МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І.І.МЕЧНИКОВА

(повне найменування вищого навчального закладу)

\_\_\_\_\_\_\_\_\_Факультет математики, фізики та інформаційних технологій\_\_\_\_\_\_\_\_\_\_\_

(повне найменування інституту, назва факультету (відділення))

\_\_\_\_\_\_\_\_\_\_\_\_Кафедра математичного забезпечення комп’ютерних систем\_\_\_\_\_\_\_\_\_\_\_

(повна назва кафедри (предметної, циклової комісії))

**Пояснювальна записка**

до курсового проекту

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_з дисципліни «Комп’ютерні мережі»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_на тему «Розробка комп‘ютерної мережі»\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Офісу компанії «Odium» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Виконав: студент \_4\_курсу, групи КА\_

напряму підготовки (спеціальності)

\_\_\_\_\_\_\_\_комп’ютерна інженерія\_\_\_\_\_\_\_

(шифр і назва напряму підготовки, спеціальності)

\_\_\_\_\_\_\_\_\_\_\_\_\_Султанов Ш.ДЖ.\_\_\_\_\_\_\_\_\_\_\_\_\_

(прізвище та ініціали)

Керівник: \_\_\_\_Волощук Л.А.\_\_\_\_\_\_\_\_\_\_\_

(прізвище та ініціали)

Рецензент: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(прізвище та ініціали)

Одеса – 2021

АНОТАЦІЯ

Мета проекту – проектування та реалізація комп’ютерної мережі в компанії «Odium».

В процесі виконання курсового проекту була спроектована комп’ютерна мережа з оптимальною топологією «зірка». Приведений приклади планів приміщення, облаштовані комп’ютерні місця для усіх співробітників, яким вони потрібні, встановлений окремий файловий сервер для зберігання даних компанії та сервер з веб-сайтом компанії. Також встановлені камери відеоспостереження та необхідний для їх функціонування сервер. Побудована структурно-логічна схема комп’ютерної мережі

Проведена калькуляція всього необхідного обладнання, тобто оформлені кабельний журнал та кошторис для спроектованої мережі. А також, промодельована схема мережі в середовищі Packet Tracer і забезпечена її безпека.

ЗМІСТ

[ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ І ТЕРМІНІВ 4](#_Toc90579370)

[ВВЕДЕННЯ 5](#_Toc90579371)

[1 ПОСТАНОВКА ЗАДАЧІ ПРОЕКТУ 6](#_Toc90579372)

[2 ТЕОРИТИЧНІ ОСНОВИ ПРОЕКТУ 8](#_Toc90579373)

[3 ПРОЕКТУВАННЯ КОМП’ЮТЕРНОЇ МЕРЕЖІ 13](#_Toc90579374)

[3.1 Побудова мережі в графічному редакторі 13](#_Toc90579375)

[3.2 Побудова структурно-логічної схеми комп’ютерної мережі 15](#_Toc90579376)

[3.3 Вибір активного і пасивного обладнання для реалізації мережі 17](#_Toc90579377)

[3.4 Оформлення кабельного журналу 26](#_Toc90579378)

[3.5 Кошторис обладнання для реалізації мережі 28](#_Toc90579379)

[3.6 Моделювання мережі в середовищі Cisco Packet Tracer 29](#_Toc90579380)

[3.7 Забезпечення безпеки мережі 39](#_Toc90579381)

[ВИСНОВОК 41](#_Toc90579382)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 42](#_Toc90579383)

[ДОДАТОК А 44](#_Toc90579384)

[ДОДАТОК Б 45](#_Toc90579385)

[ДОДАТОК В 46](#_Toc90579386)

[ДОДАТОК Г 47](#_Toc90579387)

[ДОДАТОК Д 48](#_Toc90579388)

# ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ І ТЕРМІНІВ

Скорочення:

ПЗ - програмне забезпечення;

ДМЗ - демілітаризована зона;

VLAN (Virtual Local Area Network) – віртуальна локальна комп’ютерна мережа;

ACL (Access Control List) – список контролю доступом;

NAT (Network Address Translation) – трансляція мережевих адресів.

# ВВЕДЕННЯ

Нові технології набагато спрощують наше повсякденне життя. Вони використовуються майже у всіх сферах діяльності людини. Не будуть виключенням і компанії, що використовують різні розробки техніки, аби забезпечити більш якісну, швидку та зручну роботу.

Ціллю даної курсової роботи є проектування та реалізація комп’ютерної мережі саме для одної з компаній, що займається розробкою android додатків.

В рамках поставленої цілі були сформовані наступні задачі:

1. побудова комп’ютерної мережі з можливістю додавання нових вузлів і видалення старих;
2. розділити мережу на підмережі та віртуальні мережі відповідно до існуючих відділів та їх призначенням;
3. встановлення веб-серверу компанії;
4. встановлення камер та окремого серверу для відеоспостереження;
5. встановлення файлового серверу для зберігання даних;
6. забезпечення можливості виходу в інтернет.

# 1 ПОСТАНОВКА ЗАДАЧІ ПРОЕКТУ

У рамках цієї курсової роботи проводиться проектування комп'ютерної мережі офісу IT компанії "Odium". Компанія "Odium" займається розробкою android програм. Схема офісних приміщень компанії представлена на ​​рисунку 1.

Офіс компанії складається з 13 кабінетів (приймальня, відділ маркетингу, кабінет нарад, кабінет директора, кабінет секретаря, кабінет бухгалтера, серверна, HR відділ та IT відділ – 5 кабінетів).

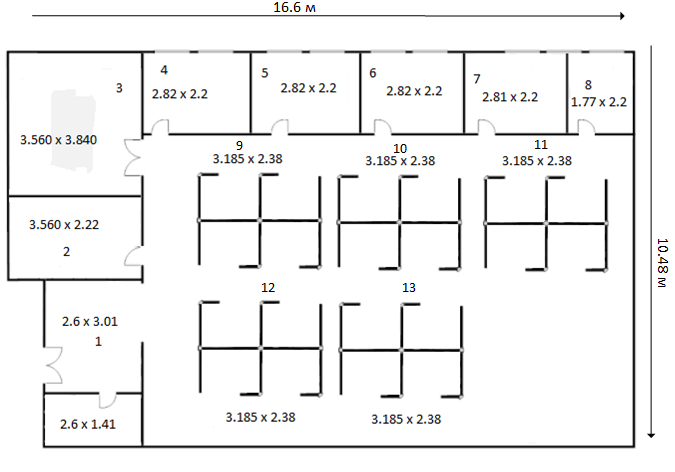


Рисунок 1.1 - Схема офісного приміщення

1 - Прийомне, одне робоче місце охорони для доступу до камер;

2 - відділ маркетингу та реклами, в ньому знаходяться 4 комп'ютеризовані робочі місця для керівника відділу, розробника реклами компанії, маркетолога та редактора-верстальника сайту;

3 - кабінет для нарад, з доступом до бездротової локальної мережі WIFI;

4 – кабінет директора, одне комп'ютеризоване робоче місце для директора;

5 – кабінет секретаря, одне комп'ютеризоване робоче місце для секретаря;

6 – кабінет бухгалтера, одне комп'ютеризоване робоче місце для бухгалтера;

7 - HR відділ з двома комп'ютеризованими робочими місцями для HR-менеджера та асистента;

8 – серверна, три сервера (один – для відеоспостережень, другий – файловий сервер, третій – веб сервер);

9,10,11,12,13 - це IT відділ де, 9-11(backend та frontend розробники), 12 - дизайнери, 13 - тестувальники.

Вимоги до проектованої мережі:

1. створення локальної комп'ютерної мережі з 30 робочими компютеризованими місцями, трьома серверами (файловий, web-сервер, сервер для відеоспостережень) та виходом до Інтернету з усіх вузлів мережі;
2. створення широкомовних доменів (VLAN) для підрозділів (точка доступу, відділ маркетингу, IT відділ, HR відділ, охорона, адміністрація (директор, бухгалтер, секретар та файловий сервер));
3. створення бездротової локальної мережі WIFI з доступом на паролі для співробітників офісу;
4. організація доступу до web-сервера з Інтернету;
5. створення системи відеоспостережень, що включає камери відеоспостереження на всіх кабінетах (крім кабінету директора), робоче місце охорони та відеосервер.

# 2 ТЕОРИТИЧНІ ОСНОВИ ПРОЕКТУ

Сукупність комп'ютерів, взаємопов'язаних через канали передачі даних для забезпечення обміну інформацією та колективного доступу користувачів до апаратних, програмних і інформаційних ресурсів мережі називаються комп’ютерною мережею. Ethernet - сімейство технологій пакетної передачі даних між пристроями для комп'ютерних і промислових мереж.

Стандарти Ethernet визначають дротяні з'єднання і електричні сигнали на фізичному рівні, формат кадру та протоколи управління доступом до середовища - на канальному рівні моделі OSI. Ethernet в основному описується стандартами IEEE групи 802.3. Ethernet став найпоширенішою технологією ЛВС в середині 1990-х років, витіснивши такі застарілі технології, як Token Ring, FDDI і ARCNET.

Назва «Ethernet» відображає первісний принцип роботи цієї технології: все, що передається одним вузлом, одночасно приймається всіма іншими. В даний час практично завжди підключення відбувається через комутатори, так що кадри, що відправляються одним вузлом, доходять лише до адресата (виняток становлять передачі на широкомовна адресу) - це підвищує швидкість роботи і безпеку мережі.

Зараз під назвою Ethernet мають на увазі стандарти:

- IEEE 802.3, швидкість передачі до 10 Мбіт/с;

- IEEE 802.3u - Fast Ethernet швидкість передачі до 100 Мбіт/с;

- IEEE 802.3z - Gigabit Ethernet швидкість передачі до 1000 Мбіт/с;

- IEEE 802.3ab - Gigabit Ethernet на витій парі категорії 5.

Fast Ethernet (FE) - загальна назва для набору стандартів передачі даних в комп'ютерних мережах за технологією Ethernet зі швидкістю до 100 Мбіт/с, на відміну від вихідних 10 Мбіт/с. Іноді позначається як 100BASE-X, де X має на увазі варіанти реалізації (наприклад, 100BASE-TX, 100BASE-FX). Варіанти для роботи по витій парі мають загальне позначення 100BASE-T.

Відмінності і подібності Fast Ethernet з Ethernet: збереження методу випадкового доступу CSMA / CD, прийнятого в Ethernet; збереження формату кадру, прийнятого в стандарті IEEE 802.3; збереження зіркоподібною топології мереж; підтримка традиційних середовищ передачі даних - витої пари і волоконно-оптичного кабелю.

Стандарт Fast Ethernet визначає три модифікації для роботи з різними видами кабелів: 100Base TX, 100Base T4 і 100Base FX. Модифікації 100Base-TX і 100Base-T4 розраховані на виту пару, а 100Base-FX був розроблений для оптичного кабелю.

100BASE-TX забезпечує передачу даних зі швидкістю до 100 Мбіт/с по кабелю, що складається з двох витих пар 5-ї категорії. Зазвичай передача даних в кожному напрямку ведеться по одній парі, забезпечуючи до 100 Мбіт/с загальної пропускної здатності в дуплексі. Довжина лінії зв'язку обмежена 100 метрами, але по одному стандартному кабелю, який має 4 пари, можна організувати два 100-мегабітних каналу зв'язку.

100BASE-T4 забезпечує передачу даних зі швидкістю до 100 Мбіт/с по кабелю, що складається з чотирьох витих пар 3-й категорії.

100BASE-FX використовує волоконно-оптичний кабель і забезпечує зв’язок випромінюванням з довжиною хвилі 1310 нм. По двох жилах – для прийому (RX) і для передачі (TX). Довжина сегмента мережі може досягати 400 метрів в напівдуплексному режимі (з гарантією виявлення колізій) і 2 кілометрів в повнодуплексному при використанні багатомодового волокна. Робота на великих відстанях можлива при використанні одномодового волокна. 100BASE-FX не сумісний з 10BASE-FL (10-мегабітним варіантом).

Захист мереж являє собою повний і необхідний комплекс заходів, який включає в себе організацію, створення програмного забезпечення, а також прийняття фізичних і технічних заходів. Тільки такий комплекс здатний забезпечити максимальне досягнення властивостей інформаційного ресурсу.

На сьогоднішній день необхідно ретельно подбати про шифрування конкретних властивостей інформаційних ресурсів. Захист мереж можлива при дотриманні необхідних заходів. Можна виділити кілька основних якостей інформаційної мережі.

1) Цілісність. Програмісти і фахівці повинні в повній мірі забезпечити актуальність і правдивість інформації, яка не суперечитиме джерел. Матеріали захищаються від будь-якого руйнування з боку і несанкціонованих змін.

2) Повна конфіденційність. Проводиться максимальне забезпечення захищеності необхідної інформації, яка може піддаватися несанкціонованого доступу шахраїв.

3) Доступність. Захист мереж проводиться в комплексі заходів, які допоможуть забезпечити всі необхідні можливості. Вони допомагають користувачам отримати доступ до збереженої і обробленої інформації.

4) Автентичність. Відбувається необхідне забезпечення дійсності суб’єктів і об’єктів, які мають доступ до певної інформації.

Несанкціонований доступ до інформації, що знаходиться в локальних мережах буває:

1) непрямих – без фізичного доступу до елементів локальних мереж;

2) прямим – з фізичним доступом до елементів локальних мереж.

Для вирішення проблем, які постають перед дисципліною захисту інформації, весь час розробляються різні комплексні механізми. Існують певні види засобів, які представляють собою основні механізми захисту, такими механізмами прийнято вважати: технічні засоби, програмні засоби, змішані апаратно-програмні та організаційні засоби

Віртуальної локальної мережею (Virtual Local Area Network, VLAN) називається група вузлів мережі, трафік якої, в тому числі широкомовний, на канальному рівні повністю ізольований від трафіку інших вузлів мережі.

Це означає, що передача кадрів між різними віртуальними мережами на основі адреси канального рівня неможлива незалежно від типу адреси (унікального, групового або широкомовного). У той же час усередині віртуальної мережі кадри передаються за технологією комутації, то якщо тільки на той порт, який пов’язаний з адресою призначення кадру.

NAT (від англ. Network Address Translation - «перетворення мережевих адрес») – це механізм в мережах TCP / IP, що дозволяє перетворювати IP-адреси транзитних пакетів.

NAT призначений для спрощення і збереження IP-адрес. Він дозволяє приватним IP-мереж, які використовують незареєстровані IP-адреси, підключатися до Інтернету. NAT працює на маршрутизаторі, який зазвичай з’єднує дві мережі, і перетворює приватні (а не глобально унікальні) адреси у внутрішній мережі в дійсні адреси перед відправкою пакетів в іншу мережу. Оскільки дана функція є частиною можливостей маршрутизатора, трансляцію мережевих адрес (NAT) можна налаштувати для відображення тільки однієї адреси всієї мережі для зовнішнього світу. Це забезпечує додаткову безпеку і дозволяє приховати внутрішню мережу від доступу ззовні. NAT підтримує спільні функції забезпечення безпеки і збереження адрес і зазвичай встановлюється в середовищах віддаленого доступу.

ACL (Access Control List) – список контролю доступу, який визначає, хто або що може отримувати доступ до конкретного об’єкта, і які саме операції дозволено або заборонено цьому суб’єкту проводити над об’єктом. Списки контролю доступу є основою систем з виборчим управлінням доступу.

 Існують різні типи списків доступу: стандартні (standard ACLs), розширені (extended ACLs), іменовані (named ACLs). Коли список доступу конфігуруються на маршрутизаторі, кожен список повинен мати унікальний ідентифікаційний номер або ім’я. Ідентифікаційний номер створеного списку доступу повинен знаходитися в межах певного діапазону, заданого для цього типу списку.

Стандартні списки доступу (Standard access lists) – для прийняття рішення (permit або deny) в IP пакеті аналізується тільки адреса джерела повідомлення.

Розширені списки доступу (Extended access lists) перевіряють як IP-адреса джерела, так і IP-адреса призначення, поле протоколу в заголовку пакета мережного рівня і номер порту в заголовку транспортного рівня.

Таким чином, для кожного протоколу, для кожного напряму трафіку і для кожного інтерфейсу може бути створений свій список доступу. Вихідні фільтри не зачіпають трафік, який йде з місцевого маршрутизатора.

Демілітаризованої зона – це сегмент мережі з білою адресацією, відокремлений фаєрволом від інтернету та локальної мережі організації. У DMZ зазвичай поміщають сервера, які повинні бути доступні з інтернету, наприклад, поштовий або веб-сервер. Так як сервера в DMZ-мережі відокремлені від локальної мережі фаєрволом, в разі їх злому, зловмисник не зможе отримати доступ до ресурсів локальної мережі.

# 3 ПРОЕКТУВАННЯ КОМП’ЮТЕРНОЇ МЕРЕЖІ

## 3.1 Побудова мережі в графічному редакторі

В якості графічного редактора була вибрана програма Microsoft Visio 2016, так як однією з її призначень є побудова різноманітних планів, у тому числі планів приміщень та планів мереж.

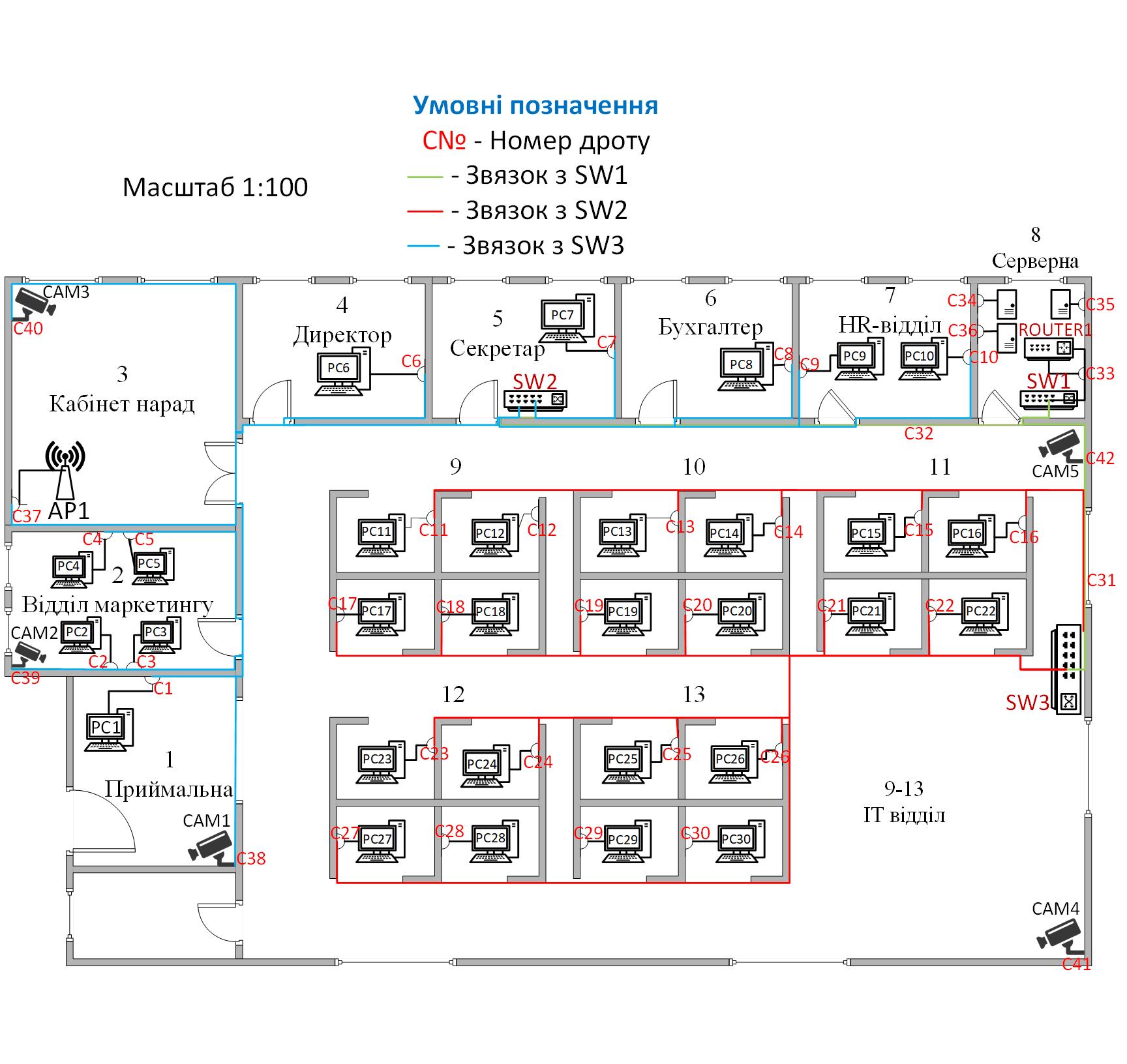


Рисунок 3.1 – Фізична топологія ЛОМ офісу компанії

У Додатку Б знаходиться план приміщення в більшому масштабі з розташованими у ньому комп’ютеризованими робочими місцями, серверами та камерами відеоспостереження. Також зазначене все обладнання, включаючи маршрутизатори, комутатори, а також розміщені кабелі, за допомогою яких утворюється мережа.

Враховуючи те, що реалізована мережа невелика, використовується лише вита пара та бездротова мережа. Мережа побудована з використанням топології «зірка». Дана топологія має наступні переваги:

* це найпростіша топологія з точки зору проектування та реалізації;
* при виході з ладу одного з кабелів, з’єднання обірветься тільки одному користувачеві;
* простий пошук несправностей і обривів в мережі. Наприклад, якщо в одного користувача будуть проблеми із з’єднанням, то пошук проблеми потрібно виконувати тільки на лінії користувача;
* простота перепідключення комп’ютерів і підключення нових користувачів;
* при правильному проектуванні досягається висока продуктивність мережі і гнучкі можливості адміністрування.

Але є і недоліки:

* несправність центрального концентратора зробить сегмент мережі непрацездатним;
* велика довжина сполучних кабелів, у порівнянні з іншими топологіями;
* обмежена кількість робочих станцій сегмента мережі портами центрального концентратора.

## 3.2 Побудова структурно-логічної схеми комп’ютерної мережі

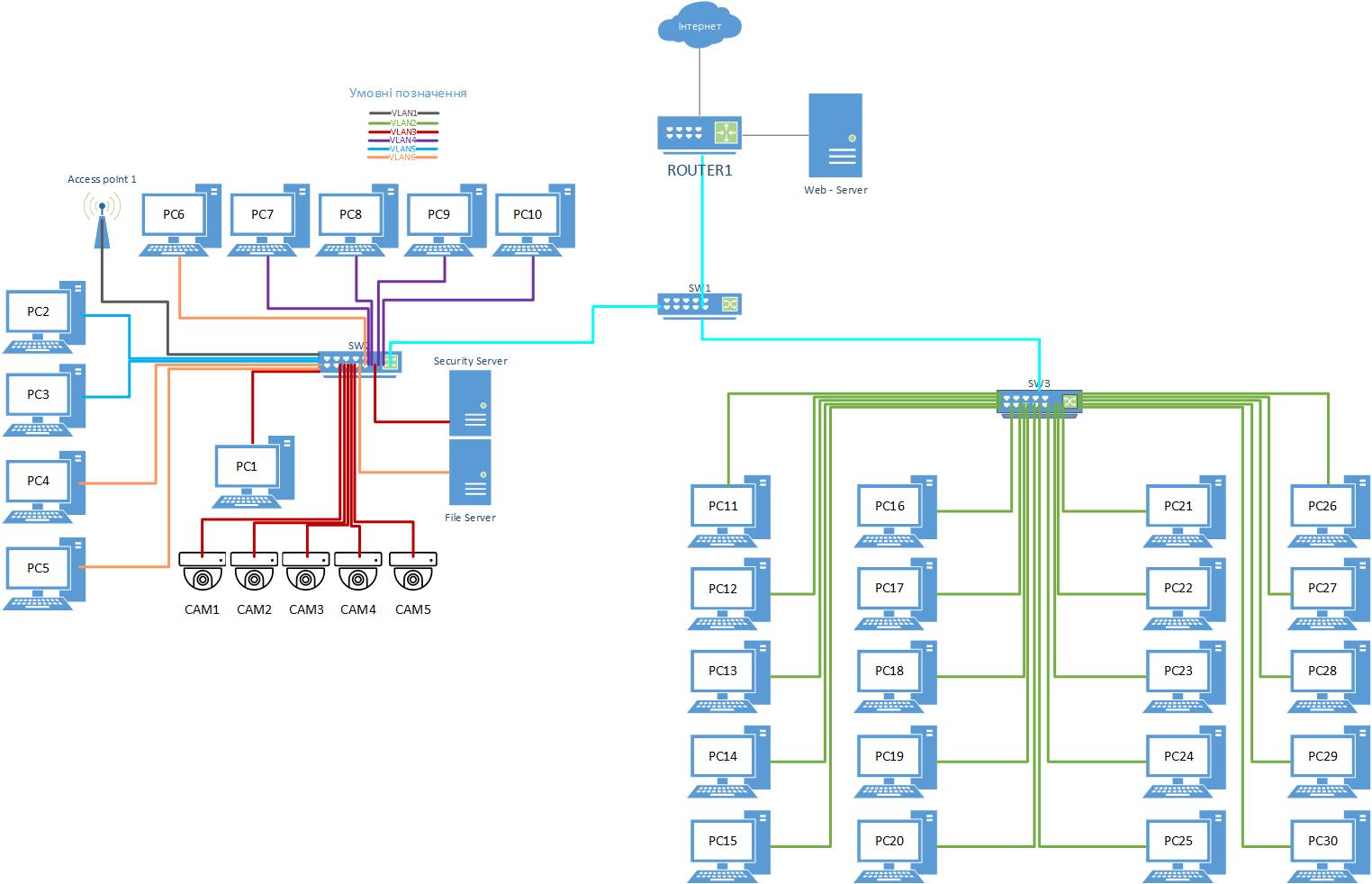


Рисунок 3.2 – Структурно-логічна схема

Створена структурно-логічна схема комп’ютерної мережі також у програмі Microsoft Visio Professional 2016. Включає основні активні та пасивні компоненти. А у Додатку В схема наведена у більшому розмірі.

Відповідно до стандарту IEEE Fast Ethernet, мережа побудована за допомогою UTP-кабелю. Максимальна відстань між комутаторами та вузлами не перевищує 100 метрів. Детальніше про довжину усього прокладеного кабелю описано у кабельному журналі (розділ 3.4).

Відповідно до постановки завдання нам потрібно створити 6 широкомовних доменів VLAN.

1. VLAN1 – для точки доступу, де реалізовано захищену бездротову мережу для підключення клієнтів та співробітників офісу.
2. VLAN2 – створена для IT відділу компанії (frontend, backend програмісти, дизайнери та тестувальники).
3. VLAN3 – окрема підмережа для охорони, з усім необхідним обладнанням (камери та окремий сервер).
4. VLAN4 – для маркетологів (керівник відділу, розробник реклами компанії, маркетолог та редактор-верстальник сайту).
5. VLAN5 – створена для HR відділу компанії (HR-менеджер та асистент).
6. VLAN6 – створена для адміністрації (директор, бухгалтер, секретар та файловий сервер).

Таблиця 3.1 – Таблиця підмереж

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Назва** | **IP-адреса/Маска** | **Адрес шлюзу** | **Діапазон адрес** | **Широкомовна адреса** |
| 1 | VLAN1 - точка доступу | 192.168.1.0/24 | 192.168.1.1 | 192.168.1.1 - 192.168.1.254 | 192.168.1.255 |
| 2 | VLAN2 – IT відділ | 192.168.2.0/24 | 192.168.2.1 | 192.168.2.1 - 192.168.1.254 | 192.168.2.255 |
| 3 | VLAN3 – відділ охорони | 192.168.3.0/24 | 192.168.3.1 | 192.168.3.1 - 192.168.1.254 | 192.168.3.255 |
| 4 | VLAN4 – відділ маркетингу | 192.168.4.0/24 | 192.168.4.1 | 192.168.4.1 - 192.168.1.254 | 192.168.4.255 |
| 5 | VLAN5 – HR відділ | 192.168.5.0/24 | 192.168.5.1 | 192.168.5.1 - 192.168.5.254 | 192.168.5.255 |
| 6 | VLAN6 – Адміністрація | 192.168.6.0/24 | 192.168.6.1 | 192.168.6.1 - 192.168.6.254 | 192.168.6.255 |
| 7 | Web- server | 220.220.1.0/30 | 220.220.1.1 | 220.220.1.1-220.220.1.2 | 220.220.1.3 |

## 

## 3.3 Вибір активного і пасивного обладнання для реалізації мережі

3.3.1 Вибір активного обладнання

1. Комутатор TP-Link (TL-SG1024D) [1]

Комутатори в локальній мережі рівномірно навантажені та більшість їх портів використовується для підключень пристроїв в мережу. З приводу цього, треба використовувати обладнання яке може витримати постійне навантаження на порти. Окрім того, задля забезпечення можливості підключення нових пристроїв, будемо використовувати коммутатори із достатньою кількістю портів. Комутатор TP-Link (TL-SG1024D) має усі вищеперелічені особливості (рис. 3.3.2). Пристрій також оснащений системою охолодження.

**Зручність використання**  
Функції автоузгодження гігабітного комутатора значно полегшують встановлення пристрою. Не потрібне додаткове налаштування. Функція авто-MDI/MDIX усуває необхідність використання кабелю з парами, що перехрещуються. Функція автоузгодження на кожному порту визначає швидкість з'єднання мережного пристрою (10, 100 або 1000 Мбіт/с) і здійснює налаштування сумісності та оптимального режиму роботи.

|  |  |
| --- | --- |
| Порти доступу | [Gigabit Ethernet](https://setevuha.ua/kommutatory/type=378:9599/) |
| Кількість портів Gigabit Ethernet (10/100/1000) | [24 шт.](https://setevuha.ua/kommutatory/type=4629:21274/) |
| Загальна кількість портів доступу (LAN) | [24 шт.](https://setevuha.ua/kommutatory/type=380:11644/) |
| Відповідність мережевим стандартам | IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x |
| Внутрішня пропускна здатність | 23,8 Млн. пакетів у сік. |
| Таблиця МАС адрес | 8K |
| Кадри Jumbo | 10 Кбайт |
| Метод комутації | Store-and-Forward |
| Робоча температура | від 0℃ до 40℃ |
| Температура зберігання | 40℃ до 70℃ |

Таблиця 3.1 – Характеристики комутатора TP-Link (TL-SG1024D)



Рисунок 3.3 – Комутатор TP-Link (TL-SG1024D)

1. Маршрутизатор Cisco SB RV130 [2]

Cпецифікації

Маршрутизатор Cisco SB RV130 підтримує надійну і високопродуктивну зв'язок в мережі, як всередині, так і поза офісом. Це надійний міжмережевий екран і VPN для захищених комунікацій.

Оснащений вбудованим 4-портовим керованим комутатором Gigabit Ethernet, який дозволяє підключати мережеві пристрої і передавати файли і дані на високій швидкості. Налаштування не займає багато часу, конфігурація маршрутизатора дозволить вам почати роботу за лічені хвилини.

Особливості

Безпека IPsec VPN;

Управління: веб-браузер, Bonjour, Universal Plug and Play (UPnP);

Пропускна здатність NAT: 800 Мбіт/с;

Міжмережевий інтерфейс IPSec VPN: 10 міжмережевих тунелів IPSec;

Стандарт шифрування: потрійне шифрування 3DES, розширений стандарт шифрування AES.

Характеристики

Інтерфейси: 4 x RJ-45 10/100/1000 Мбіт/с LAN; 1 x RJ45 10/100/1000 Мбіт/с GE WAN; 1 x USB;

LAN- і WAN-порти: Gigabit Ethernet;

USB 3G/4G/LTE;

Wi-Fi: 2.4 ГГц;

Операційна система: Linux;

Підтримка протоколів PPTP, L2TP, ICMP/IP IPsec, PPPoE, DHCP, DDNS, Bonjour;

Пропускна здатність IPsec VPN (3DES, AES): 50 Мбіт/с;



Рисунок 3.4 – Маршрутизатор Cisco SB RV130

Мережевий кабель КПВ-ВП (350) 4х2х0,51 (U/UTP-cat.5E) [2]

ЗАСТОСУВАННЯ

PBX, V.11, X.21, ISDN, Ethernet (10Base-T), ATM-25/52/155 Мбіт/с, 100VG-AnyLAN, Fast Ethernet (100BASE-TX), Token Ring 16/100 Мбіт/с , Gigabit Ethernet (1000BASE-T), Firewire 100 Мбіт/с

1. Точка доступу MikroTik RBcAPGi-5acD2nD [3]

Комп’ютерна система організації передбачає можливість бездротового з’єднання як для працівників компанії так і для клієнтів. Для того щоб забезпечити постійний доступ у кожній частині приміщення організації використовується точка доступу MikroTik RBcAPGi-5acD2nD (рис. 3.3.8). Особливістю такого обладнання є те, що вона двохдіапазонна, що поширює можливості підключення більшої кількості користувачів.



Рисунок 3.5 – Точка доступу MikroTik RBcAPGi-5acD2nD

3.3.2 Вибір пасивного обладнання

1. Мережевий кабель КПВ-ВП (350) 4х2х0,51 (U/UTP-cat.5E)[4]

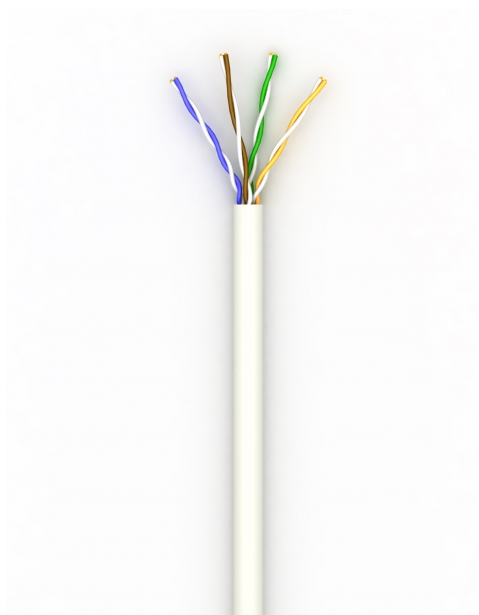


Рисунок 3.6 – Мережевий кабель КПВ-ВП (350) 4х2х0,51 (U/UTP-cat.5E)

1. Комп'ютерна розетка RJ45 зовнішня UTP CAT5e [5]

Зовнішня розетка від виробника E-server™, відмінно підходить для комп'ютерного розведення кабелю, легко встановлюється майже на будь-яку вертикальну поверхню або в короб, якщо в ньому передбачена установка розетки.

Таблиця 3.2 – Характеристика розетки RJ45 зовнішня UTP CAT5e

|  |  |
| --- | --- |
| Тип обладнання | Розетка зовнішня |
| Екранування | UTP |
| Категорія | кат. 5e |
| Тип конектора | RJ-45 |
| Колір | Білий |



Рисунок 3.7 – Інтернет розетка 1\*RJ45 зовнішня, один порт, UTP CAT5e

1. Конектор RJ45 UTP 6 кат. 8P8C 50 мкм [6]

Конектори неекрановані RJ45 8P8C використовуються для комутації в патч-панелі для обтискання UTP кабелю при побудові СКС. Мають категорію 6 із пропускною швидкістю до 10Гбітс.

Таблиця 3.3 – Характеристика Конектора RJ45 UTP 6 кат. 8P8C 50 мкм

|  |  |
| --- | --- |
| Тип обладнання | Конектори |
| Тип конектора | RJ-45 |
| Екранування | UTP |
| Категорія | кат. 6 |
| Ціна | за 1шт. |



Рисунок 3.8 – Конектор RJ45 UTP 6 кат. 8P8C 50 мкм

1. Патч-корд UTP CAT5e, фіолетовий, 0.5м, EServer [7]

Патч-корд не екранований, від компанії E-server™ має довжину 0,5 метра, для відмінної передачі сигналу провідники виготовляються з міді. Кабель категорії 5е захищений від пошкоджень полівінілхлоридною оболонкою і використовується для швидкої та зручної комутації компонентів СКС.

Таблиця 3.4 – Характеристика патч-корда UTP CAT5e, фіолетовий, 0.5м

|  |  |
| --- | --- |
| Довжина, м | 0.5 |
| Екранування | UTP |
| Категорія | кат. 5e |
| Оболонка кабелю | PVC(ПВХ) |
| Переріз кабеля | 0.51мм |
| Колір | Фіолетовий |



Рисунок 3.9 – Патч-корд UTP CAT5e, фіолетовий, 0.5м, EServer

1. Канал кабельний Schneider Electric 40x40 мм ПВХ ULT 2 м [8]

Таблиця 3.5 – Характеристика кабельного каналу Schneider Electric 40x40 мм ПВХ ULT 2 м

|  |  |
| --- | --- |
| Ціна: | 123.20 ₴/шт. |
| Тип: | кабельний канал |
| Матеріал: | ПВХ |
| Бренд: | Schneider Electric |
| Колір виробника: | Білий |
| Країна виробник: | Туреччина |
| Довжина: | 2000 мм |
| Висота: | 40 мм |
| Ступінь захисту (IP): | 40 |
| Ширина: | 40 мм |
| Діапазон робочих температур: | від -5 до +60 °C |
| Застосування: | для внутрішньої прокладки |



Рисунок 3.10 – Канал кабельний Schneider Electric 40x40 мм ПВХ ULT 2 м

1. АНТИВАНДАЛЬНИЙ ЯЩИК IPCOM БК-550-З-1-2U K-4549 [9]

Антивандальний бокс БК-550-З-1-2U встановлюється у місцях громадського доступу. Ціліснозварна конструкція з листової сталі має необхідну міцність і жорсткість для захисту від крадіжок та пошкоджень спеціалізованого обладнання. Дверцята пінального типу відсуваються в ліву сторону і замикаються надійним сувальдним замком. Ця модель призначена для внутрішньої установки. Кабельні введення спеціального виду перешкоджають розкраданню дротів. Для стабільної роботи електронних компонентів у стінках боксу передбачені вентиляційні ґрати, що забезпечують охолодження. Допускається статичне навантаження не більше 60 кг.

Таблиця 3.6 – Характеристика АНТИВАНДАЛЬНОГО ЯЩИКА IPCOM БК-550-З-1-2U K-4549

|  |  |
| --- | --- |
| Висота, мм | 500 |
| Артикул | ТЦБ-0019580 |
| Ширина, мм | 550 |
| Глибина, мм | 150 |
| Тип передніх дверей | Пенальна |
| Кабельні введення | d=22-8 шт |
| Покриття | Порошково-полімерне |
| Колір | Світло-сірий (RAL 7035) |
| Ступінь захисту | IP20 |
| Тип виконання | Настінне |
| Макс. Стат. навантаження | 60 кг |
| Вага | 11,2 кг |
| Конструктив | Ціліснозварної |
| Замок | Сувальдний |



Рисунок 3.11– АНТИВАНДАЛЬНИЙ ЯЩИК IPCOM БК-550-З-1-2U K-4549

## 3.4 Оформлення кабельного журналу

Кабельний журнал представлений у таблиці 3.4.1.

Таблиця 3.7 – Кабельний журнал

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Позначення кабелю** | **Куди** | **Звідки** | **Вид кабелю** | **Довжина, м** |
| 1 | C1 | PC1 | SW3 | UTP с.5Е | 12 |
| 2 | C2 | PC2 | SW3 | UTP с.5Е | 10 |
| 3 | C3 | PC3 | SW3 | UTP с.5Е | 9.5 |
| 4 | C4 | PC4 | SW3 | UTP с.5Е | 11 |
| 5 | C5 | PC5 | SW3 | UTP с.5Е | 10 |
| 6 | C6 | PC6 | SW3 | UTP с.5Е | 7 |
| 7 | C7 | PC7 | SW3 | UTP с.5Е | 2.5 |
| 8 | C8 | PC8 | SW3 | UTP с.5Е | 7 |
| 9 | C9 | PC9 | SW3 | UTP с.5Е | 8 |
| 10 | C10 | PC10 | SW3 | UTP с.5Е | 10.5 |
| 11 | C11 | PC11 | SW3 | UTP с.5Е | 13 |
| 12 | C12 | PC12 | SW3 | UTP с.5Е | 11 |
| 13 | C13 | PC13 | SW3 | UTP с.5Е | 9 |
| 14 | C14 | PC14 | SW3 | UTP с.5Е | 7 |
| 15 | C15 | PC15 | SW3 | UTP с.5Е | 5 |
| 16 | C16 | PC16 | SW3 | UTP с.5Е | 3.5 |
| 17 | C17 | PC17 | SW3 | UTP с.5Е | 12.5 |
| 18 | C18 | PC18 | SW3 | UTP с.5Е | 10.5 |
| 19 | C19 | PC19 | SW3 | UTP с.5Е | 8.5 |
| 20 | C20 | PC20 | SW3 | UTP с.5Е | 6.5 |
| 21 | C21 | PC21 | SW3 | UTP с.5Е | 4.5 |
| 22 | C22 | PC22 | SW3 | UTP с.5Е | 3 |
| 23 | C23 | PC23 | SW3 | UTP с.5Е | 10 |

Продовження таблиці 3.7

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 24 | C24 | PC24 | SW3 | UTP с.5Е | 8.5 |
| 25 | C25 | PC25 | SW3 | UTP с.5Е | 7 |
| 26 | C26 | PC26 | SW3 | UTP с.5Е | 5.5 |
| 27 | C27 | PC27 | SW3 | UTP с.5Е | 14.5 |
| 28 | C28 | PC28 | SW3 | UTP с.5Е | 13 |
| 29 | C29 | PC29 | SW3 | UTP с.5Е | 11 |
| 30 | C30 | PC30 | SW3 | UTP с.5Е | 9 |
| 31 | C31 | SW2 | SW1 | UTP с.6A | 11 |
| 32 | C32 | SW3 | SW1 | UTP с.6A | 10 |
| 33 | C33 | SW1 | ROUTER1 | UTP с.6A | 2 |
| 34 | C34 | VideoServer | SW2 | UTP с.5Е | 11 |
| 35 | C35 | FileServer | SW2 | UTP с.5Е | 12 |
| 36 | C36 | WebServer | ROUTER1 | UTP с.5Е | 3 |
| 37 | C37 | WirelessR1 | SW2 | UTP с.6A | 14 |
| 38 | C38 | Cam1 | SW2 | UTP с.5Е | 13 |
| 39 | C39 | Cam2 | SW2 | UTP с.5Е | 12 |
| 40 | C40 | Cam3 | SW2 | UTP с.5Е | 12 |
| 41 | C41 | Cam4 | SW2 | UTP с.5Е | 26 |
| 42 | C42 | Cam5 | SW2 | UTP с.5Е | 11 |
| **Разом: 446,5 м** | | | | | |

# 3.5 Кошторис обладнання для реалізації мережі

Кошторис обладнання представлений у таблиці 3.5.1.

Таблиця 3.8 – Кошторис обладнання

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Найменування | Одиниця виміру | Кількість | Вартість за одиницю, грн. | Сумарна вартість, грн. |
| 1 | Маршрутизатор Cisco SB RV130 | Штук | 1 | 3700 | 3700 |
| 2 | Мережевий кабель КПВ-ВП (350) 4х2х0,51 (U/UTP-cat.5E) | Метр | 470 | 10 | 4700 |
| 3 | Комутатор TP-Link (TL-SG1024D) | Штук | 3 | 3170 | 9510 |
| 4 | Інтернет розетка 1\*RJ45 зовнішня, один порт, UTP CAT5e | Штук | 45 | 36 | 1080 |
| 5 | Конектор RJ45 UTP 6 кат. 8P8C 50 мкм | Штук | 45 | 4 | 180 |
| 6 | Патч-корд UTP CAT5e, фіолетовий, 0.5м, EServer | Штук | 50 | 21 | 1050 |
| 7 | Канал кабельний Schneider Electric 40x40 мм ПВХ ULT 2 м MikroTik RBcAPGi-5acD2nD | Штук | 80 | 100 | 8000 |
| 8 | Точка доступу MikroTik RBcAPGi-5acD2nD | Штук | 1 | 2200 | 2200 |
| 9 | АНТИВАНДАЛЬНИЙ ЯЩИК IPCOM БК-550-З-1-2U K-4549 | Штук | 3 | 950 | 2850 |
| Разом: 33 370 | | | | | |

## 3.6 Моделювання мережі в середовищі Cisco Packet Tracer

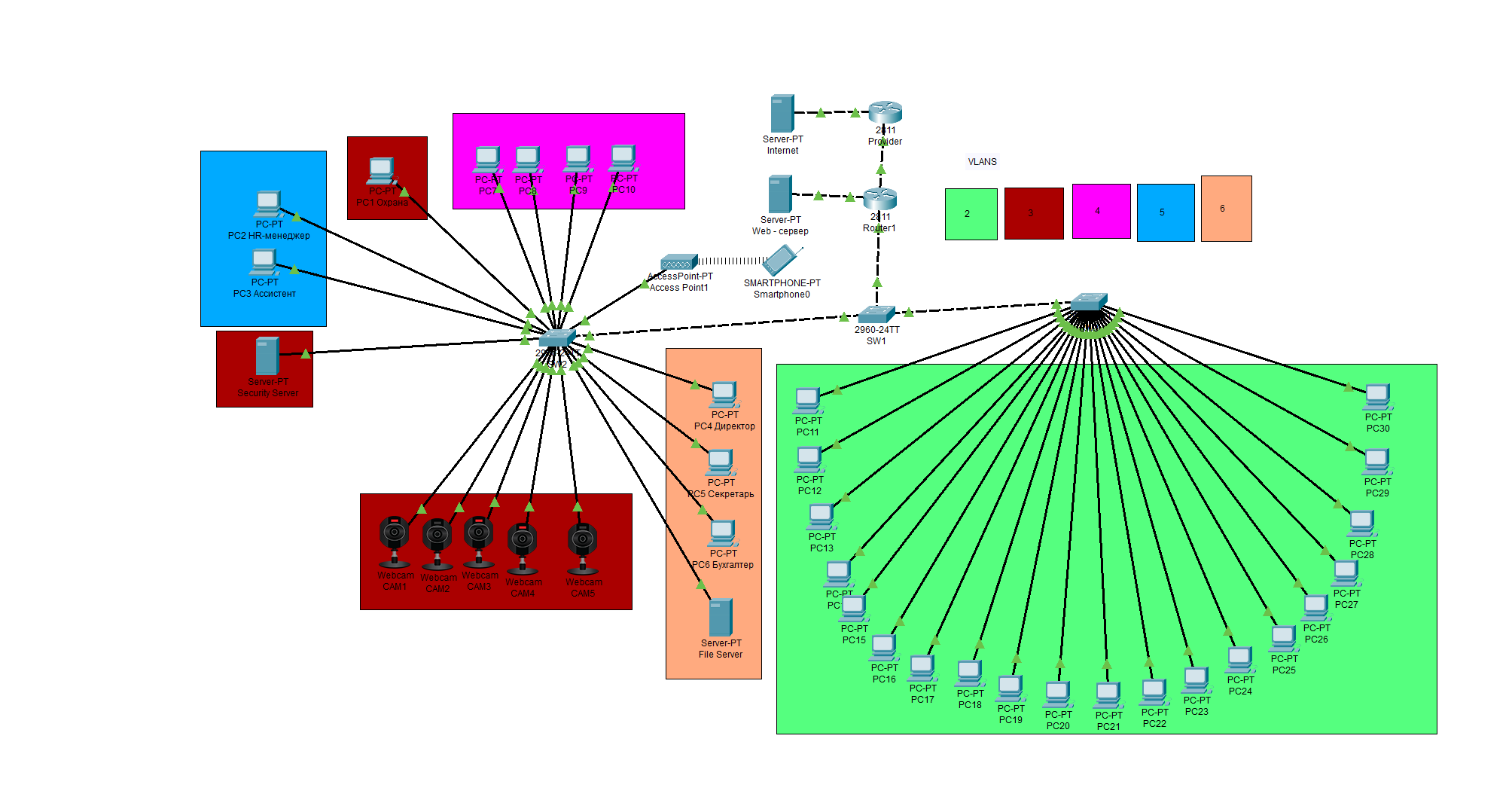


Рисунок 3.12 – Змодельована мережа в Packet Tracer

У відповідності до спроектованої структурно-логічної схеми мережі, в середовищі Cisco Packet Tracer, вибрано усе необхідне обладнання, зокрема кінцеві пристрої (комп’ютери, камери). Також у додатку Г схема наведена в більшому розмірі для наочності.

Мережа розділена на 6 віртуальних мереж (VLAN), включаючи першу за умовчуванням:

1. VLAN1 – створена для точки доступу
2. VLAN2 – створена для IT відділу компанії (frontend, backend програмісти, дизайнери та тестувальники). Має доступ до Інтернету, серверу компанії, та на веб-сервер своєї фірми;
3. VLAN3 – окрема підмережа для охорони, з усім необхідним обладнанням (камери та окремий сервер). Не має нікуди доступу а до неї має тільки директор.
4. VLAN4 – для співробітників компанії, а саме для маркетологів. Має доступ до Інтернету, серверу компанії, та на веб-сервер своєї фірми;
5. VLAN5 – створена для HR відділу компанії. Має доступ до Інтернету, серверу компанії, та на веб-сервер своєї фірми.
6. VLAN6 – створена для адміністрації (директор, бухгалтер, секретар та файловий сервер).

Обмежений доступ до всієї локальної мережі.

Розмежування на віртуальні мережі в Cisco Packet Tracer отримано шляхом налаштування на маршрутизаторі та комутаторах. Через інтерфейс командного рядку комутатора створені віртуальні мережі та відповідні призначені через порти:

#int fa0/2

#switchport mode access

#switchport access vlan 2

#exit

Комутатори між собою та з маршрутизатором з’єднані каналом типу trunk, для передачі трафіку декільком віртуальним мережам:

#int fa0/1

#switchport mode trunk

#switchport trunk allowed vlan 2,3

#end

Передача трафіку між віртуальними мережами виконується за допомогою маршрутизатора. Для того, що він це міг робити, для кожної VLAN необхідно мати свій інтерфейс, але щоб не виділяти для кожної мережі окремий фізичних інтерфейс, створюються логічні під інтерфейси:

#int fa1/0.2

#encapsulation dot1Q 2

#ip address 192.168.2.1 255.255.255.0

#exit

Таким чином налаштована вся мережа компанії. У результаті отримано 5 підінтерфейсів у маршрутизаторі (таблиця 3.6.1).

Таблиця 3.9 – Підінтерфейси маршрутизатору

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Назва підінтерфейсу | Назва VLAN | Номер VLAN | IP-адрес | Маска |
| FastEthernet1/0.2 | Vlan2 | 2 | 192.168.2.0 | 255.255.255.0 |
| FastEthernet1/0.3 | Vlan3 | 3 | 192.168.3.0 | 255.255.255.0 |
| FastEthernet1/0.4 | Vlan4 | 4 | 192.168.4.0 | 255.255.255.0 |
| FastEthernet1/0.5 | Vlan5 | 5 | 192.168.5.0 | 255.255.255.0 |
| FastEthernet1/0.6 | Vlan6 | 6 | 192.168.6.0 | 255.255.255.0 |

Також для 2,4 та 5 віртуальної мережі налаштована динамічна роздача адресів. Для інших задана статично.

ip dhcp excluded-address 192.168.2.1

ip dhcp excluded-address 192.168.4.1

ip dhcp excluded-address 192.168.5.1

ip dhcp pool IT\_green

network 192.168.2.0 255.255.255.0

default-router 192.168.2.1

ip dhcp pool MR\_purple

network 192.168.4.0 255.255.255.0

default-router 192.168.4.1

ip dhcp pool HR\_blue

network 192.168.5.0 255.255.255.0

default-router 192.168.5.1

У рисунках 3.13 та 3.14 показано статичну та динамічну роздачу адресів.

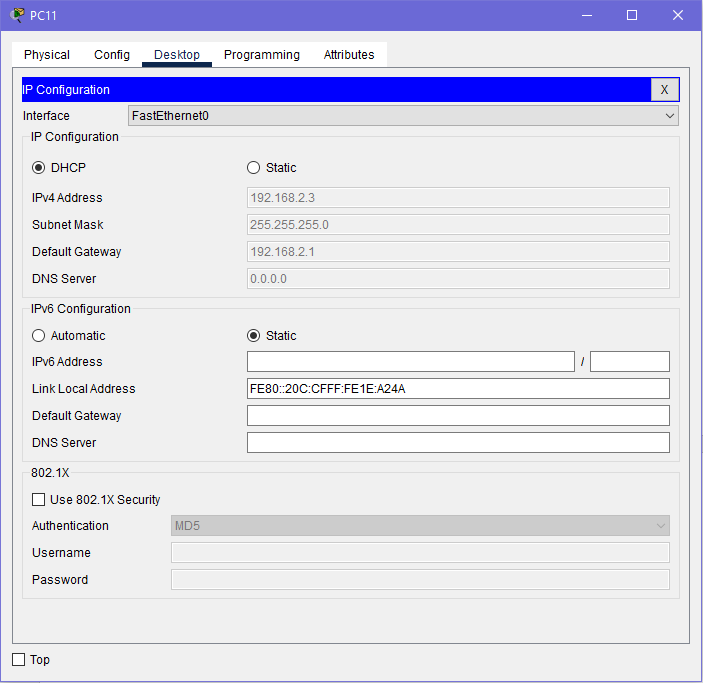


Рисунок 3.13 – Динамічна роздача адресів

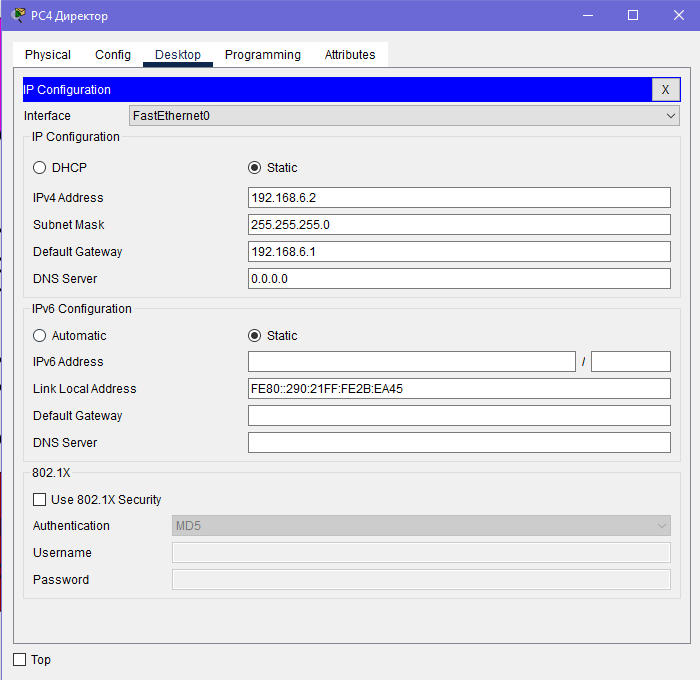


Рисунок 3.15 – Статична роздача адресів

Сервер охорони налаштован як IoT та DNS сервер, для підключення до камер та для доступу до них ком'пютеру охорони та директора.

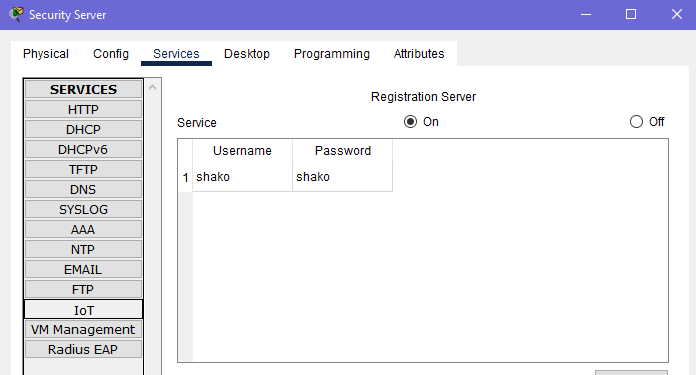


Рисунок 3.15 – IoT сервер охорони

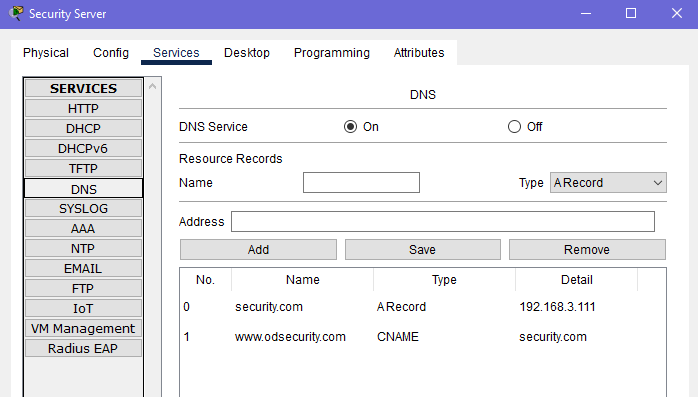


Рисунок 3.16 – DNS сервер охорони

Щоб підключитися до серверу IoT треба налаштувати IoT об’єкти (тобто камери), для цього в Config, IoT Server там де поле ServerAddress треба написати адрес IoT сервера та на полях UserName та Password, написати логін та пароль, яку можна створити через посилання Sign up now (рисунки 3.16 та 3.17).

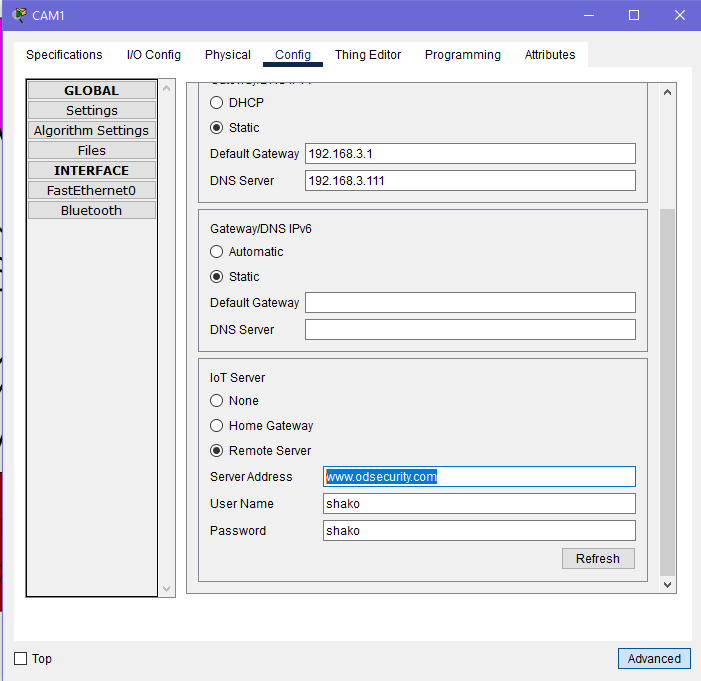


Рисунок 3.16 – Налаштування CAM1 для підключення до серверу охорони

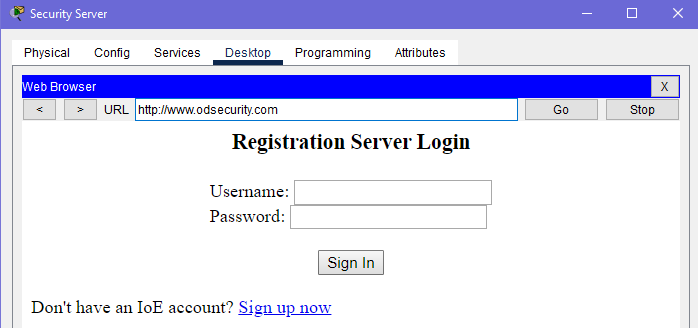


Рисунок 3.17 – сторінка підключення до серверу

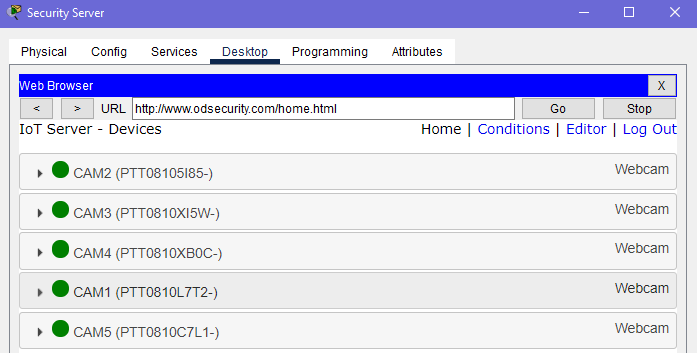


Рисунок 3.18 – Сторінка управління камерами

Для налаштування точки доступу AP1, потрібно на вкладці Config,Port 1 - у полі SSID написати назву підключення, вибрати режим автентифікації та у полі PASS PHASE написати пароль для доступу (рисунок 3.19), а для підключення треба в відповідних полях вкладки Config, Wireless написати відповідні значення (рисунок 3.20).

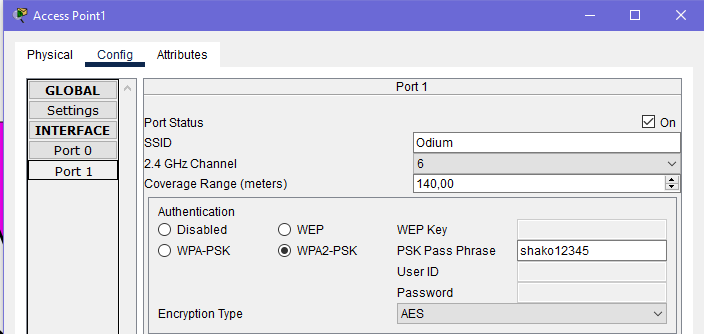


Рисунок 3.19 – Налаштування Access Point1

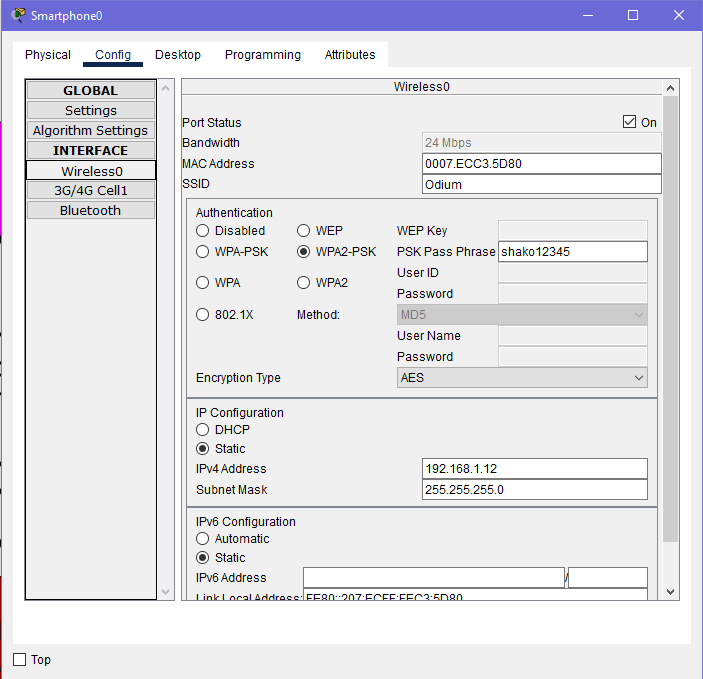


Рисунок 3.20 –Налаштування Smarpthone0

Назви вузлів та їх ІР-адреси наведені у таблиці 3.10

Таблиця 3.10 – Назви та ІР-адреси вузлів

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Имя узла** | **№ VLAN** | **Имя VLAN** | **Шлюз** | **IP-адрес** | **Маска** |
| 1 | PC1 | 3 | VLAN3 | 192.168.3.1 | 192.168.3.11 | 255.255.255.0 |
| 2 | PC2 | 5 | VLAN5 | 192.168.5.1 | DHCP | 255.255.255.0 |
| 3 | PC3 | 5 | VLAN5 | 192.168.5.1 | DHCP | 255.255.255.0 |
| 4 | PC4 | 6 | VLAN6 | 192.168.6.1 | 192.168.6.2 | 255.255.255.0 |
| 5 | PC5 | 6 | VLAN6 | 192.168.6.1 | 192.168.6.3 | 255.255.255.0 |
| 6 | PC6 | 6 | VLAN6 | 192.168.6.1 | 192.168.6.4 | 255.255.255.0 |
| 7 | PC7 | 4 | VLAN4 | 192.168.4.1 | DHCP | 255.255.255.0 |
| 8 | PC8 | 4 | VLAN4 | 192.168.4.1 | DHCP | 255.255.255.0 |
| 9 | PC9 | 4 | VLAN4 | 192.168.4.1 | DHCP | 255.255.255.0 |
| 10 | PC10 | 4 | VLAN4 | 192.168.4.1 | DHCP | 255.255.255.0 |
| 11 | PC11 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 12 | PC12 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 13 | PC13 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 14 | PC14 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 15 | PC15 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 16 | PC16 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 17 | PC17 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 18 | PC18 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 19 | PC19 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 20 | PC20 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 21 | PC21 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 22 | PC22 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 23 | PC23 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |

Продовження таблиці 3.10

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 24 | PC24 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 25 | PC25 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 26 | PC26 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 27 | PC27 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 28 | PC28 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 29 | PC29 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 30 | PC30 | 2 | VLAN2 | 192.168.2.1 | DHCP | 255.255.255.0 |
| 31 | CAM1 | 3 | VLAN3 | 192.168.3.1 | 192.168.3.31 | 255.255.255.0 |
| 32 | CAM2 | 3 | VLAN3 | 192.168.3.1 | 192.168.3.32 | 255.255.255.0 |
| 33 | CAM3 | 3 | VLAN3 | 192.168.3.1 | 192.168.3.33 | 255.255.255.0 |
| 34 | CAM4 | 3 | VLAN3 | 192.168.3.1 | 192.168.3.34 | 255.255.255.0 |
| 35 | CAM5 | 3 | VLAN3 | 192.168.3.1 | 192.168.3.35 | 255.255.255.0 |
| 36 | FileServer | 6 | VLAN6 | 192.168.6.1 | 192.168.6.99 | 255.255.255.0 |

## 3.7 Забезпечення безпеки мережі

Політика безпеки мережі:

* **Налаштування трансляції мережевих адрес – NAT;**
* **контроль доступу до web-сервера, що знаходиться в ДМЗ;**
* **ПЗ для безпеки серверів та комп'ютера;**
* **директор має повний доступ до всіх вузлів мережі, до нього мають доступ лише секретар та бухгалтер;**
* **секретар має доступ до всіх вузлів мережі, крім охорони, до нього мають доступ директор та бухгалтер;**
* **до бухгалтера має доступ лише директор та секретар;**
* **всі вузли мають доступ до Інтернету, але з інтернету доступ тільки до web-сервера;**
* **кожен користувач має доступ до Інтернету, крім охорони;**
* **доступ до файлового сервера компанії дозволено всім вузлам, крім охорони;**
* **серверам заблоковано доступ до Інтернету;**
* **доступ до сервера служби безпеки дозволено лише комп'ютеру для охорони та директора;**
* **відсутній доступ між віртуальними мережами.**

Налаштування NAT:

NAT (Network Address Translation) - трансляція мережевих адрес, технологія, яка дозволяє перетворювати (змінювати) IP адреси і порти в мережевих пакетах.

Для налаштування NAT, кожен з інтерфейсів і сабінтерфейсов маршрутизатора визначаємо внутрішнім або зовнішнім (ip nat inside / ip nat outside). Потім створюємо стандартний список доступу FOR-NAT, в який заносимо дозволені для трансляції адреси. Потім призначаємо NAT на потрібний порт маршрутизатора, вказуючи створений список доступу і оголошуючи його overload (з перевантаженням).

іp access-list standard FOR-NAT

permit 192.168.1.0 0.0.0.255

permit 192.168.2.0 0.0.0.255

permit 192.168.4.0 0.0.0.255

permit 192.168.5.0 0.0.0.255

permit 192.168.6.0 0.0.0.255

exit

interface FastEthernet0/0

ip nat outside

exit

interface range Fа1/0.2 - Fa1/0.6

ip nat inside

exit

Наступним кроком є налаштування списків доступу.

Список доступу - список правил доступу, в яких визначається хто або що може отримувати доступ до об'єкта і які саме дії виконувати.

Всього було створено 8 списків доступу: FOR-NAT, FROM-DMZ, FROM-OUTSIDE, FOR-SECUR, FOR-HR, FOR-MR, FOR-WIFI, FOR-ADMIN.

Наприклад:

ip access-list extended FOR-HR

permit ip 192.168.5.0 0.0.0.255 host 220.220.1.2

permit ip 192.168.5.0 0.0.0.255 host 210.210.1.2

permit ip 192.168.5.0 0.0.0.255 host 192.168.6.99

permit ip 192.168.5.0 0.0.0.255 host 192.168.6.2

permit ip 192.168.5.0 0.0.0.255 host 192.168.6.3

deny ip 192.168.5.0 0.0.0.255 192.168.1.0 0.0.0.255

deny ip 192.168.5.0 0.0.0.255 192.168.2.0 0.0.0.255

deny ip 192.168.5.0 0.0.0.255 192.168.3.0 0.0.0.255

deny ip 192.168.5.0 0.0.0.255 192.168.4.0 0.0.0.255

deny ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

permit ip any any

Список доступу FROM-DMZ дозволяє лише трафік у відповідь з DMZ.

ip access-list extended FROM-DMZ

deny ip host 220.220.1.2 192.168.1.0 0.0.0.255

deny ip host 220.220.1.2 192.168.2.0 0.0.0.255

deny ip host 220.220.1.2 192.168.3.0 0.0.0.255

deny ip host 220.220.1.2 192.168.4.0 0.0.0.255

deny ip host 220.220.1.2 192.168.5.0 0.0.0.255

deny ip host 220.220.1.2 192.168.6.0 0.0.0.255

permit ip any any

Список доступу FROM-OUTSIDE містить інструкції обмеження доступу з зовнішньої мережі.

ip access-list extended FROM-OUTSIDE

permit icmp any host 220.220.1.2

permit tcp any host 220.220.1.2 eq www

deny ip any any

Демілітаризованої зони в мережі інтернет виділено адресу підмережі 220.220.1.0.

Зміст списків доступу, а також інші подробиці налаштувань маршрутизатора можна подивитися в додатку Е.

Вибор ПЗ безпеки для серверов та комп’ютерів

На всіх комп'ютерах встановлена ​​операційна система Windows 10 з останніми версіями оновлень. Як засіб антивірусного захисту на всі комп'ютери була встановлена ​​програма Norton AntiVirus.

**Norton AntiVirus** – це антивірус, націлений на забезпечення максимально комфортного використання ПК та мобільних пристроїв у повсякденному житті. Робота захисту проводиться у фоновому режимі та запобігає крадіжці особистих даних, блокує шахрайські веб-сайти та інформує про підозрілий контент у посиланнях.

**МЕ pfSense**

З переваг можна виділити докладний опис умов використання та простота застосування. Характерні особливості pfSense включають:

* Міжмережевий екран - фільтрація IP / портів, обмеження з'єднань, підтримка прийому і передачі даних, клінінг.
* Таблиця станів – за замовчуванням всі правила є статусними, є кілька конфігурацій для обробки станів.
* Балансування навантаження на сервер – вбудований LB, здатний розподілити навантаження між декількома бекендами сервера.
* NAT (трансляція мережевих адрес) - переадресація та відображення портів.
* HA (можливість забезпечення безперебійної роботи) - перехід на вторинний ресурс у разі відмови роботи первинного.
* Multi-WAN (глобальна обчислювальна мережа) – можливість використовувати більше одного підключення до Інтернету.
* VPN — підтримка IPsec та OpenVPN.
* Звітність – користувач здатний зберігати інформацію про відвідані та використані ресурси.
* Моніторинг у реальному часі.
* Динамічний DNS – використання кількох DNS-клієнтів одночасно.
* Ретрансляція та DHCP.

Функції міжмережевого екрана, що надаються безкоштовно. Крім того, у користувача також є можливість встановлювати пакети лише одним клацанням миші.

Наприклад:

* Безпека — stunner, snort, tinc, nmap, arpwatch
* Моніторинг — iftop, ntopng, softflowd, urlsnarf, darkstat, mailreport
* Мережа – netio, nut, Avahi
* Маршрутизація — frr, olsrd, routed, OpenBGPD
* Послуги – iperf, widentd, syslog-ng, bind, acme, imspector, git, dns-server.

**Snort** — вільна мережева система запобігання вторгненням (IPS) та виявлення вторгнень (IDS) з відкритим вихідним кодом, здатна виконувати реєстрацію пакетів та в реальному часі здійснювати аналіз трафіку в IP-мережах.

Виконує протоколювання, аналіз, пошук за вмістом, а також широко використовується для активного блокування або пасивного виявлення цілого ряду нападів та зондувань, таких як спроби атак на переповнення буфера, приховане сканування портів, атаки на веб-додатки, SMB-зондування та спроби визначення операційної системи. Програмне забезпечення в основному використовується для запобігання проникненню, блокування атак, якщо вони мають місце.

# ВИСНОВОК

У ході виконання курсового проекту була спроектована мережа для компанії «Odium», облаштовані робочі місця співробітникам, можливість відеоспостереження та сервери (веб-сервер, сервер компанії для зберігання всієї необхідної інформації та сервер записів відеоспостереження). Спроектовані плани приміщень та схеми мережі, а саме структурно-логічна топологія та змодельована мережа у програмі Cisco Packet Tracer. Крім того, в змодельованій мережі забезпечена безпека мережі, зокрема налаштований NAT, відокремлена ДМЗ для веб-сервера, обмежені права доступу з допомогою ACL. Налаштована DHCP роздача адресів. У майбутньому є можливість масштабувати та модернізувати спроектовану мережу шляхом додавання обладнання.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. <https://rozetka.com.ua/ua/tp_link_tl_sg1024d/p203087/?gclid=EAIaIQobChMIh73Zw_7o9AIVgbt3Ch3zXw8mEAAYASAAEgIKKPD_BwE>
2. <https://rozetka.com.ua/ua/cisco_sb_rv130_vpn_rv130_k9_g5/p6279693/>
3. <https://www.itbox.ua/ua/product/Tochka_dostupa_Wi-Fi_Mikrotik_RBcAPGi-5acD2nD-p325595/?utm_content=dsa+RU&gclid=EAIaIQobChMInrWJ7f_o9AIVied3Ch0D5A7-EAAYASAAEgI_w_D_BwE>
4. <https://rozetka.com.ua/ua/passivnoe-setevoe-oborudovanie/c1230965/50285=108805;50295=108825/?gclid=EAIaIQobChMI6Mnb9f_o9AIVA-N3Ch1X-ADAEAAYAiAAEgLWyPD_BwE>
5. <https://e-server.com.ua/konnektory-rozetki/rozetki/rozetka-1-port-utp-rj45-kat-5e-belaya-detail?gclid=EAIaIQobChMI5uqThYDp9AIVluR3Ch1RQAGlEAYYASABEgIPDvD_BwE>
6. <https://e-server.com.ua/konnektory-rozetki/konnektory-kolpachki/konnektor-rj45-utp-6-kat-8p8c-50-mkm-detail?gclid=EAIaIQobChMIl-PsuoDp9AIVhud3Ch0alwVYEAQYAiABEgKr3fD_BwE>
7. <https://e-server.com.ua/uk/patch-kordi/patch-kordi-utp/patch-kord-utp-cat5e-chornij-0-5m-eserver-detail>
8. <https://rozetka.com.ua/ua/318863410/p318863410/?gclid=EAIaIQobChMI08WwqoDp9AIVBLp3Ch1kpwu5EAYYAiABEgI2vvD_BwE>
9. https://rozetka.com.ua/ua/328868965/p328868965/?gclid=EAIaIQobChMI7PiYgYHp9AIViuJ3Ch0QQQE5EAQYAyABEgK25fD\_BwE
10. Оліфер В.Г., Оліфер Н.А. Комп'ютерні мережі. Принципи, технології, протоколи: Підручник для вузів. 4-у вид. - СПб .: "Пітер", 2010. - 944 с.
11. Таненбаум Е. - Комп'ютерні мережі. 4-е изд. - СПб.: Питер, 2003. - 992 с.
12. Шаньгина В.Ф. Захист інформації в комп'ютерних системах і мережах - Москва: ДМК Пресс, 2012 - 516 с.
13. Організація комп'ютерних мереж [Електронний ресурс]: підручник: для студ. спеціальності 121 «інженерія програмного забезпечення» та 122 «Комп'ютерні науки» / КПІ ім. Ігоря Сікорського; Ю. А. Тарнавський, І. М. Кузьменко. - Київ: КПІ ім. Ігоря Сікорського, 2018. - 259 с. - Режим доступу: http://ela.kpi.ua/bitstream/123456789/25156/1/Tarnavsky\_Kuzmenko\_Org\_Komp\_merej.pdf
14. Хоменко В.Г. Комп'ютерні мережі: Навчальний посібник / В. Г. Хоменко, М. П. Павленко. - Донецьк: ЛАНДОН-ХХІ, 2011. - 316 с.

# ДОДАТОК А

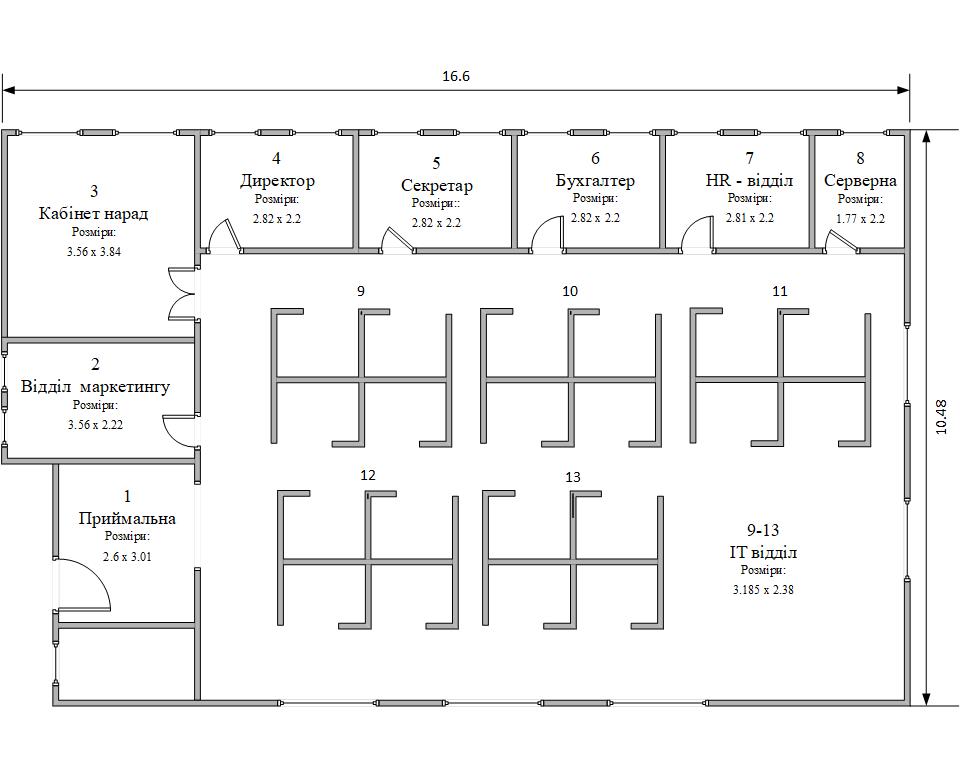


Рисунок 1 – План приміщення компанії

ДОДАТОК Б

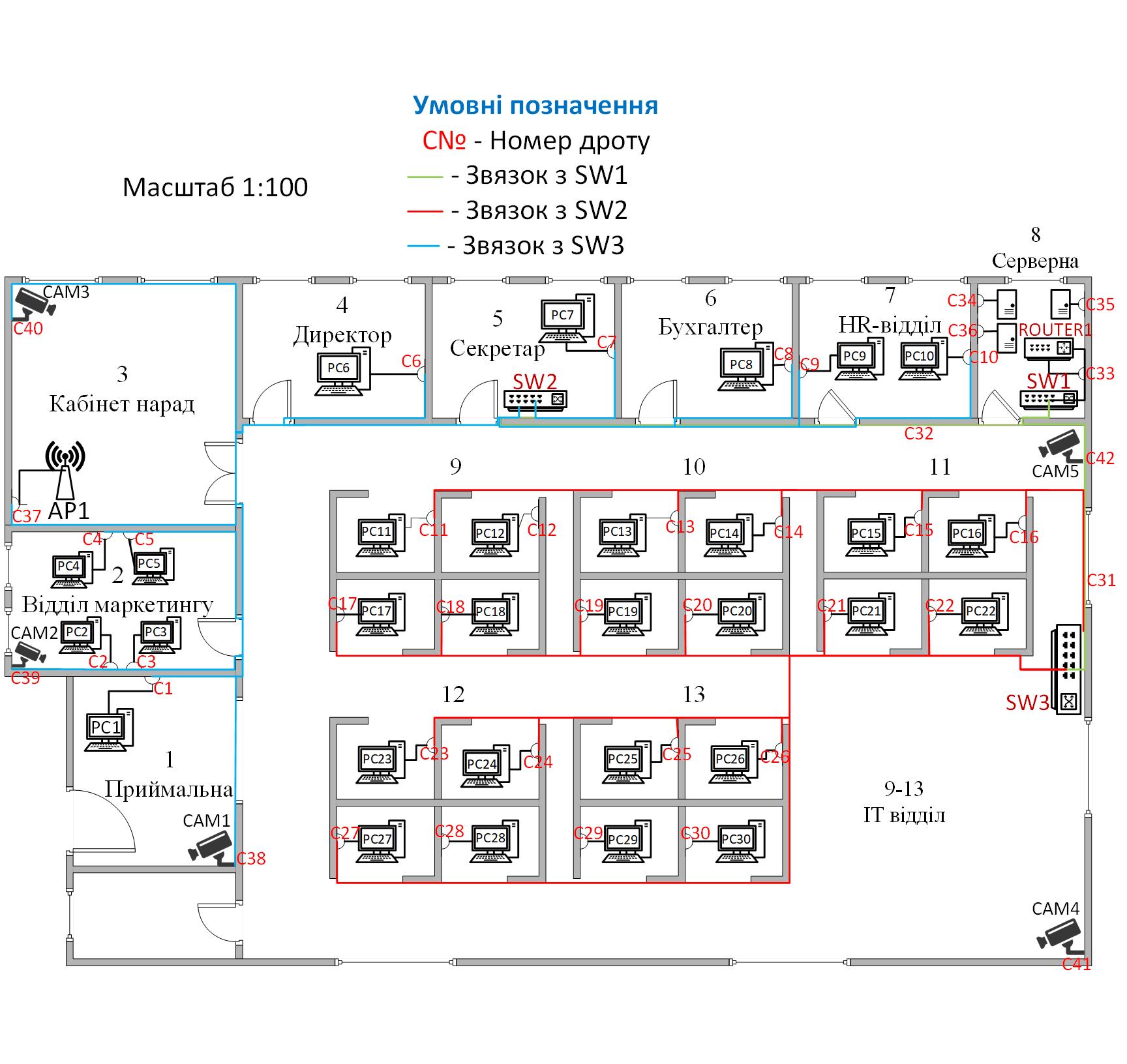


Рисунок 2 – Фізична топологія ЛОМ офісу компанії

ДОДАТОК В

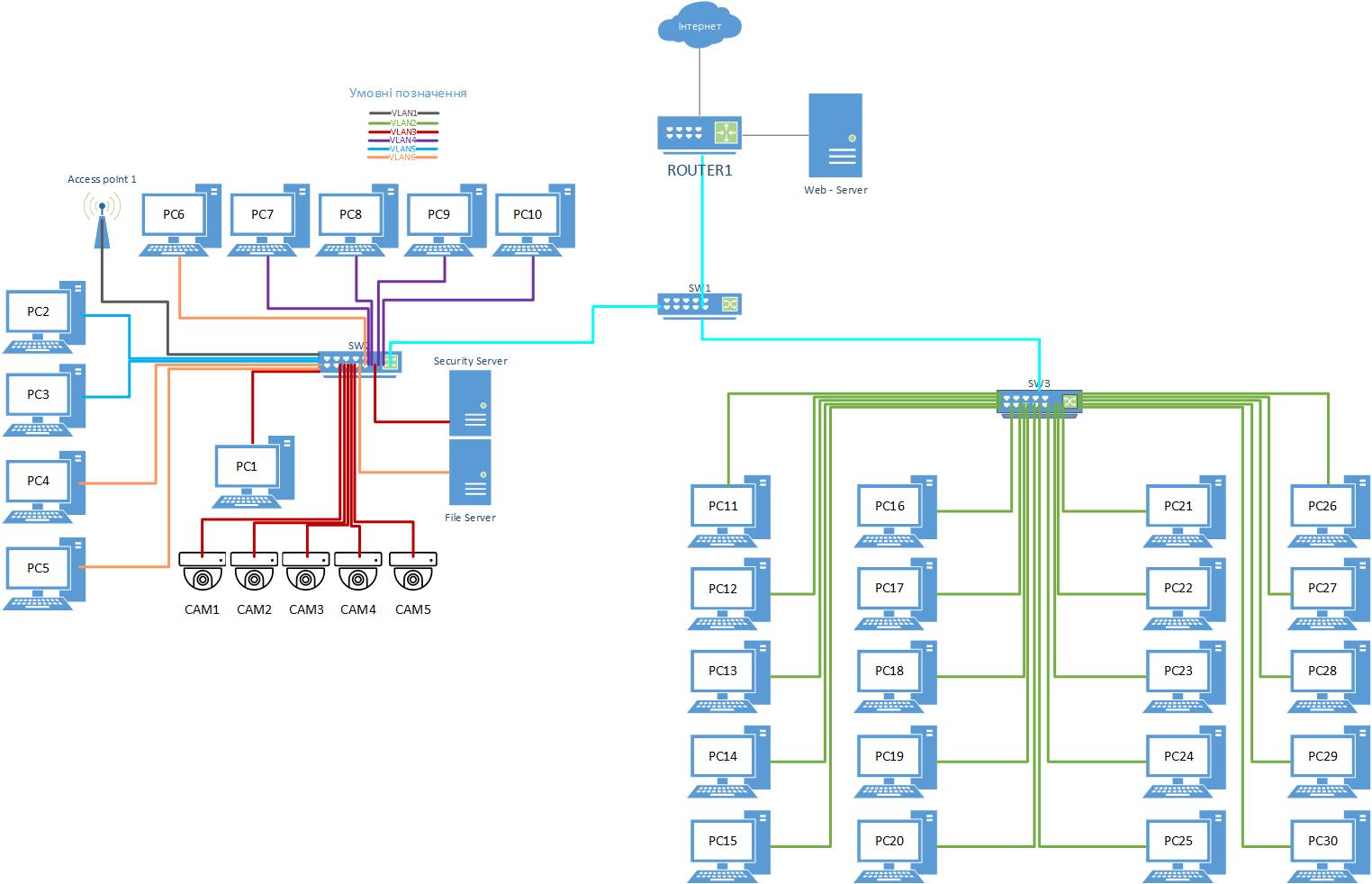


Рисунок 3 – Структурно-логічна схема

# ДОДАТОК Г

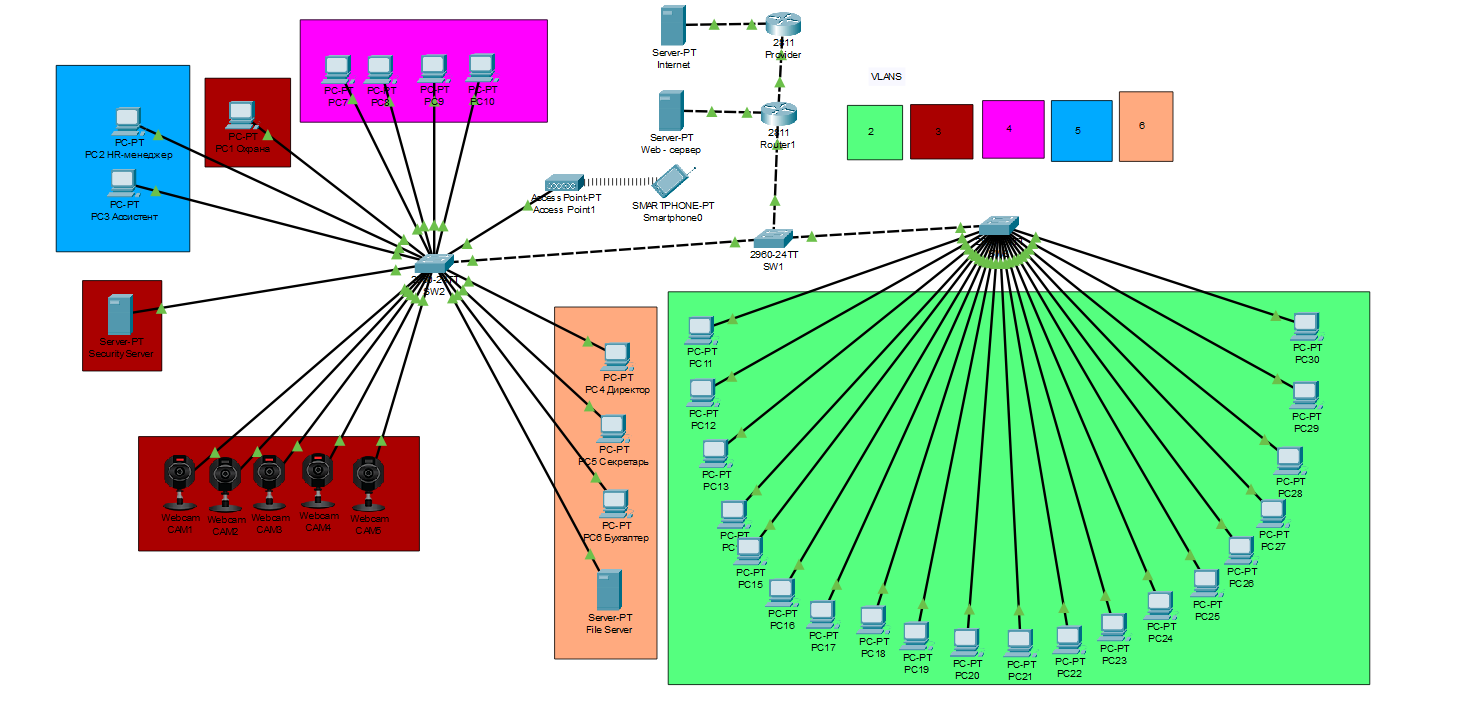


Рисунок 4 – Змодельована мережа в Packet Tracer

ДОДАТОК Д

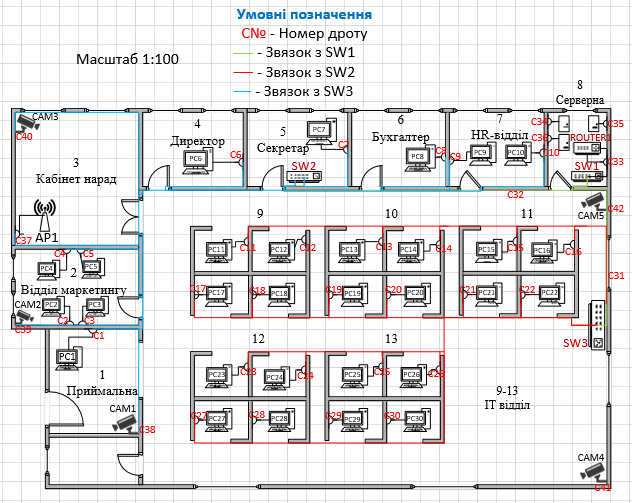


Рисунок 5 – Фізична топологія ЛОМ офісу компанії у масштабі 1:100

# ДОДАТОК Е

Router#sh r

Building configuration...

Current configuration : 5459 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname Router

!

!

!

!

ip dhcp excluded-address 192.168.2.1

ip dhcp excluded-address 192.168.4.1

ip dhcp excluded-address 192.168.5.1

!

ip dhcp pool IT\_green

network 192.168.2.0 255.255.255.0

default-router 192.168.2.1

ip dhcp pool HR\_blue

network 192.168.5.0 255.255.255.0

default-router 192.168.5.1

ip dhcp pool MR\_purple

network 192.168.4.0 255.255.255.0

default-router 192.168.4.1

!

!

!

no ip cef

no ipv6 cef

!

!

!

!

license udi pid CISCO2811/K9 sn FTX1017SJ3Z-

!

!

!

!

!

!

!

!

!

!

!

ip inspect name Inside-Outside http timeout 3600

ip inspect name Inside-Outside icmp timeout 10

ip inspect name Inside-Outside tcp timeout 3600

spanning-tree mode pvst

!

!

!

!

!

!

interface FastEthernet0/0

ip address 210.210.0.2 255.255.255.252

ip access-group FROM-OUTSIDE in

ip nat outside

duplex auto

speed auto

!

interface FastEthernet0/1

description dmz

ip address 220.220.1.1 255.255.255.252

ip access-group FROM-DMZ in

duplex auto

speed auto

!

interface FastEthernet1/0

ip address 192.168.1.1 255.255.255.0

ip access-group FOR-WIFI in

ip nat inside

ip inspect Inside-Outside in

duplex auto

speed auto

!

interface FastEthernet1/0.2

encapsulation dot1Q 2

ip address 192.168.2.1 255.255.255.0

ip access-group FOR-IT in

ip nat inside

!

interface FastEthernet1/0.3

encapsulation dot1Q 3

ip address 192.168.3.1 255.255.255.0

ip access-group FOR-SECUR2 in

ip access-group FOR-SECUR out

ip nat inside

!

interface FastEthernet1/0.4

encapsulation dot1Q 4

ip address 192.168.4.1 255.255.255.0

ip access-group FOR-MR in

ip nat inside

!

interface FastEthernet1/0.5

encapsulation dot1Q 5

ip address 192.168.5.1 255.255.255.0

ip access-group FOR-HR in

ip nat inside

!

interface FastEthernet1/0.6

encapsulation dot1Q 6

ip address 192.168.6.1 255.255.255.0

ip access-group FOR-ADMIN in

ip nat inside

!

interface Vlan1

no ip address

shutdown

!

ip nat inside source list FOR-NAT interface FastEthernet0/0 overload

ip classless

ip route 0.0.0.0 0.0.0.0 210.210.0.1

!

ip flow-export version 9

!

!

ip access-list standard FOR-NAT

permit 192.168.1.0 0.0.0.255

permit 192.168.2.0 0.0.0.255

permit 192.168.4.0 0.0.0.255

permit 192.168.5.0 0.0.0.255

permit 192.168.6.0 0.0.0.255

ip access-list extended FROM-DMZ

permit tcp host 220.220.1.2 any established

permit icmp host 220.220.1.2 any echo-reply

permit icmp host 220.220.1.2 any unreachable

ip access-list extended FROM-OUTSIDE

permit icmp any host 220.220.1.2

permit tcp any host 220.220.1.2 eq www

deny ip any any

ip access-list standard FOR-SECUR

permit host 192.168.6.2

deny any

ip access-list extended FOR-ADMIN

deny ip host 192.168.6.4 any

deny ip host 192.168.6.3 192.168.3.0 0.0.0.255

permit ip host 192.168.6.2 192.168.1.0 0.0.0.255

permit ip host 192.168.6.2 192.168.2.0 0.0.0.255

permit ip host 192.168.6.2 192.168.3.0 0.0.0.255

permit ip host 192.168.6.2 192.168.4.0 0.0.0.255

permit ip host 192.168.6.2 192.168.5.0 0.0.0.255

permit ip host 192.168.6.3 192.168.1.0 0.0.0.255

permit ip host 192.168.6.3 192.168.2.0 0.0.0.255

permit ip host 192.168.6.3 192.168.4.0 0.0.0.255

permit ip host 192.168.6.3 192.168.5.0 0.0.0.255

permit ip any any

ip access-list extended FOR-WIFI

permit ip 192.168.2.0 0.0.0.255 host 220.220.1.2

permit ip 192.168.2.0 0.0.0.255 host 210.210.1.2

deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255

deny ip 192.168.1.0 0.0.0.255 192.168.5.0 0.0.0.255

deny ip 192.168.1.0 0.0.0.255 192.168.6.0 0.0.0.255

permit ip any any

ip access-list extended FOR-HR

permit ip 192.168.5.0 0.0.0.255 host 220.220.1.2

permit ip 192.168.5.0 0.0.0.255 host 210.210.1.2

permit ip 192.168.5.0 0.0.0.255 host 192.168.6.99

permit ip 192.168.5.0 0.0.0.255 host 192.168.6.2

permit ip 192.168.5.0 0.0.0.255 host 192.168.6.3

deny ip 192.168.5.0 0.0.0.255 192.168.1.0 0.0.0.255

deny ip 192.168.5.0 0.0.0.255 192.168.2.0 0.0.0.255

deny ip 192.168.5.0 0.0.0.255 192.168.3.0 0.0.0.255

deny ip 192.168.5.0 0.0.0.255 192.168.4.0 0.0.0.255

deny ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

permit ip any any

ip access-list extended FOR-MR

permit ip 192.168.4.0 0.0.0.255 host 220.220.1.2

permit ip 192.168.4.0 0.0.0.255 host 210.210.1.2

permit ip 192.168.4.0 0.0.0.255 host 192.168.6.99

permit ip 192.168.4.0 0.0.0.255 host 192.168.6.2

permit ip 192.168.4.0 0.0.0.255 host 192.168.6.3

deny ip 192.168.4.0 0.0.0.255 192.168.1.0 0.0.0.255

deny ip 192.168.4.0 0.0.0.255 192.168.2.0 0.0.0.255

deny ip 192.168.4.0 0.0.0.255 192.168.3.0 0.0.0.255

deny ip 192.168.4.0 0.0.0.255 192.168.4.0 0.0.0.255

deny ip 192.168.4.0 0.0.0.255 192.168.6.0 0.0.0.255

permit ip any any

ip access-list extended FOR-IT

permit ip 192.168.2.0 0.0.0.255 host 220.220.1.2

permit ip 192.168.2.0 0.0.0.255 host 210.210.1.2

permit ip 192.168.2.0 0.0.0.255 host 192.168.6.2

permit ip 192.168.2.0 0.0.0.255 host 192.168.6.3

deny ip host 192.168.6.99 192.168.2.0 0.0.0.255

deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

deny ip 192.168.2.0 0.0.0.255 192.168.2.0 0.0.0.255

deny ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255

deny ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255

deny ip 192.168.2.0 0.0.0.255 192.168.6.0 0.0.0.255

permit ip any any

!

!

!

!

!

!

line con 0

!

line aux 0

!

line vty 0 4

login

!

!

!

end