

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

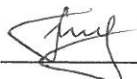
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проєкт системи захищеного обміну даними
з рухомим транспортом»

Виконав студент 4-го курсу групи ЗКБ-18
спеціальності 125 «Кібербезпека»

 Михайло Хохлов

Керівник старший викладач кафедри КІ та КБ

 Олександра Покотило

Рецензент старший викладач кафедри КІ та КБ

 Єлизавета Байлюк

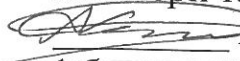
Житомир – 2022

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
1 березня 2022 р.

ЗАВДАННЯ

на випускн кваліфікаційну роботу бакалавра

Студент: Хохлов Михайло Олегович

Тема роботи: «Проект системи захищеного обміну даними з рухомим транспор-
том»

затверджена Наказом університету від 1 березня 2022 р. № 128/с

Термін здачі студентом закінченої роботи 10 червня 2022 р.

Вихідні дані роботи:

Обладнання та програмне забезпечення:

1. Програмне забезпечення Cisco Packet Tracer
2. Обладнання Cisco

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Покотило О.А.	1.03.2022	1.03.2022
2	Покотило О.А.	1.03.2022	1.03.2022
3	Покотило О.А.	1.03.2022	1.03.2022

Студент

Керівник




Михайло Хохлов

Олександра Покотило

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 березня 2022 – 7 березня 2022	Виконано
2	Розробка плану роботи	8 березня 2022 – 11 березня 2022	Виконано
3	Розробка розгорнутого плану	12 березня 2022 – 16 березня 2022	Виконано
4	Подача чернетки керівнику для перевірки	17 березня 2022 – 19 березня 2022	Виконано
5	Подача чистовика керівнику	20 березня 2022 – 24 березня 2022	Виконано
6	Затвердження графічних матеріалів у керівника	25 березня 2022 – 30 березня 2022	Виконано
7	Проведення попереднього захисту	2 червня 2022	Виконано
8	Отримання відгуку керівника	20 червня 2022 – 22 червня 2022	Виконано
9	Допуск начальника кафедри	23 червня 2022 – 24 червня 2022	Виконано
10	Подання роботи на рецензування	24 червня 2022	Виконано
11	Початок захисту кваліфікаційних робіт	27 червня 2022	Виконано

Студент  Михайло Хохлов
 Керівник  Олександра Покотило

РЕФЕРАТ

Випускна робота бакалавра складається з системи захищеного обміну даними з рухомим транспортом, топології мережі та пояснювальної записки. Пояснювальна записка до випускної роботи містить 84 сторінок, 77 ілюстрацій та 4 таблиці.

Організація інформаційної безпеки є однією з найбільш актуальних проблем в галузі інформаційних технологій на сьогоднішній день. У сучасному світі актуалізуються рішення Інтернету речей, завдання забезпечення інформаційної безпеки у яких також мають пріоритетний характер. Продовжуючи швидко розповсюджуватись та розвиватись, глобальна мережа стійко закріпилася як найбільший та найкращий спосіб комунікації. Зараз неможливо уявити побудову новітніх технологій, ідей та планів без використання цього могутнього інструменту. Саме завдяки єднанню мереж, які утворюють Інтернет, всесвітній доступ до інформації для кожного перестав бути міфом минулого. Мережі вже відіграють велику роль у розвитку суспільства та реалізації безлічі проектів.

Удосконалення безпеки інформації на транспортному підприємстві є важливим фактором подальшого успіху у розвитку та комерційній діяльності, тому було вирішено створити систему захищеного обміну даними з рухомим складом підприємства, маскимально знижуючи ризики витоку інформації.

Наведена загальна топологія мережі, опис конкретних серій обладнання, опис політики безпеки та тестування проекту. Також наводяться результати тестування захисту передачі даних мережі організації.

КЛЮЧОВІ СЛОВА: МЕРЕЖА, VPN, CISCO, ЗАХИСТ МЕРЕЖ, Internet of Things.

					Державний університет «Житомирська політехніка». 22.125.03.000 – ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата	Проект системи захищеного обміну даними з рухомим транспортом Пояснювальна записка	Літ.	Арк.	Аркушів
Розроб.		Хохлов М.О.		10.06.22				
Керівник		Покотило О. А.		24.06.22			4	117
Н. контр.						ФІКТ, гр. ЗКБ-18		
Рецензент.		Бабілюк Є.М.		24.06.22				
Зав. каф.		Єфіменко А. А.		24.06.22				

ABSTRACT

The bachelor's graduation consists of a secure data exchange system with mobile transport, network topology and explanatory note. The explanatory note to the thesis contains 84 pages, 77 illustrations and 4 tables.

The organization of information security is one of the most pressing issues in the field of information technology today. In today's world, Internet of Things solutions are becoming more and more important, in which the tasks of information security are also a priority. Continuing to spread and develop rapidly, the global network has become firmly established as the largest and best way to communicate. It is now impossible to imagine building the latest technologies, ideas and plans without the use of this powerful tool. It is thanks to the connection of the networks that make up the Internet that universal access to information for everyone has ceased to be a myth of the past. Networks already play an important role in the development of society and the implementation of many projects.

Improving information security at the transport company is an important factor in further success in development and business, so it was decided to create a secure data exchange system with the company's rolling stock, minimizing the risk of information leakage.

The general topology of the network, description of specific series of equipment, description of security policy and project testing are given. The results of testing the data protection of the organization's network are also presented.

KEY WORDS: NETWORK, VPN, CISCO, NETWORK PROTECTION, Internet of Things.

ЗМІСТ

РЕФЕРАТ.....	4
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	8
ВСТУП.....	9
РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ОБҐРУНТУВАННЯ АКТУАЛЬНОСТІ ТЕМИ РОБОТИ.....	11
1.1. ОБҐРУНТУВАННЯ АКТУАЛЬНОСТІ ТЕМИ РОБОТИ ПО РОЗРОБЦІ СИСТЕМИ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ З РУХОМИМ ТРАНСПОРТОМ.....	11
1.2. АНАЛІЗ ВІДОМИХ СИСТЕМ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ З РУХОМИМ ТРАНСПОРТОМ	14
1.3. АНАЛІЗ ЕТАЛОННОЇ АРХІТЕКТУРИ INTERNET OF THINGS (IoT)	19
1.4. АНАЛІЗ ВИМОГ ДО СИСТЕМ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ З РУХОМИМ ТРАНСПОРТОМ	24
1.5. ПОСТАНОВКА ЗАВДАННЯ	25
Висновки по 1 розділу	25
РОЗДІЛ 2. РОЗРОБКА СИСТЕМИ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ З РУХОМИМ ТРАНСПОРТОМ	26
2.1. РОЗРОБКА СТРУКТУРНОЇ СХЕМИ СИСТЕМИ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ З РУХОМИМ ТРАНСПОРТОМ	26
2.2. ВИБІР ТЕХНІЧНИХ ЗАСОБІВ ДЛЯ РЕАЛІЗАЦІЇ СИСТЕМИ.....	33
2.3. ВИБІР ПРОТОКОЛІВ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ В СИСТЕМІ.....	44
2.4. РОЗРОБКА ФУНКЦІОНАЛЬНОЇ СХЕМИ СИСТЕМИ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ З РУХОМИМ ТРАНСПОРТОМ.....	49
Висновки по 2 розділу	55
РОЗДІЛ 3. ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ ТА ЕФЕКТИВНОСТІ ПРИЙНЯТИХ РІШЕНЬ В СИСТЕМІ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ З РУХОМИМ ТРАНСПОРТОМ	56
3.1. РОЗРОБКА МОДЕЛІ СИСТЕМИ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ З РУХОМИМ ТРАНСПОРТОМ В CISCO PACKET TRACER	56
3.2. РОЗРОБКА МАКЕТУ СИСТЕМИ ТА ОЦІНКА ЇЇ ПРАЦЕЗДАТНОСТІ.....	64

3.3. РЕКОМЕНДАЦІЇ ПО ЗАСТОСУВАННЮ ТА ВДОСКОНАЛЕННЮ РОЗРОБЛЕНОЇ СИСТЕМИ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ З РУХОМИМ ТРАНСПОРТОМ	81
Висновки по 3 розділу	82
ВИСНОВКИ	83
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	84
ДОДАТКИ.....	89
Додаток А.....	90
Додаток Б	91
Додаток В.....	103

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DHCP – Dynamic Host Configuration Protocol

HSRP – Hot Standby Router Protocol, Hot Standby Redundancy Protocol

IKE – Internet Key Exchange

IP – Internet Protocol

IPSec – Internet Protocol Security

L2TP – Layer 2 Tunneling Protocol

LAN – Local Area Network

NTP – Network Time Protocol

OSI – Open Systems Interconnection

PPTP – Point-to-Point Tunneling Protocol

SYSLOG – System log

TCP – Transmission Control Protocol

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

WAN – Wide Area Network

WLAN – Wireless Local Area Network

ОС – операційна система

ВСТУП

Актуальність роботи. Забезпечення інформаційної безпеки [1] є однією з найбільш актуальних проблем в галузі інформаційних технологій на сьогоднішній день. У сучасному світі актуалізуються рішення Інтернету речей, завдання забезпечення інформаційної безпеки у яких також мають пріоритетний характер. Продовжуючи швидко розповсюджуватись та розвиватись, глобальна мережа стійко закріпилася як найбільший та найкращий спосіб комунікації. Зараз неможливо уявити побудову новітніх технологій, ідей та планів без використання цього могутнього інструменту. Саме завдяки єднанню мереж, які утворюють Інтернет, всесвітній доступ до інформації для кожного перестав бути міфом минулого. Мережі вже відіграють велику роль у розвитку суспільства та реалізації безлічі проектів.

Забезпечення безпеки кожного підприємства чи установи – це загальна проблема для усього світу. З появою корпоративних локальних мереж, виник і ризик розкриття конфіденційної інформації організації, шляхом зовнішніх хакерських атак. Завдяки постійному розвитку технологій, були розроблені методи та шляхи захисту від подібних атак, якими зараз користуються організації та підприємства по всьому світу.

Не дивлячись на наявність безлічі засобів захисту інформації та відносну безпеку даних компаній, витоки інформації все одно трапляються. Це дає поштовх для створення та розвитку більш ефективних систем безпеки інформації на підприємстві чи установі, не кажучи про економічну доцільність від впровадження таких систем, порівнюючи можливі втрати від умовних атак.

Транспорт - одна з найпопулярніших сфер застосування інтернету речей (IoT) у розвинутих країнах. У 2019 році вона поступилася першим місцем тільки промисловості. IoT на транспорті - це мережа пристроїв, здатних збирати дані про автобуси, трамваї, машини та обмінюватися ними через інтернет. IP-камери, сенсори та датчики дозволяють автоматично контролювати все, що пов'язано з транспортними засобами: від їхнього розташування до контролю тиску в шинах.

На основі цих даних розвиваються такі сервіси, як карти пробок, табло прибуття громадського транспорту, додатки для паркування та багато інших [2].

Удосконалення безпеки інформації на транспортному підприємстві є важливим фактором подальшого успіху у розвитку та комерційній діяльності, тому було вирішено створити систему захищеного обміну даними з рухомим складом підприємства, максимально знижуючи ризики витоку інформації.

Мета дипломної роботи – удосконалення рівня обміну передачі даних з рухомим транспортом на транспортному підприємстві, завдяки створенню надійної системи захисту інформації.

Об’єкт дослідження – процес забезпечення захищеності обміну інформації транспортного підприємства з рухомим складом.

Предмет дослідження – способи та алгоритми захищеного обміну даними з рухомим транспортом.

Встановлена мета обумовлює наступні завдання:

- Обґрунтування актуальності теми досліджень.
- Аналіз відомих методів захищеного обміну даними з рухомим транспортом.
- Розробка системи захищеного обміну даними з рухомим транспортом.
- Дослідження працездатності та ефективності розробленої системи захищеного обміну даними з рухомим транспортом.
- Розробка рекомендацій щодо застосування системи захищеного обміну даними з рухомим транспортом.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ОБҐРУНТУВАННЯ АКТУАЛЬНОСТІ ТЕМИ РОБОТИ

1.1. Обґрунтування актуальності теми роботи по розробці системи захищеного обміну даними з рухомим транспортом

У кожному сегменті галузі транспорту та логістики відбувається розширення поверхні кібератак. Наприклад, серед морських перевізників відносно прості системи оповіщення про лихо та забезпечення безпеки були замінені повноцінними місцевими мережами, що базуються на хмарних технологіях, такими як програма електронної навігації Міжнародної морської організації (ММО) [2]. Такі системи та мережі є дуже ласою ціллю для хакерів, оскільки відбувається безперервний збір, обіг та аналіз бортової інформації, щоб у подальшому відстежити положення суден, детальні дані про вантаж, можливі технічні проблеми, занесені до електронних журналів та інші питання, пов'язані з океанічним середовищем.

Аналогічна ситуація в залізничному секторі: традиційні дротові системи управління рухом поїздів (СУРП), зв'язок яких із зовнішніми системами раніше був обмежений, наразі поступаються сучасним бездротовим стандартам, таким як GSM-Railway - відносно широка мережа, що зв'язує поїзди з пунктами управління рухом [3].

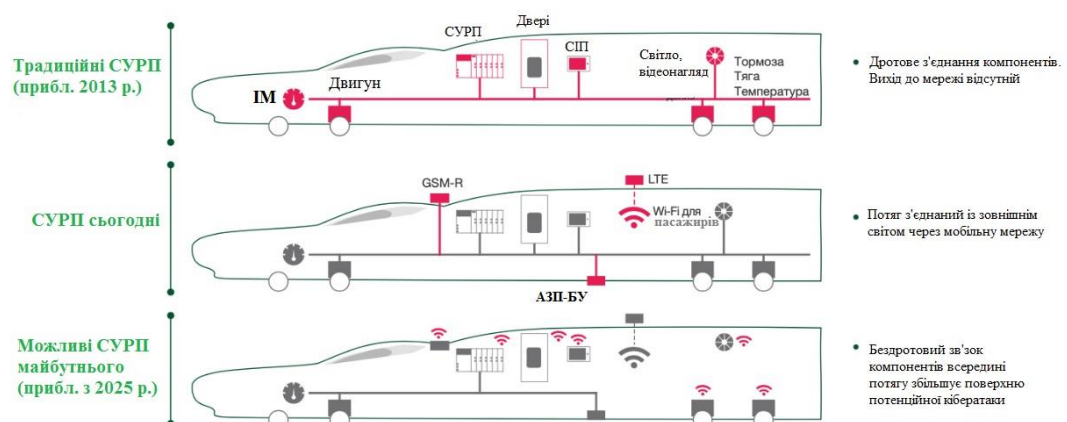


Рисунок 1.1 – Аналіз технологій потягів минулого, сьогодення та майбутнього

Примітка: ІМ – інтерфейс машиніста; СУРП – система управління рухом потягів; СІП – система інформування пасажирів; GSM-R – глобальна система зв'язку на залізниці; LTE – стандарт «довгостроковий розвиток»; АЗП – автоматична система захисту потягу; БП – бортовий прилад;

Усвідомлюючи можливу небезпеку масштабної кібератаки на галузь транспорту для світової торгівлі та економічної стабільності, регулюючі органи починають займати активнішу позицію і вимагати більшої захищеності мереж компаній. Пропоновані або вже прийняті інструменти регулювання включають Директиву ЄС про мережеву та інформаційну безпеку (NIS), окрім цього набирають чинності стандарти CLC/TS 50701 і EN 50126 [4].

Транспорт та логістика. Необхідно розмежувати великий бізнес (умовний залізничний оператор) та дрібні транспортні компанії. Проблеми великого бізнесу викликані необхідністю обслуговувати велику кількість інтерфейсів і каналів, якими відбувається обмін даними зі сторонніми організаціями. Ці дані можуть мати не лише фінансовий характер, але бути пов'язаними з характеристиками руху та трафіку на мережі. Атаки ведуться на ці інтерфейси. Внутрішні служби безпеки та ІТ працюють інтенсивно, постійно проводяться модернізації засобів захисту та контролю периметра, контролю доступу сторонніх організацій до своїх «чутливих» компонентів ландшафту додатків.

Безпосереднє відношення до транспорту має і питання забезпечення інформаційної безпеки, як захист персональних даних (ПД). Це є предметом гострих дискусій на міжнародних майданчиках. Політики різних країн намагаються знайти компроміс між забезпеченням захисту прав громадян на недоторканність приватного життя та необхідністю активізувати боротьбу з терором та тяжкими злочинами.

Проблеми громадського транспорту:

- багато роз'єднаних бортових систем, що призводить до наявності декількох шлюзів LTE/SIM-карт, а відтак і більшої вразливості всієї системи в цілому;

- Архітектура, орієнтована на старий логічний блок автомобіля (VLU), що обмежує новітні технології та обслуговування пасажирів;
- Системи часто базуються на місці і вимагають перебування персоналу на місці в Центрі управління операціями для доступу та видимості мережі.

Найбільш поширені дії правопорушників кібератак над зламаними системами, які застосовують сьогодні:

- отримали несанкціонований доступ до сервера, де зберігались конфіденційні дані;
- атакували базу даних про власників транспортних пластикових карт;
- зробили атаки на інтернет-сайти, БД, транспортних компаній різних країн;
- поширюючи віруси, навмисно перешкоджали роботі мереж, як наслідок – призупиняли роботу потягів, літаків та ін.;
- Dos-атаки (Denial of Service- "відмова в обслуговуванні") з метою погіршення трафіку або взагалі його припинення;

Впровадження новітніх систем захисту є невід'ємною частиною заходів щодо забезпечення інформаційної безпеки. Захист мережі та інформації – це один із важливих напрямків безпеки та репутації організації. Нехтуючи цим, компанії несуть великі збитки та руйнування власного іміджу. Враховуючи зростаючий інтерес зловмисників у транспортному секторі, працівникам служб безпеки компаній варто приділяти більше уваги безпеці інформації.

Таким чином, питання створення системи захисту передачі даних з рухомим складом є актуальним.

1.2 Аналіз відомих систем захищеного обміну даними з рухомим транспортом

Інформаційний обмін в сучасному світі є невід’ємною складовою нашого життя, в тому числі і для організацій та підприємств. Головною складовою будь-якої системи обміну даними, є мережа.

Розрізняють мережі двох типів:

- локальні;
- глобальні.

Локальна комп’ютерна мережа (Local Area Network – LAN) підприємства – це мережева інфраструктура, що забезпечує доступ до мережевих комунікаційних послуг і ресурсів для кінцевих користувачів і пристроїв, розташованих на одному поверсі або в одній будівлі. Важливим питанням при цьому є створення мережі підприємства, об’єднуючи групу локальних мереж, розташованих географічно неподалік. При проектуванні мережі підприємства слід пам’ятати, що вони можуть включати в себе як малі мережі, що використовують один комутатор, так і дуже великі мережі з тисячами підключень. LAN також використовується при підключенні до глобальної мережі (Wide Area Network – WAN). Конструкція забезпечує мережеву основу та послуги, зокрема:

- багаторівневе LAN-з’єднання;
- доступ працівника до дротової мережі;
- IP-Multicast для ефективного розподілу даних;
- дротова інфраструктура, готова для мультимедійних послуг.

Використовуючи ієрархічну модель проектування, дротова LAN підприємства дозволяє розподіл на певні функції, спрощуючи тим самим проектування, побудову та управління мережею.

Ієрархічний дизайн LAN включає наступні три рівні:

- рівень ядра;
- рівень розподілення;

– рівень доступу.

Рисунок 1.2 демонструє приклад ієрархічної моделі мережі:

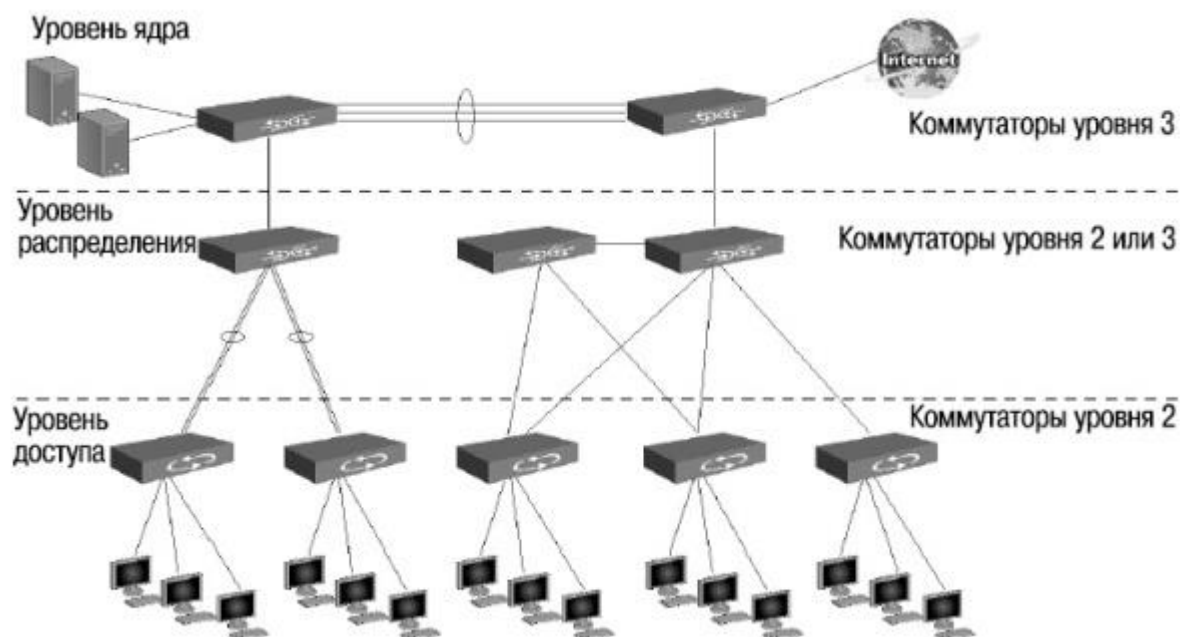


Рис. 1.2 – Ієрархічна модель мережі

Нижче наведено основні переваги розгортання трирівневих локальних мереж:

1. ієрархія

- сприяє розумінню ролі кожного пристрою на кожному рівні;
- спрощує розгортання, експлуатацію та управління;
- скорочує обсяги несправностей на кожному ярусі;

2. модульність, допомагає розширювати мережу без перешкод;

3. еластичність – задовольняє очікування користувачів щодо постійної роботи мережі;

4. гнучкість – дозволяє інтелектуально розподіляти навантаження на трафік, використовуючи всі мережеві ресурси.

Кожен рівень надає різні функціональні та мережні можливості. Так рівень ядра забезпечує зв'язок між рівнями розподілу для великих локальних мереж, рівень розподілення — групує рівні доступу і забезпечує підключення до служб, а останній, в свою чергу, — надає кінцевим точкам і користувачам прямий доступ до мережі [4].

Для з'єднання і взаємодії різних локальних мереж, в тому числі віддалених одна від одної, використовують глобальні мережі (WAN). Дана мережа може обслуговувати місто, країну або регіон світу. Вона зазвичай належить оператору зв'язку. Підприємство ж, яке використовує мережеві сервіси WAN, вносить плату за їх використання.

Враховуючи нові тенденції у розвитку технологій, транспортні підприємства з розвиненою мережею використовують технологію **VPN**. Ця технологія є захищеним шифрованим підключенням між приватними мережами за допомогою загальнодоступної мережі, наприклад Інтернету. VPN застосовує віртуальні підключення, так звані «VPN-tunnel», проходячи через Інтернет від мережі організації до віддаленого вузла або комп'ютера, в нашому випадку це буде пристрій, розміщений на транспортному засобі. Наразі, VPN поширений не лише в мережах організацій, а навіть на окремих ПК та додатках.

Кампусна мережа (CAN – Campus Area Network) – це група локальних мереж, розгорнутих на компактній території (кампусі) будь-якої установи і обслуговуючі одну цю установу – університет, промислове підприємство, порт, оптовий склад тощо. При цьому мережеве обладнання (комутатори, маршрутизатори) і середовище передачі даних (оптичноволоконний, мідний кабелі тощо) належить орендарю або власнику кампусу, підприємства, університету, уряду і так далі [5].

Простіше кажучи, кампусна мережа – це просто велика багатосегментна локальна мережа на території до декількох кілометрів в діаметрі, яка об'єднує локальні мережі близько розташованих будівель.

Загалом, багато сучасних організацій організовують з'єднання своїх відділів саме за принципом кампусної мережі. Що ж до захисту передачі даних між організацією та її віддаленою складовою (транспортним засобом), компанія Cisco вже має значний досвід у цій галузі.

Компанія Cisco Systems, на відміну від інших постачальників, пропонує не точкові продукти для захисту окремих ділянок інформаційної системи, що

вирішують завдання залізничного, морського, автомобільного та авіаційного транспорту, а саме комплексне рішення, яке інтегрується в інфраструктуру підприємства для забезпечення інформаційної безпеки бізнесу на всіх рівнях.

Self-Defending Network (SDN - "мережа, що само захищається") - стратегія компанії Cisco Systems, націлена на захист бізнес-процесів в умовах зростаючої загрози з боку шкідливих програм і зловмисників, що впливають на бізнес-процеси транспортного підприємства зсередини та ззовні.

Стратегія SDN полягає в автоматизації процесу забезпечення інформаційної безпеки за рахунок виявлення загроз, реагування відповідно до рівня критичності, ізолювання заражених або виведених з ладу вузлів, та реконфігурації мережевих пристроїв з метою запобігання повторним атакам. При цьому рішення, що входять до Self-Defending Network, однаково ефективно захищають і розподілену інфраструктуру транспортного підприємства, і його корпоративну мережу.

Захист від вторгнень (Threat Defense). Найефективніший захист бізнес-ресурсів підприємств транспортної галузі від зловмисників та шкідливих програм досягається тільки у разі ешелонованої оборони, розподіленої по всій мережі (включаючи її периметр, та її внутрішні сегменти), а не зосередженої в одному місці. Стратегія Threat Defense System інтегрує різні захисні механізми в маршрутизатори та комутатори, пропонує виділені захисні пристрої для розмежування доступу (Cisco Pix Firewall та Cisco ASA 5500 Series), відображення атак та контролю Web-контенту (Cisco IPS 4200 та Cisco Content Engine), а також дозволяє захищати кінцеві пристрої, такі як сервери та робочі станції від широкого спектру загроз (Cisco Security Agent).

Стратегія Cisco Secure Connectivity System, яка, використовує механізми аутентифікації та приховування інформації, що передається, однаково ефективно захищає дані (наприклад, від системи управління підприємством або від Web-сервера), голосу (наприклад, від IP-телефонії) та відео (наприклад, від камер відеоспостереження або в рамках відеоконференції), що передаються як

по провідних, так і бездротових з'єднаннях. Складовою частиною Secure Connectivity System є такі технології, як IPSec, SSL, SSH, GRE та MPLS [6].

Як найкращий приклад розвиненої та надійної системи, можемо розглянути проект від Cisco - Connected Mass Transit.

Connected Mass Transit забезпечує скрізну, високозахищену мережу, від транспортних засобів до зупинок громадського транспорту та ремонтних майданчиків. Система забезпечує конвергентну, багатосервісну, безпечну та засновану на стандартах інфраструктуру, завдяки якій можна покращити пасажирські та експлуатаційні можливості автобусів. Вона замінює надлишкові, запатентовані та єдині прикладні рішення з обмеженою взаємодією або взагалі без неї. Це призводить до зниження капітальних витрат, збільшення пасажиропотоку та покращення безпеки для громадського транспорту.

Ділові операції підтримують планування, комерційні, пасажирські та фінансові обрахунки. Операції автопарку зосереджені на щоденній роботі транспортної служби в режимі реального часу, включаючи розташування транспортного засобу, своєчасну роботу, відповідність маршруту та коригування маршруту, якщо необхідно. Робота транспортних засобів зосереджується на продуктивності транспортного парку, технічному обслуговуванні, оновленнях апаратних та програмних систем для оптимальної продуктивності організації.

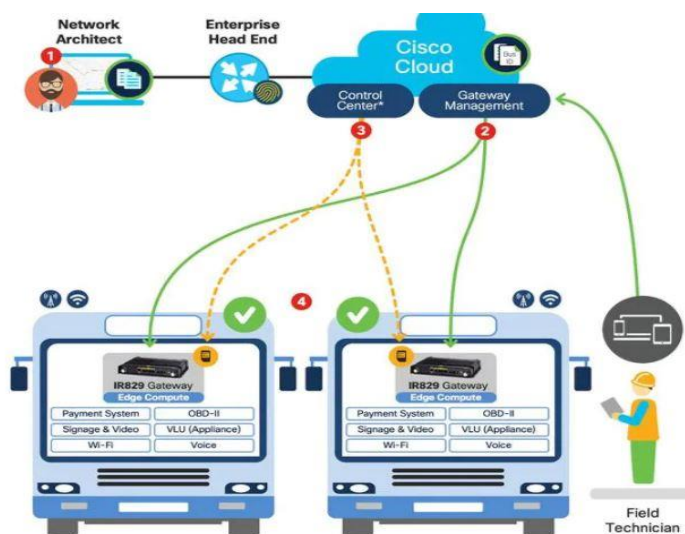


Рис. 1.3 – Приклад простого додатку від Cisco Connected Mass Transit
Основні переваги системи:

- налаштування шаблонів, використовуючи зрозумілий та доступний інтерфейс оператора. Прив'язка шлюзів до ідентифікатору транспортного засобу;
- технік розгортає шлюзи за допомогою мобільного або веб-додатку;
- єдина панель для активації/деактивації SIM-картки та керування тарифним планом за допомогою центру керування Cisco (пропонується вибраними постачальниками послуг)
- безпеку даних забезпечує сервіс Cisco Cloud;

1.3 Аналіз еталонної архітектури Internet of Things (IoT)

Архітектура будь-якої інформаційної технології чи системи (ІТС) – це комплекс взаємопов'язаних рішень на базі основних принципів вибору стандартів та технологій для створення взаємодіючих програм у ІТС, а також для формування вимог до необхідних для розробки та функціонування цих програм технологічних, технічних та телекомунікаційних засобів та інших видів забезпечення. Формування концептуального базису та визначення семантичної структури найважливіших розділів ІТС реалізується за допомогою розробки еталонних моделей, що утворюють методологічне ядро ІТС [7].

Задача побудови цілісної, несуперечливої та системно розвинутої еталонної моделі архітектури IoT зараз перебуває у стадії розвитку. Країни, зацікавлені в цьому (США, Німеччина, ЄС та ін.), а також великі міжнародні компанії (CISCO, INTEL, IBM) та організації (ITU, IEEE, ETSI, IWF, W3C) пропонують свої моделі та ведуть активну роботу в області стандартів, що покривають усі рівні архітектури IoT.

З урахуванням складності IoT, створення чотирирівневої еталонної моделі за рекомендації **ITU-T Y.2060** [8] дозволяє виділити основні компоненти системи та оцінити їх взаємозв'язок.

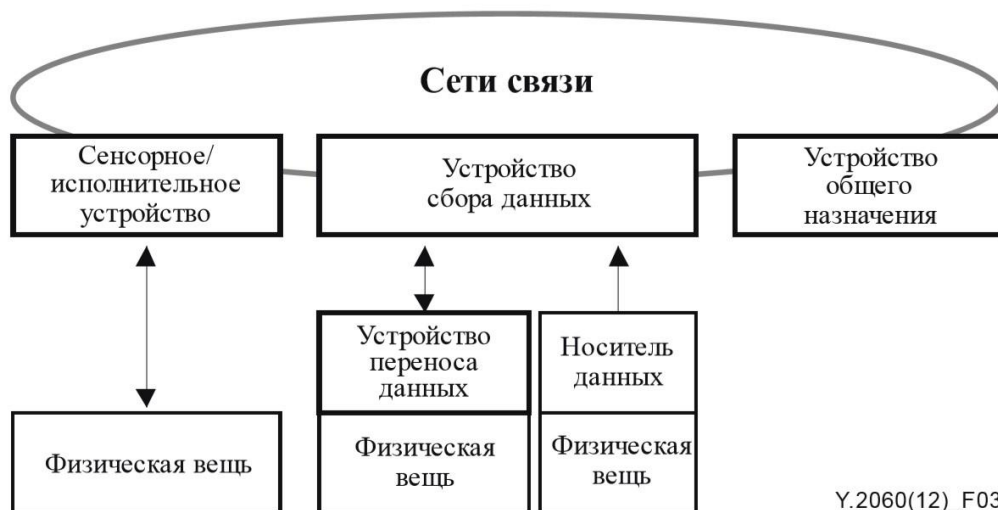


Рис. 1.4 – Типи приладів IoT та їх взаємодія

Основними рівнями при цьому є:

- рівень пристрою;
- рівень мережі;
- рівень підтримки послуг та підтримки програм;
- рівень програми;

За аналогією з традиційними мережами зв'язку, можливості управління IoT охоплюють традиційні класи:

- несправності;
- конфігурації;
- обліку;
- показників роботи та безпеки;

Відповідно до рекомендацій Сектору стандартизації електрозв'язку Міжнародного союзу електрозв'язку (ITU-T) IoT є мережею пристроїв, тісно пов'язаних з речами. Сенсорні та виконавчі пристрої взаємодіють з фізичними речами у навколишньому середовищі. Пристрої збору даних зчитують інформацію з фізичних речей або записують її на фізичні речі, взаємодіючи з пристроями передачі даних або носіями даних, підключеними або пов'язаними з фізичним об'єктом.

Тобто, IoT - це:

- фізичні/віртуальні об'єкти;
- контролери/сенсори/виконуючі механізми;
- інтернет.

Таким чином, фізичний екземпляр елемента IoT є об'єктом, який:

- інтелектуальний: має мікроконтролер та софт для управління;
- може інформувати чи діяти: містить датчик для вимірювання будь-яких фізичних параметрів або виконавчий механізм, роботою якого можна керувати;
- доступний через мережу.

Розробкою архітектури IoT також займається Всесвітній форум IoT (IoT World Forum, IWF). Це щорічна подія, в якій беруть участь представники бізнесу, держав та наукових кіл. Комітет з архітектури IWF у 2014 році опублікував свою версію еталонної моделі IoT. Вона добре доповнює варіант, запропонований ITU-T, оскільки IWF приділяє увагу не лише рівням пристроїв та шлюзу, але й верхнім рівням, важливішим для розробки додатків, проміжного софту та підтримки промислового інтернету речей [9]. Саме завдяки еталонній моделі архітектури IoT (рис. 1.5), розробники пристроїв розуміють потрібний функціонал в IoT та як вони взаємодіють.



Рис. 1.5 – Еталонна модель IoT за ITU-T Y.4000/Y2060

Всесвітній форум IoT (IoT World Forum, IWF) запропонували наступну семирівневу модель архітектури IoT (рис.1.6):

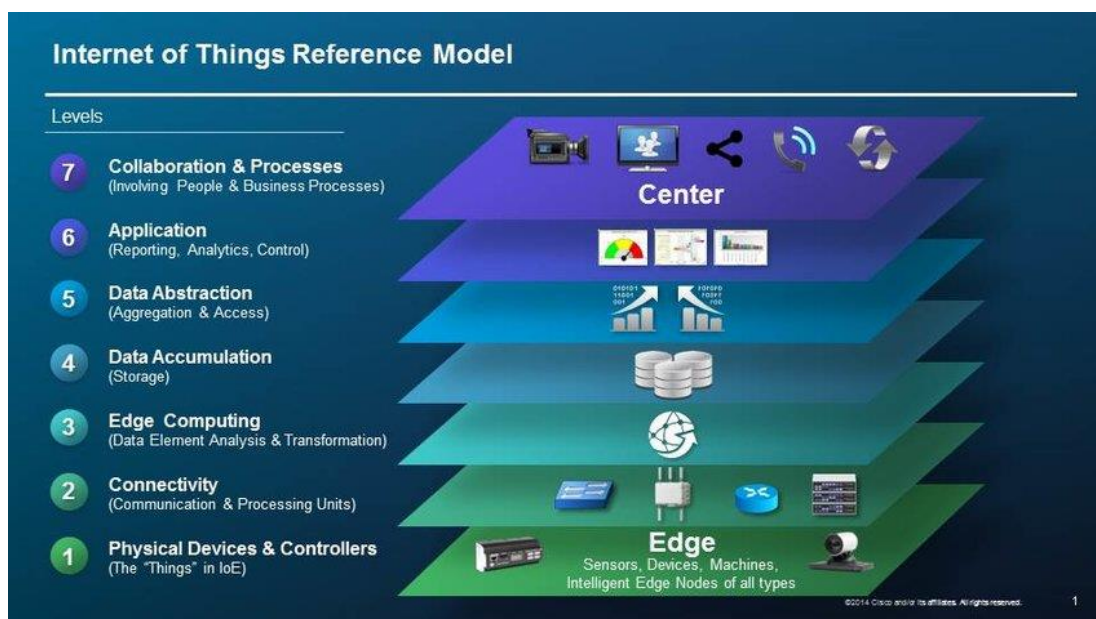


Рис. 1.6 – Еталонна модель за версією IWF [10]

- Рівень 1 утворюють фізичні пристрої та контролери (Physical Devices & Controllers). Елементи на цьому рівні – це не фізичні речі як такі, а пристрої, що взаємодіють із фізичними речами, такі як сенсорні та виконавчі пристрої;
- Рівень 2 моделі IWF відповідає рівню мережі (Connectivity), до якого відносять також мережеві пристрої – шлюзи;
- Рівень 3 елементи обробки відповідають за обробку та перетворення даних, внаслідок чого зменшується загальний об’єм інформації, який зберігається;
- Рівень 4 (Data Accumulation), дані, що надійшли з різних пристроїв, профільтовані та оброблені рівнем периферійних обчислень, розміщуються в сховище, де будуть доступні для вищих рівнів.
- Рівень 5 (Data Abstraction), може агрегувати та формувати дані способами, які роблять доступ додатків більш керованим та ефективним;

- Рівень 6, рівень додатків (Application & Analytic), містить програми будь-якого типу, які використовують дані IoT на вході або керовані IoT-пристроями. Ці додатки взаємодіють з рівнем 5 та із збереженими даними (IT Data);
- Рівень 7 взаємодії та процесу (Colaboration and Processes) з'явився в результаті визнання того, що IoT буде корисним лише тоді, коли людина вступає у взаємодію з ним. Цей рівень може включати обмін даними та/або керуючою інформацією через Інтернет.

Ключові елементи IoT:

- Протоколи – через апаратні та інші обмеження при проектування пристроїв, виявилось, що стандартні протоколи для інтернету або занадто «важкі», або не відповідають певним вимогам щодо швидкості відповіді та надійності мережі.
- 5G – зв'язок. Впровадження таких засобів допоможе зменшити затримки, та адаптовуватись під конкретні випадки, з використанням мультипідключень. З економічної точки зору зменшиться використання енергії та збільшиться швидкість передачі даних (більше 10 Гбіт/с). Що ж до затримки, у порівнянні з 4G – 10ms, в новій мережі вона становитиме до 1ms.
- Сенсори та датчики. Як і органи чуття в людини, вони допомагають пристроям тримати зв'язок із зовнішнім світом, збираючи необхідні дані та передаючи їх на сервер за допомогою протоколів: Wi-Fi, Bluetooth, NFC, RF, LoRaWAN та ін.
- IoT-платформи - забезпечують безбар'єрну інтеграцію апаратних засобів з використанням різних типів підключення, передачі даних на підключені пристрої або між ними, тобто, інтеграція обладнання в IoT буде набагато простішою та з меншими витратами.

Враховуючи вищенаведені моделі архітектур, особливості побудови кожного з рівней, великий потенціал інтеграції до існуючих систем та зростаючий попит на ринку, можна сміливо стверджувати що Інтернет речей (IoT) буде займати ще більшу роль у науковій та повсякденній сферах розвитку нашого світу.

1.4 Аналіз вимог до систем захищеного обміну даними з рухомим транспортом

На основі наведеного аналізу, та оцінки подальшого розвитку та цифровізації, навіть у сфері транспорту потрібен захист від можливого несанкціонованого проникнення в систему, викрадення персональних даних, виходу з ладу пристроїв та серверів чи навіть припинення нормального функціонування всієї системи організації.

Виділено наступні вимоги до побудови системи захищеного обміну даними з рухомим транспортом:

- Перш за все – застосування технології тунелювання трафіку (VPN), яка забезпечує високий рівень шифрування даних, що обмінюються між сервером організації та віддаленим транспортним засобом. При підключенні віддаленого користувача (або під час встановлення з'єднання з іншою захищеною мережею) сервер доступу вимагає проходження процесу ідентифікації, а потім процесу аутентифікації. Після успішного проходження обох процесів віддалений користувач (віддалена мережа) наділяється повноваженнями для роботи в мережі, тобто відбувається процес авторизації.
- Організація захищеної мережі на підприємстві, завдяки якій потенційний злоумисник буде позбавлений можливості проникнення до мережі та нанесення збитків.
- Шифрування паролів та їх ускладнення. Розмеження доступу користувачів до інформації та фізичне обмеження доступу до серверів.

1.5 Постановка завдання

У даній роботі розглядається питання розробки системи захищеного обміну даними з рухомим транспортом. Підсумовуючи, необхідно виділити такі завдання:

- Система захищеного обміну даними буде виражена як неподільна. Завдяки загальній цілі функціоналу, наявності тісного зв'язку елементів системи та ієрархічності побудови системи управління захисту передачі інформації.
- Система захищеного обміну даними з рухомим транспортом буде повинна контролювати безпеку інформації, засобів інформації, захист інтересів учасників інформаційних відносин і неможливість несанкціонованого доступу злоумисника до інформації, що захищається.
- Система захищеного обміну даними в цілому, де застосовуються методи і засоби захисту повинні бути по можливості прозорими для легітимного користувача, уникати перешкод у процесі роботи з доступом до даних.

Висновки по 1 розділу

У даному розділі проведено аналітичну працю щодо актуальності теми роботи, а саме розробки системи захищеного обміну даними з рухомим транспортом. Опрацьовано сучасні види загроз.

Проаналізовано відомі засоби захищеного обміну даними. Опрацьовано питання аналізу еталонної архітектури IoT.

Виділено вимоги до систем захисту передачі даних, зокрема такі як:

- Network Firewall.
- Програмні та апаратні засоби сканування мережі на наявність шкідливого ПЗ.
- Засоби захисту від викрадення даних, що передаються.

Виділено перелік вимог до побудови системи захищеного обміну передачі даних з транспортом.

РОЗДІЛ 2. РОЗРОБКА СИСТЕМИ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ З РУХОМИМ ТРАНСПОРТОМ

2.1 Розробка структурної схеми системи захищеного обміну даними з рухомим транспортом

При проектуванні мереж мережна інфраструктура може ґрунтуватися на низці архітектурних шаблонів [11]. Від вибору шаблону залежить об'єм впливу на безпеку мережі та визначається різниця між легко вразливою та безпечною мережею. Враховуючи, що архітектура та топологія є основними принципами безпечної мережі, стандарти промислової безпеки, такі як сімейство стандартів ISO/IEC 62443, були закладені для проектування мережі, щоб задати операторам обладнання та системним інтеграторам напрямок, за яким можливо розробляти великі ефективні мережеві структури. Одним із найважливіших принципів проектування мереж є принцип «зон і каналів». Відповідно до цього принципу промислова мережа сегментується на різні функціональні зони і з'єднання між цими зонами (каналами) передають лише дозволений трафік даних з однієї зони до іншої. Для прикладу, зона може представляти собою машину, або окрему її частину, де інші пристрої постійно обмінюються даними один з одним, не маючи ніяких перешкод.

Необхідно прийняти до уваги кілька речей при реалізації зон та каналів. Треба вжити технічні заходи щодо налаштування контролю переходу зони. Зазвичай, найбільш зручними методами сьогодення залишаються фаєрволи та списки контролю доступу (ACL).

Рисунок 2.1 демонструє як фаєрволи з обмеженим набором правил скорочують трафік між зонами. Всередині зон також встановлене обмеження трафіку від пристроїв завдяки Ethernet-комутаторам з ACL-списками. На додачу до поділу мереж на зони, бажано також захистити доступ до окремих зон. Найліпшим варіантом для цього, буде використання технології, на кшталт IEEE 802.1X, об'єднаний з протоколом автентифікації RADIUS.

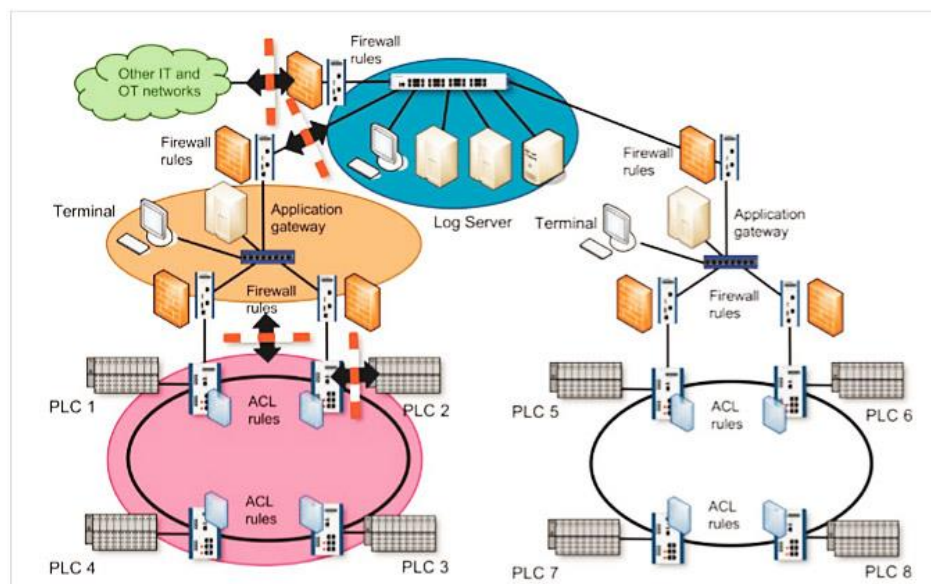


Рис. 2.1 – Простий промисловий додаток, розділений на окремі функціональні зони

Сегментування мережі на окремі зони виконується завдяки фаєрволам або шлюзам прикладного рівня (ALG), після створення правил фільтрації пакетів.

Заборонений трафік буде блокуваний фаєрволом та ACL, проходячи через фільтрацію трафіку, після аналізу метаданих підключення (IP, MAC-адреси, port number, protocol flags).

“White list” або ж “білий список” дозволяє проходження лише авторизованного трафіку, а увесь інший трафік буде блокуваний. За цим принципом працює фаєрвол з набором властивостей відповідно до бажаного та відомого трафіку. Зображений приклад демонструє, що трафік, який виходить за межі зони і не є направленим до серверу журналів, буде заблокований.

Через що, обмін інформацією через периметр зони з іншими пристроями неможливий, потенційні зловмисники будуть обмежені колом впливу ззовні периметру зони, оскільки їх зв’язок з об’єктом впливу через канали буде значно обмежений.

Розглянемо шаблони та анти-шаблони проектування розподілу мереж. У мережі, міжмережеві екрани можливо налаштовувати у різних точках. Завдяки розташуванню, визначається здатність системи, що захищена фаєрвол, чинити

опір загрозам у цій точці. За принципом білого списку, витікає непоганий шаблон за яким можна створити правила фаєрвола.

Чорний список або **black list** – це анти-модель до вищенаведеного білого списку. Його принцип заснований на пропусканні будь-якого невідомого трафіку. А процес блокування відбувається лише за умови, що проаналізований трафік відповідає певним критеріям. Окрім вищенаведених моделей встановлення правил фаєрволу, розглянемо відповідні моделі, що використовуються для зображення структури та топології мереж.

Таблиця 2.1

Анти-шаблони проектування мереж

Назва шаблону	Відомі властивості
Плоска мережа	Не має розподілу на зони, усі пристрої знаходяться в межах однієї великої зони. Зручна для будь-яких мереж через відсутність обмежень з'єднань між пристроями. Як результат – можлива повна втрата контролю над мережею під час хакерської атаки, та неможливість надати додатковий захист вразливим цілям. Такий шаблон не може об'єктивно захистити мережу організації.
Екранований хост	Використовується фаєрвол для розділення мережі на зони, але існує вразливість проходження міжзонального з'єднання крізь такий фаєрвол. Найчастіше трапляється через надання послуг від хостів однієї зони, хостам, які знаходяться в іншій.

Наведемо приклад щодо другого анти-шаблону. Ми вже згадували за сервер журналів, тепер розглянемо ситуацію, коли наш сервер об'єднує дані проколу з усіх пристроїв організації.

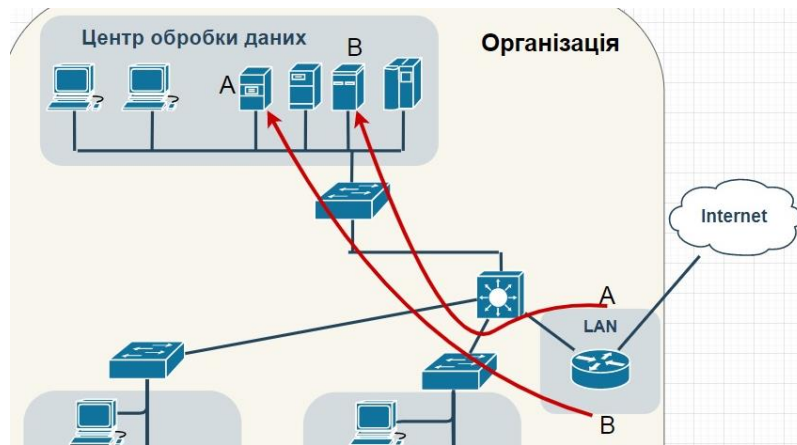


Рис. 2.2 – Анти-шаблон «Екранований хост»

Для щоб пристрої поза зони організації мали змогу підключитись до нашого серверу (хост А), системний адміністратор додає дозволяюче правило до фаєрволу, тим самим роблячи мережу більш уразливою до атак. За таким самим принципом буде відкритий доступ ззовні до хосту В. На жаль, практичний досвід демонструє, що потенційні зловмисники використовують вразливості ПЗ служб А або В, в подальшому захоплюючи сервер протоколу або хост В. Це дає їм змогу отримати подальший доступ до терміналу або контролера, завдаючи збитки організації.

Вирішення даної проблеми сховано в розподілі сервісів А та В від інших пристроїв. І тут доречно використати модель архітектури «Екранованої підмережі». Зазвичай, найбільш вразливі служби та пристрої мережі, прийнято відокремлювати до спеціальних «демілітаризованих зон» (DMZ). Їх створюють для обслуговування веб, DNS та поштових серверів. Розміщують такі зони на периметрі мережі організації, біля виходу до мережі Інтернет.

Структурно, організація розділена на кілька будівель, зокрема будівлю центру обробки даних та трьох офісних споруд. Крім цього є майданчик відпочинку рухомого транспорту, саме там встановлене додаткове обладнання для зв'язку з даним транспортом та вивантаженням інформації до серверів обробки, тоді як структурні підрозділи організації керують процесами обробки та оновлення необхідної інформації на рухомому складі.

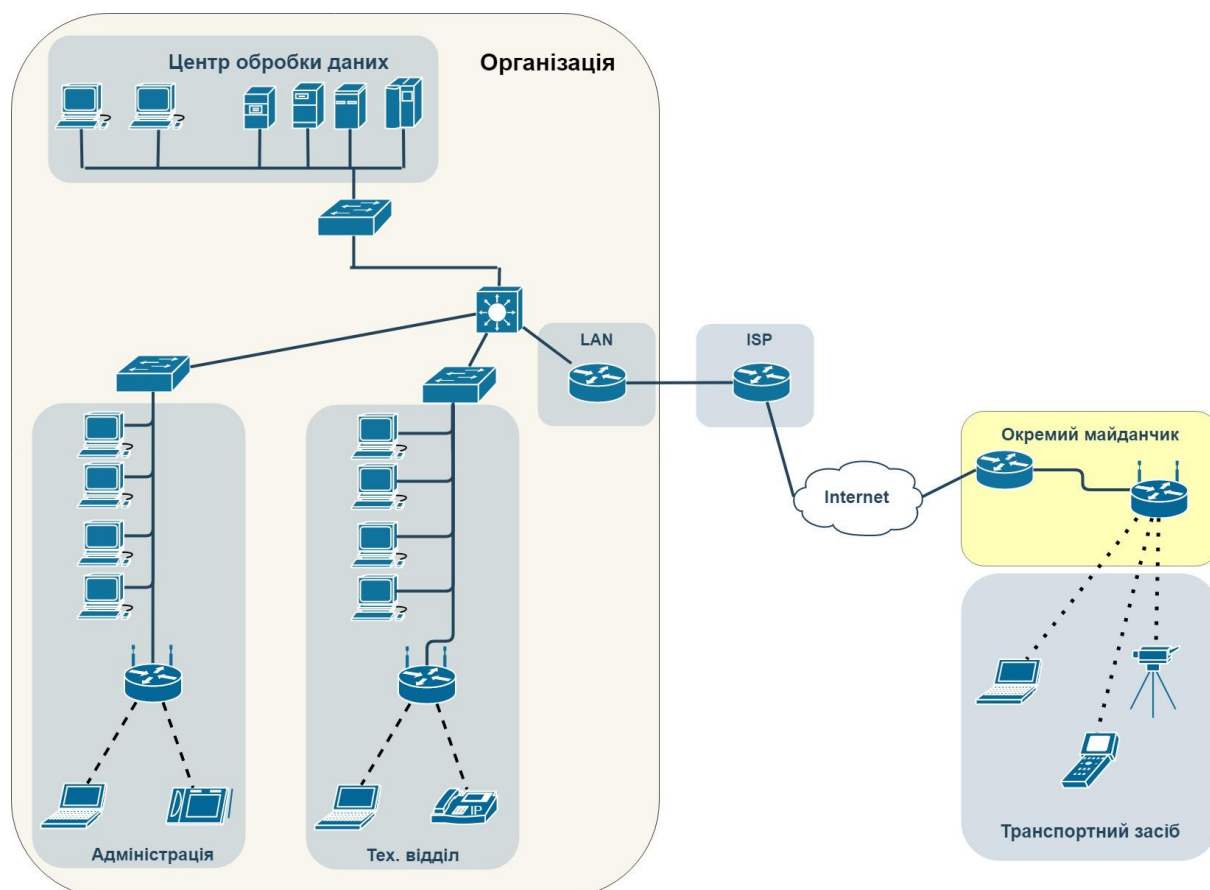


Рис. 2.3 – Структурна схема проекту системи захищеного обміну даними

Варто зазначити, що кількість підключених транспортних засобів одночасно може бути досить великою, при тому що організації не потрібно забезпечувати кожний транспортний засіб своїм власним маршрутизатором, що забезпечує заощадження витрат на встановлення даної системи.

З огляду на місця встановлення обладнання не варто забувати й про фізичний захист пристроїв мережі. Це забезпечує базовий, але тим не менш, важливий ступінь захисту мережових комунікацій в цілому. Будь-який метод захисту мережі буде марним, якщо потенційний зловмисник має безпосередній доступ до мережевого обладнання. Перш за все мережеві пристрої необхідно встановити у захищених шафах, окремих приміщеннях та обмежити коло співробітників які мають доступ до них. Таким чином, зловмисник не зможе порушити роботу обладнання або встановити несанкціоноване підключення до нього та змінити конфігурацію. Тим не менш, є випадки, коли деяке обладнання не може бути схованим, зокрема брак таких надійних місць а також наявність

WLAN систем, мікрохвилі яких можуть виходити за межі будівлі. Тому важливим пунктом є запровадження протоколів доступу до мережі, за якими пристрої та користувачі будуть ідентифіковуватись та автентифіковуватись, щоб у подальшому адміністратор мав можливість контролю входу до мережі.

Класичні методи обмеження доступу до мережі за ідентифікаторами такими як MAC та IP-адреса дуже швидко обходяться зловмисниками, через що необхідно використовувати складні паролі та/або служби автентифікації з відкритим ключом. Для прикладу, WiFi-маршрутизатор, який встановлено на майданчику відстою транспортних засобів, має увімкнений парольний доступ до мережі, а усі пристрої IoT на транспорті зконфігуровані під необхідні параметри.



Рис. 2.4 – Автентифікація нового пристрою з використанням функції доступу за паролем

Існують також інші способи захисту мережі за автентифікації користувачів, зокрема використання спеціального серверу автентифікації за допомоги стандартів IEEE 802.1X та протолу RADIUS.

IEEE 802.1X — стандарт Інституту інженерів електротехніки та електроніки, що описує процес інкапсуляції даних EAP, що передаються між запитуючими пристроями (клієнтами), системами, що перевіряють справжність (комутаторами, точками бездротового доступу), та серверами автентифікації (RADIUS) [12]. Включає в себе стандарти бездротових (**IEEE 802.11 WLAN**) та (**IEEE 802.3 Ethernet**) дротових з'єднань.

RADIUS (Remote Authentication in Dial-In User Service) - протокол для реалізації аутентифікації, авторизації та збору відомостей про використані ресурси, розроблений для передачі відомостей між центральною платформою та обладнанням [13].

Згідно стандарту, кожний клієнт мережі має свої унікальні дані входу, як логін, пароль або цифровий підпис. Ці дані в подальшому використовуються для ідентифікації на комутаторі або точці доступу бездротової мережі. Під час процесу автентифікації, дані пристрою клієнта надсилаються комутатором або роутером WLAN до серверу автентифікації. Після чого сервер проводить звірку даних доступу з власною базою даних та дає відповідну команду комутатору або роутеру дозволити або заблокувати з'єднання з клієнтом.

Переваги IEEE 802.1X в парі з RADIUS:

- Кожен пристрій має свої унікальні ідентифікаційні дані доступу до мережі. Це дає змогу розмежування рівня доступу для клієнтів, гнучке керування доступом до мережі (наприклад, у випадку демонтажу або викрадення обладнання клієнта, можливо викреслити його дані доступу з БД сервера).
- Створення окремих зон **VLAN** (від англ. Virtual Local Area Network) - віртуальна локальна комп'ютерна мережа. Являє собою групу хостів із загальним набором вимог, які взаємодіють так, ніби вони були підключені до широкомовного домену незалежно від їх фізичного місцезнаходження [14]. Пристрої з однієї VLAN мають з'єднання тільки між собою. Для підключення до інших VLAN необхідно скористатись фаєрволом.

Таким чином, ми маємо надійно захищену мережу, з централізованим керуванням доступу клієнтів, розмежуванням рівнів доступу між ними та гнучким налаштуванням підключення локальних мережевих зон. Стандарт IEEE 802.1X є універсальним методом з організації захисту мережі організації, а архітектура «екранована підмережа» ідеально підходить для даної роботи, так як віддалена локальна мережа транспортного засобу буде підключатись до локальної мережі

організації шляхом VPN технології. Але про це більш детально у наступних розділах.

2.2 Вибір технічних засобів для реалізації системи

Розмір та потужність розгортання мережі кампусу підприємств широко відрізняються. Cisco пропонує широкий, багатий портфель різноманітного обладнання для реалізації кожного з рівнів ієрархічної структури кампусної мережі.

Так для рівня ядра, звісно, слід обирати маршрутизуюче обладнання. Корпорація Cisco пропонує широкий вибір пристроїв. Вибір залежить від потреб та можливостей організації. Керуючись цим, слід обирати більш просте, чи навпаки – маршрутизуюче обладнання яке має розширені можливості.

Так для кампусу оператора транспорту та зв'язку варто розглянути побудову рівня ядра на маршрутизаторах серії Cisco ASR 9000 (рис. 2.5).



Рис. 2.5 – Серія маршрутизаторів Cisco ASR9000

Основним завданням маршрутизаторів Cisco ASR 9000 є створення мереж Carrier Networks [15]. Також пристрої працюють з технологією Network Virtualization. Формат маршрутизаторів – модульний, операційна система – віртуальна. Гнучкий розподіл ресурсів з мінімальними шансами збою та відмови в роботі. Подібні аналоги мають значно нижчі мережеві параметри.

Дана серія маршрутизаторів відрізняється підвищеною щільністю портів і високою продуктивністю. З їх допомогою провайдери можуть надавати послуги кінцевим клієнтам і забезпечувати швидку передачу хмарних, мобільних і відео сервісів. Характерною особливістю платформи виступає висока ємність на мережевому кордоні. Маршрутизатор здатний до завантаження декількох мільйонів з'єднань, тому його можна використовувати як виділений пристрій.

Розглядаючи бюджетні рішення, то тут можна зупинитись навіть на серії багатофункціональних маршрутизаторів Cisco ISR 800 (рис. 2.6).



Рис. 2.6 – Маршрутизатор серії Cisco ISR800

Маршрутизатори серії Cisco ISR 800 розроблені для невеликих комерційних компаній. Оснащені багатим функціоналом, сучасними методами керування та безпеки. За допомогою пристроїв, власник зможе підключатися до WAN і створювати бездротові мережі [16]. Більшість завдань тут автоматизовані, для запровадження обладнання в експлуатацію, як правило, вистачає 24 годин. Аналоги не мають такого ж набору властивостей. Cisco вдалось зібрати самі останні технологічні рішення, тим самим займаючи передове місце у цьому сегменті серед інших виробників.

Далі розглянемо комутаційне обладнання Cisco Catalyst. Такі пристрої підходять до більш точних бізнес-технічних та індивідуальних потреб клієнтів. Завдяки різноманітним системам, що пропонують змінну щільність портів, продуктивність комутації, масштабованість та стійкість, користувачам надається змога проектувати та конструювати високоефективну багатоядерну мережеву інфраструктуру.

Обговорюючи про рівень розподіли Cisco пропонує серію комутаторів Cisco Catalyst 6800 (рис. 2.7).



Рис. 2.7 – Серія комутаторів Cisco Catalyst 6800

Cisco Catalyst 6800 відносяться до опорних комутаторів останнього покоління і призначені для кампусних мереж, що підтримують безпечні сервіси 10, 40 і 100G, маючи легку масштабованість та передові інтелектуальні розробки [17]. Технологія миттєвого доступу, висока пропускна здатність слотів і системи робить комутатори лінійки високо захищеними при роботі в бездротових і віртуальних приватних мережах.

Рішення Catalyst 6800 дає можливість адміністраторам мережі контролювати роботу комутаторів в кампусі, в рамках єдиної керуючої системи. Всі моделі лінійки комутаторів Catalyst 6800 управляються через єдиний (батьківський) комутатор Cisco Catalyst 6500/6800 і забезпечують узгодження функцій на будь-якому рівні доступу і розподілу. Пристрої стійкі до навантажень і підтримують технологію агрегації каналів EtherChannel на декількох шасі, що мають функцію стекування і не використовують протокол для сполучного дерева при зв'язку Catalyst 6800 з батьківським комутатором. Весь обсяг трафіку від порту хоста, по низхідній лінії, відправляється батьківському модулю Instant Access, що виконує всі перемикання і приймає рішення про передачу трафіку, який перенаправляється за призначенням.

Комутатори лінійки успадковують всі функції Supervisor Engine 2T і працюють з груповими тегамі SGT, згідно зі списком контролю доступу SGACL. Моделі мають широкий протокол внутрішнього шлюзу для маршрутизації EIGRP, IPv6 і mediatrace з багатопроTOCOLЬною комутацією по мітках.

Ще одною з серій кампусних комутаторів Cisco є серія Cisco Catalyst 4500E (рис. 2.8).



Рис. 2.8 – Серія комутаторів Cisco Catalyst 4500E

Catalyst 4500E – сімейство модульних корпоративних комутаторів 3-го рівня з великою різноманітністю моделей і високою гнучкістю конфігурації [18].

Серія Cisco Catalyst 4500E є розвитком перевіреної серії 4500 з розширеним функціоналом і підвищеною пропускнуою здатністю. Комутатори 4500E підтримують як старі, так і нові (з індексом E) Line Cards сімейства 4500, а також супервізори і блоки живлення від серії 4500.

Загальні характеристики сімейства Cisco Catalyst 4500E:

- шасі на 3, 6, 7 і 10 слотів під супервізори і Line Cards;
- до 384-ох 10/100/1000 PoE портів або до 34-ох 10 GE портів;
- загальна пропускна здатність 320 Gbps або 250 mpps, до 24 Gbps на слот;
- одночасна підтримка протоколів IPv4 та IPv6;
- моделі на 7 і 10 слотів підтримують надмірність супервізорів.

Крім цього до кампусних комутаторів належить серія Cisco Catalyst 3850. Вони спираються на базу нової спеціалізованої інтегральної схеми для роботи з додатками та інтегрованими функціями контролера для роботи в мережі, високою швидкодією, множинною підтримкою точок доступу, гнучким масштабуванням та відмовостійкістю.



Рис. 2.9 – Серія комутаторів Cisco Catalyst 3850

Серія Cisco Catalyst 3850 (див. рис. 2.9) використовує в якості бази нову інтегральну схему UADP ASIC, створену для роботи з додатками, що функціонує з дотриманням уніфікованих політик для бездротової та дротової мережі, яка здійснює безперервний моніторинг системи і може забезпечувати гнучкість та оптимальну роботу додатків [19].

Всі моделі лінійки Catalyst 3850 повністю підтримують технологію електроживлення PoE+ і використовують модульні, замінні резервні вентилятори і джерела живлення.

Спорідненою є серія Cisco Catalyst 3650 (рис. 2.10).



Рис. 2.10 – Серія комутаторів Cisco Catalyst 3650

Це комутатори на основі розроблених компанією Cisco електронних компонентів – чіпів UADP, завдяки яким здійснюється кодування і декодування сигналу на швидкості носія, без затримок і зниження продуктивності. Наявність технології Power over Ethernet (PoE) окрім підключення, надає також електричне живлення пристроям мережі.

Це серія стекованих комутаторів, з технологією StackWise-160. Застосування електронних схем UADP дозволяє налаштовувати роботу бездротових мереж в поєднанні з провідними за допомогою одних і тих самих інструментів, забезпечуючи однорідне управління всіма елементами. Розроблені Cisco чіпи UADP працюють на швидкості потоку і обробляють дані без затримок, використовуючи протокол DTLS для кодування і декодування [20].

Найпростішим та найбільш дешевим рішенням для рівня доступу кампусної мережі буде серія комутаторів Cisco Catalyst 2960-X (рис. 2.11).



Рис. 2.11 – Серія комутаторів Cisco Catalyst 2960-X

Комутатори Cisco Catalyst 2960-X series є стекові комутатори Gigabit Ethernet з фіксованою конфігурацією, які забезпечують доступ корпоративного класу для додатків в кампусах і філіях. Комутатори функціонують на базі програмного забезпечення Cisco IOS і підтримують просте управління пристроями, а також керування мережею, забезпечуючи просте і оперативне конфігурування пристрою, налаштування з'єднань, моніторинг і усунення помилок [21].

Для забезпечення функціонування даної мережі організації було обрано оптимальні маршрутизатори і комутатори корпорації Cisco, котрі мають можливість модульної модернізації.

Нижче описані та охарактеризовані пристрої, які були використані для побудови мережі.

В якості основних маршрутизаторів мережі були обрані маршрутизатори Cisco 2911 (рис. 2.12).



Рис. 2.12 – Маршрутизатор Cisco 2911

Модульний маршрутизатор Cisco 2911 – це пристрій нового покоління, який має інтеграцію з сервісами другого покоління сімейства ISR G2 (Integrated Services Router Generation 2). Модель дозволяє створювати безпечне широкосмугове підключення до мережі, проводити передачу мультимедійних даних, відео, здійснювати бездротовий зв'язок, а також застосовувати безліч додаткових функцій при мінімальному рівні витрат на придбання та утримання [22].

Серія маршрутизаторів Cisco 2900 представлена 4-ма фіксованими та безліччю розширених за допомогою ліцензій і модулів моделями. Маршрутизатор Cisco ISR серії 2900 розроблено для малих і середніх підприємств, яким потрібні сучасні технологічні рішення, що забезпечують надійне високопродуктивне підключення до мережі Інтернет зі швидкістю маршрутизації до 75 мегабіт за секунду.

До особливостей маршрутизаторів Cisco 2900 серії можна віднести гігабітні Ethernet порти з можливістю переходу в оптику (SFP-роз'єми), слоти розширення EHWIC, сумісні з модулями попереднього покоління WIC / VWIC / HWIC і слоти розширення під модулі SM (Service Modules), сумісні з модулями попереднього покоління NM / NME / EVM. Також, є внутрішні роз'єми під модулі ISM (Internal Service Modules), які заміняють AIM модулі попереднього покоління (сумісність з AIM немає) і внутрішні роз'єми під модулі цифрової обробки сигналів (DSP) – PVDM3 для підтримки голосових і відео функцій (сумісні з PVDM2). Новітня технологія Services Ready Engine (SRE) забезпечує окреме, при наявності запиту, розгортання апаратних і програмних сервісів, а

підтримка VPN-мереж із застосуванням технологій GETVPN, DMVPN і Enhanced Easy VPN з вбудованими апаратними функціями шифрування IPsec / SSL гарантує високу можливість до масштабування, високу продуктивність всіх сервісів захисту, розгортання мереж VPN, і забезпечує віддаленим мережам, таким як локальна мережа транспортного засобу, захищений доступ до ресурсів компанії з боку безпечного з'єднання.

Cisco 2911 з вбудованими мережевими сервісами на 3 порта ідеально підходить для створення мереж малих і середніх організацій і підприємств. Модель має 512 МБ вбудованої і 526 МБ флеш-пам'яті, можливість підтримки PoE на портах 10/100/1000 Ethernet, а також підтримку протоколу VPN і тунелювання для здійснення надійної і безпечної передачі при побудові віддалених VPN мереж транспортних організацій.

Крім цього, на рівні розподілу, маршрутизацією займаються багаторівневі комутатори Cisco Catalyst 3650 (рис. 2.13).



Рис. 2.13 – Багаторівневий комутатор Cisco Catalyst 3650

Комутатори Cisco Catalyst 3650 – це стекові пристрої для конвергованого доступу з фіксованою конфігурацією і інтегрованим бездротовим контролером ASIC, що працюють на базі модульної операційної системи IOS XE [23]. Аналогічні ASIC використовуються в платформах Catalyst 3850 і Supervisor 8-E для Catalyst 4500-E. Комутатори Cisco Catalyst 3650 забезпечують політику безпеки і якості обслуговування QoS для трафіку дротових і бездротових клієнтів, а також моніторинг та оптимізацію цього трафіку корпоративної мережі. До особливостей моделей Catalyst 3650 можна віднести фіксовану конфігурацію з 24 або 48 портів 10/100/1000 з можливістю підтримки PoE + (до 30 Вт на порт), інтегровані uplink 4 x Gigabit Ethernet, 2 x 10 Gigabit Ethernet або 4 x 10 Gigabit Ethernet з підтримкою трансиверів SFP і SFP+, можливість

встановлення до 2 відмовостійких джерел живлення змінного струму різних потужностей і 3 кулерів охолодження. Також, в Catalyst 3650 є підтримка стека StackWise (до 9 пристроїв в стеку) при використанні опціональних модулів для стекування з пропускною спроможністю 160Гб / с і технологією SSO (Stateful Switch Over), пропускна здатність Wireless 40 Гб / с на базі ASIC UADP (Unified Access Data Plane) і операційної системи IOS XE та підтримка до 25 точок доступу і 1000 бездротових клієнтів на один комутатор 3650 або один стек StackWise з комутаторів 3650.

Розглядаючи розробку віддаленої мережі транспортного засобу та застосування водночас універсального пристрою, вибір був зупинений на маршрутизаторі Cisco-Linksys WRT300N (рис. 2.14).



Рис. 2.14 – Маршрутизатор Cisco-Linksys WRT300N

Даний бездротовий маршрутизатор виконує функціонал трьох пристроїв одночасно. **Wireless Access** - дозволяє підключатися до мережі бездротово. Є також вбудований 4-портовий модуль комутації із пропускною здатністю в 10/100 Мбіт/с. Нарешті, маршрутизатор пов'язує все це разом і дозволяє всій мережі обмінюватися високошвидкісним кабелем або DSL-з'єднанням з Інтернетом [24].

Цей маршрутизатор чудово працює з бездротовим обладнанням стандартів 802.11b/g, але коли обидва кінці бездротового зв'язку є стандарту 802.11n, то маршрутизатор може збільшити пропускну здатність ще більше, використовуючи вдвічі більше радіодіапазону, що забезпечує швидкість до 12 разів швидше, ніж попередній стандарт 802.11g.

Крім цього в даному маршрутизаторі є підтримка технології "**Multiple In, Multiple Out**" (MIMO), що примножує ефективність передачі даних [25]. На відміну від звичайних технологій бездротових мереж, які плутають відображення сигналу, MIMO фактично використовує ці відбиття для збільшення дальності та зменшення "мертвих точок" у зоні бездротового покриття. Потужний сигнал, поширюючись, підтримує бездротові з'єднання в 4 рази далі, ніж стандартний 802.11g.

У перевантажених районах режим "доброго сусіда" забезпечує те, щоб маршрутизатор перевіряв інші бездротові пристрої в цьому діапазоні, перш ніж використовувати радіополосу.

Щоб захистити ваші дані та конфіденційність, маршрутизатор може кодувати всі бездротові передачі з 256-бітовим шифруванням промислового стандарту. Він може служити DHCP-сервером мережі, має потужний брандмауер SPI для захисту пристроїв від зловмисників та найвідоміших інтернет-атак та підтримує VPN-пропуск. Конфігурація оснащена утилітою налаштування веб-браузера.

Неймовірна швидкість бездротової передачі робить його ідеальним для потреб, що орієнтовані на засоби масової інформації, таких як потокове відео, ігри та голосовий зв'язок через IP-телефонію, і надає простір для одночасного запуску декількох «важких» потоків даних через мережу.

Рівень доступу буде реалізований за допомогою комутаторів Cisco Catalyst 2960 (рис. 2.15).



Рис. 2.15 – Комутатор Cisco Catalyst 2960

Компанія Cisco розробила мережеве обладнання, що підтримує передачу найпопулярніших типів інформації, в тому числі відео та голос. Її продукти серії Catalyst 2960 Switch відповідають сучасним нормам і використовуються багатьма компаніями, як засіб для передачі всіх типів інформації. Дане обладнання підтримує масштабування своїх функцій під безперервно зростаюче підприємство [26].

Комутатори Cisco Catalyst серії 2960 мають інтерфейс, простий для користувача. Для першого налаштування використовується пакет утиліт під назвою Cisco Network Assistant, воно допоможе налаштувати робоче середовище, зробить його більш продуктивним та швидкодіючим.

Cisco Catalyst 2960 можуть використовуватись в різних типах зв'язку, наприклад, як провідна мережа, так і бездротова, саме тому ці продукти отримали таке широке поширення.

Комутаторам серії Cisco 2960 надані свої обчислювальні можливості. Користувачеві в першу чергу необхідно вказати темпи, а також важливі пріоритети, тип передачі інформації і швидкість виконання всіх операцій. Звичайно, при виконанні складних завдань продуктивність даних комутаторів може скорочуватися, але за рахунок впроваджених технологій система швидко справляється з великим навантаженням.

Комутатори Cisco Catalyst серії 2960 легко і надійно захищають робоче середовище. Користувачеві необхідно використовувати функцію доступу по пароллю, після чого проникнення з боку незареєстрованих користувачів буде виключено. Окрім цього, є функція відновлення (backup) інформації після позаштатних випадків.

Серед можливостей комутаторів даної лінійки виділяють можливість регулювати швидкість передачі на кожному порту з кроком в 64 Кбіт/с,

підтримку об'єднання портів (Link Aggregation) для організації більш швидкісних з'єднань між комутаторами і серверами та можливість організації транкових з'єднань на кожному порту за допомогою тегів 802.1q.

Майже всі серії Cisco Catalyst 2960 не підтримують маршрутизацію, але вміють фільтрувати трафік, ґрунтуючись на інформації 3-го рівня – IP.

2.3 Вибір протоколів захищеного обміну даними в системі

Для реалізації проекту системи захищеного обміну даними організації з її віддаленою мережею, розташованою на транспортному засобі, яка в свою чергу з'єднується з локальною мережею організації, було вирішено використовувати технологію VPN.

Більшість технологій VPN-шифрування розроблені Національним Інститутом Стандартів та Технологій (NIST). Розглянемо, наскільки безпечні всі ці засоби захисту, розберемо основні відмінності між протоколами VPN і тим, як вони впливають на користувачів та питання шифрування.

PPTP - (англ. Point-to-Point Tunneling Protocol) — тунельний протокол типу точка-точка, що дозволяє комп'ютеру встановлювати захищене з'єднання з сервером за рахунок створення спеціального тунелю в стандартній, незахищеній мережі [27]. Це перший VPN-протокол, який підтримується Windows, безпека забезпечується різними методами автентифікації, наприклад, найпоширеніший з них MS_CHAP v2.

Кожен пристрій, що працює з VPN, підтримує PPTP за замовчуванням, і оскільки його дуже просто налаштувати, цей протокол продовжує залишатися найпопулярнішим серед власників компаній та VPN-провайдерів. Це також найшвидший протокол, тому що для його реалізації потрібно найменше обчислень.

Хоча й за замовчуванням використовується 128-бітове шифрування, є певні вразливості безпеки, одна з найсерйозніших - неінкапсульована автентифікація MS-CHAP v2. Через це PPTP можна зламати протягом двох днів.

І хоча ця проблема була виправлена Microsoft, все ж таки рекомендується використовувати протоколи SSTP або L2TP для підвищеної безпеки.

І, звичайно, такий низький захист PPTP обумовлює те, що розшифровка цього протоколу - стандартна процедура на сьогодні. Відомий факт, що Агентство національної безпеки США розшифровує не лише справжній трафік, а й дані, які були зашифровані ще в той час, коли PPTP вважався безпечним.

L2TP и **L2TP/IPsec** - (англ. Layer 2 Tunneling Protocol – протокол тунелювання другого рівня) – у комп'ютерних мережах тунельний протокол, що використовується для підтримки віртуальних приватних мереж. Головна перевага L2TP у тому, що цей протокол дозволяє створювати тунель не тільки в мережах IP, а й у таких, як ATM, X.25 і Frame Relay [28].

Протокол тунелювання рівня 2, на відміну інших протоколів VPN, не шифрує і не захищає дані. Тому часто використовуються додаткові протоколи, зокрема IPSec, за допомогою якого дані шифруються ще до передачі. Усі сучасні пристрої та системи, сумісні з VPN, мають вбудований протокол L2TP/IPSec. Встановлення та налаштування здійснюється легко і не займає багато часу, однак може виникнути проблема з використанням порту UDP 500, який блокується фаєрволами NAT. Отже, якщо протокол використовується з брандмауером, може знадобитися переадресація портів.

Невідомо про будь-які критичні вразливості IPSec, і при правильному застосуванні, цей протокол забезпечує повний захист конфіденційних даних. Хоча дворазове капсулювання даних робить протокол не таким ефективним, як, наприклад, рішення на основі SSL, але при цьому він працює повільніше за інші протоколи.

OpenVPN — вільна реалізація технології віртуальної приватної мережі (VPN) з відкритим початковим кодом для створення шифрованих з'єднань між двома клієнтськими машинами або забезпечення роботи централізованого VPN-сервера для одночасної роботи декількох клієнтів [29]. OpenVPN використовує протоколи SSLv3/TLSv1 та бібліотеку OpenSSL, а також деякі

інші технології, що в цілому забезпечує надійне та потужне VPN-рішення для користувачів. Протокол є гнучким у налаштуванні та найкраще працює через UDP-порт, однак його можна налаштувати для роботи з будь-яким іншим портом, наприклад, сервісам типу Google буде важко їх заблокувати.

Інша важлива перевага полягає в тому, що бібліотека OpenSSL підтримує різні алгоритми шифрування, у тому числі 3DES, AES, Camellia, Blowfish, CAST-128, хоча провайдери VPN використовують практично виключно лише Blowfish або AES/, за замовчуванням надається 128-бітове шифрування Blowfish. Зазвичай воно вважається безпечним, однак було відзначено деякі вразливості.

Насамперед, швидкість OpenVPN залежить від рівня шифрування, хоча зазвичай вона вища, ніж у IPSec. І хоча OpenVPN – це підключення, яке використовується за замовчуванням більшістю VPN-провайдерів, воно не підтримується на будь-яких платформах. Проте активно розробляються програми від сторонніх виробників, зокрема Android та iOS.

Установка трохи складніша, ніж для L2TP/IPSec та PPTP, зокрема коли використовується спільний додаток для OpenVPN. Вам потрібно не просто завантажити та встановити клієнт, але ще й витратити час на зміну файлів налаштування. Деякі VPN-провайдери пропонують попередньо налаштовані клієнти.

SSTP - Secure Socket Tunneling Protocol (протокол безпечного тунелювання сокетів) — протокол прикладного рівня (application-layer protocol). Він спроектований для створення синхронного взаємозв'язку при спільному обміні інформацією двох програм. Завдяки йому можливо утворити декілька підключень програми по одному з'єднанню між вузлами, в результаті чого досягається ефективне використання мережевих ресурсів [30]. Вперше цей протокол був представлений компанією Microsoft у SP1 для Windows Vista, на сьогодні цей протокол є доступним для SEIL, Linux, RouterOS, але переважно він розрахований для роботи в Windows. У ньому використовується SSL v3, що еквівалентно OpenVPN, зокрема, можливість обходити фаєрволи NAT. SSTP – це стабільний та простий у використанні протокол, інтегрований у Windows.

IKEv2 - протокол тунелювання (протокол обміну ключами, версія 2), розроблений Cisco та Microsoft, вбудований у Windows 7 та наступні версії [31]. Протокол дозволяє модифікації з відкритим вихідним кодом, зокрема для Linux та інших платформ, а також підтримуються пристрої Blackberry.

Він добре підходить для встановлення автоматичного підключення, якщо інтернет-з'єднання періодично розривається. Користувачі мобільних пристроїв можуть скористатися ним як протоколом для бездротових мереж за замовчуванням - він дуже гнучкий і дозволяє легко перемикає мережі. Крім того, він чудово підійде для користувачів Blackberry – це один із небагатьох протоколів, з підтримкою подібних пристроїв. Хоча IKEv2 доступний на меншій кількості платформ порівняно з, наприклад, IPSec, він вважається досить хорошим протоколом з точки зору стабільності, безпеки та швидкості роботи.

Шифри - це математичні алгоритми, які у процесі шифрування, найпростіші з них більш вразливі для хакерів, оскільки дозволяють легко дешифрувати дані. На сьогодні найвідоміші та найпоширеніші шифри - це AES та Blowfish, їх можна зустріти в більшості VPN. Крім того, для шифрування та дешифрування використовується RSA, тоді як SHA-1 та SHA-2 застосовуються при аутентифікації та хешуванні.

Однак найбільш безпечним шифром для VPN вважається AES, особливо характерним є те, що саме цим шифруванням користується уряд США.

Найбільш простий спосіб зрозуміти, скільки часу потрібно, щоб дешифрувати дані - це довжина ключа та ряди нулів та одиниць, що використовуються у шифрі. При використанні методу підбору "brute force" виконується прямолінійна спроба дешифрувати ключ - перевіряються всі доступні комбінації, поки не буде знайдена відповідна. Зазвичай довжина ключа VPN становить від 128 до 256 біт, а вищі рівні використовуються для аутентифікації. Щоб зламати 128-бітний шифр, знадобиться $3,4 \times 10^{38}$ операцій. Звичайно, щоб зламати 256-бітний шифр, необхідно в 2 (128) разів більше обчислень. Підбір 256-бітного шифру вимагатиме $3,31 \times 10^{65}$ операцій, що дорівнює кількості атомів у всесвіті.

Розглянемо загальну таблицю переваг та недоліків серед вищенаведених протоколів, та виберемо найбільш оптимальний.

Таблиця 2.2

Переваги та недоліки серед протоколів VPN

	PPTP	L2TP/IPSec	OpenVPN	SSTP	IKEv2
Переваги	- висока швидкість - вбудований клієнт на багатьох платформах - просте налаштування	- відносно надійні протоколи - доступні на багатьох пристроях та системах	- гнучке налаштування - відкритий код - сумісний із різними алгоритмами шифрування	- підтримка Microsoft - Рівень безпеки залежить від вибраного шифру	- підтримка різних шифрів, зокрема 3DES, AES, AES 256 - автопідключення при роз'єднанні - зрозуміле для користувача налаштування - швидше ніж L2TP, PPTP, SSTP

Недоліки	• не гарантує повну безпеку даних • легко піддається взлому	• повільніше за OpenVPN • великий обсяг додаткової інформації, що додається до вихідного пакету	• складне налаштування • потрібне стороннє ПЗ • обмежена підтримка мобільних додатків	• Працює лише на платформах Windows	• обмежена підтримка платформ • порт UDP 500 легше заблокувати, ніж у SSTP або OpenVPN • закритий вихідний код • складне налаштування на серверах

Розглянувши вищенаведені протоколи, оцінивши переваги та недоліки кожного з них та урахувавши потреби транспортної організації, було прийнято рішення організувати VPN-тунель за допомогою протоколів **L2TP/IPSec** як простого, але водночас надійного та оптимального з боку витрат рішення захисту, доступного на багатьох платформах.

2.4 Розробка функціональної схеми системи захищеного обміну даними з рухомим транспортом

В даному проекті системи буде розглянута кампусна мережа [32] організації, що представлена одним офісом, що складається з трьох зон та віддаленою локальною мережею транспортного засобу до якої підключені

пристрої інтернету речей. Дві зони подібні між собою і утворюють робочі зони організації. Запроваджена можливість розширення мережі за рахунок збільшення кількості кінцевих пристроїв до наявних портів комутаторів та додавання ще декількох подібних зон. У третій зоні розміщені серверні потужності, які виконують обчислення інформації та підтримку зв'язку з рухомим транспортом. Спроектована трирівнева ієрархічна структура мережі. Топологія мережі доступна на рис. А.1.

Для підключення пристроїв мережі між собою використовуються високошвидкісні порти FastEthernet та GigabitEthernet. Дані порти відрізняються пропускнуою здатністю в 100Мбіт/с та 1000 Мбіт/с відповідно.

Детальну топологію з'єднань мережі можна побачити в табл. 2.3.

Таблиця 2.3

Параметри інтерфейсів пристроїв мережі

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Маршрутизатор RouterInternet	Gi0/0	Маршрутизатор RouterMain	Gi0/0
	Gi0/1	Маршрутизатор RouterBackup	Gi0/0
	Gi0/2	Маршрутизатор RouterRemote	Gi0/0
Маршрутизатор RouterMain	Gi0/0	Маршрутизатор RouterInternet	Gi0/0
	Gi0/1	Комутатор SwitchMain	Gi1/0/1
Маршрутизатор RouterBackup	Gi0/0	Маршрутизатор RouterInternet	Gi0/1
	Gi0/1	Комутатор SwitchMain	Gi1/0/2
Комутатор SwitchMain	Gi1/0/1	Маршрутизатор RouterMain	Gi0/1
	Gi1/0/2	Маршрутизатор RouterBackup	Gi0/1
	Gi1/0/3	Комутатор SwitchFirst	Gi0/1
	Gi1/0/4	Комутатор SwitchSecond	Gi0/1
	Gi1/0/5	Комутатор SwitchThird	Gi0/1

Продовження таблиці 2.3

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Комутатор SwitchFirst	Gi0/1	Комутатор SwitchMain	Gi1/0/3
	Fa0/1	Робоча станція PC1-1	Fa0
	Fa0/2	Робоча станція PC1-2	Fa0
	Fa0/23	Робоча станція PC1-3	Fa0
	Fa0/24	Робоча станція PC1-4	Fa0
	Gi0/2	Маршрутизатор RouterWiFi1	0/0
Комутатор SwitchSecond	Gi0/1	Комутатор SwitchMain	Gi1/0/4
	Fa0/1	Робоча станція PC2-1	Fa0
	Fa0/2	Робоча станція PC2-2	Fa0
	Fa0/23	Робоча станція PC2-3	Fa0
	Fa0/24	Робоча станція PC2-4	Fa0
	Gi0/2	Маршрутизатор RouterWiFi2	0/0
Комутатор SwitchThird	Gi0/1	Комутатор SwitchMain	Gi1/0/5
	Gi1/1	Сервер Server0	Gi0
	Gi2/1	Сервер Server1	Gi0
	Gi3/1	Сервер Server-DNS	Gi0
	Gi4/1	Сервер Server-IoT	Gi0
	Fa3/1	Робоча станція PC3-1	Fa0
	Fa4/1	Робоча станція PC3-2	Fa0
Маршрутизатор RouterWiFi0	0/0	Маршрутизатор RouterRemote1	Gi0/1
	Wireless	Робоча станція Transit-BC	Wireless
		Вебкамера Transit-IoT0	Wireless
		Гучномовець Transit-IoT1	Wireless
Маршрутизатор RouterWiFi1	0/0	Комутатор SwitchFirst	Gi0/2
	Wireless	Телефон Phone1	Wireless
		Робоча станція PC1-5	Wireless
Маршрутизатор RouterWiFi2	0/0	Комутатор SwitchSecond	Gi0/2
	Wireless	Телефон Phone2	Wireless
		Робоча станція PC2-5	Wireless
Робоча станція PC1-1	Fa0	Комутатор SwitchFirst	Fa0/1

Продовження таблиці 2.3

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Робоча станція PC1-2	Fa0	Комутатор SwitchFirst	Fa0/2
Робоча станція PC1-3	Fa0	Комутатор SwitchFirst	Fa0/23
Робоча станція PC1-4	Fa0	Комутатор SwitchFirst	Fa0/24
Робоча станція PC1-5	Wireless	Маршрутизатор RouterWiFi1	Wireless
Робоча станція PC2-1	Fa0	Комутатор SwitchSecond	Fa0/1
Робоча станція PC2-2	Fa0	Комутатор SwitchSecond	Fa0/2
Робоча станція PC2-3	Fa0	Комутатор SwitchSecond	Fa0/23
Робоча станція PC2-4	Fa0	Комутатор SwitchSecond	Fa0/24
Робоча станція PC2-5	Wireless	Маршрутизатор RouterWiFi2	Wireless
Робоча станція PC3-1	Fa0	Комутатор SwitchThird	Fa0/1
Робоча станція PC3-2	Fa0	Комутатор SwitchThird	Fa0/2
Робоча станція Transit-BC	Wireless	Маршрутизатор RouterWiFi0	Wireless
Вебкамера Transit-IoT0	Wireless	Маршрутизатор RouterWiFi0	Wireless
Гучномовець Transit-IoT1	Wireless	Маршрутизатор RouterWiFi0	Wireless
Телефон Phone1	Wireless	Маршрутизатор RouterWiFi1	Wireless
Телефон Phone2	Wireless	Маршрутизатор RouterWiFi2	Wireless
Сервер Server0	Gi0	Комутатор SwitchThird	Gi1/1
Сервер Server1	Gi0	Комутатор SwitchThird	Gi2/1
Сервер Sever-DNS	Gi0	Комутатор SwitchThird	Gi5/1
Сервер Server-IoT	Gi0	Комутатор SwitchThird	Gi6/1

Для забезпечення функціонування топології мережі організації, перш за все було виконано розрахунок параметрів IP-адресації. Під час розрахунку параметрів IP-адресації особлива увага була приділена економії IP-адрес, а також було приділено увагу забезпеченню захищеного обміну даними з транспортним засобом [33]. Внутрішня адресація мережі як офісів, так і транспортногo засобу буде налагоджена за рахунок протоколу динамічного налаштування вузла – Dynamic Host Configuration Protocol (DHCP). Внутрішня мережа для зручності налаштування та підвищення безпеки буде поділена на віртуальні локальні мережі – Virtual Local Area Network (VLAN). В процесі проектування була

створена функціональна схема системи захищеного обміну даними з транспортним засобом (рис. 2.15).

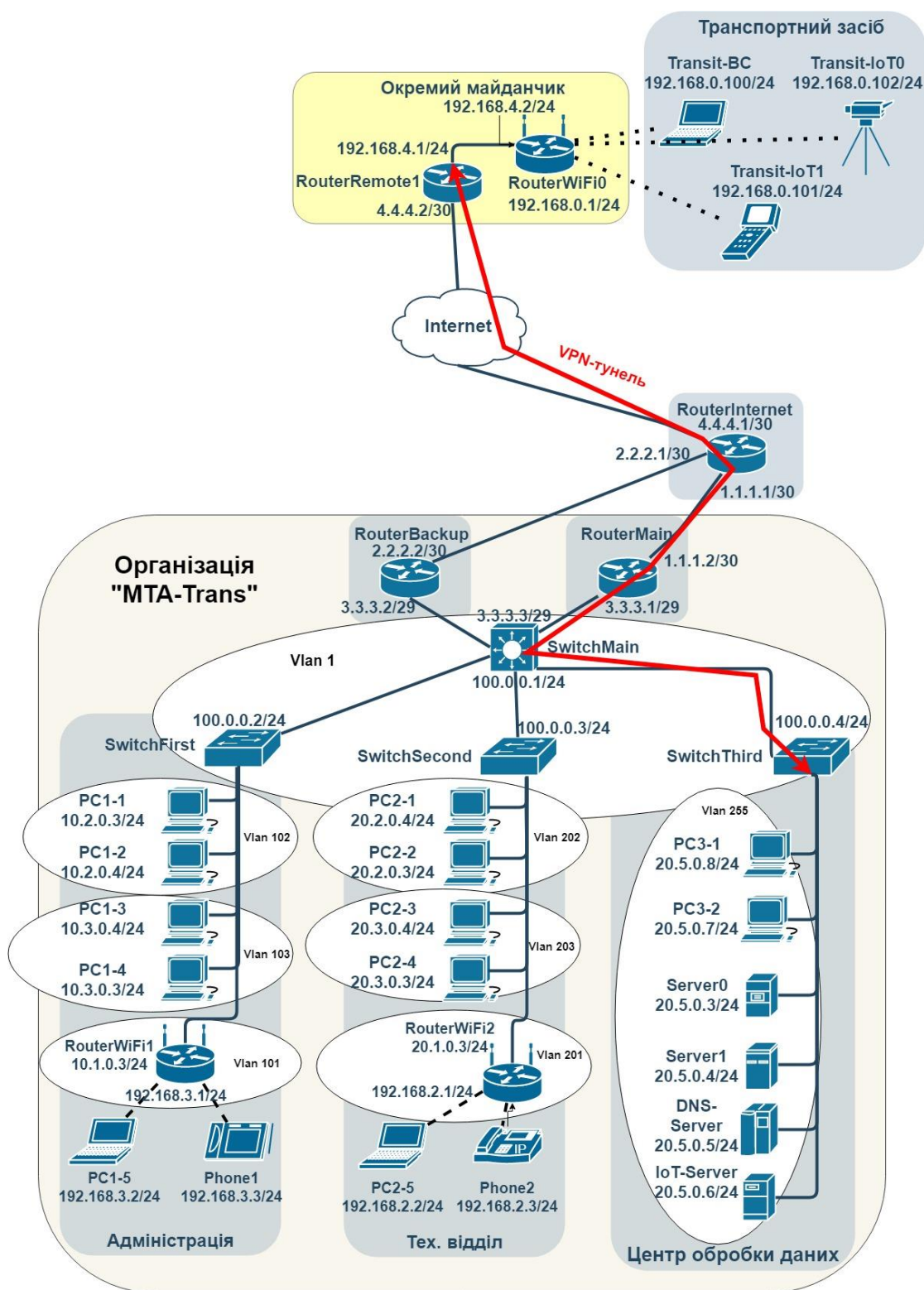


Рис. 2.15 – Функціональна схема системи захищеного обміну даними з транспортним засобом в організації

Детальні параметри адресації мережі представлені в табл. 2.4.

Таблиця 2.4

Параметри адресації пристроїв мережі

Підмережа/ Пристрій	Інтерфейс/Мереж- ний адаптер/Шлюз	ІР-адреса	Маска підмережі	Префікс
Маршрутизатор RouterInternet	Gi0/0	1.1.1.1	255.255.255.252	/30
	Gi0/1	2.2.2.1	255.255.255.252	/30
	Gi0/2	4.4.4.1	255.255.255.252	/30
Маршрутизатор RouterMain	Gi0/0	1.1.1.2	255.255.255.252	/30
	Gi0/1	3.3.3.1	255.255.255.248	/29
Маршрутизатор RouterBackup	Gi0/0	2.2.2.2	255.255.255.252	/30
	Gi0/1	3.3.3.2	255.255.255.248	/29
Маршрутизатор RouterRemote1	Gi0/0	4.4.4.2	255.255.255.252	/30
	Gi0/1	192.168.4.1	255.255.255.0	/24
Комутатор SwitchMain	Vlan1	100.0.0.1	255.255.255.0	/24
	Vlan8	3.3.3.3	255.255.255.248	/29
	Vlan101	10.1.0.1	255.255.255.0	/24
	Vlan102	10.2.0.1	255.255.255.0	/24
	Vlan103	10.3.0.1	255.255.255.0	/24
	Vlan201	20.1.0.1	255.255.255.0	/24
	Vlan202	20.2.0.1	255.255.255.0	/24
	Vlan203	20.3.0.1	255.255.255.0	/24
Комутатор SwitchFirst	Vlan255	25.5.0.1	255.255.255.0	/24
	Vlan1	100.0.0.2	255.255.255.0	/24
	Vlan101	10.1.0.2	255.255.255.0	/24
	Vlan102	10.2.0.2	255.255.255.0	/24
Комутатор SwitchSecond	Vlan103	10.3.0.2	255.255.255.0	/24
	Vlan1	100.0.0.3	255.255.255.0	/24
	Vlan201	20.1.0.2	255.255.255.0	/24
	Vlan202	20.2.0.2	255.255.255.0	/24
Комутатор SwitchThird	Vlan203	20.3.0.2	255.255.255.0	/24
	Vlan1	100.0.0.4	255.255.255.0	/24
Маршрутизатор RouterWiFi0	Vlan255	25.5.0.2	255.255.255.0	/24
	0/0	192.168.4.2	255.255.255.0	/24
Маршрутизатор RouterWiFi1	Wireless	192.168.0.1	255.255.255.0	/24
	0/0	DHCP		
Маршрутизатор RouterWiFi2	Wireless	192.168.1.1	255.255.255.0	/24
	0/0	DHCP		
Робоча станція PC1-1	Fa0	DHCP		
Робоча станція PC1-2	Fa0			
Робоча станція PC1-3	Fa0			
Робоча станція PC1-4	Fa0			
Робоча станція PC1-5	Wireless			
Робоча станція PC2-1	Fa0			
Робоча станція PC2-2	Fa0			
Робоча станція PC2-3	Fa0			
Робоча станція PC2-4	Fa0			
Робоча станція PC2-5	Wireless			

Продовження таблиці 2.4

Підмережа/ Пристрій	Інтерфейс/Мереж- ний адаптер/Шлюз	IP-адреса	Маска підмережі	Префікс
Робоча станція PC3-1	Fa0	DHCP		
Робоча станція PC3-2	Fa0			
Робоча станція Transit-BC	Wireless			
Вебкамера Transit-IoT0	Wireless			
Гучномовець Transit-IoT1	Wireless			
Телефон Phone1	Wireless			
Телефон Phone2	Wireless			
Сервер Server0	Gi0	25.5.0.3	255.255.255.0	/24
Сервер Server1	Gi0	25.5.0.4	255.255.255.0	/24
Сервер DNS-Server	Gi0	25.5.0.5	255.255.255.0	/24
Сервер IoT-Server	Gi0	25.5.0.6	255.255.255.0	/24

Висновки по 2 розділу

У даному розділі проведено роботу над розробкою системи захищеного обміну даними з рухомим транспортом. Проведено аналіз шаблонів проектування та виділено переваги та недоліки кожного з них, виділено метод екранованої підмережі, прийнято рішення дотримуватись саме цього патерну.

Проведено аналіз існуючих технічних засобів для реалізації проекту, приведені особливості та переваги комутаторів та маршрутизаторів компанії Cisco.

Прийнято рішення використовувати VPN-технології, проаналізовано та зіставлено переваги та недоліки відомих протоколів передачі даних. Як найотпимальніший варіант був вибраний протокол IPSec.

Приведено структурну схему системи, проведено аналіз можливих загроз витоку даних та представлені методи їх попередження.

Розроблено функціональну схему системи захисту з проектуванням схеми мережі транспортної організації.

РОЗДІЛ 3. ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ ТА ЕФЕКТИВНОСТІ ПРИЙНЯТИХ РІШЕНЬ В СИСТЕМІ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ З РУХОМИМ ТРАНСПОРТОМ

3.1. Розробка моделі системи захищеного обміну даними з рухомим транспортом в Cisco Packet Tracer

В даному пункті розглянуто базові налаштування пристроїв мережі організації. Для повного розуміння, який пристрій налаштовується, зручності конфігурування та перевірки зв'язку між пристроями по імені, стандартні імена елементів мережі були змінені на ті, які відповідають проекту (рис. 3.1).

```
IR800>enable
IR800#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
IR800(config)#hostname RouterRemote1
RouterRemote1(config)#
```

Рис. 3.1 – Налаштування імені на маршрутизаторі RouterRemote

Необхідно налаштувати статичну адресацію інтерфейсів мережі, тому це буде наступним кроком у налаштуванні мережі. За відповідною адресою пристрої будуть знаходити один одного у мережі.

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

```
RouterInternet(config)#int g0/0
RouterInternet(config-if)#ip add 1.1.1.1 255.255.255.252
RouterInternet(config-if)#no sh

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

Рис. 3.2 – Налаштування статичної IP-адреси на маршрутизаторі RouterInternet

Також статичні IP-адреси налаштовуються на серверах для їх незмінності (рис. 3.3). Згодом це допоможе для налаштувань різноманітних сервісів.

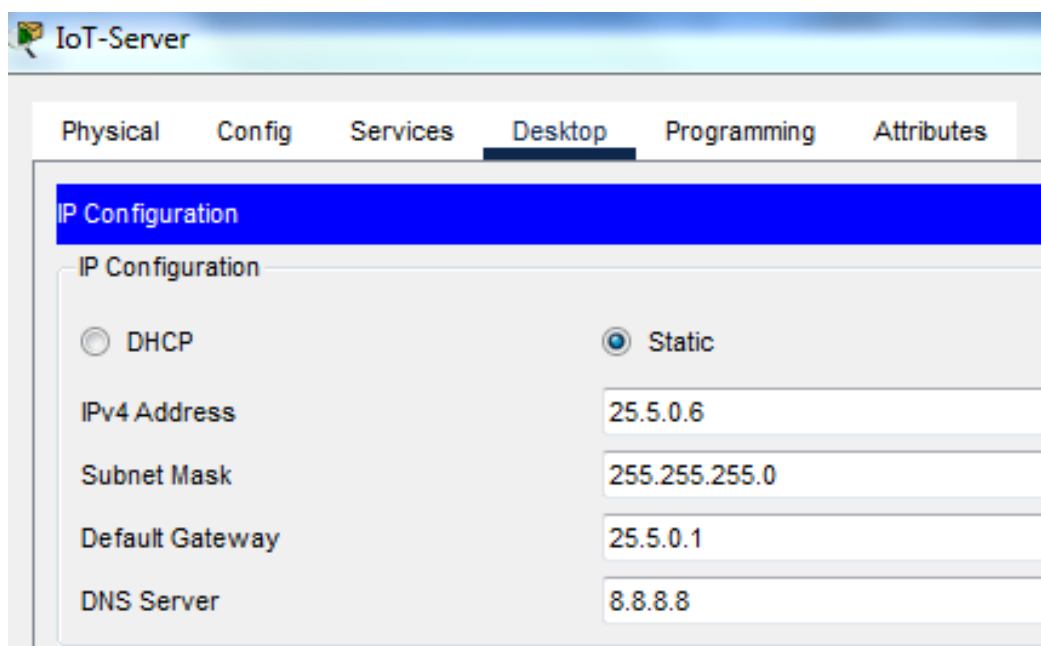


Рис. 3.3 – Налагодження статичної IP-адреси на сервері IoT-Server

Для імітації виходу до мережі Інтернет був налагоджений інтерфейс замкнення на самого себе – loopback. Даний інтерфейс являє собою петлевидний зв'язок на маршрутизаторі RouterInternet (рис. 3.4).

```
RouterInternet(config)#int loopback 1
RouterInternet(config-if)#ip add 172.16.0.1 255.255.255.252
RouterInternet(config-if)#no sh
RouterInternet(config-if)#ex
```

Рис. 3.4 – Налаштування loopback-інтерфейсу на маршрутизаторі RouterInternet

Також статичні IP-адреси використовуються на комутаторах рівня ядра та розподілу. Це дозволяє точно знати, як звернутись до комутатора для перевірки чи налаштування. Слід також зазначити, що це допоможе і у процесі віддаленого керування. На рис. 3.5 показане налаштування статичної адреси для інтерфейсу Vlan8, який буде використовуватись при реалізації зв'язку маршрутизаторів за допомогою протоколу HSRP.

```

SwitchMain(config)#vlan 8
SwitchMain(config-vlan)#name FOR_HSRP
SwitchMain(config-vlan)#ex
SwitchMain(config)#int vlan 8
SwitchMain(config-if)#
%LINK-5-CHANGED: Interface Vlan8, changed state to up

SwitchMain(config-if)#ip add 3.3.3.3 255.255.255.248
SwitchMain(config-if)#no sh

```

Рис. 3.5 – Налаштування статичної IP-адреси для інтерфейсу Vlan8 на багаторівневому комутаторі SwitchMain

Для організації більш зручного адміністрування мережі, внутрішня підмережа розділена на віртуальні локальні мережі (VLAN).

Дана структура реалізується за допомогою тегування трафіка, де вказується приналежність до тої чи іншої VLAN. Детальний опис цього є у відкритому стандарті IEEE 802.1Q який було проаналізовано у попередньому розділі. Завдяки пристроям маршрутизації, VLAN дозволяє встановлювати контроль за трафіком, та блокувати або дозволяти обмін даними. Приклад налагодження VLAN представлений на рис. 3.6.

```

SwitchMain(config)#int range g1/0/1-2
SwitchMain(config-if-range)#switchport mode access
SwitchMain(config-if-range)#switchport access vlan 8
SwitchMain(config-if-range)#ex

```

Рис. 3.6 – Зміна стандартного Vlan для портів GigabitEthernet1/0/1 та GigabitEthernet1/0/2 на багаторівневому комутаторі SwitchMain

Для доступності обміну всіх VLAN між собою та іншими мережами, в тому числі і глобальними, на комутаторах були налагоджені транкові канали зв'язку. Дані канали допускають проходження трафіку з вибраних VLAN, що дозволяє здійснювати обмін даними без перешкод. Приклад налагодження подібного каналу показаний на рис. 3.7.

```

SwitchMain(config)#int g1/0/3
SwitchMain(config-if)#switchport trunk encapsulation dot1q
SwitchMain(config-if)#switchport mode trunk

SwitchMain(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan101, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan102, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan103, changed state to up

SwitchMain(config-if)#switchport trunk allowed vlan add 1
SwitchMain(config-if)#switchport trunk allowed vlan add 101
SwitchMain(config-if)#switchport trunk allowed vlan add 102
SwitchMain(config-if)#switchport trunk allowed vlan add 103

```

Рис. 3.7 – Налаштування транкового каналу на багаторівневому комутаторі SwitchMain

Далі були сконфігуровані IP-адреси кінцевих пристроїв. Вони були згенеровані за рахунок налагодження протоколу DHCP. Даний протокол дозволяє автоматично видавати для кінцевого пристрою всі потрібні налаштування мережі – IP-адресу, маску підмережі, шлюз за замовчуванням, адресу DNS (Domain Name Server) та ім'я домену підмережі [34]. На комутаторі рівня L3 (SwitchMain), на якому зав'язані усі підмережі через комутатори L2, був налаштований даний протокол. Щоб уникнути проблем зі статичними адресам для серверів, такі адреси заздалегідь були додані у винятки (див. рис. 3.8). Налаштування самого DHCP на рис. 3.9.

```

SwitchMain#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchMain(config)#ip dhcp excluded-address 10.1.0.1 10.1.0.2
SwitchMain(config)#ip dhcp excluded-address 10.2.0.1 10.2.0.2
SwitchMain(config)#ip dhcp excluded-address 10.3.0.1 10.3.0.2
SwitchMain(config)#ip dhcp excluded-address 20.1.0.1 20.1.0.2
SwitchMain(config)#ip dhcp excluded-address 20.2.0.1 20.2.0.2
SwitchMain(config)#ip dhcp excluded-address 25.5.0.1 25.5.0.4
SwitchMain(config)#ip dhcp excluded-address 20.3.0.1 20.3.0.2
SwitchMain(config)#ip dhcp excluded-address 25.5.0.1 25.5.0.6

```

Рис. 3.8 – Додавання статичних IP-адрес у винятки переда налаштуванням DHCP на багаторівневому комутаторі SwitchMain

```
SwitchMain(config)#ip dhcp pool AdminLAN
SwitchMain(dhcp-config)#network 25.5.0.0 255.255.255.0
SwitchMain(dhcp-config)#default-router 25.5.0.1
SwitchMain(dhcp-config)#dns-server 8.8.8.8
SwitchMain(dhcp-config)#domain-name adminlan.com
SwitchMain(dhcp-config)#ex
SwitchMain(config)#|
```

Рис. 3.9 – Налаштування DHCP на багаторівневому комутаторі SwitchMain

Комутатори L2 також були налаштовані для підтримки транкових каналів обміну даними, аналогічні до вищепроведених, окрім методу інкапсуляції – на цих комутаторах є лише 802.1Q.

Внутрішній трафік від однієї VLAN до іншої називають inter-VLAN routing (внутрішня маршрутизація між VLAN). На комутаторах Cisco Catalyst він створюється на інтерфейсах третього рівня і називаються дані інтерфейси як Switch virtual interfaces (SVI) – віртуальні інтерфейси комутатора [35].

Для початку роботи inter-VLAN вводимо команду iprouting (рис. 3.10).

```
SwitchMain#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchMain(config)#ip routing
```

Рис. 3.10 – Запуск inter-VLAN routing з консолі SwitchMain

Налагодивши VLAN з комутатором L3 ми можемо не використовувати динамічні протоколи маршрутизації, але вони все ж необхідні для рівня ядра. Налаштуємо протокол динамічної маршрутизації OSPF процес чого наведено на рис. 3.11.

```
RouterBackup(config)#router ospf 1
RouterBackup(config-router)#network 2.2.2.0 255.255.255.252 area 0
RouterBackup(config-router)#network 3.3.3.0 255.255.255.248 area 0
RouterBackup(config-router)#
00:16:38: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.1 on GigabitEthernet0/1 from LOADING to FULL, Loading Done
```

Рис. 3.11 – Налаштування протоколу OSPF на маршрутизаторі RouterBackup

Перейдемо до налагодження маршрутизатору та VPN-тунелю для захищеного обміну даними з рухомим транспортом. Концептуально система будується на основі бездротового підключення пристроїв IoT та бортового комп'ютера рухомого транспорту до мережі організації, саме тому був обраний

бездротовий роутер WRT300N. Процес налагодження маршрутизатора RouterRemote1 показаний на рис. 3.12.

```
RouterRemote1(config)#int gig0/0
RouterRemote1(config-if)#ip address 4.4.4.2 255.255.255.252
RouterRemote1(config-if)#no shutdown

RouterRemote1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

RouterRemote1(config-if)#ex
RouterRemote1(config)#router ospf 100
RouterRemote1(config-router)#network 4.4.4.0 0.0.0.3 area 0
```

Рис. 3.12 – Налаштування з'єднання на маршрутизаторі RouterRemote1

Наступне це налагодження VPN-тунелю між мережею організації та транспортним засобом за допомогою обраного у попередньому розділі набору протоколів IPSec. Для цього необхідно налаштувати IPSec на кожному з роутерів по обидва кінці тунелю, а саме RouterRemote1 та RouterMain.

Для початку попередньо переконаємось, що ліцензія безпеки security9k увімкнена на кожному з обох маршрутизаторів за допомогою команди show version (рис. 3.13).

```
Technology Package License Information for Module:'c2900'

-----
Technology      Technology-package      Technology-package
Current          Type                    Next reboot
-----
ipbase          ipbasek9               Permanent            ipbasek9
security        securityk9              Evaluation            securityk9
uc              disable                 None                  None
data            disable                 None                  None

Configuration register is 0x2102
```

Рис. 3.13 – Перевірка наявності увімкненої ліцензії security9k на маршрутизаторі RouterRemote1

На маршрутизаторі RouterMain ця технологія була вимкнена, тому використовуючи команду license boot module c2900 technology-package securityk9 увімкнемо її (рис. 3.14).

```

ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot
%LICENSE-6-EULA_ACCEPTED: EULA for feature securityk9 1.0 has been accepted.
UDI=CISCO2911/K9:FTX152490IZ-; StoreIndex=0:Evaluation License Storage

RouterMain(config)#
*Jun 02, 17:58:15.5858: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name =
C2900 Next reboot level = securityk9 and License = securityk9
RouterMain(config)#

```

Рис. 3.14 – Процес налагодження технології безпеки **security9k** на маршрутизаторі RouterMain

Почнемо з налаштування маршрутизатора RouterRemote1. Першим кроком є налаштування політики ISAKMP Phase 1:

```

Enter configuration commands, one per line. End with CNTL/Z.
RouterRemote1(config)#crypto isakmp policy 10
RouterRemote1(config-isakmp)#encryption aes 256
RouterRemote1(config-isakmp)#authentication pre-share
RouterRemote1(config-isakmp)#group 5
RouterRemote1(config-isakmp)#

```

Рис. 3.15 – Процес налаштування політики ISAKMP Phase 1 на маршрутизаторі RouterRemote1

Далі ми збираємось визначити Pre-Shared ключ для аутентифікації з RouterMain за допомогою наступної команди зображеної на рис 3.16.

```

RouterRemote1(config-isakmp)#ex
RouterRemote1(config)#crypto isakmp key secretkey address 1.1.1.2
RouterRemote1(config)#

```

Рис. 3.16 – Визначення спільного ключа для аутентифікації **secretkey** між двома маршрутизаторами зі вказівкою публічної адреси RouterMain

Для налаштування IPSec нам необхідно створити розширений access-list, набір перетворення IPSec, криптографічну карту (Crypto Map), та застосувати дану карту до загальнодоступного (public) інтерфейсу.

Нам потрібно створити розширений access-list і в ньому визначити, який трафік ми хочемо пропускати через VPN-тунель (рис. 3.17).

```
RouterRemotel(config)#access-list 100 permit ip 192.168.4.0 0.0.0.255 3.3.3.0 0.0.0.7
RouterRemotel(config)#access-list 100 permit ip 192.168.4.0 0.0.0.255 25.5.0.0 0.0.0.7
RouterRemotel(config)#
```

Рис. 3.17 – Налаштування розширеного списку доступу на маршрутизаторі RouterRemotel1

Наступним кроком є створення набору перетворення (Transform Set), що використовується для захисту даних (рис 3.18), де **esp-aes** – метод шифрування, а **sha** – алгоритм шифрування.

```
RouterRemotel(config)#crypto ipsec transform-set vpna esp-aes 256 esp-sha-hmac
RouterRemotel(config)#
```

Рис. 3.18 – Створення набору перетворення на маршрутизаторі RouterRemotel1

Crypto Map є останнім етапом налаштування та об'єднує раніше задані конфігурації ISAKMP та IPSec (рис. 3.19).

```
RouterRemotel(config)#crypto map IPSEC-MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
RouterRemotel(config-crypto-map)# set peer 1.1.1.2
RouterRemotel(config-crypto-map)# set peer 2.2.2.2
RouterRemotel(config-crypto-map)# set pfs group5
RouterRemotel(config-crypto-map)# set security-association lifetime seconds 86400
RouterRemotel(config-crypto-map)# set transform-set vpna
RouterRemotel(config-crypto-map)# match address 100
RouterRemotel(config-crypto-map)#exit
RouterRemotel(config)#
RouterRemotel(config)#
```

Рис. 3.19 – Створення Crypto Map на маршрутизаторі RouterRemotel1

Застосуємо криптографічну карту до інтерфейсу маршрутизатора, через який виходить трафік. При цьому варто звернути увагу, що до інтерфейсу може бути закріплена тільки одна криптокарта (рис. 3.20).

```
RouterRemotel(config)#int gig0/0
RouterRemotel(config-if)#
RouterRemotel(config-if)#crypt
RouterRemotel(config-if)#crypto map IPSEC-MAP
*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
RouterRemotel(config-if)#
```

Рис. 3.20 – Застосування криптографічної карти до інтерфейсу маршрутизатора RouterRemotel1

Налаштування для RouterMain та RouterBackup ідентичні, з відмінностями лише в IP-адресах та ACL.

3.2. Розробка макету системи та оцінка її працездатності

Ми завершили початкове налаштування мережі, наступним кроком буде більше детальне налагодження складових пристроїв.

Додатково організуємо протокол маршрутизації мережевого рівня HSRP, що використовується для резервування шлюзу в Ethernet-мережах [36]. Процес налаштування показаний на рис. 3.21.

```
RouterMain(config)#int g0/1
RouterMain(config-if)#standby 1 ip 3.3.3.6
RouterMain(config-if)#standby 1 priority 50
%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Speak -> Standby
%HSRP-6-STATECHANGE: GigabitEthernet0/1 Grp 1 state Standby -> Active
FOR_INTERNET
RouterMain(config-if)#standby 1 track g0/0
RouterMain(config-if)#standby timers 5 10
RouterMain(config-if)#exit
```

Рис. 3.21 – Налагодження HSRP на маршрутизаторі RouterMain

Налаштовано маршрутизатори, що містять радіомодуль, тому виступають безпроводними точками доступу. Їх налаштування відрізняються від інших моделей маршрутизаторів (рис. 3.22-3.24).

Network Mode:	Mixed
Network Name (SSID):	T2476T
Radio Band:	Auto
Wide Channel:	Auto
Standard Channel:	1 - 2.412GHz
SSID Broadcast:	☒ Enabled ☐ Disabled

Рис. 3.22 – Налаштування базових конфігурацій радіомодуля на маршрутизаторі RouterWiFi0

Internet IP Address:	192	168	4	2
Subnet Mask:	255	255	255	0
Default Gateway:	192	168	4	1
DNS 1:	8	8	8	8
DNS 2 (Optional):	0	0	0	0
DNS 3 (Optional):	0	0	0	0
Host Name:				
Domain Name:				
MTU:		Size: 1500		
IP Address:	192	168	0	1
Subnet Mask:	255.255.255.0			
DHCP Server:	☒ Enabled ☐ Disabled		DHCP Reservation	
Start IP Address:	192.168.0.	100		
Maximum number of Users:	50			
IP Address Range: 192.168.0. 100 - 149				
Client Lease Time:	0			minutes (0 means one day)
Static DNS 1:	8	8	8	8

Рис. 3.23 – Налаштування внутрішньої та зовнішньої мережі на маршрутизаторі RouterWiFi0

Security Mode:	WPA2 Personal
Encryption:	AES
Passphrase:	Passt2476
Key Renewal:	3600 seconds

Рис. 3.24 – Налаштування автентифікації на маршрутизаторі Router WiFi1

Підключаємо наші кінцеві пристрої до безпроводної мережі (рис. 3.25-3.26).

Link Information

Connect

Profiles

Below is a list of available wireless networks. To search for more wireless networks, click the **Refresh** button. To view more information about a network, select the wireless network name. To connect to that network, click the **Connect** button below.

Wireless Network Name	CH	Signal
Wi-Fi2	11	40%
Wi-Fi1	1	39%
T2478T	1	38%

Site Information

Wireless Mode Infrastructure
Network Type Mixed B/G/N
Radio Band Auto
Security WPA2-PSK
MAC Address 0006.2ACA.6506

Refresh

Connect

2.4GHz


Adapter is Active

Wireless-N Notebook Adapter
Wireless Network Monitor v1.0
Model No. WPC300N

Рис. 3.25 – Підключення кінцевого пристрою Transit-BC до бездротової мережі

WPA2-Personal Needed for Connection

This wireless network has WPA2-Personal enabled. To connect to this network, enter the required passphrase in the appropriate field below. Then click the **Connect** button.

Security

WPA2-Personal

Please select the wireless security method used by your existing wireless network.

Pre-shared Key

Passt2476

Please enter a Pre-shared Key that is 8 to 63 characters in length.

Cancel

Connect

Рис. 3.26 – Підключення кінцевого пристрою Transit-BC до бездротової мережі

Налагоджено сервіси HTTP/HTTPS, TFTP, SYSLOG, NTP, DNS та IoT на серверах організації (рис. 3.27-3.32).

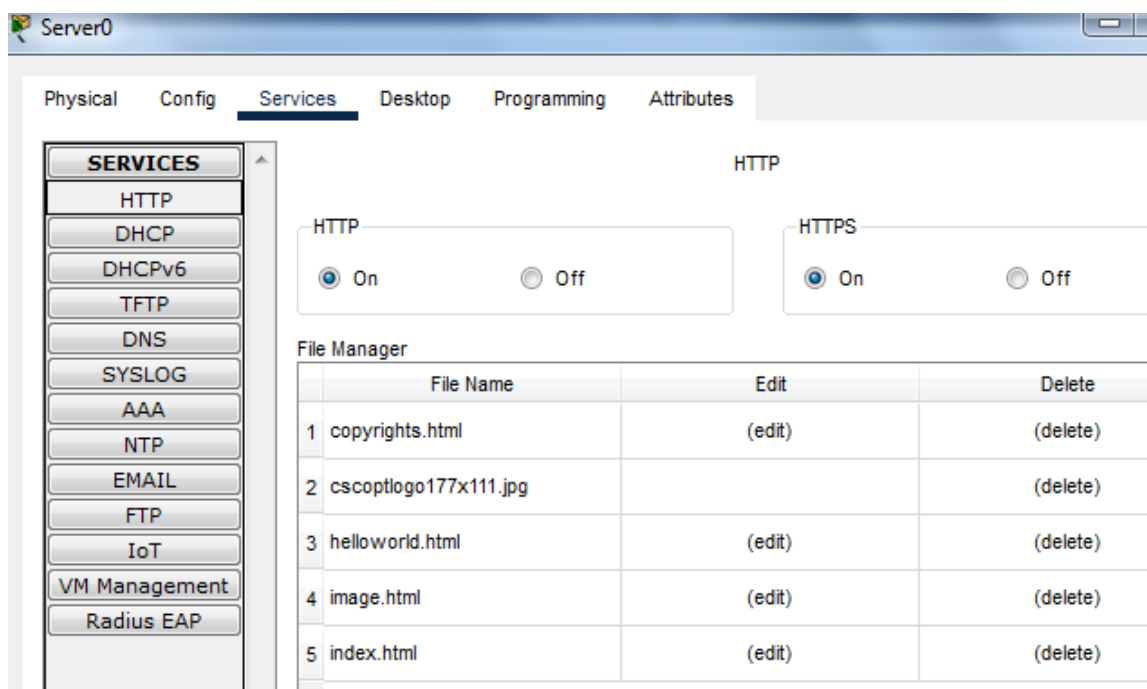


Рис. 3.27 – Налаштування сервісів HTTP/HTTPS [37] на сервері Server0

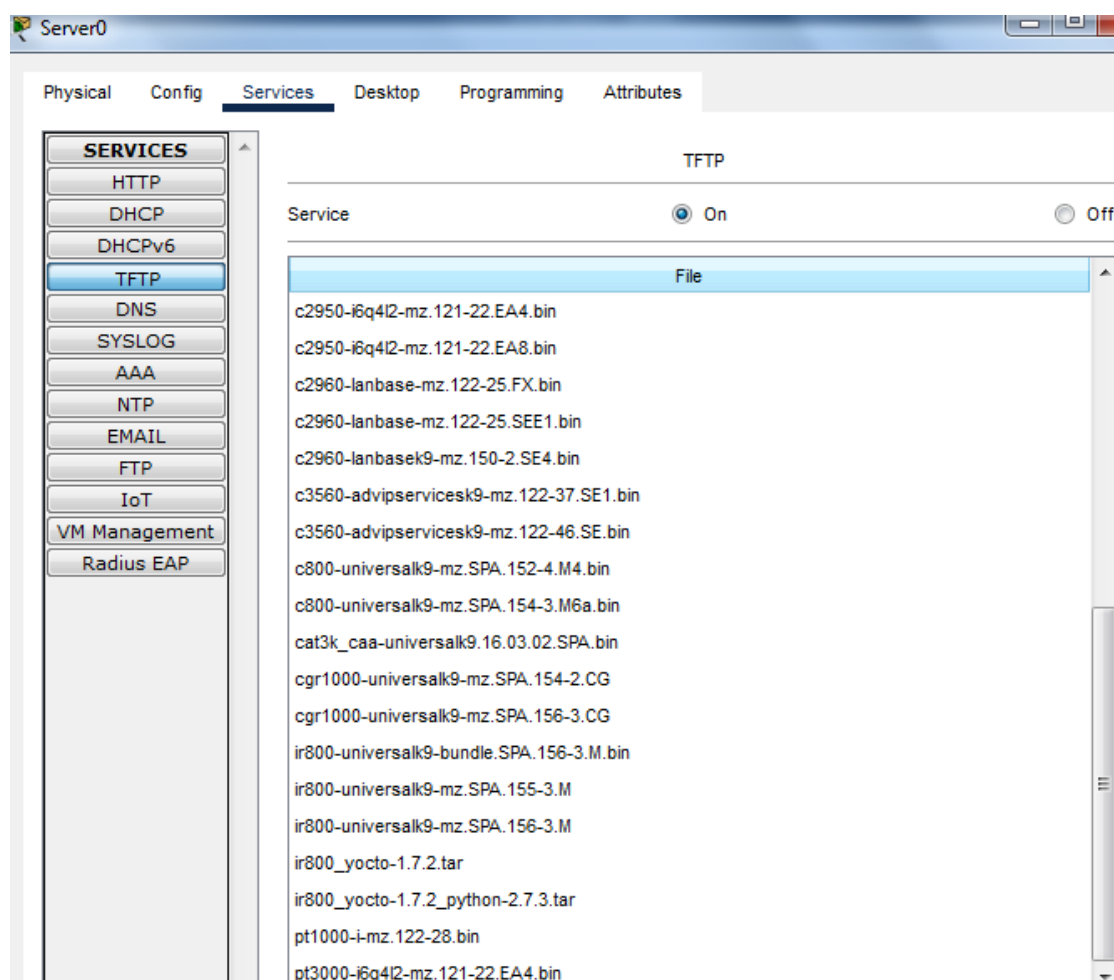


Рис. 3.28 – Налаштування сервісу TFTP [39] на сервері Server0

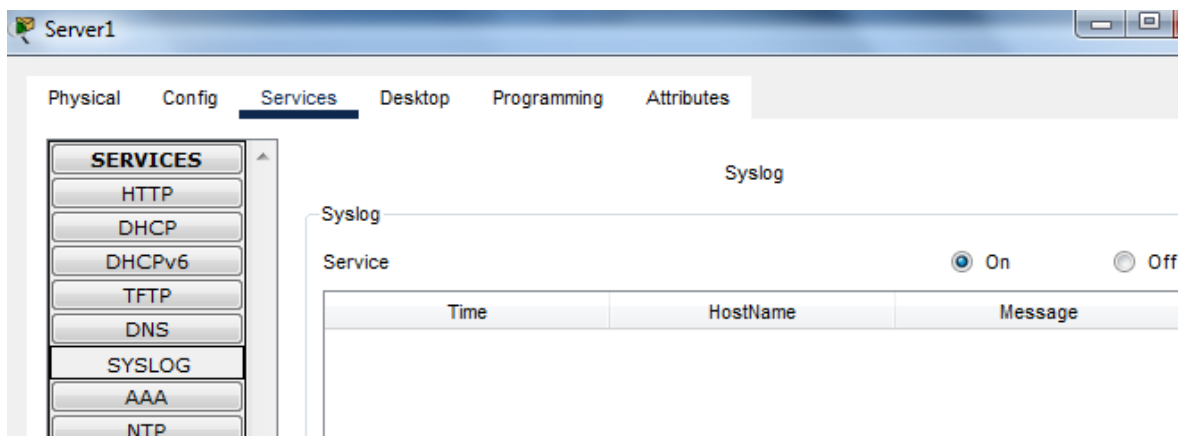


Рис. 3.29 – Налаштування сервісу SYSLOG на сервері Server1

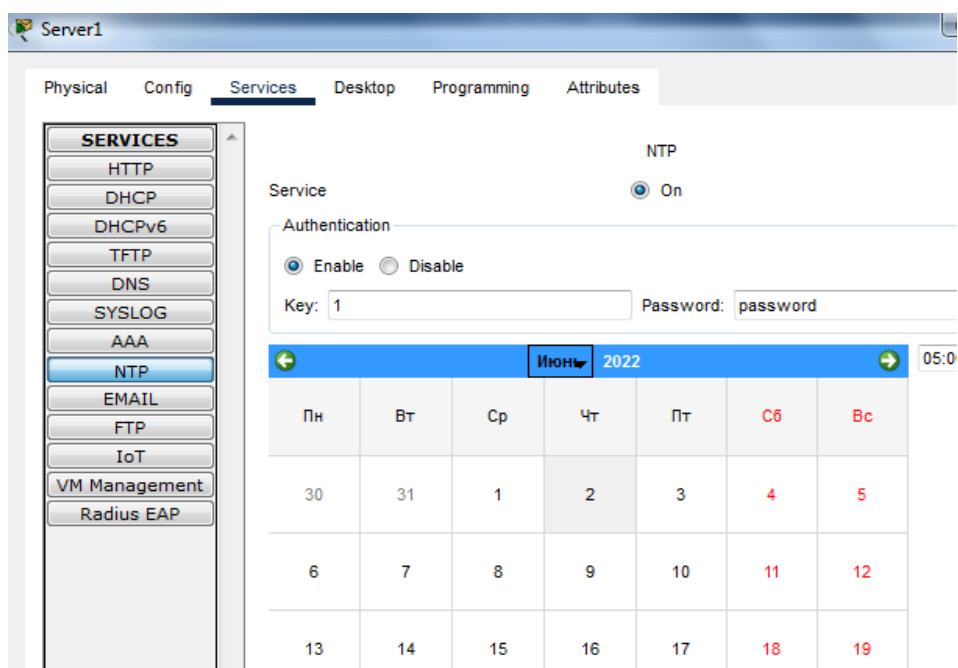


Рис. 3.30 – Налаштування сервісу NTP на сервері Server1

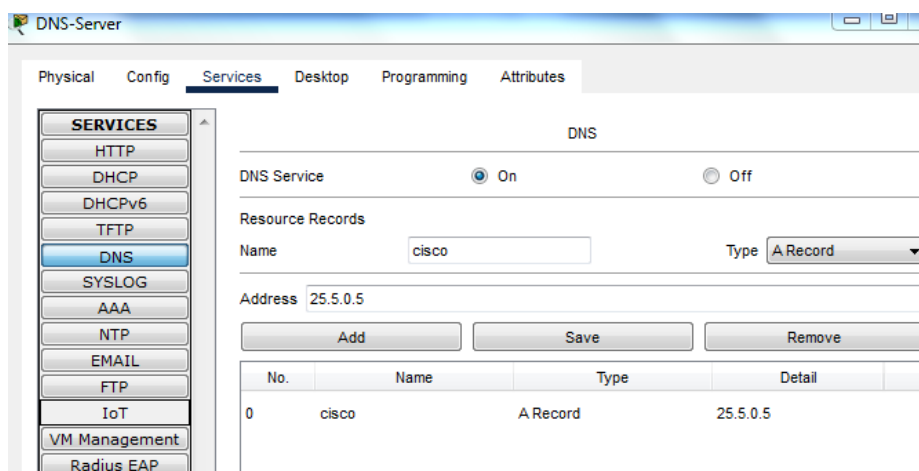


Рис. 3.31 – Налаштування сервісу DNS на сервері DNS-Server

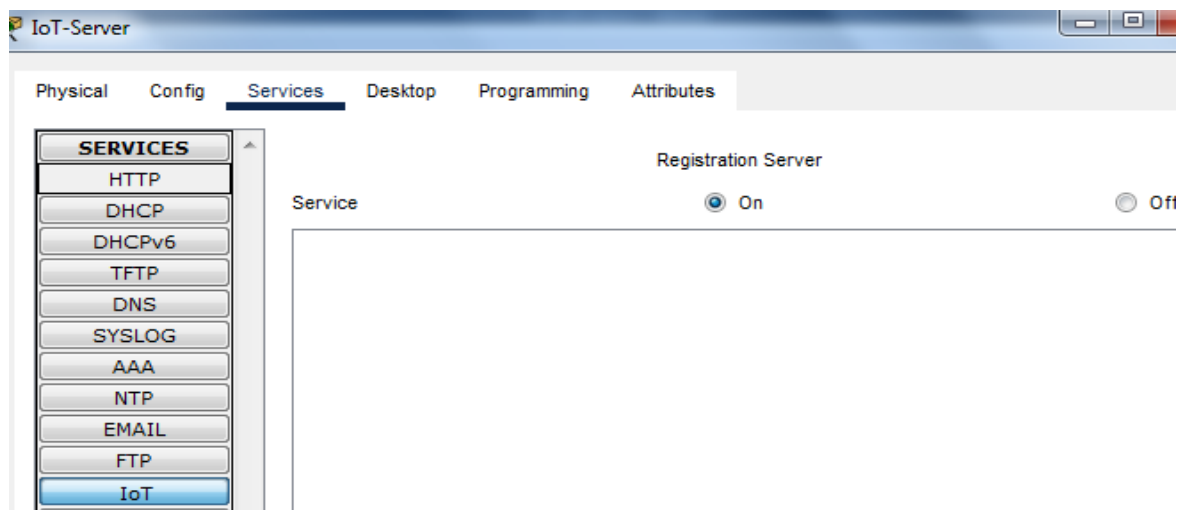


Рис. 3.32 – Налаштування сервісу IoT на сервері IoT-Server

Після того, як сервіси на серверах активовані, слід налаштувати ці сервіси на мережних пристроях. Першим з них є NTP – протокол системного часу [38]. Він призначений для синхронізації дій в мережі. При налагодженні використовується автентифікація, визначається сервер, що є джерелом часу та параметри корегування часу. Налаштування є однотипним, як для маршрутизаторів, так і для комутаторів (рис. 3.33).

```
SwitchThird(config)#service timestamps log datetime msec
SwitchThird(config)#service timestamps debug datetime msec
SwitchThird(config)#clock timezone EET 2
SwitchThird(config)#ntp server 25.5.0.4 key 1
SwitchThird(config)#ntp authenticate
SwitchThird(config)#ntp authentication-key 1 md5 password
SwitchThird(config)#ntp trusted-key 1
SwitchThird(config)#
SwitchThird#
```

Рис. 3.33 – Налаштування сервісу NTP на комутаторі SwitchThird

Перед тим як запустити сервіс журналів подій SYSLOG, був налагоджений віддалений доступ за допомогою протоколу SSH, зі створенням користувачів на пристроях [40] (рис. 3.34).

```

RouterInternet(config)#banner motd # Connection to router RouterInternet For legal users only #
RouterInternet(config)#username adminer privilege 15 secret adminerpass
RouterInternet(config)#username technic privilege 1 secret technicpass
RouterInternet(config)#enable secret enablepass
RouterInternet(config)#
RouterInternet(config)#crypto key generate rsa general-keys modulus 1024
% You already have RSA keys defined named RouterInternet.internet.com
% They will be replaced.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*июл 31 0:26:33.702: %SSH-5-ENABLED: SSH 2 has been enabled
RouterInternet(config)#ip ssh version 2
RouterInternet(config)#ip ssh time-out 60
RouterInternet(config)#ip ssh authentication-retries 5
RouterInternet(config)#line console 0
RouterInternet(config-line)#logging synchronous
RouterInternet(config-line)#login local
RouterInternet(config-line)#exit
RouterInternet(config)#line vty 0 4
RouterInternet(config-line)#transport input ssh
RouterInternet(config-line)#transport output ssh
RouterInternet(config-line)#logging synchronous
RouterInternet(config-line)#login local
RouterInternet(config-line)#exit
RouterInternet(config)#login block-for 10 attempts 3 within 3
RouterInternet(config)#login on-failure log
RouterInternet(config)#login on-success log
RouterInternet(config)#ex

```

Рис. 3.34 – Налаштування віддаленого підключення та користувачів на маршрутизаторі RouterInternet

Тепер налагодимо систему журналювання подій SYSLOG. Налаштування аналогічне для маршрутизаторів і комутаторів (рис. 3.35).

```

RouterInternet(config)#service timestamps log datetime msec
RouterInternet(config)#service timestamps debug datetime msec
RouterInternet(config)#logging on
RouterInternet(config)#logging 25.5.0.4
RouterInternet(config)#logging userinfo
RouterInternet(config)#logging trap debugging
RouterInternet(config)#logging buffered 64000
RouterInternet(config)#ex

```

Рис. 3.35 – Налаштування системи журналювання SYSLOG на маршрутизаторі RouterInternet

В мережі нашого транспортного засобу окрім бортового комп'ютера, присутні також пристрої інтернету речей, які необхідно підключити до серверу IoT-Server локальної мережі організації. Приклад наведено на рис. 3.36-3.37.



Рис. 3.36 – Реєстрація нового користувача на сервері IoT-Server

Після того як ми зареєструвались на сервері, можна підключити наші пристрої IoT з рухомого складу (рис. 3.37).

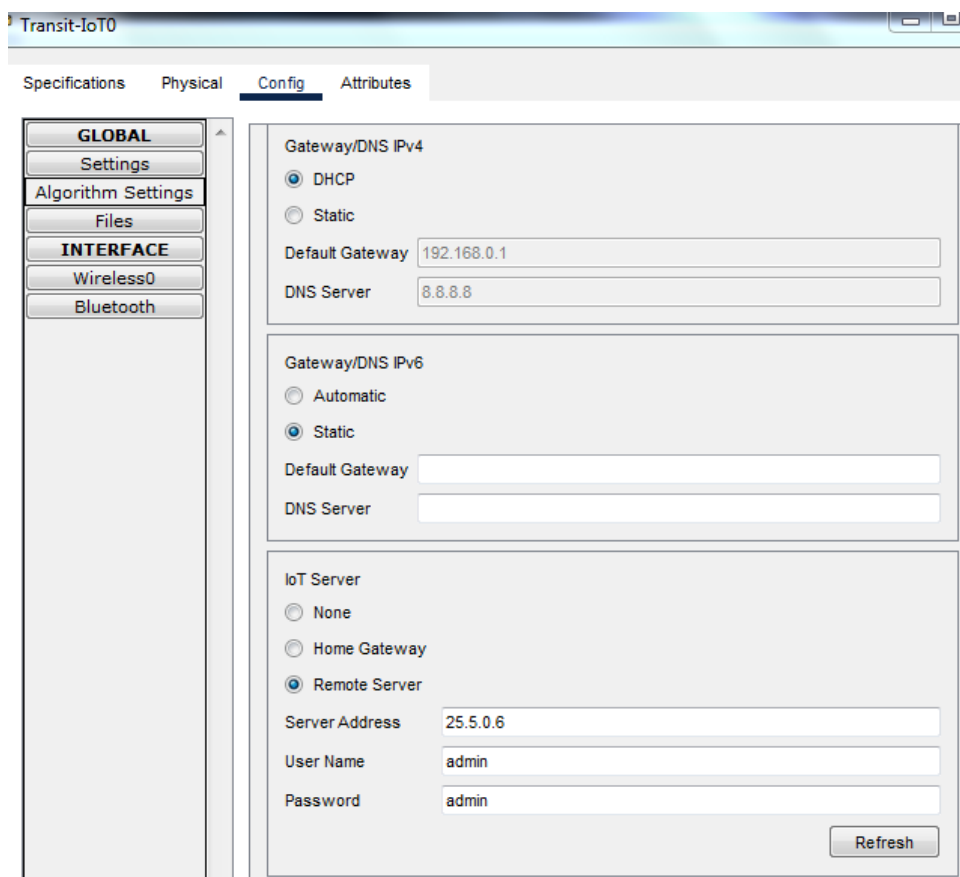


Рис. 3.37 – Налаштування адреси серверу IoT для камери Transit-IoT0

Аналогічне налаштування було проведено і для інших пристроїв IoT. Для перевірки правильності зроблених налаштувань проведемо кілька тестів. В цьому нам

допоможуть різноманітні діагностичні команди та візуальні відображення на кінцевих пристроях.

Організуємо перевірку на правильність розділу на віртуальні підмережі з мережних пристроїв організації. Зображення на рис. 3.38, показує, що дане розділення існує, за необхідності трафік можливо обмежити між віртуальними мережами за допомоги списків доступу.

VLAN	Name	Status	Ports
1	default	active	Gig1/0/6, Gig1/0/7, Gig1/0/8, Gig1/0/9 Gig1/0/10, Gig1/0/11, Gig1/0/12, Gig1/0/13 Gig1/0/14, Gig1/0/15, Gig1/0/16, Gig1/0/17 Gig1/0/18, Gig1/0/19, Gig1/0/20, Gig1/0/21 Gig1/0/22, Gig1/0/23, Gig1/0/24, Gig1/1/1 Gig1/1/2, Gig1/1/3, Gig1/1/4 Gig1/0/1, Gig1/0/2
8	FOR_HSRP	active	
101	Wi-Fi1	active	
102	LAN1-1	active	
103	LAN1-2	active	
201	Wi-Fi2	active	
202	LAN2-1	active	
203	LAN2-2	active	
255	AdminLAN	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
8	enet	100008	1500	-	-	-	-	-	0	0
101	enet	100101	1500	-	-	-	-	-	0	0
102	enet	100102	1500	-	-	-	-	-	0	0
103	enet	100103	1500	-	-	-	-	-	0	0
201	enet	100201	1500	-	-	-	-	-	0	0
202	enet	100202	1500	-	-	-	-	-	0	0
203	enet	100203	1500	-	-	-	-	-	0	0
255	enet	100255	1500	-	-	-	-	-	0	0

Рис. 3.38 – Результат команди show vlan на комутаторі SwitchMain

Тепер перевіримо налаштування DHCP-серверу за допомогою команд та одного із кінцевих пристроїв (рис. 3.39-3.40).

```
SwitchMain#show ip dhcp binding
IP address      Client-ID/      Lease expiration  Type
Hardware address
10.1.0.3        0060.7085.B901   --                Automatic
10.2.0.4        0060.4768.0B95   --                Automatic
10.2.0.3        0001.97A0.138B   --                Automatic
10.3.0.3        0001.42E3.8844   --                Automatic
10.3.0.4        0001.423C.E72D   --                Automatic
20.1.0.3        00D0.FF49.08E0   --                Automatic
20.2.0.3        0060.7041.98B9   --                Automatic
20.2.0.4        000A.F358.800C   --                Automatic
25.5.0.8        000D.BDA4.80C2   --                Automatic
25.5.0.7        0090.0CEE.139C   --                Automatic
20.3.0.4        0001.431B.87D6   --                Automatic
20.3.0.3        0040.0BC5.45E4   --                Automatic
SwitchMain#show ip dhcp pool

Pool Wi-Fi1 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next)    : 0 / 0
Total addresses              : 254
Leased addresses             : 1
Excluded addresses          : 8
Pending event                : none

1 subnet is currently in the pool
Current index  IP address range  Leased/Excluded/Total
10.1.0.1      10.1.0.1 - 10.1.0.254  1 / 8 / 254

Pool LAN1-1 :
Utilization mark (high/low) : 100 / 0
Subnet size (first/next)    : 0 / 0
Total addresses              : 254
Leased addresses             : 2
Excluded addresses          : 8
Pending event                : none

1 subnet is currently in the pool
```

Рис. 3.39 – Результат виконання діагностичних команд show ip dhcp binding та show ip dhcp pool на багаторівневому комутаторі SwitchMain

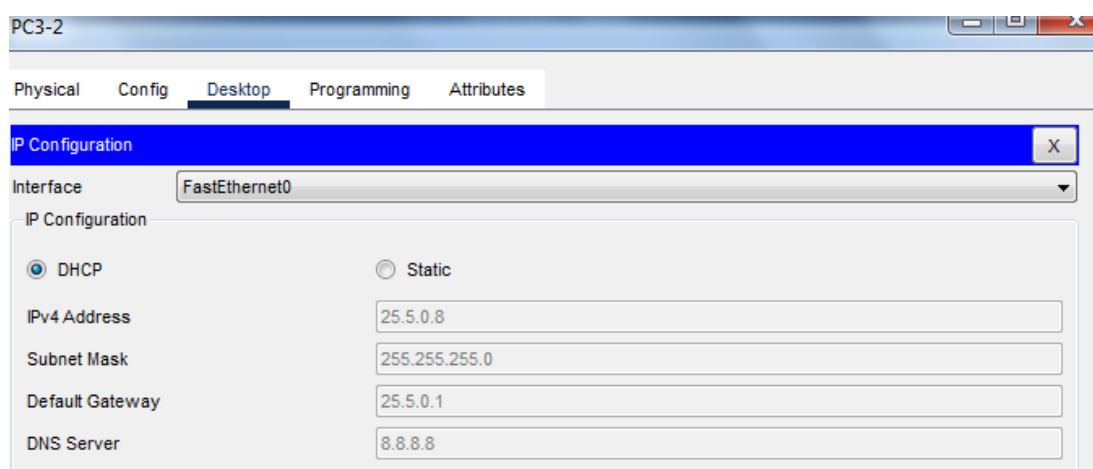


Рис. 3.40 – Результат виконання DHCP-запиту на робочій станції PC3-2

Глобальну мережу Інтернет змодельюємо за допомогою інтерфейса замикання на себе Loopback на маршрутизаторі RouterInternet. Адреса даного інтерфейсу була обрана як 172.16.0.1. Перевірка з'єднання виконана з локальної робочої станції (рис. 3.41).

```
C:\>ping 172.16.0.1

Pinging 172.16.0.1 with 32 bytes of data:

Reply from 172.16.0.1: bytes=32 time<1ms TTL=253
Reply from 172.16.0.1: bytes=32 time<1ms TTL=253
Reply from 172.16.0.1: bytes=32 time<1ms TTL=253
Reply from 172.16.0.1: bytes=32 time<1ms TTL=253

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рис. 3.41 – Результат тестування доступності мережі Інтернет на робочій станції PC3-2

Так само перевіримо доступність інших VLAN організації. Як видно на рис. 3.42, на команду *ping <адреса>* приходять відповідь з вказаною кількістю байт та часом затримки.

```
C:\>ping 20.2.0.4

Pinging 20.2.0.4 with 32 bytes of data:

Request timed out.
Reply from 20.2.0.4: bytes=32 time<1ms TTL=127
Reply from 20.2.0.4: bytes=32 time<1ms TTL=127
Reply from 20.2.0.4: bytes=32 time<1ms TTL=127

Ping statistics for 20.2.0.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 20.3.0.4

Pinging 20.3.0.4 with 32 bytes of data:

Request timed out.
Reply from 20.3.0.4: bytes=32 time<1ms TTL=127
Reply from 20.3.0.4: bytes=32 time<1ms TTL=127
Reply from 20.3.0.4: bytes=32 time<1ms TTL=127

Ping statistics for 20.3.0.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рис. 3.42 – Результат тестування доступності сусідніх будівель на робочій станції PC3-2

Перевіримо правильність роботи HSRP – виведемо діагностичні команди щодо HSRP на відповідних пристроях [41] (рис. 3.43-3.44).

```
RouterMain#sh standby
GigabitEthernet0/1 - Group 1
  State is Active
    6 state changes, last state change 00:00:27
  Virtual IP address is 3.3.3.6
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.301 secs
  Preemption disabled
  Active router is local
  Standby router is 3.3.3.2
  Priority 50 (configured 50)
    Track interface GigabitEthernet0/0 state Up decrement 10
  Group name is hsrp-Gig0/1-1 (default)
RouterMain#sh standby brief
      P indicates configured to preempt.
      |
Interface   Grp  Pri P State   Active           Standby           Virtual IP
Gig0/1      1    50  P Active  local           3.3.3.2           3.3.3.6
```

Рис. 3.43 – Результат виконання діагностичних команд show standby та show standby brief на маршрутизаторі RouterMain

```
RouterBackup#sh standby
GigabitEthernet0/1 - Group 1
  State is Standby
    11 state changes, last state change 00:00:00
  Virtual IP address is 3.3.3.6
  Active virtual MAC address is 0000.0C07.AC01
    Local virtual MAC address is 0000.0C07.AC01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.668 secs
  Preemption disabled
  Active router is 3.3.3.1
  Standby router is local
  Priority 45 (configured 45)
    Track interface GigabitEthernet0/0 state Up decrement 10
  Group name is hsrp-Gig0/1-1 (default)
RouterBackup#sh standby brief
      P indicates configured to preempt.
      |
Interface   Grp  Pri P State   Active           Standby           Virtual IP
Gig0/1      1    45  P Standby  3.3.3.1         local             3.3.3.6
```

Рис. 3.44 – Результат виконання діагностичних команд show standby та show standby brief на маршрутизаторі RouterBackup

Перейдемо до перевірки сервісів серверів. Першим перевіримо доступність HTTP/HTTPS (рис. 3.45).

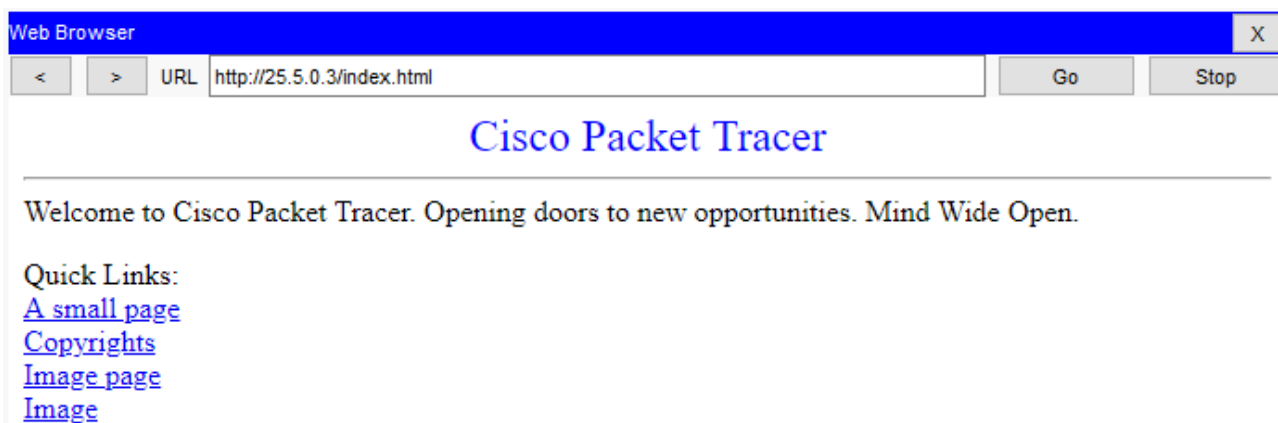


Рис. 3.45 – Результат тестування доступності HTTP-серверу на робочій станції
PC1-1

Тепер спробуємо скопіювати стартову конфігурацію пристрою на сервер, тим самим перевіривши TFTP (рис. 3.46-3.47).

```
RouterBackup#copy startup-config tftp
Address or name of remote host []? 25.5.0.3
Destination filename [RouterBackup-config]? routerBackup_config

Writing startup-config...!!
[OK - 1921 bytes]

1921 bytes copied in 0 secs
RouterBackup#
```

Рис. 3.46 – Копіювання стартової конфігурації маршрутизатора RouterBackup на
TFTP-сервер

```
—
ir800_yocto-1.7.2_python-2.7.3.tar
pt1000-i-mz.122-28.bin
pt3000-i6q4l2-mz.121-22.EA4.bin
routerBackup_config
```

Рис. 3.47 – Наявність скопійованого файлу стартової конфігурації
маршрутизатора RouterBackup на TFTP-сервері

Також на сервері перевіримо наявність повідомлень у журналі подій SYSLOG [42] (рис. 3.48).

Syslog

Service ☒ On ☐ 0

	Time	HostName	Message
1	06.02.2022 06:57:13.012 PM	3.3.3.1	18:57:13: %OSPF-5-...
2	06.02.2022 06:57:45.012 PM	1.1.1.1	18:57:45: %OSPF-5-...
3	06.02.2022 06:57:29.032 PM	25.5.0.1	18:57:29: %OSPF-5-...
4	06.02.2022 06:57:45.047 PM	3.3.3.2	18:57:45: %OSPF-5-...
5	06.02.2022 06:57:45.360 PM	3.3.3.2	%HSRP-6-STATECHANGE:...
6	06.02.2022 06:57:34.003 PM	25.5.0.1	18:57:34: %OSPF-5-...
7	06.02.2022 06:57:18.003 PM	3.3.3.1	18:57:18: %OSPF-5-...
8	06.02.2022 06:57:50.003 PM	3.3.3.2	18:57:50: %OSPF-5-...
9	06.02.2022 06:57:50.023 PM	1.1.1.1	18:57:50: %OSPF-5-...
10	06.02.2022 06:57:28.020 PM	3.3.3.1	18:57:28: %OSPF-5-...
11	06.02.2022 06:58:00.020 PM	3.3.3.2	18:58:00: %OSPF-5-...
12	06.02.2022 06:58:45.306 PM	3.3.3.1	%SYS-5-CONFIG_1: Configured from console b...
13	06.02.2022 06:58:45.306 PM	3.3.3.1	%SYS-5-CONFIG_1: Configured from console b...
			%SYS-5-CONFIG_1:

Рис. 3.48 – Наявність записів в журналі подій SYSLOG

Перевірка сервісу NTP за допомоги діагностичних команд [43]. (рис. 3.49-3.50).

```
SwitchMain#sh clock detail
*21:45:15.849 EET Thu Jul 30 2020
Time source is hardware calendar
SwitchMain#sh ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1990)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec.
loopfilter state is 'FSET' (Drift set from file), drift is - 0.000001193 s/s system poll interval is 4, never updated.
SwitchMain#sh ntp associations

address      ref clock    st  when    poll  reach  delay      offset    disp
~25.5.0.4    .INIT.      16   -       64    0      0.00      0.00     0.47
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

Рис. 3.49 – Результат виконання діагностичних команд show clock detail, show ntp status та show ntp associations на багаторівневому комутаторі SwitchMain

```

RouterMain#sh clock detail
21:52:28.638 EET Thu Jul 30 2020
Time source is NTP
RouterMain#sh ntp status
Clock is synchronized, stratum 2, reference is 25.5.0.4
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is 0C6DFF06.000000E9 (19:52:38.233 UTC Чт июл 30 2020)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 155.97 msec, peer dispersion is 0.12 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll interval is 4, last update was 2 sec ago.
RouterMain#sh ntp association

address      ref clock    st  when  poll  reach delay    offset    disp
*~25.5.0.4    127.127.1.1  1   2     16    377  1.00    0.00     0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

```

Рис. 3.50 – Результат виконання діагностичних команд show clock detail, show ntp status та show ntp associations на маршрутизаторі RouterMain

Наостанок переходимо до перевірки VPN з'єднання з віддаленою мережею транспортного засобу. Його перевірять за допомогою робочих станцій PC3-1 та PC2-4, використовуючи команди **show crypto isakmp sa** та **show crypto ipsec sa**.

Спершу відправимо пакет даних з робочої станції PC2-4 (рис. 3.51)

```

Pinging 192.168.4.1 with 32 bytes of data:

Reply from 192.168.4.1: bytes=32 time<1ms TTL=252
Reply from 192.168.4.1: bytes=32 time<1ms TTL=252
Reply from 192.168.4.1: bytes=32 time<1ms TTL=252
Reply from 192.168.4.1: bytes=32 time=1ms TTL=252

Ping statistics for 192.168.4.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

Рис. 3.51 – Перевірка з'єднання з локальним інтерфейсом маршрутизатора RouterRemote1

Тепер перевіримо, чи відбулось шифрування даних за допомогою вищенаведених команд (рис. 3.52).

```

*Jun 02, 17:07:37.077: SYS-5-CONFIG_I: Configured from console by console
RouterMain#
RouterMain#
RouterMain#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status

IPv6 Crypto ISAKMP SA

RouterMain#show crypto ipsec sa

interface: GigabitEthernet0/0
  Crypto map tag: IPSEC-MAP, local addr 1.1.1.2

protected vrf: (none)
local  ident (addr/mask/prot/port): (25.5.0.0/255.255.255.248/0/0)
remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
current_peer 4.4.4.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 1.1.1.2, remote crypto endpt.: 4.4.4.2
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0x0(0)

inbound esp sas:

inbound ah sas:

inbound pcsp sas:

outbound esp sas:

outbound ah sas:

outbound pcsp sas:

```

Рис. 3.52 – Перевірка шифрування пакетів VPN-тунелю на маршрутизаторі RouterMain

Як бачимо, жоден відправлений пакет даних не був зашифрований, оскільки робоча станція PC2-4 знаходиться в мережі, яка не була додана до списків доступу шифрування трафіку.

Давайте спробуємо надіслати запит з робочої станції PC3-2 (рис. 3.53-3.54)

```
C:\>ping 192.168.4.1

Pinging 192.168.4.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.4.1: bytes=32 time<1ms TTL=253
Request timed out.
Reply from 192.168.4.1: bytes=32 time<1ms TTL=253

Ping statistics for 192.168.4.1:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рис. 3.53 – Перевірка зв'язку з локальним інтерфейсом RouterRemote

```
RouterMain#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
4.4.4.2      1.1.1.2      QM_IDLE       1096      0 ACTIVE

IPv6 Crypto ISAKMP SA

RouterMain#show crypto ipsec sa

interface: GigabitEthernet0/0
  Crypto map tag: IPSEC-MAP, local addr 1.1.1.2

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (25.5.0.0/255.255.255.248/0/0)
  remote ident (addr/mask/prot/port): (192.168.4.0/255.255.255.0/0/0)
  current_peer 4.4.4.2 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
    #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

    local crypto endpt.: 1.1.1.2, remote crypto endpt.: 4.4.4.2
    path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0x49E6B17A(1239855482)
```

Рис. 3.54 – Повторна перевірка шифрування трафіку на маршрутизаторі RouterMain

Тепер трафік був зашифрований, так як вищевказана робоча станція знаходиться в мережі, яка була додана до списків доступу VPN-тунелю. Таким чином можливо контролювати шифрування важливого та конфіденційного трафіку, який надходить до серверів організації, та пропускати увесь інший. Наприклад, дані що надходить з камери спостереження на сервер IoT будуть попередньо зашифровані.

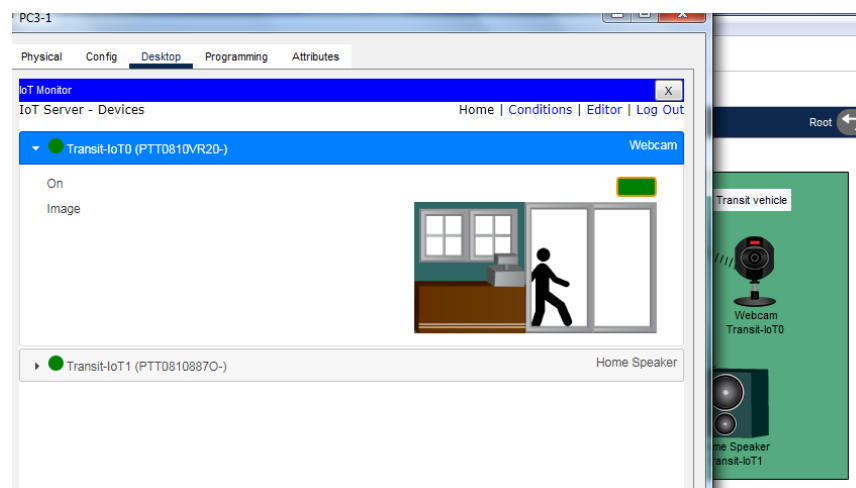


Рис. 3.55 – Перевірка роботи камери спостереження Transit-IoT0

3.3. Рекомендації по застосуванню та вдосконаленню розробленої системи захищеного обміну даними з рухомим транспортом

Розроблена система та подібні аналоги необхідно впроваджувати у великих мережах транспортних організацій, наприклад КП «Дніпровський транспорт» вже має позитивний досвід від використання подібної системи.

Дана система має низку переваг, які направлені на збільшення захисту даних що передаються між транспортним засобом та офісом організації:

- Надійний захист даних користувачів громадського транспорту, що унеможливорює викрадення приватної інформації зловмисниками.
- Надійний канал передачі інформації про місце перебування транспортного засобу, стан сенсорів, контроль використання пального та багато іншого.

Розроблена система може бути легко підлаштована під вимоги замовника та застосована у будь-якій транспортній організації. Можливі модифікації системи:

- Збільшення кількості обладнання IoT на рухомому складі, що дозволяє автоматизувати збір та аналітику інформації;
- Уніфікувати мережеві підключення транспорту до серверів організації: один маршрутизатор – одна SIM-картка;

- Використання більш сучасних протоколів шифрування у разі необхідності.

Висновки по 3 розділу

В даному розділі наведена перевірка працездатності розробленої системи захищеного обміну даними. Розроблено модель системи захищеного обміну даними з рухомим транспортом в Cisco Packet Tracer, описано приклад налаштування. Проведено дослідження розробленого макету системи та оцінено її працездатність, а саме – перевірено наявність обміну даними в мережі, перевірено функціонування необхідних протоколів та перевірено особливості захисту трафіку VPN-каналу обміну даними з рухомим транспортом.

Розроблено рекомендації щодо застосування проаналізованої системи захищеного обміну даними.

ВИСНОВКИ

В процесі виконання кваліфікаційної роботи був розроблений проект системи захищеного обміну даними з рухомим транспортом.

Дослідження аналогічних проектів даної сфери показало наявність попиту та великого потенціалу у розвитку даного напрямку комунікацій.

Було проаналізовано еталонну архітектуру Інтернету речей, досліджено архітектуру шаблонів конструювання мереж, зіставлено хибні та правильні типи. Було обрано організувати мережу підприємства за кампусним типом як найбільш актуальним з використанням оптимальних витрат.

Проведені та обрані необхідні засоби для реалізації системи: виробника обладнання, конкретні моделі обладнання, методи та технології розподілу IP-адрес, оцінено переваги та недоліки протоколів VPN, методи захисту обладнання від зовнішнього зловмисного впливу, симулятор роботи з мережним обладнанням;

Проаналізовано процеси роботи мережі та наведено прикладі з її створення. Розглянуто реалізацію основних функцій необхідних для системи: віртуальні приватні мережі, InterVLANrouting, VPN-тунелювання, встановлення паролів на мережне обладнання.

Налаштовано, оцінено та проаналізовано всю топологію мережі за допомогою Cisco Packet Tracer.

Система представлена як тестовий додадок, але може бути удосконалена, модифікована додатковими функціями у процесі потенційного розгортання та використана для майбутніх досліджень у сфері захисту обміну даними з транспортом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «Актуальность обеспечения информационной безопасности в сетях IoT» [Електронний ресурс] – Режим доступу до ресурсу: <https://cyberleninka.ru/article/n/aktualnost-obespecheniya-informatsionnoy-bezopasnosti-v-setyah-iot>
2. IoT у транспорті: цифрові «двійники» трамваїв, інтернет у метро та оплата особою [Електронний ресурс] – Режим доступу до ресурсу: <https://hightech.fm/2020/07/15/iot-transport-russia>
3. «Информационная безопасность в логистике и на транспорте» [Електронний ресурс] – Режим доступу до ресурсу: <https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C%D0%B2%D0%BB%D0%BE%D0%B3%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B5%D0%B8%D0%BD%D0%B0%D1%82%D1%80%D0%B0%D0%BD%D1%81%D0%BF%D0%BE%D1%80%D1%82%D0%B5>
4. Телекомунікаційні та інформаційні мережі : Підручник [для вищих навчальних закладів] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко. – К.: САММІТ-Книга, 2010. – 708 с.: іл
5. Кампусна мережа [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Campus_Area_Network
6. «Информационная безопасность предприятий транспорта решения Cisco Systems» [Електронний ресурс] – Режим доступу до ресурсу: <https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-predpriyatiy-transporta-resheniya-cisco-systems>
7. МОДЕЛЬ АРХИТЕКТУРЫ РАСПРЕДЕЛЕННОЙ СИСТЕМЫ IoT [Електронний ресурс] – Режим доступу до ресурсу:

- https://openarchive.nure.ua/bitstream/document/9236/1/Dudka_AA_291-292.pdf
8. ITU-T Y.2060 SERIES Y: Provides an overview of the Internet of things (IoT) (06/2012)
 9. «Что нужно знать об Интернете вещей: фундаментальный ликбез» [Электронный ресурс] – Режим доступа до ресурсу: <https://habr.com/ru/company/toshibarus/blog/473024/>
 10. An IoT Edge-as-a-service (EaaS) Distributed Architecture & Reference Implementation [Электронный ресурс] – Режим доступа до ресурсу: https://www.researchgate.net/figure/Illustration-of-the-IoT-Reference-Model-by-Cisco-1_fig1_336564357
 11. «Шаблоны проектирования для повышения безопасности в промышленных сетях» [Электронный ресурс] – Режим доступа до ресурсу: <https://www.proxis.ua/ru/show-article/206/>
 12. IEEE 802.1X [Электронный ресурс] – Режим доступа до ресурсу: https://uk.wikipedia.org/wiki/IEEE_802.1X
 13. RADIUS [Электронный ресурс] – Режим доступа до ресурсу: <https://uk.wikipedia.org/wiki/RADIUS>
 14. VLAN [Электронный ресурс] – Режим доступа до ресурсу: <https://uk.wikipedia.org/wiki/VLAN>
 15. Cisco ASR9000 [Электронный ресурс] – Режим доступа до ресурсу: <https://www.cisco-parts.ru/catalog-cisco/cisco-for-providers-network-core/cisco-asr-9000/>
 16. Cisco ISR800 [Электронный ресурс] – Режим доступа до ресурсу: <https://www.cisco-parts.ru/catalog-cisco/routers-for-small-business/cisco-isr-800/>
 17. Cisco Catalyst 6800 [Электронный ресурс] – Режим доступа до ресурсу: <https://www.cisco-parts.ru/catalog-cisco/cisco-campus-lan-switches-core-distribution/cisco-catalyst-6800/>

18. Cisco Catalyst 4500E [Електронний ресурс] – Режим доступу до ресурсу:
<https://altastor.ru/products/commutation/cisco/catalyst/4500e/>
19. Cisco Catalyst 3850 [Електронний ресурс] – Режим доступу до ресурсу:
<https://www.cisco-parts.ru/catalog-cisco/cisco-campus-lan-switches-access/cisco-catalyst-3850/>
20. Cisco Catalyst 3650 [Електронний ресурс] – Режим доступу до ресурсу:
<https://www.cisco-parts.ru/catalog-cisco/cisco-campus-lan-switches-access/cisco-catalyst-3650/>
21. Cisco Catalyst 2960-X [Електронний ресурс] – Режим доступу до ресурсу:
<https://www.cisco-parts.ru/catalog-cisco/cisco-campus-lan-switches-access/cisco-catalyst-2960-x/>
22. Маршрутизатор Cisco 2911/K9 [Електронний ресурс] – Режим доступу до ресурсу: <https://stack-systems.com.ua/marshrutizator-cisco-2911-k9>
23. Cisco Catalyst 3650 [Електронний ресурс] – Режим доступу до ресурсу:
<https://lantorg.com/products/kommutator-cisco-catalyst-3650-24ts-sws-c3650-24ts-s#:~:text=%D0%9A%D0%BE%D0%BC%D0%BC%D1%83%D1%82%D0%B0%D1%82%D0%BE%D1%80%D1%8B%20Cisco%20Catalyst%203650%20%D1%81%D0%B5%D1%80%D0%B8%D0%B8,%D0%BC%D0%BE%D0%B4%D1%83%D0%BB%D1%8C%D0%BD%D0%BE%D0%B9%20%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B%20IOS%20XE>
24. Cisco-Linksys WRT300N Wireless-N Broadband Router [Електронний ресурс] – Режим доступу до ресурсу: <https://www.amazon.com/Cisco-Linksys-WRT300N-Wireless-N-Broadband-Router/dp/B000FDOWQK>
25. Новые возможности Wi-Fi. App Hosting, User Defined Network (UDN) [Електронний ресурс] – Режим доступу до ресурсу:
https://www.cisco.com/c/dam/m/ru_ua/training-events/2021/cisco-tech-talks/pdf/user-defined-network-application.pdf

26. КОММУТАТОРЫ CISCO CATALYST 2960 СЕРИИ [Электронный ресурс] – Режим доступа до ресурсу: https://www.karma-group.ru/catalog/cisco_switches/cisco_catalyst_2960_series_switches/
27. PPTP [Электронный ресурс] – Режим доступа до ресурсу: <https://uk.wikipedia.org/wiki/PPTP>
28. L2TP [Электронный ресурс] – Режим доступа до ресурсу: <https://uk.wikipedia.org/wiki/L2TP>
29. OpenVPN [Электронный ресурс] – Режим доступа до ресурсу: <https://ru.vpnmentor.com/blog/%D1%81%D1%80%D0%B0%D0%B2%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BF%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB%D0%BE%D0%B2-vpn-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/>
30. SSTP [Электронный ресурс] – Режим доступа до ресурсу: <https://en.wikipedia.org/wiki/SSTP>
31. IKEv2 [Электронный ресурс] – Режим доступа до ресурсу: https://en.wikipedia.org/wiki/Internet_Key_Exchange
32. Cisco Enterprise Campus Infrastructure. Best Practices Guide // Cisco Systems, Inc. – 2014. – С. 45.
33. Амато В. Основы организации сетей Cisco / Вито Амато., 2004. – 464 с. – ("Вильямс").
34. DHCP [Электронный ресурс] – Режим доступа до ресурсу: <https://uk.wikipedia.org/wiki/DHCP>
35. Configure InterVLAN Routing on Layer 3 Switches [Электронный ресурс] – Режим доступа до ресурсу: <https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html>
36. HSRP [Электронный ресурс] – Режим доступа до ресурсу: <https://ru.wikipedia.org/wiki/HSRP>
37. HTTP [Электронный ресурс]– Режим доступа до ресурсу: <https://uk.wikipedia.org/wiki/HTTP>

38. NTP [Електронний ресурс] – Режим доступу до ресурсу:
<https://uk.wikipedia.org/wiki/NTP>
39. TFTP [Електронний ресурс] – Режим доступу до ресурсу:
<https://uk.wikipedia.org/wiki/TFTP>
40. SSH [Електронний ресурс] – Режим доступу до ресурсу:
<https://uk.wikipedia.org/wiki/SSH>
41. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛУ ДИНАМІЧНОГО РЕЗЕРВУВАННЯ ШЛЮЗУ HSRP У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO [Електронний ресурс] – Режим доступу до ресурсу:
https://learn.ztu.edu.ua/pluginfile.php/69819/mod_resource/content/1/KM_KI_KB_LR-30-2019-2020_KI-3_KB-2-1_KB-2-2_KBK-19-1.pdf
42. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПІДСИСТЕМИ ЖУРНАЛЮВАННЯ ПОДІЙ SYSLOG У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO [Електронний ресурс] – Режим доступу до ресурсу:
https://learn.ztu.edu.ua/pluginfile.php/94656/mod_resource/content/1/KM_KI_KB_LR-34-2019-2020_KI-3_KB-2-1_KB-2-2_KBK-19-1.pdf
43. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛУ МЕРЕЖНОГО ЧАСУ NTP У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO [Електронний ресурс] – Режим доступу до ресурсу:
https://learn.ztu.edu.ua/pluginfile.php/94655/mod_resource/content/1/KM_KI_KB_LR-33-2019-2020_KI-3_KB-2-1_KB-2-2_KBK-19-1.pdf

ДОДАТКИ

					Державний університет «Житомирська політехніка».22.125.04.000 – ПЗ	
						89

Топологія мережі

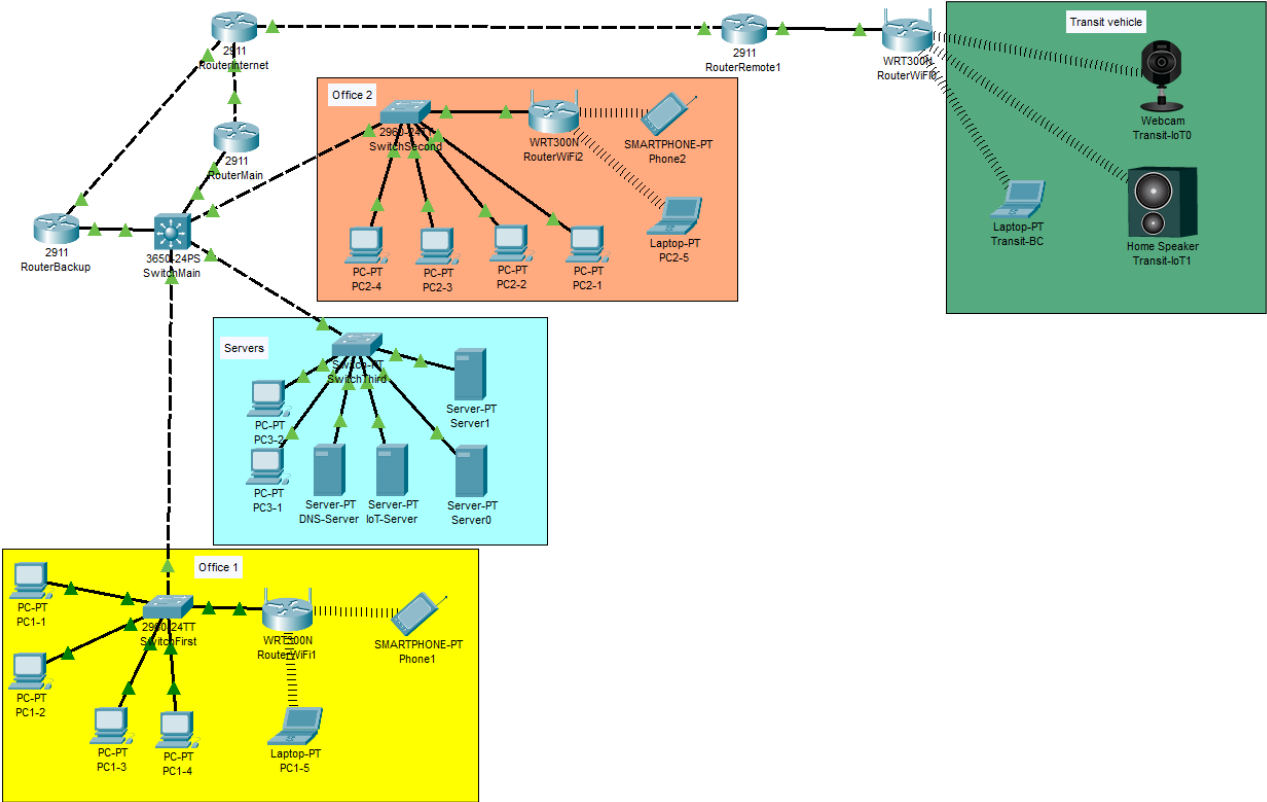


Рис. А.1 – Топологія мережі

Лістинги конфігураційних файлів граничного маршрутизуючого обладнання

```

RouterInternet#show run
Building configuration...

Current configuration : 2125 bytes
!
version 15.1
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname RouterInternet
!
logging userinfo
login block-for 10 attempts 3 within 3
login on-failure log
login on-success log
!
!
enable secret 5 $1$mERr$VOZFZ/5R0sAyeHvev4Sch1
!
!
!
clock timezone EET 2
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username adminer privilege 15 secret 5
$1$mERr$sy5570Y8chTcnA2SwGenM.
username technic secret 5 $1$mERr$N.AgdQZ1YY5E8rDIvsV1L1
!
!
license udi pid CISCO2911/K9 sn FTX15244I35-
!
!
!
!
!
!
!
!
ip ssh version 2
ip ssh authentication-retries 5

```

```

ip ssh time-out 60
ip domain-name internet.com
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Loopback1
 ip address 172.16.0.1 255.255.255.252
!
interface GigabitEthernet0/0
 ip address 1.1.1.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 2.2.2.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 4.4.4.1 255.255.255.252
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 100
 log-adjacency-changes
 redistribute static
 passive-interface Loopback1
 network 1.1.1.0 0.0.0.3 area 0
 network 4.4.4.0 0.0.0.3 area 0
 network 2.2.2.0 0.0.0.3 area 0
 network 172.16.0.0 0.0.0.3 area 0
!
ip classless
ip route 25.5.0.0 255.255.255.0 1.1.1.2
ip route 25.5.0.0 255.255.255.0 2.2.2.2 2
ip route 0.0.0.0 0.0.0.0 Loopback1
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
 deny tcp any any eq telnet
 deny tcp any any eq www

```

```

deny tcp any any eq 22
permit tcp any any eq 22
!
banner motd ^C Connection to router RouterInternet For legal users
only ^C
!
!
!
!
!
logging trap debugging
logging 25.5.0.4
line con 0
logging synchronous
login local
!
line aux 0
!
line vty 0 4
logging synchronous
login local
transport input ssh
transport output ssh
!
!
ntp authentication-key 1 md5 08314D5D1A0E0A0516 7
ntp authenticate
ntp trusted-key 1
ntp server 25.5.0.4 key 1
!
end

```

```

RouterMain#show run
Building configuration...

Current configuration : 2506 bytes
!
version 15.1
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname RouterMain
!
logging userinfo
login block-for 10 attempts 3 within 3
login on-failure log
login on-success log
!
!
enable secret 5 $1$mERr$VOZFZ/5R0sAyeHvev4ScH1
!
!
!
clock timezone EET 2
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username adminer privilege 15 secret 5
$1$mERr$sy5570Y8chTcnA2SwGenM.
username technic secret 5 $1$mERr$N.AgdQZ1YY5E8rDIvsV1L1
!
!
license udi pid CISC02911/K9 sn FTX152490IZ-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 5
!
crypto isakmp key secretkey address 4.4.4.2
!
!
!
crypto ipsec transform-set vpna esp-aes 256 esp-sha-hmac
!

```

```

crypto map IPSEC-MAP 10 ipsec-isakmp
  set peer 4.4.4.2
  set pfs group5
  set security-association lifetime seconds 86400
  set transform-set vpna
  match address 100
!
!
!
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
ip domain-name RouterMain.main
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
  ip address 1.1.1.2 255.255.255.252
  duplex auto
  speed auto
  crypto map IPSEC-MAP
!
interface GigabitEthernet0/1
  ip address 3.3.3.1 255.255.255.248
  duplex auto
  speed auto
  standby 1 ip 3.3.3.6
  standby 1 priority 50
  standby 1 track GigabitEthernet0/0
  standby 0 timers 5 10
!
interface GigabitEthernet0/2
  no ip address
  duplex auto
  speed auto
  shutdown
!
interface GigabitEthernet0/0/0
  no ip address
  shutdown
!
interface Vlan1
  no ip address
  shutdown
!
!

```

```

router ospf 100
  log-adjacency-changes
  network 1.1.1.0 0.0.0.3 area 0
  network 3.3.3.0 0.0.0.7 area 0
!
ip classless
ip route 25.5.0.0 255.255.255.0 3.3.3.3
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
  deny tcp any any eq telnet
  deny tcp any any eq www
  deny tcp any any eq 22
  permit tcp any any eq 22
access-list 100 permit ip 25.5.0.0 0.0.0.7 192.168.4.0 0.0.0.255
!
no cdp run
!
banner motd ^C Connection to router RouterMain For legal users
only ^C
!
!
!
!
!
logging trap debugging
logging 25.5.0.4
line con 0
  logging synchronous
  login local
!
line aux 0
!
line vty 0 4
  logging synchronous
  login local
  transport input ssh
  transport output ssh
!
!
ntp authentication-key 1 md5 08314D5D1A0E0A0516 7
ntp authenticate
ntp trusted-key 1
ntp server 25.5.0.4 key 1
ntp update-calendar
!
end

```

```

RouterBackup#show run
Building configuration...

Current configuration : 2473 bytes
!
version 15.1
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname RouterBackup
!
logging userinfo
login block-for 10 attempts 3 within 3
login on-failure log
login on-success log
!
!
enable secret 5 $1$mERr$VOZFZ/5R0sAyeHvev4ScH1
!
!
!
clock timezone EET 2
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username adminer privilege 15 secret 5
$1$mERr$sy5570Y8chTcnA2SwGenM.
username technic secret 5 $1$mERr$N.AgdQZ1YY5E8rDIvsV1L1
!
!
license udi pid CISC02911/K9 sn FTX1524WE52-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 5
!
crypto isakmp key secretkey address 4.4.4.2
!
!
!
crypto ipsec transform-set vpna esp-aes 256 esp-sha-hmac
!

```

```

crypto map IPSEC-MAP 10 ipsec-isakmp
  set peer 4.4.4.2
  set pfs group5
  set security-association lifetime seconds 86400
  set transform-set vpna
  match address 100
!
!
!
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
ip domain-name RouterBackup.backup
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
  ip address 2.2.2.2 255.255.255.252
  duplex auto
  speed auto
  crypto map IPSEC-MAP
!
interface GigabitEthernet0/1
  ip address 3.3.3.2 255.255.255.248
  duplex auto
  speed auto
  standby 1 ip 3.3.3.6
  standby 1 priority 45
  standby 1 track GigabitEthernet0/0
  standby 0 timers 5 10
!
interface GigabitEthernet0/2
  no ip address
  duplex auto
  speed auto
  shutdown
!
interface GigabitEthernet0/1/0
  no ip address
  shutdown
!
interface Vlan1
  no ip address
  shutdown
!
router ospf 1

```

```

log-adjacency-changes
network 2.2.2.0 0.0.0.3 area 0
network 3.3.3.0 0.0.0.7 area 0
!
ip classless
ip route 25.5.0.0 255.255.255.0 3.3.3.3
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
access-list 100 permit ip 3.3.3.0 0.0.0.7 192.168.4.0 0.0.0.255
access-list 100 permit ip 25.5.0.0 0.0.0.7 192.168.4.0 0.0.0.255
!
no cdp run
!
banner motd ^C Connection to router RouterBackup For legal users
only ^C
!
!
!
!
!
logging trap debugging
logging 25.5.0.4
line con 0
logging synchronous
login local
!
line aux 0
!
line vty 0 4
logging synchronous
login local
transport input ssh
transport output ssh
!
!
ntp authentication-key 1 md5 08314D5D1A0E0A0516 7
ntp authenticate
ntp trusted-key 1
ntp server 25.5.0.4 key 1
ntp update-calendar
!
end

```

```

RouterRemotel#show run
Building configuration...

Current configuration : 1403 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname RouterRemotel
!
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
!
license udi pid CISCO2911/K9 sn FTX152409NE-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 5
!
crypto isakmp key secretkey address 1.1.1.2
!
!
!
crypto ipsec transform-set vpna esp-aes 256 esp-sha-hmac
!
crypto map IPSEC-MAP 10 ipsec-isakmp
  set peer 1.1.1.2
  set peer 2.2.2.2
  set pfs group5
  set security-association lifetime seconds 86400
  set transform-set vpna
  match address 100
!
!
!
!
!

```

```

!
spanning-tree mode pvst
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 4.4.4.2 255.255.255.252
 duplex auto
 speed auto
 crypto map IPSEC-MAP
!
interface GigabitEthernet0/1
 ip address 192.168.4.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 100
 log-adjacency-changes
 network 4.4.4.0 0.0.0.3 area 0
 network 192.168.4.0 0.0.0.255 area 0
!
ip classless
!
ip flow-export version 9
!
!
access-list 100 permit ip 192.168.4.0 0.0.0.255 3.3.3.0 0.0.0.7
access-list 100 permit ip 192.168.4.0 0.0.0.255 25.5.0.0 0.0.0.7
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 login

```

!
!
!
end

Лістинг конфігураційних файлів комутаторів внутрішньої локальної мережі організації

```
SwitchMain#sh run
```

```
Building configuration...
```

```
Current configuration : 4766 bytes
```

```
!
```

```
version 16.3.2
```

```
service timestamps log datetime msec
```

```
service timestamps debug datetime msec
```

```
no service password-encryption
```

```
!
```

```
hostname SwitchMain
```

```
!
```

```
logging userinfo
```

```
login block-for 10 attempts 3 within 3
```

```
login on-failure log
```

```
login on-success log
```

```
!
```

```
enable secret 5 $1$mERr$VOZFZ/5R0sAyeHvev4Sch1
```

```
!
```

```
!
```

```
ip dhcp excluded-address 10.1.0.1 10.1.0.2
```

```
ip dhcp excluded-address 10.2.0.1 10.2.0.2
```

```
ip dhcp excluded-address 10.3.0.1 10.3.0.2
```

```
ip dhcp excluded-address 20.1.0.1 20.1.0.2
```

```
ip dhcp excluded-address 20.2.0.1 20.2.0.2
```

```
ip dhcp excluded-address 25.5.0.1 25.5.0.4
```

```
ip dhcp excluded-address 20.3.0.1 20.3.0.2
```

```
ip dhcp excluded-address 25.5.0.1 25.5.0.6
```

```
!
```

```
ip dhcp pool Wi-Fi1
```

```
network 10.1.0.0 255.255.255.0
```

```
default-router 10.1.0.1
```

```
dns-server 8.8.8.8
```

```
domain-name wifil.com
```

```
ip dhcp pool LAN1-1
```

```
network 10.2.0.0 255.255.255.0
```

```
default-router 10.2.0.1
```

```
dns-server 8.8.8.8
```

```
domain-name lan1-1.com
```

```
ip dhcp pool LAN1-2
```

```
network 10.3.0.0 255.255.255.0
```

```
default-router 10.3.0.1
```

```
dns-server 8.8.8.8
```

```
domain-name lan1-2.com
```

```
ip dhcp pool Wi-Fi2
```

```
network 20.1.0.0 255.255.255.0
```

```
default-router 20.1.0.1
```

```
dns-server 8.8.8.8
```

```
domain-name wifi2.com
```

```

ip dhcp pool LAN2-1
  network 20.2.0.0 255.255.255.0
  default-router 20.2.0.1
  dns-server 8.8.8.8
  domain-name lan2-1.com
ip dhcp pool AdminLAN
  network 25.5.0.0 255.255.255.0
  default-router 25.5.0.1
  dns-server 8.8.8.8
  domain-name adminlan.com
ip dhcp pool LAN2-2
  network 20.3.0.0 255.255.255.0
  default-router 20.3.0.1
  dns-server 8.8.8.8
  domain-name lan2-2.com
clock timezone EET 2
!
!
!
!
no ip cef
ip routing
!
no ipv6 cef
!
!
!
username adminer privilege 15 secret 5
$1$mERr$sy5570Y8chTcnA2SwGenM.
username technic secret 5 $1$mERr$N.AgdQZ1YY5E8rDIvsV1L1
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
ip domain-name SwitchMain.main
!
!
spanning-tree mode pvst
!
!
!
!
!
!
!
!
!
!

```

```

interface GigabitEthernet1/0/1
  switchport access vlan 8
  switchport mode access
  switchport nonegotiate
!
interface GigabitEthernet1/0/2
  switchport access vlan 8
  switchport mode access
  switchport nonegotiate
!
interface GigabitEthernet1/0/3
  switchport mode trunk
!
interface GigabitEthernet1/0/4
  switchport mode trunk
!
interface GigabitEthernet1/0/5
  switchport mode trunk
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!

```

```

interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/1/1
!
interface GigabitEthernet1/1/2
!
interface GigabitEthernet1/1/3
!
interface GigabitEthernet1/1/4
!
interface Vlan1
 ip address 100.0.0.1 255.255.255.0
!
interface Vlan8
 mac-address 0010.11c0.c801
 ip address 3.3.3.3 255.255.255.248
!
interface Vlan101
 mac-address 0010.11c0.c802
 ip address 10.1.0.1 255.255.255.0
!
interface Vlan102
 mac-address 0010.11c0.c803
 ip address 10.2.0.1 255.255.255.0
!
interface Vlan103
 mac-address 0010.11c0.c804
 ip address 10.3.0.1 255.255.255.0
!
interface Vlan201
 mac-address 0010.11c0.c805
 ip address 20.1.0.1 255.255.255.0
!
interface Vlan202
 mac-address 0010.11c0.c806
 ip address 20.2.0.1 255.255.255.0
!
interface Vlan203
 mac-address 0010.11c0.c807
 ip address 20.3.0.1 255.255.255.0
!
interface Vlan255
 mac-address 0010.11c0.c808
 ip address 25.5.0.1 255.255.255.0
!
router ospf 1
 router-id 3.3.3.3
 log-adjacency-changes
 network 3.3.3.0 0.0.0.7 area 0
 network 10.1.0.0 0.0.0.255 area 0
 network 10.2.0.0 0.0.0.255 area 0

```

```

network 10.3.0.0 0.0.0.255 area 0
network 20.1.0.0 0.0.0.255 area 0
network 20.2.0.0 0.0.0.255 area 0
network 20.3.0.0 0.0.0.255 area 0
network 25.5.0.0 0.0.0.255 area 0
!
ip classless
ip route 25.5.0.0 255.255.255.0 25.5.0.2
ip route 0.0.0.0 0.0.0.0 3.3.3.1
ip route 0.0.0.0 0.0.0.0 3.3.3.2 2
!
ip flow-export version 9
!
!
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
!
banner motd ^C Connection to switch SwitchMain For legal users
only ^C
!
!
!
!
!
logging trap debugging
logging 25.5.0.4
line con 0
logging synchronous
login local
!
line aux 0
!
line vty 0 4
logging synchronous
login local
transport input ssh
transport output ssh
!
!
!
ntp authentication-key 1 md5 08314D5D1A0E0A0516 7
ntp authenticate
ntp trusted-key 1
ntp server 25.5.0.4 key 1
ntp update-calendar
!
end

```

```

SwitchFirst#sh run
Building configuration...

Current configuration : 3173 bytes
!
version 12.2
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname SwitchFirst
!
enable secret 5 $1$mERr$VOZFZ/5R0sAyeHvev4ScH1
!
!
!
clock timezone EET 2
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
ip domain-name SwitchFirst.first
!
username adminer secret 5 $1$mERr$sy5570Y8chTcnA2SwGenM.
username technic secret 5 $1$mERr$N.AgdQZ1YY5E8rDIvsV1L1
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
    switchport access vlan 102
    switchport mode access
!
interface FastEthernet0/2
    switchport access vlan 102
    switchport mode access
!
interface FastEthernet0/3
    switchport access vlan 102
    switchport mode access
!
interface FastEthernet0/4
    switchport access vlan 102
    switchport mode access
!
interface FastEthernet0/5
    switchport access vlan 102
    switchport mode access
!
interface FastEthernet0/6
    switchport access vlan 102

```

```

switchport mode access
!
interface FastEthernet0/7
switchport access vlan 102
switchport mode access
!
interface FastEthernet0/8
switchport access vlan 102
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 102
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 102
switchport mode access
!
interface FastEthernet0/11
switchport access vlan 102
switchport mode access
!
interface FastEthernet0/12
switchport access vlan 102
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 103
switchport mode access
!
interface FastEthernet0/14
switchport access vlan 103
switchport mode access
!
interface FastEthernet0/15
switchport access vlan 103
switchport mode access
!
interface FastEthernet0/16
switchport access vlan 103
switchport mode access
!
interface FastEthernet0/17
switchport access vlan 103
switchport mode access
!
interface FastEthernet0/18
switchport access vlan 103
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 103
switchport mode access

```

```

!
interface FastEthernet0/20
  switchport access vlan 103
  switchport mode access
!
interface FastEthernet0/21
  switchport access vlan 103
  switchport mode access
!
interface FastEthernet0/22
  switchport access vlan 103
  switchport mode access
!
interface FastEthernet0/23
  switchport access vlan 103
  switchport mode access
!
interface FastEthernet0/24
  switchport access vlan 103
  switchport mode access
!
interface GigabitEthernet0/1
  switchport mode trunk
!
interface GigabitEthernet0/2
  switchport access vlan 101
  switchport mode access
!
interface Vlan1
  ip address 100.0.0.2 255.255.255.0
!
interface Vlan101
  ip address 10.1.0.2 255.255.255.0
!
interface Vlan102
  ip address 10.2.0.2 255.255.255.0
!
interface Vlan103
  ip address 10.3.0.2 255.255.255.0
!
ip default-gateway 100.0.0.1
!
banner motd ^C Connection to switch SwitchFirst For legal users
only ^C
logging trap debugging
logging 25.5.0.4
!
!
!
line con 0
  logging synchronous
  login local
!

```

```

line vty 0 4
  logging synchronous
  login local
  transport input ssh
  transport output ssh
line vty 5 15
  login
!
!
!
ntp authenticate
ntp trusted-key 1
ntp server 25.5.0.4 key 1
!
end

```

```

SwitchSecond#sh run
Building configuration...

Current configuration : 3177 bytes
!
version 12.2
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname SwitchSecond
!
enable secret 5 $1$mERr$VOZfZ/5R0sAyeHvev4ScH1
!
!
!
clock timezone EET 2
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
ip domain-name SwitchSecond.second
!
username adminer secret 5 $1$mERr$sy5570Y8chTcnA2SwGenM.
username technic secret 5 $1$mERr$N.AgdQZ1YY5E8rDIvsV1L1
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
    switchport access vlan 202
    switchport mode access
!
interface FastEthernet0/2
    switchport access vlan 202
    switchport mode access
!
interface FastEthernet0/3
    switchport access vlan 202
    switchport mode access
!
interface FastEthernet0/4
    switchport access vlan 202
    switchport mode access
!
interface FastEthernet0/5
    switchport access vlan 202
    switchport mode access
!
interface FastEthernet0/6
    switchport access vlan 202

```

```

    switchport mode access
    !
interface FastEthernet0/7
    switchport access vlan 202
    switchport mode access
    !
interface FastEthernet0/8
    switchport access vlan 202
    switchport mode access
    !
interface FastEthernet0/9
    switchport access vlan 202
    switchport mode access
    !
interface FastEthernet0/10
    switchport access vlan 202
    switchport mode access
    !
interface FastEthernet0/11
    switchport access vlan 202
    switchport mode access
    !
interface FastEthernet0/12
    switchport access vlan 202
    switchport mode access
    !
interface FastEthernet0/13
    switchport access vlan 203
    switchport mode access
    !
interface FastEthernet0/14
    switchport access vlan 203
    switchport mode access
    !
interface FastEthernet0/15
    switchport access vlan 203
    switchport mode access
    !
interface FastEthernet0/16
    switchport access vlan 203
    switchport mode access
    !
interface FastEthernet0/17
    switchport access vlan 203
    switchport mode access
    !
interface FastEthernet0/18
    switchport access vlan 203
    switchport mode access
    !
interface FastEthernet0/19
    switchport access vlan 203
    switchport mode access

```

```

!
interface FastEthernet0/20
  switchport access vlan 203
  switchport mode access
!
interface FastEthernet0/21
  switchport access vlan 203
  switchport mode access
!
interface FastEthernet0/22
  switchport access vlan 203
  switchport mode access
!
interface FastEthernet0/23
  switchport access vlan 203
  switchport mode access
!
interface FastEthernet0/24
  switchport access vlan 203
  switchport mode access
!
interface GigabitEthernet0/1
  switchport mode trunk
!
interface GigabitEthernet0/2
  switchport access vlan 201
  switchport mode access
!
interface Vlan1
  ip address 100.0.0.3 255.255.255.0
!
interface Vlan201
  ip address 20.1.0.2 255.255.255.0
!
interface Vlan202
  ip address 20.2.0.2 255.255.255.0
!
interface Vlan203
  ip address 20.3.0.2 255.255.255.0
!
ip default-gateway 100.0.0.1
!
banner motd ^C Connection to switch SwitchSecond For legal users
only ^C
logging trap debugging
logging 25.5.0.4
!
!
!
line con 0
  logging synchronous
  login local
!

```

```

line vty 0 4
  logging synchronous
  login local
  transport input ssh
  transport output ssh
line vty 5 15
  login
!
!
!
ntp authenticate
ntp trusted-key 1
ntp server 25.5.0.4 key 1
!
end

```

```

SwitchThird#sh run
Building configuration...

Current configuration : 1506 bytes
!
version 12.1
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname SwitchThird
!
enable secret 5 $1$mERr$VOZFZ/5R0sAyeHvev4Sch1
!
!
!
clock timezone EET 2
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
ip domain-name SwitchThird.third
!
username adminer secret 5 $1$mERr$sy5570Y8chTcnA2SwGenM.
username technic secret 5 $1$mERr$N.AgdQZ1YY5E8rDIvsV1L1
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface GigabitEthernet0/1
    switchport mode trunk
!
interface GigabitEthernet1/1
    switchport access vlan 255
    switchport mode access
!
interface GigabitEthernet2/1
    switchport access vlan 255
    switchport mode access
!
interface FastEthernet3/1
    switchport access vlan 255
    switchport mode access
!
interface FastEthernet4/1
    switchport access vlan 255
    switchport mode access
!
interface GigabitEthernet5/1
    switchport access vlan 255
    switchport mode access

```

```

!
interface GigabitEthernet6/1
  switchport access vlan 255
  switchport mode access
!
interface Vlan1
  ip address 100.0.0.4 255.255.255.0
!
interface Vlan255
  ip address 25.5.0.2 255.255.255.0
!
banner motd ^C Connection to switch SwitchThird For legal users
only ^C
logging trap debugging
logging 25.5.0.4
!
!
!
line con 0
  logging synchronous
  login local
!
line vty 0 4
  logging synchronous
  login local
  transport input ssh
  transport output ssh
line vty 5 15
  login
!
!
!
ntp authenticate
ntp trusted-key 1
ntp server 25.5.0.4 key 1
!
end

```