

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Інститут інформатики та радіоелектроніки
Факультет радіоелектроніки та телекомунікацій
(повне найменування інституту, факультету)

Кафедра радіоелектроніки та телекомунікацій
(повне найменування кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

бакалавр

(ступінь вищої освіти)

на тему ОРГАНІЗАЦІЯ ЗВ'ЯЗКУ МІЖ ДВОМА ОФІСАМИ

Виконав: студент(ка) 4 курсу, групи РТ-917

Спеціальності _____

172 «Телекомунікації та радіотехніка»

(код і найменування спеціальності)

Освітня програма (спеціалізація)

«Інформаційні мережі зв'язку»

Жуковська Марія Василівна

(прізвище та ініціали)

Керівник Костенко В.О.

(прізвище та ініціали)

Рецензент Касьян М.М.

(прізвище та ініціали)

2021 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування закладу вищої освіти)

Інститут, факультет Інстит інформатики та радіоелектроніки, ФРЕТ
Кафедра Радіотехніка та телекомунікації
Ступінь вищої освіти Бакалавр
Спеціальність 172 «Телекомунікації та радіотехніка»
(код і найменування)
Освітня програма (спеціалізація) «Інформаційні мережі зв'язку
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ

Завідувач кафедри РКТ 
Морщавка С.В.
« » червня 2021 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

Жуковської Марії Василівної
(прізвище, ім'я, по батькові)

1. Тема проєкту (роботи) Організація зв'язку між двома офісами

керівник проєкту (роботи) Костенко Валеріан Остапович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти від « » квітня 2021 року №

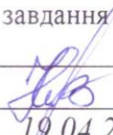
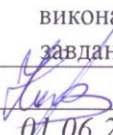
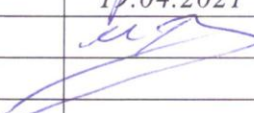
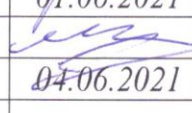
2. Строк подання студентом проєкту (роботи) 04 червня 2021 року

3. Вихідні дані до проєкту (роботи) Стабільне інтернет підключення надане зовнішнім провайдером, кількість співробітників, що працюють в офісах, швидкість передачі даних для певних сервісів мережі, розміщення офісів.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Актуальність роботи та загальні принципи побудови VPN-мереж. Постановка задачі на виконання. Виконання поставленої задачі.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Презентація роботи в Microsoft PowerPoint з поясненням алгоритму побудови VPN-мережі, проєктуванням офісної топології, поясненням принципу обміну даними по тунелю, розрахунком трафіку, що генерується у вузлах.

6. Консультанти розділів проєкту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-3	Костенко В.О., доцент	 19.04.2021	 01.06.2021
нормокон троль	Мороз Г. В., ст. викладач		 04.06.2021

7. Дата видачі завдання « 19 » квітня 20 21 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Актуальність роботи та загальні принципи побудови VPN- мережі	1-й тиждень	виконано
2	Постановка задачі на її виконання	2-й тиждень	виконано
3	Визначення пріоритетів при проєктуванні мережі	2-й тиждень	виконано
4	Проєктування мережі головного офісу	3-й тиждень	виконано
5	Проєктування мережі філії	3-й тиждень	виконано
6	Розрахунок трафіку в мережі	4-й тиждень	виконано
7	Оформлення пояснювальної записки	5-й тиждень	виконано
8	Проходження норм контролю, рецензування, анти-плагіату	6-й тиждень	виконано

Студент(ка)


(підпис)

Жуковська М. В.
(прізвище та ініціали)

Керівник проєкту (роботи)


(підпис)

Костенко В.О.
(прізвище та ініціали)

РЕФЕРАТ

ПЗ: 51 сторінка, 17 рисунків, 5 таблиць, 7 джерел

Мета роботи – об'єднання двох офісних мереж в одну цілісну мережу.

В дипломній роботі проведено побудову та розрахунок трафіку для даних мереж. Приведено приклад організації сервісу VPN для корпоративних клієнтів. Розглянута класифікація VPN. Основні принципи функціонування VPN-мережі. Застосування тунелювання при побудові VPN-мережі та для чого воно потрібно. Проаналізуємо принципи побудови VPN. Розрахунок трафіку, що передається мережею та його втрати при увімкненому VPN.

**ВІРТУАЛЬНА ПРИВАТНА МЕРЕЖА, ЛОКАЛЬНА МЕРЕЖА,
ТРАФІК, МІЖМЕРЕЖЕВИЙ ПРОТОКОЛ, ВІДДАЛЕНИЙ ДОСТУП,
ПАКЕТ ДАНИХ**

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ.....	6
ВСТУП	8
1 АКТУАЛЬНІСТЬ РОБОТИ ТА ЗАГАЛЬНІ ПРИНЦИПИ ОРГАНІЗАЦІЇ VPN	10
1.1 Актуальність об'єднання двох офісів у наш час.....	10
1.2 Класифікація VPN мережі.....	12
1.3 Функції VPN по захисту даних.....	14
1.4 Застосування тунелів для VPN	16
1.5 Побудова VPN-мережі.....	19
2 ПОСТАНОВКА ЗАВДАННЯ НА ЇЇ ВИКОНАННЯ	26
2.1 Постановка задачі.....	26
2.2 Загальні положення для створюваної мережі	27
3 ВИКОНАННЯ ПОСТАВЛЕНОЇ ЗАДАЧІ	31
3.1 Вибір обладнання для створення мережі.....	31
3.2 Проєктування мережі головного офісу	37
3.3 Проєктування мережі для філіалу	40
3.4 Створення інформаційної моделі об'єкту	43
3.5 Розрахунок трафіку	45
ВИСНОВКИ.....	50
ПЕРЕЛІК ПОСИЛАНЬ	51

ПЕРЕЛІК СКОРОЧЕНЬ

ЛОМ	–	локальна обчислювальна мережа
ПАК	–	програмно-апаратний комплекс
ПЗ	–	програмне забезпечення
ПК	–	персональний комп'ютер
ТМІ	–	транспортну мережу інфокомунікацій
ATM	–	(Asynchronous Transfer Mode) асинхронний спосіб передачі даних
BGP	–	(Border Gateway Protocol) протокол граничного шлюзу
CEF	–	(Cisco Express Forwarding) технологія високошвидкісної маршрутизації
CER	–	(Customer Edge Router) граничний маршрутизатор клієнта
EIGRP	–	(Enhanced Interior Gateway Routing Protocol) протокол маршрутизації
IP	–	(Internet Protocol) міжмережевий протокол
IPSec	–	(IP Security) протокол захисту даних, що передається через IP
LAN	–	(Local Area Network) локальна мережа
LSP	–	(Label Switch Path) тунель, шлях в MPLS.
LSR	–	(Label switching router) комутуючий мітки маршрутизатор
MAC	–	(Media Access Control) фізична адреса пристрою
MPLS	–	(Multiprotocol Label Switching) багатопроTOCOLьна комутація по міткам
NGN	–	(Next Generation Network) мережі нового покоління
OSPF	–	(Open Shortest Path First) протокол динамічної маршрутизації.
PER	–	(Provider Edge Router) граничний маршрутизатор мережі провайдера
POP	–	(Point of presence) точка присутності
PPPoE	–	(Point-to-point protocol over Ethernet) протокол передачі кадрів PPP через Ethernet
PPTP	–	(Point-to-Point Tunneling Protocol) тунельний протокол точка-

точка

- SIP – (Session Initiation Protocol) протокол передачі даних
- STP – (Spanning Tree Protocol) протокол покривного дерева
- TCP – (Transmission Control Protocol) протокол керування передачею даних
- VLAN – (Virtual Local Area Network) віртуальна локальна мережа
- VPLS – (Virtual Private Local Area Network Service) віртуальна приватна локальна мережа
- VPN – (Virtual Private Network) віртуальна приватна мережа
- VRF – (Virtual Routing and Forwarding) технологія, що дозволяє реалізовувати на базі одного фізичного маршрутизатора мати декілька віртуальних
- WAN – (Wide Area Network) глобальна мережа

ВСТУП

З розвитком суспільства все більше розвивається і методи комунікацій між людьми та місцями їх роботи. Більшість офісів відкривають свої філіали в різних містах, що забезпечує їм велику клієнтську базу та створення робочих місць.

Для організації зв'язку між офісами в різних містах та співробітниками, що можуть працювати віддалено я вибрала технологію VPN-доступу. Вона значно знижує вартість корпоративної мережі за рахунок більш дешевого підключення віддаленого офісу чи співробітника, що працює віддалено (з дому, наприклад).

Організація зв'язку між двома офісами включає в себе безліч факторів. Але в пріоритеті, її мінімальна вартість та надійність при передачі даних, та також мобільність, щоб працівники могли спокійно працювати з дому по захищених каналах передачі.

Приблизно з 2012-2013 років технологія VPN почала активно зростати. В основу такого зростання попиту на цю технологію лягло декілька факторів, а саме: різні геополітичні конфлікти, все більше людей почали користуватися мережею Інтернет, що призвело до зацікавлення для захисту персональних даних, як окремої людини, так і країни в цілому.

Користувачі мережі Інтернет використовують цю технологію, здебільшого, щоб обійти обмеження з боку провайдера чи адміністратора і отримати доступ до різних ресурсів. Найчастіше VPN використовують для організації віддаленого доступу до робочої інформації в корпоративному секторі.

Різкий стрибок у використанні VPN в Україні відбувся 2016 року з блокування російських сайтів, таких як «Вконтакті», «Яндекс» (пошукової системи), «Mail.ru» та багато інших. У зв'язку з цим, більшість мережевих користувачів почали використовувати VPN, щоб обійти державну заборону на доступ до цих сайтів.

Можна виділити основні можливості використання VPN-сервісів у світі: доступ до іншого континенту, соціальних мереж і новин, спілкування, збереження анонімності в мережі провайдера, доступ до робочих файлів (для співробітників віддаленого доступу), приховування місця знаходження та багато іншого. Все більше компаній почали використовувати цю технологію і з цим збільшився його ринок використання та продовжує зростати і в наш час. Навіть, самі провайдери можуть пропонувати дану послугу, все залежить від уподобань як окремого користувача мережі так і підприємства в цілому. На мою думку, головною перевагою використання VPN є те, що створюється захищене з'єднання. При авторизації та аутентифікації через брандмауер, для звичайного користувача відбувається отримання доступу до цієї мережі, що гарантує цю саму «безпеку», для тих, хто скористався послугою VPN.

1 АКТУАЛЬНІСТЬ РОБОТИ ТА ЗАГАЛЬНІ ПРИНЦИПИ ОРГАНІЗАЦІЇ VPN

1.1 Актуальність об'єднання двох офісів у наш час

З розвитком мережі Інтернет відбувається і розвиток бізнесу. Підприємці можуть відкривати свої торгові місця, офіси та т. п., не обмежуючи себе, в плані відстані між головним офісом і його філіалами. Вони можуть бути розташовані як і в різних містах, так і в різних країнах, континентах. Найголовніше те, що обмін між користувачами може проходити миттєво, звісно, в залежності та стабільності Інтернет підключення. Тому при розрахунках варто врахувати якість Інтернет-провайдера, відстань між офісами та штатом співробітників. Організація комунікації між двома офісами спрощує роботу цілої компанії не треба чекати поки дійдуть документи з одного офісу до іншого. Створюючи єдину базу, співробітники можуть обмінюватися файлами всередині цієї мережі. Це дозволяє відкривати філії в різних містах, тим самим створюючи робочі місця. За допомогою використання технології VPN будуть об'єднанні офіси в даній роботі.

VPN (англ. Virtual Private Network – віртуальна приватна мережа) – ця технологія забезпечує зашифроване з'єднання між двома мережами або окремим користувачем та мережею, за її допомоги всі дані користувача при підключенні до Інтернету зашифровуються. Також дана технологія дозволяє забезпечувати одну чи декілька мережевих з'єднань (логічну мережу) на поверхні іншої мережі [1].

Головна ціль VPN полягає у захисті трафіку, тому ця мережа повинна задовольняти деякий перелік потреб і в першу чергу, мати надійну криптографію, гарантований захист від прослуховувань, надійний захист системи управління ключами і криптоінтерфейс, який дозволяє здійснювати крипто операції: захист пошти, програм шифрування дисків і файлів і т.д.

При використанні VPN-технології можна забезпечити:

- захист (конфіденційність і цілісність мережі) інформації, що передається по мережі;
- захист внутрішніх сегментів мережі від несанкціонованого доступу з боку мережі загального доступу;
- ідентифікація і аутентифікація користувача мережевих об'єктів.

В залежності від вимог підприємства щодо захисту, числа сайтів, критичних ситуацій, складності маршрутизації, обсягу трафіку та т.п., можна розділити мережу VPN на три основні види:

- внутрішньокорпоративні VPN (Intranet VPN);
- міжкорпоративні VPN (Extranet VPN);
- VPN з віддаленим доступом (Remote Access VPN).

Один із варіантів, який підійде для організації зв'язку між офісами, що задовольняє вимоги об'єднання кілька окремих між собою ліній в одну єдину, по відкритих каналах буде Intranet VPN (рис. 1.1).

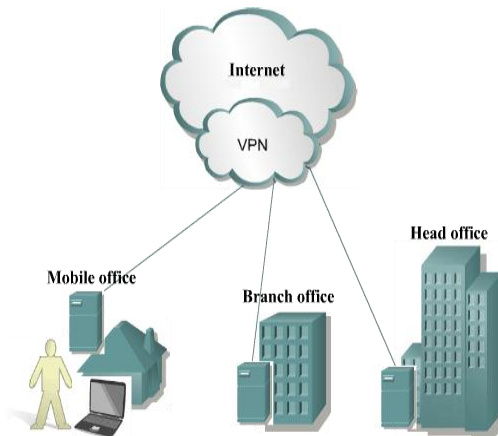


Рисунок 1.1 – Приклад мережі Intranet VPN

1.2 Класифікація VPN-мережі

Розглянемо класифікацію VPN-мережі за різними типами (рис. 1.2).

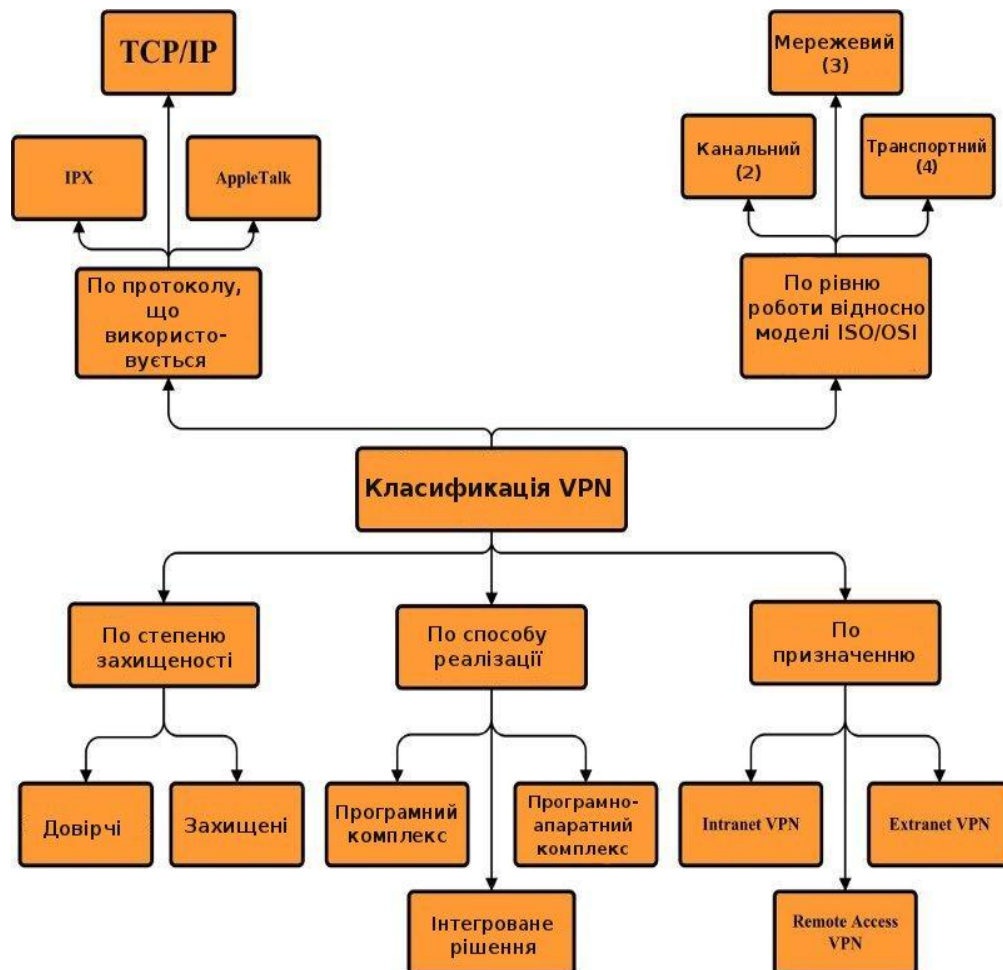


Рисунок 1.2 – Класифікація VPN

VPN можна класифікувати за різними параметрами. Розберемо кожен з цих блоків докладніше.

За ступенем захищеності поділяється на: довірчі та захищені.

Довірчі. Використовуються коли мережу по якій проходить потік даних можна вважати надійною, і одне що залишається, це реалізувати створення віртуальної підмережі в рамках цієї.

Захищені. Найчастіше використовуються коли потрібно створити надійну і захищену підмережу на основі звичайної, наприклад, Internet. Протоколи, які використовуються при даному типі: Ipsec, SSL, PPTP.

По способу реалізації поділяються на:

- програмний комплекс;
- програмно-апаратне рішення;
- інтегроване рішення.

Для функціонування VPN використовують ПК із спеціалізованим ПЗ.

Програмно-апаратне рішення. В даному типі VPN реалізується через використання комплексу спеціальних програмно-апаратних засобів. За їх рахунок забезпечується висока продуктивність та захищеність.

Інтегроване рішення. У цьому випадку реалізацію VPN забезпечує ПАК, який також вирішує задачі щодо організації мережевого екрану, фільтрації трафіку та т.п. [1].

За призначенням Intranet VPN – об'єднує в захищену мережу ряд філій однієї компанії, що знаходяться не на одній місцевості, для обміну по відкритим каналам.

Extranet VPN. Особливість даного типу, що до нього можуть підключатися користувачі поза мережі – клієнти або замовники. В даному випадку, створюються певні правила для даних користувачів, оскільки вони мають менші права, ніж інші співробітники фірми, тому є необхідність обмежувати доступ до бази даних головного офісу або філій.

Remote Access VPN. Застосовується для забезпечення доступу тих співробітників, які працюють з дому. Вони підключаються по захищеному каналу між корпоративною мережею та користувачем.

За типом протоколу. VPN реалізується на таких рівнях реалізації як – TCP/IP, IPX та AppleTalk. Найпоширеніший TCP/IP через те, що більшість рішень підтримує його.

1.3 Функції VPN по захисту даних

Для корпоративної мережі при підключенні до публічної виникає два типи загроз:

- а) несанкціонований доступ до даних при передачі трафіку по публічній мережі;
- б) несанкціонований доступ до ресурсів локальної мережі, отриманий в результаті входу в цю мережу.

VPN базується на трьох методах реалізації:

- а) тунелювання;
- б) екранування;
- в) шифрування.

Особливу увагу варто приділити платформі підключення, де забезпечується конфіденційність даних і аутентифікація.

Захист даних за допомогою функцій VPN полягає в наступному:

– «VPN-агенти» встановлюються на всі комп'ютери, що мають доступ в Internet (або іншу мережу загального користування) – дана функція реалізується на мережевому шлюзі, який обробляє IP-пакети, що передаються мережею.

Використання серверів Windows, Unix, мережевого маршрутизатора і мережевого шлюза, на якому піднято VPN. Реалізується VPN-технологія для корпоративного зв'язку або для об'єднання віддалених офісів.

Розглянемо операції «VPN-агенту», що виконуються перед відправкою IP-пакету:

- а) аналіз IP-адреси одержувача пакета, на основі цієї інформації буде підібрано алгоритм захисту даного пакета. Якщо у налаштуванні VPN-агента нема такого користувача, то пакет буде відкинтий;
- б) контролюється цілісність переданих даних, а саме обчислення криптографічної контрольної суми з використанням ключа шифрування;

в) шифрування пакету разом із заголовком IP-пакету, що містить службову інформацію;

г) інкапсуляція пакету, де формується новий заголовок і замість адреси одержувача, вказується адреса його VPN-агента.

Відбувається зворотній процес при отриманні IP-пакету:

а) спочатку витягується інформація з нового заголовку про VPN-агента, потім проходить « фільтрацію» по списку дозволених, то, якщо пакет не входить в даний список, він відкидається, дана ситуація подібна і коли заголовок пакету пошкоджений випадково або навмисно;

б) підбір ключей для розшифрування цього пакету згідно з налаштуваннями криптографічних алгоритмів та перевірка цілісності;

в) як висновок, після всіх зворотних процесів пакет перетворюється в початковий вигляд і відправляється по локальній мережі справжньому адресату.

Інформаційний потік по загальній мережі передається по захищеному каналу. Для створення цього каналу використовують аутентифікацію, авторизацію та шифрування.

При використанні методів шифрування потрібно врахувати, щоб на кінцях тунелів використовувався один і той самий алгоритм. Також слід врахувати, що для успішного дешифрування даних потрібен обмін ключами між даними джерела і одержувача. Шифрування даних використовується не завжди, оскільки цей процес дороговартісний, що вимагає додаткових приставок із-за чого може страждати швидкість передачі даних маршрутизатора.

Аутентифікація визначає користувача або кінцевий пристрій, дозволяє встановлювати з'єднання лиш між зареєстрованими користувачами, забезпечує безпеку від несанкціонованого доступу інших користувачів до ресурсів мережі. Перевірка проходить в дві сторони, одна доводить свою автентичність, а інша приймає рішення. При аутентифікації застосовується пароль. При застосуванні паролів можуть виникнути ряд недоліків, таких як

їх розкриття, тому при становленні паролю варто подбати про його надійність.

Авторизація – ця процедура проходить після аутентифікації та передбачає надання доступу до ресурсів всім користувачам, що зареєстровані в даній мережі та паралельно виконується контроль санкціонованих користувачів до ресурсів мережі.

1.4 Застосування тунелів для VPN

На рисунку 1.3 показано приклад роботи в режимі «тунелю», де інтрамережі взаємодіють з комп'ютерами інших інтрамереж шляхом маршрутизації пакетів через тунель IPsec між двома шлюзами.

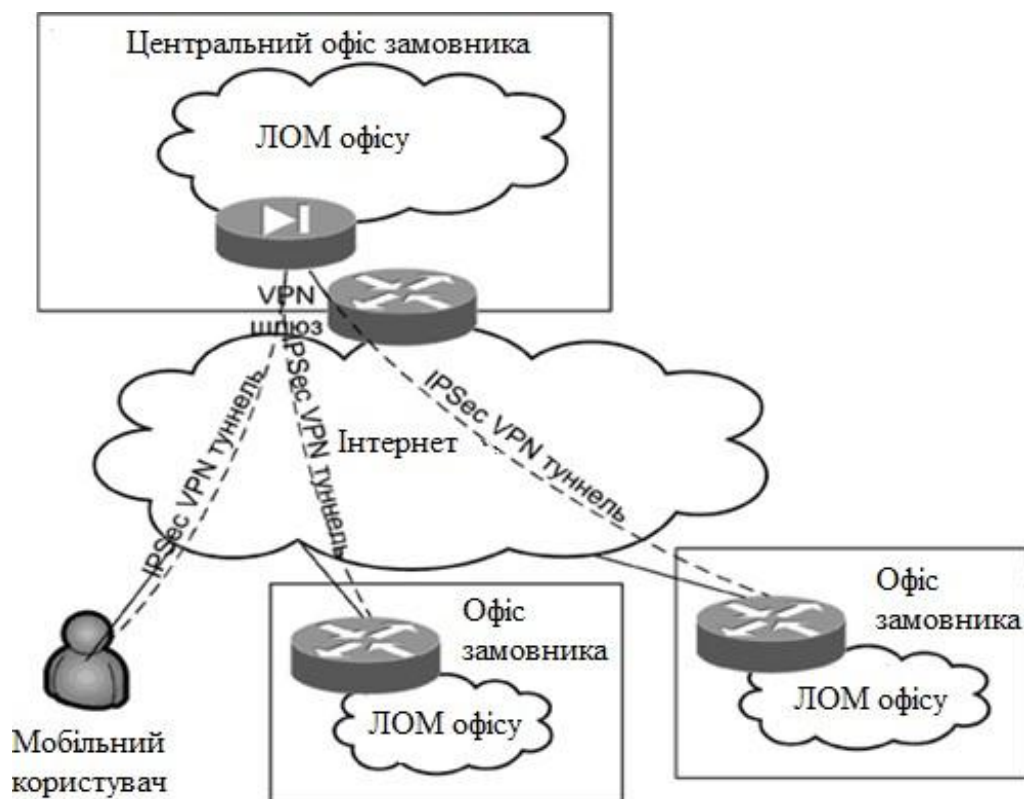


Рисунок 1.3 – Приклад роботи в режимі «тунелю»

Механізм тунелювання в своїй роботі використовує протоколи захищеного каналу. При цій методиці дані передаються через загальнодоступну мережу як по звичайному двоточковому з'єднанню. На рисунку 1.4 показано, як між кожною парою «відправника-одержувача даних» виникає «тунель» – безпечне логічне з'єднання, за допомогою якого відбувається інкапсуляція даних одного протоколу в пакети іншого.

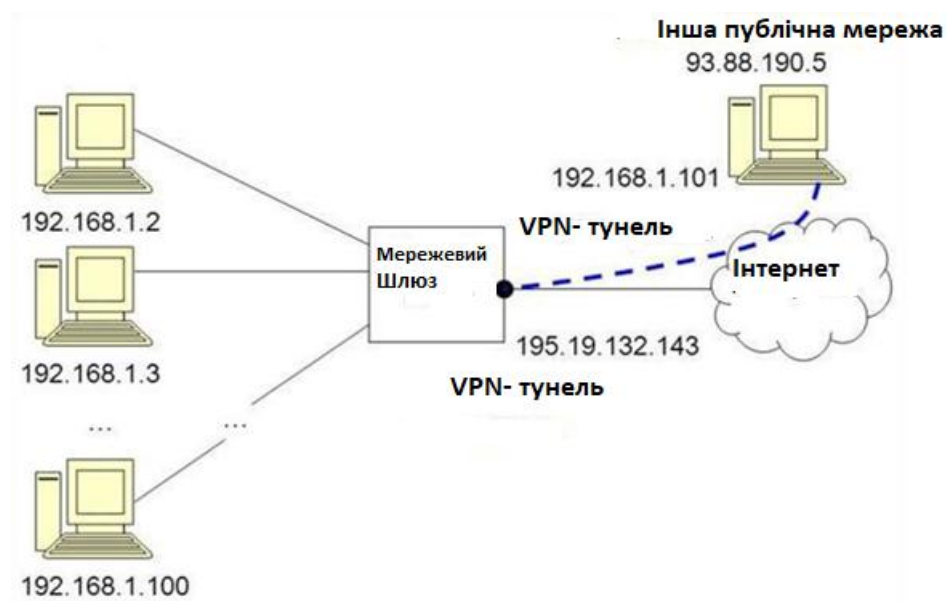


Рисунок 1.4 – Приклад тунелювання

«Політика безпеки» – це правила, які прописані в налаштуваннях VPN-агентів, для створення тунелів. Проходить сортування IP-пакетів при направленні в той чи інший тунель. Перевірка проходить в декілька етапів:

- IP-адреса джерела;
- IP-адреса призначення;
- протоколу до якого належить даний пакет даних;
- інформація про номер порта з якого відправлено дані.

За допомогою цього процесу пакет протокола з нижчим рівнем переходить в поле даних пакета до більш високого або такого ж самого.

Даний механізм застосовується для безпеки передачі інформації по публічній мережі шляхом інкапсуляції пакетів під зовнішню оболонку. Розміщується тунель між двома пристроями, що межують між собою, які розміщуються в точках доступу в мережу. Візуальне зображення тунелю показано на рисунку 1.5.

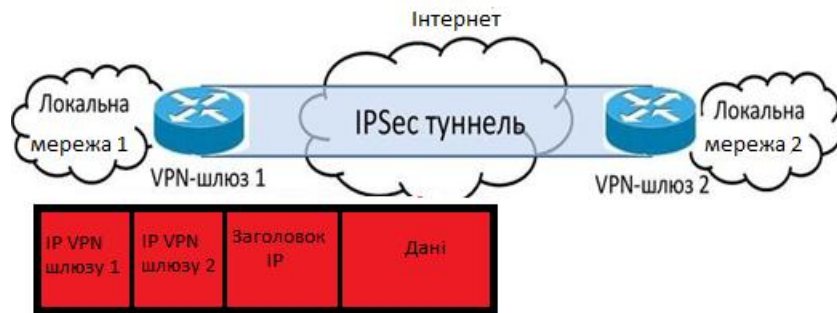


Рисунок 1.5 – Приклад «тунелю»

За допомогою даної технології можна зашифрувати вихідний пакет повністю, сюди входить і заголовок, і все поле даних. Далі даний зашифрований пакет поміщається в інший, але з відкритим заголовком. Для транспортування по загальній мережі ми використовуємо даний заголовок. Зашифрований заголовок витягується з кінцевої точки захищеного каналу і буде використаний для подальшої передачі даних. Тунель, більше за все, використовують на ділянках мережі загального доступу, де особливо варто приділити увагу конфіденційності і цілісності даних.

Також варто відзначити, що механізм тунелювання застосовують для забезпечення цілісності та автентичності, а не тільки для захисту при передачі інформації. При транспортуванні даних також виникає потреба в тунелюванні, а саме: узгоджується різні транспортні технології, наприклад, якщо дані одного транспортного рівня необхідно передати через транзитну мережу з іншим протоколом.

Розглянемо які протоколи використовують для формування VPN: PPTP, IPsec, IP-IP, L2TP. При застосуванні протоколу PPTP – проходить інкапсуляція IP-, IPX-і, NetBEUI – трафіку в заголовки IP для передачі по IP-мережі, наприклад Internet.

За допомогою протоколу L2TP відбувається шифрування і передача IP-трафіку з використання будь-яких протоколів, що підтримують режим «точка-точка» доставки датаграм. Сюди можна віднести протокол IP, асинхронний режим передачі (ATM) і ретрансляцію кадрів.

При використанні протоколу IPsec можна зашифрувати та інкапсулювати корисну інформацію IP протоколу в заголовки IP для передачі по IP-мережі (рис. 1.6).

Модель OSI	Протоколи захищеного каналу
Прикладний	MIME
Представлення	SSL, TLS
Сеансовий	
Транспортний	
Мережевий	IPSec
Канальний	PPTP
Фізичний	

Рисунок 1.6 – Модель OSI, протоколи захищеного каналу

1.5 Побудова VPN-мережі

Починаючи побудову VPN-мережі, варто приділити увагу вибору технології та оптимальному варіанту, що підходить підприємству.

Розглянемо такі варіанти технологій, як MPLS VPN, IPsec VPN, VPN, що базується на технології тунелювання PPTP, L2TP. Спільне для всіх цих технологій, те що трафік надходить в мережу провайдера за протоколом IP, що дозволяє провайдеру надавати доступ не тільки послугу VPN, але і інших таких як, контроль роботи клієнтської мережі, хостинг поштових служб і спеціалізованих додатків клієнта.

На рисунку 1.7 зображено загальний вигляд варіанту побудови ВПМ, що базується на загальнодоступній мережі провайдера. Мережа кожного клієнта розподілена на територіальні офіси, що з'єднуються між собою «тунелями» та проходять через мережу провайдера.

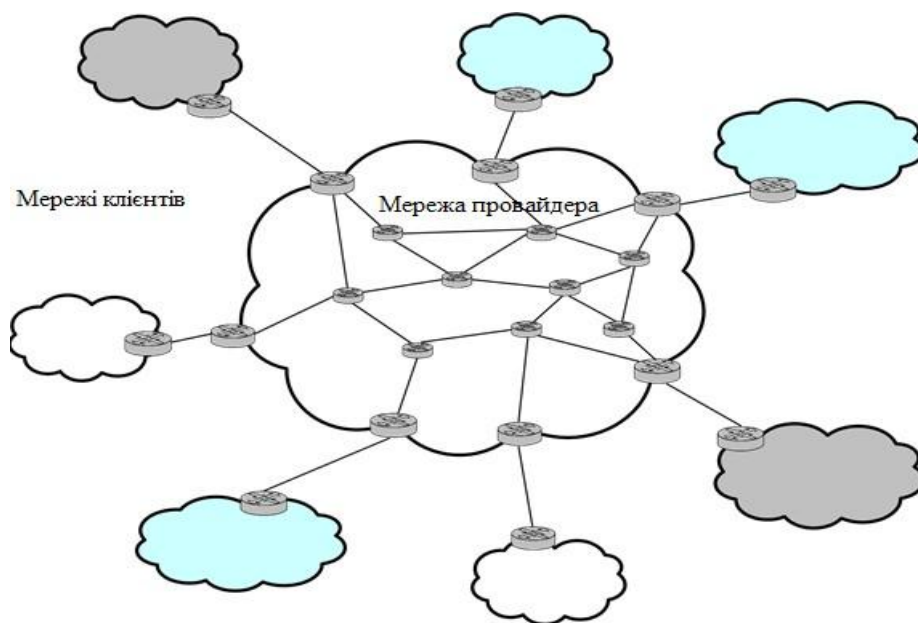


Рисунок 1.7 – Загальний вигляд віртуальної приватної мережі

До найбільш поширених і популярних технологій VPN, можна віднести Internet Protocol Security. При застосуванні стандарту IPsec, ми отримуємо високий рівень гнучкості, що в подальшому дозволяє вибрати потрібний режим захисту даних і використати різні алгоритми шифрування і аутентифікації. Використовуючи інкапсуляцію пакетів можна ізолювати

адреси клієнта і провайдера за рахунок застосування двох IP (зовнішнього і внутрішнього).

Для тих VPN, що підтримуються провайдером, застосовується IPsec – ті тунелі, що в них будуються використовують базу пристроїв клієнта, але конфігурація відбувається віддалено безпосередньо під управлінням провайдера.

Щодо встановлення і захищення каналу за допомогою IPsec, можна вирішити такі завдання:

- при ініціалізації каналу проходить аутентифікація користувачів або комп'ютерів;
- при передачі даних між кінцевими точками відбувається шифрування і аутентифікації;
- автоматичне постачання точок секретними ключами для забезпечення роботи протоколів аутентифікації і шифрування.

Дана технологія має ряд недоліків, вона реалізує тільки захищеність та ізолюваність адресного простору. Відсутня підтримка пропускну здатності та інших параметрів QoS та орієнтована виключно на IP-протокол.

Метод тунелювання через IP для створення VPN, включає в себе всі методи, що використовують «тунелі» через IP-мережу. При даному методі відбувається ізолювання адресного простору користувача, що в свою чергу надає можливість переносити незахищений трафік клієнта (L2TP) або шифрувати його (PPTP).

За допомогою протоколу PPTP відбувається підтримка управління потоками даних і багатопротокольне тунелювання, що базується на IP-протоколу. Користувачам з віддаленим доступом даний протокол дозволяє отримувати доступ до бази даних корпоративної мережі через підключення по телефонній лінії до місцевого провайдера, обходячи пряме підключення до мережі компанії. PPTP – забезпечує кожному клієнту, що знаходиться віддалено, сполучення з потрібним сервером. Це спрощує роботу мережевих адміністраторів, які повинні забезпечувати підтримку всіх користувачів

віддаленого доступу, але хочуть з економити на обслуговуванні мережевих каналів віддаленого доступу. Специфікації L2TP розробляє IETF, основний напрямок спрямовано на підтримку багатопроTOCOLьного тунелювання та забезпечення сумісності всіх продуктів L2TP.

Основними недоліками L2TP і PPTP протоколів – відсутність вбудованих алгоритмів шифрування.

Розглянемо технологію MPLS VPN, вона поділяється на дві області:

- IP-мережа користувачів;
- магістральна мережа провайдера, що виконує об'єднання клієнтів у єдину мережу.

Для кожного клієнта, у загальному випадку, може бути відокремлено кілька територіальних IP-мереж, які у свою чергу, входять у підмережі, що зв'язані маршрутизаторами. Даний тип територіально ізольованих мережевих елементів корпоративної мережі, має назву – сайт. Обмін файлами, що належать одному клієнту, проходить через мережу провайдера MPLS, тим самим утворюють віртуальну приватну мережу цього користувача. В середині сайту обмін інформацією проходить по одному з внутрішніх протоколів маршрутизації IGP.

Структура MPLS VPN складається з трьох основних компонентів мережі:

- граничний маніпулятор клієнта – Customer Edge Router, CE;
- внутрішній маршрутизатор магістральної мережі провайдера – Provider Router, P;
- граничний маршрутизатор мережі провайдера – Provider Edge Router, PE.

За допомогою граничного маршрутизатора клієнта відбувається підключення сайту користувача до внутрішньої мережі провайдера. Дані маршрутизатора, що належать клієнту, нічого не знають про існування VPN. Граничні маршрутизатори мережі провайдера проходять через маршрутизатори CE сайтів клієнта та внутрішні маршрутизатори мережі

провайдера. При взаємодії CE і PE відбувається реалізація на основі стандартних протоколів стеку TCP/IP.

Різні сайти не обмінюються маршрутною інформацією безпосередньо, і навіть, можуть не знати один про одного, це відбувається при використанні – CE-маршрутизатора сайтів. Входячи до складу VPN адресні простори підмережі, мають здатність перекриватися, це означає, що унікальний адрес дотримується тільки, безпосередньо, в межах конкретної підмережі. Таке стало можливим при використанні IP-адреси в VPN-IP-адресу і використовуючи для роботи з цими адресами протоколу MP-BGP. До одного сайту відносяться CE-маршрутизатори, але сам сайт може належати до кількох VPN. До PE-маршрутизатор може бути підключено декілька CE-маршрутизаторів, що відносяться до різних VPN та знаходяться на різних сайтах.

CE – маршрутизатори можуть не підтримувати технологію багатопроTOCOLьної комутації, підтримка MPLS потрібна тільки для маршрутизатора внутрішніх інтерфейсів PE, та для всіх інтерфейсів маршрутизаторів Р. Граничні маршрутизатори мережі провайдера являються більш складними по своїй функціональній побудові. Вони забезпечують функції підтримки VPN таких як: розподіл маршрутів та даних, що приходять від різних клієнтів, також ці маршрутизатори виступають кінцевими точками шляхів LSP між сайтами замовника.

Виконується закономірність, для кожного PE-маршрутизатора підтримується стільки таблиць маршрутизації, скільки користувачів на сайті, при цьому відбувається організація кілька віртуальних каналів на одному фізичному. Сама маршрутна інформація, що має відношення тільки до конкретної VPN, знаходиться тільки в PE-маршрутизаторах. Це вирішує проблему масштабування, яка виникає в разі наявності цієї інформації на всіх маршрутизаторах мережі оператора.

Створюється асоційована таблиця маршрутизації для кожного нового сайту-клієнта через PE, для кожної таблиці присвоюється один або кілька

атрибутів RT, що визначають набір сайтів при вході в конкретну VPN. При асоціації маршруту з атрибутом VPN of Origin, заодно проходить ідентифікація групи сайтів та відповідних маршрутів.

Розподіл маршрутизатора PE відбувається між клієнтськими сайтами і зоною ядра провайдера. Розташування інтерфейсів відбувається таким чином: по один бік інтерфейси, через які PE взаємодіють з маршрутизаторами P, з іншого боку інтерфейси, до яких під'єднані самі користувачі. Відбувається надходження оголошень про маршрути магістральної мережі, з одного боку, а з іншого – про маршрути в мережах користувачів.

Якщо обмежується область поширення маршрутної інформації межами окремих VPN, це призводить до ізоляції адрес кожної VPN, що в свою чергу дозволяє застосувати і її межах як адреси загального доступу, так і приватні адреса. Усі адреси адресного простору однієї VPN призначається префікс, розрізнявач маршрутів (Router Distinguisher, RD), що забезпечує унікальний ідентифікатор для VPN. Завдяки цим діям на маршрутизаторі PE всі адреси, що відносяться до різних VPN, обов'язково будуть мати різні IP-адреси, навіть, якщо одна частина адреси буде збігатися.

Для обміну маршрутної інформації між сайтами кожної окремої VPN використовують управління протоколу MP-BGP (Multiprotocol BGP). У даному типі відсутнє шифрування і аутентифікація, як при IPsec, але при цьому є можливість застосування додаткових заходів захисту, таких як Traffic Engineering або DiffServ.

При побудові захищеної корпоративної мережі на базі приватної мережевої інфраструктури однієї компанії використовують VPN MPLS. Використовуючи цей варіант ми отримаємо ряд переваг, таких як застосування IP-протоколу з безпекою приватних мереж та якість обслуговування, які надає технологія MPLS.

Найбільш ефективно дана технологія підійде для створення корпоративного простору для електронної комерції, що в свою чергу

забезпечує єдине мережеве середовище для підрозділів корпорації і організацію екстра мережі. Також вони можуть стати основою для електронної комерційної діяльності підприємства.

2 ПОСТАНОВКА ЗАВДАННЯ НА ЇЇ ВИКОНАННЯ

2.1 Постановка задачі

Щоб об'єднати офіси потрібно побудувати транспортну мережу інфокомунікацій, для цього будемо використовувати сучасні технології.

Метою даного дипломного проекту організація об'єднаного доступу двох офісних мереж в єдину мережу за допомогою VPN-доступу. Основні цілі даної роботи:

- спроектувати мережу головного офісу;
- спроектувати мережу філії;
- розрахунок трафіку, що передається в мережі головного офісу;
- розрахунок втрат трафіку для створеної мережі.

Для моєї дипломної роботи я вибрала офіси, що знаходяться в двох містах, на відстані 600 кілометрів, тому прокладка кабелю між ними буде економічно не вигідною. Треба забезпечити шифрування каналів між офісами, щоб оберегти важливі файли від витоку інформації у вільний доступ.

Компанія займається розробкою мікросхем на акустичні прилади різного виду і варіацій, від динаміків, радіоприладів до авто магнітол. Тому, перш за все, повинна бути налагоджена передача файлів електричних схем, креслень.

В офісах знаходиться обладнання одного типу, тільки в різних кількостях, в залежності від потреб співробітників. Транспортна мережа повинна забезпечувати Інтернет, телефонію та конференц – зв'язок між офісами.

Також наша ціль створити захищений канал передачі даних між офісами для безпечного обміну інформації та доступу до бази даних на сервері центрального офісу.

2.2 Загальні положення для створюваної мережі

Компанія складає з себе:

- а) головний офіс в місті Києві;
- б) віддалений офіс в місті Запоріжжі.

Кількість співробітників в офісах:

а) у першому офісі 16 осіб з них: 1 – гендиректор, 1 – начальник відділу автоматизації, 1-маркетолог, 1 – головний бухгалтер, 2 – співробітники відділу бухгалтерії, 1 – інженер проектувальник та 9 – співробітників;

б) у другому офісі 34 особи з них: 1 – керівник філіалу, 1 – бухгалтер, 1 – інженер проектувальник, 1 – співробітник відділу автоматизації та 30 – співробітників.

Визначимо основні положення для транспортної мережі інфокомунікацій:

- доступ до бази даних головного сервера повинен бути і у філіалу та співробітників, що працюють віддалено, якщо такі є;
- забезпечення всіх видів зв'язку між двома офісами (телефонний, інтернет, факсимільний та конференц-зв'язок);
- визначення пріоритетів доступу до мережевих ресурсів компанії.

Варто детальніше розібрати рівні доступу, котрі будуть доступні окремим користувачам в мережі, хто може мати доступ до всіх файлів компанії, хто до окремих підрозділів та право редагування.

Виділимо 5 рівнів доступу для даної топології.

Перший рівень – об'єднує в собі доступ до бази даних, отримувати та редагувати її, інформацію по бухгалтерії, FTP, файлових та поштових серверів головного офісу та філіалу, доступ до мережі. Доступ до цього рівня мають генеральний директор, бухгалтер, маркетолог і головний інженер.

Другий рівень – об'єднує в собі дозвіл отримувати інформацію з бази даних, FTP, файлових та поштових серверів, доступ в мережу. Доступ до

даного рівня мають керівник філіалу, інженер проєктувальник, офісні інженери.

Третій рівень – об'єднує в собі доступ до бази даних бухгалтерії, загальної бази даних, FTP, файлового серверу, але тільки в межах свого офісу. Даний рівень мають бухгалтери всіх офісів.

Четвертий рівень – для всіх співробітників компанії, вони мають доступ до бази даних, поштового серверу, FTP, файлового серверу в межах своєї філії / офісу.

П'ятий рівень – даний рівень забезпечує доступ до всіх ресурсів мережі для оптимізації та механізації роботи. Доступ до цього рівню мають начальник відділу автоматизації та інші співробітники цього відділу.

Для забезпечення стабільної роботи, економічності та швидким обміном інформації між офісами необхідно забезпечити розвинену інфокомунікаційну мережу. Це найголовніша задача при створенні комп'ютерної мережі, тому що треба забезпечити контроль над виробничими процесами в режимі реального часу без затримок. Також, варто звернути увагу на надійність комп'ютерної мережі, тому що відмова однієї ланки може призвести до матеріальних збитків та перериванню роботи кожного окремого співробітника.

Для наших офісів ми створимо локальну мережу в середині кожного із них, а далі вони будуть об'єднані між собою регіональною мережею.

Центральний офіс являє собою центр, в якому буде зберігатися база даних, у якій буде зберігатися вся інформація офісів. Тому ТМІ для даної структури повинна мати велику стресостійкість та мати гарантійну роботу в 99.98% випадків. Також, варто звернути увагу на гнучкість мережі, щоб у випадку її розширення можна було легко перелаштуватись – це масштабність мережі.

Необхідно вибрати обладнання, скласти проєкт мережі, виконати монтаж комунікацій локальної мережі для забезпечення стабільної роботи в середині офісу. Зазвичай, для цих робіт можуть бути наняті спеціальні

робітники, які безпосередньо спеціалізуються на даній роботі, знають специфіку прокладки кабелю, щоб була створена надійна мережа з мінімальними втратами при передачі даних.

Перш за все варто звернути увагу на безперебійну роботу мережі в разі відключення електроживлення. Джерела безперебійного електроживлення, серед даного роду різноманіття приладів на ринку, необхідно вибрати прилад, який буде задовольняти потреби підприємства через те, що даний прилад впливає на роботу та строк служби всіх інших електроприладів в приміщенні. Перш за все ДБЖ впливає на вихід $\sin$ за межі відхилення ($220 \pm 10\%$) і вирівнює напругу, що своєю чергою впливає на економію підприємства і збільшує строк служби приладів на 20-30%.

Для підприємства будемо будувати локальну мережу по ієрархічному принципу, тобто відокремимо один або декілька спец. комп'ютерів – серверів. На місті серверу буде високопродуктивний ПК з серверною операційною системою, захистом від збоїв і т.п. На даному сервері буде зберігатися вся інформація, яку будуть використовувати інші комп'ютерні мережі. Це дає нам змогу контролювати дану мережу, хоча її створення та обслуговування більш затратне.

Виділимо основні плюси ієрархічної мережі:

- забезпечення високого рівня безпеки;
- при виході зі строю робочих станцій, не відбивається на роботі основної мережі в цілому;
- організація локальної мережі з великою кількістю робочих станцій;
- з сервера відбувається централізоване адміністрування мережі.

Дана модель має свої недоліки:

- при створенні виділених серверів підвищується загальна вартість мережі;
- при підборі співробітників варто звертати увагу на їх знання в ІТ-технологіях і адмініструванні домену;

– для стабільної роботи мережі використовувати резервні канали, це дає можливість уберегти дані від втрат при збоях або несправностях мережі.

Використання VPN-каналів дасть нам змогу об'єднати воедино локальні мережі, швидкість по ним не залежить від часових проміжків (днів тижня чи часу в добі). Це дуже добре буде при використанні IP-телефонії, для забезпечення високої якості зв'язку, що надходить корпоративною мережею.

В приватній чи публічній мережі VPN з'єднання являє в собі підключення «точка-точка». Через тунельні протоколи на основі TCP/IP протоколів VPN-серверу відбувається використання VPN-клієнтів для віртуального спілкування. Зазвичай, реалізація VPN-клієнту ініціюється по Internet віртуальне підключення типу «точка-точка» до віддаленого сервера. Даний сервер приймає виклики, перевіряє оригінальність тієї сторони, що робить виклик і передає дані між VPN-клієнтом та приватною мережею.

Добавляється заголовок (інкапсуляція) для емуляції каналу типу «точка-точка». В нього входять дані про маршрутизацію, які забезпечують проходження по приватній мережі чи загальній до кінцевого пункту. Особливо, приділяється роль шифруванню при проходженні пакету, без відповідного ключа його неможливу розшифрувати. VPN-підключення це назва каналу, на якому передаються приватні дані в інкапсульованому і зашифрованому вигляді.

З ВИКОНАННЯ ПОСТАВЛЕНОЇ ЗАДАЧІ

3.1 Вибір обладнання для створення мережі

Для офісної мережі варто звернути увагу на вибір обладнання. Так як ми маємо два офіси, то обладнання буде ідентичним.

Вибір кабелю для з'єднання робочих станцій.

Для надійної роботи системи треба звернути увагу на вибір кабелю, котрий буде з'єднувати робочі місця між собою. «Каркасом» буде слугувати кабель виті пари стандарту 5Е, даний кабель за своїми характеристиками підходить для побудови комп'ютерних мереж. Кабель має пропускну здатність до 1 Гбіт/с, робоча частота 125 МГц. Кабель має 4 пари, котрі у свою чергу мають свій варіант скручування. Даний кабель чудово підходить для стандартів типу Ethernet, 100Base-TX та 100Base-T. Вони бувають двох видів тверді та гнучкі, краще за все вибрати варіант кабелю гнучкого типу тому, що прокладка кабелю в середині офісу передбачає собою різні види деформацій, а коли кабель з легкістю їм піддається, то це спрощує роботу в його монтуванні. Кабель твердого краще застосовувати для прокладки в таких місцях, де не буде заломлень (в середині стіни, біля роз'ємів, що не пропускають ізоляцію). Матеріал даного кабелю складається з провідників типу AWG 24-26 та міді. Радіус згину кабелю має не менше, ніж 4 зовнішніх діаметрів цього кабелю. Протяжність до 100 метрів на більшій відстані потрібно підключати активне обладнання (повторювачі чи комутатори).

Даний кабель показаний на рисунку 3.1. Він буде використовуватися тільки для з'єднання робочих місць між собою. Також нам необхідно резервний шматок кабелю у випадку розширення чи заміни. При їх прокладанні коропи також повинні мати резерв приблизно до 20% у випадку розширення мережі. Тобто, при виборі кабелю варто звернути увагу на його довговічність і місце де буде прокладка, адже для того щоб запобігти виходу мережі зі строю, треба до цього віднестися відповідально.



Рисунок 3.1 – Кабель витої пари типу 5Е

Вибір активного обладнання для офісу.

При виборі активного обладнання для початку виберемо технологію в нашому випадку при побудові локальної мережі був застосований стандарт типу 100BaseT, даний тип забезпечує відповідну швидкість для передачі даних в середині мережі.

Маючи в головному офісі 16 робочих місць краще за все взяти комутатор на 24 порти і такий самий у якості резервного. Вибір став на комутаторі компанії D-link DES-1100-24. Пропускна здатність до 100 Мбіт/с, управляти даним комутатором просто, можна робити це за допомогою програми SmartConsole або при використанні Web-інтерфейсу. Він має такі функції:

- віддзеркалення портів;
- статистика;
- IGMP Snooping, що в свою чергу збільшує трафік всередині мережі;
- Loopback Detection, застосовується для відключення портів у яких з'явилися петлі.

Дані комутатори підтримують функцію VLAN, що дозволяє контролювати смугу пропускання для кожного порту. Тобто, він обмежує вхідний або вихідний трафік до мінімуму 512 кбіт/с. Комутатор може блокувати пакети або взагалі їх відкидати, щоб не перевантажувати мережу. Віддзеркалення мережі застосовується у тих випадках, коли адміністратору

варто прослідкувати проходження трафіку, продуктивність комутатора для діагностики даних. На рисунку 3.2 зображено комутатор який підходить по характеристиках нашому офісу.



Рисунок 3.2 – Комутатор D-link DES-1100-24

При виборі маршрутизатору для офісу звернемо увагу на такі характеристики:

- максимальна кількість підключених робочих місць;
- швидкість передачі даних;
- наявність функції VPN доступу;
- функції по захисту даних;
- простий інтерфейс програми по налаштуванню.

Під наші мінімальні вимоги попав маршрутизатор фірми TP-LINK TL-ER7206, який зображено на рисунку 3.3.



Рисунок 3.3 – Маршрутизатор фірми TP-LINK TL-ER7206

Даний маршрутизатор має такі функції і основні характеристики:

- L2TP, PPPoE, PPTP, VPN;
- частота роботи Wi-Fi – 5 ГГц;
- стандарт роботи Wi-Fi – 802.11 b/g/n/ac;
- швидкість передачі даних – до 300 Мбіт/с;
- швидкість LAN/WAN портів – до 1 Гбіт/с.

Підтримує такі функції безпеки:

- захист від Dos-атак;
- між мережевий екран SPI;
- фільтрація MAC-адрес.

Даний маршрутизатор підтримує VPN-підключення IPsec/PPTP/L2TP за допомогою протоколу IPsec/SSL. Підключення до 100 абонентів по порту LAN-to-LAN Ipsec, по програмі OpenVPN – 50 підключень. По 50 підключень припадає на L2TP, PPTP VPN. Для шифрування і передачі даних, а також управління і розвиток мережі використовують автоматичне VPN-підключення Ipsec, яке спрощує налаштування VPN.

Використання функції фільтрації трафіку. Маршрутизатор встановлює певні параметри для користувачів мережі за допомогою фільтрації IP/ MAC/ URL-адрес і списку управління (ACL). Використання порту аутентифікації для спрощення за контролем трафіку шляхом фіксації, аутентифікації і класифікації для всіх користувачів, які мають доступ. Також, можна розділити трафік між своїм користувачем і гостем мережі, кожному з них можна відокремити певний сегмент трафіку мережі [4].

Для зберігання даних у нашому офісі буде використано 5 серверів, дана кількість підрахована під загальні вимоги компанії. У якості серверу буде виділений комп'ютер. Найголовніше, варто звернути увагу на великий об'єм пам'яті та стабільність його роботи, особливості резервування даних. Через те що, наш офіс є центральним і вся інформація буде зберігатися у ньому, треба підібрати потужний комп'ютер.

У якості серверу буде використано прилад Dell PowerEdge T110. Його особливості:

- чотирьох ядерний процесор типу Xeon;
- підтримка великої кількості операційних систем і програм візуалізації;
- оперативна пам'ять представлена модулями 1,2,4,8 Гбайт. В сервері налічується чотири компоненти, які встановлюють в комірці DIMM. Максимальний об'єм оперативної пам'яті може дорівнювати 32 Гбайт;
- система підтримує жорсткі диски і накопичувачі малого і великого типорозміру.

Дана модель має ряд переваг:

- використання консолідації внутрішньої інфраструктури, за допомогою якої кожний співробітник отримує доступ до будь-якої бази даних будь-якого комп'ютера, якщо немає обмежень;
- за допомогою вбудованих опцій шифрування відбувається забезпечення конфіденційності внутрішньої інформації. При цьому з боку адміністратора може встановлюватися певні рівні доступу до тієї чи іншої бази даних;
- простий у встановленні програмного забезпечення [3].

На рисунку 3.4 зображено сервер даного типу, що описаний вище.



Рисунок 3.4 – Виділений сервер Dell PowerEdge T110

Вибір іншої техніки та ПЗ.

Для організації телефонного зв'язку в компанії будемо використовувати IP-телефонію.

IP-телефонія – простими словами, це телефон котрий виконує свою діяльність через комп'ютерну мережу. Передача сигналу відбувається у цифровому вигляді, що спрощує його шифрування, якщо воно необхідне. У офісі буде використовуватися IP-телефонія з провідним підключенням до мережі. Виділимо переваги використання даного виду IP-телефонів:

- порівнюючи з усіма видами обладнання VoIP являються найнадійнішими;
- мають простий інтерфейс налаштування;
- при підключенні до SIP відсутнє проміжне обладнання (тільки маршрутизатор), мають високу надійність, рідко виходять з ладу, живлення надходить від мережі, тому вони стабільно тримають SIP реєстрацію;
- гарна якість зв'язку;
- довгий строк служби.

На рисунку 3.5 зображено IP-телефон який буде використовуватися в межах нашого офісу.



Рисунок 3.5 – IP-телефон Panasonic KX-HDV130

Для ведення бухгалтерського обліку в мережі офісу буде використовуватися програма 1С. Налаштувати дану програму може і сам бухгалтер, враховуючи всі потреби для розрахунків. Дана програма виступає основною в якості рішення для ведення обліку та аудиту та має відносно недорогу вартість, що ідеально підходить для нашого підприємства [5].

3.2 Проектування мережі головного офісу

Проектована нами мережа центрального офісу виділяється як головний центр приймання, обробки, передачі даних з усіх офісів, у нашому випадку з філіалу в місті Запоріжжі. На рисунку 3.6 показана схема фізичної топології центрального офісу.

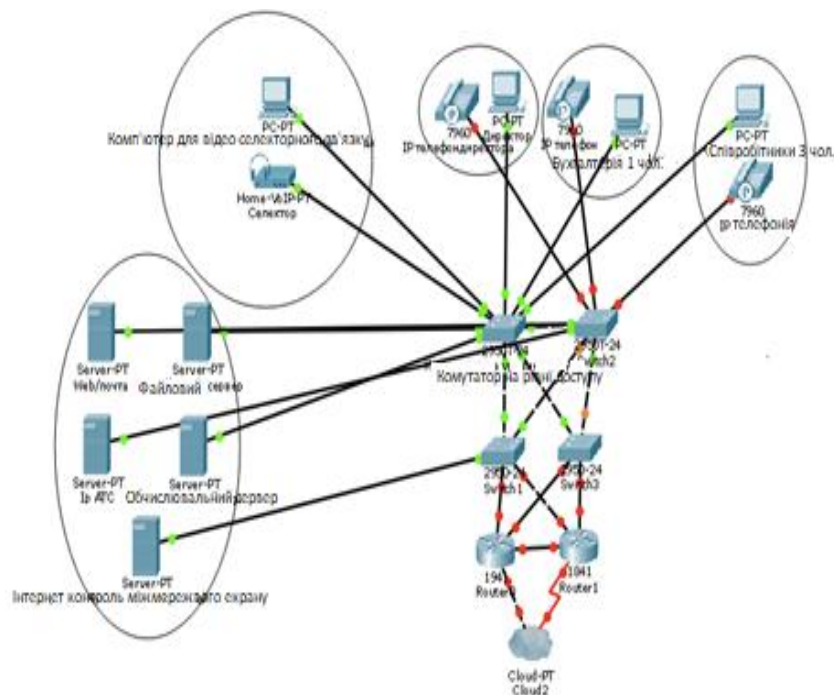


Рисунок 3.6 – Схема фізичної топології центрального офісу

Наш офіс має типову локальну мережу для невеликого офісу. В офісі налічується десять локальних розеток з них, п'ять буде використовуватися

для постійної роботи, в них увімкнені персональні комп'ютери кожного співробітника і п'ять про запас, у випадку розширення штабу. До столу кожного співробітника підведена IP-телефонія і всі ці пристрої підключені до комутатору, який розміщений в окремому приміщенні. В даному приміщенні зібраний комутаційний вузол і сервер, кількість серверів, що знаходяться у цій кімнаті поділяються на сервер електронної пошти, контролю трафіку, web-сервер, сервер IP АТС, файловий сервер та сервер бухгалтерії, ці п'ять серверів обслуговують офіс. До цього приміщення підведені оптоволоконні лінії зв'язку провайдера.

Також дане приміщення відведене для створення відеозв'язку, у вигляді групового чату, що дозволяє брати участь у зборах до 80 людей, вони авторизуються за допомогою логіну та паролю, при цьому максимальна кількість користувачів, що може одночасно знаходитись з увімкненим зображення не більше трьох: ведучий, доповідач і промовець.

Розподілити учасників, умовно, можна на дві групи:

- доповідачі – ті хто, надають певну інформацію з використанням звуку і зображення, від них надходить доступ до всіх інших користувачів (ведучий, доповідач і т.д.);
- глядачі – це всі інші авторизовані користувачі. Вони не мають доступу до показу зображення, але можуть надсилати до чату повідомлення друкованого типу або аудіо, якщо це дозволяє їм клієнтський інтерфейс даного додатку.

При здійсненні конференції вибирається ведучий котрий має такі функції:

- відбір учасників на конференцію;
- розподіл і передача ролі доповідача між учасниками;
- передача ролі промовця для підбивання підсумків конференції.

Щоб наша робота була стабільною треба забезпечити відповідне, інтернет підключення зі швидкістю вихідного трафіку – 128 кбіт/с, вхідного – 384 кбіт/с.

Перш за все топологія мережі головного офісу повинна витримувати велике навантаження та забезпечувати стабільну роботу всієї системи. Для забезпечення цієї самої роботи варто звернути увагу на вибір маршрутизаторів та комутатора.

Маршрутизатор – мережевий пристрій, який має мережевий інтерфейс, відповідає за передачу даних в середині вибраної топології маючи свою таблицю маршрутизації.

Комутатор – мережевий пристрій, робота якого заключається в об'єднанні вузлів комп'ютерної мережі в межах одного або декількох сегментів цієї мережі. Робота даного приладу відбувається на канальному рівні моделі OSI.

Для даного офісу можна вибрати два комутатори на 24 порти, для основного використання і для резервного. Варто звернути увагу, що при розподілі співробітників на групи, комутатор повинен бути з підтримкою VLAN.

VLAN – це віртуальна локальна мережа, що являє собою групу об'єднаних між собою хостів із загальним набором потреб, що взаємодіють між собою, так ніби підключені до одного домену не вважаючи на їх фізичне розташування.

Проксі-сервер – за допомогою нього, виконуються непрямі запити до ресурсів мережі. В першу чергу відбувається з'єднання клієнта з проксі-сервером і посилається на який-небудь ресурс (e-mail), що розташовується на іншому сервері. Далі відбувається підключення проксі-серверу до конкретно заданого сервера та отримання ресурсу у нього або відновлення ресурсу з власного кешу (для тих випадків, якщо він є у проксі-сервера). Також проксі-сервер може зберігати анонімність користувача в мережі і захищати комп'ютер клієнта від мережевих атак (рис. 3.6) [2].

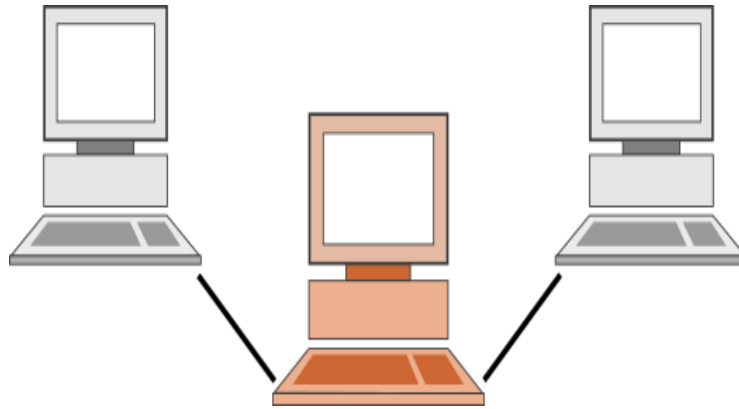


Рисунок 3.6 – Схематичне зображення проксі-серверу, де комп'ютер в середині діє як проксі-сервер між двома іншими

Використовувати проксі-сервер можна для доступу до бази даних, наприклад 1С, при віддаленій роботі філіалу. Щоб підтримати стабільність роботи, треба задати її пріоритетність ACL.

До нашої мережі підключені комп'ютери які мають статистичний IP-адрес, що дає нам змогу обмежити доступ до окремих груп по цьому критерію. Основний пріоритет буде у директора компанії, бухгалтера і директора філіалу.

3.3 Проєктування мережі для філіалу

На відстані 600 км від центрального офісу розташований філіал. На рисунку 3.7 показана схема фізичної топології центрального офісу.

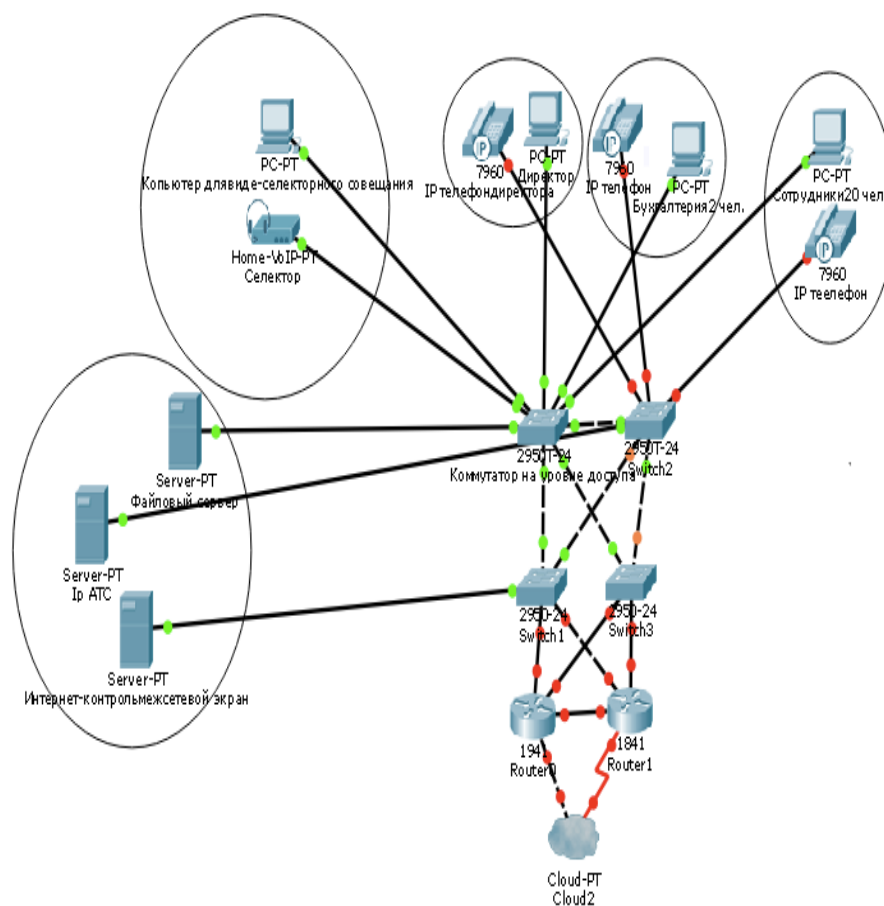


Рисунок 3.7 – Схема фізичної топології офісу в місті Запоріжжі

Даний офіс має таку саму ієрархію як і головний центр, тільки відмінність полягає в тому, що необхідно використання більш потужнішого обладнання, адже в цьому офісі зосереджена більша кількість співробітників.

Проведення конференцій відбувається по тому ж принципу, що і в головному офісі.

В даному офісі необхідно використовувати переважно обчислювальні сервери з базами даних, тому відпадає необхідність у використанні бухгалтерії. У Запорізькому офісі використовується тільки IP-телефонія, навантаження розподіляється між серверами, зовнішнього, між мережевого екрана і внутрішнього файлового сервера. Основне місце зберігання всіх даних (документація, пошта, розрахунки, операції з базами даних)

відбувається на серверах центрального офісу. Це дає змогу контролювати надходження даних і зберігати їх в одному місці.

Загальна протяжність між офісами представлена на рисунку 3.8 для візуально представлення персональної лінії, якою можна було би з'єднати офіси.

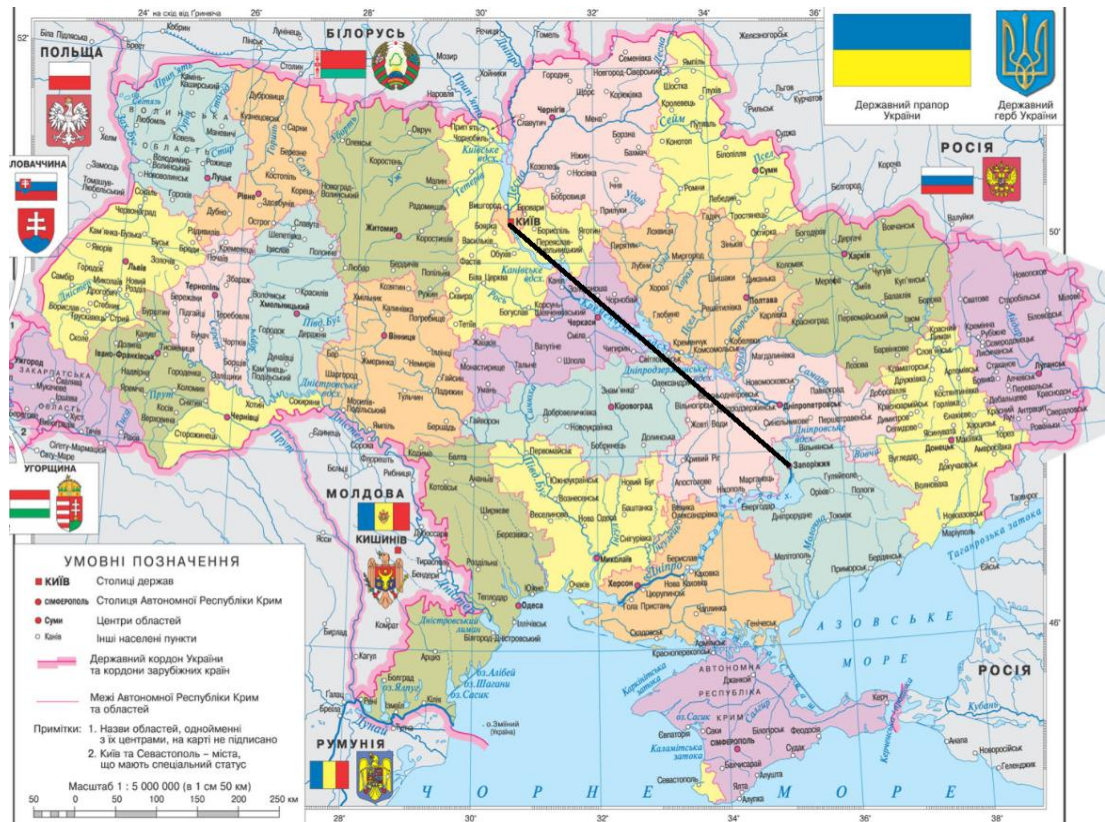


Рисунок 3.8 – Загальна протяжність між офісами

При проєктуванні мережі даного типу, використання персональної лінії на таку відстань має великі фінансові затрати. Тому, щоб зменшити витрати для створення єдиної мережі, ми використаємо поставника послуг інтернет (ISP).

Використання VPN-каналу забезпечує:

- об'єднання офісу і філіалу в єдину мережу через створення локальної мережі;
- за допомогою VPN-каналу відбувається захищена передача даних;

– через VPN-з'єднання відбувається в єдину точку доступу в Internet.

При VPN-з'єднанні ми можемо використовувати різні види шифрування, тому використання віртуальної приватної мережі являється надійним способом для передачі даних і забезпечення її конфіденційності. Також створення VPN-каналу дозволяє підключати співробітників, що працюють віддалено до загального доступу корпоративної мережі. Тому вся інформація, яка передається всередині мережі, надійно захищається і ніхто сторонній не може під'єднатися до неї. Підключення співробітників відбувається через окремо виділений канал передачі даних.

3.4 Створення інформаційної моделі об'єкту

Щоб поєднати офіси необхідно розробити телекомунікаційну мережу. Вона буде поділятися на 2 вузли головний і філіал (таблиця 3.1). Так як у нас одна компанія, то функції будуть однакові, також використання сервісів мережі в офісах буде схоже. Робітників ми розділимо на 6 категорій (таблиця 3.2). Кожна категорія буде мати ті сервіси, які їй необхідні для роботи.

Таблиця 3.1 – Типи вузлів мережі

Тип	Вузли	Сервіси мережі					
		VoIP	Конференц-зв'язок	БД	Інтернет	Поштові сервіси	FTP
1	Головний офіс	+	+	+	+	+	+
2	Філіал	+	+	+	+	+	+

Таблиця 3.2 – Категорії користувачів мережі

Категорія	Співробітники	Сервіси мережі					
		VoIP	Конференц-зв'язок	FTP	БД	Інтернет	Поштові сервіси
1	Керівники	+	+	+	+	+	+
2	Бухгалтерія	+	-	+	+	+	+
3	Інженери	+	-	+	+	+	+
4	Маркетолог	+	-	+	+	+	+
5	Відділ автоматизації	+	+	+	+	+	+
6	Інші працівники	+	-	+	+	+	+

Для кожного вузла є своя кількість абонентів, в залежності від його типу. Дане співвідношення показане в таблиці 3.3.

Таблиця 3.3 – Кількість користувачів

Вузол	Категорія	Кількість користувачів
1	1	1
	2	3
	3	1
	4	1
	5	1
	6	9
2	1	1
	2	1
	3	-
	4	1
	5	1
	6	30

Усього доступно 6 послуг. Загальна база даних знаходиться в головному офісі. Всі співробітники мають вихід в інтернет. На рисунку 3.9 зображено 2 вузла включаючи категорії співробітників, що там працюють та послуги якими вони користуються.

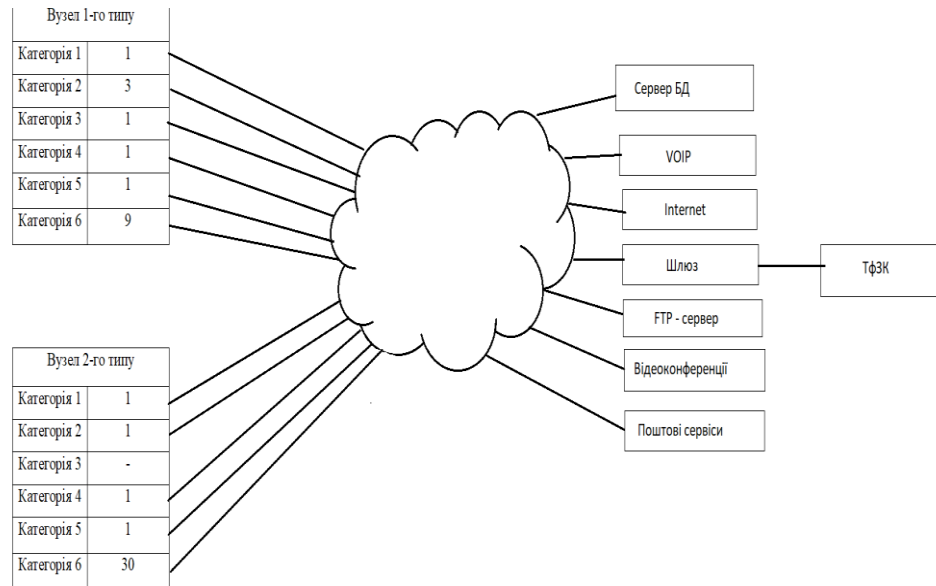


Рисунок 3.9 – Інформаційна модель об'єкту

3.5 Розрахунок трафіку

Розрахунок трафіку проводиться окремо для кожного вузла даної мережі. Для розрахунку будемо використовувати формулу (3.1) [6].

$$\gamma_i^{(k)} = B_{cp}^{(k)} \cdot N_{a\bar{q}_i}^{(k)} \cdot Y^{(k)}, \quad (3.1)$$

де k – номер мережної послуги;

i – номер вузла;

$\gamma_i^{(k)}$ – математичне очікування трафіку, який генерується k -ю послугою на i -му вузлі;

$B_{cp}^{(k)}$ – швидкість передачі даних (у бітах чи пакетах на секунду) – середня пропускна здатність каналу зв'язку, якої достатньо для якісної передачі трафіку k -ї послуги;

$N_{аб_i}^{(k)}$ – кількість абонентів на i -му вузлі, які користуються k -ю послугою;

$Y^{(k)}$ – вірогідність використання k -ї послуги в час найбільшого навантаження (ЧНН).

З урахуванням часу використання послуги:

$$Y = T_c^{(k)} \cdot f_{викл.i}^{(k)} = T_c^{(k)} \cdot \frac{N_{виклЧННi}^{(k)}}{3600} \leq 1, (Epl). \quad (3.2)$$

де $N_{виклЧННi}^{(k)}$ – кількість викликів в ЧНН k -ї послуги;

$T_c^{(k)}$ – середня тривалість сеансу зв'язку для k -ї послуги;

$f_{викл_i}^{(k)}$ – середня кількість викликів у час найбільшого навантаження для користувачів i -го вузла, які використовують k -у послугу.

Тут швидкість передачі даних $B_{cp}^{(k)}$ знаходиться за формулою (3.3):

$$B_{cp}^{(k)} = \frac{B_{max}^{(k)}}{P^{(k)}}, \quad (3.3)$$

де $B_{max}^{(k)}$ – максимальна пропускна здатність каналу зв'язку;

$P^{(k)}$ – пачковість на одного абонента – відношення між максимальною та середньою пропускною здатністю, необхідною для забезпечення k -ї послуги; ця величина характеризує вибухообразність трафіку.

Сумарний трафік, що генерується на i -му вузлі, дорівнює:

$$\gamma_{\sum i} = \sum_{k=1}^{N_k} \gamma_i^{(k)}. \quad (3.4)$$

Для розрахунку трафіку нам необхідно задати такі параметри:

- пачковість;
- тривалість сеансу зв'язку;
- кількість викликів у ЧНН;
- мінімальна швидкість, яка потрібна для працездатності послуги.

Для послуг, якими користуються наші абоненти розглянемо їхні характеристики.

Для офісної телефонії будуть використовуватися VOIP з кодеками G711 u/a-law. Вибір пав саме на цей варіант тому, що він найкраще підходить для провідної телефонії. Необхідна пропускна здатність інтернет- каналу для передачі головних повідомлень – від 64 кбіт/с. Задовольняє потреби при шифруванні інформації. Середня тривалість дзвінка дорівнює 180 с (3 хв.). Будемо вважати, що в ЧНН частота викликів дорівнюватиме 2. Пачечність даної послуги буде дорівнювати одиниці тому, що дії відбуваються у реальному часі.

Мінімальна швидкість для комфортної роботи з файлами складає від 25 Мбіт/с. Дана швидкість розрахована з врахуванням середнього розміру файлу 10 Мбайт, котрий передається за 3 сек., щоб не виникало затримок в роботі при отримуванні інформації. Для цієї послуги характерним є велика печечність та низькі частоти, тому варто розрахувати даний вид трафіку, адже вся робота компанії обертається біля передачі великих і малих даних.

При використанні БД треба забезпечити необхідну пропускну здатність та пачечність при цьому, що частота викликів буде більшою, адже до бази даних відбувається найбільше звернень.

Щоб забезпечити комфортну роботу співробітникам необхідний трафік від 10 Мбіт/с для швидкої передачі даних, перегляду файлів і т.п. Через те, що надходить багато запитів та відповідей на них тривалість сеансу може складати 2 хвилини.

Для конференц-зв'язку необхідно забезпечити стабільне підключення в 2 Мбіт/с тому, що зображення тільки одного екрану буде передаватися на інші.

При передачі файлів електронною поштою необхідно забезпечити підключення від 10 Мбіт/с. Частота викликів ЧНН 1 хвилина.

Всі дані зведемо в таблиці 3.4 і 3.5 для розрахунку трафіку в вузлі.

Таблиця 3.4 – Розрахунок трафіку, що генерується вузлом 1-го типу

Служба	Швидкість, Мбіт/с	Пачечність	Тривалість сеансу зв'язку, с	Частота викликів у ЧНН	Співробіт- ники	Трафік, що генеруює- ться вузлом, Мбіт/с
VoIP	0,064	1	180	2	5	0.08
FTP	25	15	3	3	9	0.0375
Сервер БД	20	100	2	15	16	0.0267
Інтернет	10	300	120	5	16	0.0889
Конференц- зв'язок	2	1	360	1	2	0.4
Поштовий сервіс	10	30	10	2	11	0.02
					Σ	0.6532

Таблиця 3.5 – Розрахунок трафіку, що генерується 2-м вузлом

Служба	Швидкість, Мбіт/с	Пачечність	Тривалість сеансу зв'язку, с	Частота викликів у ЧНН	Співробітники	Трафік, що генерується вузлом, Мбіт/с
VoIP	0,064	1	180	5	10	0.16
FTP	25	15	3	3	20	0.083
Сервер БД	20	200	2	30	34	0.0567
Інтернет	10	500	120	10	34	0.227
Конференц- зв'язок	2	1	360	1	2	0.4
Поштові сервіси	10	50	15	3	25	0.0625
					Σ	0.9892

ВИСНОВКИ

У ході даної дипломної роботи було об'єднано мережу двох офісів в одну цільну мережу на основі технології VPN. Було спроектовано локальні мережі кожного з офісів, підібрано спеціальне обладнання. Приведені плюси та мінуси використання цієї технології. Було спроектовано офісні мережі, розібрано обладнання яке необхідне для стабільної роботи підприємства. Розрахували трафік який протікає в кожній мережі офісу у вузлі 1 при 16 абонентах проходить трафік 0.6532 Мбіт/с. У вузлі 2 протікає трафік 0.9892 Мбіт/с.

Було розписані класифікації VPN та приклади тунелювання. Створена мережа може бути доповнена співробітниками, що працюють з дому. Використовуючи окремо встановлені додатки для вільного доступу до бази даних.

Основною перевагою VPN-мережі є встановлення шифрувального каналу котрий забезпечує безпеку даних.

ПЕРЕЛІК ПОСИЛАНЬ

1. VPN – Віртуальна приватна мережа. [Електронний ресурс]: Режим доступу: <https://uk.wikipedia.org/wiki/VPN> .
2. Proxi-server – Проксі-сервер. [Електронний ресурс]: Режим доступу: https://en.wikipedia.org/wiki/Proxy_server .
3. TP-LINK TL-ER7206 – Маршрутизатор типу TP-Link. [Електронний ресурс]:
Режим доступу: https://www.moyo.ua/multiservisnyy_marshrutizator_tp-link_tl-er7206_2xge_lan_1xge_wan_2xge_lan_1xsfv_vpn_omada/491556.html .
4. Dell PowerEdge T110 II – Виділений сервер. [Електронний ресурс]:
Режим доступу: <https://www.dell-poweredge.ru/catalog/servery-v-bashennom-korpuse/poweredge-t110-ii> .
5. Program 1C – Програма 1C: Підприємство 8. [Електронний ресурс]:
Режим доступу: <https://www.netsoft.com.ua/1C-Predpriyatiye-8-opisaniye-osnovnyye-kharakteristiki.html> .
6. Близнюк В.Л. Дослідження і проектування мультисервісної мережі для середніх і малих міст Донецької області: магістерська робота. [Електронний ресурс]: Режим доступу: <http://masters.donntu.org/2008/kita/bliznuk/diss/index.htm> .
7. Бараш Л. Виртуальные частные сети на базе MPLS / Леонид Бараш // Компьютерное Обозрение. – 2004. – № 17. – С. 14-16.