Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

здобувача Барзенець Данила Андрійовича
(ПІБ)

академічної групи 123-22ск-1
(шифр)

спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

за освітньо-професійною програмою Комп'ютерна інженерія
(офіційна назва)

на тему «Комп'ютерна система центра надання адміністративних послуг з детальною розробкою контейнеризованого застосунку збору та аналізу телеметричних даних»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Молодець Б.В.			
спеціальної частини	доц. Молодець Б.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2025

ЗАТВЕРДЖЕНО:

завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)
« » _____ 2025 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

здобувача Барзенець Д. А. **академічної групи** 123-22ск-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія

за освітньо-професійною програмою Комп'ютерна інженерія
(офіційна назва)

на тему «Комп'ютерна система центра надання адміністративних послуг з детальною розробкою контейнеризованого застосунку збору та аналізу телеметричних даних»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 05.05.2025 № 336-с

Розділ	**Зміст**	**Термін виконання**
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел виконати огляд існуючих рішень для моніторингу навантаження на порти комутаторів	11.05.2025
Розробка апаратної частини	Розробити вимоги до функцій, виконуваними системою	18.05.2025
Розробка корпоративної мережі	Побудувати в Packet Tracer модель корпоративної мережі ЦНАП, виконати налаштування та перевірку роботи системи	25.05.2025
Розробка компонента системи	Розробити рішення для виявлення перевантажених портів на базі мережевого обладнання Cisco Catalyst 9000	01.06.2025

Завдання видано _____ доц. Молодець Б.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі 25.02.2025

Дата подання до екзаменаційної комісії 20.06.2025

Прийнято до виконання _____ Барзенець Д.А.
(підпис здобувача) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 64 с., 30 рис., 5 табл., 2 додатки, 11 джерел.

ЦНАП, ТЕЛЕМЕТРІЯ, CISCO CATALYST 9300, IOX, DOCKER, INFLUXDB, FLASK, TELEMETRYRECEIVER, DEVNET SANDBOX.

Об’єкт професійної діяльності − комп’ютерна система центру надання адміністративних послуг (ЦНАП), зокрема комутаційноме обладнання Cisco Catalyst 9300 із підтримкою контейнерних технологій.

Мета роботи − реалізація та впровадження контейнеризованого застосунку для збору, аналізу та візуалізації телеметричних даних із комутатора Cisco Catalyst 9300, з використанням SNMP-протоколу та внутрішнього хостингу додатків на платформі Cisco IOx.

У результаті вирішення поставлених задач:

– побудовано структурну модель комп’ютерної мережі ЦНАП із логічним розподілом VLAN, маршрутизацією, NAT та безпековими політиками;

– розроблено застосунок мовою Python, що реалізує збір телеметрії з портів комутатора, її збереження у базі даних InfluxDB та надання користувачу через веб-інтерфейс, створений на Flask;

– реалізовано контейнеризацію застосунку з використанням Docker та підготовлено архів для інсталяції через Cisco IOx;

– виконано розгортання у середовищі Cisco Catalyst 9300 Always-On Sandbox.

Розроблений контейнер протестовано у публічному середовищі Cisco DevNet, підтверджено працездатність рішення у режимі реального часу, що свідчить про можливість його впровадження у реальних інфраструктурах центрів надання адміністративних послуг або інших установ.

Рішення може бути використано для організації централізованого моніторингу у державних установах, навчальних закладах та корпоративних мережах.

ЗМІСТ

Перелік скорочень, умовних познак, символів, одиниць і термінів 7
Вступ 8
1 Стан питання і постановка завдання 9
1.1 Стисла характеристика галузі та умов застосування комп'ютерної системи центра надання адміністративних послуг 9
1.2 Стислі відомості про топологічне розміщення структурних підрозділів ЦНАП та технології збору і передачі інформації 12
1.3 Розробка схеми організаційної структури ЦНАП 15
1.4 Огляд існуючих рішень для моніторингу навантаження на порти комутаторів 18
1.5 Обґрунтування вибраного напрямку інженерного рішення 20
1.6 Завдання і мета роботи 21
2 Спеціальний розділ 23
2.1 Технічні вимоги до КС ЦНАП 23
2.1.1 Найменування і призначення КС ЦНАП 23
2.1.2 Вимоги до структури і функціонуванню системи 23
2.1.2.1 Перелік підсистем, їх призначення та основні характеристики 23
2.1.2.2 Вимоги до способів і засобів зв'язку між компонентами комп'ютерної системи 25
2.1.2.3 Вимоги до режимів функціонування системи 26
2.1.3 Вимоги до видів забезпечення комп'ютерної системи 26
2.1.3.1 Вимоги до математичного забезпечення 26
2.1.3.2 Вимоги до інформаційного забезпечення 27
2.1.3.3 Вимоги до технічного забезпечення 27
2.1.3.4 Вимоги до організаційного забезпечення 27

2.1.3.5 Вимоги до методичного забезпечення 27
2.2 Розробка апаратної частини комп'ютерної системи 27
2.2.1 Розробка загальної архітектури мережі підприємства 27
2.2.2 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи 29
2.2.3 Розробка специфікації апаратних засобів комп'ютерної системи 32
3 Розробка корпоративної мережі ЦНАП 33
3.1 Розробка фізичної топологої 33
3.2 Розробка логічної топології 35
3.3 Розрахунок схеми адресації мережі 37
3.3.2 Вибір та налаштування способу маршрутизації 38
3.3.3 Налаштування мереж VLAN, маршрутизації між VLAN 40
3.3.4 Вибір і налаштування службових мережевих сервісів 42
3.4 Налаштування обладнання відповідно до вимог безпеки ЦНАП 44
3.4.1 Запобігання підміни DHCP-сервера: DHCP-Snooping 45
3.4.2 Зміна native VLAN за замовчуванням 45
3.4.3 Захист на рівні доступу: Port Security 46
3.4.4 Захист від ARP-спуфінгу за допомогою Dynamic ARP Inspection 49
3.4.5 Захист від широкомовних штормів за допомогою Storm Control . 50
3.4.6 Захищене з'єднання віддалених співробітників 51
3.4.7 Контроль доступу до зовнішніх державних сервісів 52
3.4.8 Аудит безпеки та журналювання подій 53
3.5 Тестування та перевірка працездатності розробленої мережі 53
4 Розробка контейнеризованого застосунку для збору та аналізу телеметричних даних 55
4.1 Обґрунтування вибору архітектури 55
4.2 Середовище розгортання 56
4.3 Вибір засобів розробки 57
4.4 Структура та функціонування застосунку 57
4.5 Створення контейнера 58

4.6 Розгортання контейнерного застосунку на комутаторі Cisco 9300 58
4.7 Вивід телеметричних даних 59
4.8 Тестування та результати 60
Висновки 62
Перелік джерел посилання 63
Додаток А. Текст програми налаштування комутатора SW_R1 65
Додаток Б. Текст програми застосунку для збору телеметричних даних для Cisco Catalyst 9300.....71

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ЦНАП – центр надання адміністративних послуг;

СЕД – систему електронного документообігу

КС – комп’ютерна система;

API – англ. Application Programming Interface – інтерфейс прикладного програмування;

CLI – англ. Command Line Interface, інтерфейс командного рядка;

JSON – англ. JavaScript Object Notation, формат представлення структурованих даних;

Cisco IOX – платформа для розгортання контейнеризованих застосунків безпосередньо на мережевому обладнанні Cisco

ВСТУП

Сфера надання адміністративних послуг в Україні постійно розвивається, зокрема завдяки впровадженню цифрових технологій. Центри надання адміністративних послуг (ЦНАП) забезпечують громадянам доступ до різноманітних послуг, таких як реєстрація бізнесу, отримання дозволів, оформлення документів тощо.

Сучасні корпоративні мережі є основою для забезпечення безперебійної роботи бізнес-процесів, обміну даними та доступу до інформаційних ресурсів. Зі зростанням обсягів трафіку, кількості підключених пристроїв та вимог до продуктивності мережі, виникає необхідність у впровадженні ефективних рішень для моніторингу та управління мережевою інфраструктурою. Особливу увагу приділяють комутаторам, які є ключовими елементами мережі, що забезпечують з'єднання між сегментами мережі та кінцевими пристроями.

У зв’язку з цим виникає потреба у моніторингу навантаження на мережеві порти, що дозволить запобігти перевантаженням, простоям та забезпечувати оптимальну продуктивність мережі ЦНАП.

Основною метою роботи є розробка контейнеризованого застосунку, що дозволить збирати телеметричні дані з комутаторів у реальному часі, аналізувати їх та оперативно реагувати на проблеми.

Основні завдання роботи:

– розробити архітектуру застосунку для збору та аналізу телеметричних даних;

– реалізувати модулі збору даних, аналізу та створення сповіщень;

– створити алгоритм аналізу навантаження;

– забезпечити інтеграцію з системами моніторингу;

– розробити механізм сповіщень про перевантаження портів.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування комп’ютерної системи центра надання адміністративних послуг

У сучасному суспільстві, де ефективність та доступність державних послуг відіграють ключову роль у розвитку громадянського суспільства та економіки, комп'ютерні системи центрів надання адміністративних послуг (ЦНАП) стають невід'ємною частиною процесу взаємодії громадян з державою. ЦНАП – це інституція, створена з метою забезпечення зручного та прозорого доступу до адміністративних послуг, що надаються різними органами державної влади та місцевого самоврядування. Згідно з новим законодавством “Центр надання адміністративних послуг – це постійно діючий робочий орган або виконавчий орган (структурний підрозділ) органу місцевого самоврядування або місцевої державної адміністрації, що зазначені у частині другій цієї статті, в якому надаються адміністративні послуги згідно з переліком, визначеним відповідно до цього Закону ” (ч. 1 ст. 12 Закону України “Про адміністративні послуги” від 06.08.2012 р.) [1].

Головні характеристики ЦНАП:

– достатній перелік послуг, який включає найбільш важливі та популярні послуги серед громадян; доступ до повної інформації про всі адміністративні послуги в ЦНАП, у тому числі через мережу Інтернет;

– комфортне приміщення та некабінетна система обслуговування (зони прийому, інформування, очікування й обслуговування);

– консультування, прийом документів і видача оформлених результатів адміністративних послуг через одну посадову особу – адміністратора;

– контроль за строками оформлення адміністративних послуг через адміністратора;

– зручні години прийому відвідувачів;

– зручності для людей з особливими потребами.

Галузь, яку охоплюють ЦНАП, надзвичайно широка та постійно розширюється, включаючи реєстрацію бізнесу, нерухомості, видачу документів, ліцензування, соціальні послуги, реєстрація підприємницької діяльності тощо.

Ключовою характеристикою галузі є її клієнтоорієнтованість. Основна мета діяльності ЦНАП полягає в спрощенні процедур, зменшенні часових витрат та підвищенні задоволеності громадян від отримання адміністративних послуг. Цього досягають завдяки принципам "єдиного вікна", коли заявник подає документи та отримує результат через одного оператора, і "єдиного офісу", що передбачає надання комплексу послуг в одному місці. Такий підхід мінімізує бюрократичні перепони та знижує корупційні ризики.

Комп'ютерна система ЦНАП є ядром його функціонування. Вона забезпечує автоматизацію процесів прийняття та обробки документів, моніторинг термінів надання послуг, ведення електронного документообігу та забезпечення зручного онлайн-доступу для громадян. Основні компоненти такої системи включають:

– електронний кабінет заявника для подачі документів, відстеження статусу заявки та отримання результатів онлайн;

– систему управління чергою, що оптимізує процес обслуговування клієнтів в офісі ЦНАП;

– систему електронного документообігу (СЕД), що забезпечує автоматизований обмін документами між ЦНАП та органами, що надають послуги;

– база даних, що містить інформацію про заявників, надані послуги, стан розгляду заявок та інші релевантні дані;

– інтеграцію з іншими державними реєстрами та базами даних для перевірки достовірності інформації та обміну даними між відомствами;

– система аналітики та звітності для моніторингу ефективності роботи ЦНАП та прийняття обґрунтованих управлінських рішень.

Впровадження та ефективне використання комп'ютерних систем ЦНАП є важливим кроком до побудови сучасної та ефективної системи надання адміністративних послуг, що сприяє підвищенню прозорості, зменшенню корупції та підвищенню рівня довіри громадян до державних органів.

Умови застосування комп’ютерної системи ЦНАП залежать від багатьох факторів, включаючи обсяг послуг, кількість населення, технічну інфраструктуру та фінансові можливості. Ефективне впровадження та використання системи вимагає:

– наявності кваліфікованого персоналу, оператори ЦНАП повинні володіти навичками роботи з комп'ютерною технікою та програмним забезпеченням;

– надійної технічної інфраструктури для забезпечення безперебійного доступу до Інтернету, наявності серверного обладнання та комп'ютерної техніки;

– забезпечення системи захисту інформації від несанкціонованого доступу та кібератак;

– інтеграцію з іншими державними системами для забезпечення сумісності та обміну даними;

– постійної підтримки та оновлення системи для забезпечення її актуальності та відповідності законодавчим вимогам.

Комп’ютерна система (КС), що використовується в ЦНАП, включає серверну інфраструктуру, робочі станції персоналу, мережеве обладнання та засоби кібербезпеки. В умовах великого навантаження на систему важливим є її стабільне функціонування, що забезпечується впровадженням механізмів моніторингу та аналізу продуктивності.

Умови застосування комп'ютерної системи (КС) включають:

– високий обсяг запитів від громадян;

– необхідність інтеграції з державними реєстрами та базами даних;

– потреба в забезпеченні безпеки та конфіденційності даних.

1.2 Стислі відомості про топологічне розміщення структурних підрозділів ЦНАП та технології збору і передачі інформації

Топологічне розміщення структурних підрозділів ЦНАП визначає ефективність організації роботи та забезпечення зручності для відвідувачів. Основними компонентами топології є:

а) Головний офіс ЦНАП. Зазвичай у центральній будівлі розташовані основні функціональні підрозділи, зокрема адміністративний відділ, відділ надання адміністративних послуг, юридичний та фінансовий відділи. Це створює зручність для координації роботи та швидкого ухвалення рішень. На рисунку 1.2 наведено офіси ЦНАП в м. Дніпро.

б) Територіальні підрозділи. ЦНАП може мати декілька територіальних підрозділів, які забезпечують доступ до послуг у різних районах. Це дає змогу скоротити час на подорож до ЦНАП, сприяючи більшій доступності послуг для населення. На рисунку 1.2 наведено територіальні підрозділи ЦНАП в м. Дніпро.

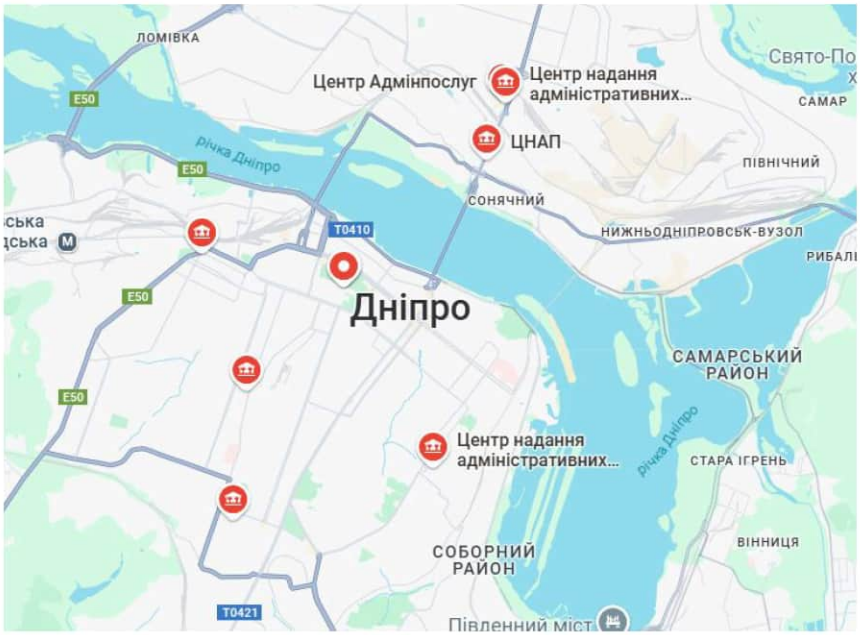

Рисунок 1.1 – Територіальні підрозділи ЦНАП в м. Дніпро

в) Віддалені робочі місця адміністраторів. Віддалені робочі місця для адміністраторів дозволяють здійснювати обробку заявок прямо в територіальних громадах. Це рішення спрощує доступ до адміністративних послуг і зменшує навантаження на центральний офіс.

Приміщення ЦНАП зазвичай передбачає створення функціональних зон, орієнтованих на зручність клієнтів та ефективність обробки запитів. Це включає зони прийому та консультацій, зони обробки документів, зони очікування та, можливо, зони самообслуговування. Типовий план приміщення ЦНАП наведено на рисунку 1.2.

Рисунок 1.2 – План приміщення ЦНАП

Зал 1 – сектор надання адміністративних послуг відділу.

Зал 2 – сектор дозвільних процедур відділу.

Зал 3 – сектор надання послуг виконавчих органів ради відділу.

Зал 5 – паспортний відділ.

Для забезпечення ефективної роботи ЦНАП використовуються сучасні технології збору та передачі інформації. Основні технологічні рішення включають:

а) Інформаційні системи. Використовуються системи управління даними, які дозволяють автоматизувати процеси обробки заявок і отримання статистики. Ці системи забезпечують швидкий доступ до даних та зменшують ймовірність людських помилок.

б) Електронні реєстраційні платформи. Громадяни можуть подавати заявки на адміністративні послуги через веб-портал, що спрощує процес

звернення і дозволяє уникати черг. Також передбачається можливість онлайн-консультацій.

в) Мережеві технології. Використання локальної та глобальної мережі для передачі даних між підрозділами ЦНАП. Це передбачає належну організацію Wi-Fi та LAN-мереж, що забезпечує стабільний доступ до інформаційних систем у всіх підрозділах.

г) Системи моніторингу. Постійний моніторинг навантаження на мережеві ресурси дозволяє виявляти проблеми в режимі реального часу, що веде до оперативного реагування на збої та запобігання затримкам у наданні послуг.

д) Інтерфейси для обміну даними. Впровадження API для інтеграції з іншими державними реєстрами та базами даних. Це забезпечує автоматичну перевірку даних, що знижує навантаження на адміністраторів та підвищує якість обслуговування.

Технології збору та передачі інформації базуються на принципах інтеграції інформаційних систем різних органів влади. Збір інформації здійснюється через веб-портал ЦНАП, системи електронного документообігу, та особисте звернення. Передача даних відбувається захищеними каналами зв'язку, із використанням електронного цифрового підпису та протоколів шифрування, забезпечуючи конфіденційність та цілісність інформації.

Умови застосування КС характеризуються високими вимогами до доступності та продуктивності мережевих сервісів, а також необхідністю забезпечення безпеки інформації.

Мережа підприємства складається з декількох підмереж, з'єднаних комутатором Cisco Catalyst 9000 (рис. 1.3). Ця серія підтримує програмування через Cisco IOS XE, що дозволяє використовувати такі технології, як:

– Python Scripting для запуску Python-скриптів для автоматизації задач;
– REST API для управління та моніторингу пристроїв;
– NETCONF/YANG для конфігурації та управління через XML.

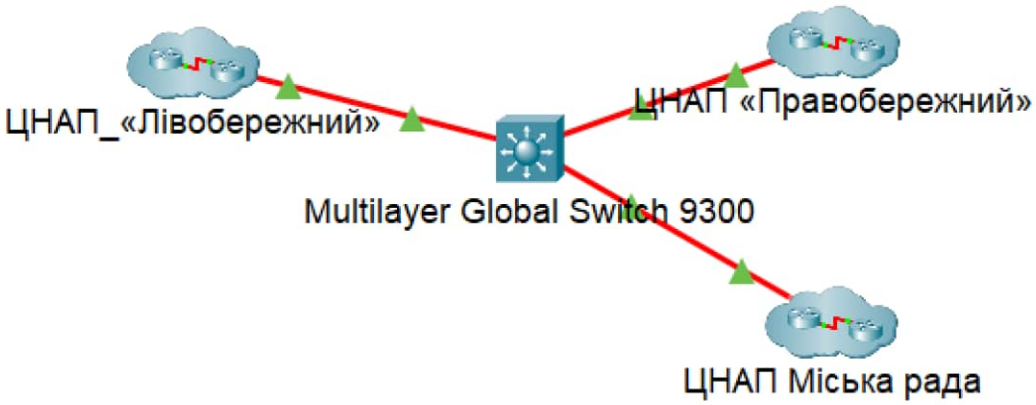

Рисунок 1.3 – Мережа філіалів ЦНАП

1.3 Розробка схеми організаційної структури ЦНАП

Загальна структура ЦНАП визначається як єдиний комплекс організаційних і технологічних засобів надання адміністративних послуг суб'єктам звернень, що включає відділи ЦНАП, територіальні підрозділи ЦНАП та віддалені робочі місця адміністраторів ЦНАП.

Ефективна організаційна структура ЦНАП є критичною для забезпечення якісного та своєчасного надання послуг.

Типова організаційна структура ЦНАП, як правило, передбачає наявність керівництва (директор, заступник), адміністраторів, спеціалістів з різних напрямків (наприклад, державна реєстрація, реєстрація бізнесу, соціальні послуги), а також підрозділи забезпечення (бухгалтерія, IT-підтримка) (рис. 1.4).

Керівник ЦНАП відповідно до завдань, покладених на ЦНАП [2]:

– здійснює керівництво роботою ЦНАП, несе персональну відповідальність за організацію діяльності ЦНАП;

– організовує діяльність ЦНАП, у тому числі щодо взаємодії з суб’єктами надання адміністративних послуг, вживає заходів щодо підвищення ефективності роботи ЦНАП;

– організовує інформаційне забезпечення роботи ЦНАП, роботу із засобами масової інформації, визначає зміст та час проведення інформаційних

заходів;

– сприяє створенню належних умов праці у ЦНАП, вносить пропозиції керівництву Департаменту щодо матеріально-технічного забезпечення ЦНАП;

– розглядає скарги на діяльність чи бездіяльність адміністраторів.

Рисунок 1.4 – Організаційна структура ЦНАП

Начальники відділів ЦНАП (далі – відділи) відповідно до завдань, покладених на відділи:

– здійснюють керівництво роботою відділів;

– несуть персональну відповідальність за організацію діяльності;

– організовують діяльність відділів, у тому числі взаємодію з суб'єктами надання адміністративних послуг, вмивають заходів щодо підвищення ефективності роботи відділів;

– контролюють якість та своєчасність виконання адміністраторами відділів своїх обов'язків;

– забезпечують належні умови праці у відділах;

– вносять пропозиції керівництву Департаменту, управління щодо матеріально-технічного забезпечення відділів.

– можуть здійснювати функції адміністратора.

Основні завдання адміністраторів:

– надання суб'єктам звернень вичерпної інформації та консультацій

щодо вимог та порядку надання адміністративних послуг;

– прийняття від суб'єктів звернень документів, необхідних для отримання ними адміністративних послуг, їх реєстрація та подання документів (їх копій) відповідним суб'єктам надання адміністративних послуг не пізніше наступного робочого дня після їх отримання з дотриманням вимог Закону України «Про захист персональних даних»;

– видача або забезпечення надсилання через засоби поштового або телекомунікаційного зав'язків суб'єктам звернень результатів надання адміністративних послуг (у тому числі рішення про відмову в задоволенні заяви суб'єкта звернення), повідомлення про можливість отримання адміністративних послуг, оформлених суб'єктами надання адміністративних послуг;

– організаційне забезпечення надання адміністративних послуг субєктами їх надання;

– складання протоколів про адміністративні правопорушення у випадках, передбачених законодавством;

– здійснення контролю за додержанням суб'єктами надання адміністративних послуг строку розгляду справ та прийняття рішень.

Організаційна структура включає IT-відділ, який відповідає за підтримку мережевої інфраструктури, та відділ розробки, який займається створенням програмного забезпечення. IT-відділ складається з мережевих інженерів, які забезпечують налаштування та моніторинг мережі.

При розробці схеми важливо враховувати принципи клієнтоорієнтованості, прозорості та підзвітності. Організаційна структура повинна сприяти швидкому та ефективному вирішенню питань, мінімізувати бюрократичні перешкоди та забезпечувати високий рівень задоволеності громадян.

1.4 Огляд існуючих рішень для моніторингу навантаження на порти комутаторів

Одночасно сфера моніторингу та управління мережами підприємств є критично важливою для забезпечення безперебійної роботи бізнес-процесів. Зростаюча складність мережевої інфраструктури, збільшення обсягів трафіку та вимоги до високої доступності сервісів вимагають ефективних інструментів для моніторингу та аналізу навантаження на мережеві пристрої. Особливо важливим є моніторинг комутаторів, які є ключовими елементами мережі, що забезпечують з'єднання між різними сегментами та пристроями.

Основними проблемами сучасних корпоративних мереж є:

– відсутність оперативного моніторингу навантаження на порти;

– неможливість швидкого виявлення вузьких місць мережевої інфраструктури;

– брак інструментів для прогнозування мережевих інцидентів;

– складність збору та аналізу телеметричних даних з мережевого обладнання.

В ЦНАП спостерігаються періодичні затримки в роботі мережевих сервісів, що призводить до уповільнення процесу надання адміністративних послуг, збільшення черг, а також зростання рівня невдоволення серед відвідувачів.

Однією з причин є перевантаження окремих портів комутаторів Cisco Catalyst 9000, що призводить до втрати пакетів та збільшення затримки. Існуючі інструменти моніторингу не надають достатньо детальної інформації про навантаження на порти в реальному часі, що ускладнює виявлення та усунення проблем.

У галузі мережевих технологій активно розвиваються інструменти для аналізу навантаження на мережеві пристрої, виявлення перевантажень та оптимізації роботи мережі.

Існуючі інженерні рішення для моніторингу навантаження на порти комутаторів включають:

Існуючі рішення для моніторингу навантаження на порти комутаторів охоплюють широкий спектр технологій та підходів, від простих інструментів командного рядка до комплексних платформ управління мережею. Одним з найпоширеніших методів є використання Simple Network Management Protocol (SNMP), який дозволяє збирати дані про трафік, що проходить через кожен порт, включаючи кількість прийнятих та відправлених пакетів, швидкість передачі даних та рівень утилізації порту. Перевагами SNMP є його широка підтримка виробниками комутаційного обладнання, стандартизований формат даних та відносна легкість в інтеграції з існуючими системами моніторингу. Недоліком є потенційне навантаження на процесор комутатора при частому зборі даних, а також обмеженість у можливостях глибокого аналізу трафіку.

Іншим популярним рішенням є використання технології NetFlow (або її аналогів, таких як sFlow та J-Flow), яка дозволяє збирати статистику про потоки даних, що проходять через комутатор, включаючи джерела, призначення, протоколи та об'єми трафіку. NetFlow забезпечує більш детальну інформацію про трафік порівняно з SNMP, дозволяючи ідентифікувати "важкі" додатки, аномалії в трафіку та потенційні проблеми з безпекою. Однак, налаштування та конфігурація NetFlow потребує більше зусиль, а збір та аналіз даних можуть вимагати використання спеціалізованого програмного забезпечення. Крім того, NetFlow може спричинити значне навантаження на процесор комутатора, особливо при великих об'ємах трафіку, що потребує використання потужного обладнання.

Сучасні платформи управління мережею (NMS), такі як Cisco Prime Infrastructure, SolarWinds Network Performance Monitor, часто включають в себе вбудовані інструменти для моніторингу навантаження на порти комутаторів, використовуючи комбінацію різних технологій, таких як SNMP, NetFlow та власних протоколів. Ці платформи забезпечують візуалізацію даних у вигляді графіків та діаграм, дозволяючи швидко ідентифікувати проблеми та тренди в трафіку. Перевагами NMS є централізоване управління та моніторинг

усієї мережевої інфраструктури, автоматизація рутинних задач та можливість інтеграції з іншими системами управління IT-інфраструктурою. Недоліками є:

– висока вартість придбання та впровадження;

– необхідність навчання персоналу для ефективного використання платформи;

– високе навантаження на мережеві пристрої;

– складність налаштування;

– висока вартість ліцензій;

– відсутність гнучкості при адаптації під специфіку конкретної мережі;

– недостатня деталізація даних у реальному часі та складність інтеграції з існуючими системами.

Окрім вищезгаданих, існують також більш специфічні рішення, такі як аналізатори пакетів (Wireshark, tcpdump), які дозволяють захоплювати та аналізувати трафік, що проходить через конкретний порт. Ці інструменти корисні для діагностики конкретних проблем, але не підходять для постійного моніторингу навантаження.

Таким чином, сучасні інженерні рішення потребують адаптації до специфіки роботи ЦНАП. Для забезпечення безперервного контролю за портами комутаторів у реальному часі доцільною є розробка власного контейнеризованого застосунку, здатного інтегрувати SNMP-збір, аналіз та візуалізацію телеметричних даних без значного впливу на продуктивність мережі.

1.5 Обґрунтування вибраного напрямку інженерного рішення

Серія комутаторів Cisco Catalyst 9000 підтримує програмування через Cisco IOS XE. Використання API, Python та інших технологій дозволяє автоматизувати управління мережами та інтегрувати їх з іншими системами.

Серед можливих напрямків вирішення поставленого завдання – впровадження комплексної системи моніторингу на базі дорогих NMS-платформ (Cisco Prime Infrastructure, SolarWinds тощо), використання

сторонніх SaaS-рішень або розробка власного контейнеризованого застосунку. Ураховуючи вимоги ЦНАП до економічності, адаптивності та контролю над даними, оптимальним є шлях створення власного програмного рішення.

Вибраний напрямок інженерного рішення передбачає розробку контейнеризованого застосунку на базі:

– Docker – для ізоляції компонентів і забезпечення портативності розгортання;

– Python – як основної мови реалізації логіки збору даних (з використанням бібліотек pysnmp, requests, psutil);

– Prometheus – для збору метрик;

– Grafana – для візуалізації показників у реальному часі.

– гнучку архітектуру, придатну до масштабування та модифікації без зупинки сервісу;

– низьке навантаження на мережеву інфраструктуру завдяки ефективним алгоритмам опитування;

– можливість адаптації до специфіки конкретного обладнання (включаючи Catalyst 9300/9500);

– сумісність з відкритими стандартами телеметрії та мережевого моніторингу;

– повний контроль над логікою обробки, фільтрації та представлення даних.

Таким чином, запропонований підхід відповідає актуальним вимогам до ефективного управління мережевими ресурсами в інфраструктурі Центру надання адміністративних послуг та забезпечує технічну основу для підвищення якості надання електронних сервісів громадянам.

1.6 Завдання і мета роботи

Завданням даної кваліфікаційної роботи є розробка контейнеризованого застосунку для моніторингу навантаження на порти комутаторів Cisco Catalyst

9000, що дозволить виявляти перевантажені порти в реальному часі та оперативно реагувати на інциденти.

Метою роботи є підвищення ефективності моніторингу та управління мережевою інфраструктурою ЦНАП, зниження ризиків виникнення проблем з продуктивністю та забезпечення високої доступності мережних сервісів.

Основні завдання:

– сформувати технічні вимоги комп'ютерної мережі та до контейнеризованого застосунку з урахуванням особливостей роботи мережі ЦНАП;

– розробити архітектуру застосунку з використанням сучасних контейнерних технологій;

– розробити логічну та фізичну топології комп'ютерної мережі ЦНАП;

– вибір та налаштування мережевого обладнання, зокрема комутатора Cisco Catalyst 9300;

– впровадження сервісів маршрутизації, сегментації (VLAN), IP-адресації та додаткових заходів безпеки з урахування специфіки ЦНАП;

– розробка програмного застосунку для збору телеметрії з використанням протоколу SNMP;

– реалізація веб-інтерфейсу для відображення отриманої статистики;

– контейнеризація програмного рішення з використанням Docker;

– розгортання застосунку на комутаторі Cisco через платформу IOx;

– тестування рішення у лабораторному середовищі (Cisco DevNet Sandbox).

2 СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Технічні вимоги до КС ЦНАП

2.1.1 Найменування і призначення КС ЦНАП

Об’єктом професійної діяльності є комп’ютерна система Центру надання адміністративних послуг (ЦНАП) м. Дніпро, побудована з урахуванням сучасних вимог до безпеки, автоматизації та масштабованості мережевої інфраструктури.

Призначення комп’ютерної системи полягає у:

– забезпеченні стабільного функціонування IT-інфраструктури ЦНАП на основі керованих мережевих пристроїв серії Cisco Catalyst 9000, які підтримують програмування через Cisco IOS XE;

– створенні платформи для централізованого керування мережею із застосуванням API, мови Python та інших технологій автоматизації;

– інтеграції інфраструктури з електронними державними сервісами, системами документообігу, сервісами автентифікації та моніторингу;

– впровадженні власного контейнеризованого застосунку для збору, обробки та аналізу телеметричних даних з мережевих пристроїв у реальному часі з можливістю оперативного реагування на інциденти;

– побудові масштабованої та безпечної архітектури із сегментацією мережі, підтримкою VLAN, політик безпеки та засобів резервування;

– створенні умов для ефективної роботи працівників ЦНАП, а також забезпеченні високої якості обслуговування громадян.

Система реалізується відповідно до рекомендацій Cisco Smart Business Architecture (SBA) та принципів інституційного створення ЦНАП, визначених у рамках Програми «U-LEAD з Європою».

2.1.2 Вимоги до структури і функціонуванню системи

2.1.2.1 Перелік підсистем, їх призначення та основні характеристики

Комп’ютерна система ЦНАП у м. Дніпро має містити такі підсистеми.

а) Підсистема комутації та маршрутизації: забезпечення комунікації між сегментами мережі, підтримка VLAN та політик безпеки. Заснована на Cisco Catalyst 9000 з Cisco IOS XE; підтримка L2/L3, ACL, QoS, NetFlow.

б) Підсистема безпеки: захист внутрішньої мережі від несанкціонованого доступу та загроз. Заснована на Cisco Firepower, IPS/IDS, VPN, Zone-Based Policy Firewall.

в) Підсистема збирання телеметрії: моніторинг стану мережевого обладнання та каналів у реальному часі. Контейнеризований застосунок, що використовує API Cisco IOS XE, Python, Prometheus.

г) Серверна підсистема: забезпечення обчислювальних потужностей для сервісів ЦНА. Сервери Dell PowerEdge, віртуалізація, Linux/Windows Server, підтримка Docker/KVM.

д) Підсистема зберігання даних: централізоване зберігання файлів, резервне копіювання. NAS Synology з RAID, інтеграція з серверами та резервне копіювання конфігурацій.

е) Підсистема користувацького доступу: робочі місця операторів, адміністраторів і керівників. ПК, IP-телефони, сканери, принтери, 2 монітори; підтримка локального та доменного входу.

ж) Підсистема бездротового доступу: підключення мобільних пристроїв у зонах очікування та службових приміщеннях. Wi-Fi Cisco Aironet 2800, підтримка WPA2/WPA3, гостьовий доступ, роумінг.

з) Підсистема відеоспостереження: забезпечення фізичної безпеки приміщень ЦНАП. Камери Hikvision, запис на NVR, IP-підключення, зовнішній та внутрішній контроль.

и) Підсистема живлення: гарантування безперервної роботи критичних компонентів при збоях електропостачання. ДБЖ APC, підтримка моніторингу стану, час автономної роботи – до 30 хвилин.

2.1.2.2 Вимоги до способів і засобів зв'язку між компонентами комп'ютерної системи

Для успішного функціонування комп'ютерної системи ЦНАП у м.Дніпро передбачено поєднання провідних та бездротових технологій передачі даних. Таке рішення забезпечує надійний обмін інформацією між усіма компонентами системи – від серверів і робочих станцій до IoT-пристроїв і систем відеоспостереження.

На рівні ядра мережі використовується технологія Ethernet з обладнанням Cisco Catalyst 9000, що забезпечує високу пропускну здатність, низьку затримку та стабільне з'єднання для критично важливих служб (серверна частина, маршрутизатори, міжмережеві екрани тощо). Комутатори серії Catalyst 9000 підтримують Cisco IOS XE та API-програмування, що дає змогу централізовано керувати мережевими потоками, збирати телеметрію та інтегрувати з зовнішніми системами моніторингу.

Для рівня доступу передбачене використання технології WiFi 6 (802.11ax), що забезпечує зручний і захищений бездротовий доступ для мобільних пристроїв працівників та IoT-систем (наприклад, систем відеоспостереження, датчиків присутності, контролерів доступу). Безпека бездротової мережі гарантується через WPA2-Enterprise з можливістю переходу на WPA3.

Для організації логічної та фізичної мережевої структури в рамках CIDR-діапазону 172.21.96.0/21 передбачено:

а) поділ корпоративної мережі на кілька підмереж із використанням VLSM з урахуванням кількості кінцевих пристроїв у кожному підрозділі:

– адміністрація (до 250 пристроїв);

– відділ фінансовий (до 70 пристроїв);

– відділ IT та кластер серверів (до 135 пристроїв);

– відділ з обслуговування громадян (до 160 пристроїв);

– вектор маркетингу та ЗМІ (до 50 пристроїв);

б) забезпечення автоматичного призначення IP-адрес кінцевим пристроям за допомогою DHCP;

в) впровадження маршрутизації EIGRP в усій інфраструктурі для забезпечення швидкої конвергенції та гнучкої маршрутизації;

г) надання доступу до Інтернету з використанням NAT/PAT, з зовнішнім пулом адрес 209.165.202.5 – 209.165.202.30 (/28);

д) впровадження серверної частини для телеметрії та IoT-даних у вигляді контейнеризованого застосунку (Docker), розгорнутого у кластері IT-відділу, з підтримкою API-підключення до комутаторів Catalyst 9000;

е) реалізація віддаленого доступу до конфігурацій маршрутизаторів для резервного копіювання та керування.

2.1.2.3 Вимоги до режимів функціонування системи

Цілодобова робота серверної та мережевої інфраструктури.

Автоматизований моніторинг та сповіщення при виявленні перевантаження мережевих інтерфейсів (>80%).

Застосунок працює в режимі реального часу, збираючи та аналізуючи дані кожні 5 секунд. Він також підтримує режим періодичного аналізу, коли дані збираються та аналізуються раз на годину. У випадку помилок підключення до комутатора, застосунок намагається відновити з’єднання кожні 30 секунд.

2.1.3 Вимоги до видів забезпечення комп’ютерної системи

2.1.3.1 Вимоги до математичного забезпечення

Для розрахунку середнього навантаження на порти використовується формула:

Average_Utilization = (Input_Bytes + Output_Bytes) / (Interface_Speed * Time_Interval)

В перспективі використання методів машинного навчання для аналізу аномалій у трафіку.

2.1.3.2 Вимоги до інформаційного забезпечення

Використовується YANG модель `Cisco-IOS-XE-interfaces-oper` для отримання даних про використання інтерфейсів. Дані зберігаються в форматі JSON.

2.1.3.3 Вимоги до технічного забезпечення

Обладнання Catalyst 9000 з IOS XE 17.3 або вище:

– IOx Runtime 2.0 або вище;

– мінімум 1 vCPU та 512MB RAM для контейнера;

Використання Python для аналізу мережевих метрик та управління контейнерами.

Використання REST API для взаємодії з мережевими пристроями.

Контейнеризовані середовища на базі Docker + Kubernetes.

2.1.3.4 Вимоги до організаційного забезпечення

Для розгортання та налаштування застосунку потрібен мережевий інженер з досвідом роботи з Cisco Catalyst 9000 та IOx.

2.1.3.5 Вимоги до методичного забезпечення

Потрібна документація з встановлення, налаштування та використання застосунку.

2.2 Розробка апаратної частини комп’ютерної системи

2.2.1 Розробка загальної архітектури мережі підприємства

Побудова надійної комп’ютерної мережі є критично важливою складовою для функціонування ЦНАП, оскільки вона забезпечує ефективну взаємодію між робочими місцями співробітників, серверами, системами

зберігання даних, засобами контролю доступу, а також користувацькими сервісами.

З урахуванням рекомендацій Cisco Smart Business Architecture (SBA) [2] та матеріалів посібника «Як створити ЦНАП» [3], було розроблено трирівневу модель архітектури комп'ютерної мережі, що включає (рис. 2.5):

– рівень ядра (Core Layer) – високошвидкісна магістраль, яка забезпечує з'єднання між основними підсистемами мережі. На цьому рівні працюють високопродуктивні комутатори, які забезпечують мінімальну затримку та максимальну пропускну здатність;

– рівень розподілу (Distribution Layer) – виконує функції маршрутизації, фільтрації трафіку, реалізації політик безпеки та балансування навантаження. Тут відбувається сегментація мережі за допомогою VLAN;

– рівень доступу (Access Layer) – забезпечує підключення кінцевих пристроїв користувачів (ПК, IP-телефонів, принтерів, IoT-пристроїв). На цьому рівні застосовуються керовані комутатори з підтримкою 802.1Q, PoE та функцій захисту портів.

–

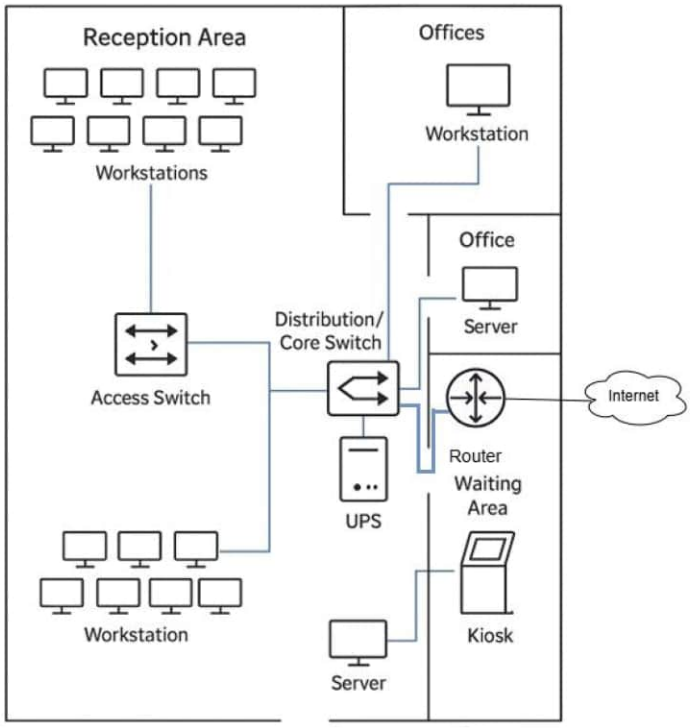

Рисунок 2.5 – Загальна архітектура мережі ЦНАП

Для забезпечення багаторівневої відмовостійкості та безперервної роботи ЦНАПу, архітектура передбачає:

– резервування каналів зв’язку та ключових пристроїв на рівнях ядра і розподілу;

– застосування політик безпеки через фаєрволи та розмежування доступу на основі ролей (RBAC);

– підтримку віртуальних локальних мереж (VLAN) для логічного розділення служб (реєстрація, електронна черга, бек-офіс, технічний моніторинг тощо);

– централізоване керування за допомогою системи моніторингу та логування подій.

Загальна схема побудови мережі узгоджується з концепцією "Campus Network", яка передбачає централізовану мережу в межах одного або кількох пов’язаних офісів. Цей підхід забезпечує масштабованість, централізацію адміністрування, спрощення підтримки, а також оптимальне використання ресурсів.

Відповідно до потреб ЦНАПу, також передбачено окремі підмережі для:

– внутрішнього документообігу;

– систем відеонагляду;

– систем телеметрії (IoT);

– гостьового Wi-Fi-доступу з ізоляцією від внутрішньої мережі.

Проєктна архітектура є гнучкою та дозволяє розширення функціоналу у разі потреби: підключення нових робочих місць, серверів або додаткових філій ЦНАПу.

2.2.2 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп’ютерної системи

В основу розробки структурної схеми комплексу технічних засобів ЦНАП покладено модульний підхід, що дозволяє ефективно реалізувати

архітектуру мережі відповідно до моделі SBA. Такий підхід забезпечує гнучке масштабування, централізоване управління та високий рівень надійності.

Для побудови надійної, масштабованої та безпечної комп'ютерної мережі ЦНАП у місті Дніпро було прийнято рішення використовувати обладнання від компанії Cisco, що відповідає рекомендаціям Cisco Smart Business Architecture (SBA) для середніх організацій.

а) Комутатори рівня доступу.

На рівні доступу запропоновано використати комутатори серії Cisco Catalyst 2960-X. Вони забезпечують до 48 портів Fast або Gigabit Ethernet із підтримкою PoE для підключення IP-телефонів, точок доступу Wi-Fi, а також клієнтських ПК. Комутатори цієї серії підтримують базові функції безпеки, QoS, VLAN, Spanning Tree Protocol та інтегруються в централізовану систему моніторингу.

б) Комутатори рівня розподілу.

На розподільчому рівні рекомендовано встановити Cisco Catalyst 3560-CX або подібну серію з підтримкою Layer 3 функцій. Ці комутатори дозволяють здійснювати маршрутизацію між VLAN, підтримують протоколи OSPF та EIGRP, а також забезпечують агрегацію трафіку з рівня доступу. Розміщення обладнання на цьому рівні дозволяє зменшити навантаження на маршрутизатор та локалізувати обробку даних на рівні підмереж.

в) Комутатор ядра.

Ключовим елементом є Cisco Catalyst 9500 Series – високопродуктивний комутатор ядра корпоративного класу, призначений для обробки великих обсягів трафіку та забезпечення централізованого управління. Він функціонує під керуванням Cisco IOS XE, що надає розширені можливості для програмного керування через RESTCONF, NETCONF, gRPC та підтримку моделей YANG. Це забезпечує гнучкість, необхідну для реалізації телеметрії та автоматизації, а також дозволяє інтегрувати мережу з контейнеризованими сервісами у майбутньому.

г) Маршрутизатор та міжмережевий екран.

Для маршрутизації трафіку між зовнішніми та внутрішніми мережами застосовується Cisco ISR 4331, що підтримує апаратне шифрування, VPN-тунелі та забезпечує достатній рівень продуктивності для ЦНАП середнього масштабу.

д) Бездротова інфраструктура.

Покриття Wi-Fi у публічних зонах (зала очікування, зони самообслуговування) реалізується за допомогою Cisco Aironet 2800 Series, що підтримують стандарти 802.11ac Wave 2, MU-MIMO та централізоване управління через Cisco Wireless LAN Controller. Створюються окремі SSID для гостьового доступу та внутрішніх служб.

є) Серверна інфраструктура.

У серверній кімнаті розгортається віртуалізоване середовище на базі HP ProLiant DL380 Gen10 із підтримкою гіпервізора Proxmox VE. У цьому середовищі розміщуються сервери:

– DHCP, DNS, AD;

– баз даних та обліку;

– моніторингу мережі;

– телеметричних сервісів (розділ 4).

Серверне обладнання підключається через окремий інтерфейс до ядра мережі та має ізольовану VLAN для підвищення рівня безпеки.

ж) Периферійне обладнання.

Додатково до складу інфраструктури входять мережеві принтери, POS-термінали, термінали електронної черги, відеокамери, а також система резервного живлення (UPS), що забезпечує безперервність роботи критично важливих систем у разі відключення електроенергії.

Обрана апаратна платформа є масштабованою, сертифікованою відповідно до міжнародних стандартів та дозволяє забезпечити якісне надання адміністративних послуг відповідно до сучасних вимог до ЦНАП.

2.2.3 Розробка специфікації апаратних засобів комп'ютерної системи

Для забезпечення стабільної та безперервної роботи ЦНАП, було сформовано детальну специфікацію апаратного забезпечення комп'ютерної системи (таблиця 2.1).

Таблиця 2.1 – Специфікація апаратного забезпечення комп'ютерної системи ЦНАП

№ з/п	Категорія	Найменування	Кіл.	Призначення
1	Комутатори ядра	Cisco Catalyst 9500	2	Агрегація трафіку, забезпечення високої доступності
2	Комутатори розподілу	Cisco Catalyst 9300	2	Реалізація VLAN, маршрутизація, політики безпеки
3	Комутатори доступу	Cisco Catalyst 9200 (24 порти, PoE)	4	Підключення кінцевих пристроїв (ПК, IP-телефони, Wi-Fi)
4	Wi-Fi точки доступу	Cisco Aironet 2800	3	Бездротовий доступ у зонах очікування та бек-офісі
5	Маршрутизатор	Cisco ISR 4331	1	Маршрутизація, NAT, VPN
6	Фаєрвол	Cisco Firepower 1010	1	Міжмережевий екран, контроль доступу, IPS
7	Сервери	Dell PowerEdge R740, 2×Intel Xeon, 128 ГБ ОЗП	2	Розміщення сервісів авторизації, документообігу, моніторингу
8	NAS-сховище	Synology RS820+ з RAID	1	Централізоване зберігання, резервне копіювання
9	Робочі станції	ПК Core i5, 16 ГБ ОЗП, SSD 512 ГБ, 2 монітори	20	Робочі місця адміністраторів та операторів
10	IP-телефони	Cisco 8841	20	Внутрішній і зовнішній зв'язок
11	Принтери	HP LaserJet Enterprise M507dn	4	Друк документів
12	Сканери	Canon DR-C225 II	3	Оцифрування документів
13	Камери відеонагляду	Hikvision DS-2CD2146G1	8	Внутрішній і зовнішній контроль
14	Відеореєстратор	Hikvision NVR з PoE	1	Запис і зберігання відео
15	UPS	APC Smart-UPS 1500VA	4	Живлення критичних систем при відключенні електрики
16	Мережеве оснащення	19" стійки, патч-панелі, кабелі Cat 6a, розетки RJ-45	комплект	Структурована кабельна система

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ ЦНАП

3.1 Розробка фізичної топологої

Для мережі офісу ЦНАП визначено фізичну топологію, яка відображає розміщення мережевого обладнання, кабельних трас, вузлів підключення та користувацьких пристроїв у межах будівлі центрального офісу.

Фізична топологія проєктується на основі архітектурних та планувальних характеристик приміщення, що забезпечують умови для ефективного функціонування комп'ютерної системи. Розроблена узагальнена фізична топологія з 3-х філіалів ЦНАП представлена на рис. 3.1.

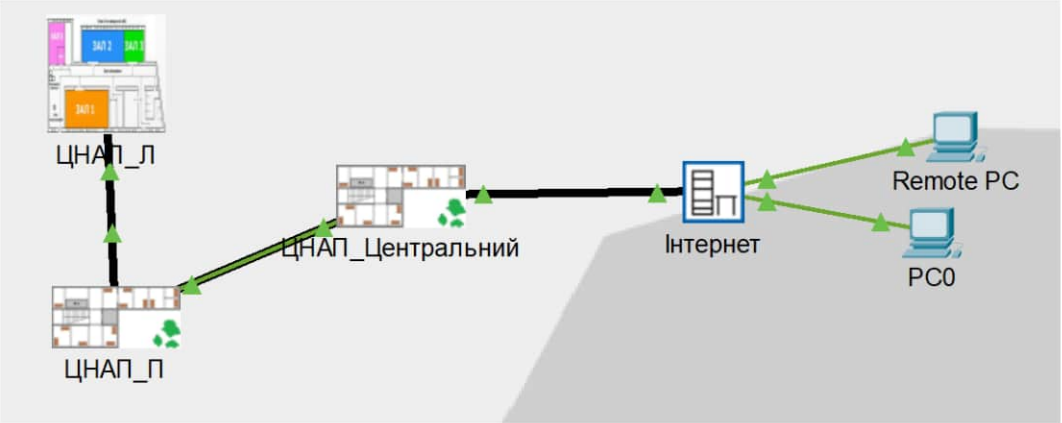

Рисунок 3.6 – Фізична топологія філіалів ЦНАП в PT

Центральне відділення ЦНАП (Central) розміщене в одноповерховій будівлі загальною площею приблизно 300 м², поділеній на такі функціональні зони (рис.3.2):

– зона прийому громадян (відкрита зала з 12 робочими місцями адміністраторів);

– зал очікування з інформаційним терміналом і системою електронної черги;

– серверна кімната, ізольована для розміщення активного обладнання;

– кабінети керівництва та технічного персоналу;

– кімнати обслуговування спеціальних категорій громадян.

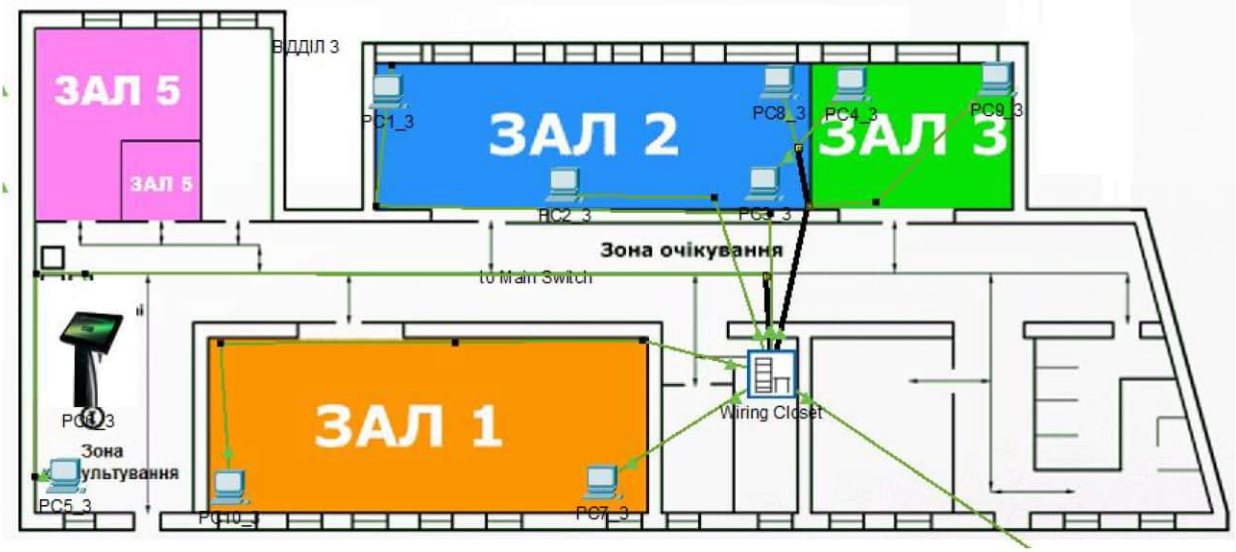

Рисунок 3.1 – Мережа центрального офісу ЦНАП

Мережеве обладнання встановлюється у централізованій телекомунікаційній шафі, яка розташована в серверній кімнаті. Усі кабельні траси прокладаються через підвісну стелю та кабель-канали вздовж стін. Основні сегменти мережі формуються на базі структури типу «зірка», де всі кінцеві пристрої з’єднуються з комутаторами рівня доступу. Кабелі прокладено вздовж стін таким чином, аби вони були якомога коротшими, але водночас не псували загального враження від будівлі. Для зручності розрізнення різні відділи позначені кабелями різних кольорів

Для об’єднання робочих станцій персоналу, інформаційних терміналів, принтерів та систем відеоспостереження використовується мідна витка пара категорії Cat6A, що забезпечує швидкість передачі до 10 Гбіт/с на відстань до 100 метрів. Також передбачено використання оптоволоконних з'єднань між комутаторами доступу та ядра мережі для забезпечення резервування та високої пропускної здатності.

Електроживлення критичних компонентів забезпечується за допомогою блоків безперебійного живлення (UPS), розрахованих на щонайменше 30 хвилин автономної роботи.

З наведеного плану зрозуміло, що “серцем” кожного поверху є технічне приміщення – кімната мережевого обладанання (або англ. *Main Wiring Closet*). Окрім маршрутизаторів та комутаторів, у ній розташовані також сервери.

3.2 Розробка логічної топології

Логічна топологія мережі ЦНАП визначає спосіб організації взаємодії між пристроями на рівні протоколів та служб, незалежно від фізичного розташування обладнання. Вона відображає логічну структуру мережі, що забезпечує ефективний обмін даними, безпеку і масштабованість системи.

Для проєктованої мережі ЦНАП обрана логічна топологія типу «зірка» з централізованим управлінням, що забезпечує оптимальну організацію трафіку, легкість адміністрування і високу надійність роботи.

Основні компоненти логічної топології включають:

– центральний комутатор рівня доступу (Access Switch), який об’єднує всі робочі станції працівників, серверне обладнання та периферійні пристрої в локальну мережу;

– маршрутизатор, що здійснює зв’язок локальної мережі ЦНАП із зовнішніми мережами (інтернет, державні інформаційні системи), а також реалізує функції безпеки (мережевий екран, NAT, VPN);

– сегментація мережі за допомогою VLAN, що забезпечує логічне розділення трафіку між різними підрозділами та службами, підвищуючи безпеку та ізоляцію даних;

– сервери служб мережевих сервісів (DHCP, DNS, TFTP, HTTP), які надають необхідну функціональність для автоматизації налаштувань і роботи мережі.

Використання логічної топології «зірка» дозволяє централізовано контролювати доступ і політику безпеки, а також забезпечує масштабованість системи у разі розширення ЦНАП.

Схематично логічна топологія мережі представлена на рисунку 3.2.

Спроектована мережа розділена на 7 VLAN (включно з т.зв. Native, 50):

– 10, 20, 30 – для філіалів №1,2,3 відповідно;

– 40 – керування підрозділами;

– 60 – бездротового доступу;

– 70 – серверів (TFTP та E-mail).

Для збільшення пропускної здатності виконано агрегацію інтерфейсів.

Налаштовано бездротову точку доступу, вказано пароль доступу PSK cisco123, назву SSID Central_Wireless. Лістинг налаштувань див. додатку А.

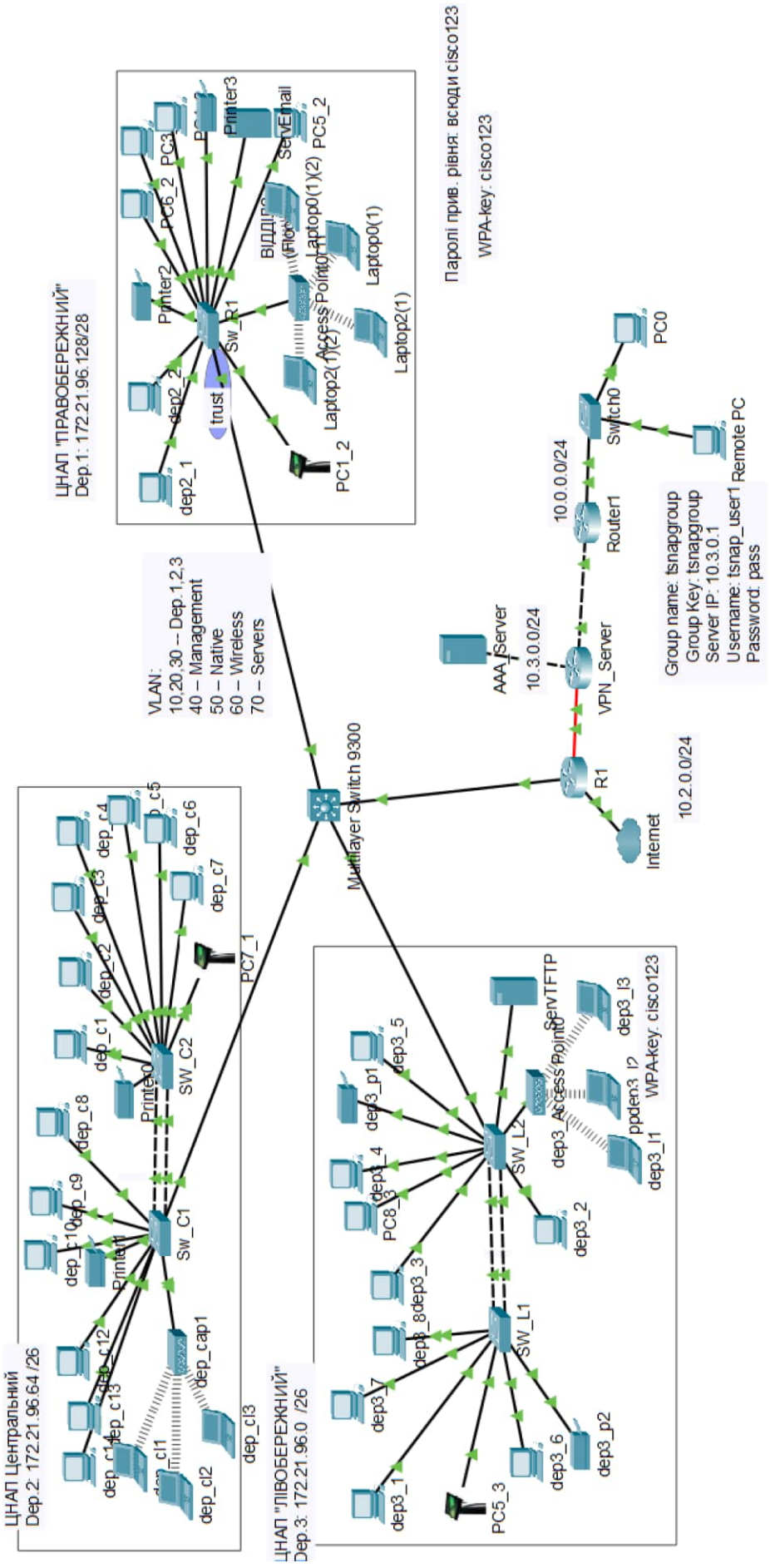

Рисунок 3.2 – Логічна топологія мереж ЦНАП

3.3 Розрахунок схеми адресації мережі

Для забезпечення ефективної маршрутизації, логічної ізоляції трафіку та централізованого керування було реалізовано сегментацію мережі за допомогою VLAN (Virtual Local Area Network). Кожному підрозділу та типу пристроїв у мережі ЦНАП виділено окрему підмережу з унікальним номером VLAN та відповідним діапазоном IP-адрес. Це дозволяє забезпечити:

– обмеження широкомовного трафіку в межах кожного VLAN;

– підвищення рівня безпеки завдяки ізоляції мережевих сегментів;

– гнучкість при розгортанні сервісів і пристроїв;

– можливість централізованого моніторингу та адміністрування.

Адресний простір побудовано на основі приватного діапазону IP-адрес IPv4 класу B 172.21.96.0/21. Загальна схема адресації наведена в таблиці 3.2, а інтерфейсів пристроїв в табл. 3.3.

Таблиця 3.2 – Схема адресації мережі

Ім’я VLAN	Номер VLAN	Адреса підмережі	Маска	Діапазон допустимих IP-адрес вузлів
Dep1	10	172.21.96.128	255.255.255.240	172.21.96.129 – 172.21.96.142
Dep2	20	172.21.96.64	255.255.255.192	172.21.96.65 – 172.21.96.126
Dep3	30	172.21.96.0	255.255.255.192	172.21.96.0 – 172.21.96.62
Management	40	172.21.96.144	255.255.255.248	172.21.96.145 – 172.21.96.150
Native	50	–	_	—
Wireless	60	172.21.96.160	255.255.255.224	172.21.96.161 – 172.21.96.190
Servers	70	172.21.96.240	255.255.255.240	172.21.96.241 – 172.21.96.254

Таблиця 3.3 – Схема адресації пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN ID
R1	Gig0/0/0:10	172.21.96.129	255.255.255.240	6.1.19.5	10
	Gig0/0/0:20	172.21.96.65	255.255.255.192	6.1.19.5	20
	Gig0/0/0:30	172.21.96.1	255.255.255.192	6.1.19.5	30
	Gig0/0/0:40	172.21.96.145	255.255.255.248	6.1.19.5	40
	Gig0/0/0:60	172.21.96.161	255.255.255.224	6.1.19.5	60
	Gig0/0/0:70	172.21.96.241	255.255.255.240	6.1.19.5	70
	Gig0/0/1	6.1.19.5	255.255.255.0	6.1.19.5	Default
Sw_9300	Fa0/21-22	–	–	–	50
	vlan 10	172.21.96.130	255.255.255.240	–	10
	vlan 20	172.21.96.66	255.255.255.192	–	20
	vlan 30	172.21.96.2	255.255.255.192	–	30
	vlan 40	172.21.96.146	255.255.255.248	–	40
	vlan 60	172.21.96.162	255.255.255.224	–	60
Sw_C	vlan 40	172.21.96.147	255.255.255.248	172.21.96.145	40
Sw_L	vlan 40	172.21.96.148	255.255.255.248	172.21.96.145	40
Sw_R	vlan 40	172.21.96.149	255.255.255.248	172.21.96.145	40

3.3.2 Вибір та налаштування способу маршрутизації

Для забезпечення взаємодії між окремими підмережами VLAN, реалізованими в межах мережі ЦНАП, а також для організації виходу до глобальної мережі Інтернет, було прийнято рішення використовувати інтервіланову маршрутизацію (Inter-VLAN Routing) на базі маршрутизатора з підтримкою протоколу OSPF (Open Shortest Path First). OSPF є внутрішньосистемним протоколом динамічної маршрутизації класу link-state, який дозволяє швидко реагувати на зміни в топології та підтримує масштабованість. Протокол підтримує VLSM (змінну довжину маски підмережі), що дає змогу ефективно використовувати адресний простір.

Маршрутизатор R1 у мережі ЦНАП виконує роль централізованого вузла маршрутизації (Router-on-a-Stick), обслуговуючи підключення до транкового порту комутатора та створюючи підінтерфейси для кожного VLAN.

Конфігурація інтервіланової маршрутизації реалізована за допомогою підінтерфейсів на фізичному інтерфейсі маршрутизатора GigabitEthernet0/0/0. Кожному підінтерфейсу присвоєно відповідний VLAN ID та IP-адресу шлюзу для відповідної підмережі. Фрагмент конфігурації наведено нижче:

```
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 172.21.96.129 255.255.255.240

interface GigabitEthernet0/1.20
 encapsulation dot1Q 20
 ip address 172.21.96.65 255.255.255.192

interface GigabitEthernet0/1.30
 encapsulation dot1Q 30
 ip address 172.21.96.1 255.255.255.192

interface GigabitEthernet0/1.40
 encapsulation dot1Q 40
 ip address 172.21.96.145 255.255.255.248

interface GigabitEthernet0/1.60
 encapsulation dot1Q 60
 ip address 172.21.96.161 255.255.255.224

interface GigabitEthernet0/1.70
 encapsulation dot1Q 70
 ip address 172.21.96.241 255.255.255.240
```

OSPF налаштовується наступним чином:

```
router ospf 1
 network 172.21.96.0 0.0.0.255 area 0
```

Тут використано одну область (area 0), яка охоплює всі підмережі в межах офісу. У перспективі така архітектура дозволяє легко додавати нові вузли або сегменти без порушення загальної логіки маршрутизації.

Оскільки маршрутизатор у Central єдиний, для зв’язку з віддаленими мережами доцільно використати статичний маршрут за замовчуванням через вихідний інтерфейс GigabitEthernet0/0/1:

```
ip route 0.0.0.0 0.0.0.0 192.168.100.1
```

Таким чином, обраний підхід поєднує переваги централізованого контролю, динамічного оновлення маршрутів і ефективного управління адресним простором.

Зовнішньому інтерфейсу маршрутизатора надано адресу з діапазону адрес глобальної мережі WAN: 6.1.19.5 з префіксом /24.

Таким чином забезпечено маршрутизацію між VLAN та назовні.

На рисунку 3.4 таблиці маршрутизації на маршрутизаторі центрального відділеня має підінтерфейси до підрозділів (Inter-VLAN) та маршрут за замовучуванням в Інтернет.

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     6.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       6.1.19.0/24 is directly connected, GigabitEthernet0/0/2
L       6.1.19.5/32 is directly connected, GigabitEthernet0/0/2
     172.21.0.0/16 is variably subnetted, 12 subnets, 5 masks
C       172.21.96.0/26 is directly connected, GigabitEthernet0/0/0.30
L       172.21.96.1/32 is directly connected, GigabitEthernet0/0/0.30
C       172.21.96.64/26 is directly connected, GigabitEthernet0/0/0.20
L       172.21.96.65/32 is directly connected, GigabitEthernet0/0/0.20
C       172.21.96.128/28 is directly connected, GigabitEthernet0/0/0.10
L       172.21.96.129/32 is directly connected, GigabitEthernet0/0/0.10
C       172.21.96.144/29 is directly connected, GigabitEthernet0/0/0.40
L       172.21.96.145/32 is directly connected, GigabitEthernet0/0/0.40
C       172.21.96.160/27 is directly connected, GigabitEthernet0/0/0.60
L       172.21.96.161/32 is directly connected, GigabitEthernet0/0/0.60
C       172.21.96.240/28 is directly connected, GigabitEthernet0/0/0.70
L       172.21.96.241/32 is directly connected, GigabitEthernet0/0/0.70
S*   0.0.0.0/0 is directly connected, GigabitEthernet0/0/2
```

Рисунок 3.3 – Таблиця маршрутизації на маршрутизаторі Central

3.3.3 Налаштування мереж VLAN, маршрутизації між VLAN

Для забезпечення структурованої організації трафіку та логічної ізоляції мережі Центру надання адміністративних послуг, було реалізовано сегментацію комутаційної інфраструктури за допомогою VLAN (Virtual Local

Area Network). Кожен VLAN обслуговує окрему групу користувачів або пристроїв, відповідно до функціонального призначення.

На основі фізичної топології й функціональних вимог, у таблиці 3.4 наведено розподіл портів комутаторів між відповідними VLAN, а також режими роботи портів.

Таблиця 3.4 – Мережі VLAN и призначень портів

VLAN ID	Ім'я VLAN	Порт	Режим роботи
10	Dep1	На головному комутаторі: Fa0/1-5; На комутаторі Відділу 1: Fa0/1-22.	access
20	Dep2	На головному комутаторі: Fa0/6-10; комутаторах Відділу 2: Fa0/1-22.	access
30	Dep3	На головному комутаторі: Fa0/11-15; комутаторах Відділу 3: Fa0/1-22.	access
40	Management	На головному омутаторі: Fa0/16-20; На інших комутаторах: Fa0/23-24.	access
50	Native	Gig0/1-2; Решта незайнятих портів на всіх комутаторах	trunk
60	Wireless	Gig0/2 на головному комутаторі	access
70	Servers	Fa0/23-24 на головному комутаторі	access

Приклад налаштування VLAN на Multilayer Switch 9300 показано на рис.3.4.

Рисунок 3.4 – Налаштування VLAN на Multilayer Switch 9300

3.3.4 Вибір і налаштування службових мережевих сервісів

Для забезпечення повноцінного функціонування мережевої інфраструктури ЦНАП було реалізовано набір службових сервісів, які розгорнуто у VLAN 70 (Servers). Їхнє розміщення в окремому логічному сегменті підвищує безпеку, полегшує адміністрування та дозволяє централізовано обслуговувати користувачів із різних підрозділів.

До складу мережевих сервісів входять:

– DHCP-сервер –автоматичне надання IP-адрес, шлюзів і параметрів DNS-клієнтам у межах кожного VLAN;

– DNS-сервер –служба імен, яка забезпечує трансляцію доменних імен у IP-адреси в межах локальної мережі;

– сервер аналітики телеметрії – окрема частина контейнеризованої системи збору телеметрії (детально розглянуто в розділі 4).

DHCP-сервер автоматично призначає IP-адреси користувацьким пристроям у VLAN Dep1–Dep3, Wireless і Management. Вирішено використати маршрутизатор R1 в якості DHCP-сервера. У відповідності до поділу Central на відділи, підмережу керування відділами та бездротовий доступ, визначено наступні блоки адрес DHCP, або пули (pools): Pool_1, Pool_2, Pool_3, Pool_Management, Pool_Wireless. Кожен з них, природно, містить адреси, непримустимі для надання користувачам – це адреси мережевих пристроїв (інтерфейсів маршрутизатора та VLAN на комутаторах), що забезпечує коректну роботу протоколу DCHP. В додатку А наведено конфігурація DHCP-сервера на базі Cisco.

Для перевірки оновим адресу на ПК в ЦНАП «лівобережний» (рис..3.5). Вузол отримав адресу з відповідного пулу, і на роутері формується таблиця прив’язок (рис. 3.6).

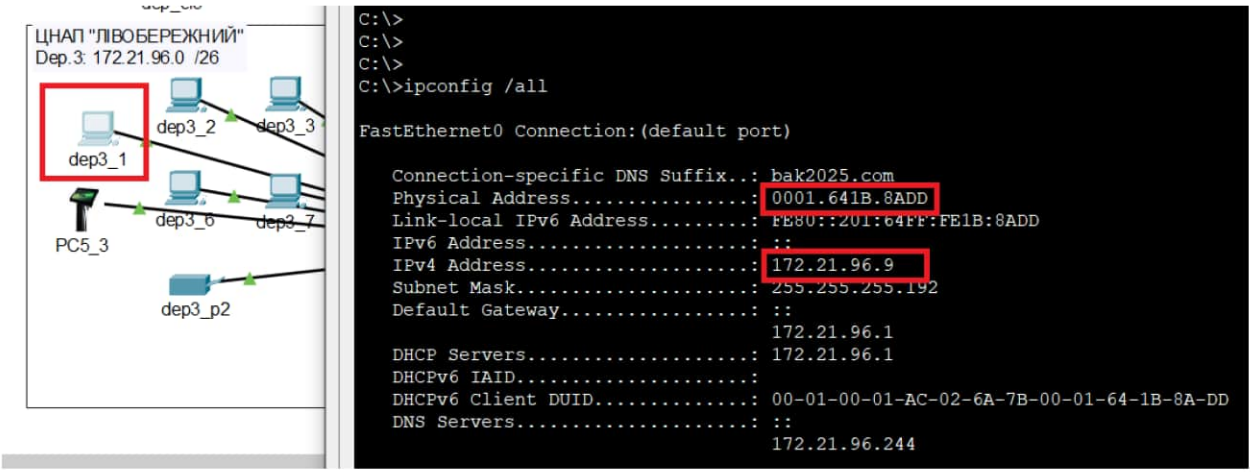

Рисунок 3.5 – Динамічне отримання IP-адреси в dep3

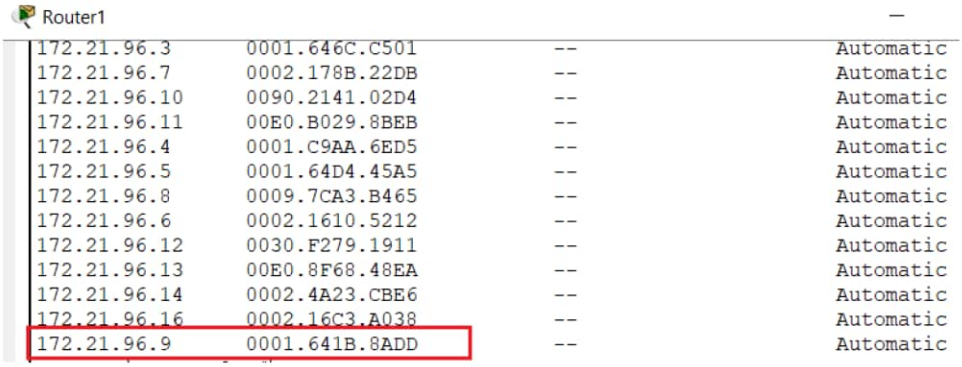

Рисунок 3.6 – Таблиця ip dhcp binding

В мережі ЦНАП "ПРАВОБЕРЕЖНИЙ" налаштовано Email-server в VLAN 70 з адресою 172.21.96.243. Та додано 3 користувача (рис. 3.7).

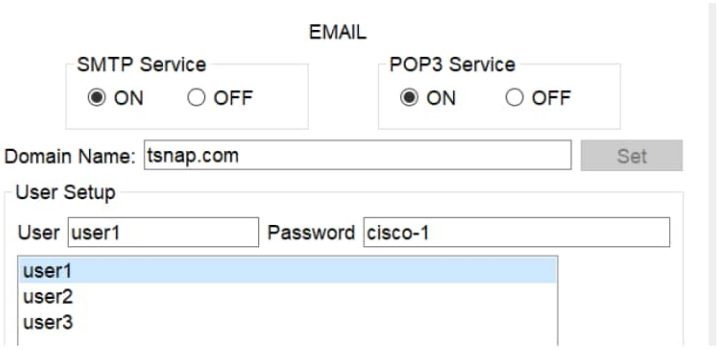

Рисунок 3.7 – Налаштування служби ServEmail

На ПК dep_1 та dep_2 налаштовані поштові клієнти user1 та user2 відповідно (рис. 3.8).

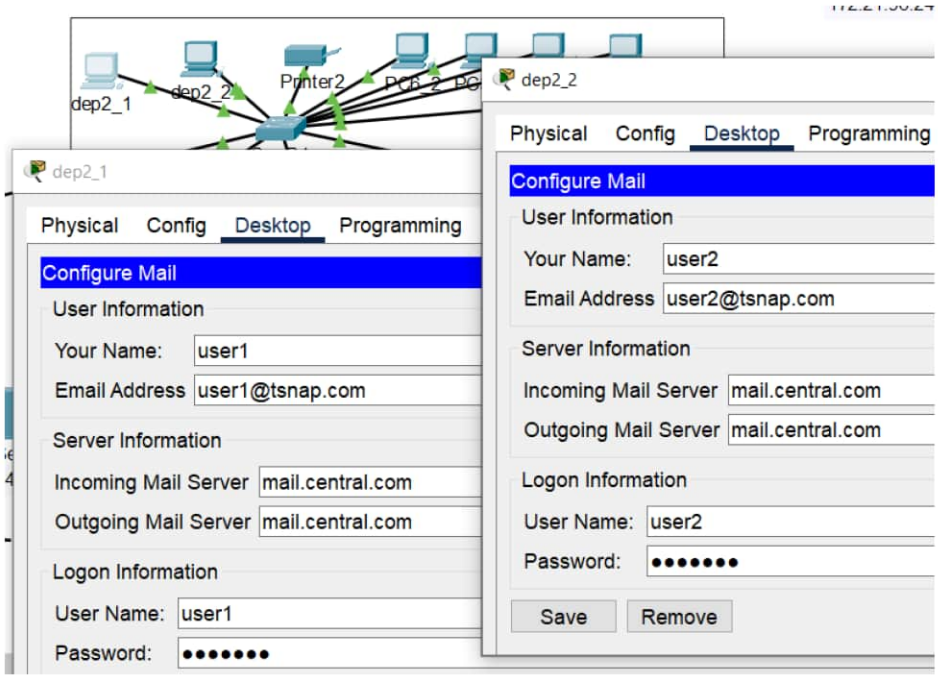

Рисунок 3.8 – Налаштування пошти на ПК dep2_1

Для перевірки коректності налаштування поштової служби на Email-сервері надіслано лист від користувача User1 до User2. Процес надсилання показаний на рис. 3.9. Лист надійшов успішно.

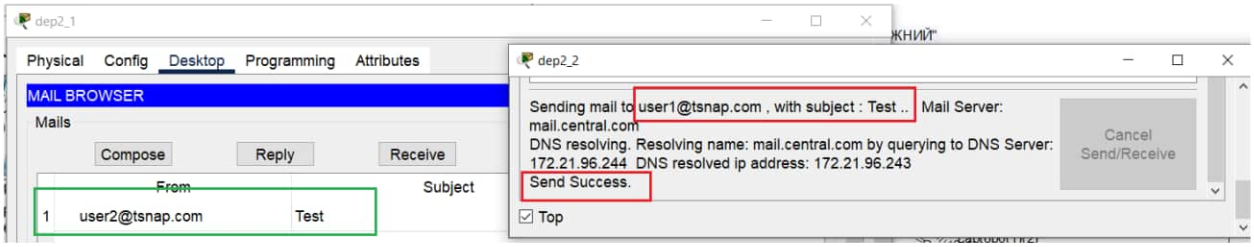

Рисунок 3.9 – Надсилання листа в поштовому домені `tsnap.com`

3.4 Налаштування обладнання відповідно до вимог безпеки ЦНАП

Функціонування ЦНАП передбачає обробку персональних даних громадян, доступ до національних інформаційних ресурсів (реєстрів), а також підтримку внутрішнього документообігу та сервісів взаємодії між державними установами. У зв'язку з цим до проєктованої мережевої інфраструктури пред'являються специфічні вимоги з безпеки, контролю доступу, сегментації трафіку, захисту від DHCP-підміни та підтримки захищених каналів зв'язку з

віддаленими підрозділами. У цьому підрозділі розглянуто реалізацію відповідних технічних заходів

3.4.1 Запобігання підміни DHCP-сервера: DHCP-Snooping

На мережному обладнанні задані паролі привілейованого та віддаленого доступу. Це запобігає зміні або знищенню налаштувань мережевих пристроїв (насамперед маршрутизатора R1).

Для запобігання підміни DHCP-сервера з боку користувачів відділів шляхом надсилання “фальшивих” оновлень DHCP на маршрутизаторах рівня доступу застосовано т.зв. DHCP-snooping. Далі наведено лістинг відповідних команд для Sw_L (аналогічно для Sw_C, Sw_R).

```
ip dhcp snooping vlan 10,20,30,40,60
int range g0/1
ip dhcp snooping trust
```

Застосування NAT перетворює маршрутизатор на своєрідний firewall, не дозволяючи звертатись до пристроїв за їхніми публічними адресами, таким чином підвищує стійкість мережі центрального офісу до атак ззовні.

3.4.2 Зміна native VLAN за замовчуванням

Було прийнято рішення про зміну VLAN за замовчуванням (native VLAN) з 1 на 50 з метою підвищення рівня мережевої безпеки та запобігання несанкціонованому доступу до керованого трафіку в транкових з’єднаннях. Зміна native VLAN є рекомендованою практикою в захисті інфраструктури комутованих мереж, оскільки VLAN 1 використовується за замовчуванням у багатьох службових протоколах Cisco, зокрема VTP, CDP, DTP, PAgP тощо.

Основні ризики використання VLAN 1 як native VLAN:

– використовується більшістю мережевих протоколів за замовчуванням, що робить її мішенню для атак типу VLAN hopping;

– усі порти комутатора, якщо не налаштовано інакше, належать до VLAN 1, що збільшує поверхню атаки;

– службовий трафік (наприклад, DTP або VTP) може бути інтерпретований неправильно або використаний зловмисником.

Зміна native VLAN зменшує ризик таких атак, як:

– VLAN hopping (double-tagging attack) – коли фальсифіковані фрейми із тегами VLAN можуть «перестрибувати» між VLAN;

– спуфінг службових протоколів (VTP, DTP), що може призвести до зміни мережевої конфігурації або відмови в обслуговуванні.

Фрагмент конфігурації для комутаторів Cisco:

```
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 50
 switchport mode trunk
```

В результаті впровадження:

– службовий трафік відокремлено від користувацького;

– усі транкові з’єднання переведено на VLAN 50 як native VLAN;

– VLAN 1 заблоковано для користування в межах офісної мережі ЦНАП.

Зміна native VLAN є важливим етапом у реалізації моделі безпечної мережі доступу. Вона мінімізує можливість зловживання базовими функціями комутаторів та забезпечує ізоляцію службового трафіку, що критично важливо для стабільної роботи ЦНАП.

3.4.3 Захист на рівні доступу: Port Security

З метою обмеження несанкціонованого доступу до мережевої інфраструктури ЦНАП реалізовано механізм Port Security, який дозволяє контролювати доступ клієнтських пристроїв до комутаторів рівня доступу, фіксуючи дозволені MAC-адреси на фізичних інтерфейсах.

Port Security забезпечує захист від таких загроз, як:

– підключення стороннього пристрою з метою сканування мережі або прослуховування трафіку;

– атаки типу MAC flooding, які можуть вивести з ладу таблицю MAC-адрес комутатора;

– заміна або підміна клієнтського пристрою без відома адміністратора мережі.

Port Security обмежує кількість MAC-адрес, які можуть бути вивчені на певному порту комутатора. Якщо кількість MAC-адрес перевищено, порт може бути вимкнений (shutdown), обмежений (restrict) або просто ігнорувати нові адреси (protect). Таким чином, забезпечується захист від:

– підключення сторонніх пристроїв до мережі без дозволу;

– атак типу MAC flooding, при яких заповнюється таблиця MAC-адрес комутатора псевдовипадковими адресами з метою переведення його в режим широкомовної ретрансляції;

– підміни пристроїв користувачів із метою захоплення їхнього мережевого трафіку.

Приклад реалізації Port Security

```
// На портах доступу (до Attacker PC/Server, PCPT PCx)
Switch(config)# interface [type/number]
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
// Дозволити лише 1 MAC-адресу на порту
Switch(config-if)# switchport port-security maximum 1
// Найсуворіша дія при порушенні
Switch(config-if)# switchport port-security violation
shutdown
// Вивчає MAC-адресу та зберігає її в конфіг
Switch(config-if)# switchport port-security mac-address
sticky
```

У рамках побудованої мережної інфраструктури Port Security було застосовано до портів, які забезпечують підключення кінцевих пристроїв співробітників. Конфігурація проводилася з використанням методу shutdown.

У наведеній конфігурації:

– обмежується кількість дозволених MAC-адрес на порті до однієї;

– у випадку порушення порт вимикається повністю;

– автоматично зберігається MAC-адреса першого легітимного пристрою (sticky), що спрощує адміністрування.

На рис. 3.11 інформація на інтерфейсі FastEthernet 0/1 комутатора ETRX1 підтверджує, що Port Security активний і дозволяє підключати тільки один пристрій із конкретною MAC-адресою на порт FastEthernet0/1, а в разі порушення відбувається обмеження і порт відключається.

```
Sw_R1#show port-security interface f0/6
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

Рисунок 3.10 – Стан Port Security на інтерфейсі FastEthernet 0/1 ETRX1

Для підтвердження ефективності впровадженого механізму Port Security було проведено імітацію порушення: PC6_2 було вимкнено, замість нього до того ж порту під'єднано інший пристрій з іншою MAC-адресою (рис.3.11).

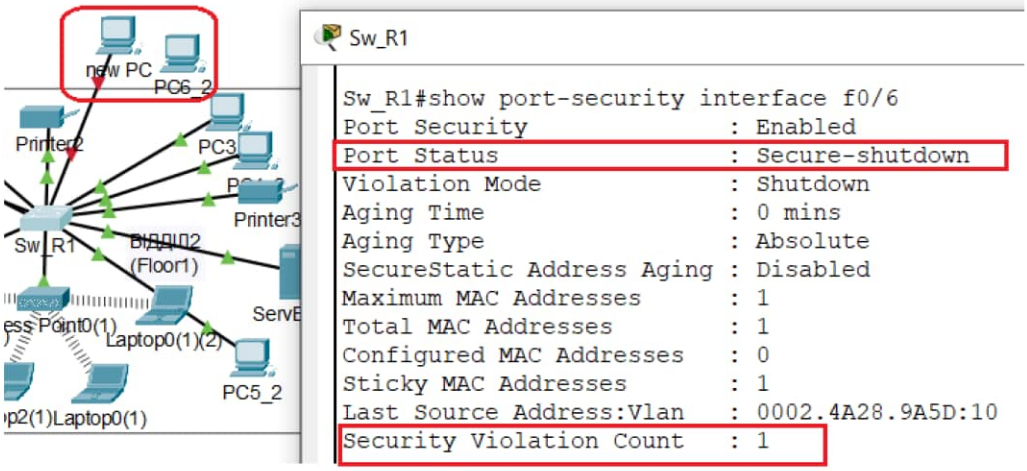

Рисунок 3.11 – Перевірка роботи Port Security

В результаті відбулася подія порушення безпеки, у відповідь комутатор вимкнув порт. У виведеному звіті (рис. 3.11) спостерігаються збільшення кількість порушень (1) і MAC-адреса-порушника не була додана до списку дозволених.

3.4.4 Захист від ARP-спуфінгу за допомогою Dynamic ARP Inspection

Для забезпечення захисту мережі ЦНАП від ARP-спуфінгу та підміни MAC-адрес впроваджено механізм Dynamic ARP Inspection (DAI). Цей механізм забезпечує перевірку достовірності ARP-повідомлень, що надходять до комутатора, та блокує фальшиві запити, які можуть бути використані для перехоплення трафіку або організації MITM-атак (Man-in-the-Middle).

Суть атаки ARP-spoofing: зловмисник надсилає фальшиві ARP-відповіді в мережу, примушуючи інші пристрої кешувати неправильну відповідність MAC ↔ IP. Це дозволяє перенаправляти або прослуховувати трафік, що є критичним порушенням конфіденційності в інформаційних системах державних установ.

DAI використовує базу даних DHCP Snooping (таблицю прив'язок) для перевірки ARP-запитів та відповідей. Він гарантує, що ARP-повідомлення надсилаються лише з легітимними зв'язками IP-MAC. Це критично для запобігання ARP-спуфінгу, який часто використовується після атаки Rogue DHCP Server (щоб видати себе за шлюз за замовчуванням).

Для налаштування DAI необхідно:

– увімкнути функцію DHCP Snooping у відповідному VLAN;

– активувати DAI для VLAN командою ip arp inspection vlan <ID>;

– позначити порти, що ведуть до довірених пристроїв (наприклад, шлюзів або DHCP-серверів), як trusted (рис. 3.12);

– у разі необхідності, встановити обмеження на швидкість надсилання ARP-запитів на портах користувачів.

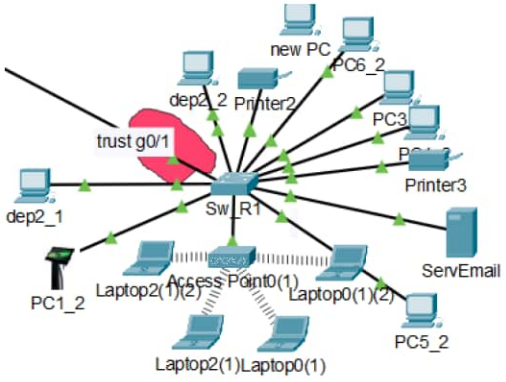

Рисунок 3.12 – Trust-порт на SW-R1

Конфігурація DAI на SW-R1 (рис.3.12):

```
ip arp inspection vlan 10
interface GigabitEthernet0/1
 ip arp inspection trust
```

Переваги, які надасть впровадження DAI в ЦНАП:

– запобігання атакам типу ARP-spoofing;

– зменшення ризиків прослуховування або модифікації трафіку;

– збереження цілісності мережевої комунікації;

– підвищення рівня довіри до локального сегмента мережі.

3.4.5 Захист від широкомовних штормів за допомогою Storm Control

У мережевій інфраструктурі ЦНАП передбачено впровадження механізму Storm Control для запобігання перевантаженню мережі широкомовним (broadcast), багатомовним (multicast) або невідомим (unknown unicast) трафіком, що може бути наслідком неправильної конфігурації пристроїв або деструктивної діяльності зловмисника.

Broadcast storm (шторм широкомовних пакетів) – це ситуація, коли кількість broadcast-пакетів у мережі різко зростає, що призводить до перевантаження комутаторів, підвищення затримки, зниження пропускної здатності або повної відмови мережевої інфраструктури.

Storm Control дозволяє обмежити кількість небажаного трафіку, що проходить через інтерфейс комутатора, встановлюючи допустимий поріг у відсотках від загальної пропускної здатності порту.

Конфігурація Storm Control на Cisco Catalyst 9000:

```
interface range GigabitEthernet1/0/1 - 24
 storm-control broadcast level 0.80
```

Якщо рівень широкомовного трафіку перевищує 80% пропускної здатності порту – спрацьовує захист/

3.4.6 Захищене з'єднання віддалених співробітників

Для віддалених співробітників налаштовано VPN_Server для VPN-доступу за допомогою VPN-клієнта на настільних ПК. Реалізовано класичний IPsec Remote Access VPN (на основі IKEv1 + dynamic crypto map), сумісний з Cisco VPN-клієнтами, з підтримкою групових ключів і RADIUS-автентифікації. Це досі прийнятна модель для невеликих організацій

Конфігурація на рис. 3.13 показує, як віддалені користувачі можуть підключатися до компанійської мережі через VPN, забезпечуючи безпеку та аутентифікацію. Авторизація клієнтів використовується через AAA-сервер по протоколу RADIUS.

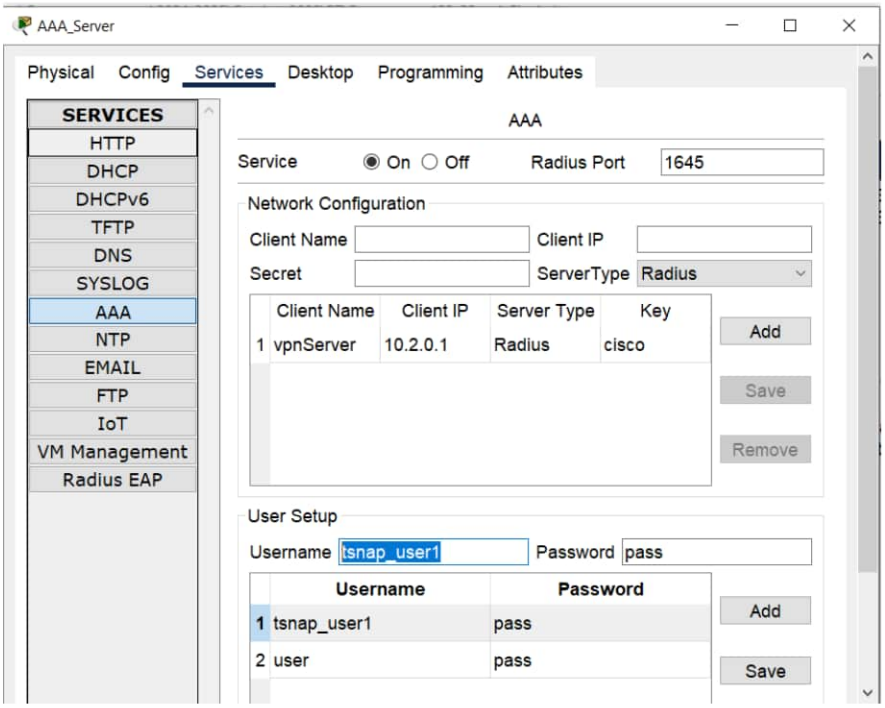

Рисунок 3.13 – Параметри AAA для VPN-клієнтів

Після підключення Remote PC має запустити додаток з налаштуваннями VPN та ввести свої дані (рис. 3.14). Після підключення має бути призначена адреса 10.1.1.100 (рис. 3.15).

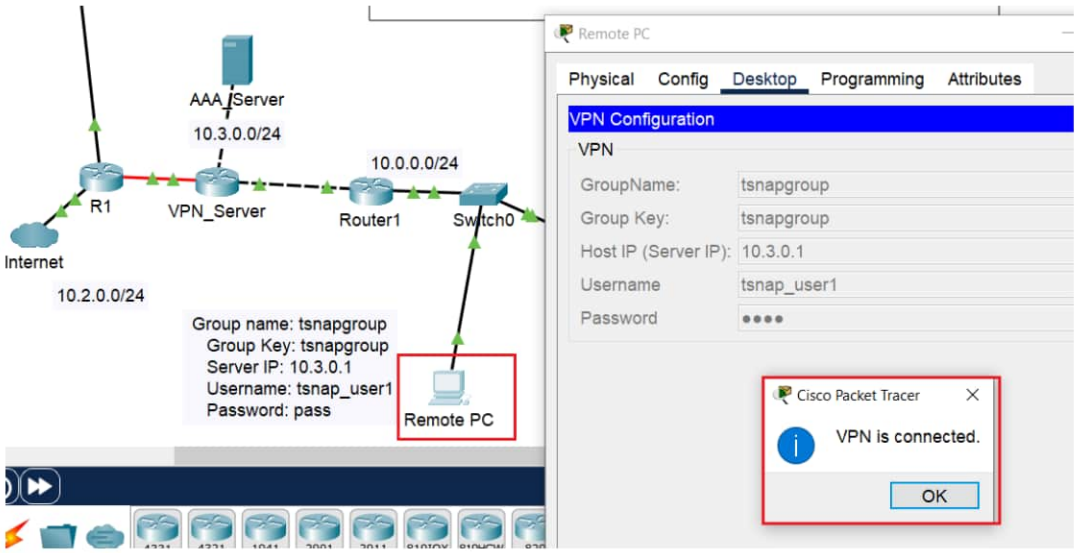

Рисунок 3.14 – Підключення клієнта через VPN

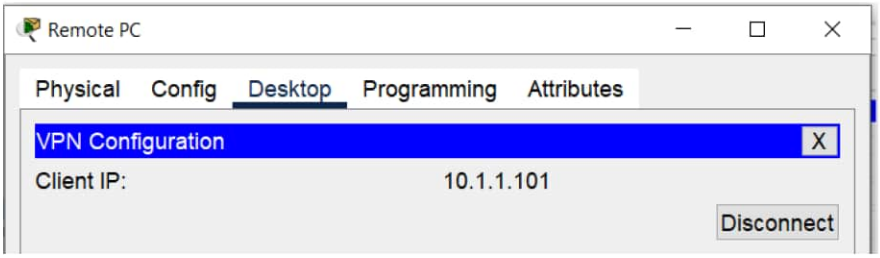

Рисунок 3.15 – Успішне підключення через VPN

3.4.7 Контроль доступу до зовнішніх державних сервісів

Для забезпечення обмеженого доступу до інформаційних систем, наприклад до API державних реєстрів (ЄДР, реєстру НАЗК, порталу Дія тощо), у мережі впроваджено списки контролю доступу (ACL). Це дає змогу обмежити вихідні з’єднання лише до дозволених IP-адрес на певних портах.

Приклад реалізації ACL на маршрутизаторі:

```
ip access-list extended CNAP-SECURITY
 permit tcp 172.21.96.0 0.0.0.63 host 185.69.144.12 eq 443
 permit tcp 172.21.96.0 0.0.0.63 host 185.69.144.13 eq 443
 deny ip 172.21.96.0 0.0.0.63 any log

interface GigabitEthernet0/0
 ip access-group CNAP-SECURITY out
```

Така політика дозволяє вузлам VLAN Dep3 (адміністратори) підключатися тільки до зазначених IP-адрес по HTTPS і блокує всі інші вихідні запити.

3.4.8 Аудит безпеки та журналювання подій

З метою відповідності вимогам КСЗІ і запобігання інцидентам у мережі реалізовано аудит дій користувачів та адміністраторів.

Увімкнено syslog-запис на центральному маршрутизаторі:

```
logging 172.21.96.244
logging trap informational
service timestamps log datetime msec
```

3.5 Тестування та перевірка працездатності розробленої мережі

Виконано т.зв. echo-запити з комп'ютерів кожного відділу на сервер організації E-mail та між собою (див. рис. 3.16). Результати виконання запитів відображені у табл. 2.4.

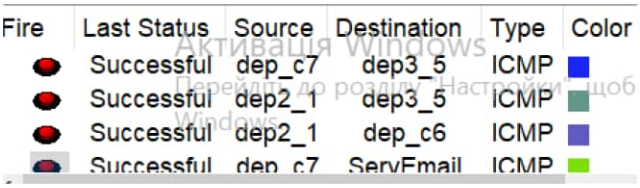

Рисунок 3.16 – Результати `ping`

Таблиця 2.4 – Результати `ping` в межах Central

Від	До	Чи успішний запит?
Відділ 1	Відділ 2	успішно
Відділ 2	Відділ 3	успішно
Відділ 3	Відділ 1	успішно
Відділ 1	Email-сервер	успішно
Відділ 2	Email-сервер.	успішно
Відділ 3	Email-сервер	успішно
Wireless	Email-сервер	успішно
Wireless	Відділ 1	успішно
Wireless	Відділ 2	успішно
Wireless	Відділ 3	успішно

В додатку А конфігураційний файл комутатора Cisco SW_R1 обсягом 2988 байт включає в себе важливі налаштування, які впливають на мережеву безпеку та управління трафіком. Конфігурація комутатора SW_R1 передбачає значні зусилля щодо забезпечення мережевої безпеки через використання ARP Inspection і DHCP Snooping, а також налаштування Port Security

4 РОЗРОБКА КОНТЕЙНЕРИЗОВАНОГО ЗАСТОСУНКУ ДЛЯ ЗБОРУ ТА АНАЛІЗУ ТЕЛЕМЕТРИЧНИХ ДАНИХ

4.1 Обґрунтування вибору архітектури

З урахуванням потреби у гнучкому та масштабованому рішенні для моніторингу стану комутаційного обладнання в ЦНАП, було обрано підхід із використанням контейнеризованого програмного забезпечення. Для реалізації збору телеметрії з пристрою Cisco Catalyst 9300 застосовано можливості платформи Cisco IOx, яка забезпечує виконання легких Linux-контейнерів безпосередньо на мережевому пристрої.

Контейнерний застосунок побудований за мікросервісним принципом і складається з наступних функціональних блоків (рис.4.1):

– модуля збору телеметрії через протокол SNMP;

– бази даних InfluxDB, яка слугує для зберігання часових рядів;

– веб-сервера Flask, що надає інтерфейс для перегляду останніх показників;

– механізму контейнеризації на основі Docker.

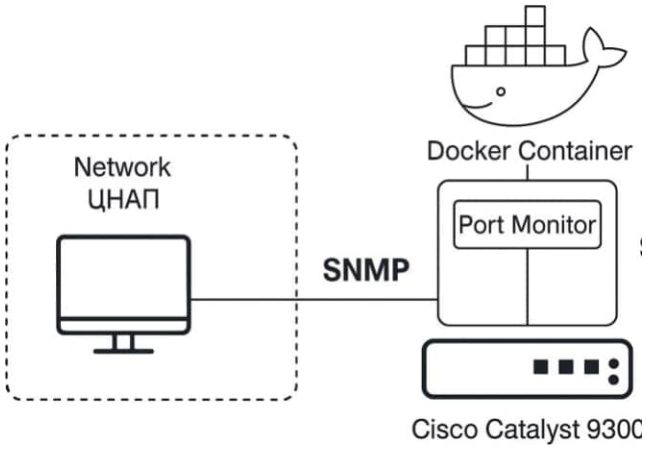

Рисунок 4.1 – Архітектура застосунку

Таким чином, уся система моніторингу функціонує автономно, без потреби у зовнішньому сервері, що значно спрощує інфраструктуру й підвищує надійність.

4.2 Середовище розгортання

Для тестування та демонстрації працездатності розробленого контейнеризованого рішення було використано публічну лабораторію Cisco DevNet Sandbox, зокрема конфігурацію Catalyst 9000 Always-On (доступна за посиланням: https://devnetsandbox.cisco.com/DevNet/catalog/Cat9k-Always-On_cat9k-always-on) (рис.4.2).

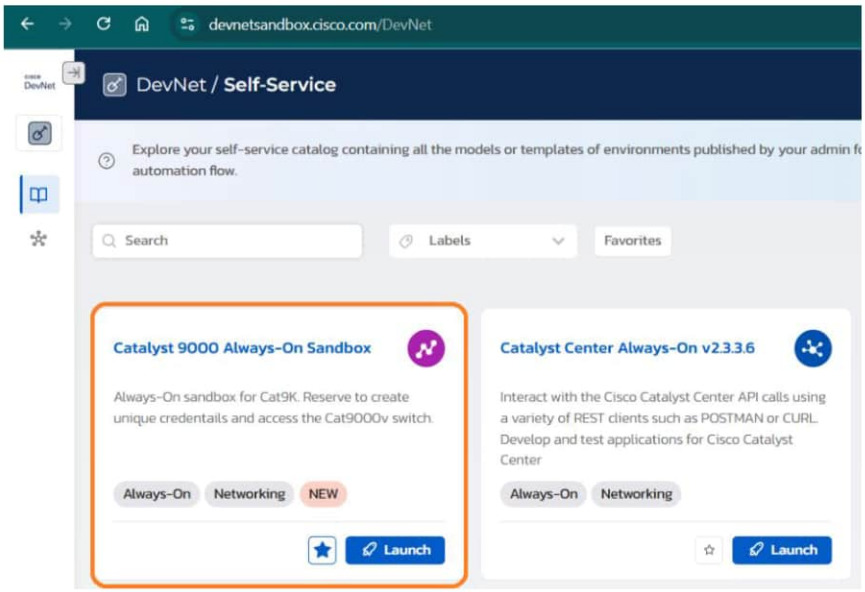

Рисунок 4.2 – DevNet Sandbox Catalyst 9000 Always-On

Це віртуальне середовище надає доступ до Cisco Catalyst C9300 з активованою платформою IOx, а також дозволяє підключення через SSH (рис. 4.3) та доступ до Linux Shell.

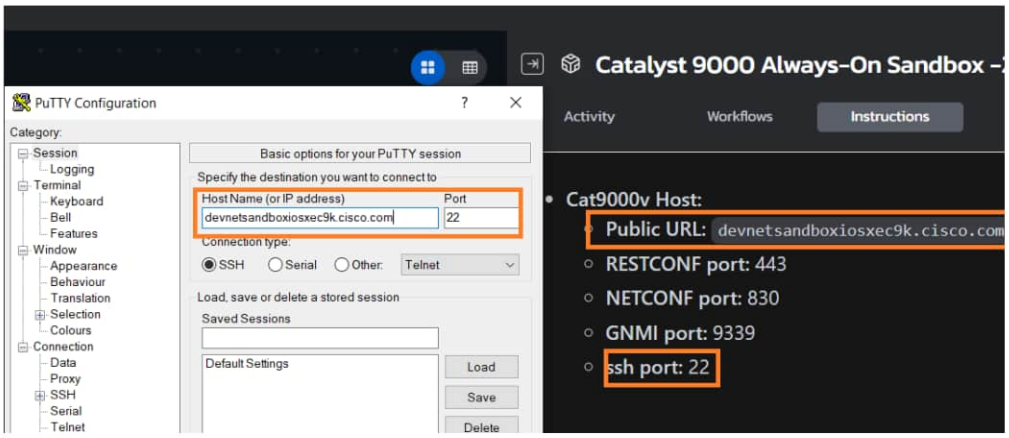

Рисунок 4.3 – Підключення до Cisco Catalyst C9300 по ssh

4.3 Вибір засобів розробки

Для реалізації завдання були обрані наступні програмні засоби:

– мова Python 3.10 завдяки гнучкості, багатій бібліотечній екосистемі та підтримці роботи зі SNMP, REST, базами даних;

– бібліотека pysnmp для взаємодії з SNMP-агентом комутатора;

– influxdb-client для збереження телеметричних даних;

– Flask легковаговий веб-фреймворк для реалізації простого інтерфейсу користувача;

– Docker як засіб контейнеризації, підтримуваний на пристроях Cisco 9300 через платформу IOx.

4.4 Структура та функціонування застосунку

У межах проєкту було реалізовано Python-застосунок, що складається з декількох логічно взаємопов’язаних модулів (рис. 4.4).

Модуль snmp_collector.py відповідає за періодичний збір телеметрії (кількість вхідних і вихідних октетів) з двох портів комутатора за допомогою SNMP-підключення. Використовуються стандартні OID:

– 1.3.6.1.2.1.2.2.1.10 – ifInOctets;

– 1.3.6.1.2.1.2.2.1.16 – ifOutOctets.

Він кожні 30 секунд збирає in_bytes та out_bytes з портів GigabitEthernet1/0/1 і 1/0/2. Визначає байти вхідного та вихідного трафіку за допомогою SNMP (ifInOctets та ifOutOctets). Зберігає кожний знімок у JSON файлі з таймштампом у папці data/.

Модуль analyzer.py бере два останні JSON-файли з папки data/, розраховує середнє навантаження за заданий інтервал часу, виводить % використання кожного порту.

Модуль notifier.py імпортує модулі аналізу (analyzer.py), розраховує навантаження, створює попередження для портів, де навантаження перевищує 80%. Зберігає сповіщення у вигляді JSON у папці data/.

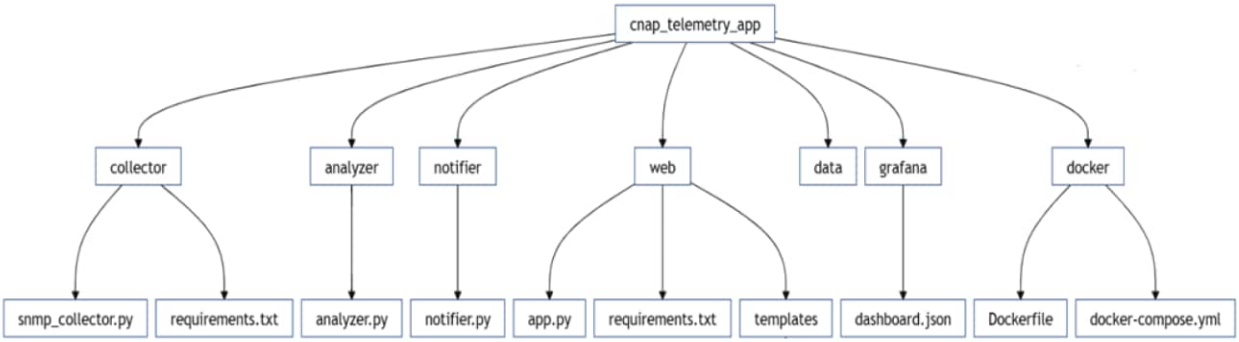

Рисунок 4.4 – Діагарма розгортання

Модуль influx_config.py забезпечує ініціалізацію клієнта InfluxDB та створення бази даних, якщо вона відсутня.

Веб-сервер app.py реалізовано на Flask. Дозволяє переглядати останні зібрані показники через HTML-інтерфейс. Дані вибираються з бази даних за допомогою мови запитів InfluxQL.

Структура web:

– app.py – основний Flask-сервер;

– templates/index.html – простий шаблон для відображення даних;

– requirements.txt – залежності (Flask, requests).

Шаблон dashboard.html забезпечує табличне відображення останніх 10 записів з телеметричними показниками.

Уся система обгорнута у Dockerfile, який описує процес контейнеризації. При запуску контейнера запускаються обидва процеси: збір телеметрії та веб-інтерфейс.

4.5 Створення контейнера

```
docker pull dockercisco/telemetryreceiver
docker tag dockercisco/telemetryreceiver port-monitor-
receiver
docker save port-monitor-receiver > telemetryreceiver.tar
```

4.6 Розгортання контейнерного застосунку на комутаторі Cisco 9300

Після цього його було упаковано у .tar-архів, придатний для інсталяції через app-hosting CLI Cisco.

Застосунок розгортається безпосередньо на комутаторі Cisco Catalyst 9300 з підтримкою IOx, що дозволяє запускати Docker-контейнери. Наступні команди послідовно активують контейнер, прив’язують ресурси і запускають процес моніторингу.

Увімкнення IOx-сервісу:

```
conf t
iox
```

#Завантаження підготовленого контейнера через SCP:

```
scp telemetryreceiver.tar developer@<sandbox-ip>:flash:
```

#Інсталяція та активація контейнера:

```
app-hosting install appid telemetryreceiver package
flash:telemetryreceiver.tar
app-hosting activate appid telemetryreceiver

app-hosting start appid telemetryreceiver
```

#Взаємодія з контейнером через консоль:

```
app-hosting connect appid port-monitor console
```

Перевірка статусу

```
app-hosting list
app-hosting show appid telemetryreceiver
```

Контейнер працює у фоновому режимі, з періодичним (раз на 10 секунд) опитуванням SNMP-агента комутатора, збереженням даних до InfluxDB та обслуговуванням локального веб-інтерфейсу.

4.7 Вивід телеметричних даних

Налаштування потоку телеметрії (на Catalyst 9300) на прикладі iperf.

```
telemetry ietf subscription 100
 encoding encode-kvgpb
 filter xpath /interfaces/interface/state
 stream yang-push
 update-policy sample interval 1000
 receiver ip address 172.16.1.2 port 50001 protocol grpc-tcp
```

Перевірити:

```
show telemetry ietf subscription
```

На рис. 4.5 наведено приклад фрагменту веб-інтерфейсу, який відображає останні зібрані телеметричні значення. Можемо перейти за адресою http://localhost:5000 для перегляду графіків.

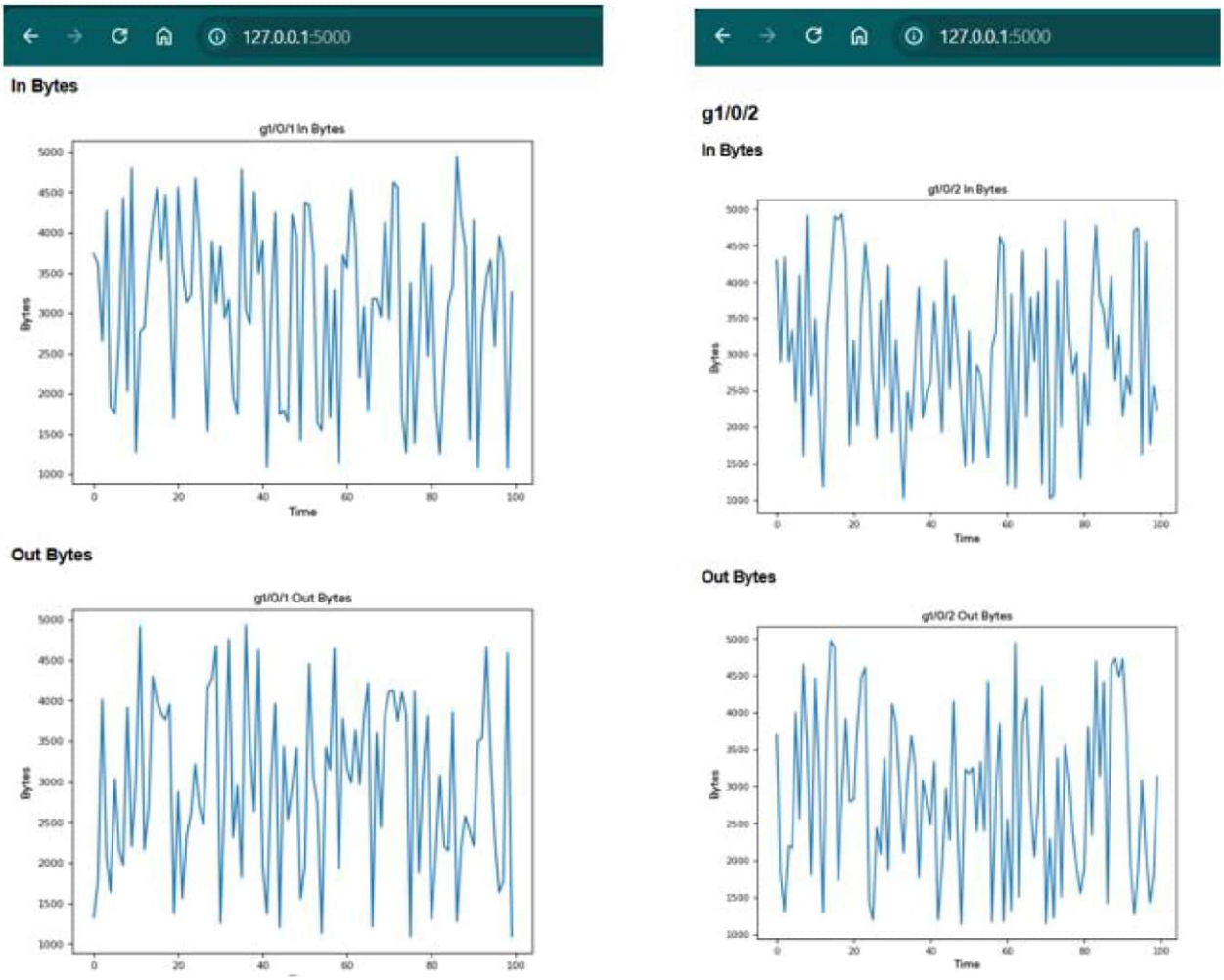

Рисунок 4.5 – Вивід телеметричних даних

4.8 Тестування та результати

Для тестування системи на наявність перевантажень, збоїв і аномалій було згеровано фіктивні дані в до 5 разів для кожного порту.

Щоб згенерувати мережний трафік для 1-гігабітного порту, ми повинні врахувати, що 1 Гігабіт на секунду (Гбіт/с) дорівнює 1 000 000 000 біт/с або приблизно 125 000 000 байт/с. За допомогою цієї інформації, ми можемо створити дані, які симулюють трафік, що може досягати 1 Гб/с, і врахувати перевищення порогового значення.

У нашому випадку, ми можемо згенерувати дані для in_bytes та out_bytes, які варіюються від 0 до 125 000 000 байт (наближаючись до 1 Гб) за певний проміжок часу.

Відображення графіків для вхідного й вихідного трафіку з показником порогу як червона лінія на рисунку 4.6.

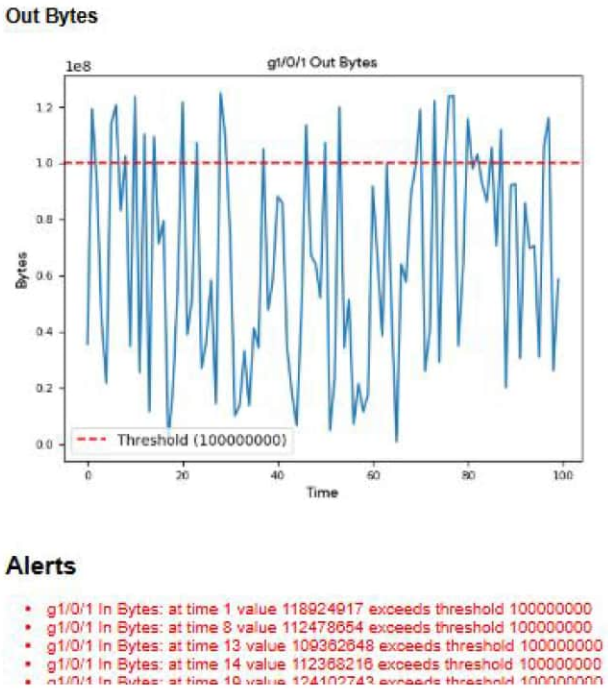

Рисунок 4.6 – Мережний трафік з перевантаженням

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи досягнуто поставлену мету – розроблено та протестовано комп'ютерну систему для центру надання адміністративних послуг (ЦНАП), що включає сучасну інфраструктуру корпоративної мережі та спеціалізований контейнеризований застосунок для збору телеметричних даних з комутаційного обладнання.

Під час виконання роботи було:

– проаналізовано вимоги до функціонування IT-системи ЦНАП, визначено логічну та фізичну топологію мережі, запропоновано структуру з поділом на VLAN, централізованими сервісами DHCP, DNS, NAT, а також інтеграцією засобів моніторингу;

– обґрунтовано вибір комутатора Cisco Catalyst 9300 як базового елемента інфраструктури, що підтримує розміщення застосунків у контейнерах через платформу IOx;

– розроблено контейнеризований застосунок на мові Python, який здійснює періодичний збір телеметричних показників через SNMP-протокол (in/out octets інтерфейсів), зберігає їх у базі даних InfluxDB та надає доступ до інформації через веб-інтерфейс, створений з використанням Flask;

– зібрано Docker-образ, який було протестовано на реальному пристрої Cisco Catalyst 9300 у середовищі Cisco DevNet Sandbox, що підтвердило стабільність та відповідність рішення технічним вимогам;

У результаті було реалізовано повноцінну систему моніторингу телеметричних даних на основі контейнеризованого застосунку, що розгортається безпосередньо на мережевому комутаторі. Система характеризується автономністю, низькими ресурсними вимогами, розширюваністю та можливістю подальшої інтеграції з зовнішніми інструментами візуалізації (наприклад, Grafana). Це дозволяє використовувати запропоноване рішення у масштабованій інфраструктурі ЦНАП для контролю стану мережевих інтерфейсів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1 Про адміністративні послуги [Електронний ресурс] : Закон України № 5203-VI від 06.09.2012 р. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/5203-17.

2 Design Zone SBA Navigation. AI Infrastructure, Secure Networking, and Software Solutions - Cisco. URL: https://www.cisco.com/assets/sol/ent/dz/sba/subway/index.html (date of access: 18.06.2025).

3 Як створити ЦНАП – досвід інституційного створення ЦНАП у рамках Програми «U-LEAD з Європою». 2021. 200 с. URL: https://prosto.in.ua/documents/41/Well-functioning-ASC_2021.pdf (дата звернення: 01.05.2025).

4 ITU-T Recommendation X.1037. Security Architecture for Internet Protocol Networking / International Telecommunication Union. – 2022.

5 Stallings, W. Data and Computer Communications / W. Stallings. – 11-е вид. – Boston : Pearson, 2020. – С. 315–328.

6 Kumar, M. Simulation Based Study of DHCP Snooping and ARP Inspection Using Cisco Packet Tracer / M. Kumar, R. Kaur // International Journal of Advanced Research in Computer Science and Software Engineering. – 2018. – Т. 8, № 4. – С. 212–218.

7 DHCP Starvation Attack. ProSec GmbH. URL: https://www.prosec-networks.com/en/blog/dhcp-starvation-attack/ (date of access: 21.04.2025).

8 DHCP STARVATION URL: https://www.researchgate.net/publication/364604011_DHCP_STARVATION (date of access: 21.04.2025).

9 Атаки типу Man-In-The-Middle: що треба знати кожному. Домени – перевірка та реєстрація доменів в Україні | Imena.ua. URL: https://www.imena.ua/blog/man-in-the-middle/ (дата звернення: 25.04.2025).

10 Programmability Configuration Guide, Cisco IOS XE 17.14.x - Application Hosting [Cisco IOS XE 17.14.1]. Cisco. URL:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/1714/b_1714_programmability_cg/m_1714_prog_app_hosting.html (date of access: 22.06.2025).

11 DevNet C. Sample Application: TRex - Deploy an Application to the Catalyst 9000 - Application Hosting on Catalyst 9K Switching - Cisco DevNet Learning Labs Center. Cisco DevNet Learning Labs Center. URL: https://developer.cisco.com/learning/modules/app-hosting-cat9k/app-hosting-deploy/sample-application-trex/ (date of access: 22.05.2025).

Додаток А

Текст програми налаштування комутатора SW_R1

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ КОМУТАТОРА SW_R1

Текст програми

804.02070743.25002-01 12 01

Листів 5

2025

АНОТАЦІЯ

Дане налаштування належить комутатору Cisco SW_R1 обсягом 2988 байт та включає в себе важливі налаштування, які впливають на мережеву безпеку та управління трафіком. Конфігурація комутатора SW_R1 передбачає значні зусилля щодо забезпечення мережевої безпеки через використання ARP Inspection і DHCP Snooping, а також налаштування Port Security

ЗМІСТ

1. Конфігураційний файл комутатора SW_R1 ……4

Конфігураційний файл комутатора SW_R1

```
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sw_R1
!
enable secret 5 $1$mERr$5.a6P4JqbNiMX01usIfka/
!
!
no ip domain-lookup
ip domain-name bak2025.com
!
username admin privilege 1 password 7 0822455D0A16
!
ip arp inspection vlan 10
!
ip dhcp snooping vlan 10,20,30,40,60
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/6
 switchport access vlan 10
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0030.A391.2EAA
!
```

```
interface FastEthernet0/7
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/8
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/9
 switchport access vlan 10
 switchport mode access
!
!
interface GigabitEthernet0/1
 switchport trunk native vlan 50
 ip arp inspection trust
 ip dhcp snooping trust
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk native vlan 50
 switchport mode trunk
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan40
 ip address 172.21.96.147 255.255.255.248
!
!
line con 0
 password 7 0822455D0A16544541
!
line vty 0 4
 password 7 0822455D0A16544541
 login
 transport input ssh
line vty 5 15
 login
!
!
!
!
end
```

Додаток Б

Текст програми застосунку для збору телеметричних даних для Cisco Catalyst 9300

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ

КОНТЕЙНЕРЗОВАНИЙ ЗАСТОСУНОК ДЛЯ ЗБОРУ ТЕЛЕМЕТРИЧНИХ ДАНИХ НА CISCO CATALYST 9300

Текст програми

804.02070743.25002-01 12 01

Листів 8

2025

АНОТАЦІЯ

Додаток містить повний вихідний код програмного застосунку, реалізованого в межах кваліфікаційної роботи, який забезпечує збір, обробку, зберігання та візуалізацію телеметричних даних з портів комутатора Cisco Catalyst 9300.

Застосунок реалізовано мовою програмування Python 3.10 із використанням бібліотек pysnmp, influxdb-client та Flask, які забезпечують відповідно:

– виконання SNMP-запитів до пристрою для отримання показників завантаження портів (вхідні та вихідні октети);

– збереження даних у базі InfluxDB у вигляді часових рядів;

– побудову веб-інтерфейсу, через який користувач може переглядати поточні показники в табличному вигляді.

ЗМІСТ

1. snmp_collector.py ……..……..……4
2. analyzer.py ……..……..……5
3. notifier.py……..6
4. app.py…….……..……7
5. Dockerfile…….……8

1. Код для збору даних за допомогою SNMP

snmp_collector.py

```
import time
import json
from pysnmp.hlapi import *

class SNMPCollector:
    def __init__(self, host: str, port: int, community: str,
interfaces: list):
        self.host = host
        self.port = port
        self.community = community
        self.interfaces = interfaces

    def get_snmp_data(self, oid: str):
        iterator = getCmd(
            SnmpEngine(),
            CommunityData(self.community),
            UdpTransportTarget((self.host, self.port)),
            ContextData(),
            ObjectType(ObjectIdentity(oid))
        )
        errorIndication, errorStatus, errorIndex, varBinds =
next(iterator)

        if errorIndication:
            print(errorIndication)
        elif errorStatus:
            print(f'Error: {errorStatus.prettyPrint()}')
        else:
            return {str(varBinds[0].getOid()):
str(varBinds[0].getValue())}

    def collect_data(self):
        data = {}
        for interface in self.interfaces:
            input_bytes_oid =
f'1.3.6.1.2.1.2.2.1.10.{interface}'  # ifInOctets
            output_bytes_oid =
f'1.3.6.1.2.1.2.2.1.16.{interface}'  # ifOutOctets
            interface_speed_oid =
f'1.3.6.1.2.1.2.2.1.5.{interface}'  # ifSpeed

            input_bytes =
self.get_snmp_data(input_bytes_oid)
            output_bytes =
self.get_snmp_data(output_bytes_oid)
            interface_speed =
self.get_snmp_data(interface_speed_oid)
```

```
            data[interface] = {
                'input_bytes':
int(input_bytes.get(input_bytes_oid, 0)),
                'output_bytes':
int(output_bytes.get(output_bytes_oid, 0)),
                'interface_speed':
int(interface_speed.get(interface_speed_oid, 0))
            }
        return data

if __name__ == '__main__':
    collector = SNMPCollector('192.168.1.1', 161, 'public',
['1', '2'])
    while True:
        collected_data = collector.collect_data()
        print(json.dumps(collected_data, indent=4))
        time.sleep(60)
```

2. Файл: analyzer.py

```
class Analyzer:
    def __init__(self, data: dict, time_interval: int):
        self.data = data
        self.time_interval = time_interval

    def average_utilization(self, input_bytes, output_bytes,
interface_speed):
        if interface_speed == 0:
            return 0
        return (input_bytes + output_bytes) /
(interface_speed * self.time_interval)

    def analyze(self):
        results = {}
        for interface, values in self.data.items():
            utilization =
self.average_utilization(values['input_bytes'],

values['output_bytes'],

values['interface_speed'])
            results[interface] = utilization
        return results

Код для сповіщення про перевантаження
Файл: notifier.py
import smtplib
from email.mime.text import MIMEText

class Notifier:
    def __init__(self, threshold: float, recipient_email:
str):
```

```
        self.threshold = threshold
        self.recipient_email = recipient_email

    def send_notification(self, interface: str, utilization:
float):
        msg = MIMEText(f"Warning: Port {interface} is
overloaded with utilization {utilization:.2f}%.")
        msg['Subject'] = 'Port Overload Notification'
        msg['From'] = 'monitoring@yourdomain.com'
        msg['To'] = self.recipient_email

        try:
            with smtplib.SMTP('smtp.yourdomain.com') as
server:
                server.login('your_email', 'your_password')
                server.sendmail(msg['From'], [msg['To']],
msg.as_string())
            print(f"Notification sent for {interface} with
utilization {utilization:.2f}%.")
        except Exception as e:
            print(f"Failed to send notification: {e}")

    def check_utilization(self, utilization_results: dict):
        for interface, utilization in
utilization_results.items():
            if utilization > self.threshold:
                self.send_notification(interface,
utilization)
```

3. notifier.py

```
import json
import os
import time
from analyzer.analyzer import load_latest_two_snapshots,
analyze_utilization

# ????? ????????????? (? %)
THRESHOLD = 80.0

def check_overload(utilization):
    alerts = {}
    for iface, load in utilization.items():
        if load > THRESHOLD:
            alerts[iface] = f"?? ????????????? ?? ?????
{iface}: {load}%"
    return alerts

def save_alerts(alerts, folder="data"):
    timestamp = int(time.time())
    filename = os.path.join(folder,
f"alerts_{timestamp}.json")
```

```
    with open(filename, "w") as f:
        json.dump(alerts, f, indent=4)
    print(f"?????????? ????????? ? ????: {filename}")

if __name__ == "__main__":
    try:
        snap1, snap2 = load_latest_two_snapshots()
        utilization = analyze_utilization(snap1, snap2)
        alerts = check_overload(utilization)

        if alerts:
            for alert in alerts.values():
                print(alert)
            save_alerts(alerts)
        else:
            print("????????????? ?? ????????.")

    except Exception as e:
        print(f"??????? ??? ????????? ?????????: {e}")
```

4. app.py

```
from flask import Flask, render_template, jsonify
import os
import json
import glob

app = Flask(__name__)

DATA_FOLDER = "../data"

def load_latest_json(pattern):
    files = sorted(glob.glob(os.path.join(DATA_FOLDER,
pattern)), reverse=True)
    if files:
        with open(files[0], 'r', encoding='utf-8') as f:
            return json.load(f)
    return {}

@app.route("/")
def index():
    telemetry = load_latest_json("telemetry_*.json")
    alerts = load_latest_json("alerts_*.json")
    return render_template("index.html",
telemetry=telemetry, alerts=alerts)

@app.route("/api/telemetry")
def api_telemetry():
    telemetry = load_latest_json("telemetry_*.json")
    return jsonify(telemetry)

@app.route("/api/alerts")
```

```
def api_alerts():
    alerts = load_latest_json("alerts_*.json")
    return jsonify(alerts)

if __name__ == "__main__":
    app.run(host="0.0.0.0", port=5000, debug=True)
```

5. Dockerfile

```
# Базовий образ
FROM python:3.9-slim

# Встановлення залежностей
COPY requirements.txt .
RUN pip install --no-cache-dir -r requirements.txt

# Копіюємо файли з проекту
COPY . /app
WORKDIR /app

# Запуск Flask додатка
CMD ["python", "app.py"]


ocker Compose файл
Файл: docker-compose.yml

version: '3'

services:
  snmp_collector:
    build: .
    ports:
      - "5000:5000"

  influxdb:
    image: influxdb:1.8
    ports:
      - "8086:8086"
    volumes:
      - influxdb-data:/var/lib/influxdb

volumes:
  influxdb-data:
```