Data Unit)

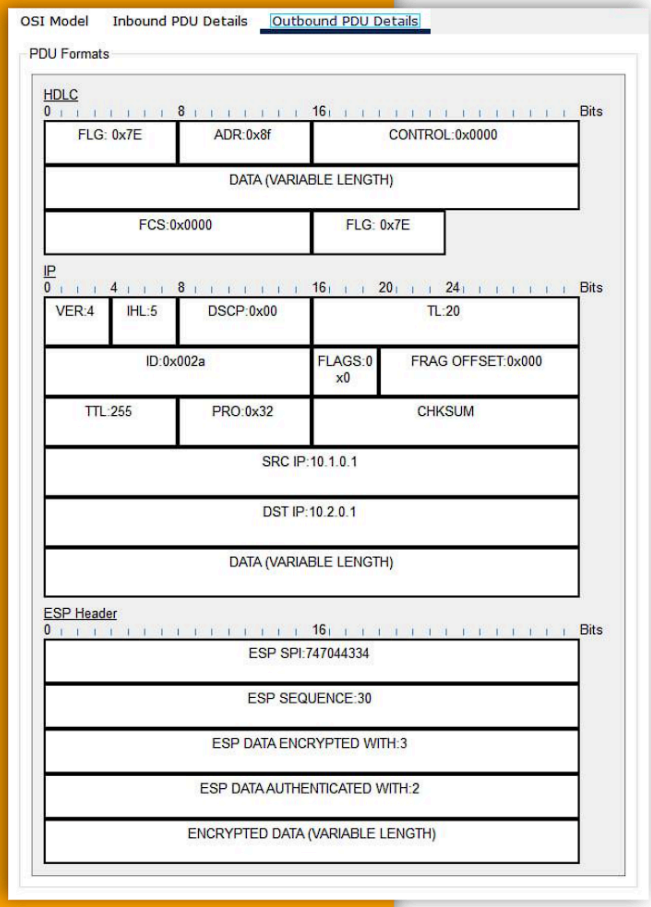
Описує пакет, що надходить до пристрою Router0. Він складається з кількох рівнів протоколів, зокрема Ethernet II, IP, та ICMP.

SRC IP (IP-адреса джерела): Адреса відправника пакета (192.168.14.3). Ця адреса використовується для зворотного зв'язку або відповіді на запит.

DST IP (IP-адреса призначення): Адреса отримувача пакета (172.16.14.3). Визначає кінцевий пункт призначення пакета в мережі.

TYPE (Тип повідомлення): Поле визначає тип ICMP повідомлення. Значення 0x08 означає Echo Request, тобто запит на відгук (ping), що використовується для перевірки доступності пристрою в мережі.





Outbound PDU (Protocol Data Unit)

Структура даних, яка передається з вихідного пристрою (у цьому випадку Router0). Вона містить три основні рівні протоколів: HDLC, IP, та ESP Header.

ESP SPI (Security Parameters Index): Унікальний ідентифікатор параметрів безпеки для з'єднання, що дозволяє приймачу визначити використовувану криптографічну політику для шифрування та аутентифікації.

ESP DATA ENCRYPTED: Всі дані в межах IPSec тунелю шифруються, щоб запобігти їх доступу сторонніми особами.

ESP DATA AUTHENTICATED: Для забезпечення цілісності та автентичності даних використовуються спеціальні механізми автентифікації, такі як HMAC.

Аналіз переваг та недоліків

Аналіз результатів моделювання дозволяє визначити основні переваги та недоліки мережі, виявити можливі проблеми, що можуть виникнути під час експлуатації, а також спланувати заходи для покращення її роботи

Масштабованість

Розподілена корпоративна мережа дозволяє легко додавати нові офіси або пристрої без значних змін у її структурі. Це забезпечує гнучкість у разі розширення бізнесу або збільшення навантаження.

Безпека

Використання сучасних протоколів, таких як IPSec і VPN, забезпечує захищену передачу даних між віддаленими сегментами мережі. Мережа має вбудовані механізми захисту від атак та витоку інформації.

Затримки

Через віддаленість вузлів і складну маршрутизацію можуть виникати затримки в передачі даних, особливо при великому трафіку. Це може вплинути на якість роботи в режимі реального часу, наприклад, відеоконференцій.

Обмежена відмовостійкість

У разі виходу з ладу одного з ключових вузлів або обладнання, функціональність мережі може бути частково порушена. Це вимагає додаткових ресурсів для впровадження механізмів резервування та моніторингу.

Висновки по роботі

У результаті виконаної роботи було розроблено ефективну модель розподіленої корпоративної мережі, що враховує всі важливі аспекти проектування, включаючи вибір концепції мережі, структуру, стандарти та протоколи, а також методи забезпечення безпеки. Використання протоколу IPSec для захищених з'єднань між віддаленими офісами стало ключовим елементом для забезпечення конфіденційності та цілісності переданих даних, що є критично важливим у сучасних умовах. Моделювання мережі в Cisco Packet Tracer дозволило візуалізувати та тестувати усі етапи реалізації мережевої інфраструктури, що забезпечує її надійність і стабільність.

Отримані результати підтверджують, що за допомогою сучасних технологій і підходів можна створити надійну і безпечну корпоративну мережу, яка здатна ефективно функціонувати в умовах високих вимог до безпеки та масштабованості. Розроблена модель мережі може бути використана як основа для подальших практичних розробок і впровадження в реальних умовах, що дозволить значно підвищити ефективність управління та захисту корпоративних даних.