

# ВІДЗИВ НАУКОВОГО КЕРІВНИКА НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ

Студента Горенчука Юрія Сергійовича  
представлену на здобуття освітнього ступеня бакалавр  
зі спеціальності 123 «Комп'ютерна інженерія»

Робота виконана на тему „Проект гетерогенної мережі комерційного підприємства”.

Актуальність роботи зумовлена потребою у надійних системних рішеннях для створення і експлуатації відмовостійких гетерогенних мереж комерційних підприємств.

Основний зміст пояснювальної записки роботи викладено на 73 сторінках тексту, записка містить 2 таблиці, 47 ілюстрації. Список використаних літературних джерел налічує 24 найменування.

Пояснювальна записка складається з реферату, вступу, трьох розділів основного тексту, висновків, списку використаної літератури та додатків.

Розділ 1 присвячений аналізу літературних джерел, дослідження принципів побудови і організації гетерогенних мереж підприємств. Було проаналізовано роботу сучасних локальних і глобальних мереж, розглянуто найбільш поширене обладнання, яке використовується, а також проаналізовано основні вимоги до гетерогенних мереж.

Розділ 2 присвячений питанням проектування гетерогенної мережі. Було обрано топологію, обладнання і протоколи на основі яких функціонуватиме мережа. Особлива увага приділялась питанням надійності і безпеки мережі.

Розділ 3 присвячений питанням розробки, налаштування і тестування гетерогенної мережі. В цьому розділі проводиться моделювання і перевірка працездатності мережі

Висновки містять сумарні результати проведеної роботи.

Список використаних літературних джерел має достатній для даного виду робіт обсяг, є правильно оформленим та повністю опрацьованим у ході виконання роботи.

Таблиця та ілюстрації оформлені досить якісно, є інформативними та наведені у відповідних місцях роботи.

Якість оформлення роботи є високою. Виявлені на етапі попереднього захисту недоліки оформлення пояснювальної записки та презентації усунені. Рекомендації стосовно покращення проекту враховані та виправлені.

Ставлення студента до виконання випускної кваліфікаційної роботи – відповідальне.

У цілому при написанні випускної кваліфікаційної роботи студент Горенчук Ю.С. виявив здібності до оволодіння знаннями, уміннями і навичками з таких дисциплін, як «Захист інформації в інформаційно-комунікаційних системах», «Адміністрування комп'ютерних систем та мереж». Також студент Горенчук Ю.С. показав вміння підібрати необхідну літературу та інші інформаційні джерела, проаналізувати їх, виконати постановку задачі на розробку, розробити гетерогенну надійну мережу і оформити свої розробки та напрацювання як випускну кваліфікаційну роботу.

Випускна кваліфікаційна робота студента Горенчука Ю.С. написана на високому рівні та може бути допущена до захисту в Екзаменаційній комісії.

Пропонована оцінка – «відмінно».

Науковий керівник  
ст. викл. каф. БІ та Т  
21 червня 2020 року



Д.С. Морозов

РЕЦЕНЗІЯ  
на кваліфікаційну роботу  
студента 4 курсу групи КІ-2 спеціальності 123 «Комп'ютерна інженерія»  
факультету інформаційно-комп'ютерних технологій  
Державного університету «Житомирська політехніка»  
Горенчука Юрія Сергійовича  
на тему: „Проект гетерогенної мережі комерційного підприємства”

Кваліфікаційну роботу студента Горенчука Ю. С. “Проект гетерогенної мережі комерційного підприємства” присвячено актуальній тематиці – розробленню гетерогенних мереж.

Робота містить проект гетерогенної мережі комерційного підприємства, виконаний засобами GNS3. До складу пояснювальної записки входить вступ, три розділи основного тексту, висновки, список використаної літератури та додатки.

У першому розділі пояснювальної записки розглянуто загальні аспекти побудови гетерогенних мереж. Зокрема, описано основні принципи побудови локальних та глобальних мереж підприємств, а також гетерогенних мереж.

У другому розділі пояснювальної записки виконано проектування гетерогенної мережі організації, обґрунтовано вибір обладнання, методів та технологій побудови проектованої мережі.

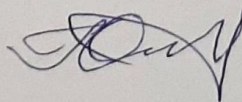
У третьому розділі пояснювальної записки описано процес налаштування гетерогенної мережі та її тестування. Зокрема, розглянуто реалізацію основних функцій захисту системи, таких як трансляція адрес, віртуальні приватні мережі, парольний доступ до мережного обладнання, налаштовано, досліджено та проаналізовано об'єднання дротових мереж, Wi-Fi та IP-телефонії.

Зміст роботи відповідає поставленому завданню. Тему роботи розкрито досить повно. Студентом продемонстровано необхідні теоретичні знання та практичні навички. Пояснювальну записку загалом сформовано логічно, науково й технічно грамотно. Функціонал проекту мережі відповідає заявленому.

Позитивний бік роботи полягає у тому, що одержані результати може бути застосовано для налаштування реального обладнання мережі та для дослідження аналогічних мереж. Водночас, робота має недоліки, серед яких: відсутність висновків за окремими розділами, неповна відповідність формулювання мети у рефераті формулюванню мети у вступі, граматичні та стилістичні помилки, окремі недоліки оформлення.

У цілому кваліфікаційна робота студента Горенчука Юрія Сергійовича “Проект гетерогенної мережі комерційного підприємства” відповідає вимогам рівня вищої освіти “бакалавр” спеціальності 123 “Комп'ютерна інженерія” і рекомендується до захисту в ЕК.

Рецензент:  
доцент кафедри КІ та КБ,  
к. пед. н.  
24 червня 2020 р.



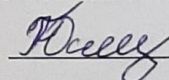
О. С. Головня

Міністерство освіти і науки України  
Державний університет «Житомирська політехніка»  
Факультет інформаційно-комп'ютерних технологій  
Кафедра комп'ютерної інженерії та кібербезпеки

## ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра на тему:  
«Проект гетерогенної мережі комерційного підприємства»

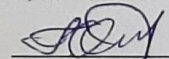
Виконав студент 4-го курсу, групи КІ-2  
спеціальності 123 «Комп'ютерна інженерія»

 Горенчук Ю. С.

Керівник, старший викладач кафедри БІ та Т

 Морозов Д. С.

Рецензент к.пед.н., доцент кафедри КІ та КБ

 Головня О. С.

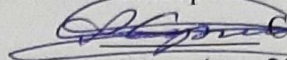
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»  
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ  
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ  
СПЕЦІАЛЬНІСТЬ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ

Завідувач кафедри

комп'ютерної інженерії

та кібербезпеки

 Шіменко А. А.

«06» квітня 2020 р.

**ЗАВДАННЯ**

на випускню кваліфікаційну роботу

Студента **Горенчука Юрія Сергійовича**

Тема роботи: **Проект гетерогенної мережі комерційного підприємства**

затверджена Наказом по університету від «06» квітня 2020 р. № 98с

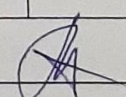
Термін здачі студентом закінченої роботи – **1 червня 2020 р.**

Вихідні дані для роботи:

1. Фізична топологія мережі
2. Міжмережний екран Cisco ASA серії 55xx
3. Маршрутизатори Cisco 7200
4. Комутатори Cisco 2960
5. Графічний симулятор мереж GNS3

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

| Розділ | Консультант   | Підпис, дата   |                  |
|--------|---------------|----------------|------------------|
|        |               | Завдання видав | Завдання прийняв |
| 1      | Морозов Д. С. | 06.04.2020     | 06.04.2020       |
| 2      | Морозов Д. С. | 20.04.2020     | 20.04.2020       |
| 3      | Морозов Д. С. | 11.05.2020     | 11.05.2020       |

Керівник  Морозов Д. С.

### Календарний план

| № з/п | Назва етапів випускної кваліфікаційної роботи                                           | Термін виконання етапів роботи  | Примітка |
|-------|-----------------------------------------------------------------------------------------|---------------------------------|----------|
| 1     | Постановка завдання                                                                     | 6 квітня 2020 – 7 квітня 2020   | Виконано |
| 2     | Пошук, огляд та аналіз літературних джерел щодо організації сучасних гетерогенних мереж | 8 квітня 2020 – 11 квітня 2020  | Виконано |
| 3     | Аналіз технологій побудови локальних мереж підприємств                                  | 12 квітня 2020 – 16 квітня 2020 | Виконано |
| 4     | Аналіз технологій побудови глобальних мереж підприємств                                 | 17 квітня 2020 – 19 квітня 2020 | Виконано |
| 5     | Огляд компонентів гетерогенних мереж                                                    | 20 квітня 2020 – 24 квітня 2020 | Виконано |
| 6     | Проектування фізичної топології організації                                             | 25 квітня 2020 – 30 квітня 2020 | Виконано |
| 7     | Вибір необхідного обладнання                                                            | 1 травня 2020 – 4 травня 2020   | Виконано |
| 8     | Вибір необхідних технологій та протоколів                                               | 5 травня 2020 – 9 травня 2020   | Виконано |
| 9     | Проектування та створення сценаріїв тестування функціоналу підсистеми                   | 10 травня 2020 – 13 травня 2020 | Виконано |
| 10    | Базове налагодження пристроїв мережі                                                    | 14 травня 2020 – 18 травня 2020 | Виконано |
| 11    | Конфігурування пристроїв гетерогенної мережі                                            | 19 травня 2020 – 22 травня 2020 | Виконано |
| 12    | Тестування роботи гетерогенної мережі                                                   | 23 травня 2020 – 24 травня 2020 | Виконано |
| 13    | Аналіз результатів тестування                                                           | 25 травня 2020 – 29 травня 2020 | Виконано |
| 14    | Написання пояснювальної записки                                                         | 30 травня 2020 – 31 травня 2020 | Виконано |
| 15    | Підготовка презентації та виступу                                                       | 4 червня 2020 – 8 червня 2020   | Виконано |
| 16    | Отримання відгуку керівника та рецензії на кваліфікаційну роботу                        | 13 червня 2020                  | Виконано |
| 17    | Захист                                                                                  | 25 червня 2020                  | Виконано |

Студент Горенчук Ю. С.

Керівник Морозов Д. С.

## РЕФЕРАТ

Випускна робота бакалавра складається з топології гетерогенної мережі та пояснювальної записки. Пояснювальна записка до випускної роботи містить 73 сторінок, 47 ілюстрацій та 2 таблиці.

Метою роботи є розробка проекту гетерогенної мережі на базі обладнання Cisco.

В роботі визначено основні завдання на розробку гетерогенної мережі, обґрунтовано актуальність даної розробки та описана сфера її використання, обґрунтований вибір виробника обладнання – Cisco. Наведений сценарій налаштування гетерогенної мережі, загальна топологія мережі, опис конкретних серій обладнання, опис технологій та протоколів, що використовуються в проекті, та тестування проекту. Також наводяться результати тестування.

**КЛЮЧОВІ СЛОВА:** ДРОТОВЕ З'ЄДНАННЯ, WI-FI, IP-ТЕЛЕФОНІЯ, ГЕТЕРОГЕННА МЕРЕЖА, CISCO, ПІДСИСТЕМА ЗАХИСТУ ПЕРИМЕТРУ МЕРЕЖІ.

|            |      |                |                                                                                     |       |                                                                                                       |      |  |      |                                                                   |
|------------|------|----------------|-------------------------------------------------------------------------------------|-------|-------------------------------------------------------------------------------------------------------|------|--|------|-------------------------------------------------------------------|
|            |      |                |                                                                                     |       | КІК.КР.Б – 123 – 20 – ПЗ                                                                              |      |  |      |                                                                   |
| Зм.        | Арк. | № докум.       | Підпис                                                                              | Дата  | Проект підсистеми захисту<br>периметру мережі на базі<br>обладнання Cisco<br><br>Пояснювальна записка | Літ. |  | Арк. | Аркушів                                                           |
| Розроб.    |      | Горенчук Ю. С. |  | 24.06 |                                                                                                       |      |  | 4    | 73                                                                |
| Керівник   |      | Морозов Д. С.  |  | 24.06 |                                                                                                       |      |  |      |                                                                   |
| Н. контр   |      | Єфіменко А. А. |  | 24.06 |                                                                                                       |      |  |      |                                                                   |
| Рецензент. |      | Головня О. С.  |  | 24.06 |                                                                                                       |      |  |      |                                                                   |
| Зав. каф.  |      | Єфіменко А. А. |  | 24.06 |                                                                                                       |      |  |      | Державний університет<br>«Житомирська<br>політехніка», група КІ-2 |

## ABSTRACT

The final work of the bachelor consists of a heterogeneous network topology and an explanatory note. The explanatory note to the final work contains 85 pages, 56 illustrations and 6 tables.

The purpose of this work is to develop a heterogeneous network project based on Cisco equipment.

The paper defines the main tasks for the development of a heterogeneous network, substantiates the relevance of this development and describes the scope of its use, the reasonable choice of the equipment manufacturer-Cisco. The given scenario for configuring a heterogeneous network, the General network topology, a description of specific hardware series, a description of the technologies and protocols used in the project, and testing the project. Test results are also provided.

KEYWORDS: WIRED CONNECTION, WI-FI, IP TELEPHONY, HETEROGENEOUS NETWORK, CISCO, NETWORK PERIMETER PROTECTION SUBSYSTEM.

## ЗМІСТ

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| ЗМІСТ .....                                                                   | 6  |
| ВСТУП .....                                                                   | 8  |
| РОЗДІЛ 1. ПРИНЦИПИ ПОБУДОВИ І ОРГАНІЗАЦІЇ ГЕТЕРОГЕННИХ МЕРЕЖ ПІДПРИЄМСТВ..... | 10 |
| 1.1. ОСНОВНІ ПРИНЦИПИ ПОБУДОВИ ЛОКАЛЬНИХ МЕРЕЖ ПІДПРИЄМСТВ .....              | 10 |
| 1.2. ОСНОВНІ ПРИНЦИПИ ПОБУДОВИ ГЛОБАЛЬНИХ МЕРЕЖ ПІДПРИЄМСТВ .....             | 16 |
| 1.3. ГЕТЕРОГЕННІ МЕРЕЖІ. КОМПОНЕНТИ ГЕТЕРОГЕННИХ МЕРЕЖ .....                  | 27 |
| РОЗДІЛ 2. ПРОЕКТ ГЕТЕРОГЕННОЇ МЕРЕЖІ .....                                    | 37 |
| 2.1. ПРОЕКТ МЕРЕЖІ ОРГАНІЗАЦІЇ .....                                          | 37 |
| 2.2. ОПИС ВИБРАНОГО ОБЛАДНАННЯ.....                                           | 39 |
| 2.3. ОПИС ВИБРАНИХ ТЕХНОЛОГІЙ ТА ПРОТОКОЛІВ.....                              | 48 |
| РОЗДІЛ 3. НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ГЕТЕРОГЕНОЇ МЕРЕЖІ                       | 56 |
| 3.1. БАЗОВЕ НАЛАГОДЖЕННЯ ПРИСТРОЇВ МЕРЕЖІ.....                                | 56 |
| 3.2. НАЛАШТУВАННЯ ГЕТЕРОГЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ.....                       | 59 |
| 3.3. ТЕСТУВАННЯ НАЛАШТУВАНЬ .....                                             | 66 |
| ВИСНОВКИ.....                                                                 | 69 |
| СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ .....                                              | 70 |
| ДОДАТКИ.....                                                                  | 72 |

## ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ACL – Access Control List

ОС – операційна система

МЕ – міжмережний екран

OSI – Open Systems Interconnection

TCP – Transmission Control Protocol

WAN – Wide Area Network

IP – Internet Protocol

LAN – Local Area Network

NAT – Network Address Translation

ASA – Adaptive Security Appliances

|  |  |  |  |  |                          |   |
|--|--|--|--|--|--------------------------|---|
|  |  |  |  |  | КІК.КР.Б – 123 – 20 – ПЗ |   |
|  |  |  |  |  |                          |   |
|  |  |  |  |  |                          | 7 |

## ВСТУП

**Актуальність теми.** Комунікації є важливою складовою нашого життя. Комунікаційні технології, а зокрема Інтернет, дозволяють нам залишатись завжди на зв'язку з оточуючими. Глобальна мережа розвивається стрімкими темпами і в недалекому майбутньому саме вона стане основою, якщо не монополістом усіх комунікаційних мереж. У міру втілення в життя все нових і нових ідей та проектів, які здавалися раніше недосяжними, можливості об'єднаних мереж, що утворюють Інтернет, будуть грати все більш зростаючу роль в реалізації цих проектів.

Одна з найважливіших і основних потреб людини – взаємодія з іншими людьми. На сьогоднішній день спілкування стає для нас так само важливим, як повітря, вода, їжа і дах.

У теперішньому світі, як ніколи, нас зв'язує один з одним використання гетерогенних мереж. Щоб втілити свої ідеї в життя, ми просто і легко можемо миттєво зв'язуватися з іншими людьми та ділитися ними. Відкриття чи будь-які новини стають відомими у всьому світі в лічені секунди. Вихід в мережу і гра з іншими людьми, що знаходяться на інших континентах – лише забавка, що стала доступною завдяки комунікаціям.

Тому слід впроваджувати новітні технології, що з кожним днем надходять в наші домівки та офіси. Одними з них є технологія Wi-Fi та IP-телефонія. Їх метою є забезпечення більш надійної комунікації більшої кількості людей.

Актуальність обраної теми полягає в тому, що впровадження даної гетерогенності в мережу вирішить проблему комунікації в організації. Функціональні можливості гетерогенної мережі дозволять використовувати її у відповідності до поставлених задач.

Метою кваліфікаційної роботи є розробка проекту гетерогенної мережі комерційного підприємства.

Встановлена мета обумовлює наступні завдання:

- аналіз основних підходів побудови гетерогенних мереж;
- вибір засобів реалізації мережі;

|  |  |  |  |  |                          |   |
|--|--|--|--|--|--------------------------|---|
|  |  |  |  |  | КІК.КР.Б – 123 – 20 – ПЗ |   |
|  |  |  |  |  |                          |   |
|  |  |  |  |  |                          | 8 |

- вибір сучасного технічного забезпечення системи;
- розробка системи комунікацій, придатної для розширення надалі;
- реалізація гетерогенної мережі.

Об'єктом дослідження є процес взаємодії гетерогенної мережі комерційного підприємства.

Предметом дослідження є методи і засоби об'єднання різного мережевого обладнання в гетерогенну мережу.

В процесі виконання кваліфікаційної роботи був розроблений проект гетерогенної мережі комерційного підприємства. При цьому були використані дротові з'єднання, Wi-Fi та IP-телефонія.

## РОЗДІЛ 1. ПРИНЦИПИ ПОБУДОВИ І ОРГАНІЗАЦІЇ ГЕТЕРОГЕННИХ МЕРЕЖ ПІДПРИЄМСТВ

### 1.1. Основні принципи побудови локальних мереж підприємств

Локальна комп'ютерна мережа (Local Area Network – LAN) підприємства – це мережева інфраструктура, що забезпечує доступ до мережевих комунікаційних послуг і ресурсів для кінцевих користувачів і пристроїв, розташованих на одному поверсі або в одній будівлі. Важливим питанням постає створення мережі підприємства, об'єднуючи групу локальних мереж, розподілених на невеликій географічній території. Концепції проектування мережі підприємства включають в себе як малі мережі, що використовують один комутатор LAN, так і дуже великі мережі з тисячами підключень. Провідна LAN підприємства створюється з метою здійснення зв'язку між пристроями в будівлі або групою будинків, а також підключення до глобальної мережі (Wide Area Network – WAN) і до периметру мережі Інтернет на ядрі мережі. Зокрема, ця конструкція забезпечує мережеву основу та послуги, до яких можуть бути включені:

- багаторівневе LAN-з'єднання;
- доступ до провідної мережі для співробітників;
- IP-Multicast для ефективного розподілу даних;
- провідна інфраструктура, готова для мультимедійних послуг.

Дротова LAN підприємства використовує ієрархічну модель проектування, щоб розподілити проект на модульні групи. Поділ конструкції на рівні дозволяє кожному рівню реалізувати певні функції, що спрощує мережне проектування, розгортання і керування мережею. Модульність проектування мережі дозволяє створювати елементи проектування, які можна реплікувати для всієї мережі. Реплікація забезпечує простий спосіб масштабування мережі, а також послідовний метод розгортання. У плоских або сітчастих мережевих архітектурах зміни, як правило, впливають на велику кількість систем, а

ієрархічне проектування допомагає обмежити експлуатаційні зміни підмножини мережі, що також спрощує управління та підвищує стійкість. Модульне структурування мережі на невеликі, легкі для розуміння елементи також сприяє стійкості за рахунок поліпшеної ізоляції несправностей. Ієрархічний дизайн LAN включає наступні три рівні:

- рівень доступу — надання кінцевим точкам і користувачам прямого доступу до мережі;
- рівень розподілення — згрупує рівні доступу і забезпечує підключення до служб;
- рівень ядра — забезпечує зв'язок між рівнями розподілу для великих локальних мереж.

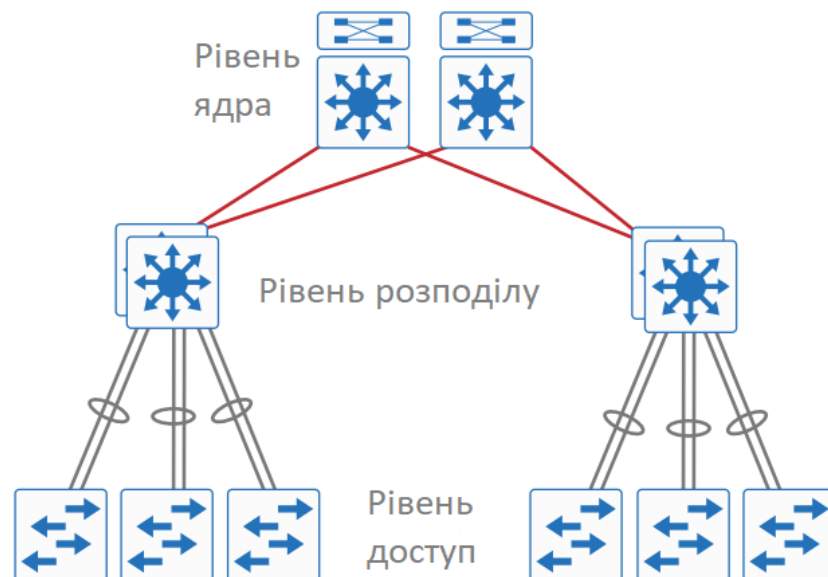


Рис. 1.1. Ієрархічний дизайн LAN

Кожен рівень (доступу, розподілу і ядра) надає різні функціональні та мережні можливості. Залежно від характеристик місця установки, може знадобитися один, два або всі три рівня. Наприклад, ділянка, що займає одну будівлю, може мати тільки рівні доступу і розподілу, в той час як підприємство, що складається з декількох будівель, швидше за все, матиме всі три рівні.

Незалежно від того, скільки рівнів реалізовано на місці, модульність цієї конструкції гарантує, що кожен з рівнів буде надавати ті ж послуги, при будь-

якому масштабуванні. Також це означає, що в цій архітектурі будуть використовуватися ті ж методи проектування.

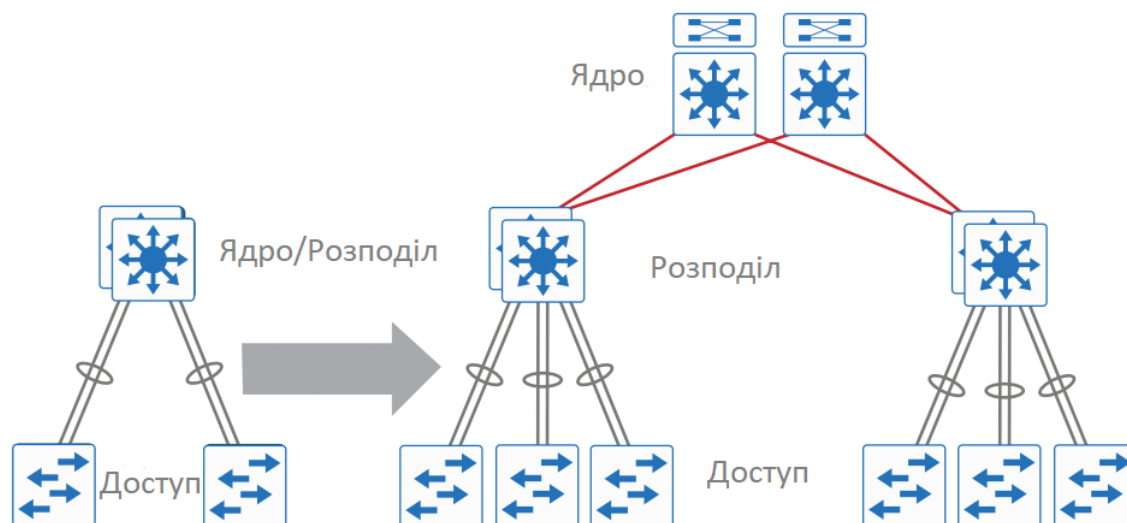


Рис. 1.2. Масштабованість за допомогою модульної конструкції

Рівень доступу — це рівень, на якому керовані користувачем пристрої і інші кінцеві пристрої є підключені до мережі. Рівень доступу забезпечує як провідне, так і бездротове підключення. Він містить функції і послуги, що забезпечують безпеку і відмовостійкість всієї підмережі.

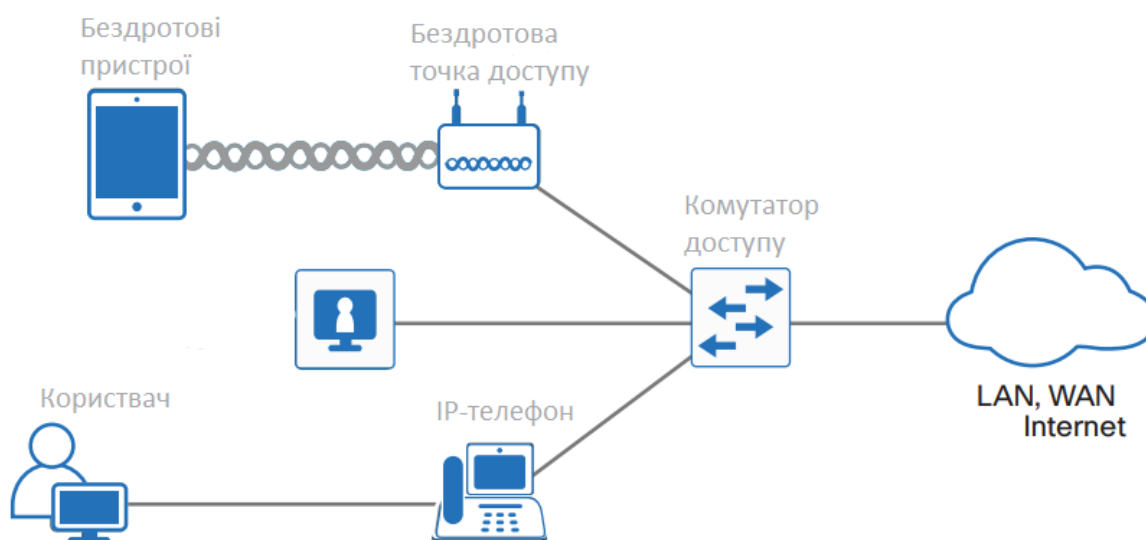


Рис. 1.3. Підключення рівня доступу

Підключення пристроїв — рівень доступу забезпечує підключення пристроїв з високою пропускнуою здатністю. Щоб зробити мережу прозорою частиною повсякденної роботи кінцевого користувача, рівень доступу повинен

підтримувати різке зростання високошвидкісного трафіку, коли користувачі будуть виконувати рутинні завдання, такі як відправка великих електронних листів або відкриття файлу з внутрішньої веб-сторінки.

Оскільки багато типів кінцевих пристроїв підключаються на рівні доступу: персональні комп'ютери, IP-телефони, бездротові точки доступу і IP-камери відеоспостереження — рівень доступу може підтримувати безліч логічних мереж, забезпечуючи переваги для продуктивності, менеджменту і безпеки.

Одною з переваг є послуги із забезпечення стійкості і безпеки. Так дизайн рівня доступу повинен забезпечувати доступність мережі для всіх користувачів, яким це потрібно і коли їм це потрібно. В якості точки з'єднання між мережею та клієнтськими пристроями рівень доступу повинен допомагати захищати мережу від людських помилок і від атак. Цей захист включає в себе забезпечення того, щоб користувачі мали доступ тільки до авторизованих служб, не дозволяючи кінцевим призначеним для користувача пристроїв брати на себе роль інших пристроїв в мережі, і коли це можливо, перевірку того, що кожен кінцевий пристрій користувача є дозволений в мережі.

Ще одною перевагою є розширені технологічні можливості. Так рівень доступу забезпечує набір мережевих послуг, що підтримують передові технології, такі як голос і відео. Рівень доступу повинен забезпечувати спеціалізований доступ для пристроїв з використанням передових технологій. Це потрібно для того, щоб трафік від цих пристроїв не постраждав від трафіку інших пристроїв, а також для забезпечення ефективної доставки трафіку, який необхідний багатьом пристроям в мережі.

Рівень розподілу підтримує багато важливих сервісів. У мережі, де з'єднання повинно перетинатись наскрізною локальною мережею, як між різними пристроями рівня доступу, так і між пристроями рівня глобальної мережі, рівень розподілу має функцію полегшення цього зв'язку.

Масштабованість на будь-якому підприємстві завжди відігравала важливу роль. З'єднання між собою більш ніж двох-трьох пристроїв рівня доступу

вважається недоцільним. Рівень розподілу служить в якості точки агрегації для декількох комутаторів рівня доступу.

Рівень розподілу може знизити експлуатаційні витрати, роблячи мережу ефективнішою, вимагаючи меншої кількості пам'яті, шляхом створення доменів відмов, які поділяють відмови або зміни в мережі, а також шляхом обробки ресурсів для пристроїв в інших місцях мережі. Рівень розподілу також збільшує доступність мережі за рахунок того, що збої, що можуть відбуватись, не зачіпають всю мережу, а відбуваються в менших доменах.

Не менш важливим є зменшення складності і підвищення відмовостійкості. Дротова LAN має можливість використовувати спрощений рівень розподілу, в якому вузол рівня розподілу складається з однієї логічної сутності, яку можна реалізувати використовуючи пару фізично окремих комутаторів, які працюють як один пристрій або за допомогою фізичного стека комутаторів які також працюють як один пристрій. Стійкість забезпечується фізично надлишковими компонентами, такими як джерела живлення, супервізори, модулі, а також перемикання на резервні логічні площини управління з контролем стану.

Такий підхід знижує складність налаштування та експлуатації рівня розподілу, оскільки потрібна менша кількість протоколів для коректної роботи мережі. Незначне налаштування або його відсутність необхідні для забезпечення конвергенції в діапазоні близько секунди або навіть суб-секунди навколо невдачі або збою.

У великих локальних мережах часто виникає необхідність мати кілька комутаторів розподільного рівня. Одна з причин цього полягає в тому, що коли комутатори рівня доступу розташовані в декількох географічно розкиданих будівлях, ви можете заощадити потенційно дорогі оптоволоконні маршрути між будівлями, розташувавши комутатор рівня розподілу в кожному з цих будинків.

У міру того, як мережі ростуть за межі трьох рівнів розподілу в одному місці, організації повинні використовувати основний рівень для оптимізації конструкції. Ще однією причиною використання декількох комутаторів рівня

розподілу є те, що кількість комутаторів рівня доступу, що підключаються до одного рівня розподілу, перевищує мету продуктивності, поставлену проектувальником мережі. В модульній, так як і в масштабованій конструкції можна розмістити рівні розподілу для центрів обробки даних, WAN-зв'язку або служб Інтернету.

Рівень розподілу забезпечує підключення до мережних служб, до WAN і до периметру Інтернету. Мережеві послуги можуть включати в себе і не обмежуватися службами широкосмтових додатків (WAAS) і контролерами WLAN. Залежно від розміру локальної мережі, ці служби і підключення до периметру WAN і Інтернету можуть розташовуватися на комутаторі рівня розподілу, який також об'єднує підключення рівня доступу до локальної мережі.

При проектуванні великих локальних мереж потрібно мати виділений рівень розподілу для мережевих послуг на відміну від спільного використання з'єднань з пристроями рівня доступу. У міру зростання щільності маршрутизаторів WAN, контролерів WAAS, периферійних пристроїв Інтернету і контролерів WLAN стає все важче управляти можливістю підключення до одного комутатора рівня розподілу. При з'єднанні трьох дистрибутивів разом, слід враховувати використання основного рівня для з'єднання дистрибутивів.

Існує ряд факторів, які визначають конструкцію локальної мережі з декількома модулями розподільного рівня:

- кількість портів і пропускна здатність портів, яку може забезпечити платформа рівня розподілу, впливають на продуктивність і пропускну здатність мережі;
- стійкість мережі є фактором, коли всі локальні мережі та мережеві сервіси покладаються на одну платформу, незалежно від цієї платформи, вона може представляти єдину точку збою або неприпустимо великий домен збою;
- управління змінами і частота впливають на стійкість. Коли всі LAN, WAN і інші мережеві служби об'єднані на одному рівні розподілу, експлуатаційні або конфігураційні помилки можуть вплинути на роботу всієї мережі.

– географічна розпорошеність комутаторів доступу до LAN по багатьом будівлям на більшому підприємстві вимагала б більшої кількості оптоволоконних з'єднань до одного зруйнованого ядра.

Як і рівень доступу, рівень розподілу також забезпечує якість обслуговування (QoS) для потоків додатків, щоб гарантувати роботу критично важливих додатків і мультимедійних додатків відповідно до плану.

## 1.2. Основні принципи побудови глобальних мереж підприємств

ІТ-інфраструктура сучасної організації в багатьох випадках передбачає з'єднання і взаємодію різних, в тому числі віддалених один від одного, локальних мереж (LAN). Дистанційні локальні мережі з'єднуються між собою за допомогою глобальних мереж (WAN). Глобальна мережа може обслуговувати місто, країну або регіон світу. Глобальна мережа належить оператору зв'язку і компанія вносить плату за використання мережевих сервісів WAN, що надаються оператором.

Сучасна WAN розпочала свою діяльність у 1969 р. розгортанням ARPANET, який був попередником сьогоdnішнього Інтернету. Технологія, що використовується для побудови Інтернету, почала комерціалізуватися на початку 1970-х років з розвитком мереж з комутацією пакетів на основі X.25.

Окрім цього тривала еволюція Інтернету, яка розпочалась з 1980-х років, спричинила розгортання чотирьох різних поколінь технологій WAN підприємств. Наприклад, в середині-кінці 1980-х для корпоративних ІТ-організацій стало звичним впроваджувати інтегровані WAN на базі TDM, щоб здійснювати як голосовий, так і трафік даних. На початку 1990-х ІТ-організації почали впроваджувати WAN на основі Frame Relay. У середині-кінці 1990-х деякі ІТ-організації замінили свої WAN на основі Frame Relay на WAN, засновані на технології ATM (Asynchronous Transfer Mode). У 2000-х роках багато ІТ-організацій замінили свої Frame Relay або ATM на WAN, засновані на MPLS.

Економія витрат була основним фактором, який спричинив впровадження кожного з чотирьох поколінь технологій WAN. Для багатьох мережевих фахівців термін WAN не відноситься до Інтернету, а стосується виключно надавання послуг WAN, такі як Frame Relay, ATM або MPLS. Відмінність полягає в тому, що послуги WAN підприємства були розроблені головним чином для підключення філій даного підприємства та центрів обробки даних, тоді як Інтернет забезпечує підключення до величезного кола ресурсів з безліччю користувачів.

Існує кілька варіантів підключення для отримання доступу до глобальної мережі, які інтернет-провайдери можуть використовувати для підключення місцевої мережі до підприємства. Ці варіанти доступу до глобальної мережі розрізняються за технологією, швидкістю і вартістю. Кожен з них має свої переваги і недоліки. Знайомство з цими технологіями є важливим етапом проектування мережі.

Як показано на рис. 1.3, доступ WAN в організації можна налагодити двома способами:

- Інфраструктура приватних глобальних мереж. Інтернет-провайдери можуть пропонувати виділені канали «точка-точка», з'єднання з комутацією каналів, наприклад ТМЗК або ISDN, і канали з комутацією пакетів, такі як WAN на основі Ethernet, ATM і Frame Relay.

- Загальнодоступна інфраструктура WAN. Оператори зв'язку забезпечують широкосмуговий доступ до Інтернету на основі цифрової абонентської лінії, систем кабельного та супутникового доступу. Широкосмугові варіанти підключення зазвичай використовуються для підключення невеликих офісів і працюють у віддаленому режимі співробітників до корпоративного вузла через Інтернет. Дані, що передаються між корпоративними вузлами по загальнодоступній глобальній мережі, повинні бути захищені з використанням VPN.

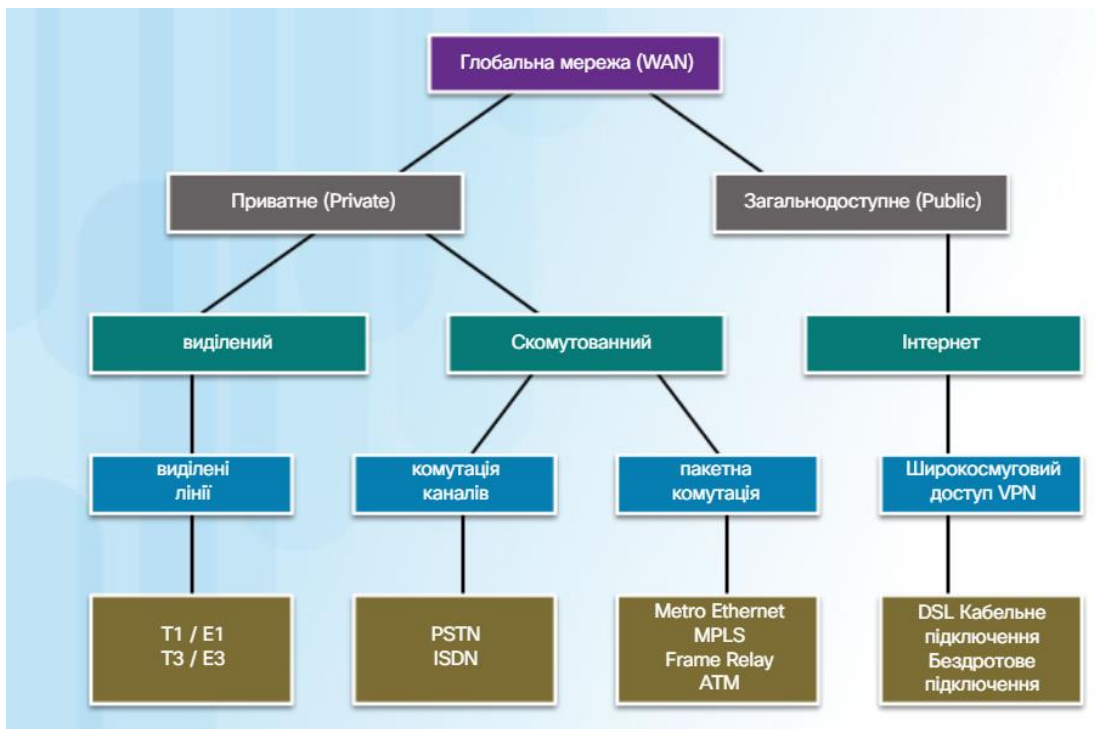


Рис. 1.3. Варіанти доступу до глобальної мережі WAN

Якщо потрібні постійні виділені підключення, канал «точка-точка» використовується для надання встановленого каналу зв'язку глобальної мережі, що йде від приміщення замовника до мережі оператора зв'язку. Канали «точка-точка», як правило, орендуються у оператора зв'язку і називається також орендованими лініями.

Орендовані лінії існують з початку 50-х рр. минулого століття, і з цієї причини для них використовуються різні назви, такі як орендований кабель, виділена лінія, послідовний канал, послідовна лінія, канал «точка-точка» або канали T1/E1 і T3/E3. Термін «оренована лінія» підкреслює той факт, що організація щомісяця платить інтернет-провайдеру за використання лінії. Орендовані лінії доступні в різних модифікаціях. Як правило, їх вартість залежить від необхідної пропускної спроможності і відстані між підключеними точками.

У Північній Америці інтернет-провайдери використовують систему T-каналів для визначення можливості передачі цифрових сигналів по послідовних каналах в мідних кабельних лініях, тоді як в Європі використовують систему E-каналів (див. рис. 1.4). Канал T1, наприклад, підтримує швидкість 1,544 Мбіт / с,

канал E1 — 2,048 Мбіт / с, T3 — 43,7 Мбіт / с, а E3 — 34,368 Мбіт / с. Для визначення швидкості передачі даних в опто-волоконній середовищі використовується набір специфікацій, званих оптичною несучою (OC).

Переваги орендованих ліній:

- простота. Установка і технічне обслуговування каналів зв'язку типу «точка-точка» вимагають мінімального досвіду;

- якість. Якщо канали зв'язку типу «точка-точка» мають необхідної пропускною спроможністю, вони зазвичай забезпечують високу якість обслуговування. Виділена пропускна здатність позбавляє від затримок і спотворень при передачі даних між кінцевими точками;

- доступність. Постійна доступність є суттєвою для деяких додатків, наприклад для електронної торгівлі. Канали зв'язку типу «точка-точка» забезпечують постійну виділену лінію, необхідну для VoIP або передачі відео по протоколу IP.

Недоліки орендованих ліній:

- вартість. Як правило, канали «точка-точка» характеризуються найвищою вартістю доступу до мережі WAN. Вартість рішень з використанням орендованих ліній може стати значною при їх використанні для підключення безлічі майданчиків, які знаходяться на великих відстанях. Крім того, для кожного кінцевого пристрою необхідний інтерфейс маршрутизатора, що збільшує вартість обладнання;

- обмежена гнучкість. Трафік WAN мінливий, а орендовані лінії мають фіксовану пропускну здатність, тому пропускна здатність лінії часто буває недостатньою. Для внесення будь-яких змін в орендовану лінію потрібно, як правило, здійснюється візит об'єкту персоналом інтернет-провайдера, щоб налаштувати пропускну здатність.



Рис. 1.4. Варіанти доступу до глобальної мережі WAN

Що ж до тих технологій, які є більш новими відносно попередніх, то слід згадати цифрову мережу з інтеграцією служб (ISDN). Дана технологія є технологією комутації каналів, яка дозволяє місцевій лінії мережі ТМЗК передавати цифрові сигнали, що призводить до підвищення пропускної спроможності комутованих підключень.

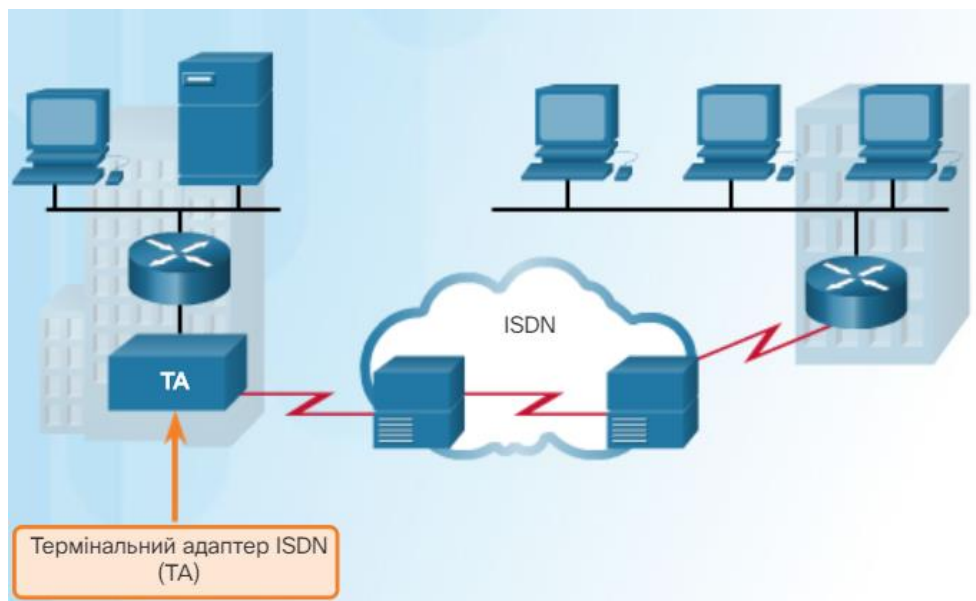


Рис. 1.5. Периметр топології ISDN

ISDN змінює внутрішні підключення ТМЗК таким чином, що крім передачі аналогових сигналів вони передають також мультимплексовані цифрові сигнали з поділом за часом (TDM). Технологія TDM дозволяє передавати по підканалах одного каналу зв'язку два або кілька сигналів, або бітових потоків.

Здається, що сигнали передаються одночасно, але фізично вони надходять в канал по черзі.

Для підключення ISDN може знадобитися термінальний адаптер (ТА), що представляє собою пристрій, що використовується для підключення інтерфейсу ISDN з базовою швидкістю (BRI) до маршрутизатора (див. рис. 1.5).

Існують два типи інтерфейсів ISDN:

– Інтерфейс основного доступу (BRI). Інтерфейс ISDN BRI призначений для будинків чи невеликих корпоративних мереж. Цей інтерфейс забезпечує два несучих канали (B) з пропускнуною спроможністю 64 Кбіт / с для передачі голосу і даних, а також один дельта-канал (D) з пропускнуною спроможністю 16 Кбіт / с для передачі службових сигналів, встановлення з'єднань та інших потреб. Часто канал D інтерфейсу основного доступу використовується не повністю, оскільки у нього для моніторингу є тільки два канали B.

– Інтерфейс з первинної швидкістю (PRI). Так само для великих підприємств доступна технологія ISDN. У Північній Америці інтерфейс PRI забезпечує 23 канала B зі швидкістю 64 Кбіт / с і один канал D зі швидкістю 64 Кбіт / с при загальній швидкості передачі даних до 1,544 Мбіт / с. Сюди включені деякі додаткові накладні витрати по синхронізації. В Європі, Австралії та інших частинах світу інтерфейс PRI забезпечує 30 каналів B і один канал D, загальна швидкість передачі даних досягає 2,048 Мбіт / с, включаючи накладні витрати по синхронізації.

Інтерфейс BRI має час встановлення виклику менше секунди, а канал B (64 Кбіт / с) забезпечує більш високу пропускну здатність, ніж канал аналогового модему. Якщо потрібна більш висока пропускну здатність, то можна активувати другий канал B для забезпечення загальної швидкості 128 Кбіт / с. Це дозволяє одночасно організувати кілька голосових з'єднань, голосовий зв'язок і передачу даних або відео-конференц-зв'язок. В останньому випадку один канал використовується для передачі голосу, другий — для передачі відео.

Інше поширене застосування технології ISDN полягає в наданні, в міру необхідності, додаткової ємності каналів для підключення по виділеній лінії.

Характеристики виділеної лінії визначаються виходячи з середнього рівня навантаження, а в періоди пікового навантаження додається ISDN. ISDN використовується також як резерв на випадок відмови виділеної лінії. Тарифи ISDN визначаються на основі вартості використання одного каналу В і схожі з тарифами на аналогові підключення голосового зв'язку.

При використанні PRI ISDN можна встановити кілька каналів В між двома кінцевими точками. Це дозволяє проводити відеоконференції і підтримувати з'єднання з високою пропускну здатністю без затримок і розсинхронізації. Однак множинні підключення при великих відстанях можуть виявитися дуже дорогими.

Прабатьком попередньої технології можна вважати Frame Relay. Це проста WAN-технологія множинного доступу без широкомовного розсилання (NBMA) рівня 2, що застосовується для з'єднання корпоративних локальних мереж. При використанні каналів PVC один інтерфейс маршрутизатора можна використовувати для підключення до декількох філій. Канали PVC використовуються для передачі як голосового трафіку, так і трафіку даних між джерелом і пунктом призначення, і підтримки швидкості передачі даних до 4 Мбіт / с, причому деякі провайдери пропонують навіть більш високі швидкості.

Граничному маршрутизатору потрібен тільки один інтерфейс, навіть якщо використовуються кілька віртуальних каналів (VC). Орендована лінія, поєднана з периметром мережі Frame Relay, дозволяє організувати недорогий зв'язок між локальними мережами, що знаходяться на великій відстані один від одного.

Frame Relay створює канали PVC, які однозначно визначаються ідентифікатором каналу передачі даних (DLCI). Канали PVC і DLCI забезпечують двосторонній зв'язок між пристроями DTE.

Продовжила розвиток технологія асинхронного режиму передачі (ATM), що здатна забезпечити передачу голосу, відео і даних по приватним мережам та мережам загального доступу. Вона створена на основі комірчастої, а не кадрової архітектури. Осередки ATM завжди мають фіксовану довжину в 53 байта. Осередок ATM містить 5-байтовий заголовок, за яким слідує 48 байтів

|  |  |  |  |  |                          |    |
|--|--|--|--|--|--------------------------|----|
|  |  |  |  |  | КІК.КР.Б – 123 – 20 – ПЗ |    |
|  |  |  |  |  |                          |    |
|  |  |  |  |  |                          | 22 |

корисного навантаження АТМ. Невеликі осередки фіксованої довжини зручні для перенесення голосового і відео трафіку, оскільки цей тип трафіку вкрай залежить від затримок. В цьому випадку при передачі відео і голосового трафіку немає необхідності в очікуванні передачі більших пакетів даних.

53-байтовий осередок АТМ менш економний, ніж кадри і пакети більшого розміру в Frame Relay. До того ж, в осередку АТМ на кожні 48 байтів корисної частини припадає 5 байтів службової інформації. Якщо в осередку переносяться сегментовані пакети мережевого рівня, то заголовок збільшується, так як комутатору АТМ необхідно повторно збирати пакети в місці призначення. Смуга пропускання типового каналу АТМ повинна бути принаймні на 20% більше Frame Relay для перенесення такого ж обсягу даних мережевого рівня.

Режим передачі АТМ розроблений як виключно масштабований і здатний підтримувати швидкості каналів T1 / E1 на рівні OC-12 (622 Мбіт / с) і більш високої швидкості.

Крім того, АТМ підтримує як канали PVC, так і канали SVC, хоча в глобальних мережах частіше використовуються канали PVC. Як і інші технології обміну такими даними, АТМ допускає використання декількох каналів VC для одного підключення до периметру мережі по орендованій лінії.

Важливою для розуміння також є технологія Ethernet. Спочатку вона була розроблена в якості технології доступу в мережах LAN. Вона була непридатна для використання технології WAN на перших етапах розвитку, оскільки допустима довжина кабелю була обмежена одним кілометром. Однак з часом з'явилися нові стандарти Ethernet на основі оптоволоконного кабелю, що цілком підходять для мереж WAN. Зокрема, стандарти IEEE 1000BASE-LX і IEEE 1000BASE-ZX передбачають підтримку оптоволоконних кабелів довжиною до 5 і 70 км відповідно.

В даний час постачальники послуг пропонують сервіс WAN на основі Ethernet з підключенням по оптоволоконному кабелю. Сервіс WAN на основі Ethernet може виступати під різними назвами, включаючи такі, як Metropolitan

Ethernet (METROE), Ethernet over MPLS (EoMPLS) і Virtual Private LAN Service (VPLS).

До переваги мереж WAN на базі Ethernet слід віднести:

– Зниження витрат і обсягу адміністрування. WAN на основі Ethernet забезпечує створення комутованої мережі 2 рівня з високою пропускну здатністю, здатної управляти передачею даних, голосу і відео в рамках однієї і тієї ж інфраструктури. Ця особливість дозволяє підвищити пропускну здатність і усуває потребу в дорогих перетвореннях, необхідних для використання інших технологій глобальної мережі. Таким чином, компанії отримують в своє розпорядження недорогу технологію для забезпечення доступу в Інтернет і організації зв'язку між різними об'єктами в межах міста.

– Простота інтеграції з існуючими мережами. WAN на основі Ethernet легко підключити до існуючих мереж LAN на основі Ethernet без великих витрат фінансів і часу.

– Підвищення продуктивності бізнесу. Застосування технології WAN на основі Ethernet дозволяє використовувати додатки IP, що підвищують продуктивність, які складно впровадити в мережах TDM або Frame Relay, наприклад зв'язок по IP, VoIP і потокове відео.

– Конфігурація, при якій віддалені працівники або офіси отримують доступ до корпоративної мережі WAN через широкосмугове інтернет-з'єднання, передбачає певні ризики безпеки. Для вирішення цієї проблеми можна використовувати VPN-з'єднання з мережевим пристроєм, який підтримує VPN і зазвичай знаходиться в межах корпоративного об'єкту.

VPN є шифрованим підключенням між приватними мережами за допомогою загальнодоступної мережі, наприклад Інтернету. Замість використання виділеного підключення на 2 рівні, наприклад виділеної лінії, в VPN використовуються віртуальні підключення, звані тунелями VPN, які прокладаються через Інтернет з приватної мережі компанії до віддаленого вузла або комп'ютера співробітника.

Як показано на рис. 1.6, в мережі VPN застосовуються віртуальні підключення, які проходять від приватної мережі організації через Інтернет до віддаленого вузла або комп'ютера співробітника. Інформація, що надходить з приватної мережі, передається в захищеному режимі по публічній мережі, що дозволяє створити віртуальну мережу.

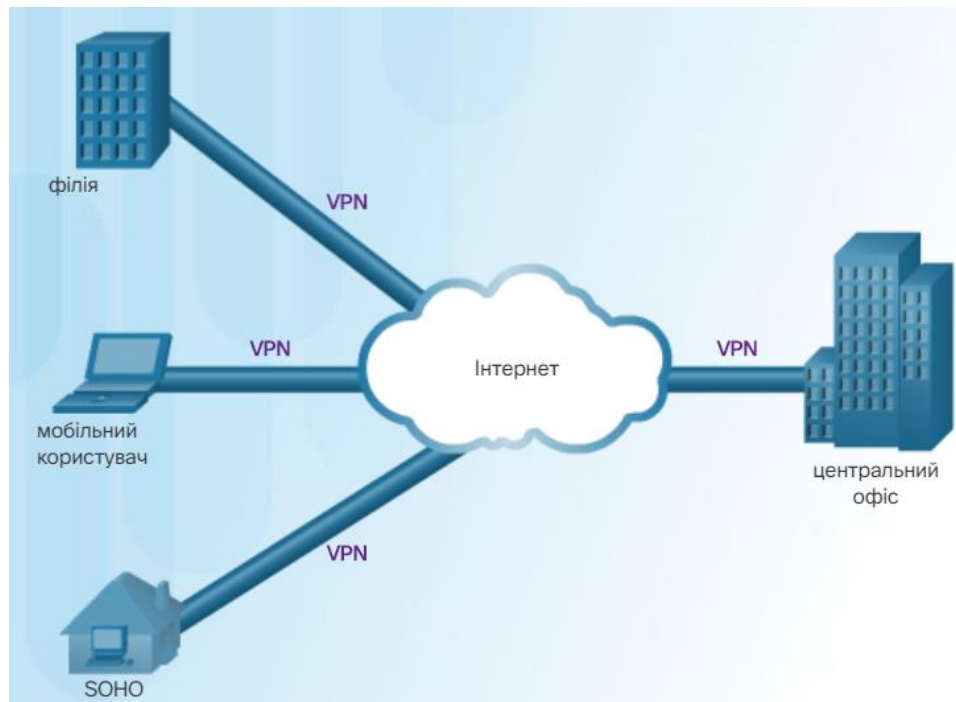


Рис. 1.6. Інтернет-підключення мережі VPN

Нижче вказані переваги мережі VPN:

1) Скорочення витрат - мережі VPN дозволяють організаціям використовувати надану сторонніми компаніями недороге транспортне середовище Інтернету для підключення віддалених офісів і користувачів до основного вузла, тобто відмовитися від застосування дорогих виділених каналів WAN і банків модемів. Крім того, завдяки появі недорогих технологій, що забезпечують високу пропускну здатність (наприклад DSL), організації можуть використовувати мережі VPN для скорочення своїх витрат на організацію зв'язку при одночасному підвищенні рівня пропускну здатності віддалених підключень.

2) Масштабованість - завдяки мережам VPN організації можуть використовувати інфраструктуру Інтернету в межах інтернет-провайдерів і пристроїв, що дозволяють спростити процедуру додавання нових користувачів.

Тому організації можуть серйозно нарощувати пропускну здатність без внесення суттєвих змін до інфраструктури.

3) Сумісність з широкосмуговою технологією - завдяки мережам VPN мобільні і віддалені співробітники можуть ефективно використовувати високошвидкісний широкосмуговий зв'язок, наприклад DSL і кабельні канали, для доступу до мереж своїх організацій. Широкосмуговий зв'язок забезпечує високу гнучкість і ефективність. Високошвидкісні широкосмугові підключення також дозволяють створювати економічні рішення для підключення віддалених офісів.

4) Безпека - мережі VPN можуть підтримувати різні механізми захисту, що забезпечують найвищий рівень безпеки, завдяки застосуванню складних протоколів шифрування і аутентифікації, що дозволяють захищати дані від несанкціонованого доступу.

Організаціям потрібні безпечні, надійні і недорогі способи з'єднання між собою декількох мереж, які дозволять підключати філії і постачальників до мережі головного офісу корпорації. Крім того, з урахуванням збільшення кількості віддалених співробітників підприємствам все частіше потрібні безпечні, надійні та економічні рішення для підключення співробітників, що працюють в секторі SOHO (Small Office / Home Office - малий офіс / домашній офіс), а також в інших віддалених місцях розташування, до ресурсів корпоративних вузлів.

За допомогою з'єднань VPN організації встановлюють двоточкові приватні мережеві з'єднання через сторонні мережі, в тому числі через Інтернет. Тунель усуває бар'єр, пов'язаний з відстанню, і дозволяє віддаленим користувачам отримувати доступ до мережевих ресурсів на центральному вузлі. VPN є приватною мережею, яка створюється за допомогою тунелювання в публічній мережі (як правило, в Інтернеті). VPN – це середовище передачі даних із суворим контролем доступу, що дозволяє встановлювати рівноправні підключення в межах певної цільової спільноти.

Перші мережі VPN представляли собою звичайні IP-тунелі, в яких перевірка справжності або шифрування даних не виконувалися. Наприклад, розроблений в Cisco протокол тунелювання GRE забезпечує інкапсуляцію широкого кола пакетів мережевого рівня в IP-тунелях, однак протокол GRE не підтримує шифрування. Завдяки цьому створюється віртуальний канал «точка-точка» до маршрутизаторів Cisco в віддалених точках поверх IP-мережі.

В даний час під віртуальними приватними мережами зазвичай розуміють захищену реалізацію мережі VPN з шифруванням (наприклад IPsec VPN).

Для реалізації мереж VPN необхідний шлюз VPN. Шлюзом VPN може бути маршрутизатор, міжмережевий екран або пристрій адаптивної захисту Cisco ASA (Adaptive Security Appliance). ASA – це автономний міжмережевий екран, який об'єднує в межах одного образу програмного забезпечення функції брандмауера, концентратора VPN, а також системи запобігання вторгнень.

Існують два типи доступу по VPN:

1) Мережі VPN типу «вузол-вузол». Такі VPN служать для підключення один до одного цілих мереж. Наприклад, з їх допомогою мережа філії може підключатися до мережі головного офісу компанії. Кожен вузол оснащений шлюзом VPN, таким як маршрутизатор, міжмережевий екран, концентратор VPN або пристрій захисту.

2) Мережі VPN для віддаленого доступу (remote access). Ці мережі забезпечують захищений доступ до мережі компанії через Інтернет з окремих вузлів, якими користуються віддалені співробітники, мобільні користувачі і клієнти в екстранеті. Зазвичай на кожному вузлі (віддалений працівник 1 і віддалений працівник 2) завантажено клієнтське ПЗ або використовується веб-клієнт.

### 1.3. Гетерогенні мережі. Компоненти гетерогенних мереж

Гетерогенна мережа (ГМ) являє собою мережу підключення комп'ютерів і інших пристроїв з різними операційними системами і / або протоколів.

Наприклад, локальні обчислювальні мережі (ЛОМ), які з'єднують Microsoft Windows і Linux на базі персональних комп'ютерів з Apple, Macintosh комп'ютери є гетерогенними. Словосполучення «гетерогенна мережа» також використовується в бездротових мережах з використанням різних технологій доступу. Наприклад, бездротова мережа, яка надає послуги через бездротову локальну мережу і може підтримувати послугу при перемиканні в стільникову мережу, називається бездротовою ГМ.

Згадка про ГМ часто вказує на використання декількох типів вузлів доступу в бездротовій мережі. Широка мережа може використовувати макросоти, пікосоти і / або фемтосоти, щоб запропонувати зону покриття бездротової мережі в середовищі з великою різноманітністю зон бездротового покриття, починаючи від відкритого зовнішнього середовища для офісних будівель, житлових будинків, закінчуючи підземними ходами. Мобільні фахівці визначають ГМ як мережу зі складною інтеперабельністю між макросотами, малими сотами, а в деяких випадках – і елементами Wi-Fi мережі, що використовуються разом, щоб забезпечити мозаїку покриття, з можливістю перемикання каналів зв'язку між мережевими елементами.

ГМ повинна мати можливість автоматизувати реконфігурації його роботи для забезпечення гарантованої якості обслуговування по всій мережі. Також вона має бути досить гнучкою, щоб передбачити зміни потреб користувачів, бізнес-цілей і абонентської поведінки. В рамках цієї самооптимізації мережі функціональність (SON) має важливе значення. Отже, в розширенні можливості SON потрібно буде враховувати зростаючі потреби користувачів, бізнес-цілей і абонентські поведінки. Важливо відзначити, що функції, пов'язані з операціями ГМ і управліннями приймають раніше можливості SON, які, можливо, були направлені лише на один домен і / або технології, а також розширити його для забезпечення автоматизованого управління якістю обслуговування по всій ГМ.

Бездротова ГМ (HWN) є окремим випадком ГМ. У той час як ГМ може складатися з мережі комп'ютерів або пристроїв з різними можливостями з точки зору операційних систем, апаратних засобів, протоколів і т.д., HWN представляє

собою бездротову мережу, яка складається з пристроїв, що використовують іншу основну технологію радіодоступу – RAT.

Є кілька проблем ще належить вирішити в бездротових ГМ, такі як:

- визначення теоретичного потенціалу HWNs;
- взаємодія технологій;
- мобільність;
- якість обслуговування;
- перешкоди між RAT.

У HWN є кілька переваг, на відміну від традиційної однорідної бездротової мережі, включаючи підвищення надійності, поліпшення ефективності використання спектра і збільшення охоплення. Підвищено надійність, тому що коли один конкретний RAT в межах HWN зазнає невдачі, він все ще може підтримувати з'єднання, відступаючи до іншого RAT. Ефективність використання спектра підвищується за рахунок використання RAT, які можуть мати кілька користувачів за рахунок використання балансування навантаження. Через RAT якість покриття може бути поліпшена, так як різні RAT можуть заповнити «дірки» в охопленні, які б будь-яка з одних тільки окремих мереж, не змогла б заповнити.

Більшість процвітаючих організацій вже активно використовують в роботі бездротові мережі Wi-Fi. З мережею даного типу є можливим вільне пересування по офісах, не втрачаючи якісного інтернет-зв'язок.

#### *Розвиток бездротових мереж*

Своїм бурхливим розвитком бездротові мережі в значній мірі зобов'язані компанії Intel, яка на початку 2000-х років зробила наявність бездротового адаптера обов'язковим для ноутбуків, що претендують на популярний логотип Intel® Centrino™. З тих пір пройшло багато часу, а в розвиток бездротових мереж Wi-Fi було вкладено величезну кількість сил і засобів.

На зміну першому стандарту 802.11b (в США ще використовувався стандарт 802.11a, але він працював на 5 ГГц, у нас в країні не працював, тому що тоді ця частота вимагала ліцензування, і т.д.), що забезпечує відносно невелику

швидкість до 11 Мбіт / сек, прийшов більш швидкісний стандарт «g» (54 Мбіт / с), а потім - «n» (150/300/600 Мбіт / с). Тут, до речі, можна відзначити цікаву річ: виробники настільки чекали новий стандарт, який пропонував більш високі швидкості обміну даними, що стали випускати пристрої з його підтримкою ще до офіційного анонсу, на чорновій специфікації N-draft. Далі ця ситуація повторилася з новим стандартом «802.11ac». Іноді деякі пристрої на «чорнових» специфікаціях відмовлялися працювати один з одним (наприклад, конкретний роутер і конкретний ноутбук), що могло стати неприємним сюрпризом.

*Бездротові мережі сьогодні: швидкості, стандарти та ін.*

Отже, на сьогодні існує два основні стандарти бездротового підключення Wi-Fi:

- IEEE 802.11n з максимальною пропускнуою здатністю від 150 до 600 Мбіт / с при використанні чотирьох антен. Стандарт передбачає бездротові мережі 2,4 ГГц і 5 ГГц;

- IEEE 802.11ac з максимальною пропускнуою спроможністю до 6,77 Гбіт / с при використанні восьми антен. Даний стандарт призначений тільки для 5 ГГц мереж.

Стандарт IEEE 802.11g з пропускнуою спроможністю 54 Мбіт / с зараз можна зустріти тільки в старих пристроях, але підтримка його в пристроях є.

Сьогодні на ринку присутній широкий вибір різного устаткування, що підтримує найсучасніші стандарти. Однак варто зазначити, що в бездротових мережах куди більше різних варіантів. Забезпечення швидкості передачі даних залежить від дуже багатьох параметрів: підтримуваних стандартів зв'язку, кількості антен і роботи MIMO, кількості антен і навіть фізичного розташування в просторі.

Загалом, за формальними показниками швидкості з'єднання бездротові мережі наздоганяють, а інколи навіть обганяють провідні. Але для них при цьому існує дуже багато застережень, через які в реальності все не так райдужно.

*Плюси бездротових мереж*

Основний плюс бездротової мережі – свобода. Співробітник може підключити і повноцінно працювати з ресурсами компанії з будь-якого місця, де можна встановити з'єднання з сигналом точки доступу. Ця відстань може досягати 30-50 м при хороших умовах зв'язку. Відповідно, працівник не прив'язаний до робочого місця і може працювати з різних пристроїв (як ПК, так і мобільних). Бездротове підключення сильно покращує зручність роботи при великій кількості нарад в окремих кімнатах, якщо співробітники працюють в робочих групах, які часто переміщуються, і т.д.

До речі, не варто забувати про те, що бездротовий зв'язок може працювати не тільки як засіб доступу до мережі, але і для доступу до обладнання – наприклад, технології Intel® Wireless Docking™ і Intel® WiDi™ дозволяють підключатися до настільної периферії (клавіатура, миша та ін.) без проводів, а також проводити презентації на зовнішньому моніторі без підключення проводом.

У разі, якщо в офісі вже розгорнута бездротова інфраструктура, то підключення додаткового робочого місця не вимагає практично ніяких додаткових витрат. Однак, не слід забувати, що пропускна здатність точки доступу ділиться на всіх клієнтів, тобто при великому обміні даних пропускна здатність на клієнта сильно впаде.

Аналогічну ситуацію можна спостерігати і при підключенні кінцевих пристроїв. Наприклад, поставити новий принтер або МФУ з підтримкою Wi-Fi – справа кількох хвилин. В результаті, в деяких випадках робота через Wi-Fi виявляється дешевше, особливо якщо кількість співробітників і пристроїв динамічно змінюється. Але не можна забувати, що розгортання бездротової інфраструктури теж коштує грошей (і часто витрати більше, ніж на дротову інфраструктуру). Також для забезпечення бездротової інфраструктури всеодно слід прокласти дротові з'єднання і розробити комутацію.

Для розуміння наведемо приклад мережі малого підприємства. Остання являє собою 802.3 Ethernet LAN. Кожен клієнт може підключатись до комутатора за допомогою мережевого кабелю. Комутатор є точкою, в якій клієнти

отримують доступ до мережі. Однак бездротова точка доступу також підключається до комутатора. Вона може бути використана для забезпечення бездротового з'єднання з мережею, тим самим замінюючи дротове з'єднання.

Але для повноти картини слід зазначити, що клієнти бездротових мереж мають використати свої бездротові мережеві карти для виявлення найближчих точок доступу, які рекламують свої SSID. Потім клієнти будуть намагатись пов'язати і аутентифікуватись з точкою доступу. Після аутентифікації бездротові користувачі мають доступ до мережевих ресурсів.

Потреби бездротового зв'язку в невеликій організації відрізняються від потреб у великій організації. Для великих бездротових розгортання потрібне додаткове бездротове обладнання, щоб спростити установку і управління бездротовою мережею.

#### *Бездротові точки доступу*

Точки доступу можна розділити на автономні точки доступу або точки доступу на базі контролера.

Автономні точки доступу, іноді звані важкими точками доступу, є автономними пристроями, що налаштовуються за допомогою Cisco CLI або графічного інтерфейсу GUI. Автономні точки доступу корисні в ситуаціях, коли в мережі потрібно всього пара точок доступу. В якості опції, декількома точками доступу можна керувати за допомогою бездротових доменних служб (WDS), а також за допомогою CiscoWorks Wireless LAN Solution Engine (WLSE).

Примітка: Домашній маршрутизатор є прикладом автономної точки доступу, оскільки вся конфігурація точки доступу знаходиться на пристрої.

Що ж до точок доступу на базі контролера – то це серверні пристрої, які не потребують початкової конфігурації. Cisco пропонує два рішення на базі контролерів. Точки доступу, засновані на контролерах, корисні в ситуаціях, коли в мережі потрібно багато точок доступу. У міру додавання нових точок доступу кожна точка доступу автоматично налаштовується і управляється контролером WLAN.

Деякі моделі AP можуть працювати як в автономному режимі, так і в режимі контролера.

Контролер бездротової локальної мережі (WLC) використовується в поєднанні з протоколом «легких точок» доступу (Lightweight Access Point Protocol – LWAPP) для управління спеціальними «легкими» точками доступу у великих кількостях адміністратором мережі або мережевим операційним центром. Контролер бездротової локальної мережі є частиною рівня передачі даних (Data Plane) в рамках бездротової моделі Cisco (Cisco Wireless Model). Контролер WLAN автоматично обробляє конфігурацію бездротових точок доступу.

#### Функції WLC:

1. виявлення та запобігання перешкод: регулювання потужністю радіочастотного випромінювання та призначення каналів відповідно до плану;
2. балансування навантаження: (вимкнено за замовчуванням), високошвидкісне балансування навантаження можна використовувати для підключення користувача до кількох точок доступу для кращого покриття та швидкості передачі даних;
3. виявлення та виправлення проблем покриття: можливість керувати рівнями потужності. Потужність може бути збільшена для покриття отворів або зменшена для захисту від перекриття ланок.

Контролер WLAN також використовує різні типи аутентифікації, такі як: 802.1X (Protected Extensible Authentication Protocol (PEAP), LEAP, EAP-TLS, Wi-Fi Protected Access (WPA), 802.11i (WPA2) та протокол тунелювання рівня 2 (L2TP).

Контролер бездротової мережі виконує автоматичний пошук, централізоване налаштування Wi-Fi точок доступу, оновлення програмного забезпечення підключених AP.

WLC може виступати в ролі DHCP-сервера, для автоматичного розподілу IP-адрес. Він проводить аналіз радіочастотного діапазону, регулюючи

потужність кожної точки доступу, канал, на якому вона працює, періодично оновлюючи дані про стан радіоефіру.

Контролер централізовано авторизує користувачів при підключенні до бездротової мережі. Його операційна система управляє всіма бездротовими з'єднаннями, забезпечує управління ресурсами радіо-інтерфейсів мережі (точками доступу).

Щоб забезпечити абсолютно м'який для клієнтського пристрою роумінг, клієнтський пристрій має підтримувати UCCX (Unified Contact Center Express). Це розширення Cisco, що розроблене саме для поліпшення роботи клієнтських пристроїв з мережею.

Також слід згадати про IP-телефонію. IP-телефонія в офіс – це комплект комунікаційних послуг для співробітників компанії і користувачів. Ці послуги здійснюються згідно з протоколом IP за допомогою мереж передачі даних.

Щоб організувати IP телефонію для офісу, необхідно програмне і апаратне забезпечення. Основне в ньому IP АТС – пристрій зі спеціальним ПО, яке:

- здійснює реєстрацію IP телефонів;
- розподіляє між абонентами відповідні налаштування;
- привласнює їм власні номери.

Крім того, IP АТС може забезпечувати обробку пакетів даних, які пересилаються між IP-телефонами та надавати ряд додаткових послуг по обробці викликів, недоступних для звичайної телефонії.

Найважливіший фактор на користь впровадження IP-телефонії в офісі - істотне зниження вартості на дзвінки між працівниками та клієнтами компанії. Адже часто після міжміських і міжнародних викликів власники компаній отримують рахунки з значними сумами за послуги ТМЗК. IP-телефонія - більш бюджетне рішення для зв'язку з віддаленими працівниками та клієнтами. Вона вимагає оплати тільки послуг мережевого провайдера і повністю окупується за рік при активному здійсненні міжнародних дзвінків.

Користувачі IP-телефонії набувають ряд послуг по обробці викликів:

- переадресація;

|  |  |  |  |  |                          |    |
|--|--|--|--|--|--------------------------|----|
|  |  |  |  |  | КІК.КР.Б – 123 – 20 – ПЗ |    |
|  |  |  |  |  |                          |    |
|  |  |  |  |  |                          | 34 |

- автовідповідач;
- автодозвон;
- конференція;
- утримання;
- складання розкладу викликів;
- голосова пошта;
- обмін миттєвими повідомленнями та ін.;
- закріплення номера за абонентом.

Переміщуючись з одного офісу в інший, користувачам не потрібно заново вносити зміни на новому робочому IP-телефоні. Вони можуть активувати свій колишній аккаунт на цьому пристрої, автоматично передаючи на нього відповідні налаштування.

Деякі виробники допускають інтеграцію IP-телефону, закріпленого за одним абонентом, з його персональним пристроєм – мобільним телефоном або смартфоном. А значить, користувач може отримувати доступ до корпоративної розсилки і з свого персонального акаунту, навіть перебуваючи за межами офісу.

Системні адміністратори можуть активно впроваджувати внутрішньокорпоративні політики для кожного із співробітників офісу. Зокрема, IP АТС:

- можна запрограмувати для здійснення розсилки повідомлень на офісні номери співробітників;
- ввести внутріофісну телефонну книгу;
- скласти план викликів для окремих номерів IP-телефонів;
- створити голосове меню і т.д.

Провідні виробники VoIP обладнання часто випускають рішення, в яких застосовані фірмові технології. Вони дозволяють підвищити якість переданого голосу і мінімізувати затримки при пересилці голосового трафіку. У таких випадках звук, навіть який передається через гучномовець, позбавлений сторонніх шумів, «булькання» і відлуння.

Переважна більшість сучасних IP-телефонів живиться за технологією PoE, через Ethernet-кабель. Це означає, що власникам компанії тепер не потрібно прокладати додаткову електричну проводку з новими розетками.

IP-телефонія робить можливим і відеоспілкування. Для цього призначені спеціальні відеотелефони або системи телеприсутності. Деякі IP-телефони з базовим функціоналом допускають підключення веб-камер. Це робить спілкування з віддаленим співрозмовником більш повноцінним.

Співробітники компанії можуть бути повністю впевнені в захищеній передачі даних (зокрема, голосового трафіку). Це досягається за рахунок таких потужних алгоритмів шифрування, як AES / DES / 3DES. Останній, зокрема, не має відомих нині кодів для злому.

Вона надає змогу спростити робочий процес користувачів. Користувачі IP-телефонів отримують значну перевагу, яка складається у спрощенні взаємодії з віддаленими співрозмовниками. Тепер можливе одночасне пересилання даних і здійснення дзвінків.

Просте розгортання послуг і перенастроювання IP-телефонії у віддалених офісах теж є вагомим плюсом. Тепер системним адміністраторам немає потреби виїжджати на місце розташування нового офісу, щоб розгорнути там послуги IP-телефонії. Досить просто підключитися до віртуальної приватної мережі через захищений тунель, щоб внести відповідні зміни.

Також до переваг слід віднести просте масштабування і модернізацію можливостей. Це зумовлено тим, що кількість підтримуваних IP-телефонів на одну IP АТС можна розширювати, набуваючи нових ліцензій ПО. Це гарне бюджетне рішення, яке, на додачу до всього, не займе багато часу на підключення нових пристроїв.

## РОЗДІЛ 2. ПРОЕКТ ГЕТЕРОГЕННОЇ МЕРЕЖІ

### 2.1. Проект мережі організації

В даній роботі була розглянута мережа організації, що представлена головним офісом та двома філіями. Офіси та філії подібні за будовою та складаються з робочих станцій, офісних комутаторів, принтерів, безпроводного обладнання, серверів (див. рис. А.1).

Для підключення пристроїв мережі між собою використовуються високошвидкісні порти FastEthernet/GigabitEthernet. Також більшість кінцевих пристроїв підключенні до мережі з допомогою технології Wi-Fi. Для економії портів на комутаторі, робочі станції були підключені через IP-телефони, що за сумісництвом є комутаторами, так як мають декілька високошвидкісних портів для підключення.

Детальну топологію з'єднань головного офісу показано в табл. 2.1.

Таблиця 2.1

Параметри інтерфейсів пристроїв головного офісу

| Пристрій                   | Інтерфейси | Підключення до пристрою    | Підключення до інтерфейсів |
|----------------------------|------------|----------------------------|----------------------------|
| Маршрутизатор R_main       | G0/0       | Internet                   |                            |
|                            | G1/0       | Міжмережний екран ASA_main | G0/1                       |
|                            | G2/0       | Міжмережний екран ASA_BKP  | G0/2                       |
| Маршрутизатор R_BKP        | G0/0       | Internet                   |                            |
|                            | G1/0       | Міжмережний екран ASA_BKP  | G0/1                       |
|                            | G2/0       | Міжмережний екран ASA_main | G0/2                       |
| Міжмережний екран ASA_main | G0/0       | Міжмережний екран ASA_BKP  | G0/0                       |
|                            | G0/1       | Маршрутизатор R_main       | G1/0                       |
|                            | G0/2       | Маршрутизатор R_BKP        | G2/0                       |
|                            | G0/3       | Комутатор SW_main          | G0/0                       |
|                            | G0/4       | Комутатор SW_main(2)       | G0/0                       |

Продовження таблиці 2.1

| Пристрій                    | Інтерфейси | Підключення до пристрою     | Підключення до інтерфейсів |
|-----------------------------|------------|-----------------------------|----------------------------|
| Міжмережний екран ASA_BKP   | G0/0       | Міжмережний екран ASA_main  | G0/0                       |
|                             | G0/1       | Маршрутизатор R_BKP         | G1/0                       |
|                             | G0/2       | Маршрутизатор R_main        | G2/0                       |
|                             | G0/3       | Комутатор SW_main           | G0/1                       |
|                             | G0/4       | Комутатор SW_main(2)        | G0/1                       |
| Комутатор SW_main           | G0/0       | Міжмережний екран ASA_main  | G0/3                       |
|                             | G0/1       | Міжмережний екран ASA_BKP   | G0/3                       |
|                             | Fa0/1      | Комутатор SW_server         | Fa0/1                      |
|                             | Fa0/2      | Контроллер W_LAN_Controller | Fa0/1                      |
|                             | Fa0/3      | Комутатор SW_CLIENT_ACC_1   | Fa0/1                      |
|                             | Fa0/4      | Комутатор SW_CLIENT_ACC_2   | Fa0/1                      |
|                             |            | Комутатор SW_main(2)        |                            |
| Комутатор SW_main(2)        | G0/0       | Міжмережний екран ASA_main  | G0/4                       |
|                             | G0/1       | Міжмережний екран ASA_BKP   | G0/4                       |
|                             | Fa0/1      | Комутатор SW_server         | Fa0/2                      |
|                             | Fa0/2      | Контроллер W_LAN_Controller | Fa0/2                      |
|                             | Fa0/3      | Комутатор SW_CLIENT_ACC_1   | Fa0/2                      |
|                             | Fa0/4      | Комутатор SW_CLIENT_ACC_2   | Fa0/2                      |
|                             |            | Комутатор SW_main           |                            |
| Контроллер W_LAN_Controller | Fa0/1      | Комутатор SW_main           | Fa0/2                      |
|                             | Fa0/2      | Комутатор SW_main(2)        | Fa0/2                      |
| Комутатор SW_server         | Fa0/1      | Комутатор SW_main           | Fa0/1                      |
|                             | Fa0/2      | Комутатор SW_main(2)        | Fa0/1                      |
|                             | Fa0/3      | Сервер SERVER_1             | Fa0                        |
|                             | Fa0/4      | Сервер SERVER_2             | Fa0                        |
|                             | Fa0/5      | Сервер SERVER_3             | Fa0                        |
| Комутатор SW_CLIENT_ACC_1   | Fa0/1      | Комутатор SW_main           | Fa0/3                      |
|                             | Fa0/2      | Комутатор SW_main(2)        | Fa0/3                      |
|                             | Fa0/3      | Точка доступу AP_1          | Fa0                        |
|                             | Fa0/4      | IP-телефон IP_Phone2        | Fa0/1                      |

Продовження таблиці 2.1

| Пристрій                  | Інтерфейси | Підключення до пристрою   | Підключення до інтерфейсів |
|---------------------------|------------|---------------------------|----------------------------|
| Комутатор SW_CLIENT_ACC_2 | Fa0/1      | Комутатор SW_main         | Fa0/4                      |
|                           | Fa0/2      | Комутатор SW_main(2)      | Fa0/4                      |
|                           | Fa0/3      | Точка доступу AP_2        | Fa0                        |
|                           | Fa0/4      | ІР-телефон IP_Phone1      | Fa0/1                      |
| ІР-телефон IP_Phone1      | Fa0/1      | Комутатор SW_CLIENT_ACC_2 | Fa0/4                      |
|                           | Fa0/2      | Робоча станція PC5        | Fa0                        |
| ІР-телефон IP_Phone2      | Fa0/1      | Комутатор SW_CLIENT_ACC_1 | Fa0/4                      |
|                           | Fa0/2      | Робоча станція PC4        | Fa0                        |
| Точка доступу AP_1        | Fa0        | Комутатор SW_CLIENT_ACC_1 | Fa0/3                      |
| Точка доступу AP_2        | Fa0        | Комутатор SW_CLIENT_ACC_2 | Fa0/3                      |
| Робоча станція PC4        | Fa0        | ІР-телефон IP_Phone2      | Fa0/2                      |
| Робоча станція PC5        | Fa0        | ІР-телефон IP_Phone1      | Fa0/2                      |
| Сервер SERVER_1           | Fa0        | Комутатор SW_server       | Fa0/3                      |
| Сервер SERVER_2           | Fa0        | Комутатор SW_server       | Fa0/4                      |
| Сервер SERVER_3           | Fa0        | Комутатор SW_server       | Fa0/5                      |

Для забезпечення роботи даної мережі підприємства було вибрано ір-телефони, маршрутизатори, і комутатори корпорації Cisco, котрі мають адаптованість під модернізацію модулями. Також обладнання даного виробника славиться своєю надійністю та стабільністю роботи.

## 2.2. Опис вибраного обладнання

Так як доступу до обладнання немає, то мережа розроблюється в симуляторі. Через це реальні моделі пристроїв назвати важко. Тому нижче розкриті характеристики серій пристроїв, що були використані при побудові мережі.

Маршрутизація мережі побудована на базі маршрутизатора Cisco з серії 7200 та ME Cisco ASA серії 5500. Крім цього у проекті будуть використані

комутатори серії Cisco Catalyst 2960S, IP-телефони Cisco 7900 Series Unified IP Phone, CAP Wi-Fi-точки та контролери бездротової мережі Cisco серії 5508.

Маршрутизатори Cisco 7200 Series – це головний вибір для вимогливих підприємств. Як і всі продукти Cisco, серія 7200 пропонує модульність та масштабованість, що і вимагає великий бізнес і все це у компактному форм факторі з широким спектром можливостей розгортання, які бажають великі мережі. З швидкістю обробки до 1 мільйона пакетів в секунду в поєднанні з провідними в галузі справністю та керованістю, такі моделі, як Cisco 7200 на процесорі NPE-G1 легко вписується в будь-яку існуючу мережеву архітектуру, дозволяючи будь-якому бізнесу досягти успіху на арені комунікацій.

Крім виняткової продуктивності, серія Cisco 7200 – це найбільш широко розгорнутий універсальний маршрутизатор сервісних мереж. Передова технологія серії 7200 пропонує:

Підтримка IP / MPLS на основі Cisco IOS (підтримка QoS, широкосмуговий агрегат, безпека, мультисервіс, MPLS);

Широкий спектр гнучких модульних інтерфейсів (від DS0 до OC12);

Підтримка Fast Ethernet, Gigabit Ethernet, Packet Over Sonet;

Повна підтримка припинення L2TP та PPP;

Підтримка до 16000 широкосмугових сеансів абонентів за допомогою NPE-G1;

Сервісний прискорювач за допомогою технології Cisco PXF;

Широкосмугова агрегація: до 16000 сеансів ДПП на шасі;

Багатопротокольна комутація міток (MPLS): провідний вибір для кращого розгортання постачальника;

IPN-безпека (IPsec) VPN: масштабується до 5000 тунелів на шасі;

Обладнання для приміщень високого класу (CPE);

Підтримка шлюзу IP-IP: надає точку інтерфейсу мережа-мережа для сигналізації взаємодії (H.323, SIP), взаємодії з медіа-повідомленнями, переклади адрес і портів (приховування конфіденційності та топології), виставлення

рахунків та нормалізації CDR та управління пропускнуою здатністю. (Маркування QoS за допомогою TOS);

Інтеграція голосу, відео та даних: VXR-шасі та адаптери голосового порту з підтримкою TDM;

Модульна конструкція: слід 3RU з широким спектром гнучких модульних інтерфейсів (від DS0 до OC-3).

IP-телефони було вибрано Cisco 7900 Series Unified IP Phone. До основних переваг даної серії можна віднести наступні характеристики:

індивідуалізація інтерфейсу. Завдяки наявності програмованих клавіш, користувачі можуть індивідуалізувати інтерфейс, забезпечивши прискорений доступ до найбільш часто використовуваних каталогів і сервісів;

підтримка передових алгоритмів шифрування. Підтримка 128-бітного алгоритму шифрування AES гарантує захищену передачу трафіку з даними і голосом. можливості оновлення ПЗ. Користувачі можуть за лічені хвилини оновити програмне забезпечення на IP телефоні завдяки підтримці протоколу TFTP;

зручна клавіатура. Зручна клавіатура, забезпечена світлодіодними індикаторами, максимально спрощує процес управління цими пристроями. Вся розмітка, якою супроводжується кожна кнопка, нанесена лазером і не схильна до стирання або вигоряння згодом;

енергоефективність. Користувачі можуть значно знизити рентабельність використання послуг VoIP за рахунок зниження енергоспоживання. Такий підхід забезпечується завдяки можливості занурення Cisco 7900 Series Unified IP Phone в сплячий режим в періоди простою;

спікерфон. Можливість спілкування з гарнітура через полнодуплексного спікерфона надає оптимальні можливості для групових бесід. Крім того, ця особливість дозволяє вільно переміщатися по приміщенню протягом бесіди, займаючись при цьому своїми справами;

Чудові Аудіо характеристики. Висока якість звучання забезпечується як для користувачів Cisco 7900 Series Unified IP Phone (за рахунок широкосмугових

динаміків), так і для їх співрозмовників (завдяки наявності чутливих мікрофонів, механізмів шумо- і ехоподавлення, а також функції ідентифікації голосової активності);

графічний дисплей. Ємнісний графічний дисплей, властивий деяким моделям Cisco 7900 Series Unified IP Phone, надає користувачам корисну інформацію, таку як вміст телефонної книги, журналу дзвінків, стан здійснення дзвінка, поточної дати і часу та ін.;

вбудований комутатор. Вбудований 10 / 100BASE-T Ethernet-комутатор реалізує підключення до LAN і ПК через два порти RJ-45.

Комутатори фіксованою конфігурації Cisco Catalyst 2960S призначаються для організації рівня доступу локальної мережі, сюди відноситься як підключення комп'ютерів, робочих станцій, принтерів і інших мережевих пристроїв. Це стекуване аналог і подальший розвиток лінійки комутаторів Cisco Catalyst 2960.

Ключові характеристики комутаторів Cisco Catalyst 2960S:

Представлені 24-х і 48-і портові моделі, гігабітні порти Ethernet 10/100/1000 + порти 10G Ethernet або SFP-конектори;

Передбачені порти POE (Power Over Ethernet) для постачання харчуванням IP-телефонів, точок доступу і т.д.;

У моделі Cisco Catalyst 2960 S присутній особливий модуль Стекування Cisco FlexStack з гарячою заміною, який служить для зв'язку комутаторів з прошивкою Lan Base між собою на швидкості 20 Gbps - до 4 комутаторів в одному стек;

Підтримка модуля Redundant Power System 2300;

Передбачені списки контролю доступу (ACL-Access Control Lists);

Контроль якості мережі QoS (Quality of Service).

Серія гігабітних комутаторів Cisco Catalyst 2960S, які надають економічно ефективний доступ до мережі і підтримують стекування. Ці комутатори корпоративного класу забезпечують надійний зв'язок з можливостями для

скорочення сукупної вартості використання, і гарантують якість надання IP (VoIP) послуг, а також бізнес-додатків.

Cisco ASA 5500 – це міцне комплексне рішення для надання безпеки мережі, яке поєднує в собі провідне на ринку технології. Збільшує продуктивність праці персоналу, завдяки функції контролю обміну файлами, чату, технології фільтрів спаму, фішингу та інших загроз.

Ця серія пристроїв дозволяє використовувати нові пропозиції, без ризику для системи безпеки. Мобільні співробітники і бізнес-партнери можуть безпечно підключатися до вашої мережі через Інтернет за допомогою IPsec або Secure Sockets Layer (SSL) VPN services.

Cisco ASA 5500 надає малим і середнім компаніям комплексний шлюз безпеки і VPN-підключення. Cisco ASA 5500 зупиняє загрози на шлюзі, перш ніж вони потрапляють в мережі і впливають на бізнес-операції. Cisco ASA 5500 Series Business Edition пропонує:

Найбільш надійні і розгорнуті технології міжмережевих екранів. Cisco PIX® сімейство пристроїв безпеки Cisco ASA 5500 Series дозволяє контролювати бізнес-трафік, зберігаючи небажаних відвідувачів. Можливості управління додатками: рішення може обмежити файлообмінну мережу, миттєвий обмін повідомленнями і шкідливий трафік, в той же час забезпечуючи безпечне розгортання нових бізнес додатків для підвищення рентабельності і конкурентоспроможності.

Лідуючі на ринку контенту можливості безпеки. З потужними можливостями захисту контенту, що надаються за допомогою опцій Content Security and Control Security Services Module (CSC-SSM), Cisco ASA 5500 Adaptive Security Appliance забезпечує життєво важливі послуги безпеки, необхідні для комплексного захисту.

Антивіруси. Зазначена нагородами антивірусна технологія захищає ваші внутрішні ресурси мережі від відомих і невідомих вірусних атак. Частка електронної пошти та веб-трафіку по периметру усуває можливість зараження шкідливими програмами.

Блокування шпигунських програм, що проводиться на рівні шлюзу. Всі шпигунські програми блокуються від вхідного інтернет-трафіку вашої мережі, e-mail трафіку. Звільняє ІТ підтримувані ресурси від дорогих процедур видалення програм-шпигунів і покращує продуктивність співробітників.

Антиспам. Технологія ефективного блокування спаму з дуже низькою ймовірністю помилкових спрацьовувань.

Антифішинг. Захист конфіденційних даних забезпечує запобігання випадкового розкриття інформації про компанії або особистих даних її співробітників, що може призвести до фінансових втрат.

Постійний захист веб-доступу, електронної пошти та передачі файлів. Захист в режимі реального часу веб-трафіку на інтернет шлюзі значно підвищує безпеку даних, навіть коли співробітники заходять на свій веб-інтерфейс з іншого комп'ютера або завантажують файли, які вже заражені.

Фільтрація URL. Web і фільтрації URL може бути використана для управління доступом персоналу в інтернеті, блокування доступу до небажаних сайтів, що значно підвищує ефективність праці співробітників.

Фільтрація контенту E-mail. Фільтрація електронної пошти мінімалізує юридичну відповідальність компанії при передачі електронного матеріалу образливого характеру. Фільтрація також підсилює відповідність нормативним вимогам і діючим законодавством вимогам в рамках компанії.

Захист інвестицій. Слот розширення для підтримки додаткових можливостей, підтримка CSC-SSM (містить функції безпеки), а також можливість розширення додатковими опціями. Ці можливості дозволяють малим підприємствам додавати нові функції в майбутньому, оскільки бізнес зростає і засоби безпеки потребують змін і розширень.

Захист загроз VPN. Cisco ASA 5500 Series являє кращу на ринку захист віддаленого доступу. Рішення забезпечує безпечний доступ віддалених користувачів до внутрішньої мережі систем і послуг. Це рішення поєднує в собі SSL і IPsec VPN можливості для максимальної гнучкості.

Просте розгортання та управління. Cisco ASA 5500 включає в себе технологію Cisco Adaptive Security Manager Device (ASDM), яка забезпечує потужний, але простий в управлінні і використанні браузер на основі інтерфейс моніторингу. Це єдине рішення забезпечує комплексну настройку і моніторинг всіх послуг в одному додатку.

Серія Cisco ASA 5500 представлена широким рядом пристроїв. Основні відмінності яких, полягають в наступних характеристиках:

- кількість і швидкість портів Ethernet;
- число SSL VPN-тунелів;
- число IPSec VPN-тунелів;
- кількість користувачів;
- продуктивність FIREWALL;
- продуктивність VPN.

Вся серія Cisco ASA 5500 складається з підсерій, кожна з яких має спільні характеристики і унікальні відмінності.

#### Cisco ASA 5505

Всі пристрої Cisco ASA 5505 мають 8 портів Fast Ethernet, 10 IPsec VPN, 2 SSL VPN, ліцензію 3DES / AES, і 1 слот розширення. Продуктивність 150 Mbps / 100 Mbps. А відрізняються вони ліцензією, яка має різну кількість користувачів.

#### Cisco ASA 5510

Всі пристрої Cisco ASA 5510 250 IPsec VPN, 2 SSL VPN, ліцензію 3DES / AES, і 1 слот розширення. А відрізняються вони ліцензією, яка має різну кількість користувачів. Продуктивність 300 Mbps / 170 Mbps. А відрізняються кількістю портів Fast Ethernet.

CAP Wi-Fi-точки доступу для контролера – це "полегшені" точки доступу, які не містять в собі налаштувань. Такі точки доступу стануть оптимальним вибором для організації масштабних мереж, коли потрібно централізоване управління.

Нижче наведені основні переваги для користувачів CAP Wi-Fi-точок доступу для контролера:

|  |  |  |  |  |                          |    |
|--|--|--|--|--|--------------------------|----|
|  |  |  |  |  | КІК.КР.Б – 123 – 20 – ПЗ |    |
|  |  |  |  |  |                          |    |
|  |  |  |  |  |                          | 45 |

Можливість організації безшовного роумінгу. Використовуючи контролер, мережевий адміністратор може організувати між керованими точками доступу безшовний роумінг. Таке рішення виключає потребу в повторній мережевій авторизації при переході із зони дії сигналу однієї точки доступу в зону дії іншої.

Два діапазону радіочастот для функціонування. Завдяки підтримці двох діапазонів частот 2,4 ГГц і 5 ГГц системний адміністратор може підключати пристрої на найменш "зашумлених" каналах зв'язку.

Можливість масштабування бездротової мережі. Для того, щоб підключити до раніше створеної бездротової мережі нову точку доступу, досить оновити налаштування на контролері.

Полегшена настройка. Варіант розгортання Wi-Fi з керованими точками доступу передбачає одноразову і загальну настройку для кожного з цих керованих елементів бездротової мережі. Тому ймовірність некоректної роботи будь-якої з CAP WIFI точок доступу для контролера практично виключена.

При виборі CAP WIFI точок доступу для контролера фахівці рекомендують звертати увагу на такі характеристики:

підтримувані стандарти WIFI. Ви можете вибрати моделі в таких конфігураціях: з підтримкою стандартів WIFI IEEE 802.11 b / g / n, 802.11 a / b / g / n або 802.11 a / b / g / b / ac. Точки доступу з підтримкою останнього варіанту комбінації стандартів забезпечує теоретичну пропускну здатність до 1,3 Гбіт / с.

тип антен. Щоб визначити тип антен CAP WIFI точок доступу для контролера, зверніть увагу на букву в артикул: "E" (моделі з зовнішніми антенами, для приміщень зі складною конфігурацією) або "I" (моделі з внутрішніми всеспрямованими антенами).

експлуатаційні характеристики. Точки доступу для внутрішньої установки справно функціонують в межах від 0 ° C до 40 ° C, а варіанти для зовнішньої установки - в діапазоні -20 ° C ... 55 ° C.

можливість многопотокової передачі даних. Завдяки технології MIMO максимально розширюється смуга пропускання, реалізуючи передачу даних одразу за декількома потокам.

Бездротові контролери Cisco серії 5500 засновані на масштабованій і гнучкою платформі, яка забезпечує загально послуги для критично важливих бездротових мереж в середніх і великих підприємствах, і кампусах. Призначені для роботи з мережевими стандартами 802.11ac і 802.11n, контролери цієї серії надають такі можливості:

- видимість і захист радіоефіру;
- можливість одночасного управління до 500 точок доступу;
- високий рівень продуктивності для якісного відтворення потокового відео і голосових додатків;
- аварійне перемикання між точками доступу і клієнтами протягом частки секунди.

Оптимізовані для високопродуктивної бездротової мережі, контролери Cisco серії 5500 забезпечують підвищену мобільність, підтримують високу щільність клієнтів і забезпечують послуги роумінгу з дев'ятиразовий перевищує пропускну здатність попередніх стандартів WIFI 802.11a / g.

Завдяки інтегрованої технології Cisco CleanAir®, контролери серії 5500 гарантують максимальну продуктивність стандарту 802.11n.

Контролери бездротової мережі Cisco серії 5508 підтримують Application Visibility and Control – технологію Cisco, яка включає в себе інструмент для розпізнавання мережних додатків NBAR-2, а також можливість глибокої інспекції пакетів (DPI). За допомогою NBAR-2 можна класифікувати додатки, застосовувати настройки QoS для поточного трафіку, а також призначати пріоритети критично важливим мережевим бізнес-додатків. Cisco AVC використовує NetFlow v.9 для експорту потоків в інфраструктурі Cisco Prime™ або в NetFlow Collector. Серія 5508 також підтримує послуги каталогів Bonjour для використання в окремому Layer 3 мережі.

Ліцензування точок доступу надає можливості для обслуговування до 500 пристроїв одночасно. Ліцензійна структура підтримує різні вимоги до мобільності, в тому числі рішення Cisco OfficeExtend для безпечної, надійної мобільної співпраці і Cisco Enterprise Wireless Mesh для організації бездротового з'єднання в важкодоступних місцях.

### 2.3. Опис вибраних технологій та протоколів

В даному проекті слід використати декілька базових протоколів.

Одним з них є протокол SSH (англ. Secure SHell, „безпечна оболонка”). Це мережний протокол віддаленого доступу, який дає змогу здійснювати віддалене управління операційною системою будь-якого мережного пристрою і безпечно передавати у незахищеному середовищі повідомлення будь-якого іншого мережного протоколу (наприклад, здійснювати тунелювання TCP-з'єднань для передачі файлів). За функціональністю схожий на протоколи Telnet, rlogin, rsh, але на відміну від них, шифрує увесь трафік, що передається, зокрема і паролі. Окрім шифрування може також здійснювати стиснення даних. Протокол SSH, як і решта протоколів віддаленого управління, побудований із використанням клієнт-серверного підходу. SSH-клієнти та SSH-сервери доступні для більшості мережних операційних систем.

Ще одним базовим протоколом є протокол динамічної конфігурації вузла (DHCP). Даний протокол мережевого управління, використовується в мережах Інтернет-протоколу, за допомогою якого DHCP-сервер динамічно призначає IP-адресу та інші параметри конфігурації мережі кожен пристрій в мережі, щоб вони могли обмінюватися даними з іншими IP-мережами. DHCP-сервер дозволяє комп'ютерам автоматично запитувати IP-адреси і мережні параметри у Інтернет провайдера (ISP), що знижує необхідність для мережевого адміністратора або користувача в ручному призначенні IP-адрес всіх мережевих пристроїв. [1] При відсутності DHCP-сервера комп'ютера або іншого пристрою в мережі необхідно

вручну призначити IP-адреса або призначити собі адресу APIPA, що не дозволить йому здійснювати зв'язок за межами локальної підмережі.

DHCP може бути реалізований в мережах розміром від домашніх мереж до великих кампусних мереж і регіональних мереж Інтернет-провайдерів.[2] Як сервер DHCP може бути включений маршрутизатор. Більшість сельбищних мережевих маршрутизаторів отримують глобальний унікальний IP-адреса всередині мережі ISP. В межах локальної мережі сервер DHCP призначає локальний IP-адресу кожному пристрою, підключеного до мережі.

Детальні параметри адресації мережі головного офісу представлена в табл. 2.4.

Таблиця 2.4

Параметри адресації мережі головного офісу

| Підмережа/<br>Пристрій        | Інтерфейс/Мереж-<br>ний адаптер/Шлюз | IP-адреса   | Маска<br>підмережі | Префікс |
|-------------------------------|--------------------------------------|-------------|--------------------|---------|
| Маршрутизатор R_main          | G0/0                                 | 1.1.1.1     | 255.0.0.0          | /8      |
|                               | G1/0                                 | 192.168.1.1 | 255.255.255.252    | /30     |
|                               | G2/0                                 | 192.168.2.1 | 255.255.255.252    | /30     |
| Маршрутизатор R_BKP           | G0/0                                 | 2.2.2.2     | 255.0.0.0          | /8      |
|                               | G1/0                                 | 192.168.3.1 | 255.255.255.252    | /30     |
|                               | G2/0                                 | 192.168.4.1 | 255.255.255.252    | /30     |
| Міжмережний екран<br>ASA_main | G0/0                                 | 192.168.5.1 | 255.255.255.252    | /30     |
|                               | G0/1                                 | 192.168.1.2 | 255.255.255.252    | /30     |
|                               | G0/2                                 | 192.168.4.2 | 255.255.255.252    | /30     |
|                               | G0/3                                 | 172.16.1.1  | 255.255.252.0      | /22     |
|                               | G0/4                                 | 172.16.1.2  | 255.255.252.0      | /22     |
| Міжмережний екран<br>ASA_BKP  | G0/0                                 | 192.168.5.2 | 255.255.255.252    | /30     |
|                               | G0/1                                 | 192.168.3.2 | 255.255.255.252    | /30     |
|                               | G0/2                                 | 192.168.2.2 | 255.255.255.252    | /30     |
|                               | G0/3                                 | 172.16.1.3  | 255.255.252.0      | /22     |
|                               | G0/4                                 | 172.16.1.4  | 255.255.252.0      | /22     |

Продовження таблиці 2.4

| Підмережа/<br>Пристрій         | Інтерфейс/Мереж-<br>ний адаптер/Шлюз | ІР-адреса   | Маска<br>підмережі | Префікс |
|--------------------------------|--------------------------------------|-------------|--------------------|---------|
| Комутатор SW_main              | Vlan21                               | 172.16.1.5  | 255.255.252.0      | /22     |
|                                | Vlan30                               | 172.16.3.1  | 255.255.255.0      | /24     |
|                                | Vlan40                               | 172.16.4.1  | 255.255.255.0      | /24     |
|                                | Vlan45                               | 172.16.5.1  | 255.255.255.0      | /24     |
|                                | Vlan176                              | 172.16.10.1 | 255.255.255.240    | /28     |
| Контроллер<br>W_LAN_Controller | Fa0/1                                | 172.16.5.4  | 255.255.255.0      | /24     |
|                                | Fa0/2                                | 172.16.5.5  | 255.255.255.0      | /24     |
| Комутатор SW_server            | Vlan30                               | 172.16.3.2  | 255.255.255.0      | /24     |
|                                | Vlan176                              | 172.16.10.2 | 255.255.255.240    | /28     |
| Комутатор<br>SW_CLIENT_ACC_1   | Vlan21                               | 172.16.1.6  | 255.255.252.0      | /22     |
|                                | Vlan40                               | 172.16.4.2  | 255.255.255.0      | /24     |
|                                | Vlan45                               | 172.16.5.2  | 255.255.255.0      | /24     |
|                                | Vlan176                              | 172.16.10.3 | 255.255.255.240    | /28     |
| Комутатор<br>SW_CLIENT_ACC_2   | Vlan21                               | 172.16.1.7  | 255.255.252.0      | /22     |
|                                | Vlan40                               | 172.16.4.3  | 255.255.255.0      | /24     |
|                                | Vlan45                               | 172.16.5.3  | 255.255.255.0      | /24     |
|                                | Vlan176                              | 172.16.10.4 | 255.255.255.240    | /28     |
| ІР-телефон IP_Phone1           | Vlan21                               | DHCP        |                    |         |
|                                | Vlan40                               |             |                    |         |
|                                | Vlan176                              | 172.16.10.5 | 255.255.255.240    | /28     |
| ІР-телефон IP_Phone2           | Vlan21                               | DHCP        |                    |         |
|                                | Vlan40                               |             |                    |         |
|                                | Vlan176                              | 172.16.10.6 | 255.255.255.240    | /28     |
| Точка доступу AP_1             | Fa0                                  | DHCP        |                    |         |
| Точка доступу AP_2             | Fa0                                  |             |                    |         |
| Робоча станція PC4             | Fa0                                  |             |                    |         |
| Робоча станція PC5             | Fa0                                  |             |                    |         |
| Сервер SERVER_1                | Fa0                                  | 172.16.3.3  | 255.255.255.0      | /24     |
| Сервер SERVER_2                | Fa0                                  | 172.16.3.4  | 255.255.255.0      | /24     |
| Сервер SERVER_3                | Fa0                                  | 172.16.3.5  | 255.255.255.0      | /24     |

LightWeight Access Point — мережевий протокол TCP/IP стеку, що використовується у великих WLAN мережах. LWAPP забезпечує взаємодію бездротових точок доступу з одним або декількома Wi-Fi контролерами. Основним завданням протоколу є автоматичне забезпечення бездротових точок доступу необхідними налаштуваннями для їх роботи у мережі, пов'язаних із SSID та параметрами, які надаються DHCP. У разі необхідності LWAPP надає точці доступу налаштування для побудови тунелю для трафіку користувачів мережі. Використання цього протоколу може допомогти системним адміністраторам великої WLAN скоротити час, що витрачається на налаштування, моніторинг та усунення несправностей. Також LWAPP є базисом для інструментів, що дозволяють аналізувати стан великої бездротової комп'ютерної мережі. LWAPP був базовим протоколом побудови Уніфікованої Бездротової Мережі Cisco (Cisco Unified Wireless Network) включно до релізу 5.1, 2008 року. До 2006 року, LWAPP пропрієтарний протокол компанії Cisco, а згодом став робочим (draft) проектом IETF. AES-шифрування та режим лічильника з протоколом кодування автентифікації повідомлень з блокуванням шифрування блоків (CCMP) використовується для трафіку керування LWAPP.

Журналювання подій (Logging, Event Logging) – це процес запису інформації про певні події, що відбуваються з об'єктами (процесами) у системі. Поряд з терміном „журналювання подій” застосовуються терміни „протоколювання подій” та „реєстрація подій”. Реєстрація інформації здійснюється у системному журналі. Особливістю системного журналу є те, що його записи створюються один за одним у хронологічному порядку. Подальший аналіз даних системного журналу дає змогу визначити, коли і за яких умов виникла та чи інша подія, тобто виконувати аудит подій. Підсистема журналювання подій є складовою підсистеми аудиту (моніторингу) подій, яка, у свою чергу, є невід'ємною складовою системи безпеки. У різних ОС підсистемах журналювання подій базуються на різних принципах та підходах стосовно розміщення та ведення системних журналів, а також стосовно інформування адміністратора про події. Системний журнал може вестися як локально, так і

централізовано. У першому випадку для кожного вузла ведеться окремий системний журнал. У другому випадку загальний системний журнал розміщується на виділеному сервері мережі (або кількох виділених серверах) і всі клієнти мережі надсилають серверу інформацію про власні події з використанням спеціального комунікаційного протоколу.

В обчислювальній техніці syslog є стандартом для реєстрації повідомлень. Він дозволяє розділити програмне забезпечення, яке генерує повідомлення, систему, яка їх зберігає, і програмне забезпечення, яке їх повідомляє та аналізує. Кожне повідомлення позначено кодом об'єкта, із зазначенням типу програмного забезпечення, що генерує повідомлення, і привласнений рівень тяжкості.

Розробники комп'ютерних систем можуть використовувати syslog для управління системою і аудиту безпеки, а також загальних інформаційних, аналітичних та налагоджувальних повідомлень. Стандарт syslog використовується в різних пристроях, таких як принтери, маршрутизатори та приймачі повідомлень на багатьох платформах. Це дозволяє консолідувати протоколюється дані з різних типів систем в центральному репозиторії. Введення syslog існує для багатьох операційних систем.

При роботі у мережі, syslog використовує клієнт-серверну архітектуру, де сервер syslog прослуховує і записує в журнал повідомлення, що надходять від клієнтів.

Правильне представлення дати та часу є актуальним як для повсякденної діяльності людини, так і для функціонування будь-якої комп'ютерної системи.

Протокол мережевого часу (NTP) - це мережевий протокол для синхронізації тактових імпульсів між комп'ютерними системами по мережах передачі даних з пакетною комутацією і змінною затримкою. Працюючи з 1985 року, NTP є одним з найстаріших Інтернет-протоколів, використовуваних в даний час. NTP був розроблений Девідом Л. Миллсом з Університету Делавера.

NTP призначений для синхронізації всіх учасників комп'ютерів з точністю до декількох мілісекунд координованого всесвітнього часу (UTC): він використовує алгоритм перетину, модифіковану версію алгоритму Марзулло,

для вибору серверів точного часу та призначений для пом'якшення ефекту змінної латентності мережі. NTP зазвичай може підтримувати час в межах десятків мілісекунд з публічного Інтернету і в ідеальних умовах може досягати точності більше однієї мілісекунди в локальних мережах. Асиметричні маршрути і перевантаженість мережі можуть привести до помилок в 100 мс і більше [2].

Зазвичай протокол описується в термінах клієнт-серверна модель, але так само легко може бути використаний в тимчасових відносинах, де обидва партнери вважають іншого потенційним джерелом часу: введення відправляє і отримує тимчасові мітки, використовуючи призначений для користувача протокол датаграм (UDP) на порту № 123. Вони також можуть використовувати трансляцію або багатоадресну передачу, коли клієнти пасивно слухають поновлення часу після первинного обміну калібруванням в обидві сторони. NTP видає попередження про майбутню коригування високосної шкали часу, але не передає ніякої інформації про місцеві часових поясах або літньому часу [3].

64-бітові мітки часу, які використовуються NTP, складаються з 32-бітної частини для секунд і 32-бітної частини для частки секунди, що дає шкалу часу, яка перевертається кожні 232 секунди (136 років), і теоретичний дозвіл 2-32 секунд (233 пікосекунди). NTP використовує епоху 1 січня 1900 року. Таким чином, перший ролловер відбувається 7 лютого 2036 року.

NTPv4 представляє 128-бітний формат дати: 64 біта для другого і 64 біта для частки секунди. Найбільш значущим 32-бітовим форматом є Era Number, який в більшості випадків дозволяє неоднозначність при перекиданні. За словами Міллса, «64-бітного значення для дробу досить, щоб визначити кількість часу, який потрібен фотону для проходження електрона зі швидкістю світла. 64-бітного другого значення досить, щоб забезпечити однозначне уявлення часу, поки всесвіт не потьмяніє».

Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2) і Wi-Fi Protected Access 3 (WPA3) - це три програми сертифікації безпеки, розроблені Альянсом Wi-Fi для забезпечення безпеки бездротових комп'ютерних мереж.

Альянс визначив їх у відповідь на серйозні недоліки, виявлені дослідниками в попередній системі, Wired Equivalent Privacy (WEP).

WPA2 замінила WPA. WPA2, яка вимагає тестування і сертифікації Wi-Fi Alliance, реалізує обов'язкові елементи IEEE 802.11i. Зокрема, він включає обов'язкову підтримку CCMP, режиму шифрування на основі AES. Сертифікація почалася у вересні 2004 р., а з 13 березня 2006 р сертифікація WPA2 є обов'язковою для всіх нових пристроїв, що носять торгову марку Wi-Fi [9].

У січні 2018 року Альянс Wi-Fi оголосив про заміну WPA3 на WPA2 [10].

Новий стандарт використовує еквівалентну 192-бітну криптографічний силу в режимі WPA3-Enterprise (AES-256 в режимі GCM з SHA-384 в якості HMAC) і як і раніше зобов'язує використовувати CCMP-128 (AES-128 в режимі CCM) в якості мінімального алгоритму шифрування в режимі WPA3-Personal.

Стандарт WPA3 також замінює попередній обмін ключами на одночасну аутентифікацію еквівалентів, як визначено в IEEE 802.11-2016, що призводить до більш безпечного початкового обміну ключами в персональному режимі [13] і прямий секретності. Альянс Wi-Fi також стверджує, що WPA3 пом'якшить проблеми безпеки, пов'язані зі слабкими паролями і спростить процес налаштування пристроїв без інтерфейсу дисплея.

Захист рамок управління, як зазначено в поправці IEEE 802.11w, також забезпечується специфікаціями WPA3.

Віртуальна LAN (VLAN) - це будь-який широкомовний домен, який розділений і ізолюваний в комп'ютерній мережі на каналному рівні (рівень OSI 2). LAN - це аббревіатура для локальної мережі і в цьому контексті віртуальна відноситься до фізичного об'єкту, відтвореному і зміненим за допомогою додаткової логіки. VLAN працюють шляхом застосування тегів до мережевих кадрів і обробки цих тегів в мережевих системах, створюючи зовнішній вигляд і функціональність мережевого трафіку, який фізично перебуває в одній мережі, але діє так, як ніби він розділений між різними мережами. Таким чином, віртуальні локальні мережі можуть тримати мережеві додатки розділеними,

незважаючи на те, що вони підключені до однієї і тієї ж фізичної мережі і не вимагають розгортання кількох наборів кабелів і мережевих пристроїв.

VLAN дозволяють мережевим адміністраторам групувати вузли разом, навіть якщо вузли не підключені безпосередньо до одного мережного комутатора. Оскільки приналежність до VLAN може бути налаштована за допомогою програмного забезпечення, це може значно спростити проектування і розгортання мережі. Без VLAN угруповання вузлів відповідно до їх ресурсами вимагає трудовитрат по переміщенню вузлів або перепідключення каналів передачі даних. У локальних мережах VLAN мережі і пристрої, які повинні бути відокремлені один від одного, можуть спільно використовувати одні й ті ж фізичні кабелі без взаємодії, що підвищує простоту, безпеку, управління трафіком або економічність. Наприклад, VLAN можна використовувати для поділу трафіку всередині підприємства через користувачів і мережевих адміністраторів або між типами трафіку, щоб користувачі або фоновий трафік не могли безпосередньо впливати на роботу мережі. Багато послуги інтернет хостингу використовують VLAN для відділення приватних зон своїх клієнтів один від одного, дозволяючи серверів кожного клієнта бути згрупованими в одному сегменті мережі, перебуваючи при цьому в будь-якому місці свого дата-центру. Необхідні деякі запобіжні заходи, щоб запобігти "витіку" трафіку з даної VLAN - експлойт, відомий як "стрибок у VLAN".

Для поділу мережі на VLAN необхідно конфігурувати мережеве обладнання. Більш просте обладнання може розбиватися тільки на фізичні порти (якщо такі є) і в цьому випадку кожна віртуальна локальна мережа підключається за допомогою виділеного мережевого кабелю. Більш складні пристрої можуть маркувати кадри за допомогою тегів VLAN так, що для передачі даних по декількох VLAN можна використовувати одне з'єднання (магістраль). Оскільки віртуальні локальні мережі мають загальну смугу пропускання, в магістралі віртуальних локальних мереж можна використовувати агрегацію каналів, пріоритизації якості обслуговування або і те, і інше для ефективної маршрутизації даних.

## РОЗДІЛ 3. НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ГЕТЕРОГЕНОЇ МЕРЕЖІ

### 3.1. Базове налагодження пристроїв мережі

В цьому розділі наведено базові налаштування пристроїв мережі. Як маршрутизатори, так і комутатори мають ім'я (hostname). Ім'я це здебільшого використовується для зручності адміністратора, щоб можна було відрізнити безліч пристроїв один від одного. Спочатку все маршрутизатори мають ім'я «Router», а комутатори - «Switch», що не сильно зручно. Правилом хорошего тону є встановлення назви пристрою насамперед, до будь-яких інших дій.

```
Switch#en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#host Switch1-1
Switch1-1(config)#
```

Рис. 3.1. Налаштування імені на комутаторі Switch1-1

Головною складовою мережі є адресація, після зміни найменувань потрібно налаштувати статичну адресацію інтерфейсів мережі. За цією адресою пристрої зможуть “спілкуватися” між собою у мережі.

В локальних мережах прийнято використовувати IP-адреси які зарезервовані для використання у приватних мережах. А для виходу в Internet використовуються так звані «білі» IP-адреси, які на віміну від приватних не можуть повторятися. На рис. 3.2 зображено призначення інтерфейсу «білої» адреси для з'єднання з глобальною мережею.

```
Router2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router2(config)#int g1/0
Router2(config-if)#ip add 2.2.2.2 255.255.255.252
Router2(config-if)#no sh
Router2(config-if)#
*May 6 14:16:45.227: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*May 6 14:16:46.227: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
Router2(config-if)#ex
Router2(config)#
```

Рис. 3.2. Налаштування статичної IP-адреси на маршрутизаторі Router2

Для віддаленого керування потрібно налаштувати статичні IP-адреси. Наприклад для комутатора потрібно призначити IP-адреси для інтерфейсів VLAN (рис. 3.3).

```
Switch1-1(config)#int vlan 1
Switch1-1(config-if)#ip add 193.2.3.126 255.255.255.252
Switch1-1(config-if)#no sh
Switch1-1(config-if)#ex
Switch1-1(config)#
```

Рис. 3.3. Налаштування статичної IP-адреси для інтерфейсу VLAN1 на комутаторі Switch1-1

На всіх пристроях налаштовано віддаленне керування за допомогою технології SSH.

```
Router3(config)#username admin privilege 15 secret adminpass
Router3(config)#username technic privilege 5 secret technicpass
Router3(config)#enable secret cisco
Router3(config)#login block-for 300 attempts 3 within 3
Router3(config)#login delay 5
Router3(config)#login on-failure log
Router3(config)#login on-success log
Router3(config)#ip domain-name office3.com
Router3(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: Router3.office3.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Router3(config)#
*May 13 09:11:58.327: %SSH-5-ENABLED: SSH 1.99 has been enabled
Router3(config)#ip ssh version 2
Router3(config)#ip ssh time-out 60
Router3(config)#ip ssh authentication-retries 5
Router3(config)#ip ssh maxstartups 5
Router3(config)#ip ssh logging events
Router3(config)#line vty 0 4
Router3(config-line)#login local
Router3(config-line)#transport input ssh
Router3(config-line)#transport output ssh
Router3(config-line)#logout-warning 30
Router3(config-line)#absolute-timeout 10
Router3(config-line)#logging synchronous
Router3(config-line)#exit
Router3(config)#
```

Рис. 3.4. Налаштування захисту віддаленого підключення на маршрутизаторі Router3

Для розділення внутрішньої мережі на комутаторах було налаштовано віртуальні локальні мережі (VLAN). Це дозволить контролювати та відмежувати трафік пристроїв. Приклад налагодження VLAN представлений на рис. 3.5.

```
Switch1-1(config)#vlan 10
Switch1-1(config-vlan)#name LAN_VM
Switch1-1(config-vlan)#exit
Switch1-1(config)#int e0/0
Switch1-1(config-if)#switchport mode access
Switch1-1(config-if)#switchport access vlan 10
Switch1-1(config-if)#ex
```

Рис. 3.5. Налаштування VLAN 10 та прив'язка порта до нього на комутаторі Switch1-1

Для того, щоб була можливість обміну даних VLAN між собою та іншими мережами, було налаштовано транкові канали зв'язку.

```
Switch1-1(config)#int range e1/2-3
Switch1-1(config-if-range)#switchport trunk encapsulation dot1q
Switch1-1(config-if-range)#switchport mode trunk
Switch1-1(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50,60
Switch1-1(config-if-range)#
```

Рис. 3.6. Налаштування транкового каналу на комутаторі Switch1-1

Також на маршрутизаційних пристроях було налаштовано транкові каналів зв'язку, за допомогою конфігурування підінтерфейсів на інтерфейсах, підключених до комутаторів.

```
Router3(config)#int g0/0
Router3(config-if)#no ip add
Router3(config-if)#no sh
Router3(config-if)#int g0/0.10
Router3(config-subif)#encapsulation dot1q 10
Router3(config-subif)#ip add 195.2.3.1 255.255.255.240
Router3(config-subif)#ex
```

Рис. 3.7. Налаштування підінтерфейса на маршрутизаторі Router3

```
Firewall1# conf t
Firewall1(config)# int g0/0
Firewall1(config-if)# no shut
Firewall1(config-if)# int g0/0.10
Firewall1(config-subif)# vlan 10
Firewall1(config-subif)# ip add 193.2.3.1 255.255.255.240
Firewall1(config-subif)# ex
```

Рис. 3.8. Налаштування підінтерфейса на ME Firewall1

IP-адреси для кінєвих пристроїв були призначенні за допомогою протоколу DHCP.

```
Router3(config)#ip dhcp exc 195.2.3.1
Router3(config)#ip dhcp pool LAN-VM
Router3(dhcp-config)#network 195.2.3.0 255.255.255.240
Router3(dhcp-config)#def 195.2.3.1
Router3(dhcp-config)#domain office3.com
Router3(dhcp-config)#dns 8.8.8.8
Router3(dhcp-config)#exit
```

Рис. 3.9. Налаштування DHCP на маршрутизаторі Router3

```

Firewall2(config)# dhcpd dns 8.8.8.8
Firewall2(config)# dhcpd domain office2.com
Firewall2(config)# dhcpd add 194.2.3.2-194.2.3.14 inside1
Firewall2(config)# dhcpd enable inside1
Firewall2(config)#

```

Рис. 3.10. Налаштування DHCP на ME Firewall2

### 3.2. Налаштування гетерогенної корпоративної мережі

В головному офісі для захисту мережі використовується два міжмережні екрани у відмовостійкому режимі та підключення до двох провайдерів. Така конфігурація мережі є більш відмовостійка.

Для налаштування режиму відмовостійкості на міжмережних екранах слід вказати їх порядковий номер «primary» чи «secondary», і відповідний інтерфейс, який буде з'єднувати зі своїм «сусідом». Конфігурація двох пристроїв є однаковою, і відрізняється лише порядковим номером пристрою (рис. 3.11).

```

Firewall1(config)# failover
Firewall1(config)# failover lan unit primary
Firewall1(config)# failover lan interface STATE g0/1
INFO: Non-failover interface config is cleared on GigabitEthernet0/1 and its sub-interfaces
Firewall1(config)# failover polltime unit 1 holdtime 3
Firewall1(config)# failover link STATE g0/1
Firewall1(config)# failover interface ip STATE 1.1.2.1 255.255.255.252 standby

```

Рис. 3.11. Налаштування режиму відмовостійкості на ME Firewall1

```

Firewall1# conf t
Firewall1(config)# same-security-traffic permit inter-interface
Firewall1(config)#

```

Рис. 3.12. Налаштування дозволу трафіку між підінтерфейсами на ME Firewall1

Для доступу до глобальної мережі, на маршрутизуючих пристроях була налаштована трансляція мережних адрес NAT (див. рис. 3.13-3.14). Трансляція дозволяє запобігти або обмежити обіг зовні до внутрішніх хостів, залишаючи можливість звернення зсередини назовні.

Таким чином з глобальної мережі доступна тільки зовнішня ір-адреса офісу, це забезпечує кращий захист корпоративної мережі від загроз ззовні.

```

Router3(config)#int g0/0.40
Router3(config-subif)#ip nat inside
Router3(config-subif)#exit
Router3(config)#int g1/0
Router3(config-if)#ip nat outside
Router3(config-if)#exit
Router3(config)#ip access-list standard NAT
Router3(config-std-nacl)#permit 195.2.3.0 0.0.0.15
Router3(config-std-nacl)#permit 195.2.3.16 0.0.0.15
Router3(config-std-nacl)#permit 195.2.3.32 0.0.0.15
Router3(config-std-nacl)#permit 195.2.3.48 0.0.0.15
Router3(config-std-nacl)#exit
Router3(config)#ip nat inside source list NAT interface g1/0 overload

```

Рис. 3.13. Налаштування NAT на маршрутизаторі

```

Firewall1(config)# object network inside1
Firewall1(config-network-object)# subnet 193.2.3.0 255.255.255.240
Firewall1(config-network-object)# nat (inside1,outside) dynamic interface
Firewall1(config-network-object)# exit
Firewall1(config)#

```

Рис. 3.14. Налаштування NAT на ME Firewall1

Для взаємодії філій з головним офісом налаштовано приватну віртуальну мережу – VPN (Virtual Private Network). Це надає безпечний зв'язок між офісами. В цьому проекті було застосовано поширений і тип VPN який найбільше підтримується задля з'єднання типу «мережа-мережа» – IPSec Site-To-Site VPN. Налаштування, які мають відношення до вище названих мереж, відбуваються в два етапи – побудування тунелю та налагодження передачі шифрованого трафіку.

Аби створити необхідну нам мережу, налаштування кожного з етапів мають бути ідентичними. Перше, що необхідно налаштувати це є створення політики шифрування (рис. 3.15-3.16).

```

Router3(config)#crypto isakmp policy 1
Router3(config-isakmp)#hash sha
Router3(config-isakmp)#authentication pre-share
Router3(config-isakmp)#group 5
Router3(config-isakmp)#lifetime 3600
Router3(config-isakmp)#encryption aes 256
Router3(config-isakmp)#ex
Router3(config)#

```

Рис. 3.15. Створення політики шифрування на маршрутизаторі Router3

```

Firewall1(config)# crypto ikev1 policy 1
Firewall1(config-ikev1-policy)# hash sha
Firewall1(config-ikev1-policy)# authentication pre-share
Firewall1(config-ikev1-policy)# group 5
Firewall1(config-ikev1-policy)# lifetime 3600
Firewall1(config-ikev1-policy)# encryption aes-256
Firewall1(config-ikev1-policy)# ex
Firewall1(config)# █

```

Рис. 3.16. Створення політики шифрування на ME Firewall1

Другим етапом є налаштуванням тунелю по ключу автентифікації. В цьому випадку для прикладу будуть налаштовані по 2 тунеля від головного офісу до філій, аби створити злагоджену роботу між трьома офісами. Приклад налаштування зображений на рис. 3.17-3.18.

```

Router3(config)#crypto isakmp key Office1ToOffice3 add 1.1.1.2
Router3(config)# █

```

Рис. 3.17. Створення ключа для тунелю на маршрутизаторі Router3

```

Firewall1(config)# tunnel-group 3.3.3.2 type ipsec-l2l
Firewall1(config)# tunnel-group 3.3.3.2 ipsec-attributes
Firewall1(config-tunnel-ipsec)# ikev1 pre-shared-key Office1ToOffice3
Firewall1(config-tunnel-ipsec)# ex
Firewall1(config)# █

```

Рис. 3.18. Створення ключа для тунелю на ME Firewall1

Не менш важливим етапом є моніторинг трафіку – трафіку, що проходить між офісами. Саме тому потрібно певний список доступу (рис. 3.19-3.20).

```

Router3(config)#$ 103 permit ip 195.2.3.0 0.0.0.63 193.2.3.0 0.0.0.63
Router3(config)# █

```

Рис. 3.19. Створення списку доступу для відловлювання «цікавого» трафіку на маршрутизаторі Router3

```

Firewall1(config)# access-list VPN extended permit ip object-group INSIDE obje$
Firewall1(config)# █

```

Рис. 3.20. Створення списку доступу для відловлювання «цікавого» трафіку на ME Firewall1

VPN налаштовується на граничних пристроях мережі, де заделегіть налаштована адресна трансляція, саме тому повз трансляцію необхідно спрямовувати «цікавий» трафік. Налаштування схожого обходу зображене на рис. 3.21-3.22.

```
Router3(config)#ip access-list extended NAT
Router3(config-ext-nacl)#deny ip 195.2.3.0 0.0.0.63 193.2.3.0 0.0.0.63
Router3(config-ext-nacl)#permit ip 195.2.3.0 0.0.0.63 any
Router3(config-ext-nacl)#ex
Router3(config)#
```

Рис. 3.21. Налаштування обходу NAT на маршрутизаторі Router3

```
Firewall1(config)# nat (inside1,outside) source static inside1 inside1 destina$
Firewall1(config)# nat (inside2,outside) source static inside2 inside2 destina$
Firewall1(config)# nat (inside3,outside) source static inside3 inside3 destina$
Firewall1(config)# nat (inside4,outside) source static inside4 inside4 destina$
Firewall1(config)#
```

Рис. 3.22 Налаштування обходу NAT на ME Firewall1

Після цих дій 1-й етап налаштувань завершується. Наступним кроком є створення правила шифрування трафіку, що проходитиме по створеним тунелям (рис. 3.23-3.24).

```
Router3(config)#crypto ipsec transform-set Offices esp-aes 256 esp-sha-hmac
Router3(cfg-crypto-trans)#mode tunnel
Router3(cfg-crypto-trans)#ex
```

Рис. 3.23. Створення правила шифрування трафіку на маршрутизаторі Router3

```
Firewall1(config)# crypto ipsec ikev1 transform-set Offices esp-aes-256 esp-sh$
Firewall1(config)#
```

Рис. 3.24. Створення правила шифрування трафіку на ME Firewall1

Завершальним етапом є налаштування криптокарти, що «збирає» всі налаштування в одному місці – зазначається цікавий трафік, правила шифрування та кінцева точка, куди спрямовується трафік. Для того, щоб скористатись криптокартою, необхідно призначити інтерфейс який буде застосовуватися. Налаштування на маршрутизаторах та міжмережевих екранах будуть відрізняються (рис. 3.25-3.26).

```
Router3(config)#crypto map OfficesMAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
Router3(config-crypto-map)#match address 103
Router3(config-crypto-map)#set transform-set Office1-Office3
Router3(config-crypto-map)#set peer 1.1.1.2
Router3(config-crypto-map)#ex
Router3(config)#int g1/0
Router3(config-if)#crypto map OfficesMAP
Router3(config-if)#
*May 6 16:13:03.215: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Рис. 3.25. Створення та застосування криптокарти на маршрутизаторі Router3

```

Firewall1(config)# crypto map OfficesMAP 1 match address 103
Firewall1(config)# crypto map OfficesMAP 1 set peer 3.3.3.2
Firewall1(config)# crypto map OfficesMAP 1 set ikev1 transform-set Office1-Off$
Firewall1(config)# crypto map OfficesMAP interface outside
Firewall1(config)#

```

Рис. 3.26. Створення та застосування криптокарти на ME Firewall1

Більшість ір-телефонів Cisco мають вбудований комутатор, настройками якого можна управляти. Найбільш часта і рекомендована практика - це поділ голосового трафіку від трафіку даних. Поділ трафіку голосового від трафіку даних забезпечує захист від перехоплення голосового трафіку. Також це дає можливість впровадити QoS більш простими методами. У специфікації телефону це називається Integrated 10/100 Ethernet switch, а в самому телефоні будуть два гнізда "COMPUTER" і "NETWORK". Порт "NETWORK" може відсилати і приймати тагированні пакети 802.1Q, і по суті є транкових портом, тобто портом приймають пакети які належать різним VLAN-ам. Іноді такий порт називають "міні-Транки", тому що "Нормальний" транк пропускає велику кількість VLAN-ів, IP-телефон тегує тільки свої пакети міткою голосового VLAN-а. Налаштовування порту комутатора для роботи з телефоном зображено на рис. 3.27.

```

SW_CLIENT_ACC_1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW_CLIENT_ACC_1(config)# interface F0/0
SW_CLIENT_ACC_1(config-if)# spanning-tree portfast
SW_CLIENT_ACC_1(config-if)# switchport access vlan 50
SW_CLIENT_ACC_1(config-if)# switchport voice vlan 10
SW_CLIENT_ACC_1(config-if)# exit
SW_CLIENT_ACC_1(config)# exit

```

Рис. 3.27. Налаштовування порту комутатора для роботи з телефоном

Ніяких додаткових налаштувань на самому телефоні робити не потрібно. Телефон отримує конфігурацію від комутатора використовуючи CDP. Після того як він отримає номер голосового VLAN, він починає тагувати власні голосові пакети міткою голосового VLAN.

Після того як налаштований DHCP-пул для телефонів на маршрутизаційному пристрої потрібно дати додаткову команду для опції 150. Вона дозволяє підтягувати і автоматично підтягувати прошивки для телефонів з TFTP сервера.

```
SW_main(config)# ip dhcp pool voice
SW_main(dhcp-config)# option 150 ip 192.168.0.1
```

Рис. 3.28. Налаштовування додаткової опції 150

Також потрібно налаштувати класичні VoIP параметри, такі як:

- max-dn - максимально - можлива кількість підтримуваних DN (Directory Numbers). Номерів, іншими словами;
- max-ephones - максимальна кількість телефонних апаратів. Зробимо за кількістю DN'ов;
- ip source-address - звідки наш роутер буде приймати дзвінки (запити) від SCCP девайсів;
- auto assign - привласнення ліній в автоматичному режимі.

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#telephony-service
Router(config-telephony)#max-dn 15
Router(config-telephony)#max-ephones 15
Router(config-telephony)#ip source-address 192.168.0.1 port 3100
Router(config-telephony)#auto assign 1 to 19
*Jun 6 22:33:09.691: CEF-HWIDB: EDSP0 LES switching vector set to Null
*Jun 6 22:33:09.691: CEF-HWIDB: EDSP0 switching vector set to Null
*Jun 6 22:33:09.695: CEF-HWIDB: EDSP0 LES switching vector set to CEF switching
*Jun 6 22:33:09.695: CEF-HWIDB: EDSP0 switching vector set to Null
Router(config-telephony)#auto assign 1 to 19
*Jun 23 22:33:10.687: %LINEPROTO-5-UPDOWN: Line protocol on Interface EDSP0, changed state to up
Router(config-telephony)#auto assign 1 to 19
Router(config-telephony)#
```

Рис. 3.29. Налаштовування додаткової опції 150

Тепер нарешті можна присвоїти телефонні номери нашим апаратам.

```
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ephone-dn 1
Router(config-ephone-dn)# number 11111
Router(config-ephone-dn)# exit
Router(config)# ephone-dn 2
Router(config-ephone-dn)# number 2222
Router(config-ephone-dn)# exit
Router(config)# ephone-dn 3
Router(config-ephone-dn)# number 3333
Router(config-ephone-dn)# exit
*Jun 23 22:50:13.171: %LINK-3-UPDOWN: Interface ephone_dsp DN 1.1, changed state to up
*Jun 23 22:50:13.479: %LINK-3-UPDOWN: Interface ephone_dsp DN 2.1, changed state to up
*Jun 23 22:50:13.487: %LINK-3-UPDOWN: Interface ephone_dsp DN 3.1, changed state to up
Router(config-ephone-dn)# exit
Router(config)#
```

Рис. 3.30. Налаштування номерів на ір-телефонах

Для налаштування WLC підключаємося по серійному порту і здійснюємо основну конфігурацію, щоб потім підключитися по Http для подальшої

конфігурації. Хоч наш контролер і управляється через командний рядок (консоль, ssh), майже всі операції по налаштуванню краще (швидше і зручніше) здійснювати через веб-інтерфейс. Контролер доступний через HTTP (за замовчуванням) з логіном-паролем, заданими при установці. Кожна бездротова мережа ідентифікується унікальним ім'ям, або SSID. Всі настройки проводяться в меню WLANs. Для створення нової мережі необхідно вибрати пункт меню «Create new», і задати базові параметри.

Рис. 3.31. Створення нової безпроводної мережі

Створивши нову мережу, ми потрапляємо в вікно з закладками: General, Security, QoS, Advanced; в якому і вказуються всі параметри її роботи. Наступний крок - підключити до контролера наявні точки доступу, які і будуть обслуговувати Wi-fi-клієнтів. Легкі точки доступу автоматично виявляють адресу WLC.

| AP Name                    | IP Address(Ipv4/Ipv6) |
|----------------------------|-----------------------|
| Light Weight Access Point1 | 192.168.1.3           |
| Light Weight Access Point0 | 192.168.1.2           |

Рис. 3.32. Виявленні контролером точки доступу

### 3.3. Тестування налаштувань

Тестування підсистеми мережі проводиться з метою перевірки налаштувань на відповідність та працездатність.

Першим, що провінимо це доступ до глобальної мережі та роботу DHCP сервера.

```
PC2> ping 8.8.8.8
84 bytes from 8.8.8.8 icmp_seq=1 ttl=64 time=1.293 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=64 time=1.489 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=64 time=1.421 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=64 time=1.624 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=64 time=1.501 ms
```

Рис. 3.33. Перевірка доступу до глобальної мережі

```
PC6> ip dhcp
DDORA IP 192.168.122.219/24 GW 192.168.122.1
PC6>
```

Рис. 3.34. Перевірка працездатності DHCP сервера

Тепер потрібно перевірити наявність зв'язку з філіями по VPN, для цього з тої ж віртуальної мережі за допомогою команди «ping» протестуємо доступність двох філій нашого підприємства.

```
PC2> ping 192.168.1.239
84 bytes from 192.168.1.239 icmp_seq=1 ttl=255 time=22.758 ms
84 bytes from 192.168.1.239 icmp_seq=2 ttl=255 time=17.806 ms
84 bytes from 192.168.1.239 icmp_seq=3 ttl=255 time=8.008 ms
84 bytes from 192.168.1.239 icmp_seq=4 ttl=255 time=6.316 ms
84 bytes from 192.168.1.239 icmp_seq=5 ttl=255 time=7.860 ms

PC2> ping 192.168.1.147
192.168.1.147 icmp_seq=1 timeout
84 bytes from 192.168.1.147 icmp_seq=2 ttl=255 time=13.611 ms
84 bytes from 192.168.1.147 icmp_seq=3 ttl=255 time=7.611 ms
84 bytes from 192.168.1.147 icmp_seq=4 ttl=255 time=6.765 ms
84 bytes from 192.168.1.147 icmp_seq=5 ttl=255 time=6.293 ms
```

Рис. 3.35. Результат тестування доступності сусідніх офісів

Також потрібно перевірити віддалений доступ до мережного обладнання за протоколом SSH. При підключенні потрібно пройти авторизацію, що є одною з політик безпеки.

```
SW_ACC#ssh -v 2 -l adminer 192.168.1.147
Password:
SW_main#
```

Рис. 3.36. Результат тестування доступності віддаленого доступу до комутатора SW\_main

Для перевірки коректності налаштувань ір-телефонії був використаний програмний додаток «Cisco Packet Tracer». Зі скриншоту нижче видно, що телефон з номером 2222 приймає дзвінок від телефону з номером 1111.

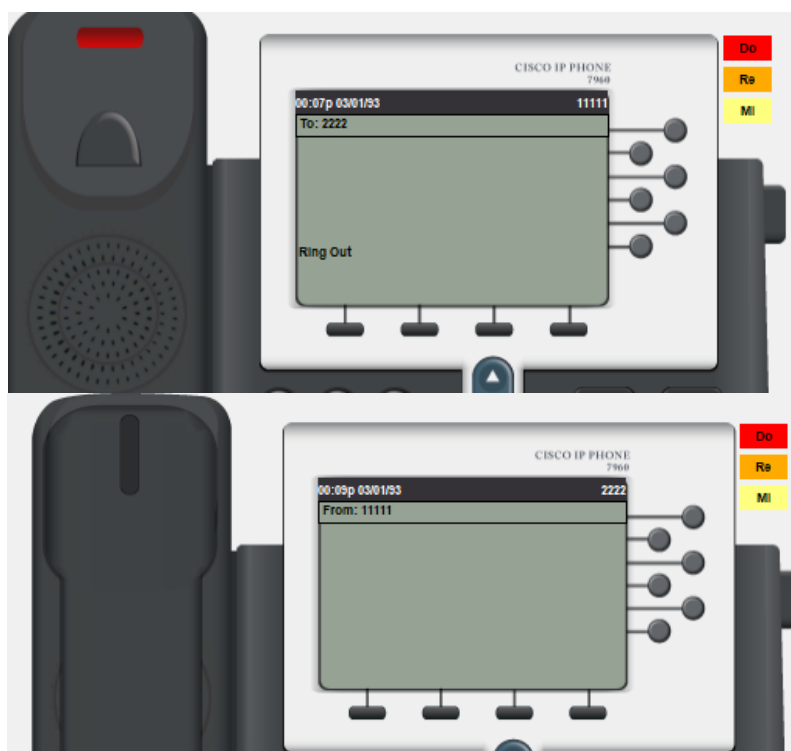


Рис. 3.37-3.38. Результат тестування налаштувань ір-телефонії

Для тестування безпроводної мережі було змодельовано спрощену схему.

Кінцеві пристрої з безпроводними модулями успішно з'єдналися з точками доступу та отримали ір-адреси, це можна побачити на рис. 3.39-3.40.

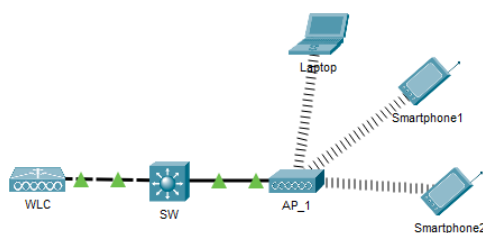


Рис. 3.39. Спрощенна схема безпроводної мережі

|                                       |                                           |                 |
|---------------------------------------|-------------------------------------------|-----------------|
| SSID                                  |                                           | corp_net        |
| Authentication                        |                                           |                 |
| <input type="radio"/> Disabled        | <input type="radio"/> WEP                 | WEP Key         |
| <input type="radio"/> WPA-PSK         | <input checked="" type="radio"/> WPA2-PSK | PSK Pass Phrase |
|                                       |                                           | 12345678        |
| <input type="radio"/> WPA             | <input type="radio"/> WPA2                | User ID         |
|                                       |                                           | Password        |
| <input type="radio"/> 802.1X          | Method:                                   | MD5             |
|                                       |                                           | User Name       |
|                                       |                                           | Password        |
| Encryption Type                       |                                           | AES             |
| IP Configuration                      |                                           |                 |
| <input checked="" type="radio"/> DHCP |                                           |                 |
| <input type="radio"/> Static          |                                           |                 |
| IP Address                            |                                           | 192.168.1.8     |
| Subnet Mask                           |                                           | 255.255.255.0   |

Рис. 3.40. Кінцеві пристрої отримали доступ до безпроводної мережі

## ВИСНОВКИ

Під час виконання випускної роботи було вирішено наступні завдання:

1. Обґрунтовано актуальність даної системи захисту та описана сфера її використання;

2. Обрано усі необхідні засоби для реалізації системи: виробника обладнання, конкретні моделі обладнання, методи та технології розподілу IP-адрес, методи захисту мереж від зовнішнього зловмисного впливу, симулятор роботи з мережним обладнанням, продукти віртуалізації для операційних систем;

3. Наведено приклади налаштування основних процесів роботи гетерогенної мережі та їх детальний опис;

4. Розглянуто реалізацію основних функцій захисту системи, таких як трансляція адрес, віртуальні приватні мережі, парольний доступ до мережного обладнання;

5. Налаштовано, досліджено та проаналізовано об'єднання дротових мереж, Wi-Fi та IP-телефонії.

Реалізована мережа є повністю готовим макетом реальної реалізації проекту. Конфігурації можуть бути застосовані для налаштування реального обладнання мережі.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Компьютерные сети. Принципы, технологии, протоколы / В. Олифер, Н. Олифер. – СПб: Питер, 2016. – 992 с. – (Серия «Учебник для вузов»).
2. Guide to Networks / Jill West, Tamara Dean, Jean Andrews, 2016. – 783 с.
3. Cisco Bring Your Own Device (BYOD). Release 2.2, 2013. – 338 с.
4. Enterprise Campus 3.0 Architecture: Overview and Framework, 2008. – 54 с.
5. Designing Cisco Network Service Architectures. Foundation Learning Guide, 2012. – 733 с.
6. Campus LAN and Wireless LAN Design Guide, 2018. – 60 с.
7. Cisco Enterprise Campus Infrastructure. Best Practices Guide, 2014. – 45 с.
8. Medium Enterprise Design Profile Reference Guide, 2010. – 376 с.
9. Next Generation Enterprise Branch Security CVD System Assurance Guide, 2007. – 146 с.
10. Подключение точек доступа к контроллеру Cisco Wi-Fi [Электронный ресурс] – Режим доступа до ресурсу: <https://habr.com/ru/post/145677/>
11. Настройка беспроводных сетей на контроллере Cisco [Электронный ресурс] – Режим доступа до ресурсу: <https://habr.com/ru/post/148903/>
12. Практика подключения телефонов Cisco [Электронный ресурс] – Режим доступа до ресурсу: <http://ciscomaster.ru/node/89>
13. НАСТРОЙКА CISCO PACKET TRACER ДЛЯ VOIP [Электронный ресурс] / – 2018. – Режим доступа до ресурсу: <https://wiki.merionet.ru/ip-telephonya/62/nastrojka-cisco-packet-tracer-dlya-voip/>
14. Cisco Wireless Controller Configuration Guide, Release 8.5 [Электронный ресурс] – Режим доступа до ресурсу: [https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b\\_cg85/ap\\_connectivity\\_to\\_cisco\\_wlc.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/ap_connectivity_to_cisco_wlc.html)
15. Cisco Wireless LAN Controller (WLC) Basic Configuration [Электронный ресурс] – Режим доступа до ресурсу: <https://networklessons.com/cisco/ccna-200-301/cisco-wireless-lan-controller-wlc-basic-configuration>

|  |  |  |  |  |                          |    |
|--|--|--|--|--|--------------------------|----|
|  |  |  |  |  | КИК.КР.Б – 123 – 20 – ПЗ |    |
|  |  |  |  |  |                          |    |
|  |  |  |  |  |                          | 70 |

16. Азы IP-телефонии от Cisco или знакомство с Cisco CallManager Express [Электронный ресурс] – Режим доступа до ресурсу: <https://habr.com/ru/post/124411/>

17. Настройка коммутатора Cisco и Voice VLAN (на примере Cisco 2960 и Cisco SPA-502) [Электронный ресурс] – Режим доступа до ресурсу: <https://voxlink.ru/kb/voip-devices-configuration/cisco-linux-vlan-trunk-configuration/>

18. Руководство администратора телефона Cisco IP серии 7800 для Cisco Unified Communications Manager [Электронный ресурс] – Режим доступа до ресурсу: [https://www.cisco.com/c/ru\\_ru/td/docs/voice\\_ip\\_comm/cuipph/7800-series/english/admin-guide/pa2d\\_b\\_7800-series-admin-guide-cucm/pa2d\\_b\\_7800-series-admin-guide-cucm\\_chapter\\_0100.html](https://www.cisco.com/c/ru_ru/td/docs/voice_ip_comm/cuipph/7800-series/english/admin-guide/pa2d_b_7800-series-admin-guide-cucm/pa2d_b_7800-series-admin-guide-cucm_chapter_0100.html)

19. ДОСТУП ПО SSH НА CISCO IOS [Электронный ресурс] – Режим доступа до ресурсу: <https://deltaconfig.ru/ssh-on-cisco-router/>

20. Virtual LAN [Электронный ресурс] – Режим доступа до ресурсу: [https://en.wikipedia.org/wiki/Virtual\\_LAN](https://en.wikipedia.org/wiki/Virtual_LAN)

21. WPA2-Enterprise, или правильный подход к безопасности Wi-Fi сети [Электронный ресурс] – Режим доступа до ресурсу: <https://habr.com/ru/post/150179/>

22. Wi-Fi Protected Access [Электронный ресурс] – Режим доступа до ресурсу: [https://en.wikipedia.org/wiki/Wi-Fi\\_Protected\\_Access](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access)

23. DHCP [Электронный ресурс] – Режим доступа до ресурсу: <https://uk.wikipedia.org/wiki/DHCP>

24. Коммутаторы Cisco Catalyst серии 2960-S [Электронный ресурс] – Режим доступа до ресурсу: [https://www.cisco.com/c/ru\\_ru/support/switches/catalyst-2960-s-series-switches/series.html#~tab-documents](https://www.cisco.com/c/ru_ru/support/switches/catalyst-2960-s-series-switches/series.html#~tab-documents)

# ДОДАТКИ

|  |  |  |  |  |                          |    |
|--|--|--|--|--|--------------------------|----|
|  |  |  |  |  | КІК.КР.Б – 123 – 20 – ПЗ |    |
|  |  |  |  |  |                          |    |
|  |  |  |  |  |                          | 72 |

## Додаток А

### Топологія мережі

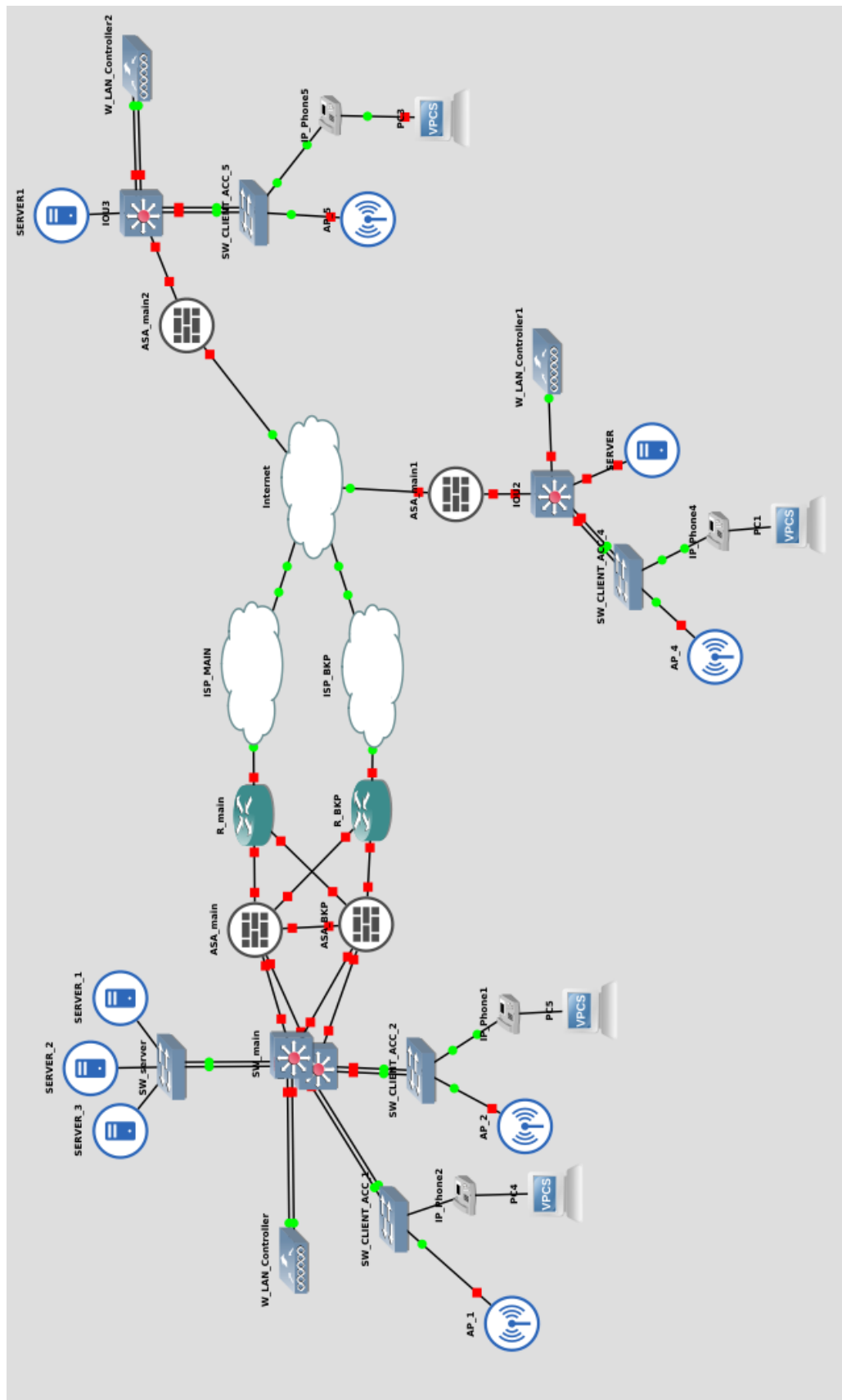


Рис. А.1. Топологія мережі