МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО «ПРИВАТНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД «ЗАПОРІЗЬКИЙ ІНСТИТУТ ЕКОНОМІКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»

Кафедра Інформаційних технологій
(назва кафедри)

ДО ЗАХИСТУ ДОПУЩЕНА

Зав. кафедрою _____
(підпис)

д.е.н.,доцент, Левицький С.І.

_____
(Науковий ступінь, вчене звання (прізвище та ініціали)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

РОЗРОБКА ВІДМОВОСТІЙКОЇ, РОЗГАЛУЖЕНОЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ АНАЛІЗУ ТРАФІКА ТА ЙОГО РОЗПОДІЛЕННЯМ ПО ЗОВНІШНІМ КАНАЛАМ

Виконав
ст. гр. - КІ-218 _____ М.А. Білецький
(підпис) (ініціали та прізвище)

Науковий керівник
_____ О.А. Хараджан
(Науковий ступінь, вчене звання, посада) (підпис) (ініціали та прізвище)

Запоріжжя

2023

ПРАТ «ПВНЗ «ЗАПОРІЗЬКИЙ ІНСТИТУТ ЕКОНОМІКИ
ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ»

Кафедра Інформаційних технологій
(назва кафедри)

ЗАТВЕРДЖУЮ

Зав. кафедрою _____
(підпис)

д.е.н.,доцент, Левицький С.І.
_____
(Науковий ступінь, вчене звання (прізвище та ініціали

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ БАКАЛАВРСЬКУ (МАГІСТЕРСЬКУ) РОБОТУ

Студенту гр.КІ-218 , спеціальності Комп'ютерна інженерія

Білецькому Максиму Анатолійовичу

1.Тема: Розробка відмовостійкої, розгалуженої мережевої інфраструктури підприємства з використанням аналізу трафіка та його розподіленням по зовнішнім каналам

затверджена наказом по інституту № 02-10 від 27.01.2023 р.

2. Термін здачі студентом закінченої роботи: 12.06. 2023 р.

3. Перелік питань, що підлягають розробці

1. Провести огляд літератури, що присвячена тематиці досліджень.

2. Провести аналіз існуючої інфраструктури та сервісів підприємства.

3. Створити карту мережі підприємства.

4. Створити технічне завдання для реалізації мережевої інфраструктури.

5. Проаналізувати задачі та знайти відповідне програмне забезпечення та обладнання.

6. Реалізувати головний вузол мережевої інфраструктури

7. Реалізувати допоміжні вузли мережевої інфраструктури та провести тестування відмовостійкої мережі

8. Оформити звіт за результатами роботи

ЗАТВЕРДЖУЮ
Зав.кафедрою_____

К А Л Е Н Д А Р Н И Й Г Р А Ф І К

підготовки бакалаврської дипломної роботи

здобувачами освіти інституту ЗІЕІТ *заочної* форми навчання

гр. _____ П.І.Б._____

2022-2023 навчальний рік

№ етапу	Зміст	Терміни виконання	Готовність по графіку %, підпис керівника	Підпис керівника про повну готовність етапу, дата
1.	Збір практичного матеріалу за темою дипломної роботи	**16.01.23-11.02.23**		
2.	**І атестація** І розділ бакалаврської дипломної роботи	**27.03.23-01.04.23**		
3.	**ІІ атестація** ІІ розділ бакалаврської дипломної роботи	**24.04.23-29.04.23**		
4.	**ІІІ атестація** ІІІ розділ бакалаврської дипломної роботи, висновки та рекомендації, додатки, реферат	**22.05.23-27.05.23**		
5.	Перевірка дипломної роботи на оригінальність	**15.05.23-12.06.23**		
6.	Доопрацювання бакалаврської дипломної роботи, підготовка презентації, отримання відгуку керівника і рецензії	**29.05.23-12.06.23**		
7.	**Попередній захист бакалаврської дипломної роботи**	**12.06.23-18.06.23**		
8.	Подача бакалаврської дипломної роботи на кафедру	**за 3 дні до захисту**		
9.	**Захист бакалаврської дипломної роботи**	**19.06.23-24.06.23**		

Керівник _____(ПІБ) «_____»_____2023р.

Студент _____(ПІБ) «_____»_____2023р.

РЕФЕРАТ

Кваліфікаційна бакалаврська робота містить 73 сторінки, 23 рисунки, 5 лістингів, 45 бібліографічних посилань, два додатки.

Метою роботи є розробка розробка захищеної розгалуженої мережі підприємства.

Об’єктом дослідження є комп’ютерні мережі.

Предметом дослідження є захищені віртуальні мережі, локальні мережі та мережа «Інтернет».

Здійснено детальний огляд предметної області. Виявлено, що розробка проекту розгалуженої комп’ютерної мережі є доцільною. Проект реалізовано за використанням мережевого обладнання компанії «MikroTik», IPsec протоколів шифрування, Cloudflare DNS сервісів. Здійснено проектування моделі предметної області, налаштування маршрутизаторів, DNS серверів.

Проект реалізовано та впроваджено на підприємстві. Це дозволило об’єднати 5 філій в одну мережу та правильно розподіляти потоки трафіку. Впровадження власного DNS серверу дозволило фільтрувати небажаний трафік під час використання інтернет ресурсів.

VPN, MIKROTIK, DOH, DNS, КОМП’ЮТЕРНА МЕРЕЖА ПІДПРИЄМСТВА, ЗАХИСТ ДАНИХ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 6
ВСТУП 7
РОЗДІЛ 1. ОСНОВНІ МЕРЕЖЕВІ КОНЦЕПЦІЇ ТА ПОНЯТТЯ. 9
1.1 Основні мережеві концепції 9
1.2 Стек протоколів. 16
1.2.1 Модель ISO/OSI 17
1.2.2. Опис рівнів моделі ISO/OSI 18
1.3. Віртуальні приватні мережі. 29
РОЗДІЛ 2. РОЗРОБКА ПРОЄКТУ ВІДМОВОСТІЙКОЇ МЕРЕЖІ. 36
2.1 Аналіз структури та сервісів підприємства. 36
2.2 Сервіси підприємства. 38
2.3 Аналіз та розподілення трафіку 42
2.4 Обладнання та канали зв’язку 47
РОЗДІЛ 3. РЕАЛІЗАЦІЯ ТА ВПРОВАДЖЕННЯ ВІДМОВОСТІЙКОЇ МЕРЕЖІ ПІДПРИЄМСТВА 52
3.1. Вибір обладнання та програмного забезпечення. 52
3.2 Налаштування зовнішніх ліній зв’язку та VPN мережі. 59
3.3. Налаштування локальної мережі, DNS серверів 66
ВИСНОВКИ 73
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 74

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

Скорочення	Повна назва	Пояснення/переклад
HTTPS	HyperText Transfer Protocol Secure	Захищений протокол передачі гіпертекстової інформації
VLAN	Virtual Local Area Network	Віртуальна локальна мережа
DNS	Domain Name System	Система доменних імен
LAN	Local Area Network	Локальна мережа
WAN	Wide Area Network	Глобальна мережа
MAN	Metropolitan Area Network	Регіональна мережа
P2P	Peer-to-peer	Одноранговa мережа
IP	Internet Protocol	Інтернет протокол
DHCP	Dynamic Host Configuration Protocol	Протокол динамічного налаштування вузла
CONS	Connection-oriented network service	Протокол з встановленим з’єднанням
CLNS	Connectionless network service	Протокол без попередньо встановленого з’єднання
TCP	Transmission control protocol	Протокол керування передаванням
VPN	Virtual Private Network	Віртуальна приватна мережа
ISP	Internet Service Provider	Інтернет провайдер

ВСТУП

На сьогодні, розвиток мереж дозволяє створювати складні розгалужені інфраструктури, котрі не обмежені фізичними розмірами та географічним розташуванням. Доступ до мережі «Інтернет» дозволяє об’єднувати підприємства з різних кутів світу в одну спільну мережу. Розвиток мережі «Інтернет» призвів до глибокої інтеграції інтернет-сервісів майже у всі аспекти життя та роботи підприємств. Наявність стабільного підключення до мережі «Інтернет» – запорука існування підприємства в цілому. Об’єктом дослідження даної роботи є комп’ютерні мережі.

З іншого боку, підключення до мережі «Інтернет» пов’язано з великими ризиками. Різноманітні злочини, такі як викрадення та підміна інформації, псування даних, незаконний доступ до закритих мереж та інші, ставлять під ризик користувачів «Інтернет». Тому при створенні мережі підприємства, захист від різноманітних атак відіграє далеко не саму останню роль.

Комп’ютерні мережі умовно можна поділити на два типи – надійні та ненадійні. До надійних мереж належать ті мережі, середовище котрих цілком контрольовано. В надійних мережах можна гарантувати захищеність даних від втрати, викрадення або псування. Доступ до надійних мереж є повністю контрольованим. До надійних мереж можна віднести локальні мережі підприємств.

Ненадійні мережі – це мережі відкритого типу. Доступ до таких мереж може мати будь-хто. Ненадійні мережі не гарантують цілісність даних та захист їх від псування та викрадення. Мережа «Інтернет» відноситься саме до ненадійних мереж. Предмет дослідження – локальні та віртуальні приватні мережі, котрі використовуються на підприємствах.

При побудові розгалуженої мережі підприємств, частково буде використана мережа «Інтернет». Тобто потрібно створити надійну захищену мережу, використовуючи ненадійні канали зв’язку. Це можливо завдяки

сучасним алгоритмам шифрування та передачі даних. Дані алгоритми дозволяють гарантувати захист даних від злочинців навіть у ненадійних мережах.

Важливим фактором побудови мережі підприємства є стандартизація обладнання та програмного забезпечення. У кожній філії підприємства потрібно намагатись використовувати однакове обладнання. Це суттєво полегшить процес створення мережі та подальший контроль. Також, стандартизовані засоби побудови значно спростять масштабування мережі у майбутньому.

Загалом, процес побудови розгалуженої мережі потрібно розділити на дрібні задачі:

— вибір обладнання;

— створення локальних мереж філій з прозорою адресацією;

— створення надійних підключень до мережі «Інтернет» з резервуванням каналів;

— створення захищених з’єднань між філіями;

— аналіз та розподілення трафіку.

Вирішивши дані задачі можливо буде побудувати надійну захищену мережу географічно розгалуженого підприємства.

Проект мережі, котрий буде розроблено в рамках даної роботи буде використано при побудові мережі реального підприємства.

РОЗДІЛ 1
ОСНОВНІ МЕРЕЖЕВІ КОНЦЕПЦІЇ ТА ПОНЯТТЯ

1.1. Основні мережеві концепції

В сучасному світі, стрімкий розвиток електроніки та сервісів призвів до того, що наразі майже не залишилось пристроїв та сервісів, які б не залежали від підключення до мережі. Наразі все, від персональних комп'ютерів до телевізорів та іншої побутової техніки підключено до мережі. Це в свою чергу призвело до стрімкого розвитку мережевих технологій, пропускної здатності та ускладненню мережевих топологій. З іншого боку глобальна цифровізація та проникнення мереж у всі сфери життя відкрило поле для злочинців, які працюють у кіберпросторі. Це викрадення, псування та підміна інформації. Злочини, направлені безпосередньо на відмову сервісів, фішингові атаки для отримання доступу до захищених мереж, тощо.

Підприємства в свою чергу ще більше залежать від роботи мережевої інфраструктури. В сучасному світі підприємства будуються з використанням розгалуженої інфраструктури. Це зумовлено саме розвитком комп'ютерних мереж. Вже немає необхідності тримати великі серверні в одному місці з робітниками. З розвитком мережевих технологій, сервіси підприємств можна використовувати так, наче вони знаходяться в одній локації з робітниками, при цьому насправді дистанція між ними може бути в тисячі кілометрів.

Загалом, основні мережеві концепції з часом не дуже змінились. Згідно визначення, мережа – це об'єднання двох чи більше комп'ютерів, котре дозволяє їм розділяти загальні ресурси. Однак в сучасному світі до мережі під'єднано не лише комп'ютери, а й інші пристрої. До мережі на сьогодні під'єднано мобільні телефони, телевізори, друкарську та іншу офісну техніку, та інше. Також, зараз майже не залишилось мереж, котрі не використовують активне мережеве обладнання в якості контролю та керування процесами в мережі. Отже потрібно дещо розширити дане

визначення. Тому мережа – це об’єднання двох чи більше пристроїв, а також засобів керування для взаємної роботи, обміну інформацією та доступу до загальних ресурсів.

За масштабом, мережі зазвичай поділяють на три категорії:

— локальні мережі;

— глобальні мережі;

— регіональні мережі.

Локальна мережа, або Local Area Network (LAN) це набор об’єднаних в мережу пристроїв, котрі фізично знаходяться в рамках одного невеликого регіону, наприклад будівлі чи комплексу будівель.

Дані пристрої, частіше за все, але не обов’язково, можуть бути частиною однієї фізичної мережі. Локальні мережі – це базові «блоки» для побудови об’єднаних та глобальних мереж.

Глобальні мережі, або Wide Area Network (WAN) це об’єднання мереж по усьому світі. Для міжмережевих з’єднань може бути використане сторонні засоби комунікації, такі як супутниковий зв’язок, радіоканали, рідше телефонні лінії, тощо.

На сьогодні глобальні мережі стрімко розвиваються. Потреба в збільшенні пропускної здатності постійно зростає. Пропускна здатність міжмережевих з’єднань вже давно значно більша, ніж пропускна здатність в локальних мережах, а вартість мережевого трафіку стрімко падає.

Третя категорія це регіональні мережі. Регіональна мережа, або Metropolitan Area Network (MAN) – це об’єднання локальних мереж в конкретному регіоні – районі міста, місті, тощо. Регіональні мережі частково використовують інструменти глобальних мереж, але в значно меншому масштабі. На сьогодні складно виділити окремі регіональні мережі, адже всі вони тісно інтегровані в глобальну мережу.

За наявність сервера комп’ютерні мережі поділяють на однорангові та мережі з виділеним сервером.

Однорангові мережі (Peer-to-peer network, P2P) – це тип мереж, в яких всі пристрої можуть виступати як клієнтами так і серверами. Так, як всі клієнти даної мережі мають однаковий ранг – такі мережі не мають централізованого керування розподіленням ресурсів. Будь-який клієнт цієї мережі може розділяти свої ресурси з будь-яким іншим клієнтом цієї мережі. Однорангові відносини в даних мережах елімінують пріоритетність клієнтів. Жоден клієнт даної мережі не має переваг над іншими.

До позитивних сторін таких мереж можна віднести наступне:

— такі мережі прості в створенні, налаштуванні та використанні;

— жоден клієнт не залежить від виділеного сервера, або активного мережевого обладнання;

— кожен клієнт здатен сам керувати своїми ресурсами;

— не потребують жодного додаткового мережевого обладнання чи програмного забезпечення;

— нема необхідності в адмініструванні даної мережі, отже не потрібно наймати системного адміністратора.

Виходячи з простоти даних мереж ми маємо й суттєві недоліки, а саме:

— налаштування політик безпеки одночасно можливе лише на одному клієнті;

— відсутність інструментів централізованої маршрутизації трафіку у мережі;

— підвищене навантаження на клієнтський пристрій під час доступу до його ресурсів іншими клієнтами;

— для забезпечення цілісності даних, потрібно проводити резервне копіювання на кожному клієнті окремо;

— відсутність централізованого каталогу інформації, котра доступна від клієнтів.

Однорангові мережі – це найпростіші мережі, котрі дозволяють швидко та дешево побудувати зв’язок між клієнтами для обміну інформацією або доступу до ресурсів (рис. 1.1). Проте використання подібних мереж значно

обмежено через їх простоту. Також відсутність централізованого вузла контролю мережі з однієї сторони здешевшує побудову мережі та підвищує відмовостійкість, але з іншої – може ускладнити налаштування. Наприклад – для побудови мережі з використанням звичайного побутового маршрутизатора, частіше за все достатньо просто фізично підключити пристрої до маршрутизатора за допомогою кабелів, або бездротового з'єднання. Маршрутизатор сам зможе налаштувати мережу та роздати параметри підключення такі як IP адресу, шлюзи, тощо за допомогою вбудованого DHCP серверу. Користувачеві в цьому випадку взагалі нічого не потрібно робити. В одноранговій мережі необхідно на кожному клієнті вказувати хоча б базові параметри підключення такі як IP адресу та маску підмережі. При цьому треба самостійно пам'ятати всі видані користувачам IP адреси для запобіганню конфлікту IP адрес (коли два або більше клієнти використовують однакові адреси).

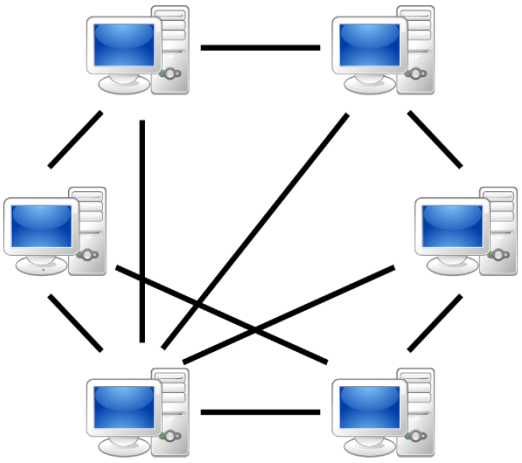


Рисунок 1.1 - Одноранговa мережа

На сьогодні однорангові мережі в класичному понятті майже не використовуються. Через значне здешевшення мережевого обладнання, користувачам простіше побудувати не однорангову мережу, навіть для самих базових задач. Проте, неможна сказати, що однорангові мережі не використовуються. Як приклад – найпопулярніша одноранговa мережа – це P2P протокол обміну інформації BitTorrent.

BitTorrent – це піринговий мережевий протокол, котрий дозволяє кооперативно обмінюватись інформацією через глобальні та локальні мережі.

Файли в торрент мережах передаються частинами за допомогою торрент-клієнтів. Торрент-клієнт отримує частини та одночасно може їх передавати далі, іншим клієнтам. Це в свою чергу значно зменшує навантаження на клієнта та забезпечує збитковість даних.

Торрент-мережі широко використовуються для обміну великими об’ємами інформації, так як мають масу переваг. Перш за все – швидкість завантаження залежить від пропускної здатності не одного серверу, а великої кількості торрент-клієнтів. Кожен клієнт може сам регулювати швидкість завантаження та роздачі інформації. Також в протоколі підтримується одночасне завантаження декількох частин файлів одразу з багатьох джерел. Збитковість даних дозволяє отримати доступ до файлів, навіть коли велика кількість клієнтів не можуть здійснити передачу даних в даний момент. Відповідно пропадає залежність від одного серверу.

Мережі з виділеним сервером.

Мережі з виділеним сервером (Server-based networks) – це основний тип мереж, котрі використовуються майже всюди. В такій мережі обов’язково присутній сервер (рис. 1.2). Сервер – це пристрій, котрий надає служби та ресурси клієнтам, керує доступом та розподіленням ресурсів, тощо. В якості серверу в мережі може виступати будь-який пристрій, котрий здатен забезпечити потреби клієнтів та мережі в цілому.

Найпростіший приклад server-based мережі це проста мережа з побутовим маршрутизатором. В такій мережі, маршрутизатор виступає в ролі центрального серверу керування. За допомогою DHCP серверу маршрутизатор забезпечує автоматичне налаштування клієнтів, видачу IP адрес. За допомогою системи контролю доступу маршрутизатор може обмежувати доступ до мережі, наприклад пропонуючи ввести пароль під час підключення до Wi-Fi. Також маючи вбудований клієнт для підключення до мережі Інтернет маршрутизатор може забезпечити доступ клієнтів до WAN

(наприклад DHCP клієнт, клієнт VPN мережі, тощо). Вбудований брандмауер забезпечує захист мережі та контроль доступу за портами, та багато іншого.

Таким чином, додавши лише один пристрій, можна суттєво підвищити відмовостійкість мережі, її безпеку та спростити процес підключення клієнтів. У якості серверу в мережі може виступати не лише активне мережеве обладнання, а й комп'ютер. Комп'ютер в якості серверу дозволяє забезпечити будь які потреби клієнтів. Наприклад можна використовувати сервер у якості сховища даних, термінального доступу, для забезпечення роботи різних систем управління базами даних, тощо. Сервер по своїй суті – це пристрій, основне призначення якого реакція на запроси клієнтів.

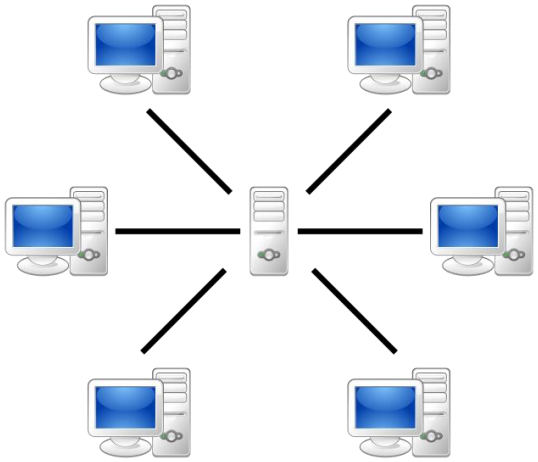


Рисунок 1.2 - Мережа з виділеним сервером

Основні переваги мереж з виділеним сервером наступні:

– забезпечення централізованого керування обліковими записами користувачів, безпекою да доступом до мережі;

– зниження навантаження на клієнтів шляхом переносу обробки запитів на більш потужне обладнання, що суттєво підвищує ефективність мережі;

– подібні мережі набагато простіше масштабувати.

Використання серверу в мережі на сьогодні це необхідність. За допомогою серверу вирішується велика кількість різноманітних задач. Використання серверу дозволяє суттєво розвантажити клієнтські пристрої та підвищує відмовостійкість системи в цілому. Наприклад. Використовуючи

сервер з термінальним доступом, можна перенести абсолютно всі задачі клієнтів на сторону сервера. Таким чином клієнтський пристрій потрібен буде лише для одної задачі – підключення до серверу. Всі задачі користувача будуть оброблюватись на сервері. По перше це зменшує вимоги до терміналу (достатньо лише мати доступ до мережі та засоби вводу та виведення інформації). По друге – це повністю відв’язує користувача від фізичного місця розташування (маючи доступ до серверу, користувач може підключитись з будь якого кута світу, з будь якого терміналу та отримати доступ до свого робочого місця). По третє – це підвищує захищеність даних. На сервері можливо налаштувати будь які політики доступу до даних, програм та систем. Системи зберігання даних та системи резервного копіювання в рази надійніші ніж звичайні клієнтські термінали.

Також, використання серверу суттєво полегшує адміністрування мережі, та дозволяє отримати прозорий контроль за доступом до даних. Так, використовуючи групові політики доступу можливо тонко та прозоро налаштувати безпеку на сервері та доступ до даних. Зберігання даних лише на сервері дозволяє контролювати їх цілісність та ефективно проводити резервне копіювання. До того ж, використовуючи RAID масиви можна майже моментально відновлювати роботу системи після збоїв обладнання.

Не зважаючи на всі переваги, існує й багато недоліків подібних систем, а саме:

– вихід із строю центрального вузла може привести до несправності всієї мережі;

– мережі з виділеним сервером потребують кваліфікованого персоналу для створення, налаштування та обслуговування, що призводить до більших затрат;

– загальна вартість подібних мереж більша за однорангові, адже з’являється необхідність в додатковому обладнанні та програмному забезпеченні.

При побудові мережі підприємства потрібно завжди аналізувати поставлені задачі, а саме:

– кількість клієнтів мережі;

– бюджет;

– дані, з якими буде працювати підприємство, їх тип та важливість;

– необхідність в доступі до спеціального програмного забезпечення, СУБД, тощо;

– необхідність в доступі до мережі Інтернет.

Сучасні мережі майже завжди будуються з використанням серверів та активного мережевого обладнання. Однорангові мережі використовуються лише як поодинокі сервіси такі як торрент-мережі, тощо.

1.2. Стек протоколів

Головна ціль побудови комп’ютерної мережі – можливість використовувати ресурси кожного пристрою усіма другими учасниками мережі. Для реалізації цієї можливості учасники повинні мати необхідні для такої взаємодії інструменти, а сама взаємодія повинна відбуватись за чіткими та прозорими правилами.

Взаємодія в мережі це комплексна задача, котра включає в собі рішення великої кількості проблем. Вибір способу адресації користувачів, узгодження сигналів на фізичному рівні, забезпечення надійної передачі даних та обробка помилок, тощо.

Для вирішення задачі мережевої взаємодії вона була розділена на декілька проблем – підзадач. Для вирішення кожної підзадачі був реалізований конкретний, чітко описаний модуль з визначеними правилами. Даний набір модулів утворює ієрархічну структуру, котра складається з різних рівнів. Для кожного рівня було визначено набір запитів, якими модулі вищих рівнів можуть звертатись для вирішення своїх задач.

Такий набір функцій, котрі виконуються даним рівнем для рівня вище, формати повідомлень та набір правил називається інтерфейсом.

Правила взаємодії клієнтів в мережі описуються у вигляді набору процедур для кожного з рівнів взаємодії. Ці правила, котрі визначають послідовність та формат повідомлень, котрими обмінюються мережеві компоненти на одному рівні, але у різних клієнтів називають протоколами.

Мережевий протокол – це набір правил, які використовуються для мережевої взаємодії. Для того, щоб два клієнти могли успішно створити взаємодію – вони повинні підтримувати загальний протокол.

Відповідно, узгоджений набір протоколів мережевої взаємодії називають стеком протоколів.

Для організації мережевої взаємодії можна використовувати два основних типи протоколів – протокол з встановленим з'єднанням, та протокол без попередньо встановленого з'єднання.

В протоколах з встановленим з'єднанням (connection-oriented network service, CONS) перед мережевою взаємодією (обміном даними) ініціатор та відповідач повинні спочатку встановити між собою з'єднання. Тобто узгодити правила, формат повідомлень, тощо, котрі будуть працювати в рамках цього обміну. Після завершення обміну з'єднання розривається. Якщо необхідно знову провести взаємодію – дана процедура виконується заново.

В протоколах без попередньо встановленого з'єднання (connectionless network service, CLNS) для обміну даними не вимагається попереднього з'єднання між учасниками. Відправник передає повідомлення тоді, коли воно готове.

1.2.1. Модель ISO/OSI

Міжнародною Організацією по Стандартам (International Standards Organization, ISO) розроблено модель, котра чітко описує та визначає рівні взаємодії систем, стандартизує імена та визначає, яку роботу повинен

виконувати той чи інший рівень. Ця модель називається модель взаємодії відкритих систем (Open System Interconnection, OSI).

В моделі ISO/OSI мережева взаємодія ділиться на сім рівнів. Кожен рівень відповідає за певній аспект взаємодії. Таким чином, комплексну задачу мережевої взаємодії декомпозовано на 7 окремих проблем. Кожна з цих семи проблем може бути вирішена незалежно від інших. Кожен рівень взаємодії підтримує інтерфейси з рівнями вище та нижче.

Модель ISO/OSI описує лише системні засоби взаємодії. Вона за включає взаємодії користувачів та додатків. Додатки можуть реалізувати власні протоколи взаємодії, використовуючи системні засоби. Також слід зазначити, що додаток може брати на себе функції верхніх рівнів моделі ISO/OSI. Таким чином, при необхідності мережевого обміну додаток напряму звертається до системних ресурсів, котрі відповідають за нижчі рівні моделі ISO/OSI.

Наприклад. Додаток може звернутись з запитом до прикладного рівня, файлового сервісу. На основі цього запиту програмне забезпечення прикладного рівня створює повідомлення стандартизованого формату, в котре розміщає службову інформацію (заголовок) та безпосередньо дані. Далі це повідомлення передається рівню представлення.

Рівень представлення, в свою чергу, додає до повідомлення свій заголовок та передає далі сеансовому рівню, котрий в свою чергу додає свій заголовок і так далі, аж поки повідомлення не потрапить на фізичний рівень, де і буде безпосередньо передане по лініям зв’язку.

Відповідно, під час отримання повідомлення отримувачем, воно навпаки пройде всі рівні вгору від фізичного до прикладного. Кожний рівень при отриманні буде видаляти свій заголовок перед передачею на рівень вище.

1.2.2. Опис рівнів моделі ISO/OSI

Мережева модель ISO/OSI складається з 7 рівнів (рис. 1.3):

– прикладний;
– представлення;
– сеансовий;
– транспортний;
– мережевий;
– канальний;
– фізичний.

Модель OSI

Дані	7 прикладний application	Доступ до мережевих служб
	6 представлень presentation	Представлення і кодування даних
	5 сеансовий session	Управління сеансом зв'язку
Сегменти	4 транспортний transport	Прямий зв'язок між кінцевими пунктами і надійність
Пакети	3 мережевий network	Визначення маршруту і логічна адресація
Кадри	2 канальний data link	Фізична адресація
Біти	1 фізичний physical	Робота з середовищем передачі , сигналами і двійковими даними

Рисунок 1.3 - Мережева модель OSI

Кожен з цих рівнів може взаємодіяти лише з сусідніми рівнями та має виконувати лише визначений перелік задач.

Прикладний рівень.

Верхній рівень моделі OSI, відомий як Прикладний рівень або Application layer, забезпечує взаємодію мережі та користувача шляхом підтримки прикладних програм, таких як веб-браузери, електронна пошта та віддалений доступ до файлів. На цьому рівні протоколи займаються передачею даних між програмами, а не між мережами, як на рівнях нижче.

Однак, навіть на цьому рівні потрібні додаткові службові протоколи, такі як DNS (Domain Name Service), для забезпечення ефективної комунікації між програмами та мережами.

Рівень представлення (Presentation layer), також відомий як Рівень подання або Представницький рівень, є шостим рівнем у моделі OSI. Цей рівень відповідає за перетворення даних, кодування та декодування протоколів. Він перетворює запити додатків з рівня додатків у формат, придатний для передачі по мережі, а також перетворює дані, отримані з мережі, у формат, зрозумілий додаткам.

Рівень представлення може виконувати функції стиснення / розпакування даних та кодування / декодування даних. Також на цьому рівні може здійснюватися перенаправлення запитів до іншого мережного ресурсу, якщо вони не можуть бути оброблені локально.

На рівні представлення інформація, що передається по мережі, не змінює змісту. Протоколи прикладних програм можуть використовувати засоби, що реалізовані на даному рівні, для погодження представлення даних з різних джерел.

Іншою важливою функцією рівня представлення є шифрування та дешифрування даних, що забезпечує таємність передачі даних. Процеси та коди, що знаходяться на рівні представлення, виконують перетворення даних, щоб забезпечити функціонування секретного обміну. Один з прикладів протоколу, який забезпечує безпеку обміну даними по мережі є рівень захищених сокетів (Secure Socket Layer, SSL).

Сеансовий рівень є п'ятим рівнем моделі OSI і має за завдання підтримувати сеанс зв'язку між програмами, що взаємодіють тривалий час. Він контролює створення та закриття сеансів, обмін інформацією, синхронізацію завдань, визначення прав на передачу даних та підтримку сеансу під час неактивності програм. Для забезпечення синхронізації передачі, контрольні точки включаються у потік даних, що дозволяє відновлювати процес при порушенні взаємодії.

Сеанси передачі складаються з запитів та відповідей, що здійснюються між програмами, а служби сеансового рівня зазвичай використовуються у середовищах програм, де необхідний віддалений виклик процедур.

Прикладами протоколів сеансового рівня є X.235 або ISO 8327, який може спробувати відновити з'єднання у разі його втрати, а також Zone Information Protocol (ZIP) - протокол AppleTalk що забезпечує узгодженість процесу зв'язування по імені, та протокол управління сеансом (SCP) - протокол рівня сеансу IV стадії проекту розробки стека протоколів DECnet.

В рамках семантичних конструкцій сеансовий рівень відповідає на запити з представницького рівня та здійснює службові запити до транспортного рівня в мережевій архітектурі OSI.

Сеансовий рівень моделі OSI відповідає за належне встановлення контрольних точок та відновлення з'єднання у разі обриву. Він забезпечує синхронізацію та правильне поєднання інформації з кількох різних потоків інформації. Як приклад – потокова передача відео, коли необхідно синхронізувати одразу декілька різних потоків інформації (звук та відео).

Транспортний рівень моделі OSI відповідає за передачу даних у правильному заданому порядку, без помилок, дублювання і втрат. Дані повинні бути передані незалежно від їх типу та маршруту. На транспортному рівні реалізується саме механізм передачі даних. Для реалізації передачі, блоки даних діляться на окремі фрагменти, розмір яких залежить від налаштувань протоколу. При цьому, за необхідністю протоколи транспортного рівня можуть і не використовувати всі зазначені вимоги. Так, наприклад, протокол UDP не гарантує ні відсутність втрат, ні послідовність даних, проте суттєво знижує розмір пакету через відсутність зайвої службової інформації.

Прикладом протоколів транспортного рівня є протоколи TCP, UDP, SPX.

Мережевий рівень. Цей рівень призначений для створення єдиної транспортної системи, що об'єднує декілька мереж з різними принципами передачі інформації між кінцевими вузлами.

Повідомлення мережевого рівня називають пакетами. При організації доставки пакетів на мережевому рівні використовується поняття «номер мережі». У цьому випадку адреса отримувача складається з номера мережі та номера комп'ютера в цій мережі.

Для того, щоб передати повідомлення від відправника, який знаходиться в одній мережі, отримувачеві, який знаходиться в іншій мережі, потрібно здійснити певну кількість транзитних передач між мережами, кожного разу вибираючи підходящий маршрут. Таким чином, маршрут представляє собою послідовність маршрутизаторів, через які проходить пакет.

Проблема вибору найкращого шляху називається маршрутизацією, і її розв’язання є головною задачею мережевого рівня. Ця проблема ускладнюється тим, що найкоротший шлях не завжди є найкращим. Часто критерієм при виборі маршруту є час передачі даних по цьому маршруту, який залежить від пропускної здатності каналів зв'язку та інтенсивності трафіку, яка може змінюватися з часом.

Два види протоколів визначаються на мережевому рівні. Перший вид відноситься до правил передачі пакетів з даними кінцевих вузлів від вузла до маршрутизатора та між маршрутизаторами. Інший вид протоколів, які називаються протоколами обміну маршрутною інформацією, також відносяться до мережевого рівня. Ці протоколи дозволяють маршрутизаторам збирати інформацію про топологію міжмережевих з'єднань. Протоколи мережевого рівня реалізовані за допомогою програмних модулів операційної системи, а також програмних та апаратних засобів маршрутизаторів. Найбільш популярними протоколами мережевого рівня є протокол IP та протокол IPX.

Канальний рівень (Data Link layer) відповідає за перевірку доступності середовища передачі та впровадження механізмів виявлення та корекції помилок. Для цього біти групуються в набори, що називаються кадрами. Канальний рівень забезпечує правильність передачі кожного кадру, додаючи спеціальну послідовність біт на початок та кінець кадра для його ідентифікації та обчислює контрольну суму для кожного кадру. При отриманні кадру отримувач також обчислює контрольну суму та порівнює результат з контрольною сумою відправленого кадру. Якщо вони співпадають, то кадр вважається правильним та приймається. Якщо ж контрольні суми не співпадають, то фіксується помилка.

Протоколи канального рівня, які використовуються в локальних мережах, мають певну структуру зв’язків між комп'ютерами та способи їх адресації. Канальний рівень забезпечує доставку кадра між будь-якими двома вузлами локальної мережі, але тільки в мережі з певною топологією зв’язків, для якої він був розроблений. До типових топологій, які підтримуються протоколами канального рівня локальних мереж, належать загальна шина, кільце та зірка. Прикладами протоколів канального рівня є протоколи Ethernet, Token Ring, FDDI.

Фізичний рівень, також відомий як фізичний шар англ. physical layer, є першим рівнем в мережевій моделі OSI. Цей рівень визначає метод передачі двійкових даних між пристроями, такими як комп'ютери. Різні організації, включаючи Інститут інженерів з електротехніки та електроніки, Альянс електронної промисловості та Європейський інститут телекомунікаційних стандартів, займаються розробкою методів передачі даних на цьому рівні.

Фізичний рівень передає електричні або оптичні сигнали через кабелі або радіочастотний діапазон і перетворює їх на біти даних згідно з методами кодування цифрових сигналів. На цьому рівні працюють також концентратори, повторювачі сигналу та медіаконвертери. Функції фізичного рівня реалізуються на всіх пристроях, підключених до мережі, і виконуються мережевим адаптером або послідовним портом з боку комп'ютера.

Фізичний рівень включає фізичні, електричні та механічні інтерфейси між двома системами. Він також визначає різні види середовищ передачі даних, такі як оптоволокно, вита пара, коаксіальний кабель та супутниковий канал передачі даних. До стандартних типів мережевих інтерфейсів, які відносяться до фізичного рівня, належать V.35, RS-232, RS-485, RJ-11, RJ-45, роз'єми AUI і BNC.

Функції рівнів моделі ISO/OSI можна умовно поділити на дві групи: перша група залежить від конкретної реалізації мережі, інша група не залежить від мережі та направлена на роботу з додатками користувача.

Три самі нижні рівні, а саме фізичний, канальний та мережевий – це мережезалежні рівні. Протоколи цих рівнів тісно пов’язані з топологією мережі, її технічною реалізацією та обладнанням, що використовується. Наприклад, фізичному рівню важливо, за допомогою чого була утворена передача даних (за допомогою звитої пари чи з використанням Wi-Fi) и так далі.

Три верхні рівні не залежать від обраної мережі, та орієнтовані більше на роботу додатків. Протоколи цих рівнів не залежать від обраної топології, методу фізичної передачі сигналів, тощо.

Транспортний же рівень, є проміжним, та по суті приховує існування нижніх рівнів від верхніх. Це дозволяє розробляти протоколи та додатки, котрі не будуть залежить від технічних засобів, а безпосередньо займатись передачею повідомлень.

Так як модель ISO/OSI є більш описовою та абстрактною моделлю, а її повна реалізація вважається надто складною, в реальному житті вона так і не була реалізована. Проте, частково ця модель пересікається зі стеком протоколів TCP/IP, котрий зараз використовується майже всюди.

Стек протоколів TCP/IP – це набір протоколів мережі Інтернет. Він складається з двох протоколів – Internet Protocol (IP), та Transmission Control Protocol.

Internet Protocol, або IP – це протокол мережевого рівня, котрий служить для передачі дейтаграм між мережами.

IP-протокол - це найбільш поширена реалізація ієрархічної мережевої адресації, яка використовується в Інтернеті. Цей протокол забезпечує адресацію пакетів, але не забезпечує встановлення з'єднання, не є надійним і дозволяє лише негарантовану доставку даних. Термін "протокол без встановлення з'єднання" означає, що протокол не потребує виділеного каналу для взаємодії між мережевими вузлами, як у телефонній розмові, і не потребує процедури виклику перед передачею даних.

IP-протокол вибирає найефективніший шлях з доступних варіантів на основі прийнятих протоколом маршрутизації. Хоча він не забезпечує надійність та гарантовану доставку даних, це не означає, що система працює погано або ненадійно. Протокол IP не здійснює жодних спроб перевірити, чи досягли пакети своєї мети, але ці функції забезпечуються протоколами транспортного та вищих рівнів. Транспортний рівень відповідає за збірку пакетів в потрібній послідовності.

Протокол IP може розпізнати заголовок та хвіст пакету та будь яку іншу службову інформацію, але йому байдуже на фактичні дані. Він лише передає оброблений фрейм рівням вище.

Структура IP пакету (рис. 1.4):

– Версія (Version) – Поле, 4 біт, котре описує версію протоколу IP. Під час мережевої взаємодії, всі пристрої повинні використовувати однакову версію протоколу.

– Довжина заголовку (IP Header Length, HLEN) – Поле, 4 біт, котре тримає в собі довжину заголовку пакету.

– Тип сервісу (Type Of Service, TOS) – Поле, 8 біт, котре тримає в собі рівень важливості переданої інформації. Це поле заповнюється протоколами вищого рівня.

– Загальна довжина (Total Length) – Поле, 16 біт, що тримає в собі повний розмір пакету разом з даними та службовою інформацією. Для визначення довжини блоку даних потрібно від цієї довжини відняти HLEN.

– Ідентифікатор (Identification) – Поле, 16 біт, котре зберігає в собі послідовний номер пакету.

– Прапори (Flags) – Поле, 3 біта. Зберігає в собі інформацію щодо фрагментації пакету та ознак останнього фрагменту в пакеті.

– Офсет фрагментації (Fragment Offset) – Поле, 13 біт, котре приймає участь у зборці фрагментованих пакетів.

– Час «життя» пакету (Time to live, TTL) – Поле, 8 біт. В ньому зберігається задане число, котре зменшується всякий раз, коли пакет проходить певний вузол. Коли лічильник дійде до нуля – пакет буде автоматично відбракований.

– Протокол (Protocol) – Поле, 8 біт, в ньому зберігається тип протоколу, котрому призначений даний пакет.

– Контрольна сума (Header Checksum) – Поле, 16 біт. Тримає в собі обчислену контрольну суму заголовку, що забезпечує правильну передачу службової інформації.

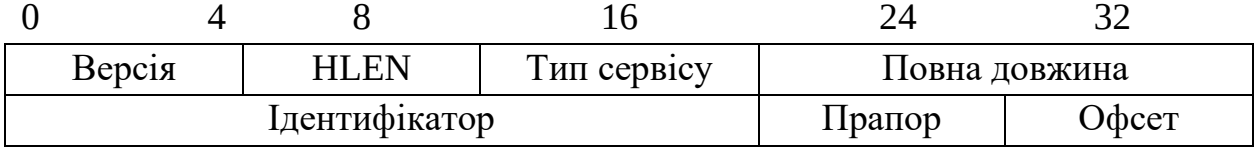
– Відправник (Source IP) – Поле, 32 біт. В ньому знаходиться адреса відправника.

– Отримувач (Destination IP) – Поле, 32 біт. В ньому знаходиться адреса отримувача.

– Опції (Options) – додаткові службові опції. Змінна довжина

– Padding – використовується для додавання нулів для того, щоб заголовок пакету був кратний 32 бітам.

– Дані (Data) – поле змінної довжини, що тримає в собі корисні дані для передачі.



Час життя	Протокол	Контрольна сума
Відправник		
Отримувач		
Опції		Padding
Дані		
…		

Рисунок 1.4 - Структура IP пакету

Transmission Control Protocol (TCP) – це протокол контролю передачі. Цей протокол транспортного рівня виконує функцію керування передачею даних в мережі. Даний протокол забезпечує та гарантує надійну передачу даних між клієнтами та належить до протоколів з встановленим з’єднанням.

Цей протокол отримує інформацію від протоколів віщого рівня (прикладного). Кожен протокол верхнього рівня має свій унікальний порт передачі даних. Наприклад незахищений порт передачі гіпертекстової інформації веб-сторінок – 80.

Далі інформація розбивається на сегменти та додається службова інформація, така як номер сегменту, контрольна сума, тощо. Далі сегменти вбудовуються в IP пакети та передаються за допомогою IP протоколів.

Після отримання пакету вираховується контрольна сума та порівнюється з сумою в заголовкові. Якщо вони збігаються – пакет вважається непошкодженим, а передача даних – успішна та надсилається запит на нову партію даних. Якщо пакет вважається пошкодженим – отримувач запитає повторну передачу даних від відправника.

При успішній передачі порції пакетів вони вилучаються з IP пакетів, розміщуються в заданому порядку та відправляються протоколам вищого рівня.

TCP пакет складається з заголовку та поля даних. Розмір стандартного заголовку 20 байт. Опціонально він може бути збільшений до 60 байт. Ці опції встановлюються на етапі ініціалізації з’єднання.

Блок даних визначається розміром MTU (Maximum Transfer Unit). Чим вище значення MTU тим менше службових даних буде передано в мережі, але при пошкодженні пакету кількість повторно переданих даних буде значно більша. Стандартним розміром MTU в сучасних мережах Ethernet є 1500 байт.

Стек протоколів TCP/IP ділиться на 4 рівні:

- прикладний;
- транспортний;
- міжмережевий;
- рівень доступу до середовища передачі даних.

Протоколи прикладного рівня дозволяють організувати передачу інформації між різними додатками. Вони описують правила та форми передачі інформації між клієнтом та сервером. Ці протоколи направлені на вирішення конкретних прикладних задач, наприклад передача гіпертекстової інформації через HTTP, обмін файлами по FTP, та поштою POP3, SMTP та багато інших.

Транспортний рівень забезпечує транспортування інформації, котра була згенерована прикладним рівнем. Два основних протокола транспортного рівня це UDP та TCP. Кожен додаток, який передає інформацію через протоколи UDP та TCP має свій унікальний порт. Це використовується для швидкої ідентифікації процесів. Основна відмінність протоколів TCP та UDP полягає в тому, що для передачі даних по протоколу TCP необхідно встановлення з’єднання між клієнтами, тоді, коли протокол UDP передає дані без попереднього з’єднання, хоча і не гарантує збереженість даних.

Міжмережевий рівень забезпечує передачу інформації та встановлення з’єднання між мережами з різними типами та архітектурою. Протоколи міжмережевого рівня це IP, ARP – адресний протокол, RARP – реверсивний адресний протокол та протокол діагностики мереж ICMP. Останній

допомагає передавати в мережі інформацію про збої обладнання та помилки маршрутизації, тощо.

На цьому рівні виконується маршрутизація пакетів з використанням таблиць маршрутизації, котрі були створені динамічно, за допомогою протоколів RIP та OSPF або в ручному режимі.

Рівень доступу до середовища передачі даних.

На цьому рівні виконується прив’язка IP адрес до фізичних адрес пристроїв, інкапсуляція IP пакетів для передачі даних по фізичним каналам.

Таким чином, стек протоколів TCP/IP частково наслідує функціональну модель ISO/OSI, але значно спрощує її реалізацію. Цей стек протоколів дозволяє одночасно керувати адресацією в мережі, вирішує проблеми маршрутизації, а також забезпечує безпечну та відмовостійку передачу даних в мережі за вимогою.

1.3. Віртуальні приватні мережі

Під час побудови мережі в рамках однієї, фізично невеликої області, можна використовувати стандарти побудови локальних мереж. Це можуть бути звичайні маршрутизатори для керування мережею та виходу в інтернет, мережеве обладнання таке як комутатори та підсилювачі сигналу, тощо. В якості медіа для передачі даних використовують звичайну звиту пару, Wi-Fi, рідше – оптичний кабель. Це все буде працювати, коли мережа будується в межах однієї будівлі. Проте, що робити, коли потрібно створити локальну мережу, але будівлі знаходяться за багато кілометрів одна від одної? Можна створити канали між будівлями, фізично проклавши оптичний кабель, або безпровідний канал. Але це все дуже затратні процедури, котрі не зможуть гарантувати надійної передачі даних. На допомогу приходять віртуальні приватні мережі.

Віртуальна приватна мережа (Virtual Private Network, VPN) – це узагальнена назва технологій, котрі дозволяють створювати віртуальні мережі поверх інших мереж. Для роботи мережі створюється так званий VPN

тунель, котрий дозволяє клієнту користуватись сервісами мережі так, начеб він знаходився безпосередньо локально всередині цієї мережі. Для VPN мереж можна налаштувати шифрування. Це допомагає забезпечити необхідний рівень безпеки навіть при використанні відкритих мереж, таких як Інтернет.

Використовуючи технології VPN можна об’єднувати фізично розгалужені вузли, за допомогою шифрованих каналів зв’язку таким чином, що для клієнтів всередині цих вузлів всі мережеві сервіси нічим не будуть відрізнятись від принципів локальної мережі.

Структурно VPN – це серверна мережа, яка складається з однієї або більше внутрішніх мереж, та зовнішньої мережі, через яку відбувається передача даних. Підключення мереж та окремих клієнтів до VPN відбувається за допомогою спеціального VPN серверу, який має мати доступ одночасно як до внутрішніх ресурсів, так і до зовнішньої мережі. VPN сервер виконує функції ідентифікації та аутентифікації користувачів та з’єднань, шифрування та дешифрування даних, контроль за цілісністю інформації, тощо. Часто в ролі VPN серверів можуть виступати маршрутизатори. Тоді окрім вищезазначених функцій вони будуть виконувати трансляцію адрес, маршрутизацію, тощо.

Віртуальні приватні мережі поділяють за середовищем на захищені та довірчі (рис.1.5).

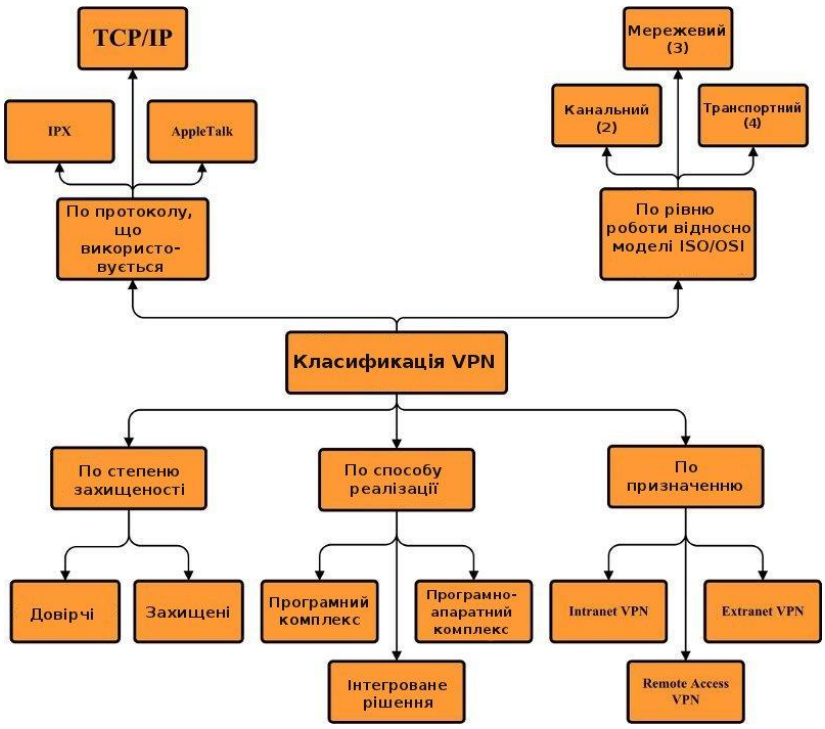


Рисунок 1.5 - Класифікація VPN

Захищені мережі – це мережі, котрі в якості середовища для передачі інформації використовують ненадійні мережі, наприклад Інтернет. При побудові таких мереж, відповідальність за захист даних полягає на VPN сервер та обраний протокол передачі. Протокол в таких мережах має бути захищений з використанням шифрування. Одні з найпоширеніших протоколів для використання в ненадійних мережах це IPSec, SSL та PPTP.

IPSec це набір протоколів, котрі гарантують захист даних під час передачі їх за допомогою протоколу IP. IPSec дозволяє проводити верифікацію даних, шифрування та дешифрування пакетів, обмін ключами. Цей протокол досить гнучкий, адже він працює на мережевому рівні та не залежить від обраного транспортного протоколу. По суті це додаток до IP протоколу, котрий дозволяє встановлювати з’єднання як безпосередньо між кінцевими користувачами, так і між вузлами мережі.

Рівень захищених сокетів (Secure Socket Layer, SSL) – це протокол шифрування даних, котрий дозволяє встановити шифроване захищене з’єднання. Цей протокол забезпечує конфіденційний обмін даними по протоколу TCP/IP з використанням шифрування відкритим ключем. Під час

такого шифрування використовується пара ключів. Будь який з цих двох ключів може бути використано для шифрування. При цьому, якщо один ключ було використано для шифрування – відповідно інший ключ потрібно використовувати для дешифрування. Таким чином можна забезпечити захищений обмін публікуючи відкритий ключ та зберігаючи секретний. Для роботи SSL з'єднання обов'язково повинен бути встановлений SSL сертифікат.

PPTP (Point-to-Point Tunneling Protocol) – протокол тунелів точка-точка, який забезпечує шифроване захищене підключення до серверу за допомогою тунелю в ненадійній мережі. Цей протокол працює за допомогою інкапсуляції фреймів PPP до пакетів IP. Для утворення тунелю використовується окреме з'єднання за допомогою TCP.

Інший приклад віртуальних приватних мереж – довірчі мережі. Довірчі мережі можна використовувати тоді, коли мережа, на базі якої створюється VPN є надійною та безпечною. Таким чином нема необхідності в надійному з'єднані та шифруванні, а забезпечення безпеки даних лягає на існуючу мережу. Прикладом протоколів для довірчих мереж є MPLS та L2TP.

Протокол тунелювання другого рівня (Layer 2 Tunneling Protocol, L2TP) – це протокол, котрий використовується для створення віртуальних приватних мереж. Цей протокол не забезпечує безпечної передачі даних. При використанні в довірчих мережах такого протоколу достатньо. Для використання в ненадійних мережах цей протокол поєднують з протоколом IPSec, на якого покладають функції забезпечення безпеки. Такий тип з'єднання VPN називають L2TP/IPSec.

За способом реалізації виділяють наступні приватні мережі.

В вигляді спеціального, апаратно-програмного комплексу.

В такому виді, мережа створюється за допомогою спеціального, окремо виділеного серверу, котрий включає в собі спеціальне програмне забезпечення. Переваги такого методу полягають в тому, що окремий пристрій буде більш продуктивний, ніж інші рішення.

В вигляді програмного забезпечення.

Такий спосіб побудови мережі можна створити на базі будь-якого комп’ютера чи сервера використовуючи спеціальне програмне забезпечення. До переваг можна віднести відносно низьку ціну реалізації (при використанні безкоштовного ПЗ).

В вигляді інтегрованого рішення.

Такий спосіб побудови можна реалізувати на базі спеціальних маршрутизаторів, котрі підтримують функцію створення VPN серверу. Цей метод створення приватної мережі є найбільш популярним, адже дозволяє вирішити одразу багато мережевих задач. Окрім створення безпосередньо самої мережі, можна одразу організувати захист мережі за допомогою брандмауерів, налаштувати маршрутизації та відслідковувати трафік. До того ж маршрутизатори значно більш енергоефективні за звичайні персональні комп’ютери.

За призначенням VPN поділяють на:

- Intranet VPN;
- Remote-access VPN;
- Extranet VPN;
- Internet VPN;
- Client/server VPN.

Intranet VPN. Використовують для об’єднання декількох філій підприємств в одну мережу з використанням ненадійних каналів зв’язку.

Remote-access VPN. Використовується для створення захищених каналів зв’язку між сегментом розподіленої мережі та клієнтом, котрий підключається до мережі з комп’ютера або смартфона.

Extranet VPN. Використовується для надання доступу до корпоративної мережі стороннім користувачам. В такому випадку користувачі не отримують безпосередній доступ до корпоративної мережі, так як

вважаються ненадійними, а знаходяться у так званій «гостьовій» приватній мережі з обмеженими правами.

Internet VPN. Використовується провайдерами для надання доступу клієнтам до мережі Інтернет. Зазвичай такий метод підключення використовується тоді, коли доступ до мережі Інтернет надається одразу декільком користувачам через один фізичний канал. Такий метод підключення був популярний на просторах країн СНГ. Це допомагало розділити внутрішній трафік в домовій мережі та зовнішній Інтернет трафік. Так, користувач при вимкненому VPN отримував доступ лише до внутрішньої мережі (трафік в якій, був безкоштовним), а підключення до VPN давало можливість вийти назовні, з оплатою.

Client/server VPN. Це підключення між двома вузлами мережі. Таке підключення утворюється між двома вузлами однієї мережі. Наприклад, якщо всередині однієї фізичної мережі потрібно створити декілька логічних для розділення трафіку, тощо. Дане підключення схоже на використання технології VLAN, але включає в себе шифрування трафіку.

Одним зі способів використання VPN мереж є так званий VPN міст. На відміну від звичайних підключень, VPN міст будується не між клієнтами, а між цілими мережами (рис. 1.6). Коли в якості сервера та клієнта використовують, наприклад, маршрутизатори.

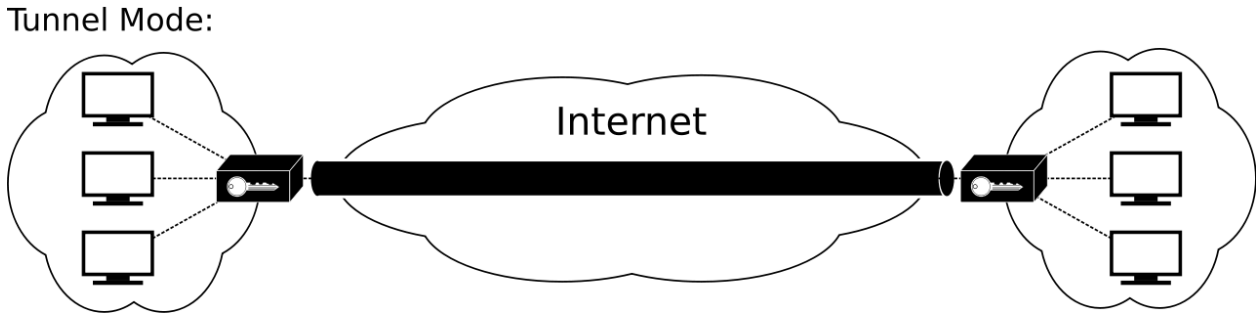


Рисунок 1.6 - VPN тунель

Таке підключення використовується тоді, коли є необхідність в об’єднанні декількох розгалужених мереж в одну. Такий тип підключення

схожий на Intranet VPN, але при використанні Intranet VPN, з’єднання ініціює кінцевий користувач (комп’ютер, смартфон). При використанні мосту – з’єднання відбувається безпосередньо на вузлових пристроях, наприклад – маршрутизаторах. Таким чином всі клієнти, котрі підключені до такого маршрутизатору зможуть отримати доступ до всієї мережі так, наче вони знаходяться фізично в одній локальній мережі. До того ж, використання мосту дозволяє правильно маршрутизувати трафік в мережі. Наприклад Інтернет трафік можна відправляти прямо, не через VPN, а VPN використовувати лише для доступу до внутрішніх сервісів компанії.

РОЗДІЛ 2
РОЗРОБКА ПРОЄКТУ ВІДМОВОСТІЙКОЇ МЕРЕЖІ

2.1. Аналіз структури та сервісів підприємства

Розвиток високошвидкісного інтернету та мережевих технологій дозволив підприємствам створювати складні розгалужені структури, котрі не обмежуються географічним розташуванням. На сьогодні можливо побудувати підприємство, котре буде працювати в одній мережі, підпорядковуватись цілісній системі сервісів, але при цьому знаходитись у різних районах міста, або навіть у різних країнах. Впровадження віртуальних приватних мереж з шифруванням дозволяє використовувати ненадійні канали зв’язку для передачі захищеної інформації та майже повністю виключає вторгнення третіх осіб до систем підприємства.

Підприємство займається поліграфією, фотографією, обробкою фото та відео матеріалів та іншими супутніми послугами. Підприємство поділено на 5 філій, котрі розташовані в різних районах міста. Частина сервісів розміщена на окремих виділених серверах, котрі знаходяться в іншій країні.

На підприємстві використовується велика кількість різноманітних мережевих сервісів, відмово стійкість яких напряму залежить від роботи мережі. Більшість цих сервісів є критично важливими для роботи підприємства, відмова багатьох з них може зупинити обробку замовлень. Тому при побудові мережі багато уваги буде приділено резервуванню каналів зв’язку. Сервіси, котрі використовуються на підприємстві:

– IP телефонія;
– Сховища файлів з мережевим доступом;
– Відеоспостереження;
– Друкарська техніка з мережевим доступом;
– Внутрішні радіостанції для відтворення музики та рекламних повідомлень;

– Гостьові мережі;
– Касові апарати;
– Доступ до віддалених серверів, та інші.

Ці сервіси складаються з локальної частини, котра може знаходитись в філії, та віддаленої частини у вигляді сервера, або іншого обладнання, котре знаходиться фізично у центральному офісі. Наприклад IP телефонія буде складатись з локально розміщеного телефонного апарату, та серверу телефонії у центральному офісі. Також, доступ до деяких сервісів, наприклад, відеоспостереженню, повинен бути з будь якої частини мережі. Тому необхідно забезпечити зв'язок як між філіями та центральним офісом, так і безпосередньо між самими філіями (рис 2.1).

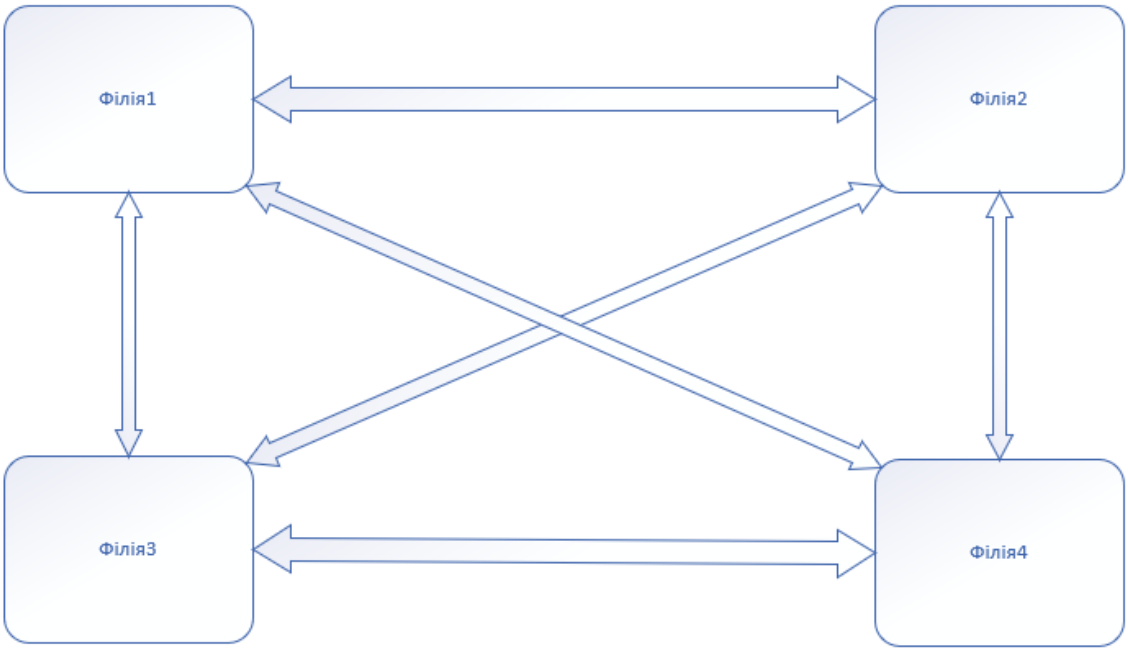


Рисунок 2.1 - Схема зв'язку між філіями підприємства

Для реалізації такої схеми взаємодії, всі філії повинні знаходитись в одній мережі. Для побудови мережі через відкриті канали зв'язку буде використано VPN.

2.2. Сервіси підприємства

Для правильної побудови мережі потрібно проаналізувати всі сервіси підприємства. Для цього умовно поділимо сервіси на користувацькі та адміністративні. До користувацьких сервісів можна віднести ті сервіси, котрі будуть використовуватись простими користувачами на підприємстві. Це телефонія, файлові сховища, доступ до техніки, відеоспостереження, тощо. До адміністративних сервісів віднесемо сервіси для керування системами, захисту та аналізу. Наприклад: VNC, системи резервного копіювання, тощо.

Сервер IP телефонії розміщено в центральному офісі. Для роботи використовуються IP телефони, програмні телефони відсутні, загальна кількість телефонів – 21. На сервері також реалізовано підключення лінії для вихідних дзвінків. Роботу телефонії можна реалізувати двома способами. Перший – підключення серверу телефонії до зовнішнього IP адресу через відповідний порт. Другий – використання віртуальної приватної мережі, та доступ до серверу через локальну адресу. Перший спосіб підключення має свої суттєві недоліки. Через використання відкритого каналу зв’язку між сервером телефонії та телефонними апаратами, потрібно використовувати шифрування. Також, відкритий назовні порт телефонії може нести загрозу мережі. Тому телефонія буде використовуватись через віртуальну приватну мережу. Сервер та телефони отримають свої локальні адреси, підключення зовнішньої лінії буде відбуватись через файервол (рис. 2.2).

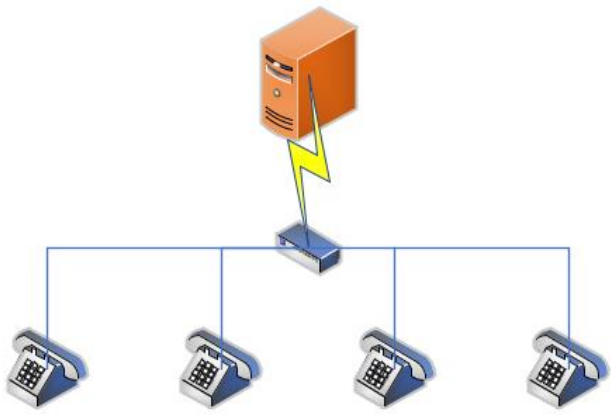


Рисунок 2.2 - Підключення IP телефонії

Так як, підприємство працює з великими медіа файлами (фото, відео, тощо), з’являється необхідність у використанні сховищ даних, та їх мережевій взаємодії. Так, замовлення клієнтів спочатку потрапляють на робочі комп’ютери працівників. Далі вони можуть бути збережені на сховищах даних. Також для передачі замовлень на інші філії потрібно реалізувати мережевий доступ до сховищ. Можна реалізувати одне централізоване сховище, але це зумовить підвищене навантаження на мережу через часті передачі великих об’ємів даних. Також сховища будуть використовуватись для зберігання різних службових даних, таких як дистрибутиви програм, резервні копії, документи тощо (рис 2.3).

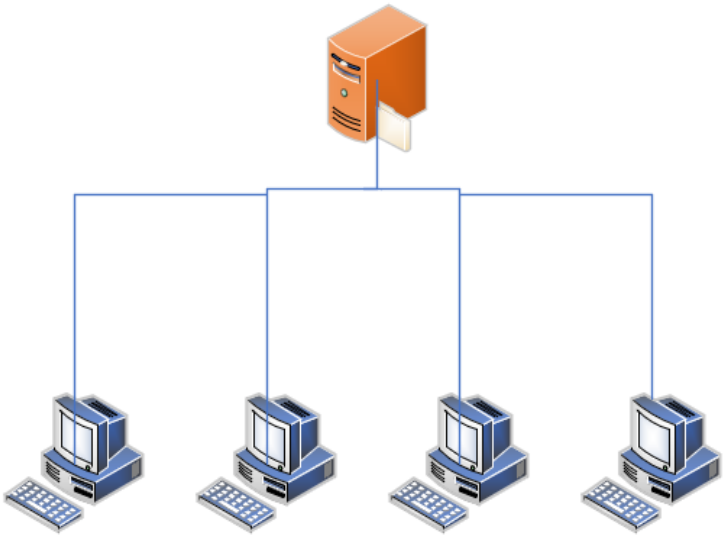


Рисунок 2.3 - Підключення сховищ даних

Системи відеоспостереження та друкарську техніку з мережевим доступом буде підключено за схожими схемами. Так, доступ до друкарської техніки реалізовано лише в межах однієї філії. Друк за межами філії буде заборонено. Відеоспостереження реалізовано за допомогою мережевих відео реєстраторів та камер з аналоговим підключенням. Відео реєстратор це записуючий пристрій, котрий дозволяє циклічно записувати відео з камер спостереження та може надавати мережевий доступ до перегляду записів та відео в реальному часі. В кожній філії розташовано свій відео реєстратор,

котрий приєднаний до мережі. Потрібно налаштувати доступ до реєстраторів як з середини мережі, так і ззовні. Для доступу до реєстраторів зсередини мережі достатньо просто налаштувати відповідну адресацію та облікові записи користувачів. Для доступу ззовні – потрібно обов'язково відкривати відповідні порти для реєстратора (рис 2.4). Доступ ззовні потрібен на той випадок, коли з'являється необхідність в перегляді відео не знаходячись при цьому в мережі підприємства. Наприклад підключення до реєстратора за допомогою мобільного телефону використовуючи мобільний інтернет.

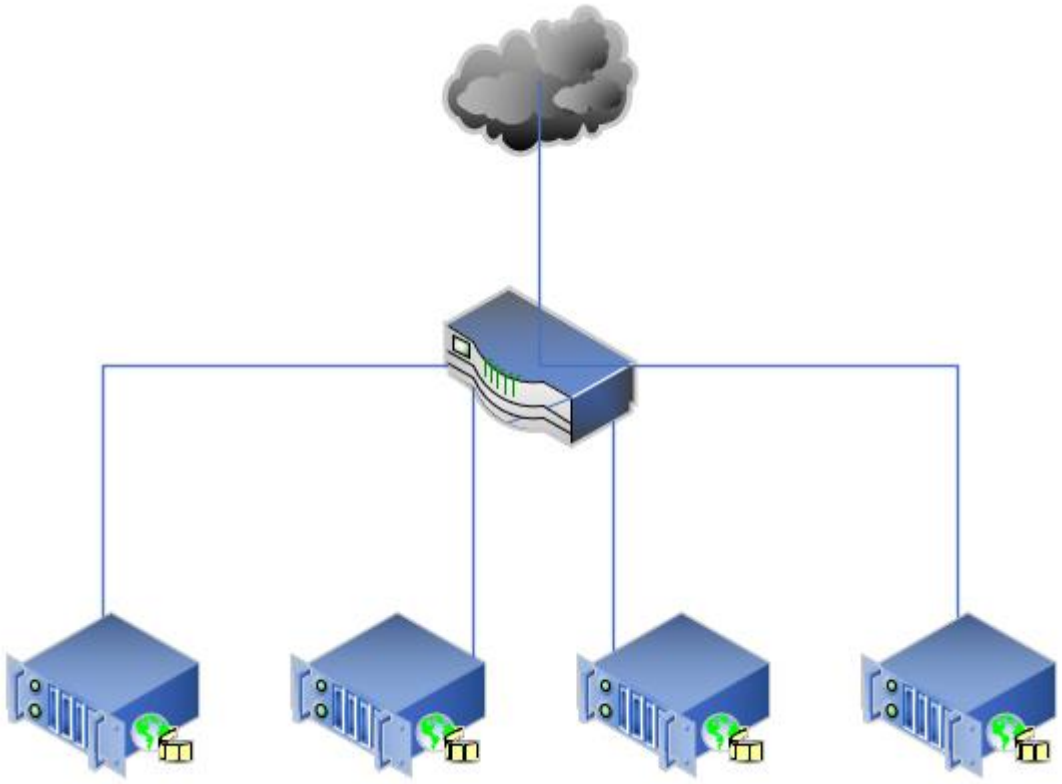


Рисунок 2.4 - Схема підключення відео реєстраторів

Внутрішні радіостанції – це комплекси з мережевих пристроїв відтворення звукових файлів і мережевих радіостанцій та звукової апаратури (звукові підсилювачі та динаміки). Радіостанції використовуються для програвання інтернет радіостанцій та заздалегідь записаних рекламних повідомлень. Для роботи інтернет радіостанцій, потрібне постійне підключення до мережі Інтернет. У користувачів нема необхідності в доступі

до даних пристроїв. Налаштування можна проводити зсередини мережі, тому відкриття портів назовні непотрібне.

В кожній філії буде створено гостьові мережі для доступу відвідувачів до мережі Інтернет. Гостьові мережі повинні бути повністю ізольовані від внутрішньої мережі підприємства. Для цього в кожній філії буде створену гостьову підмережу з виходом до Інтернет. При цьому вона не буде ні частиною локальної, ні частиною віртуальної приватної мережі. Проте, трафік гостьової мережі буде проходити через ті самі брандмауери та керуватись тими ж правилами, що і мережа підприємства.

Касові апарати – це мережеві пристрої, котрі будуть розташовані в кожній філії підприємства. Касовий апарат – це по суті мережевий термопринтер, котрий містить захищену пам’ять для зберігання даних про реалізації. Однією з функцій касового апарату є постійний зв’язок з серверами податкової служби. Касовий апарат постійно передає дані про здійснені операції, такі як відкриття та закриття касової зміни, дані про реалізації та повернення, тощо. Дані передаються на заздалегідь вказану адресу податкової служби та через заданий порт у двосторонньому напрямку. Тобто відбувається як відправка повідомлень так і їх отримання. Для отримання повідомлень касовий апарат повинен бути доступний ззовні через заздалегідь заданий порт.

Частина сервісів підприємства буде розташовано на орендованих виділених серверах за межами центрального офісу. Дані сервери орендовано за межами країни в великих датацентрах.

Розташування сервісів на хмарних серверах має як переваги так і недоліки. До переваг використання хмарних серверів відносять:

- відсутність необхідності придбання обладнання;
- відсутність необхідності обслуговування обладнання;
- відсутність витрат на електроенергію;
- більш просте масштабування систем;
- інтегровані системи резервного копіювання;

– захищена інфраструктура серверів.
– недоліки використання хмарних серверів наступні:
– необхідність щомісячної орендної плати;
– залежність від підключення до мережі інтернет.

З розвитком ринку датацентрів послуги оренди обладнання стали доступними навіть невеликим підприємствам. Так, за відносно невелику оплату орендар може отримати в користування повноцінний виділений сервер, котрий може використовувати для своїх потреб майже без обмежень. Оренда серверів допомагає суттєво зекономити на покупці та обслуговуванні обладнання, економить електроенергію. Також у разі виходу зі строю обладнання, зазвичай датацентри швидко можуть провести заміну без втрати даних та навіть без повторного налаштування системи. Також, датацентри надають більш швидкісний доступ до серверів. Розташування серверів у закордонних датацентрах суттєво підвищує надійність зберігання інформації.

Проте, використовуючи орендовані хмарні сервіси користувач має постійно платити орендну плату. При розташуванні серверів всередині компанії доступ до них проводиться лише за допомогою інструментів локальної мережі, для доступу до хмарних сервісів необхідно постійно бути підключеним до Інтернет. Тому при відсутності доступу до мережі Інтернет хмарні сервіси будуть недоступні, а значить робота підприємства може бути порушена. Хоча, з теперішньою інтеграцією Інтернету до всіх сфер діяльності, навіть при локальному розташуванні серверів, під час відсутності доступу до Інтернет роботу підприємства буде порушено.

2.3. Аналіз та розподілення трафіку

Так як на підприємстві буде реалізовано віртуальну приватну мережу, весь трафік за замовчуванням буде проходить саме через неї. Тобто увесь трафік піде спочатку на центральний вузол віртуальної приватної мережі, а вже потім назовні. Такий метод побудови мережі з одного боку значно

спростить керування мережею, адже точка обміну трафіком буде лише одна, проте з іншого боку може сповільнити роботу мережі. При такій схемі весь трафік з усіх філій підприємства буде проходити через центральний офіс. Відповідно Інтернет канал в цій точці буде поділено між всіма філіями. Для того, щоб уникнути перенавантаження мережі, пропускна здатність центрального вузла повинна дорівнювати сумарній пропускній здатності всіх філій. Тоді, навіть при пікових навантаженнях, можна бути уникнути падіння пропускної здатності вихідного каналу і, як наслідок, сповільнення мережі та сервісів.

Також, при використанні такого методу підключення, в мережі створюється центральний вузол, який може погіршити відмово стійкість. Так, при відсутності зв’язку, або пошкодженні обладнання на центральному вузлі, вся мережа та всі філії будуть не працездатні. Для уникнення подібних ситуацій, а також для підвищення відмово стійкості мережі в цілому, потрібно розділити трафік умовно на декілька типів.

Розглянемо базові сервіси підприємства, та умовно розділимо їх за призначенням трафіку.

Внутрішні сервіси філій. Сюди можна віднести роботу всієї локальної мережі в межах однієї філії, котра фізично знаходиться в одному місці. Це доступ до друкарського обладнання, локальний обмін файлами та доступ до мережевого сховища даних філії, доступ до систем відеоспостереження, тощо. Всі ці сервіси можуть працювати за умови доступності локальної мережі філії, та не залежать ні від зовнішнього Інтернет каналу, ні від доступності віртуальної приватної мережі.

Сервіси взаємодії між філіями та спільні сервіси. До такого типу сервісів віднесемо всі сервіси спільного використання. Це телефонія, доступ до сховищ даних, обмін даними між філіями. Ці сервіси залежать від роботи віртуальної приватної мережі. Якщо мережа буде недоступна – сервіси відповідно теж будуть недоступні.

Зовнішні сервіси філій. Сюди віднесемо всі сервіси, котрі напряму залежать від доступності мережі Інтернет. Це хмарний сервер, робота касових апаратів, робота інтернет-браузерів та різноманітних месенджерів, доступність систем відеоспостереження ззовні, різноманітні службові програми, радіостанції, гостьові мережі, тощо.

Відповідно весь трафік потрібно розділити на три категорії:

– внутрішній;
– зовнішній;
– VPN.

Адресація по філіям буде роздільна. Так кожна філія буде мати свою унікальну підмережу, наприклад 192.168.1.0/24 для першої філії, 192.168.2.0/24 для другої і так далі. Відповідно, для внутрішнього трафіку філій достатньо маршрутизувати трафік, котрий буде іти на відповідні адреси внутрішньої мережі. Якщо немає необхідності – Інтернет трафік повинен йти напряму з філії не потрапляючи до центрального офісу та VPN (рис. 2.5).

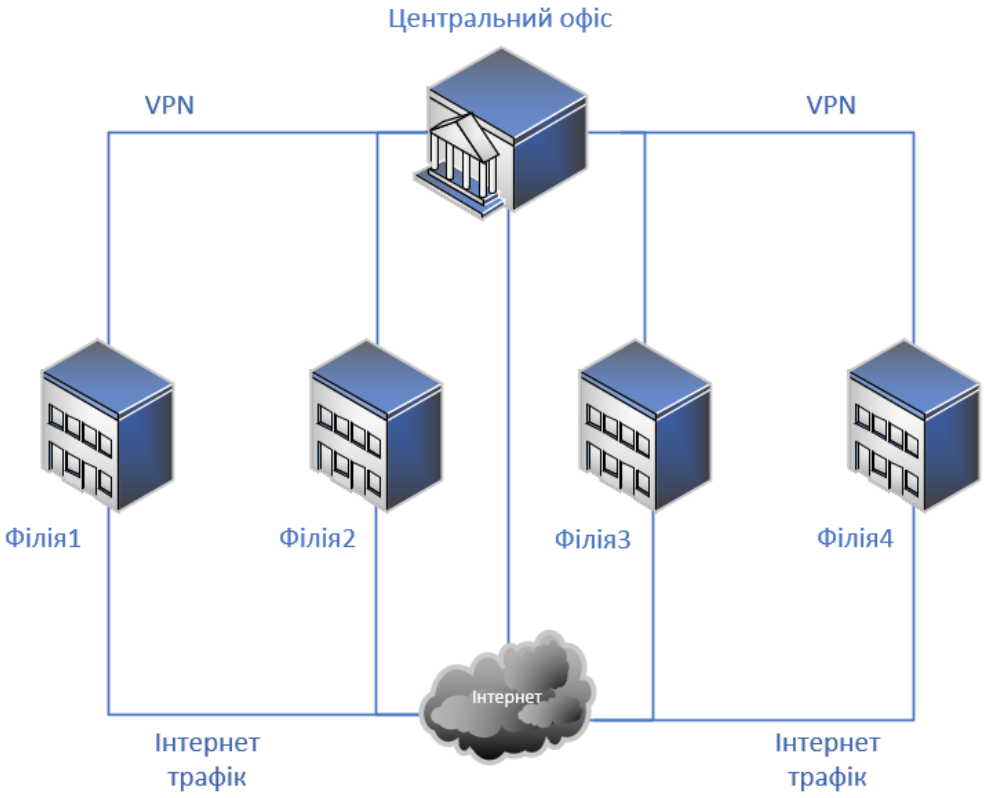


Рисунок 2.5 - Схема руху трафіку на підприємстві

Весь внутрішній трафік можна вважати безпечним. Використання брандмауерів для внутрішнього трафіку не передбачено. Адресація всередині філій буде сталою. Тобто кожен пристрій буде мати свою фіксовану адресу. Це полегшить подальше налаштування та управління мережею. Сталу адресацію можна реалізувати через ручне задання адрес та налаштувань мережі, або з використанням DHCP серверу та подальшою прив'язкою адреси до пристрою на самому маршрутизаторі. Використання DHCP суттєво спростить налаштування мережі та під'єднання нових пристроїв у разі необхідності.

Доступ до зовнішніх сервісів, таких як мережа «Інтернет», месенджери, хмарний сервер буде керуватись маршрутизатором. Для всього зовнішнього трафіку буде встановлено правила брандмауера, в яких буде заборонено все, окрім необхідних виключень. Серед виключень можуть бути порти для доступу до відеоспостереження, касових апаратів, тощо. При чому, порти потрібно відкривати не на всю мережу, а на конкретні пристрої з заданими адресами. Також, потрібно реалізувати ізольовану гостьову мережу для відвідувачів. Ця мережа повинна мати свою адресацію, доступ з неї до внутрішніх сервісів підприємства має бути заборонений. До того ж, не заважало б обмежити швидкість трафіку в гостьовій мережі для того, щоб відвідувачі не заважали роботі сервісів філії, котрі залежать від мережі «Інтернет».

Треба зазначити, що, хоча це і більш небезпечно, доступ до хмарних серверів буде відбуватись безпосередньо з філій, а не через мережу VPN. Це зумовлено тим, що доступ до цих серверів є максимально критичним. На серверах розташовано бухгалтерські системи обліку, CRM системи, налаштовано касове обладнання. Відмова доступу до сервера призведе до повної зупинки філії або всього підприємства. Тому, для того щоб уникнути залежності від роботи центрального вузла з VPN сервером, доступ до хмарних серверів буде реалізовано незалежно від роботи віртуальної приватної мережі.

Віртуальну приватну мережу буде реалізовано на базі маршрутизаторів. Так маршрутизатор в центральному офісі буде виконувати роль VPN серверу, а маршрутизатори у філіях відповідно будуть клієнтами. Так, як VPN будується на базі ненадійної мережі «Інтернет», весь трафік в мережі має бути зашифровано. Одна з задач побудови мережі – адресація трафіку. Потрібно побудувати маршрути таким чином, щоб пристрої з різних філій могли отримувати доступ один до одного, наче вони знаходяться в одній мережі. Наприклад пристрій з адресом 192.168.1.56 міг обмінятись даними з пристроєм в іншій мережі – 192.168.5.97. Віртуальна приватна мережа буде підпорядковуватись тим самим правилам брандмауера, що і зовнішній трафік.

Окремим видом буде спеціальний трафік. Сюди можна віднести весь службовий трафік, забезпечення роботи VNC, інших систем віддаленого доступу. Однією з задач є реалізація на підприємстві сервісу для обходу блокування «Інтернет» ресурсів. Так як, існує велика кількість заблокованих ресурсів мережі «Інтернет» в Україні, потрібно реалізувати сервіс обходу блокування. Обхід блокування «Інтернет» сторінок можливий з використанням публічних VPN мереж або власних VPN мереж, котрі знаходяться територіально в іншій країні. Так, при підключенні до публічної VPN мережі, весь трафік шифрується, і провайдер не може ні проаналізувати пакети ні заблокувати доступ до ресурсів. Однак, направляти весь трафік через публічні VPN сервіси неможна. По перше використання VPN може суттєво сповільнити роботу мережі через обмеженість каналу зв’язку, по друге – це небезпечно, адже використовуючи публічний VPN неможливо гарантувати, що трафік не буде прочитано або навіть змінено третіми особами.

Блокування інтернет ресурсів з боку провайдерів відбувається за декількома напрямками. Це може бути як блокування безпосередньо IP адрес (або діапазонів IP адрес) так і блокування лише DNS записів.

Тому розблокування заблокованих «Інтернет» ресурсів потрібно проводити за двома напрямками. Перш за все спробувати обійти блокування DNS записів за допомогою сторонніх DNS провайдерів. А вже потім потрібно направити відповідні адреси не напряму в мережу, а використовуючи VPN сервіси. Так для перенаправлення трафіку через VPN в таблицю маршрутизації достатньо занести адресу, котру потрібно перенаправити. Однак, багато сервісів мають динамічні адреси, коли домене ім’я фіксоване, а його відповідна IP адреса ні. Тому список адрес для перенаправлення необхідно або правити вручну, або оновлювати автоматично.

2.4. Обладнання та канали зв’язку

В усіх філіях буде використано типовий набір обладнання. Сюди відноситься мережеве обладнання, супутнє обладнання та клієнти. В якості клієнтів використовуються персональні комп’ютери, мобільні телефони, друкарська техніка, та інші пристрої котрі буде приєднано до мережі.

Супутнє обладнання складається з різноманітних пристроїв для реалізації тих чи інших необхідних сервісів. Наприклад відео реєстратори, програвачі радіостанцій, сервери зберігання даних тощо.

До мережевого обладнання відносяться всі пристрої, котрі забезпечують безперебійну роботу мережі. Це маршрутизатори, точки доступу, мережеві концентратори, медіаконвертери та інше.

Так, типова схема підключення мережі у філії виглядатиме наступним чином. Інтернет від провайдерів буде підключено до маршрутизатора. Маршрутизатор виконуватиме роль клієнта VPN, DHCP сервер, брандмауера. Далі маршрутизатор буде підключено до мережевого комутатора. Комутатор – це мережевий пристрій, призначений для об’єднання декількох вузлів комп’ютерної мережі. Він працює на другому рівні мережевої моделі OSI. До комутатора підключаються всі мережеві пристрої за допомогою кабелів.

Окремо до маршрутизатора буде підключено безпровідні точки доступу для гостьової та внутрішніх мереж (рис. 2.6).

Необхідно реалізувати таку кількість фізичних каналів (кабелів, розеток), щоб на місцях була повна відсутність додаткових мережевих концентраторів, комутаторів та іншого мережевого обладнання. Тобто все мережеве обладнання повинно бути розташовано в точці підключення (комутаційна шафа або серверна стійка). На місцях допускається лише розташування безпровідних точок доступу у разі необхідності.

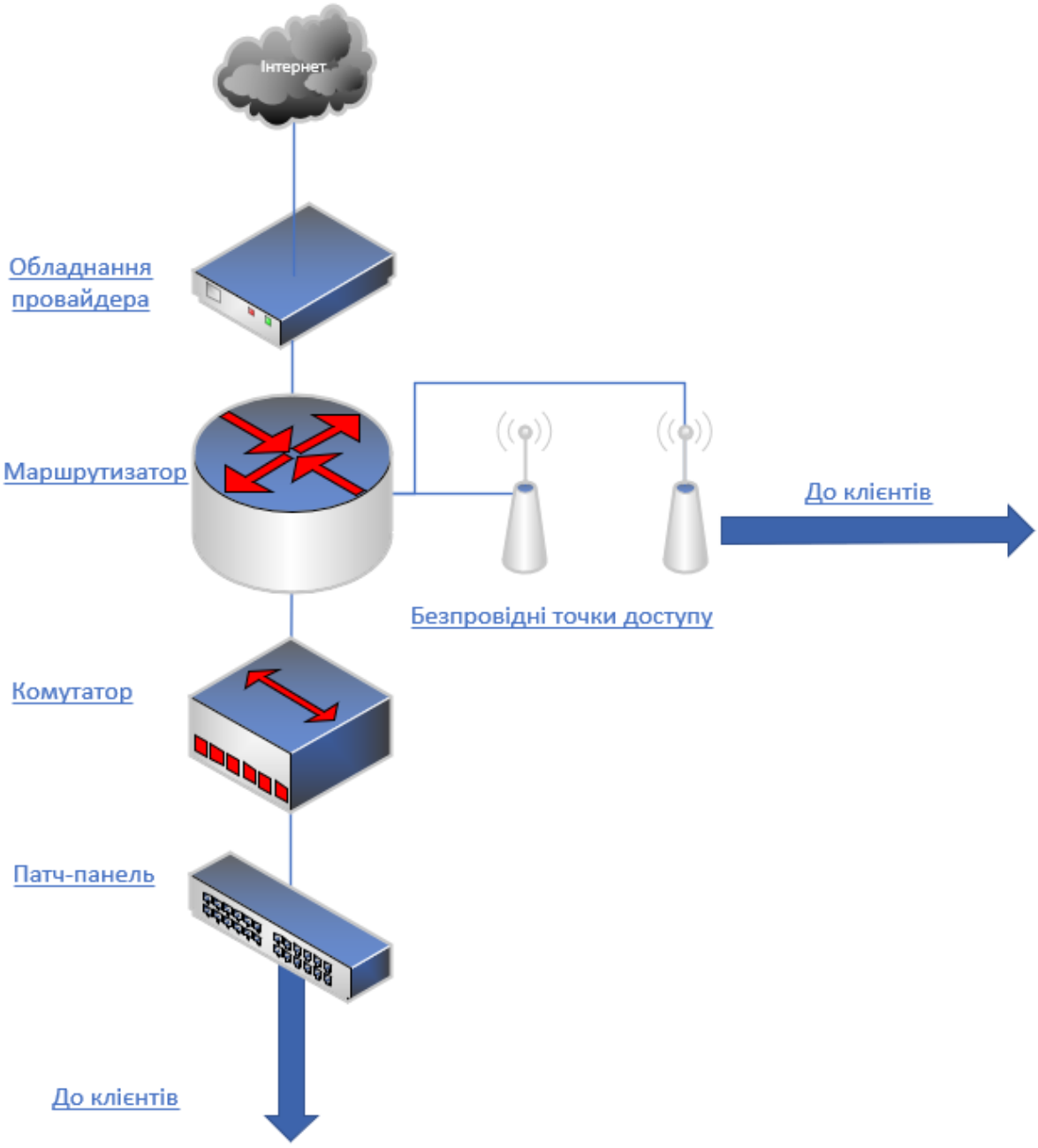


Рисунок 2.6 - Типова схема мережевого обладнання філій

Для забезпечення безперебійної роботи мережі потрібно підключати резервні канали «Інтернет». При чому, резервний канал має бути не від провайдеру основного каналу. Також на маршрутизаторі потрібно реалізувати автоматичну зміну каналу зв’язку у разі виникнення збоїв. Зміну каналу зв’язку потрібно робити не лише для зовнішнього трафіку, а й перемикати канал підключення до VPN. Мінімальна пропускна здатність основного каналу зв’язку має становити 100 Мбіт/с. Побудова локальної мережі має відбуватись за стандартом не нижче Fast Ethernet 100BASE-TX з гарантованою швидкістю передачі всередині мережі до 100 Мбіт/с. Відповідно комутатор повинен бути стандарту не нижче Fast Ethernet.

Безпровідні точки доступу мають бути стандарту не нижче 802.11ac для внутрішньої мережі, та не нижче 802.11n для гостьової. В залежності від конфігурації приміщення кількість точок доступу можна збільшити для розширення зони покриття.

В комутаційній шафі буде розташовано все мережеве обладнання та необхідне супутнє обладнання. Так, крім мережевого обладнання в комутаційній шафі буде розміщено відеореєстратор з блоками живлення для камер, аудіоапаратура для внутрішньої радіостанції, сервер зберігання даних, джерело безперебійного живлення для комутаційної шафи (рис 2.7).

Рисунок 2.7 - Схема розташування обладнання в комутаційній шафі

Реалізація мережі розгалуженого підприємства є досить комплексною задачею. Для побудови такої мережі потрібно провести докладний аналіз усіх сервісів компанії, проаналізувати фінансові можливості, можливість підключення провайдерів інтернету, тощо.

Здешевлення хмарних технологій та швидкісного доступу до мережі «Інтернет» дозволяє підприємствам не закупати дороге серверне обладнання та не витрачати на його обслуговування кошти. Оренда обладнання допомагає суттєво спростити обслуговування системи підприємства та уникнути старіння техніки. При закінченні строку експлуатації – достатньо лише орендувати новий сервер.

З нинішнім проникненням інтернету у всі сфери життя, стабільний доступ до мережі – запорука безперебійної роботи майже будь якого підприємства. Тому вибір надійного провайдера та реалізація додаткових резервних каналів зв’язку є однією з основних задач.

Грамотна побудова мережі, створення надлишкових вузлів та точок підключення – гарантія простого масштабування в майбутньому та простого відновлення підключення у разі поломок.

Правильна конфігурація маршрутизаторів, детальне налаштування правил брандмауеру допомагає підвищити захищеність даних підприємства від викрадення та псування. А контроль мережевого доступу – допомагає захистити систему підприємства в цілому.

Розвиток віртуальних приватних мереж зробив можливим створення складних мереж підприємства не обмежуючись фізичним розташуванням. Використання шифрування та контролю доступу дозволяє будувати віртуальні приватні мережі на основі ненадійних відкритих мереж, таких як «Інтернет».

РОЗДІЛ 3
РЕАЛІЗАЦІЯ ТА ВПРОВАДЖЕННЯ ВІДМОВОСТІЙКОЇ МЕРЕЖІ ПІДПРИЄМСТВА

3.1. Вибір обладнання та програмного забезпечення

Виходячи з розробленого проектного завдання необхідно побудувати мережу підприємства. Підприємство складається з 4 філій та 1 центрального офісу. Для спрощення впровадження, а також для більш стабільної роботи мережі, потрібно стандартизувати обладнання між філіями. Тобто моделі маршрутизаторів, комутаторів, іншого обладнання повинні бути максимально однакові, схожі за принципом роботи, програмним забезпеченням, тощо. Це частково стосується і головного офісу. Через підвищене навантаження, в головному офісі допускається встановлення обладнання з більшою продуктивністю та додатковим функціоналом. Для забезпечення безперебійної роботи мережі, канали зв’язку у всіх філіях потрібно дублювати.

В якості маршрутизаторів буде використано маршрутизатори «RouterBoard» компанії Mikrotik. Компанія Mikrotik – це латвійський виробник мережевого обладнання, котрий розробляє маршрутизатори, комутатори, точки доступу, а також власне програмне забезпечення.

Маршрутизатори компанії Mikrotik працюють на операційній системі власної розробки RouterOS, котра створена на базі Linux. Дана операційна підтримує багато модулів, сервісів та протоколів, котрі можна використовувати як у невеликих так і у складних мережах. Керування маршрутизаторами на базі RouterOS відбувається за допомогою графічного інтерфейсу WinBox, веб інтерфейсу, або безпосередньо в текстовому вигляді через командну строку. В RouterOS реалізована повна підтримка таких популярних утиліт як iptables та iproute, що суттєво спрощує налаштування маршрутизаторів. Також, в операційній системі реалізовано широкі

можливості резервного копіювання та відновлення як налаштувань так і знімків операційної системи. Не маловажним є те, що перенос конфігурацій та знімків операційної мережі допускається між маршрутизаторами різних моделей, та навіть різних сімейств.

Вибір в якості маршрутизаторів саме RouterBOARD зумовлено їх перевагами з поміж інших, а саме:

– значно нижча вартість, порівнюючи з іншими промисловими рішеннями такими, наприклад Cisco.

– відсутність моделі «за підпискою», коли за оновлення програмного забезпечення виробник стягує додаткову плату.

– можливість швидкої заміни маршрутизаторів, навіть на іншу модель, із зберіганням конфігурацій.

– підтримка всіх необхідних сервісів, таких як шифровані VPN тунелі, брандмауери, тощо.

– більш висока продуктивність у порівнянні з маршрутизаторами домашнього сегменту.

В якості маршрутизаторів в філіях буде використано Mikrotik hAP RB951UI-2nD. Особливості:

– 5 BASE-T портів 10/100 Мбіт/с, 1 USB 2.0;

– 802.11gn Wi-Fi;

– канальна швидкість 300 Мбіт/с;

– routerOS Level4;

– можливість використовувати у якості джерела живлення адаптер 10-28 В, або PoE.

Даний маршрутизатор було обрано через добре співвідношення ціни до характеристик та продуктивності. Він підтримує всі необхідні сервіси, котрі будуть використовуватись у філіях. Безпровідний доступ на маршрутизаторі буде використовуватись лише для налаштування та адміністрування. Для простих користувачів безпровідна мережа буде заблокована.

Для здешевлення мережі, прийнято рішення не використовувати на філіях обладнання з підтримкою Gigabit ethernet (швидкостями до 1000 Мбіт/с).

В якості основного маршрутизатора у центральному офісі використано MikroTik RB2011UiAS-RM. Цей маршрутизатор для встановлення в серверну стійку має наступні особливості:

– 5 BASE-T портів 10/100 Мбіт/с, 5 BASE-T портів 10/100/1000 Мбіт/с, 1 SFP порт;

– канальна швидкість до 1500 Мбіт/с;

– RouterOS Level5 з можливістю створення VPN тунелів, обмеження та фільтрації трафіку, динамічною маршрутизацією, тощо.

Використання даного маршрутизатору в якості центрального зумовлено його підвищеною потужністю, адже навантаження на нього буде значно вище від маршрутизаторів у філіях. До того ж, порти з підтримкою швидкості до 1000 Мбіт/с дозволять за необхідності підключати швидкісне високонавантажене обладнання та високошвидкісні канали Інтернет.

В якості комутаторів буде використано TP-Link TL-SF1048. Це не керовані комутатори з 48 портами 100BASE-T (швидкість до 100 Мбіт/с). Внутрішня пропускна здатність комутатора сягає 9,6 Гбіт/с. Дані комутатори буде використано для кабельної комутації всіх клієнтів. Також цей комутатор буде під’єднано до маршрутизатору.

Для реалізації бездротової мережі використано точки доступу Ubiquiti UniFi UAP-AC-LR. Це дводіапазонні точки доступу, з підтримкою Wi-Fi 2.4 та 5 ГГц. Пропускна здатність відповідно 450 та 867 Мбіт/с. Дані точки доступу підключаються за допомогою PoE інжекторів, що суттєво полегшує їх монтаж. Переваги даних точок доступу наступні:

– безшовний роумінг. Можливість переключатись між точками доступу без обриву інтернет з’єднання та втручання користувача.

– висока стабільність сигналу. Дводіапазонна триполярна антена з коефіцієнтом підсилення 3 дбі та підсилювачі на 24 дбм дозволяють реалізувати стабільне підключення на відстані до 183 метрів без перешкод.

– підтримується більше 200 одночасних підключень.

– можливість реалізувати дводіапазонну мережу, коли під одним ім’ям реалізовано мережу зі стандартом 2.4 та 5 Ггц.

– можливість створення гостьових мереж без доступу до основної.

Налаштування точок доступу Ubiquiti можливо з використанням додатку на смартфоні, або за допомогою спеціального програмного забезпечення UniFi Controller. Дане програмне забезпечення дозволяє налаштовувати всі точки доступу в мережі, контролювати їх та вести статистику. UniFi Controller буде встановлено на окремому сервері.

В якості серверу зберігання даних використовуються звичайні x86 комп’ютери в корпусах для серверної стойки. В якості операційної системи буде встановлено Ubuntu Server 22.04 LTS. Спільний доступ до сховища буде реалізовано за допомогою Samba.

Для роботи внутрішнього-радіо та інших дрібних сервісів буде використано, міні-комп’ютери на базі ARM процесору, RaspberryPi model 3B. Дані міні-комп’ютери дозволяють встановити повноцінну операційну систему на базі Linux та використовувати всі її переваги. Так, на RaspberryPi буде реалізовано відтворення музики з файлів формату mp3 або інтернет-радіо та попередньо записаних рекламних повідомлень.

Також, в кожному відділенні, на базі RaspberryPi буде реалізовано власний DNS сервер з використанням Pi-hole. Pi-hole – це Linux додаток, який дозволяє блокувати рекламний трафік в мережі, а також блокує інтернет-треккери. Він представляє собою окремий DNS сервер, в котрий завантажено списки DNS імен, які потрібно заблокувати. При отриманні запиту на таке ім’я Pi-hole блокує його. Таким чином рекламні повідомлення в браузерах, додатках, пристроях перестають працювати. Pi-hole виконує функції брандмауера реклами, працюючи на рівні DNS запитів.

Для роботи IP телефонії буде використано окремий x86 сервер на базі системи Ubuntu Server 22.04 LTS та програмне забезпечення Asterisk. Asterisk – це безкоштовне програмне забезпечення для реалізації роботи IP телефонії. Воно працює на таких операційних системах як Linux, FreeBSD, Solaris, OpenBSD та ін. Дане програмне забезпечення дозволяє реалізувати повноцінну АТС з підтримкою багатьох протоколів та широким функціоналом, а саме:

- голосова пошта;
- групові дзвінки;
- інтерактивні голосові меню;
- колл-центри з розподіленням вхідних дзвінків;
- запис дзвінків та багато іншого.

У якості основного серверу буде використано орендований VDS сервер. VDS (англ. Virtual Dedicated Server) це віртуальний виділений сервер, котрий надається в оренду провайдерами. З боку керування VDS сервери максимально наближені до звичайних фізичних серверів. Провайдер може надати повноцінний root доступ до обладнання, можливість встановлення будь яких операційних систем, власну IP адресу, налаштування брандмауерів та маршрутизації. Розміщення серверів в великих центрах обробки даних дозволяє гарантувати майже безперебійну доступність серверу та високошвидкісний доступ до мережі Інтернет. Серед переваг використання орендованих серверів можна виділити наступні:

- відсутність необхідності придбання обладнання;
- відсутність необхідності обслуговування обладнання;
- швидка заміна обладнання у разі пошкодження;
- максимальна доступність серверу через використання резервних каналів зв’язку та джерел безперебійного живлення;
- можливість простого та швидкого масштабування у разі необхідності;
- економія електроенергії;

– розміщення серверів в окремих цод підвищує захист інформації від фізичного пошкодження та викрадення (у разі фізичного пошкодження або викрадення серверу).

До умовних недоліків використання орендованих серверів можна віднести наступне:

– залежність від підключення до мережі «Інтернет»;

– щомісячна абонентська плата;

– при оренді за кордоном, використання серверів може регулюватись законами країни розміщення центру обробки даних;

– можливість повної втрати серверу через дії недобросовісного орендодавця.

Так, при використанні орендованих серверів, компанія може суттєво зменшити свої витрати, адже нема необхідності в закупівлі дорогого обладнання та супутніх витратах. Нема необхідності в закупівлі серверу, джерел та безперебійного живлення. Не потрібно фізично обслуговувати серверне обладнання, резервувати сервери, проводити регулярну заміну накопичувачів, тощо. Також це знижує витрати електроенергії, адже серверне обладнання має працювати цілодобово. При необхідності орендований сервер можна покращити, або замінити на інший без значних витрат. Фізичне розміщення серверів в центрах обробки даних допомагає нівелювати ризики фізичної втрати серверу або його викрадення.

Проте, використовуючи орендовані сервери, компанія стає цілком залежною від підключення до мережі «Інтернет». При розміщенні серверу безпосередньо на підприємстві, у разі відсутності доступу до мережі Інтернет, сервер може залишатись доступним через локальну мережу. Для доступу до орендованих рішень – наявність зовнішнього каналу зв’язку – обов’язкова. При використанні VDS, присутня орендна плата, котра залежить від тарифів орендодавця, характеристик серверу та інших супутніх послуг. Якщо сервер орендовано у закордонного ЦОД, дії користувача можуть регулюватись законами країни походження ЦОД. Наприклад, в деяких

країнах уряду можуть надавати доступ до серверів та трафіку для аналізу. Використання не ліцензійного ПЗ або інших матеріалів може каратись законом. При виборі місця розташування VDS потрібно аналізувати умови оренди та закони.

На підприємстві використовується сервер, котрий орендовано в німецькій компанії Hetzner з наступними параметрами:

– 64 Гб оперативної пам’яті;
– процесор Intel Core i7-6700;
– PCI-E NVME накопичувачі на 2 Тб.

На сервері встановлено операційну систему Windows Server 2019 Standard Edition. Основне призначення серверу – системи бухгалтерського обліку, системи контролю замовлень, віртуальні контрольно-касові машини. В якості системи обліку встановлено програмне забезпечення «1С Підприємство» та сервер баз даних Microsoft SQL Server 2019.

Потрібно забезпечити безперебійний доступ до серверу, адже за допомогою нього відбуватиметься збір та видача замовлень, видача касових чеків, ведення бухгалтерського обліку та податкової звітності. Доступ до серверу буде відбуватись за допомогою шифрованих RDP з’єднань у термінальному режимі. Для виключення залежності доступності серверу від роботи VPN мережі, підключення потрібно проводити напряму.

Задачу створення відмовостійкої розгалуженої мережевої інфраструктури підприємства можна розділити на декілька етапів. Перш за все потрібно підключити та налаштувати зовнішні канали зв’язку від провайдерів, налаштувати резервні канали та методи автоматичного переключення між ними. Далі потрібно створити захищену VPN мережу, котра дозволить об’єднати всі філії в одну. Далі, налаштувати аналіз трафіку, виділити потоки, котрі підуть через VPN мережу, виділити потоки, які будуть іти напряму до мережі «Інтернет». На основі аналізу побудувати таблиці маршрутизації та адресації в мережі. Налаштувати інші супутні сервіси, такі як DNS фільтри, доступи до заблокованих ресурсів, тощо.

3.2. Налаштування зовнішніх ліній зв’язку та VPN мережі

На сьогодні, майже будь яке підприємство залежить від доступу до мережі «Інтернет». Створення надійного безперебійного підключення до мережі «Інтернет» є одною з найголовніших задач.

Для забезпечення безперебійного доступу до мережі «Інтернет», у кожній філії підприємства буде підключено два різні канали зв’язку. Ці канали повинні бути надані різними провайдерами. Адже, якщо підключити два канали від одного провайдеру, то з’являється велика вірогідність того, що обидва канали зв’язку будуть недоступні в один проміжок часу. У якості основного інтернет провайдеру обрано компанію «Київстар». У якості резервного каналу – компанію «Датагруп». Залежно від філії, доступ до «Інтернет» буде підключено за допомогою звитої пари, або з використанням оптоволоконного кабелю. В головному офісі, швидкість підключення основного провайдеру до 1 Гбіт/с. В усіх інших філіях швидкість доступу до мережі «Інтернет» буде до 100 Мбіт/с. Резервні канали матимуть швидкість до 100 Мбіт/с. Кожен канал зв’язку (основний та резервний) буде мати свою виділену IP адресу.

Для забезпечення безперебійного доступу до мережі «Інтернет», потрібно налаштувати автоматичне переключення провайдерів. Так, потрібно визначити основного провайдера, перевіряти доступність мережі «Інтернет» на ньому, та у разі відключення доступу – змінювати канал на резервний. Як тільки запрацює основний канал – потрібно одразу підключити його. Автоматичне переключення провайдерів можна реалізувати наступним чином.

Перш за все потрібно визначити, як буде підключено провайдерів до маршрутизаторів. Візьмемо за правило, що на кожній філії, до першого Ethernet порту буде підключено основний провайдер. До другого, відповідно, резервний. Почнемо з конфігурації першого порту.

Так як, у нас підключення до мережі «Інтернет» відбувається за допомогою DHCP з'єднання, тобто ми отримуємо автоматичні налаштування від провайдеру, налаштуємо DHCP клієнт на першому порту (рис. 3.1).

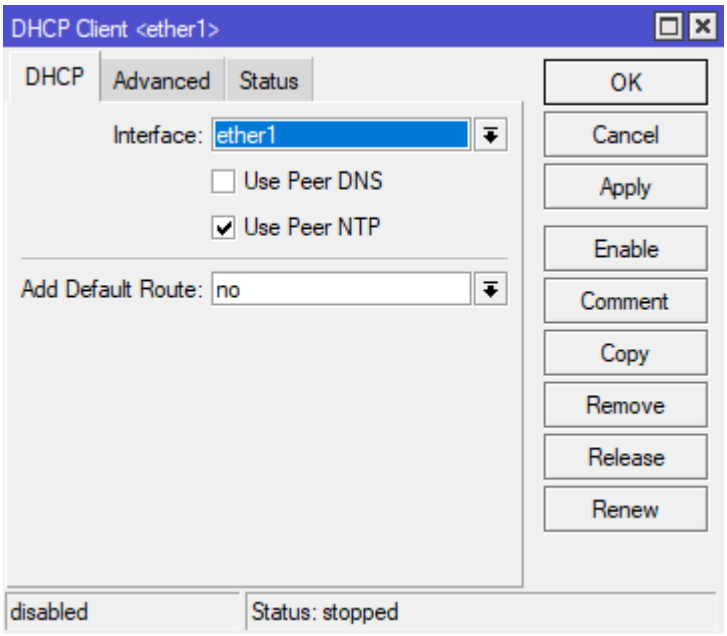


Рисунок 3.1 - Налаштування DHCP клієнта на першому порту маршрутизатора

Обов'язково потрібно відключити опцію «Add Default Route». Ця опція додає маршрут «за замовчуванням» до таблиці маршрутизації. Цей маршрут використовується маршрутизатором для трафіку, котрий не пішов по іншим заданим маршрутам.

Для другого порту налаштування DHCP клієнту аналогічні, потрібно тільки змінити інтерфейс на «ether2». Так, як у нас відключено опцію «Add Default Route», потрібно налаштувати маршрути вручну. Для цього в меню IP-Routes додаємо маршрут для першого провайдера (рис.3.2). Тут потрібно вказати gateway провайдера та distance. Gateway можна взяти з статусу клієнта DHCP першого провайдеру. Distance – це значення пріоритетності маршруту. Чим менше це значення – тим більш високий пріоритет маршруту. Також, для спрощення подальшого налаштування, встановимо коментар для маршруту «ISP1».

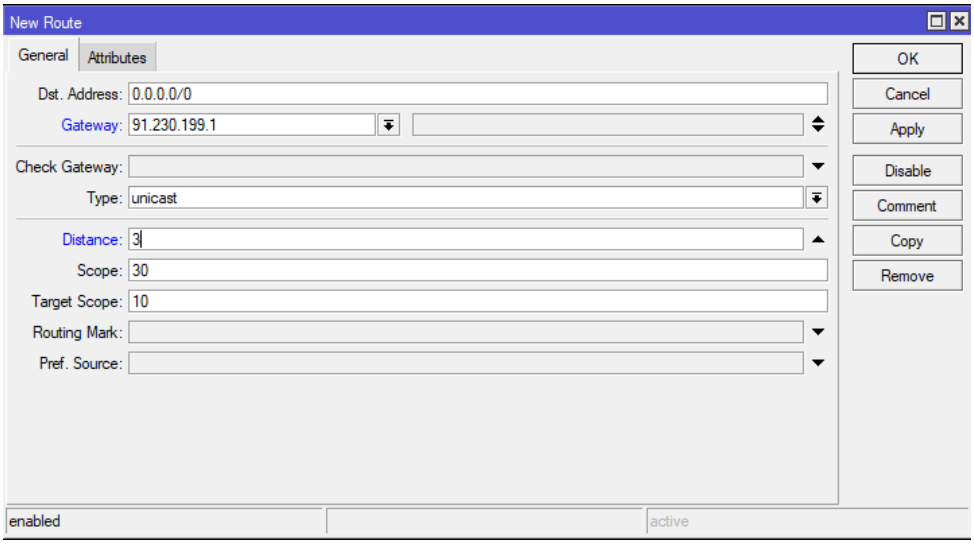


Рисунок 3.2 - Створення маршруту для першого провайдеру

По аналогії з маршрутом першого провайдеру налаштуємо маршрут другого. В якості Gateway впишемо адресу шлюзу другого провайдера, Distance встановимо 2, коментар – «ISP2».

Тепер створимо ще один маршрут, котрий буде направляти всі запити до перевірочної адреси через першого провайдера (рис.3.3). У якості перевірочної адреси слід обирати адресу в мережі «Інтернет», котра матиме 100 відсотків доступності у будь який проміжок часу. Використаємо адресу DNS серверу Cloudflare 1.1.1.1.

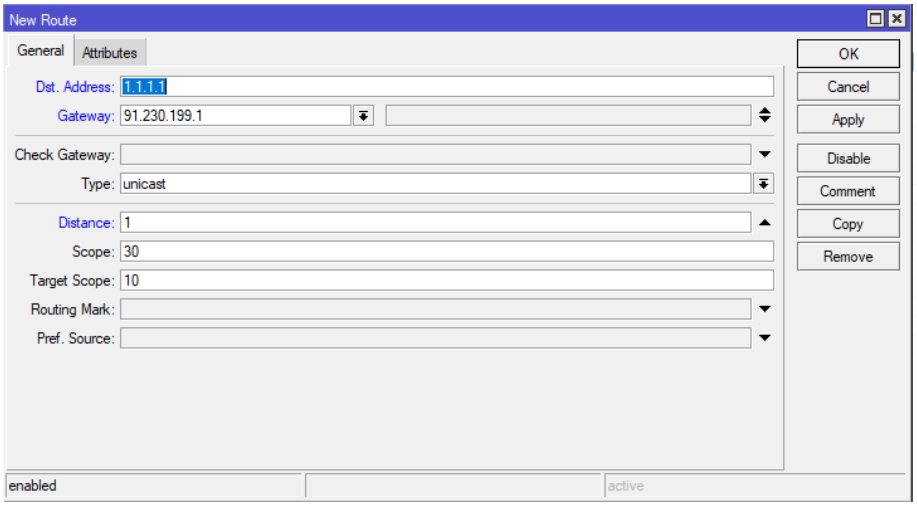


Рисунок 3.3 - Маршрут для перевірки доступності мережі Інтернет

Тепер, за допомогою брандмауера (IP-Firewall), потрібно заборонити доступ до адреси 1.1.1.1 з резервного каналу. Це необхідно для того, щоб перевірка доступності працювала лише з основного каналу. Для цього потрібно додати правило у ланцюгу «Output» з вказанням адреси призначення 1.1.1.1, вихідного інтерфейсу другого провайдера «ether2» та дією «drop».

Тепер, за допомогою утиліти «Netwatch» можна організувати перевірку доступності інтернету на першому провайдері та автоматичне переключення на резервний канал. Для цього створимо нове правило перевірки на адресу 1.1.1.1 з інтервалом у 30 секунд (рис. 3.4).

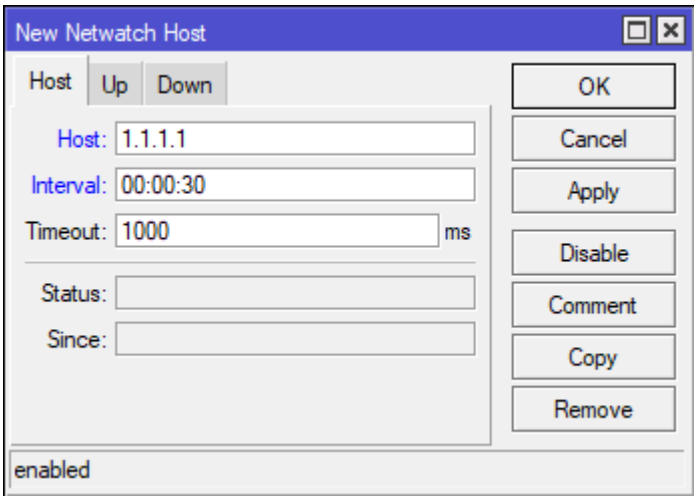


Рисунок 3.4 - Правило «Netwatch» для перевірки доступності інтернету

Для «Netwatch» можна указати дії при доступності мережі («Up») та при недоступності («Down»). При недоступності потрібно активувати маршрут через другого провайдера командою /ip route enable [find comment="ISP2"]. При доступності, відповідно, маршрут буде деактивовано /ip route disable [find comment="ISP2"]. При цьому, маршрут через першого провайдера можна не деактивувати, адже в нього вказано менший пріоритет (distance 3, проти distance 2 у резервного), тому при активації резервного маршруту трафік піде саме через нього.

Дані налаштування можна використати на всіх філіях. При цьому потрібно лише змінити шлюзи на відповідні.

VPN між філіями буде організовано за допомогою IP тунелів. IP тунель – це протокол каналу зв'язку між мережами. Транспортування відбувається з використанням інших протоколів шляхом інкапсуляції пакетів. Даний протокол є повністю відкритим, та не має в собі жодних механізмів забезпечення безпеки, таких як шифрування та аутентифікація. Для забезпечення безпеки використаємо протокол IPsec, зверху якого будемо створювати IP тунель. З особливостей також слід відмітити те, що дані протоколи працюють в режимі stateless, тобто не забезпечують збереження стану з'єднання, а також не використовують порти. Тому для створення тунелю необхідно, щоб між маршрутизаторами не було сторонніх NAT, а контроль за з'єднанням потрібно реалізовувати засобами маршрутизатора, наприклад, за допомогою «Netwatch».

Для створення тунелю потрібно додати відповідний інтерфейс в меню Interfaces-IP Tunnel. Тут вказується ім'я тунелю, локальну адресу та віддалену адресу, а також кодову фразу для IPsec. В якості локальної адреси вказується виділена IP адреса маршрутизатора, на якому відбувається налаштування, в якості віддаленої адреси – адреса маршрутизатора з іншої сторони тунелю (рис. 3.5). На другому маршрутизаторі налаштовується все аналогічно, тільки міняються місцями локальна та віддалена адреса.

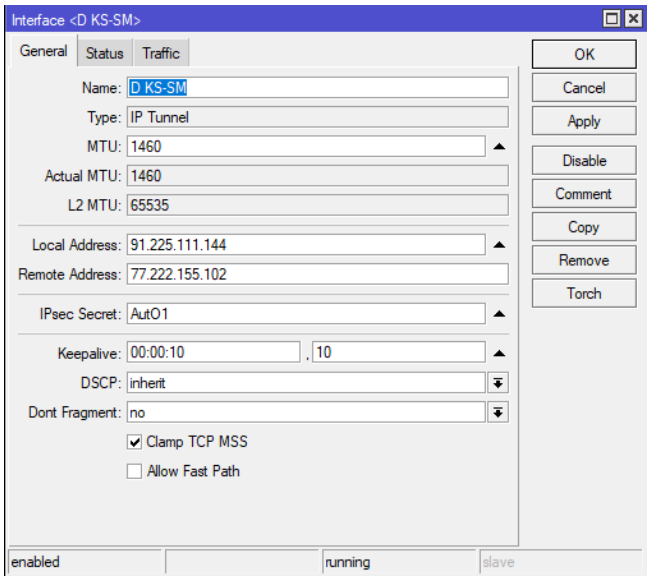


Рисунок 3.5 - Налаштування IP тунелю

Слід зазначити, що при використанні IPsec потрібно вимикати опцію Allow Fast Path. «Fast Path» дозволяє направляти пакети без додаткової обробки в ядрі Linux. Цей метод суттєво підвищує швидкість перенаправлення пакетів, проте він не сумісний з додатковими обробками, такими як IPsec.

Тунелі буде налаштовано від всіх філій до центрального офісу. Для забезпечення безперебійної роботи мережі потрібно налаштувати тунелі між всіма провайдерами, як резервними, так і основними. Таким чином, між однією філією та центральним офісом потрібно створити 4 тунелі:

- основний провайдер 1 до основного провайдеру 2;
- основний провайдер 1 до резервного провайдеру 2;
- резервний провайдер 1 до основного провайдеру 2;
- резервний провайдер 1 до резервного провайдеру 2.

Така схема підключення дозволить швидко змінювати тунель з мінімальними затримками в мережі. Це не створить додаткового навантаження на маршрутизатор, так як основна робота буде проводитись лише під час обміну пакетами через конкретний тунель.

Для подальшого налаштування потрібно визначити адресацію в мережі. Для цього визначимо наступні підмережі:

- центральний офіс, локальна мережа 192.168.0.0/24;
- філія 1, локальна мережа 192.168.1.0/24;
- філія 2, локальна мережа 192.168.2.0/24;
- філія 3, локальна мережа 192.168.3.0/24;
- філія 4, локальна мережа 192.168.4.0/24;
- філія 5, локальна мережа 192.168.5.0/24;

Адреси IP тунелів буде визначено за наступним принципом: філія 1 – підмережі 10.10.10.0/24, 10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24, відповідно до 4х тунелів; філія 2 – підмережі 10.10.20.0/24, 10.10.21.0/24, 10.10.22.0/24, 10.10.23.0/24 і так далі.

Тепер потрібно налаштувати адресацію для тунелів. Перш за все призначимо адресу першому тунелю в центральному офісі, та тунелю у першій філії (рис. 3.6).

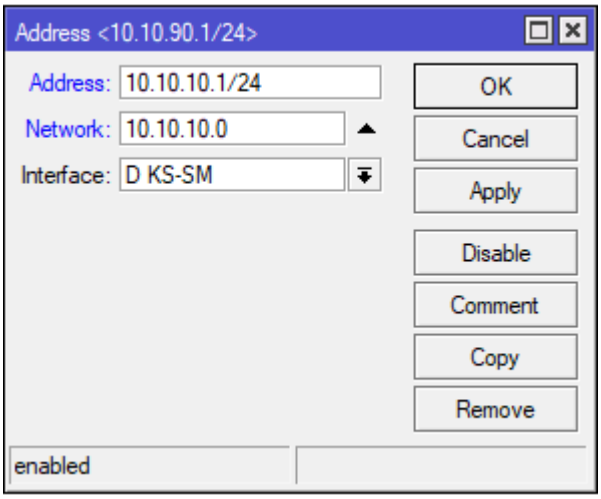


Рисунок 3.6 - Призначення адреси IP тунелю

Так, адреса тунелю в центральному офісі буде мати вигляд 10.10.10.1/24, мережа, відповідно 10.10.10.0. З іншого боку тунелю, у філії, адреса має бути 10.10.10.2/24 тієї ж мережі. Залишиться лише вказати маршрут в таблиці маршрутизації. Для цього на маршрутизаторі в центральному офісі потрібно маршрут до мережі філії через IP тунель (рис. 3.7).

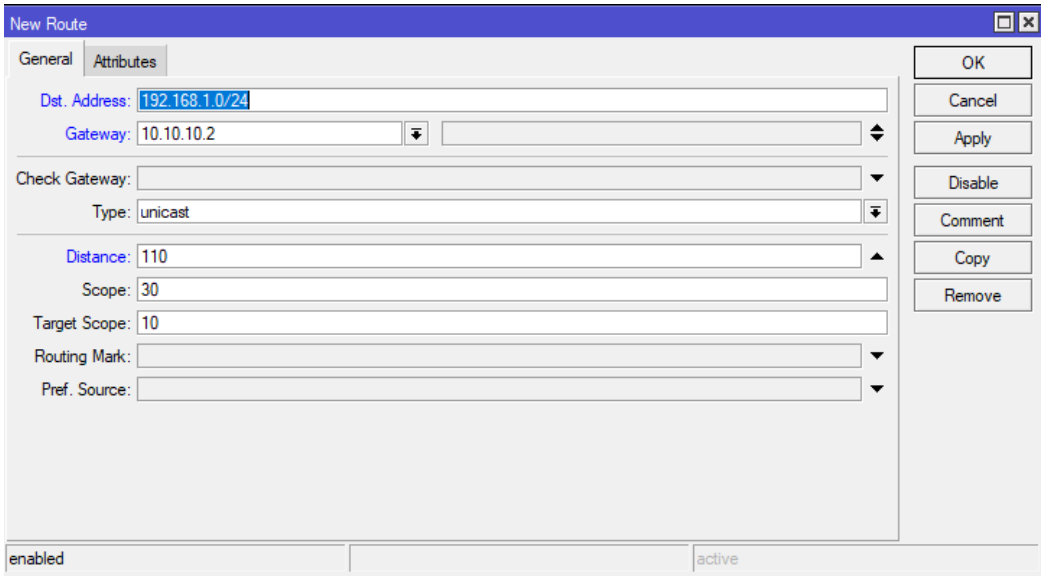


Рисунок 3.7 - Маршрут до мережі через тунель

Тут в якості Dst. Address вказується підмережа, куди потрібно отримати доступ (мережа Філії 1), Gateway – шлюз, через який буде надано доступ (в даному випадку адреса IP тунелю у Філії 1) та Distance. Параметр Distance заданий великим числом для того, щоб мінімізувати пріоритет цього маршруту. При такому пріоритеті, весь трафік спочатку намагатиметься іти через основні маршрути (маршрути провайдерів), а вже потім піде через IP тунель. Якщо встановити пріоритет вище, наприклад, 1, тоді абсолютно весь трафік, буде направлено через IP тунель. Цього робити не потрібно, адже це призведе до підвищення навантаження на мережу та канал в центральному офісі. Також потрібно додати коментар до маршруту «Tunnel1 1-1».

З іншого боку тунелю, на маршрутизаторі потрібно зробити такі самі налаштування, беручи до уваги адреси маршрутизатора та мережі. Таким чином налаштовуються всі тунелі між філіями та центральним офісом.

Для автоматичного переключення маршрутів потрібно створити відповідні правила в «Netwatch». Так потрібно перевіряти доступність шлюзу в конкретному тунелі та перемикати маршрут у разі необхідності. Наприклад для вищеописаного тунелю правило матиме наступний вигляд: перевірка доступності адреси шлюзу 10.10.10.2, якщо недоступно - /ip route enable [find comment="Tunnel 1-2"], /ip route disable [find comment="Tunnel 1-1"], якщо доступно - /ip route enable [find comment="Tunnel 1-1"], /ip route disable [find comment="Tunnel 1-2"]. Так можна добитись автоматичної зміни тунелю у випадку переходу на резервного провайдера.

3.3. Налаштування локальної мережі, DNS серверів

Локальні мережі у філіях та центральному офісі буде побудовано за однією схемою. Всі клієнти локальної мережі будуть підключатись за допомогою DHCP. В маршрутизаторі буде налаштовано DHCP сервер на відповідну адресацію. Буде задано пул адрес у заданих діапазонах, наприклад 192.168.0.50-192.168.0.200. Час оренди адреси – 30 хвилин. Важливою

умовою підключення клієнтів до мережі є правильне ім’я клієнта. Це може бути ім’я комп’ютеру, назва принтеру, мобільного пристрою, тощо. Правильне іменування суттєво полегшить аналіз та усунення проблем у разі їх виникнення. Сталі клієнти, та ті пристрої, до яких потрібен віддалений доступ будуть мати статичну адресу. Це можна зробити безпосередньо в налаштуваннях DHCP серверу (рис 3.8).

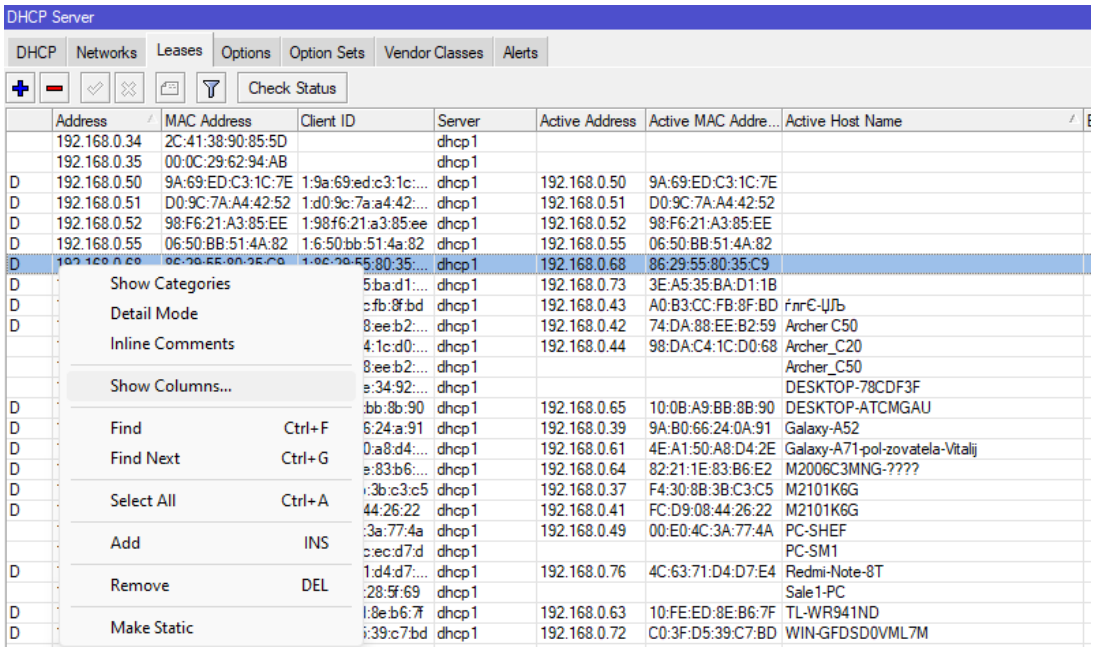


Рисунок 3.8 - Адреси, видані DHCP сервером

Клієнти з підключенням за допомогою кабелів буде приєднано до комутатору. Комутатор в свою чергу буде приєднано до порту номер 3 на маршрутизаторі. Точка доступу до безпровідної мережі буде приєднана до порту номер 4. В якості точки доступу виступатиме Ubiquiti UniFi UAP-AC-LR. Для її налаштування необхідно встановити на сервер програмне забезпечення UniFi Controller. Налаштування точки доступу досить просте и зводиться до вибору імені мережі, створення гостьової мережі та задання необхідних параметрів аутентифікації. Точка доступу не буде сама роздавати адреси, в якості DHCP серверу буде використано маршрутизатор. Порти 3 та 4 буде поєднано мостом.

Для покращення роботи мережі, підвищення захисту та блокування реклами і небажаного трафіку потрібно створити власний DNS. DNS сервер буде створено на базі RaspberryPi. За основу буде взято дистрибутив Pi-hole.

Реалізація DNS серверу буде відбуватись в два етапи. Спочатку потрібно встановити та налаштувати дистрибутив Pi-hole. Наступним кроком буде встановлення програми cloudflared та перехід на DNS-over-HTTPS.

Для встановлення Pi-hole потрібно виконати наступну команду:

```
curl -sSL https://install.pi-hole.net | bash.
```

Дана команда завантажить дистрибутив для встановлення та запустить інсталяційний скрипт. Під час установки потрібно лише вказати дані аутентифікації до веб інтерфейсу (рис 3.9). Разом з дистрибутивом буде встановлено списки DNS записів, котрі вважаються рекламними або небажаними. Ці записи буде заблоковано.

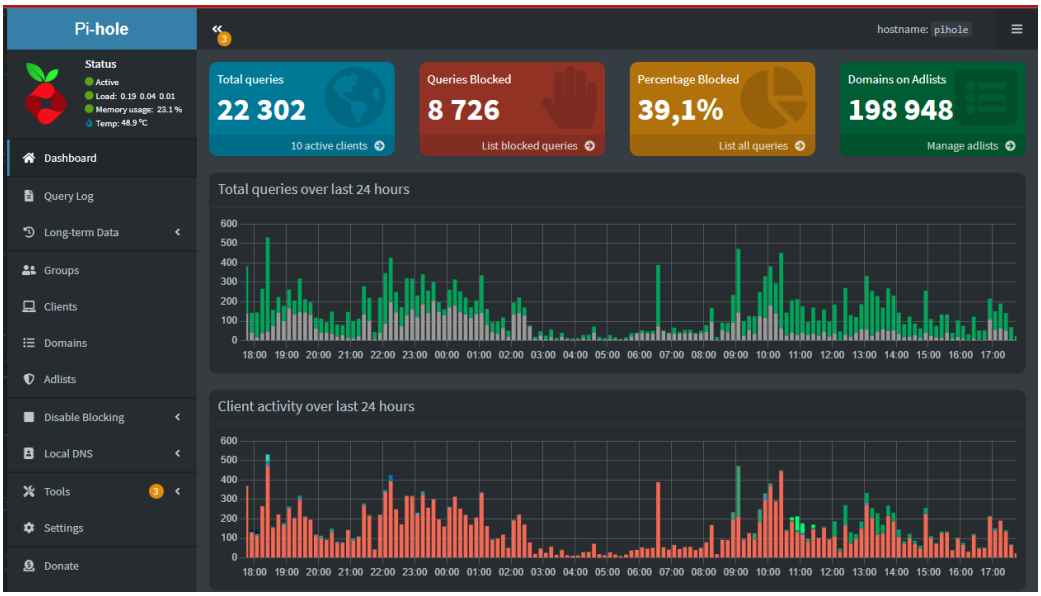


Рисунок 3.9 - Графічний інтерфейс Pi-hole

Наступним кроком є встановлення cloudflared та перехід на DNS-over-HTTPS. Даний протокол дозволяє передавати DNS запити та відповіді через зашифрований HTTPS протокол. Демон cloudflared в нашій конфігурації

використовується в якості DNS-over-HTTPS проксі. Всі запити, відповідно, буде опрацьовано за допомогою сервісу Cloudflare.

Для встановлення cloudflared потрібно виконати наступну команду:

```
cd /tmp
wget https://bin.equinox.io/c/VdrWdbjqyF/cloudflared-stable-linux-amd64.deb
apt-get install ./cloudflared-stable-linux-amd64.deb
cloudflared -v
```

Після встановлення необхідно додати користувача для роботи демона та створити файл конфігурації в каталозі /etc/default/cloudflared:

```
useradd -s /usr/sbin/nologin -r -M cloudflared
echo "CLOUDFLARED_OPTS=--port 5053 --upstream https://1.1.1.1/dns-query --upstream https://1.0.0.1/dns-query" > /etc/default/cloudflared
```

Далі потрібно обов’язково дати права на файл конфігурації та бінарний файл створеному користувачеві Cloudflared:

```
chown cloudflared:cloudflared /etc/default/cloudflared
chown cloudflared:cloudflared /usr/local/bin/cloudflared
```

Для того, щоб демон запускався як служба, потрібно інтегрувати його в system. Для цього потрібно створити файл в каталозі /lib/systemd/system/cloudflared.service з наступним змістом:

```
[Unit]
Description=cloudflared DNS over HTTPS proxy
After=syslog.target network-online.target
```

```
[Service]
Type=simple
User=cloudflared
EnvironmentFile=/etc/default/cloudflared
ExecStart=/usr/local/bin/cloudflared proxy-dns $CLOUDFLARED_OPTS
Restart=on-failure
RestartSec=10
KillMode=process

[Install]
WantedBy=multi-user.target
```

Тепер залишається лише активувати cloudflared як сервіс наступними командами:

```
systemctl enable cloudflared
systemctl start cloudflared
```

Налаштування демону cloudflared на цьому закінчено. Залишається лише вказати в налаштуваннях Pi-hole адресу та порт встановленого cloudflared у якості upstream DNS серверу. Так як демон встановлено на тому ж пристрої що і Pi-hole, адреса буде 127.0.0.1 (рис 3.10).

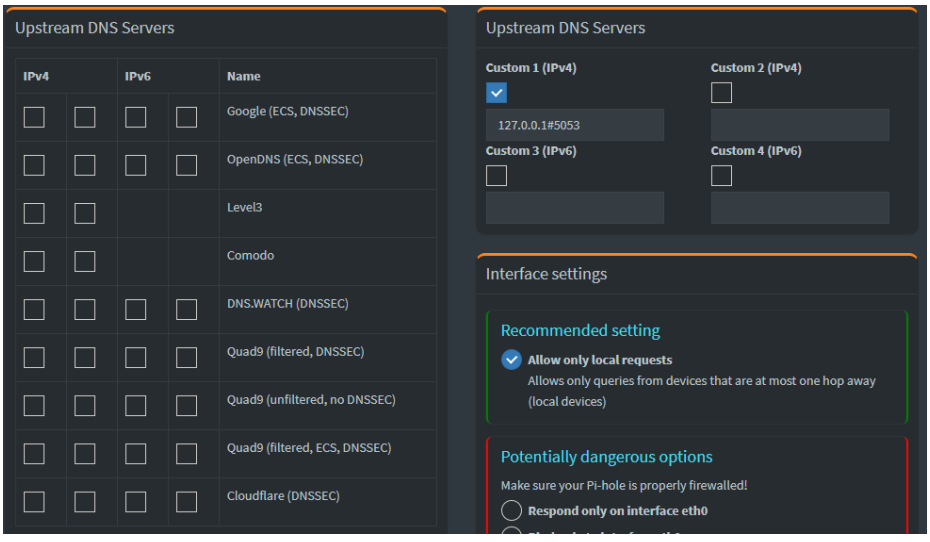


Рисунок 3.10 - Налаштування DNS в Pi-hole

Тепер необхідно налаштувати маршрутизатор на обробку DNS запитів за допомогою Pi-hole. Для цього потрібно вказати адресу пристрою з Pi-hole у якості DNS серверу (рис. 3.11).

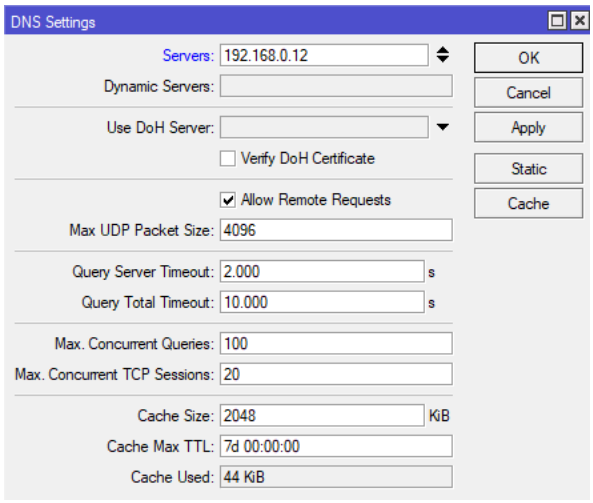


Рисунок 3.11 - Налаштування DNS серверу на маршрутизаторі

Для відмовостійкості мережі бажано, щоб в мережі було декілька DNS серверів. Маршрутизатор дозволяє вказати більше однієї адреси в якості DNS серверу, проте у випадку з Pi-hole, така конфігурація буде працювати не коректно. Так, при налаштуванні альтернативного DNS серверу, маршрутизатор може в будь-який час переключитись на нього, навіть коли Pi-hole знаходиться в мережі та працює. Для реалізації переходу на альтернативні DNS сервери можна використати утиліту «Netwatch». Потрібно перевіряти доступність пристрою з Pi-hole. У разі недоступності виконати команду

```
ip dns set servers=8.8.8.8,8.8.4.4
ip dns cache flush
```

А у разі відновлення роботи команду:

```
ip dns set servers=192.168.0.12
ip dns cache flush
```

Перший рядок задає адресу DNS серверу, другий очищує кеш DNS на маршрутизаторі.

Таким чином робота DNS в мережі реалізовано за наступною схемою. Для користувачів в мережі DNS сервером виступає маршрутизатор. Він кешує DNS записи з серверу та спочатку шукає відповідь на запит користувача в своєму кеші. Для маршрутизатору DNS сервером є Pi-hole. Якщо маршрутизатор не знаходить в своєму кеші відповідь на запит користувача, він звертається до Pi-hole. Pi-hole аналізує запит, шукає співпадіння у списках заблокованих записів, якщо знаходить запит як небажаний – відповідає адресою 0.0.0.0. Якщо в списку заблокованих немає такого запису – Pi-hole оброблює запит за допомогою демону cloudflared. Cloudflared передає запит через протокол DNS-over-HTTPS на сервери Cloudflare та отримує відповідь. Далі вона повертається маршрутизатору на зберігається в його DNS кеші відповідно до заданого TTL.

Слід відмітити, що DNS-over-HTTPS проводить обмін даними через шифрований протокол. Це значить, що DNS запити приховані від будь яких зовнішніх впливів. Особливо це стосується блокування доступу до певних Інтернет ресурсів з боку провайдерів. До того ж використання Pi-hole дозволяє фільтрувати як рекламний трафік, так і інші небажані ресурси, такі як фішингові сайти, тощо.

ВИСНОВКИ

За результатами роботи було створено повноцінну мережеву інфраструктуру географічно розгалуженого підприємства. Було об’єднано в одну спільну мережу 5 окремих філій, використовуючи мережу «Інтернет».

Розділення локальних мереж на відкриті гостьові та закриті допомагає контролювати доступ до внутрішніх сервісів компанії. Прозора адресація та іменування клієнтів суттєво спрощує процес контролю та адміністрування мережі. Підключення філій до мережі «Інтернет» з використання двох різних провайдерів та автоматичним переключенням дозволяє підвищити доступність інтернет сервісів та віртуальної приватної мережі підприємства.

Використання шифрування дозволило гарантувати надійність передачі даних в мережі підприємства. Розділення трафіку на локальний, VPN трафік та зовнішній, дозволяє зменшити залежність від роботи VPN мережі, а також знизити навантаження на саму мережу.

Створення власного DNS серверу з використанням шифрування дозволяє фільтрувати небажану рекламу, фішингові ресурси, тощо. Також, шифрування DNS запитів від провайдерів дозволяє обходити деякі блокування інтернет-ресурсів.

В перспективі можливо створення та впровадження власного VPN сервісу для роботи веб браузерів. Це дозволить розблокувати всі заблоковані інтернет-ресурси та забезпечити шифрування трафіку.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Оліфер В., Оліфер Н. Комп'ютерні мережі. Принципи, технології, протоколи:Ювілейне видання.: Пітер, 2020. – 1008 с. ISBN 978-5-4461-1426-9

2. Повна документація по налаштуванню MikroTik. [Електронний ресурс]. – Режим доступу: www. URL: https://mikrotik.wiki/ (дата звернення:05.03.23).

3. Краузе Д. Windows Server 2016 Administration Fundamentals.: Packt 2017. – 386 с. ISBN 978-1-78588-890-8.

4. Халфакри Г., Raspberry Pi. Официальное руководство для начинающих.: ДМК Пресс 2021. – 386 с. ISBN 978-5-97060-902-6.

5. Негус К., Библия Linux. 10-е издание.: Пітер 2022. – 386 с. 978-5-4461-1797-0.

6. Переводим на DoH домашнюю сеть, или еще один щелчок по носу фильтрации. [Електронний ресурс] – Режим доступу: www. URL: https://habr.com/ru/articles/468621/ (дата звернення:10.03.23).

7. Настраиваем отказоустойчивость Pi-Hole в связке с Mikrotik [Електронний ресурс]. – Режим доступу: www. URL: https://habr.com/ru/articles/556024/ (дата звернення:10.03.23)

8. ДСТУ 3008:2015. «Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання» [Чинний від 2017-07-01]. Київ, 2016. 32 с.

ДОДАТОК А.

Firewall

```
# may/17/2023 16:06:45 by RouterOS 6.45.1
# software id = 0818-BGII
#
# model = RouterBOARD 750G r3
# serial number = 6F3807F3F2AC
/ip firewall filter
add action=accept chain=forward comment=Established connection-state=\
    established,related in-interface-list=WAN
add action=accept chain=input connection-state=established,related \
    in-interface-list=WAN
add action=drop chain=forward comment=Invalid connection-state=invalid \
    in-interface-list=WAN
add action=drop chain=input connection-state=invalid in-interface-list=WAN
add action=drop chain=input comment="Drop ext DNS" dst-port=53 \
    in-interface-list=WAN protocol=tcp
add action=drop chain=input dst-port=53 in-interface-list=WAN protocol=udp
add action=drop chain=output comment=\
    "\D2\E5\F1\F2 \F0\E5\E7\E5\F0\E2\ED\EE\E3\EE \EA\E0\ED\E0\EB\E0" \
    disabled=yes dst-address=8.8.8.8 log=yes out-interface=pppoe-out1 \
    protocol=icmp
add action=accept chain=input in-interface-list=WAN protocol=udp src-port=53
add action=accept chain=input comment="OpenVPN \D2\D3\D2" dst-port=443 \
    in-interface-list=WAN protocol=tcp
add action=accept chain=input comment=\
    "OpenVPN \CD\C0 \C4\D0\D3\C3\CE\CC \CA\CE\CC\CF\C5" dst-port=444 \
    in-interface-list=WAN protocol=tcp
```

```
add action=accept chain=input comment=Ping protocol=icmp
add action=accept chain=input in-interface-list=WAN protocol=icmp
add action=accept chain=input comment=WinBox dst-port=8291 protocol=tcp \
    src-address-list=!BAD-CONTINENTS
add action=accept chain=input comment=SSH dst-port=222 protocol=tcp \
    src-address-list=!BAD-CONTINENTS
add action=accept chain=forward comment="Client services" dst-port=222,443 \
    in-interface-list=WAN protocol=tcp
add action=accept chain=forward comment="\CE\D2\CA\D0\DB\C2\C0\C5\CC
\CF\CE\D0\
    \D2 \C2\C8\C4\C8\CC\CE\CD\C0\C1\CB\DE\C4\C5\CD\C8\C5" dst-port=\
    37777,34667 in-interface-list=WAN protocol=tcp
add action=accept chain=forward comment="\EF\F0\EE\E1\EF\F0\EE\F1
\EF\EE\F0\F2\
    \E0 \ED\E0 \E4\F0\F3\E3\EE\E9 \EA\EE\EC\EF" dst-port=444 \
    in-interface-list=WAN protocol=tcp
add action=accept chain=input comment=L2TP disabled=yes dst-port=\
    1701,500,4500 in-interface-list=WAN protocol=udp src-address-list=\
    !BAD-CONTINENTS
add action=accept chain=input protocol=ipsec-esp
add action=accept chain=input comment=OpenVPN dst-port=443 in-interface-
list=\
    WAN protocol=tcp
add action=accept chain=input comment=PPtP disabled=yes dst-port=1723 \
    protocol=tcp src-address-list=!BAD-CONTINENTS
add action=accept chain=input protocol=gre src-address-list=!BAD-
CONTINENTS
add action=accept chain=forward comment=Asterisk disabled=yes dst-port=\
    5060,4569,36600-39999 in-interface-list=WAN protocol=udp \
    src-address-list=!BAD-CONTINENTS
```

```
add action=drop chain=input comment=Drop in-interface-list=WAN
add action=drop chain=forward in-interface-list=WAN
add action=drop chain=forward comment="block inet" out-interface-list=WAN \
    src-address-list=!NO-INET
```

ДОДАТОК Б.

Mangle

```
# may/17/2023 16:06:45 by RouterOS 6.45.1
# software id = 0818-BGII
#
# model = RouterBOARD 750G r3
# serial number = 6F3807F3F2AC
/ip firewall mangle
add action=change-mss chain=forward new-mss=1440 out-interface=all-ppp \
    passthrough=yes protocol=tcp tcp-flags=syn tcp-mss=1441-65535
add action=change-mss chain=forward in-interface=all-ppp new-mss=1440 \
    passthrough=yes protocol=tcp tcp-flags=syn tcp-mss=1441-65535
add action=accept chain=prerouting disabled=yes
add action=add-src-to-address-list address-list=Router address-list-timeout=\
    none-dynamic chain=prerouting in-interface=bridge-local ttl=equal:63
add action=add-src-to-address-list address-list=Router address-list-timeout=\
    none-dynamic chain=prerouting in-interface=bridge-local ttl=equal:127
add action=mark-routing chain=prerouting comment=YANDEX_VPN dst-address-list=\
    zaborona_vpn new-routing-mark=yandex_vpn passthrough=no
add action=mark-routing chain=output comment=ISP1 connection-mark=from-ISP1 \
    new-routing-mark=ISP1 passthrough=yes
add action=mark-routing chain=prerouting comment=ISP1 connection-mark=\
    from-ISP1 new-routing-mark=ISP1 passthrough=yes
add action=mark-connection chain=forward comment=ISP1 in-interface-list=ISP1 \
    new-connection-mark=ISP1-conn-f passthrough=no
add action=mark-routing chain=prerouting comment=ISP1 connection-mark=\
    ISP1-conn-f in-interface=bridge-local new-routing-mark=ISP1 passthrough=\
```

```
    yes
add action=mark-routing chain=output comment=ISP2 connection-mark=from-ISP2 \
    new-routing-mark=ISP2 passthrough=yes
add action=mark-routing chain=prerouting comment=ISP2 connection-mark=\
    from-ISP2 new-routing-mark=ISP2 passthrough=yes
add action=mark-connection chain=forward comment=ISP2 in-interface-list=ISP2 \
    new-connection-mark=ISP2-conn-f passthrough=no
add action=mark-routing chain=prerouting comment=ISP2 connection-mark=\
    ISP2-conn-f in-interface=bridge-local new-routing-mark=ISP2 passthrough=\
    yes
add action=mark-connection chain=prerouting comment="Autoroute script ISP1" \
    connection-state=new in-interface=ether2 new-connection-mark=from-ISP1 \
    passthrough=yes
add action=mark-connection chain=prerouting comment="Autoroute script ISP2" \
    connection-state=new in-interface=pppoe-out1 new-connection-mark=\
    from-ISP2 passthrough=yes
```

ДОДАТОК В

NAT

```
# may/17/2023 16:06:45 by RouterOS 6.45.1
# software id = 0818-BGII
#
# model = RouterBOARD 750G r3
# serial number = 6F3807F3F2AC
/ip firewall nat
add action=masquerade chain=srcnat comment=hairpin dst-address=192.168.3.0/24 \
    log-prefix=hairpin out-interface=bridge-local src-address=192.168.3.0/24
add action=masquerade chain=srcnat comment=WAN out-interface-list=WAN
add action=dst-nat chain=dstnat dst-port=444 in-interface-list=WAN protocol=\
    tcp to-addresses=192.168.3.2 to-ports=81
add action=dst-nat chain=dstnat comment=\
    "\EF\F0\EE\E1\F0\EE\F1 \E2\E8\E4\E8\EC\EE\ED\E0\E1\EB\FE\E4\E5\ED\E8\E5" \
    dst-port=37777,34667 in-interface-list=WAN protocol=tcp to-addresses=\
    192.168.35.10
# ovpn-yandex not ready
add action=masquerade chain=srcnat comment=YANDEX_VPN out-interface=\
    ovpn-yandex
```

ДОДАТОК Г

DHCP Pool

```
# may/17/2023 16:06:45 by RouterOS 6.45.1
# software id = 0818-BGII
#
# model = RouterBOARD 750G r3
# serial number = 6F3807F3F2AC
/ip dhcp-server network
add address=172.24.188.0/24 dns-server=\
    172.24.188.1,74.82.42.42,8.8.8.8,8.8.4.4 gateway=172.24.188.1 netmask=24 \
    ntp-server=172.24.188.1
add address=192.168.3.0/24 boot-file-name=pxelinux.0 dns-server=\
    192.168.3.1,8.8.8.8 gateway=192.168.3.1 netmask=24 next-server=\
    192.168.3.2 ntp-server=192.168.3.1
```

ДОДАТОК Д

Маршрутизація

```
# may/17/2023 16:06:45 by RouterOS 6.45.1
# software id = 0818-BGII
#
# model = RouterBOARD 750G r3
# serial number = 6F3807F3F2AC
/ip route
add comment=YANDEX_VPN distance=1 gateway=ovpn-yandex routing-mark=yandex_vpn
add check-gateway=ping comment="Autoroute script ISP1" distance=1 gateway=\
    8.8.8.8 routing-mark=ISP1
add check-gateway=ping comment="Autoroute script ISP2" distance=2 gateway=\
    8.8.4.4 routing-mark=ISP1
add check-gateway=ping comment="Autoroute script ISP2" distance=1 gateway=\
    8.8.4.4 routing-mark=ISP2
add check-gateway=ping comment="Autoroute script ISP1" distance=2 gateway=\
    8.8.8.8 routing-mark=ISP2
add check-gateway=ping comment="Autoroute script ISP1" distance=1 gateway=\
    8.8.8.8 scope=10
add check-gateway=ping comment="Autoroute script ISP2" distance=2 gateway=\
    8.8.4.4 scope=10
add comment="Autoroute script ISP2" distance=1 dst-address=8.8.4.4/32 \
    gateway=188.0.95.255 scope=10
add comment="Autoroute script ISP1" distance=1 dst-address=8.8.8.8/32 \
    gateway=91.230.199.1 scope=10
add comment="Cloud Server" distance=1 dst-address=10.42.1.200/32 gateway=\
    172.16.16.1
add comment="TEST Slawus Cloud SRV" disabled=yes distance=1 dst-address=\
```

```
    10.42.1.200/32 gateway=172.16.11.1
add distance=1 dst-address=91.237.123.214/32 gateway=pppoe-out1
add comment=avgreen disabled=yes distance=1 dst-address=149.154.167.220/32 \
    gateway=pppoe-out1
/ip route rule
add action=unreachable comment=Guest dst-address=192.168.0.0/16 src-address=\
    172.24.188.0/24
add action=unreachable comment=Guest dst-address=172.24.188.0/24 src-address=\
    192.168.0.0/16
```