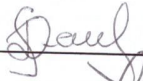


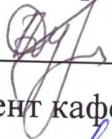
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

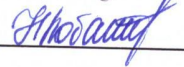
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект системи відеоспостереження для
підприємства»

Виконав студент 4-го курсу, групи КІ-3
спеціальності 123 «Комп'ютерна інженерія»

 А.О. Дацюк
Керівник к.т.н., доцент, доцент кафедри БІ та Т

 О.Ф. Дубина
Рецензент к.т.н., доцент, доцент кафедри КІ та КБ

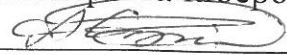
 Н.М. Лобанчикова

Житомир – 2021

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

ЗАТВЕРДЖУЮ

Зав. кафедри комп'ютерної
інженерії та кібербезпеки

 Єфіменко А.А.

« 12 » 04 20 21 р.

ЗАВДАННЯ
на випускню кваліфікаційну роботу

Студента Дацюка Андрія Олександровича

Тема роботи: Проект системи відеоспостереження для підприємства

Затверджена Наказом університету від «12» квітня 20 21 р. № 133\С

Термін здачі студентом закінченої роботи 18 серпня 2021 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження)

модель розробити на основі Cisco Packet Tracer

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1			
2			
3			

Керівник  Дубина О.Ф.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Видача завдання	12.04.21	
2	Розробка плану роботи	14.04.21 – 18.04.21	
3	Розробка розгорнутого плану	19.04.21 – 20.04.21	
4	Подача чернетки керівнику для перевірки	24.04.21	
5	Подача чистовика керівнику	27.04.21 – 29.05.21	
6	Затвердження графічних матеріалів у керівника	01.06.21 – 04.06.21	
7	Проведення попереднього захисту	05.06.21	
8	Отримання відгуку керівника	15.06.21	
9	Допуск завідувача кафедри	16.06.21	
10	Подання роботи на рецензування	16.06.21	
11	Захист		

Студент  Дацюк А.О

Керівник  Дубина О.Ф

РЕФЕРАТ

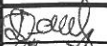
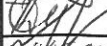
Випускна робота бакалавра присвячена розробці проекту системи відеоспостереження для підприємства.

Метою роботи є розробка за допомогою Cisco Packet Tracer проекту системи відеоспостереження, що матиме можливість віддаленого доступу управління.

В роботі визначено основні завдання на розробку системи, проаналізовано аналоги розробленої системи. Наведено лістинги налаштувань обладнання, алгоритм роботи виконавчого пристрою, показано топологію мережі та її проект за генпланом, налагоджено віддалений доступ до камер відеоспостереження. Також наводяться результати тестування системи.

Пояснювальна записка до випускної бакалаврської роботи містить 87 сторінок, 83 рисунки, 5 таблиць, 2 додатка та 24 літературних джерела.

КЛЮЧОВІ СЛОВА: СКУД, камери, відеоспостереження, мережа, система, захист, Cisco, схема, сервер.

					КІК.КР.Б – 123 – 05 – ПЗ		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Дацюк А.О.		22.06.21	Проект системи відеоспостереження для підприємства		
Керівник		Дубина О.Ф.		22.06.21			
Рецензент		Лобанчикова Н.М.		22.06.21			
н. контр.							
Зав. каф.		Сфіменко А.А.		22.06.21	Пояснювальна записка		
					Лім.	Арк.	Аркушів
						4	
					Житомирська політехніка Група КІ-3		

ABSTRACT

The bachelor's thesis is devoted to the development of a video surveillance system project for the company.

The aim of the work is to develop with the help of Cisco Packet Tracer a project of a video surveillance system that will have the ability to remotely control.

The main tasks for system development are defined in the work, analogues of the developed system are analyzed. Listings of equipment settings, algorithm of operation of the executive device are given, the topology of the network and its project according to the general plan are shown, remote access to video surveillance cameras is adjusted. The results of system testing are also given.

The explanatory note to the bachelor's thesis contains 85 pages, 83 figures, 5 tables, 2 appendices and 24 references.

KEY WORDS: ACS, cameras, video surveillance, network, system, protection, Cisco, circuit, server.

ЗМІСТ

РЕФЕРАТ.....	ERROR! BOOKMARK NOT DEFINED.
ABSTRACT	5
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	7
ВСТУП.....	8
РОЗДІЛ 1. ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ РОЗРОБКИ СИСТЕМИ	
ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ПІДПРИЄМСТВА.....	10
1.1. АНАЛІЗ СУЧАСНИХ СИСТЕМ ОХОРОНИ.....	10
1.2. АНАЛІЗ СУЧАСНИХ СИСТЕМ КУД.....	19
1.3. ВИБІР ТА АНАЛІЗ КАМЕР ВІДЕОСПОСТЕРЕЖЕННЯ	25
1.4. АНАЛІЗ НЕОБХІДНОГО ЗАХИСТУ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ	33
1.5. ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ ТА ВИСУВАННЯ ВИМОГ ДО ВІДЕОСПОСТЕРЕЖЕННЯ ...	41
Висновки до розділу 1	44
РОЗДІЛ 2. РОЗРОБКА ПРОЕКТУ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ	
ПІДПРИЄМСТВА	45
2.1. ПРОЕКТ МЕРЕЖІ ПІДПРИЄМСТВА	45
2.2. ВИБІР ОБЛАДНАННЯ	48
2.3. РОЗРОБКА СХЕМИ АДРЕСАЦІЇ МЕРЕЖІ	56
Висновки до розділу 2	58
РОЗДІЛ 3. НАЛАГОДЖЕННЯ МЕРЕЖІ ПІДПРИЄМСТВА.....	
3.1. БАЗОВЕ НАЛАГОДЖЕННЯ ПРИСТРОЇВ МЕРЕЖІ.....	59
3.2. НАЛАГОДЖЕННЯ ПРОМИСЛОВОЇ МЕРЕЖІ ТА ЇЇ ЗАХИСТУ	64
3.3. ТЕСТУВАННЯ НАЛАШТУВАНЬ.....	74
Висновки до розділу 3	85
ВИСНОВКИ.....	86
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	88
ДОДАТКИ	91
ДОДАТОК А	92
ДОДАТОК Б	94

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CCTV – Closed-circuit television - системи закритої трансляції телебачення.

СКУД – Система контролю і управління доступом.

IP – Internet Protocol.

APM – Автоматизоване робоче місце.

BPM – Віддалене робоче місце.

VLAN – Virtual Local Area Network.

VPN – Virtual Private Network.

PoE – Power over Ethernet.

RFID – Radio Frequency Identification.

ВСТУП

Система контролю доступу - це сукупність програмно-технічних засобів та чітко сформованої системи управління рухом персоналу та часу його перебування на об'єкті. Основними місцями для встановлення систем контролю доступу на підприємствах є прохідні, офісні, приміщення особового призначення та пункти в'їзду та виїзду автотранспорту.

Система контролю доступу може бути автономною або однієї із складових інтегрованої системи безпеки будівлі. Вона дозволяє значно підвищити ефективність контролю для запобігання несанкціонованому доступу сторонніх на територію підприємства. Для швидкого та безперервного проходження персоналу в прохідній встановлюються електромеханічні турнікети. Співробітники проходять через турнікет, прикладаючи до зчитувача карти доступу, що дозволяє виключити людський фактор при перевірці пропусків та реєстрації запізнень на роботу, фактично зводячи до нуля можливості помилки та зловживання.

Захист від передачі пропуску іншій особі реалізується наступним чином: система не дозволить два рази перейти на підприємство за одним пропуском без здійснення виходів. Система контролю доступу постійно забезпечує контроль за порядком на об'єкті.

Автоматизована система контролю доступу відслідковує всі переміщення співробітників на території підприємства.

Звіти про запізнених, людей, які не вийшли на роботу або вийшли з роботи раніше часу можуть формуватися як щоденно, так і за будь-який проміжок часу. Програмовий модуль обліку робочого часу забезпечує автоматизований облік робочого часу при організації багатозмінних та змінних графіків будь-якої складності, автоматично формує таблицю встановлених форм, у відповідності до індивідуальних графіків роботи кожного співробітника. Модуль видачі пропусків дозволяє формувати карту доступу у вигляді пропуску: з фотографією, ПІБ, посадою, назвою підрозділу.

Співробітникам та відвідувачам можуть задаватися індивідуальні права доступу на об'єкті або в приміщеннях. Доступ може обмежуватися:

за часом - кожному співробітнику задається індивідуальний тимчасовий графік доступу до об'єкта;

за статусом - для кожного співробітника можна визначити приміщення, в які він має право входу та право постановки/зняття приміщень з охрани.

Для відвідувачів та тимчасових співробітників у системі передбачено разові та тимчасові пропуски. Пропуск із закінченим терміном дії автоматично забороняється в системі.

Системи відеоспостереження дозволяють здійснювати відеоконтроль за ситуацією на об'єкті. Системи відеоспостереження дають унікальну можливість відеореєстрації того, що відбувається, контролю та запису на цифрові носії інформації або у хмарні середовища.

Існують стандартні системи відеоспостереження та комп'ютерні системи відеоспостереження. Останні рахуються найбільш актуальними та відрізняються великою функціональністю у сукупності з простотою в експлуатації. У залежності від типу об'єкта комплектація системи відеоспостереження варіюється. Наприклад, при встановленні системи відеоспостереження можна використовувати різні види відеокамер.

РОЗДІЛ 1. ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ РОЗРОБКИ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ПІДПРИЄМСТВА

1.1. Аналіз сучасних систем охорони

Надійний спосіб забезпечити безпеку приміщення – установка охоронної системи[1]. І якщо в квартирі в основному застосовується тільки один її тип – захист від проникнення, – то в офісах система безпеки може включати різні підсистеми: спостереження за підходами та під'їздами до будівлі, охорона периметра, охорона внутрішніх приміщень. Існує чотири основних види охоронних систем:

- ¶ СОТС – система охорони і тривожної сигналізації. При проникненні в приміщення спрацьовують тривожні датчики, і на пульт охоронної служби надходить сигнал. Це найпоширеніший вид охорони квартир і офісів в багатоповерхових будівлях.
- ¶ СКУД – система контролю і управління доступом. З її допомогою можна управляти замками, приводами зовнішніх воріт, здійснювати контроль доступу в приміщення, куди вхід сторонніх небажаний.
- ¶ СОВ – система охоронного відеоспостереження, що здійснюється за допомогою спеціальних камер.
- ¶ СІТУ – система інженерно-технічного укріплення. До неї відноситься в тому числі висота огорожі, міцність вікон та брам, надійність дверних замків, наявність бункера або потайних укріплених кімнат - все, що може ускладнити зловмисникам доступ в приміщення.

Система охорони і тривожної сигналізації

За допомогою системи охорони і тривожної сигналізації можна здійснювати цілодобовий контроль за будь-яким об'єктом – квартирою, котеджем, офісом, складом і т.д. СОТС[2] є надійним способом захистити об'єкт, що охороняється від проникнення.

					КІК.КР.Б – 123 – 05 – ПЗ	
						10

СОТС ділиться на два типи:

Пасивна система охоронної сигналізації. При несанкціонованому вторгненні на територію, що охороняється подається світловий і звуковий сигнал тривоги. При цьому ні на пульт охорони, ні власнику тривожний сигнал не надходить. Система розрахована тільки на психологічний вплив на злочинців, що не завжди може бути ефективним.

Активна СОТС. В приміщенні встановлюють датчики. Вони автоматично дають тривожний сигнал на пульт охоронної організації після того, як стороння людина відкриє двері і не зніме приміщення з сигналізації. Співробітники Чопа відразу ж візьмуть заявку і протягом декількох хвилин приїдуть на місце. Також активна охоронна система включає тривожну кнопку. Але вона спрацьовує тільки при безпосередньому натисканні. Чи не вийде активізувати її віддалено. Сигнал також йде на пульт. За рахунок джерел безперебійного живлення система працює і захищає об'єкт навіть при виключенні електроживлення.

Зазвичай СОТС має на увазі перелік взаємодіючих пристроїв:

- ¶ датчики;
- ¶ пристрої оповіщення;
- ¶ пульт керування;
- ¶ пристрій контролю стану сповіщувачів і кабельних ліній в СОТС;
- ¶ безперебійні джерела живлення.

Одним з основних елементів СОТС є датчики. Саме вони відповідають за оперативне реагування системи на вторгнення(див. рис. 1.1).

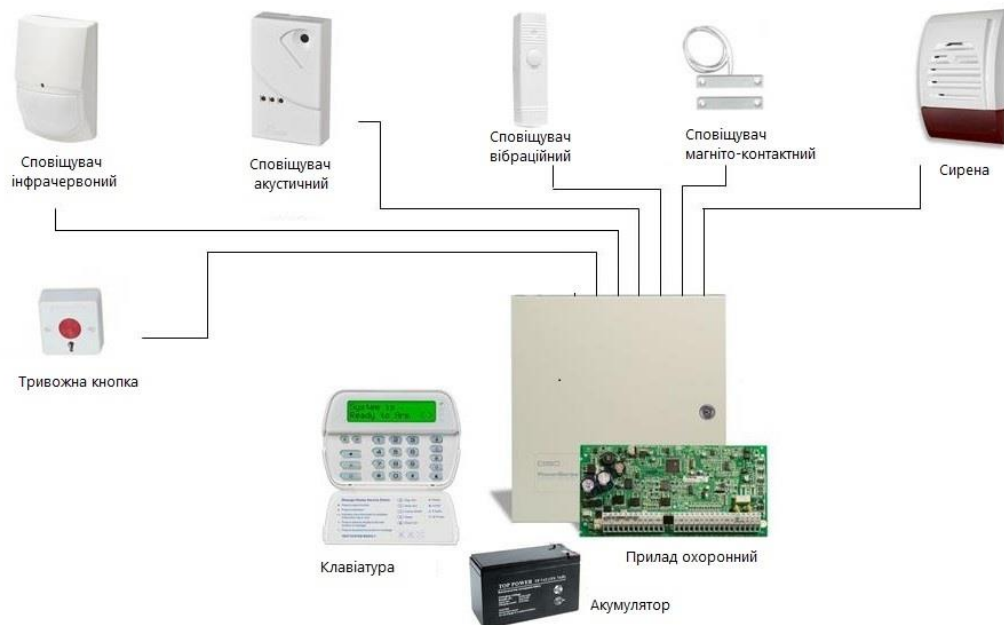


Рисунок 1.1 - Приклад СОТС

Датчики руху і присутності автоматично включають / вимикають освітлення в приміщенні в залежності від інтенсивності природного потоку світла і / або присутності людей. Принцип їх дії заснований на реєстрації зміни інфрачервоного (ІЧ) випромінювання, викликаного переміщенням або діяльністю людини. Ємнісний датчик створює в об'єкті, що охороняється поле з певною ємністю. При попаданні в поле будь-якого предмета ємність поля змінюється, викликаючи спрацювання сигналізації.

Вібродатчики. Принцип дії заснований на реєстрації механічних коливань охоронного інженерного загородження, на якому встановлюється чутливий елемент, що перетворює ці коливання в електричний сигнал, який обробляється в аналізаторі за спеціальним алгоритмом, відповідно до якого визначається сигнал «тривога». Як чутливий елемент можуть виступати як спеціалізований чутливий кабель, що володіє трибоелектричних або мікрофонними властивостями, так і точкові вібродатчики

Система контролю і управління доступом

Сучасні автоматизовані СКУД призначені для захисту від несанкціонованого доступу в приміщення або певні зони і для ідентифікації осіб, які мають право доступу. Сучасні СКУД представлені різноманітними технологіями:

безконтактні перезаписуючі карти, біометричні системи, електронні замки і циліндри, енергозберігаючі контролери, системи енергозбереження.

СКУД складається з декількох основних елементів: контролера, зчитувача, ідентифікатора і виконавчого пристрою. Контролер є керівним елементом системи який отримує та передає сигнали. Зчитувач отримує інформацію, записану на ідентифікатор, і передає її в контролер на обробку. Ідентифікатори бувають таких видів:

- ¶ електронний ключ;
- ¶ карта доступу.

Ідентифікатор доступу може бути у вигляді зчитувача радужної оболонки ока чи зчитувача відбитків пальців.

Після ідентифікації з контролера подається команда виконавчому пристрою - дозволити допуск чи ні (див. рис. 1.2).

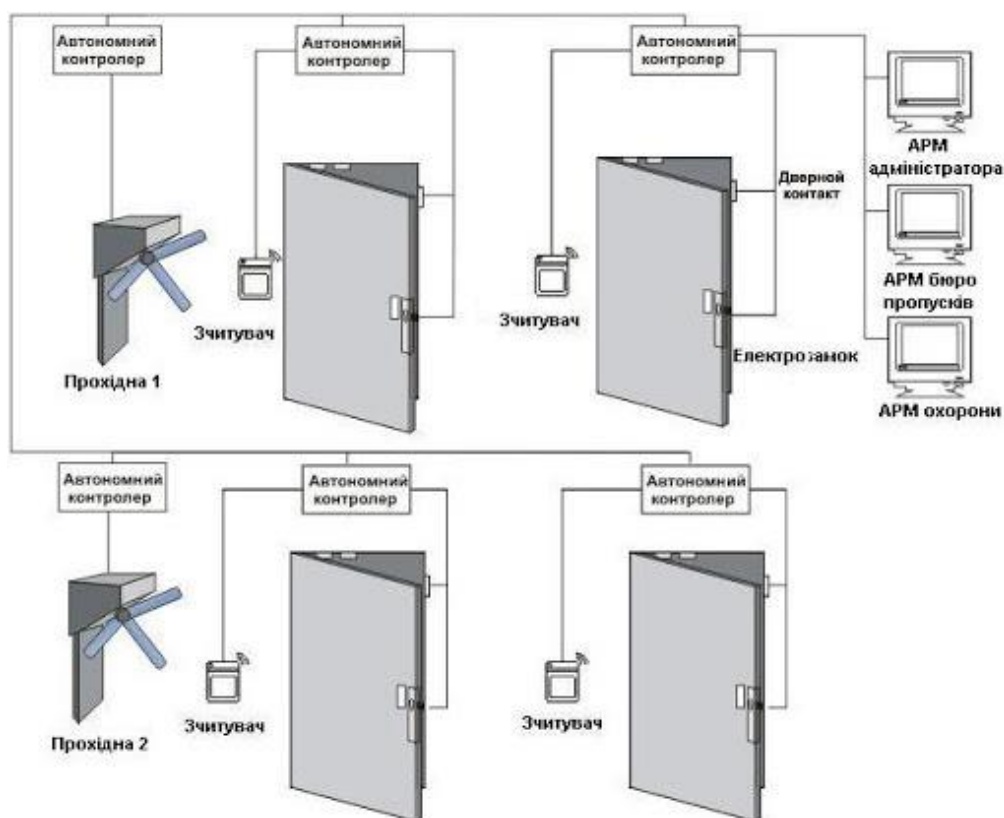


Рисунок 1.2 - Приклад СКУД

Система охоронного відеоспостереження

Система охоронного відеоспостереження (ззовні) призначена для візуального спостереження за об'єктом, що охороняється за допомогою

відеокамер. Охоронне відеоспостереження дозволяє стежити одночасно за одним або кількома об'єктами. Камери відеоспостереження можна встановити як всередині приміщення, так і зовні. Завдання охоронного відеоспостереження складається в наочному поданні відеоінформації про оперативну обстановку на контрольованому об'єкті. Головне завдання відеоспостереження – забезпечення безпеки об'єкта шляхом візуального спостереження без передачі інформації в зовнішні загальнодоступні мережі.

За способом обробки сигналу системи діляться на аналогові, комбіновані і цифрові.

За способом передачі відеосигналу СОВ можуть бути дротяними і бездротовими. Бездротові системи можна встановлювати в самих важкодоступних місцях. Дротяні, у свою чергу, більш дешеві та надійніші. Приклад СОВ зображено на рис. 1.3:

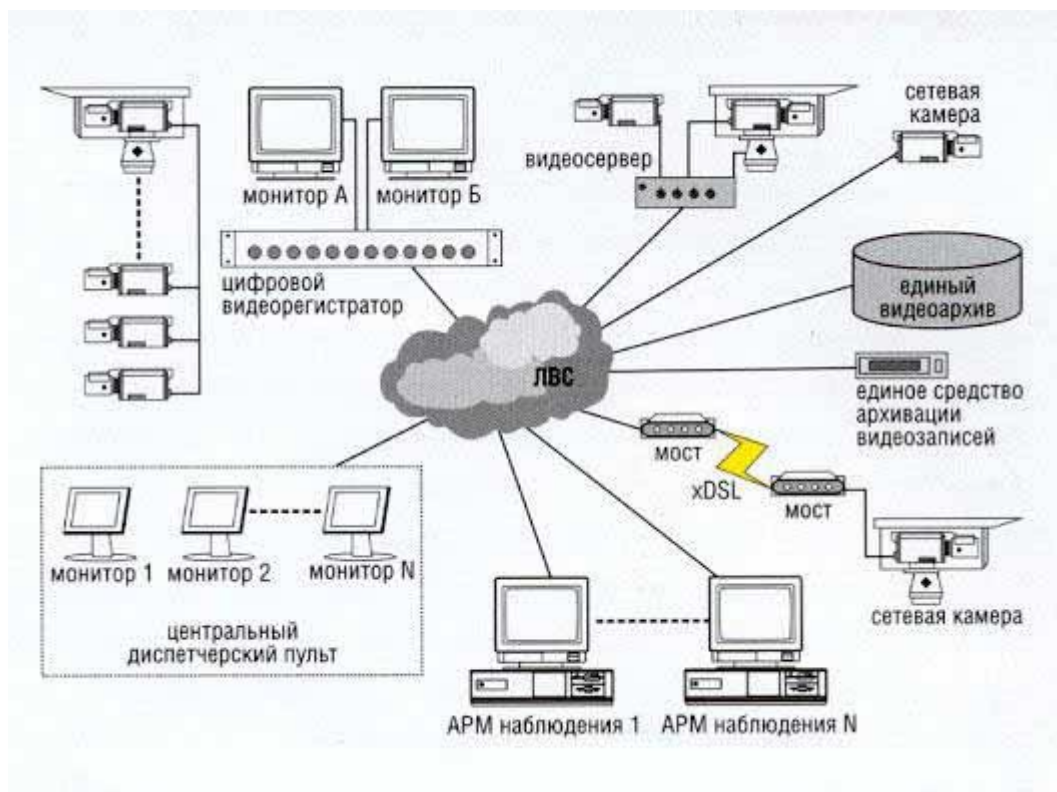


Рисунок 1.3 - Приклад СОВ

Камери СОВ також підрозділяються на види в залежності від самих різних технічних характеристик. Дві найбільших категорії – це цифрові і аналогові камери. Цифрові, або IP-камери, використовують у своїй роботі цифровий

сигнал, їх досить просто інтегрувати в мережу, тому цифрове відеоспостереження легко можна масштабувати при необхідності. Роздільна здатність в цифрових камерах значно вище, ніж в аналогових, але іноді у високій роздільній здатності просто немає необхідності, тим більше що воно вимагає ємних систем зберігання даних.

Крім того, камери СОВ можуть бути зовнішніми і внутрішніми - від типу залежить місце їх установки. За особливостями конструкції камери можна розділити на корпусні, модульні, купольні, мініатюрні і відеоглазки.

Корпусні відеокамери.

У системах відеоспостереження корпусні камери займають одну з лідируючих позицій. У ряді випадків вони можуть не комплектуватися об'єктивами, мережевими адаптерами або кронштейнами.

На відміну від модульних пристроїв корпусні відеокамери оснащуються різними органами управління і зовнішніми інтерфейсами (роз'ємами), що дозволяє зробити процес установки і настройки більш зручним. Корпусні камери можуть випускатися як з вбудованими, так і зі змінними об'єктивами. Приклад корпусної камери зображено на рис. 1.4.



Рисунок 1.4 - Корпусна IP-відеокамера Hikvision DS-2CD4012F-A

У більшості випадків корпусні камера відеоспостереження комплектується ПЗС матрицею високої чутливості. Це сприяє отриманню детального відеоряду контрольованого об'єкта. Більшість камер має досить широкі функціональні можливості. Система настройки дозволяє змінити наступні параметри в автоматичному і / або ручному режимі:

- ¶ шумозаглушення;
- ¶ компенсація фонові засвітки;

- ¶ маскування;
- ¶ програмна або апаратна детекція руху і т.п.

Модульні відеокамери.

Модульні, вони ж безкорпусні камери відеоспостереження є платою з закріпленим на ній об'єктивом (див. рис. 1.5). При непоказному зовнішньому вигляді вони можуть мати дуже непоганими технічними характеристиками.



Рисунок 1.5 - Модульна відеокамера Oltec AHD-113-3.6

Дійсно, параметри і функціональні можливості відеокамер пріоритетно визначаються:

- ¶ матрицею;
- ¶ схемою обробки сигналу;
- ¶ об'єктивом.

Всі ці компоненти в бескорпусном виконанні присутні, а значить за характеристиками такі камери потенційно нічим не поступаються іншим видам. Таким чином діапазон можливостей цих камер дуже широкий, об'єднує їх лише необхідність установки в відповідний корпус. Теоретично при внутрішній установці можна обійтися і без нього, але періодично видаляти з плати пил може бути важко.

Купольні відеокамери.

Купольна відеокамера – це камера, яка встановлена в спеціальний корпус, який за формою нагадує купол (див. рис. 1.6). В англійській мові такі камери мають інше найменування – dome. Купольні камери діляться на поворотні і стаціонарні, а також можуть виготовлятися з додатковим захистом, якщо необхідний захист від атмосферних опадів або вандалізму. Купольні

відеокамери широко застосовуються в відеоспостереження, так як забезпечують максимальний огляд території, що охороняється.



Рисунок 1.6 - Купольна відеокамера Hikvision DS-2CE76H8T-ITMF

Стационарні купольні камери використовуються в місцях, де вони повинні бути максимально непомітними. Сучасні технології дозволяють виготовляти мініатюрну оптику, так що купол таких пристроїв може мати діаметр близько 5 см. Зазвичай їх встановлюють так, щоб забезпечити максимальний огляд території, що охороняється. Основна сфера застосування стаціонарних купольних камер відеоспостереження - магазини і торгові центри.

Мініатюрні відеокамери.

Коли необхідно встановити систему відеоспостереження за будинком або зовнішньої території, використовуються мініатюрні відеокамери. Назва цих камер говорить сама за себе - маленький розмір дає можливість заховати їх від сторонніх очей. Одна з різновидів малогабаритних камер - безкорпусні міні камери. Ці пристрої досить прості в застосуванні. Але головна їхня перевага в тому, що безкорпусні камери набагато простіше зробити непомітними для зломисників, ніж звичайні відеокамери маленьких габаритів. Вони піддаються маскуванню і легко монтуються в предмети інтер'єру (див. рис. 1.7).



Рисунок 1.7 - Мініатюрна відеокамера Ambertek RS101

Область застосування міні відеокамер досить широка. Їх охоче використовують керівники великих підприємств з метою спостереження за діяльністю співробітників. Нерідко міні відеокамери встановлюються в магазинах і супермаркетах. Таким чином їх власники намагаються захистити товар, що продається від крадіжок.

Відеоочки.

Відеоочко – це максимально просте обладнання, призначене для підвищення безпеки на об'єкті. Він дозволяє користувачеві конкретно знати, хто прийшов в гості, навіть якщо сам знаходиться на іншому континенті. Завдяки технічному прогресу і старанням відомих брендів, подібне компактний пристрій знайшло масу сенсорів, датчиків, мікрофонів і має можливість передавати дані через GSM - мобільну лінію оператора.

Відеоочко є мініатюрним охоронним приладом (див. рис. 1.8), який аналогічно встановлюється в місце для стандартного вічка і записує все, що відбувається, повідомляючи власникові про гостей або інші події, які трапилися на об'єкті. Всі дані зберігаються на карту Micro-SD. Це гарантує, що не буде втрати даних під час якихось збоїв і т.д.



Рисунок 1.8 - "R9" (dark grey) Wi-Fi Відеоочко

Завжди є можливість подивитися, що відбувається біля дверей, наприклад, з комп'ютера або смартфона, куди буде надходити сигнал з відеоочка. Конструктивне відміну від іншого обладнання в тому, що монтується відеоочко безпосередньо у входних дверях, тому ніхто не буде знати, що за ними ведеться цілодобове відеоспостереження. За допомогою подібного обладнання користувач зможе убезпечити себе і власне майно від вандалів і злодіїв.

Система інженерно-технічної укріпленості

Система інженерно-технічної укріпленості[2] (СІТУ) будь-якої будівлі – це захист від несанкціонованого проникнення шляхом посилення його конструктивних елементів. В ідеалі кожна СІТУ повинна мати 5 охоронюваних зон:

- периметр території;
- периметр будівлі;
- приміщення, доступні для відвідувачів;
- приміщення, доступні тільки для господарів будинку;
- приміщення з максимально обмеженим доступом – збройові, сейфові.

В якості засобів захисту периметра ділянки використовуються паркани, ворота, пропускні пункти, шлюзи для перевірки і пропуску транспортних засобів. Для захисту будівлі - віконні решітки та ґрати для підсилення стін, тамбури, оснащені засобами безпеки, укріплені двері, замки(див. рис. 1.9).

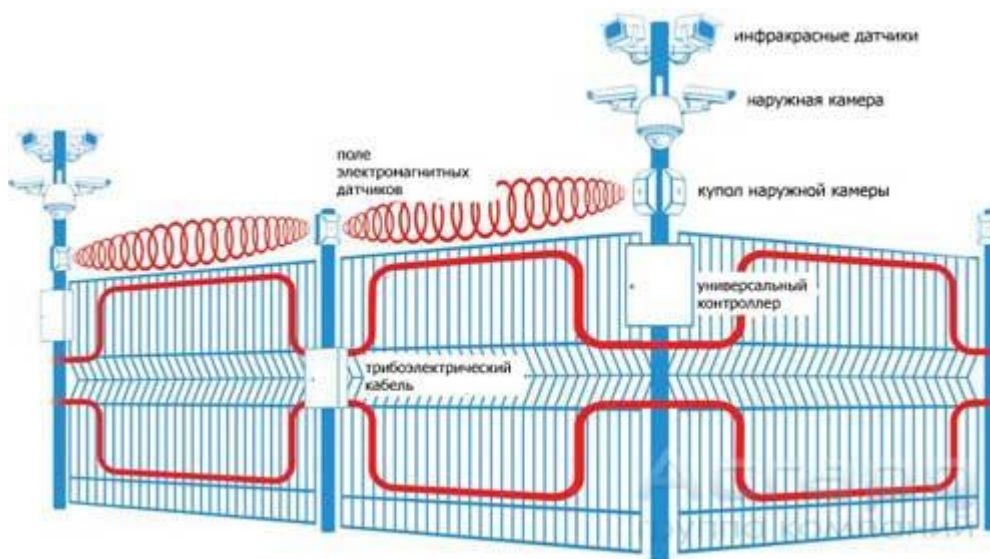


Рисунок 1.9 - Пример СІТУ

1.2. Аналіз сучасних систем КУД

Сучасні СКУД дозволяють вирішувати широкий спектр завдань[4], таких як:

- ¶ захист від промислового шпигунства;
- ¶ захист від крадіжки;

- ¶ протидія саботажу;
- ¶ захист від навмисного пошкодження або руйнування матеріальної власності організації;
- ¶ облік робочого часу;
- ¶ контроль своєчасності догляду і приходу співробітників;
- ¶ захист конфіденційної інформації від несанкціонованого доступу;
- ¶ контроль потоку відвідувачів на об'єкті;
- ¶ контроль в'їзду та виїзду транспорту.

Основне призначення будь-якої СКУД – обмеження доступу на режимні об'єкти і сховища даних. Крім того, такого роду системи можуть успішно здійснювати функції обліку робочого часу, контролю трудової дисципліни, збереження матеріальних цінностей та ін. В цілому СКУД є сукупністю програмно-технічних засобів, а також організаційно-методичних засобів, що дозволяють вирішити перераховані вище завдання.

Як перегороджуючі бар'єри, найбільш часто використовуваних в складі СКУД, можна виділити наступні: турнікети звичайні і настінні, турнікети в коридорах, шлюзові кабінки, автоматичні хвіртки, роторні турнікети, що обертаються двері, дорожні блокіратори, шлагбауми, паркувальні системи, круглі розсувні двері, трьохштангові турнікети, повнозростові турнікети, розсувні турнікети.

Дуже важливим є питання про можливість інтеграції СКУД з будь-якою системою безпеки з використанням відкритого протоколу. Використовуючи входи і виходи в інформаційних системах за допомогою конекторів, можна отримувати і вилучати дані з систем для їх спільної взаємодії.

Розподіл системи контролю та управління доступом на класи виконується на основі порівняльного аналізу ряду їх функціональних можливостей: оперативного перепрограмування, рівня секретності, автоматичної ідентифікації, автоматичного збору та аналізу даних, розмежування повноважень користувачів по доступу, вибіркової роздруковки даних, надійного

механічного замикання точок доступу з можливістю аварійного ручного відкриття.

Зазвичай установку відеоспостереження іСКУД[5] проводять одночасно. В результаті створюється єдиний комплекс, що дозволяє розпізнавати і пропускати співробітників, які перебувають в заздалегідь складеній базі даних. Іноді їх монтують окремо.

Всі системи контролю та управління доступом поділяють на 4 класи:

СКУД 1 класу – системи малої місткості, що володіють обмеженим функціоналом. Працюють в автономному режимі і здійснюють допуск всіх осіб, які мають ідентифікатор. Такі системи використовують ручне або автоматичне керування виконавчими пристроями, а також світлову, звукову або світлозвукову сигналізацію;

СКУД 2 класу – це багатофункціональні системи. Дані системи можуть бути як однорівневими, так і багаторівневими. Можуть працювати як в автономному, так і мережевому режимі. Підтримують розбиття відвідувачів на групи. Мають функціонал, що дозволяє надавати допуск особам або групам осіб за датою або тимчасових інтервалах. Система здатна забезпечувати автоматичну реєстрацію подій і автоматичне керування автоматичними пристроями;

СКУД 3 і 4 класу – в основному мережеві системи контролю та управління доступом. У таких системах використовуються більш складні ідентифікатори і різні рівні мережевої взаємодії (клієнт-сервер, інтерфейси зчитувачів карт Виганда або магнітних карт, спеціалізовані інтерфейси і т.д.).

Схема загальної класифікаціїСКУД зображена на рис. 1.10:

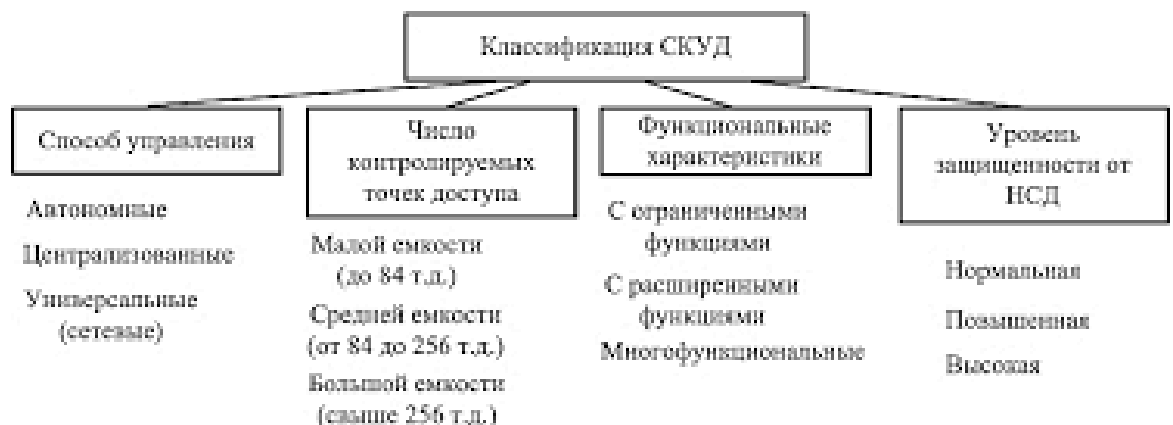


Рисунок 1.10 - Загальна класифікація систем контролю та управління доступом.

На сьогоднішній день існує досить СКУД від різних виробників, що складаються з різних компонентів, зібраних в різні конфігурації в залежності від призначення системи і побажань клієнта. При цьому всі системи контролю та управління доступом складаються з чотирьох основних елементів:

- ¶ ідентифікатор користувача;
- ¶ пристрій ідентифікації (зчитувачі);
- ¶ керуючий контролер;
- ¶ виконавчі пристрої.

Ідентифікатори користувача.

Ідентифікатором доступу є носій унікальної ідентифікаційної ознаки, за якою визначаються повноваження користувача системи контролю та управління доступом і здійснюється управління доступом в зону, що охороняється. В якості такого носія може використовуватися як технічний пристрій, так і сама людина (її індивідуальні біологічні ознаки або пам'ять).

Залежно від виду ідентифікаційного ознаки, ідентифікатори доступу можуть бути атрибутними (використовують речовинний код, який передається носію за допомогою спеціальної технології) або біометричними (запам'ятовується код або індивідуальні фізичні ознаки людини).

В якості атрибутних ідентифікаторів використовують автономні носії ознак допуску: магнітні карти, безконтактні proximity-карти, контактні брелки «touch-memory», різні радіобрелоки.

До біометричних ідентифікаторів відносяться зображення райдужної оболонки ока, відбиток пальця, відбиток долоні, риси обличчя і багато інших фізичних ознак. Кожен ідентифікатор характеризується певним унікальним двійковим кодом.

Пристрої ідентифікації.

Пристрої ідентифікації доступу (ідентифікатори та зчитувачі) підтверджує права людини на вхід, знаходження і переміщення в квадраті об'єкту, що

охороняється. Це можливо за рахунок читки і розшифровки закодованої інформації йде з різних типів ідентифікаторів, встановлених в місці контролю. Найчастіше контролюються входи і виходи в будівлю, в окремі кабінети і окремі території. Ці зони обладнуються зчитувачем, ідентифікатором або іншими контролерами, які встановлюються на дверні замки, турнікети, спеціальні кабінки для входу.

Ідентифікатор – невеликий предмет, носій закодованої інформації, яка підтверджує право людини, його використовує на можливість пройти і знаходиться на території об'єкту, що охороняється. Кодову інформацію за допомогою сучасних пристроїв і технологій, можна нанести на ідентифікатори у вигляді ключів, брелоків, пластикових карт і ін (детальніше у пункті «Ідентифікатори користувача»).

Зчитувач – електронний пристрій, який зчитує закодовану інформацію з карти. Код ідентифікується, розшифровується і в зручному форматі передається на контролер, який її аналізує, приймає певне рішення, в залежності від отриманого результату. Система СКУД налічує близько 10 видів пристроїв ідентифікації доступу[6]. Залежно від секретності інформації або всього важливості об'єкту, що охороняється система СКУД використовує складність способу запису, зчитування і зберігання закодованої інформації. Саме ця складова і формує ціновий діапазон.

Керуючі контролери.

Головним керуючим блоком СКУД є контролер.

Контролер СКУД – електронний пристрій, призначений для управління виконавчим обладнанням СКУД. Працює він за принципом «подія – рішення – команда».

Подією є зовнішня інформація – код суб'єкта, натискання кнопки, сигнал про відкриття дверей.

Рішення приймається на основі параметрів події (хто, коли і де доклав карту), базових даних про суб'єкта (дозволені і заборонені для проходу

приміщення і інтервали часу) і програмних алгоритмів. На виході системи прийняття рішень формується команда (або команди).

Команда – це, перш за все, сигнал на включення реле, керуючого виконавчим пристроєм. При цьому на замикає пристрій подається напруга (або знімається – залежно від типу замка або турнікета). Можуть виконуватися і інші команди: індикація, включення декількох реле, запис рішення у власну базу даних або передача його зовнішній програмі.

Часто рішення приймається не контролером, а керуючим СКУД програмним забезпеченням. У цьому випадку контролер стає ретранслятором, передаючи Серверу СКУД (або майстер-контролера) події і приймаючи від нього команди.

Режими роботи контролерів:

Комплексний режим – має на увазі роботу Системи під управлінням головного сервера. У такому режимі СКУД функціонує на більшості об'єктів, там, де необхідно контролювати роботу системи в режимі реального часу.

Автономний режим – режим роботи контролерів СКУД як самостійних одиниць. Кожен контролер в цьому режимі самостійно приймає рішення з прав доступу. Автономний режим може використовуватися як аварійний, коли на сервері, наприклад, ведуться профілактичні роботи, і як основний, коли для роботи СКУД не потрібний комп'ютер.

Поєднання комплексного і автономного режимів роботи СКУД - режим, в якому контролери працюють автономно (тобто приймають рішення), але при цьому в режимі реального часу передають на сервер повідомлення, а з сервера приймають необхідну інформацію - коди ключів і права доступу.

Виконавчі пристрої.

Виконавчі пристрої – це замки, турнікети, приводи воріт, шлагбауми, кнопки, тобто все те, що є фізичною перешкодою для несанкціонованого доступу[3].

Існуючі СКУД мають різними можливостями щодо масштабування, мають свої особливості для максимального задоволення потреби будь-якої муніципальної організації. Системи відмінно збалансовані, мають найширший

функціонал і можливості обробки великих обсягів даних з великою кількістю співробітників, відділів і підрозділів, в яких вони працюють. Системи здатні легко інтегруватися в існуючі інженерні системи, легко переносити модернізацію, підвищуючи масштаб, функціонал і надійність. У сучасності всі приведені вище складові систем управління та контролю доступу застосовуються не лише у комерційних підприємствах, а і в звичайних житлових комплексах комплексно або роздрібно задля забезпечення цілісності майна та безпеки жильців. СКУД вже давно вважаються складовою систем «Розумних домівок», що є автономним масштабним механізмом підвищення комфорту та безпеки життя.

1.3. Вибір та аналіз камер відеоспостереження

IP-камера відеоспостереження являє собою відеокамеру і комп'ютер, об'єднані в один пристрій. Захоплення і передача в реальному часі зображень в мережевій ip камері відбувається через мережу, дозволяючи авторизованим користувачам локально / віддалено переглядати, зберігати і управляти відеопотоком за стандартною мережевою інфраструктурою на базі IP.

IP-камера володіє власною IP адресою, вбудованим WEB сервером, FTP сервером, FTP клієнтом, поштовим клієнтом, модулем тривоги, можливістю програмування і т.д. IP камера необов'язково повинна бути приєднана до комп'ютера безпосередньо, IP камера управляється незалежно і може встановлюватися де завгодно в межах підключення до ip мережі.

Порівняння мережових ip камер з аналоговими камерами відеоспостереження:

IP-камери часто перевершують аналогові за рахунок ряду додаткових функцій. Коротко: аналогова камера передає лише сигнал в одному напрямку, що закінчується відеореєстратором, обладнанням шифрування і т.п., в той час як IP-камера повністю має двонаправлений потік (сигнал мовлення і потік управління), а отже і збільшує зручність експлуатації, гнучкість в управлінні,

					КІК.КР.Б – 123 – 05 – ПЗ	25

дає широкі функціональні можливості, що природним чином позитивно позначається на масштабованості системи відеоспостереження в комплексі безпеки.

Компактна мережева камера AXIS 216FD (рисунок 2.15) компанії AXIS Communications є фіксованою камерою напрямом огляду, який налаштовується вручну, і ступенем наближення, розміщена під ударостійким прозорим куполом. Конструкція AXIS 216FD дозволяє монтувати їх на стелю, в фальшпотолок і на стіни приміщень, а також організувати двосторонній аудіо зв'язок з об'єктом відеоспостереження. Ця мережева камера оснащена CMOS-матрицею і варіфокальним об'єктивом Fujinon і мають чутливість 1 лк. Вони здійснюють одночасну передачу по LAN / WAN-мереж потоків відео в форматах MPEG-4 і M-JPEG з роздільною здатністю кадру до 640x480 пикс. і швидкістю до 30 кадр / с.



Рисунок 2.1 - Зовнішній вигляд камери AXIS 216FD

До складу конструкції AXIS 216FD входить камерний блок з варіфокальним об'єктивом, поміщений в компактний корпус з полікарбонату і закритий ударостійким прозорим куполом. У середині корпусу камера встановлена на трьохкоординатний поворотний механізм з фіксатором, який дозволяє вручну налаштувати напрямом огляду шляхом повороту камери відносно трьох осей в межах $\pm 180^\circ$ / $\pm 85^\circ$ / $\pm 170^\circ$. Кут огляду: від 20° до 73° по горизонталі. Камеру рекомендується встановити в коридорах підприємства.

Ф у н к ц і о н а л ь н і м о ж л и в о с т і :

					КІК.КР.Б – 123 – 05 – ПЗ	
						26

- ¶ корпус фіксованої купольної мережевої камери AXIS 216FD виконаний з міцного пластику в антивандальному виконанні з неагресивним дизайном, він забезпечує максимальний захист;
- ¶ в AXIS 216FD вбудований механізм, що дозволяє ручне панорамування на ± 180 градусів і обертання на ± 170 градусів в площині основи корпусу камери і нахил на ± 85 градусів в площині, перпендикулярній основі;
- ¶ IP-камера AXIS 216FD підтримує технологію PoE (Power over Ethernet). Завдяки цьому електроживлення може подаватися до неї по звичайній парі 5 категорії, що значно скорочує витрати на прокладку силового кабелю при її інсталяції;
- ¶ в камері встановлена CMOS матриця з прогресивним скануванням і високоякісний об'єктив Fujinon, що дозволяє формувати і передавати відеозображення чудової якості;
- ¶ мережева камера працює при низьких умовах освітленості - 1 люкс;
- ¶ AXIS 216FD має вбудований мікрофон, а також роз'єми для підключення зовнішніх мікрофона і динаміка. Це дає користувачеві можливість не тільки бачити і отримувати аудіо інформацію з місця події а й передавати мовні команди, що значно розширює функції контролю;
- ¶ для обмеження доступу до камери використовується система паролів і фільтрація IP адрес, які можуть бути задані зі списку (до 256 адрес), з яких дозволений доступ до AXIS 216FD, із зазначенням рівня доступу (Користувач, Оператор, Адміністратор). Щоб запобігти неавторизованому використанню відео з AXIS 216FD на інтернет-ресурсах, може бути вказана IP-адреса сервера, на якому розміщується веб-сайт, який використовує відеопотік з AXIS 216FD авторизовано. Для забезпечення додаткової безпеки передачі даних купольна відеокамера підтримує кодування HTTPS;

- ¶ мережева камера має багатовіконний детектор руху, тривожний вхід для підключення датчиків і релейний вихід для підключення зовнішнього керованого пристрою;
- ¶ мережева відеокамера AXIS 216FD може одночасно передавати відеопотік в форматах Motion-JPEG і MPEG-4 з роздільною здатністю 640 * 480 і швидкістю до 30 кадр / с і оптимізувати його за якістю переданого зображення і смузі пропускання;
- ¶ завдяки підтримці багатокористувацького доступу надходячу з камери інформацію можуть одночасно переглядати по мережі до 20 користувачів в форматі MotionJPEG і необмежену кількість користувачів в форматі MPEG-4 в режимі Multicast;
- ¶ AXIS 216FD підтримує практично всі мережеві протоколи, в тому числі і DNS, що дозволяє підключати її через DSL з'єднання, які не забезпечують статичну IP адресу;
- ¶ повідомлення про тривогу і тривожні послідовності кадрів IP-камера може відсилати по e-mail, FTP, TCP, HTTP. Завдяки підтримці протоколу SOCKS IP-камера, встановлена усередині LAN, може передавати дані до вузла мережі, розташованому поза даної локальної мережі, минаючи сервер firewall / проху.

В і д е м о н с т р а ц і я A X I S 2 2 5 F D

Стационарна IP-відеокамера AXIS 225FD (рисунок 2.16), розміщена в куполоподібному всепогодному кожусі з вмонтованим вентилятором і обігрівачем, призначена для роботи у вуличних системах відеостеження при температурі від -20 до +50 градусів.

Камера оснащена рухомим ІЧ-фільтром і автоматично перемикається в режим чорно-білого відеоспостереження при паденні освітленості на об'єкті нижче 1 люкс. До складу конструкції AXIS 225FD входить камерний блок з варіфокальним об'єктивом.

Завдяки центральному процесору нового покоління IP-відеокамери підтримують технологію PoE і паралельну передачу MJPEG і MPEG-4 потоків з роздільною здатністю до 640x480 пікселів зі швидкістю до 30 кадр / с. Об'єктив варіфокальний, 2,8-5,8 мм, F1.4, автом. діафрагма DC IRIS, горизонтальний кут огляду: 36-75°. Камеру рекомендується встановити на вулиці.



Р и с у н о - к о ж н ь о г о в и г л я д у к а м е р и

Функціональні особливості:

- ¶ корпус фіксованої купольної камери AXIS 225FD виготовлений в антивандальному виконанні і призначений для роботи як всередині, так і зовні. Вона забезпечує максимальний захист при впливі несприятливих факторів як погодних, так і антропогенних (людських);
- ¶ в AXIS 225FD вбудований механізм, дозволяючий ручне панорамування на +/- 180 градусів і обертання на +/- 170 градусів в площині основи корпусу камери, а також нахил на +/- 85 градусів в площині, перпендикулярній основі;
- ¶ IP-камера AXIS 225FD підтримує технологію PoE (Power over Ethernet), завдяки цьому електроживлення може подаватися до неї по звичайній парі 5-ої категорії, що суттєво скорочує затрати на прокладку силового кабеля при її інсталяції;
- ¶ в камері встановлена матриця зі скануванням і високоякісний об'єктив Pentax, що дозволяє формувати і передавати відеозображення високої якості;

- ¶ в камері встановлена матриця зі скануванням і високоякісниц об'єктив Pentax, що дозволяє формувати і передавати відеозображення високої якості;
- ¶ мережева камера має вбудований ІЧ-фільтр, який дозволяє отримати відеозображення з камери навіть при низьких рівнях освітленості. При освітленості вище 1 люкс AXIS 225FD передає кольорове зображення, при більш низькому рівні вона автоматично перемикається в інфрачервоний режим і передає чорно-біле зображення;
- ¶ для обмеження доступу до камери використовується система паролей і фільтрація IP адрес, які можуть бути задані з списку (до 256 адрес), із зазначенням рівня доступу (користувач, оператор або адміністратор). Для забезпечення додаткової безпеки передачі даних відеокамера підтримує кодування HTTPS;
- ¶ мережева камера має багатовіконний детектор руху, а також два тревожних входи для підключення датчиків і релейний вихід для підключення зовнішнього керуючого пристрою;
- ¶ меню налаштувань зображення з камери дозволяє регулювати рівень стиснення (11 рівнів для M-JPEG і 23 - для MPEG-4), яскравості і насиченості, а також обирати необхідну роздільну здатність (16 варіантів, від 160x120 пікселів до 640x480 пікселів);
- ¶ завдяки рухливому ІЧ-фільтру камера може використовуватися для цілодобового відеспостереження: при зниженні освітленості на об'єкті відеоспостереження до 1 люкс відеокамера переходить в режим ч/б відеоспостереження з чутливістю 0,2 лк. При встановленні ІЧ прожектора вулична відеокамера може здійснювати відеонагляд в повній темряві;
- ¶ напрямлення огляду встановлюється і фіксується вручну за допомогою шарнірного механізму кронштейна, закріпленого на корпусі купола камери;

- ¶ ударостійкий всепогодний корпус з вбудованим обігрівачем і термopapapoю дозволяє встановлювати відеокамеру на залізничних, морських і аеропортах, в готелях, на складах і в неопалювальних приміщеннях;
- ¶ для тимчасового зберігання тривожних кадрів відеокамера має циклічний відеобуфер об'ємом 9 Мбайт;
- ¶ операційна система Linux 2.4 і інтерфейс вбудованого веб сервера надають користувачу широкий вибір налаштувань параметрів вуличної камери.

В і д е о к а м е р а A X I S 2 0 9 M F D

AXIS 209MFD - це мегapіксельна фіксована - ку мегapіксельною матрицею, яка забезп і д е н т и ф і к а ц і ю л ю д е й і п р е д м е т і в (р и с розмірів деваолньино підходять для приміщ готелях, магазинів. AXIS 209MFD вхідудиктоьнсктф блок з варіфокальним об'єктивом. Ка м робить їх непомітними, і з а й м а ю т ь в о в і д о с я г н е н н я к a x i s 2 0 9 M F D : н о з , т 6 . м м ; 1 , 8 ; ф і к с о г л я д у п о г о р и з о н т а л і : 7 4 ° . Ф о к у с н а в

Технологія живлення через мережевий 8 0 2 . 3 a f) д о з в і с л у ж а т ю п в и т р а т и н а у с т а т е x н o л o г і ї P o w e r o v e r E t h e r n e t (P o B з о б р а ж е н н я і о т р и м у ю т ь ж и в л е н н я ч е р е у с т а н o в к а с т а є м a к c и м a л ь н o з p y ч н o p y c , л е л e k t p o ж и в л e н н я .



Рисунок 2.3 - Зовнішній вигляд камери Axis 209MFD

					КІК.КР.Б – 123 – 05 – ПЗ	31

Камери AXIS 209MFD формують відеопотоки в форматах Motion JPEG і MPEG-4 одночасно. Можна оптимізувати якість зображення і ширину смуги пропускання, налаштовуючи частоту кадрів, роздільну здатність, рівень стиснення і формат. Камери AXIS 209MFD швидко і легко встановлюються. Їх зручний дизайн робить можливим налаштування кута нахилу об'єктива і регулювання камери в горизонтальній площині, що дозволяє використовувати різні варіанти кріплення на стіни і стелі. Камеру рекомендується встановити в холі усіх будівель.

Технічні характеристики.

Відеокамера мережева купольна мегапіксельна мініатюрна, MotionJPEG / MPEG-4, до 12 кадр / с при дозволі 1280x1024, PT + -10 ° / 90 °, 3 лк, фіксована діафрагма, багатовіконний детектор руху, живлення тільки по PoE, HTTPS, вбудований WEB- сервер.

Функціональні можливості:

- ¶ AXIS 209MFD є непомітну мережеву камеру розміром з долоню, спеціально розроблену для спостереження за магазинами, готельними фойє і коридорами;
- ¶ завдяки невеликому розміру AXIS 209MFD є ідеальним рішенням в таких ситуаціях - для її кріплення потрібна незначна площа плоскої поверхні;
- ¶ якщо використовується традиційна при зупинці кадру записаного відео AXIS 209MFD встановлюється з прогресивним різко знижує розмитість кадру як зображення, без спотворень, характерних для спостереження. Чіткі і чисті AXIS 209MFD, полегшують розпізнання людей та об'єктів;
- ¶ AXIS 209MFD забезпечує одночасну передачу MotionJPEG і MPEG-4, що дозволяє оптимальне зображення і пропускну здатність,

					КІК.КР.Б – 123 – 05 – ПЗ	
						32

передачі кадрів, дозволу, рівня ст

¶ встановлюється AXIS 209 MFD легко дозволяє встановити її на стелі або бок може бути компенсований горизонтальною установкою кутів нахилу і обертання «AXIS Installation Monitor», щоб поворот камери, перевірити позицію

¶ AXIS 209 MFD містить інтелектуальний захист зовнішньому впливі, що значно збільшує сигнал спрацьовує, якщо камера була окроплена

¶ AXIS 209 MFD забезпечує високу стійкість багаторівневі паролі, фільтрацію управління подіями реалізовано за допомогою детектору-іризатору в одній буферизації

AXIS 209 MFD включає в себе програмування Axis API і Axis Client, що дозволяє обладнання Axis в програмні рішення великою кількістю додатків, розроблених

1.4. Аналіз необхідного захисту системи відеоспостереження

Говорячи про системи охоронного відеоспостереження, слід зазначити і про їх захист: що потрібно захищати у відеоспостереженні і від чого.

Досвід показує, що найцінніше у відеоспостереженні це:

- ¶ відеоархіви і бази даних;
- ¶ канали зв'язку, що використовуються в системі відеоспостереження;
- ¶ пристрої: камери, комутатори, сервери, і інші розумні пристрої.

Відеоархів – головний результат роботи СОВ, адже, саме записи архіву служать основою для розбору й аналізу подій. Записи можуть піддаватися таким атакам:

- ¶ втрата записів відеоархіву, псування файлів;
- ¶ підміна файлів відеоархіву;
- ¶ несанкціонований перегляд відеоархіву.

Якщо говорити про канали зв'язку, то тут мова піде саме про лінії зв'язку:

- ¶ з IP-камерами;
- ¶ між сервером і ВРМ;
- ¶ між серверами (в розподіленій системі);
- ¶ між сервером і мережевим сховищем;
- ¶ між сервером і інтегрованою сторонньою системою СКУД.

Щодо станційного встаткування, камер та інших пристроїв, то в цих рамках можна виділити наступні вразливі місця:

- ¶ Конфігурація (програмні налаштування обладнання). Порушення цілісності конфігурації означає, що заданий режим роботи не буде виконуватися: ПЗ, яке “злетіло” може взагалі не вести запис, якість зображення з камери може знизитися нижче допустимого. Наслідок - завдання, поставлені перед системою, не будуть виконуватися.
- ¶ Несанкціонований доступ до зображення і управління. Доступ до зображення з IP-камер або управління ПЗ не порушує режиму роботи системи, але дає можливість визначити слабкі місця в системі відеоспостереження або погіршити ефективність визначення тривожних подій.

Якщо йдеться про те, від чого треба захищати відеоспостереження, то це, перш за все, людський фактор. І цю “групу небезпек” варто розділити на дві категорії.

Перша категорія - зловмисники. Ці люди, які не ріжуть дроти і не мажуть фарбою об'єктиви - їхні методи акуратні і непомітні. Можливо, саме тому відстежити такого роду загрози дуже важко. Нерідко можна почути фрази типу

					КІК.КР.Б – 123 – 05 – ПЗ	34

«хакеру нецікава моя система - там немає нічого для нього цінного». У корені невірно! Хакеру цікава будь-яка система. Немає нічого цінного - можна використовувати як «проміжний майданчик» для атаки інформаційної системи іншої організації. Не підходить як майданчик - можна використовувати як «тестовий полігон» для відпрацювання нових методів злому.

Друга категорія - некваліфікований персонал. На відміну від попередньої категорії загроз, тут відсутня злий умисел. Однак результати неграмотного або неакуратне користування можуть бути рівно такі ж, як і в разі наявності умислу, а саме:

- ¶ знищення або підміна записів архівів;
- ¶ зміна налаштувань і режимів роботи системи;
- ¶ несанкціонований доступ до спостереження і перегляду архівів;
- ¶ використання системи для власних завдань хакера (видобування криптовалюти і т.д.).

Також варто звернути увагу на шкідливе ПЗ. Всім відомі «віруси», «троянці», «шифрувальники» ... Як не дивно, незважаючи на широку популярність, дуже на багатьох об'єктах досі взагалі немає ніякого захисту від цього типу загроз. Можливі наслідки:

- ¶ псування записів архівів;
- ¶ гальмування, припинення роботи ПЗ;
- ¶ зависання, відмова системи.

Особливість цієї категорії в тому, що ці загрози, хоч і з'являються в результаті умисних дій людини, діють самостійно, тобто не вимагають якогось безпосереднього контролю з боку зловмисника. Тому вони виділені в окрему групу.

Існує три варіанти захисту з урахуванням специфіки галузі CCTV:

1. Вбудований захист ПЗ відеоспостереження.
2. Захист на рівні комутаційного обладнання.
3. Власний захист обладнання відеоспостереження.

Далі розглянемо кожен варіант окремо.

					КІК.КР.Б – 123 – 05 – ПЗ	
						35

Вбудований захист ПЗ відеоспостереження. Як приклад нижче представлено можливості найбільш відомого ПЗ.

Таблиця 1.1

Вбудований захист ПЗ відеоспостереження

Функції	Інтелект	Aххon Next	Macroscop	Trassir	Xprotect (Milestone)
Шифрування трафіку клієнт-сервер	Немає	Немає	Є	Є	Є
Шифрування трафіку камера-сервер	Немає	Немає	Немає	Немає	Немає
Контроль цілісності конфігурації БД	Немає*	Немає	Є	Немає	Немає
Захист від підбору паролів	Є	Є	Є	Є**	Є
Захист архіву від доступу через провідник	Немає	Є	Немає	Немає	Немає
Захист паролем експортованого архіву	Є	Є	Немає	Є	Є
Шифрування експортованого архіву	Немає	Немає	Немає	Немає	Немає

* В стандартному дистрибутиві відсутній; є в спеціальному виконанні ПО.

** Потрібне додаткове програмування скриптів в ПЗ інсталятором.

Як видно з таблиці - різне ПЗ влаштовано по-різному. Відповідно - різна ступінь придатності для різних завдань.

Захист на рівні комутаційного обладнання. Маються на увазі, перш за все, комутатори. Комутатори, як і ПЗ, теж бувають різні. Але точно можна сказати - некеровані комутатори засобів захисту практично не мають. Якщо потрібно захистити лінії зв'язку - потрібно використовувати керовані комутатори. Засобів і способів захисту тут чимало, тому обмежимося типовими:

1. Засоби обмеження доступу. Сюди можна віднести: фільтрацію по MAC-адресі з підтримкою «білих» списків, роботу з VLAN, VPN, блокування невикористовуваних портів.
2. Засоби шифрування. Так, деякі комутатори можуть самі шифрувати дані, які приходять і передавати їх далі на пристрій, який буде виконувати розшифровку потоку.
3. Засоби аудиту. Суть в тому, що деякі комутатори можуть відстежувати спроби несанкціонованого доступу, або якісь зміни в локальній мережі і повідомляти про них адміністратора системи. Наприклад, через електронну пошту.

Варто зауважити, що остання категорія засобів передбачає наявність в штаті ІТ-фахівця, який контролює роботу мережевого обладнання. В іншому випадку цей функціонал не потрібен.

Власне, IP-камери і комутатори досить захищені. Реальний ефект тут визначається, перш за все, компетенцією і сумлінністю інсталятора, який повинен виконати приписи виробника - змінити «дефолтні» паролі і налаштування, вимкнути функції, які не використовуються, перевірити актуальність прошивки тощо.

З захистом серверів, ВРМ та мережевих сховищ трохи складніше. З одного боку - як було показано вище - встановлене ПЗ відеоспостереження має ряд вбудованих функцій забезпечення безпеки, ОС має власні механізми захисту. З іншого боку - практика показує, що цього недостатньо. Тому необхідно опрацьовувати додаткові засоби і способи захисту, і тут вже питання до відповідальності виробника саме готового відеосерверу.

Прикладом додаткового захисту є:

- ¶ встановлення антивірусних програм;
- ¶ програм обмеження доступу до інтерфейсів ОС;
- ¶ використання спеціальних версій ОС.

Не зайвим буде нагадати і про заходи фізичного захисту систем відеоспостереження:

- ¶ Використання телекомунікаційних шаф, які замикаються. Особливо для комутаторів доступу поза серверної і кросових.
- ¶ Розміщення серверного і важливого комутаційного обладнання в виділеному приміщенні, яке замикається.
- ¶ Використання для прокладки і монтажу кабелів труб, закритих лотків і боксів, монтажних коробок.
- ¶ Використання обладнання в спеціальному антивандальному виконанні на особливо відповідальних ділянках або в легкодоступних місцях.

Захист систем IP-відеоспостереження. виходити слід перш за все з характеру і структури системи IP-відеоспостереження, так як цим визначається список можливих загроз і, відповідно, список заходів захисту. Нижче було розділено відеоспостереження на три категорії, залежно від розміру і особливостей мереж зв'язку.

Мережа тільки для задач відеоспостереження, сервери, камери, сховища, УРМ, ніяких зовнішніх підключень. Відносно проста система з точки зору інформаційного захисту.



Рисунок 1.12 - Закрита система

Таблиця 1.2

Програма-мінімум забезпечення безпеки

Завдання	Рекомендації проектувальнику	Рекомендації інсталятора
Захист архівів і БД	вибір топології «сервер без відображення - ВРМ для персоналу»	створення резервних копій БД
	вибір ПЗ з можливістю створення резервних копій БД	обмеження доступу користувачів до налаштувань ПЗ
Захист ліній зв'язку	вибір керованого комутатора з можливостями фільтрації по MAC-адресами і відключення невикористовуваних портів	налаштування «білого списку» MAC-адрес
		відключення невикористовуваних портів комутатора
Захист обладнання	вибір станційного устаткування з обмеженням доступу до ОС	зміна паролів доступу до налаштувань комутатора
		зміна всіх паролів доступу до IP-пристроїв
	Вибір ПЗ з захистом від підбору паролів	налаштування і перевірка роботи функції захисту від підбору паролів

Мережа тільки для відеоспостереження, сервери, камери, сховища, ВРМ, є підключення до внутрішньої мережі підприємства, одне або кілька ВРМ в корпоративній мережі.



Рисунок 1.13 - Інтегрована з корпоративною мережею система

У подібних системах зона відповідальності проектувальників і інсталяторів, як правило, закінчується на комутаторі, з якого йде кабель у власну мережу організації. Головне завдання при цьому - закласти і

налаштувати комутатор, що дозволяє обмежити доступ ззовні тільки завданнями перегляду зображення в клієнтських додатках ПЗ відеоспостереження.

Таблиця 1.3

Програма-мінімум забезпечення безпеки

Завдання	Рекомендації проектувальнику	Рекомендації інсталятору
Захист архівів і БД	вибір топології «сервер без відображення - ВРМ для персоналу»	створення резервних копій БД
	вибір ПЗ з можливістю створення резервних копій БД	обмеження доступу користувачів до налаштувань ПЗ
Захист ліній зв'язку	вибір керованого комутатора з можливостями фільтрації по MAC-адресами і відключення невикористовуваних портів	налаштування «білого списку» MAC-адрес
		відключення невикористовуваних портів комутатора
	організація підключення до корпоративної мережі через виділений комутатор з функціями «білого списку», VLAN, VPN, маршрутизації портів	налаштування безпечного підключення в корпоративній мережі до мережі спостереження згідно з вимогами проекту та IT-відділу
Захист обладнання	згідно з вимогами і можливостями існуючої корпоративної мережі	фільтрація IP-портів згідно з документацією ПЗ відеоспостереження
	вибір станційного устаткування з обмеженням доступу до ОС	зміна паролів доступу до налаштувань комутатора
		зміна всіх паролів доступу до IP-пристроїв
	Вибір ПЗ з захистом від підбору паролів	налаштування і перевірка роботи функції захисту від підбору паролів
	наявність антивірусного ПЗ в складі відеосерверу	відмова від використання стандартних TCP / IP / RTSP / RDP / HTTP-портів

Кілька мережевих сегментів тільки для задач відеоспостереження, сервери, камери, сховища, ВРМ. Для зв'язку між сегментами використовується Інтернет і / або корпоративна мережа організації.



Рисунок 1.14 -Розподілена система на базі зовнішніх неконтрольованих мереж зв'язку

У таких системах на проектувальників і інсталяторів лягає певна відповідальність не тільки за «двері» (комутатори, через які здійснюється підключення до зовнішніх каналів зв'язку), а й за «дорогу» (настройка самого каналу зв'язку). Програма-мінімум забезпечення безпеки аналогічна до інтегрованої з корпоративною мережею системою.

1.5. Обґрунтування необхідності та висування вимог до відеоспостереження

Основна мета систем відеоспостереження полягає в підвищенні рівня безпеки на певній території. На сьогоднішній день збільшується популярність на дані системи не тільки серед інвесторів і власників бізнесу, а й серед простих людей, тому що градація цін, виходячи з поставлених завдань, доступна практично для кожного. Нічого не викликає сумнівів, що дана тенденція у розвитку та вдосконаленні систем безпеки матиме тільки тенденцію до зростання.

Сучасні системи відеоспостереження (CCTV) - це програмно-апаратний комплекс, що складається з відеокамер, об'єктивів, моніторів, реєстраторів і ін.

устаткування, і призначений для організації відеоконтролю як на локальних об'єктах, так і на територіально-розподілених об'єктах.

На поточний момент системи відеоспостереження дозволяють встановлювати відеоконтроль за об'єктами будь-якої складності, а робота на ньому оперативного персоналу не вимагає високої кваліфікації. Як пристрої запису використовують як цифрові відеореєстратори (DVR), так і звичайні комп'ютери з платою відеозахвату. Серед переваг відеореєстраторів можна виділити функції квадратора (мультиплексора), відеодетектора руху, відеомагнітофона і т.д. Також сучасні відеореєстратори забезпечені мережевим або модемним інтерфейсом, що дозволяє передавати відеодані по IP протоколу. На відміну від DVR систем, системи, побудовані на базі персональних комп'ютерів, мають більш широкий діапазон функціональних можливостей, високу продуктивність і ємність архівів, а також звичний для користувачів ПК інтерфейс.

Відеоспостереження є сьогодні невід'ємним елементом будь-якої сучасної системи безпеки.

Система відеоспостереження повинна забезпечувати виконання таких функцій:

- ¶ візуальний контроль ситуації на об'єкті, що охороняється - надання інформації на пост спостереження в мультиекран режимі (в режимі очікування) або в повноекранному режимі (зображення від однієї телекамери на весь екран) в режимі реального часу. Це забезпечує можливість прийняття оперативних рішень, адекватної конкретної ситуації;
- ¶ організацію безперервного відеозапису відеоспостереження на цифровий відеореєстратор або комп'ютерну систему - це дозволяє документально підтвердити факт порушення й надає можливість для проведення ефективного аналізу кожної ситуації;

¶ виконання функцій охоронної сигналізації при використанні детекторів руху відеокамер або зовнішніх охоронних датчиків і інформованість оператора системи про виникнення тривоги в контрольованій зоні за допомогою світлового або звукового сигналу оповіщення. При цьому спрацьовування детектора руху може автоматично активувати запис для повної реєстрації тривожної ситуації, запускатися один з безлічі сценаріїв реакції системи - запуск виконавчих механізмів, зміна режиму роботи компонента системи, запуск інших додатків або ж комбінація всіх цих подій.

Так як системи відеоспостереження найчастіше використовуються як складові частини СКУД, нижче було висуното вимоги до останніх.

СКУД повинна забезпечувати виконання таких функцій:

- ¶ формування і видачу команд управління виконавчим пристроям (турнікетами), встановленим на прохідних ділянках при зчитуванні зареєстрованого в пам'яті підсистеми ідентифікаційна ознака (біометричні дані або безконтактні карти доступу);
- ¶ автоматичне і ручне розблокування для проходу при аварійних ситуаціях, пожежі, технічні несправності з видачею сигналу «Тривога»;
- ¶ передачу інформації про стан системи на АРМи;
- ¶ облік часу перебування співробітників і відвідувачів.

Програмна частина включає в себе наступні компоненти:

- ¶ комплект серверного і призначеного для користувача програмного забезпечення;
- ¶ додаткові утиліти для налаштування і конфігурації обладнання (при необхідності);
- ¶ набір засобів розробки (SDK) і відкритий програмний інтерфейс (API) для забезпечення інтеграції системи СКУД зі сторонніми системами, функціонуючими, або планують ввести в дію на об'єкті.

Апаратна частина повинна включати в себе:

- ¶ контролери СКУД;
- ¶ периферійне устаткування: біометричні зчитувачі, турнікети;
- ¶ сервер СКУД з СУБД;
- ¶ існуючі автоматизовані робочі місця операторів.

Висновки до розділу 1

Інформаційний захист систем відеоспостереження - завдання, що вимагає зусиль як проектувальників, так і інсталяторів. Перші повинні закласти обладнання, що має засоби захисту, другі - належним чином його налаштувати. Так, це додаткова робота, найчастіше досить нудна й вимагає чимало часу. Але в кінцевому рахунку виграють всі. Тому що в сучасному світі все ми в тій чи іншій мірі користуємося результатами роботи встановлених систем безпеки і відеоспостереження.

Тривалий досвід використання СКУД показує позитивні результати. Якщо бізнес вже знаходиться на тому рівні, коли стоїть питання про обмеження доступу сторонніх в приміщення, варто задуматися про установку СКУД. Дана система є прекрасним помічником в охороні офісу і контролі діяльності співробітників.

РОЗДІЛ 2. РОЗРОБКА ПРОЕКТУ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ПІДПРИЄМСТВА

2.1. Проект мережі підприємства

СВ і д п о в і д н о до генерального плану наступна схема розміщення турнікетів в рисунку 3.1. В даній роботі була підприємства, що складається з двох зон, які між собою формують робочі зони організації (верхня та ліва будівлі). Продумана можливість розширення мережі за рахунок збільшення кількості кінцевих пристроїв до вільних портів комутаторів та додавання ще декількох подібних зон. Що ж до третьої – то це обчислювальний центр організації, в якому розміщуються сервери. Спроектована трирівнева ієрархічна структура мережі. Топологію мережі можна побачити на рис. 3.2.

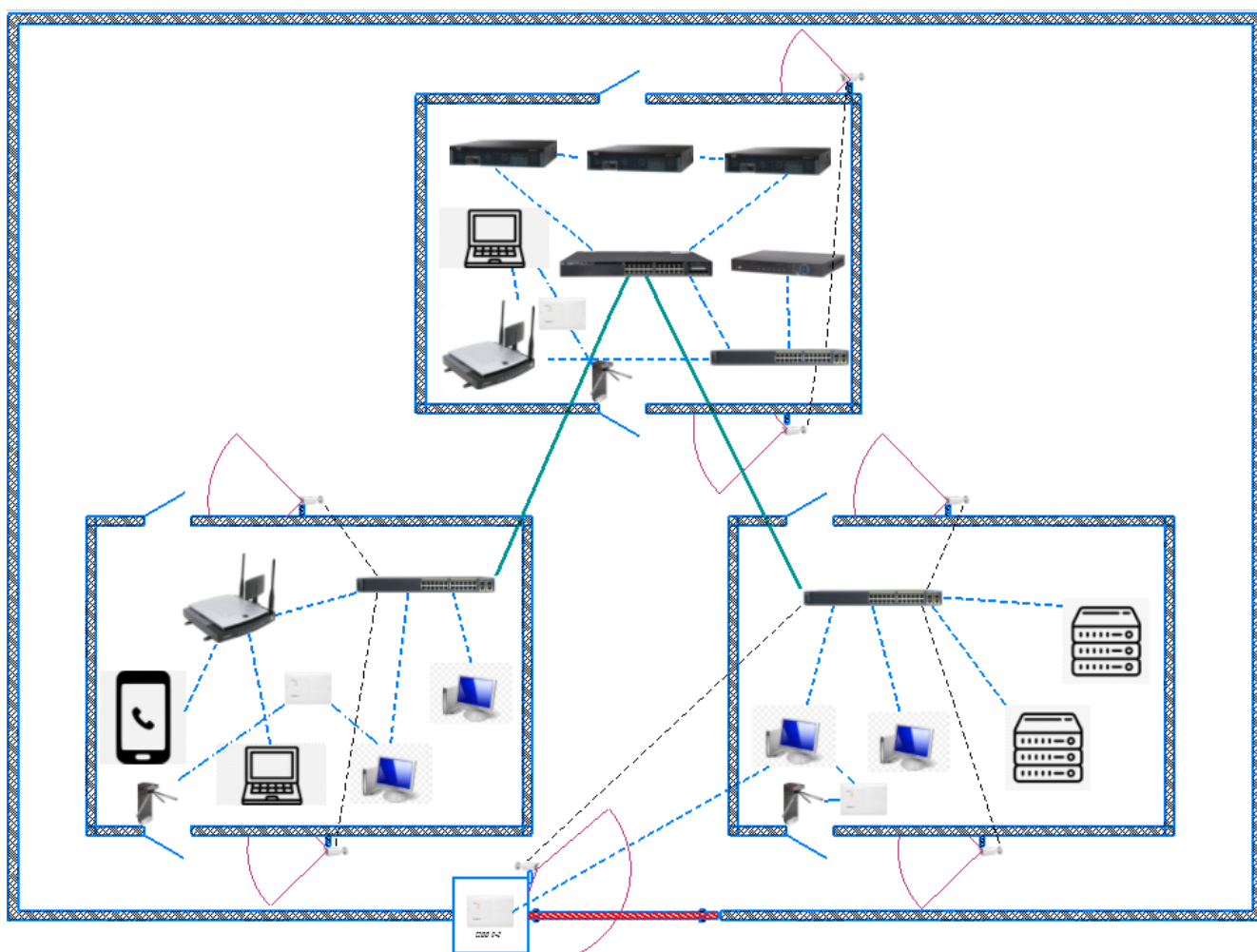


Рисунок 2.4 – Проект мережі підприємства за генпланом

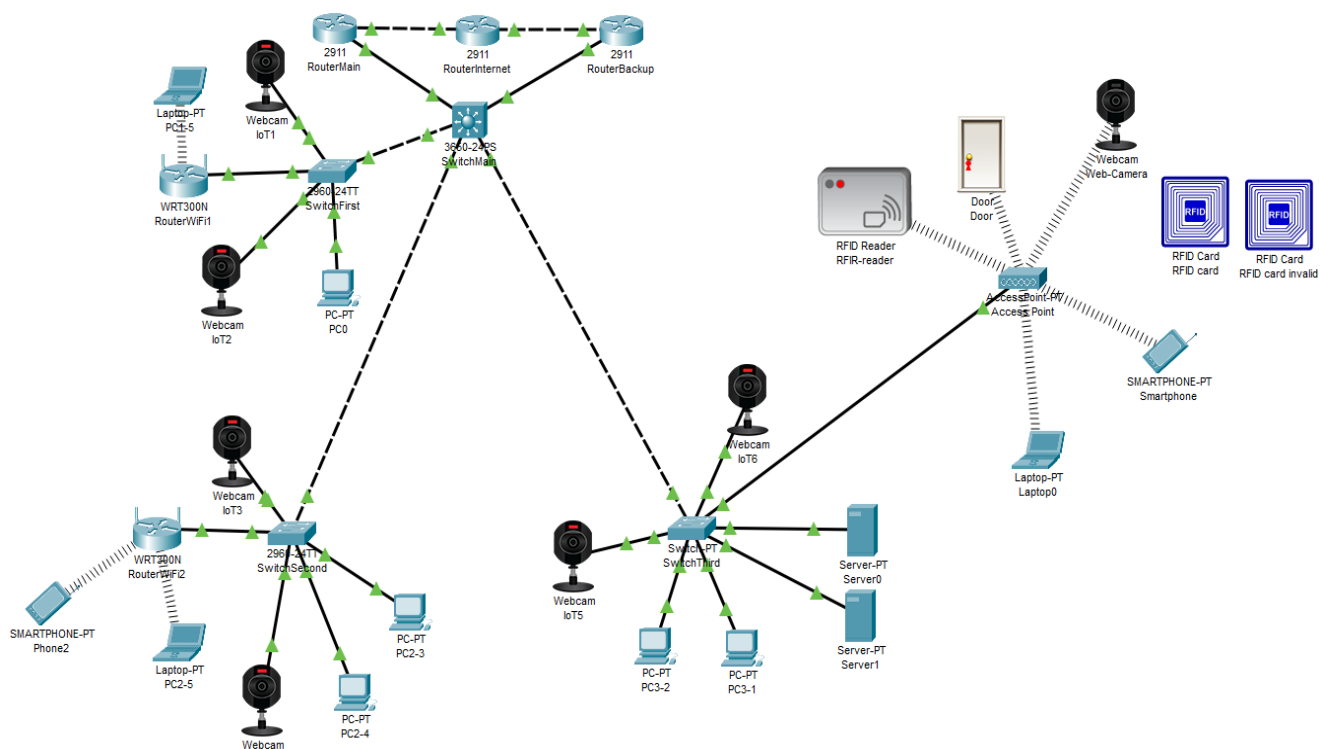


Рисунок 2.5 – Топологія мережі

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

Детальну топологію з'єднань мережі можна побачити в табл. 2.1.

Таблиця 2.1

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	Internet	
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	КомутаторSwitchThird	Gi0/1
КомутаторSwitchFirst	Gi0/1	Комутатор SwitchMain	Gi1/0/3
	Gi0/2	Маршрутизатор RouterWiFi1	0/0
	Fa0/3	Робоча станція PC0	Fa0
	Fa0/1	Webcam IoT2	Eth0
	Fa0/2	Webcam IoT1	Eth0
КомутаторSwitchSecond	Gi0/1	Комутатор SwitchMain	Gi1/0/4
	Fa0/23	Робоча станція PC2-1	Fa0
	Fa0/24	Робоча станція PC2-2	Fa0
	Gi0/2	Маршрутизатор RouterWiFi2	0/0
	Fa0/1	Webcam IoT3	Eth0
	Fa0/2	Webcam IoT4	Eth0

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
КомутаторSwitchThird	Gi0/1	Комутатор SwitchMain	Gi1/0/5
	Gi1/1	Сервер Server0	Gi0
	Gi2/1	Сервер Server1	Gi0
	Fa3/1	Робоча станція PC3-1	Fa0
	Fa4/1	Робоча станція PC3-2	Fa0
	Fa8/1	Webcam IoT5	Fa0
	Fa7/1	Webcam IoT6	Fa0
	Gig5/1	AccessPoint-PT	
Маршрутизатор RouterWiFi1	0/0	КомутаторSwitchFirst	Gi0/2
	Wireless	Робоча станція PC1-1	Wireless
Маршрутизатор RouterWiFi2	0/0	КомутаторSwitchSecond	Gi0/2
	Wireless	Телефон Phone2	Wireless
		Робоча станція PC2-3	Wireless
Робоча станція PC1-1	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	Wireless	Маршрутизатор RouterWiFi2	Wireless
Робоча станція PC3-1	Fa0	Комутатор SwitchThird	Fa0/1
Робоча станція PC3-2	Fa0	Комутатор SwitchThird	Fa0/2
Телефон Phone2	Wireless	Маршрутизатор RouterWiFi2	Wireless
Сервер Server0	Gi0	Комутатор SwitchThird	Gi1/1
Сервер Server1	Gi0	Комутатор SwitchThird	Gi2/1

2.2. Вибір обладнання

Для забезпечення функціонування даної мережі організації було обрано оптимальні маршрутизатори і комутатори корпорації Cisco, котрі мають адаптованість під модернізацію модулями.

Так як доступ до реального обладнання відсутній, то проект мережі розробляється в графічному симуляторі Cisco Packet Tracer. Нижче описані та охарактеризовані пристрої, які були використані для побудови мережі.

В якості основних маршрутизаторів мережі були обрані маршрутизатори Cisco 2911 (рис. 3.3).



Рисунок 2.6 - Маршрутизатор Cisco 2911

Модульний маршрутизатор Cisco 2911 – це пристрій нового покоління, що 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.

Даний маршрутизатор було розміщено у верхній будівлі підприємства (рис. 3.3) у кількості 3 штук. Серія маршрутизаторів Cisco 2900 представлена 4-ма фіксованими і 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 в секунду.

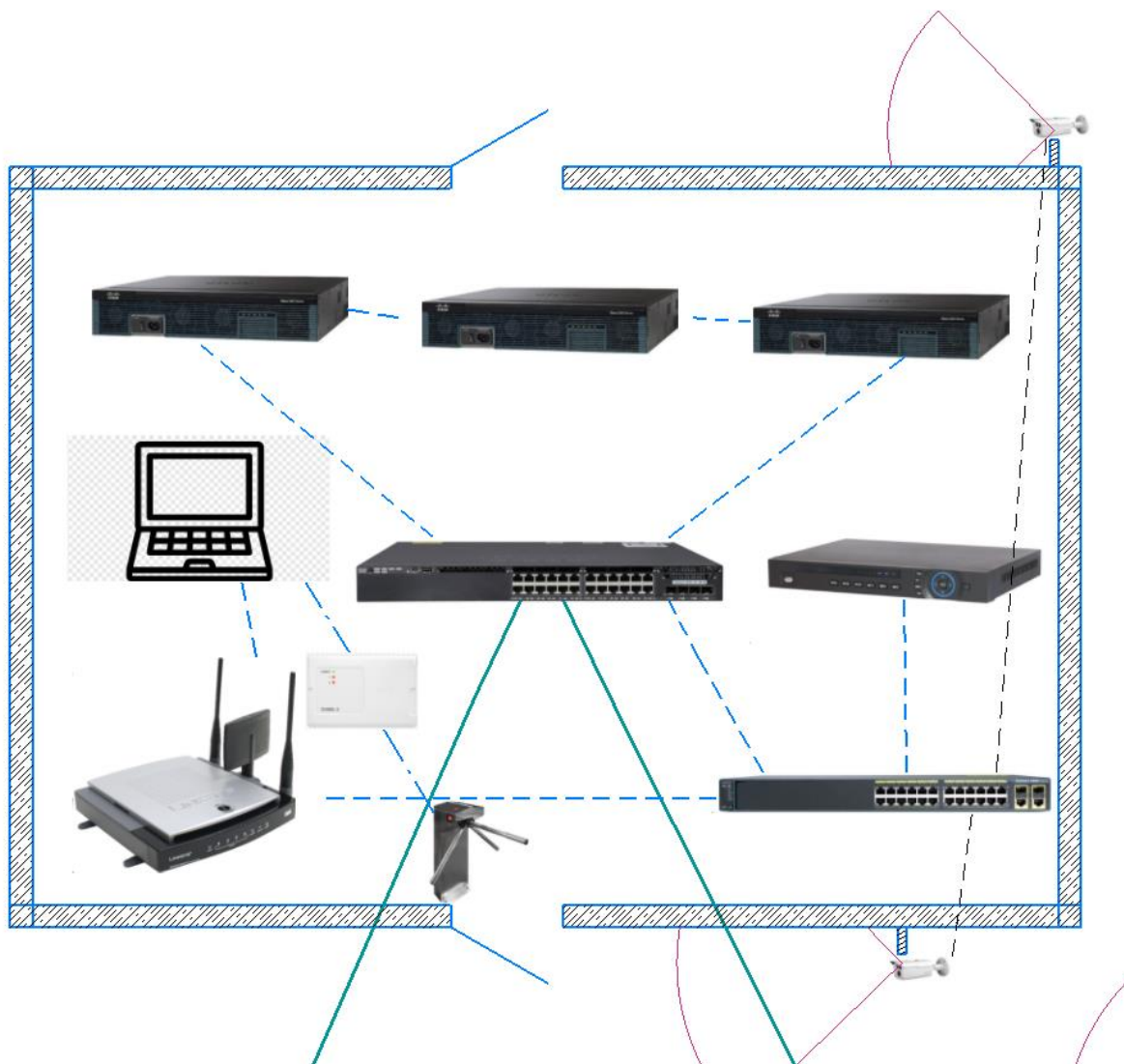


Рисунок 2.7 – Розміщення маршрутизаторів та багаторівневого комутатора у верхній будівлі

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 замінюють 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, за запитом, 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 співробітникам захищений доступ до ресурсів компанії з 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.

Крім цього, на рівні розподілу, маршрутизацією займаються багаторівневі комутатори CiscoCatalyst 3650 (рис. 3.5).



Рисунок 2.8 - Багаторівневий комутатор Cisco Catalyst 3650

Комутатори Cisco Catalyst 3650 серії – це стекові пристрої для конвергованого доступу з фіксованою конфігурацією і інтегрованим бездротовим контролером ASIC, що працюють на базі модульної операційної системи IOS XE. 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 вентиляторів охолодження. Також, в Catalyst

3650 є підтримка стека StackWise (до 9 пристроїв в стеку) при використанні опціональних модулів для стекування з пропускнуою спроможністю 160 Гб / с і технологією SSO (Stateful SwitchOver), пропускна здатність Wireless 40 Гб / с на базі ASIC UADP (Unified Access Data Plane) і операційної системи IOS XE і підтримка до 25 точок доступу і 1000 бездротових клієнтів на один комутатор 3650 або один стек StackWise з комутаторів 3650.

Для підключення безпроводних кінцевих пристроїв в проекті вирішено використовувати маршрутизатор Cisco-Linksys WRT300N (рис. 3.6).



Рисунок 2.9 - Маршрутизатор Cisco-Linksys WRT300N

Даний бездротовий маршрутизатор – це справді три пристрої в одній коробці. По-перше, є точка WirelessAccess, яка дозволяє вам підключатися до мережі без проводів. Є також вбудований 4-портовий модуль комутації з пропускнуою 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. 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 802.11 g.

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 промислової потужності. Він може служити DHCP-сервером вашої мережі, має потужний брандмауер SPI для захисту ваших ПК 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 дає вам достатньо місця для одночасного запуску декількох медіаінтенсивних потоків даних через мережу.

Завдяки широкосмуговому маршрутизатору Linksys в центрі вашої домашньої або офісної мережі ви можете ділитися швидкісним підключенням до Інтернету, файлами, принтерами та іграми для багатьох гравців, а також запускати медіа-інтенсивні програми швидше ніж 10/100 швидкість дротової мережі, без клопоту про проводи.

Рівень доступу буде реалізований за допомогою комутаторів CiscoCatalyst 2960 (рис. 3.7).



Рисунок 2.10 - Комутатор Cisco Catalyst 2960

Дані комутатори розміщені в лівій та правій будівлі підприємства (рис. 3.7-3.8). 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 здатне масштабувати свої функції під безперервно зростаюче підприємство.

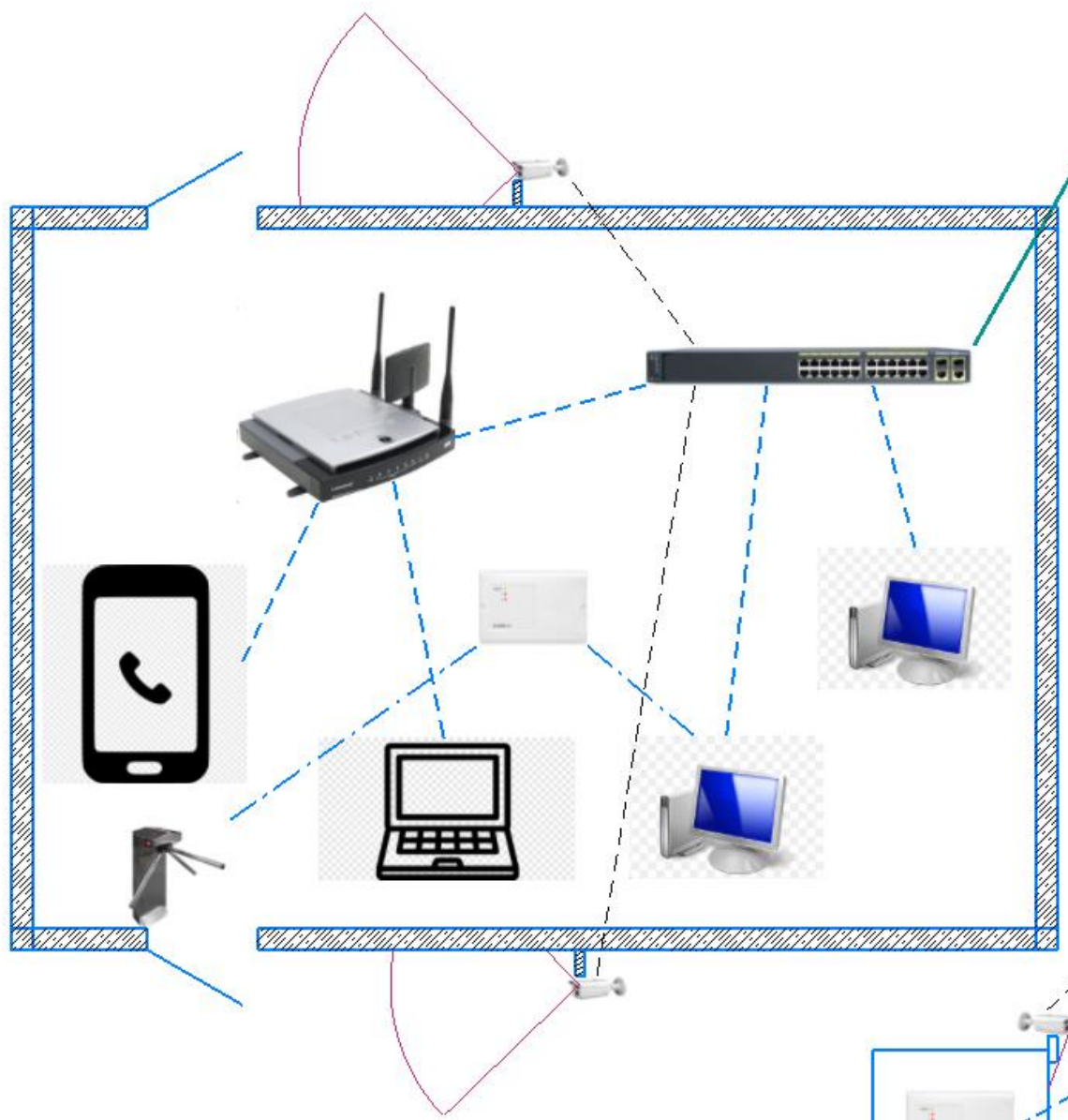


Рисунок 2.11 – Розміщення комутатора та бездротового маршрутизатора в лівій будівлі

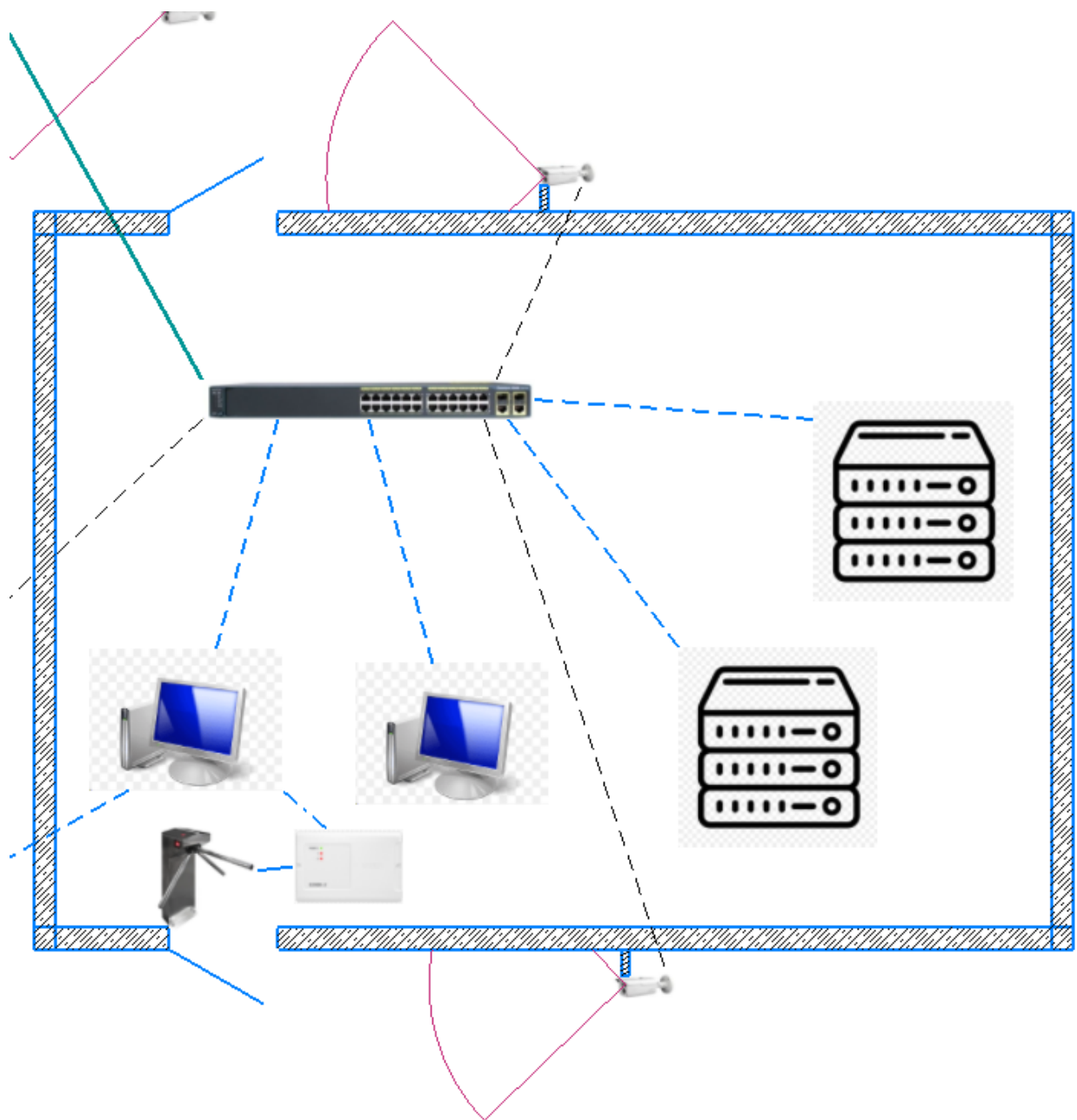


Рисунок 2.12 – Розміщення комутатора та периферії в правій будівлі

Комутатори Cisco Catalyst серії 2960 мають інтерфейс, простий для користувача. При першому налаштуванні необхідно скористатися пакетом утиліт під назвою Cisco Network Assistant, воно допоможе налаштувати робоче середовище, зробить його більш продуктивним і швидкодіючим.

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

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.

Крім того дані комутатори здатні відновлювати інформацію в разі непередбачуваних аварій, але адміністратор повинен постаратися створити такі умови, щоб продукт працював в безперервному режимі.

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

2.3. Розробка схеми адресації мережі

Для забезпечення функціонування топології мережі підприємства 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 можливості розширення внутрішньої мережі. Внутрішня адресація мережі 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). Детальні параметри адресації мережі представлені в табл. 2.3.

Таблиця 2.2

Параметри адресації пристроїв мережі

Підмережа/ Пристрій	Інтерфейс/Мереж- ний адаптер/Шлюз	ІР-адреса	Маска підмережі	Префікс
МаршрутизаторRouterInter net	Gi0/0	1.1.1.1	255.255.255.252	/30
	Gi0/1	2.2.2.1	255.255.255.252	/30
	Gi0/2	Internet		
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
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
КомутаторSwitchFirst	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
	Vlan103	10.3.0.2	255.255.255.0	/24
КомутаторSwitchSecond	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
	Vlan203	20.3.0.2	255.255.255.0	/24
КомутаторSwitchThird	Vlan1	100.0.0.4	255.255.255.0	/24
	Vlan255	25.5.0.2	255.255.255.0	/24
Маршрутизатор RouterWiFi1	0/0	DHCP		
	Wireless	192.168.1.1	255.255.255.0	/24
Маршрутизатор RouterWiFi2	0/0	DHCP		
	Wireless	192.168.2.1	255.255.255.0	/24
Робоча станція PC1-1	Wireless	DHCP		
Робоча станція PC2-1	Fa0			
Робоча станція PC2-2	Fa0			
Робоча станція PC2-3	Wireless			
Робоча станція PC3-1	Fa0			
Робоча станція PC3-2	Fa0			
Webcam IoT1	Vlan102			
Webcam IoT2	Vlan102			
Webcam IoT5	Vlan102			
Webcam IoT6	Vlan102			
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

Висновки до розділу 2

В даному розділі було розглянуто та детально описано камери відеоспостереження, їх функціональні можливості. Також нами був розроблений проект мережі промислового підприємства та схему розміщення камер відеоспостереження та мережевого обладнання за генпланом, обрано усі необхідні засоби для реалізації системи: виробника обладнання, конкретні моделі обладнання, методи та технології розподілу IP-адрес, методи захисту обладнання від зовнішнього зловмисного впливу, симулятор роботи з мережним обладнанням.

РОЗДІЛ 3. НАЛАГОДЖЕННЯ МЕРЕЖІ ПІДПРИЄМСТВА

3.1. Базове налагодження пристроїв мережі

В даному пункті розглянуто базові налаштування пристроїв мережі промислового підприємства. 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).

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

Рисунок 3.1 - Налаштування імені на маршрутизаторі RouterInternet

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 повторюватися. 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
```

Рисунок 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.

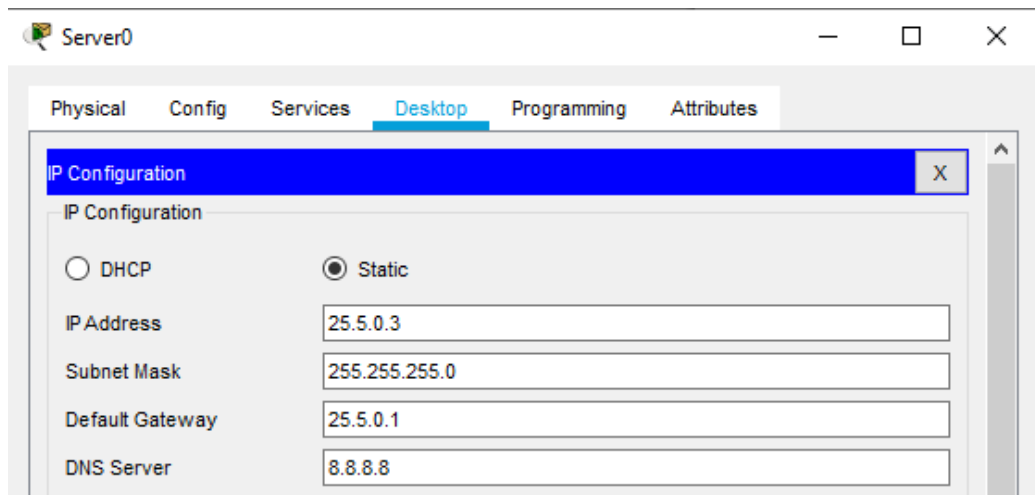


Рисунок 3.3 - Налаштування статичної IP-адреси на сервері Server0

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
```

Рисунок 3.4 - Налаштування loopback-інтерфейсу на маршрутизаторі RouterInternet

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. 3.5).

```
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
```

Рисунок 3.5 - 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. 3.6 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
```

Рисунок 3.6 - Налаштування статичної IP-адреси для інтерфейсу Vlan8 на багаторівневому комутаторі SwitchMain

Далі на комутаторах було зроблене розділення внутрішньої мережі на підмережі. Для цього були налаштовані 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. В подальшому використання VLAN дозволить контролювати трафік між ними за рахунок пристроїв маршрутизації, та у разі потреби – блокувати/дозволяти його. Приклад налагодження VLAN представлений на рис. 3.7.

```
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
```

Рисунок 3.7 - Зміна стандартного Vlan на 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 і дозволяє досягти вищесказаного. Приклад налагодження подібного каналу показаний на рис. 3.8.

```

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

```

Рисунок 3.8. Налаштування транкового каналу на багаторівневому комутаторі SwitchMain

Далі були сконфігуровані IP-адреси кінцевих пристроїв. Вони були згенеровані за рахунок протокол динамічного конфігурування вузлів 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. Для реалізації відповідних дій на багаторівневому комутаторі SwitchMain, який має підключення до всіх підмереж через комутатори L2, був налагоджений цей протокол. Для того, щоб не відбувалось конфліктів динамічних та статичних IP-адрес, останні були додані у винятки (див. рис. 3.9). Налаштування самого протоколу показано на рис. 3.10.

```

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 25.5.0.2

```

Рисунок 3.9 - Додавання статичних IP-адрес у винятки для протоколу DHCP на багаторівневому комутаторі SwitchMain

```

SwitchMain(config)#ip dhcp pool Wi-Fil
SwitchMain(dhcp-config)#network 10.1.0.0 255.255.255.0
SwitchMain(dhcp-config)#default-router 10.1.0.1
SwitchMain(dhcp-config)#dns 8.8.8.8
SwitchMain(dhcp-config)#domain wifil.com
SwitchMain(dhcp-config)#ex

```

Рисунок 3.10- Налаштування DHCP на багаторівневому комутаторі SwitchMain

Відповідно з боку комутаторів другого рівня також були проведені налаштування транкових каналів зв'язку, які аналогічні до попередніх. Єдиною відмінністю є те, що на комутаторах другого рівня непотрібно вказувати метод інкапсуляції, так як на них він підтримується тільки один – 802.1Q.

Кожного разу, коли кінцевим пристроям, що знаходяться в одній VLAN потрібен доступ до кінцевих пристроїв у іншій VLAN, трафік повинен маршрутизуватись між VLAN-ами. Дане переміщення трафіку між VLAN називається *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.

В нашому випадку все що потрібно для реалізації *inter-VLAN routing* вже зроблено і лишається лише увімкнути його командою *ip routing* (рис. 3.11).

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

Рисунок 3.11-Увімкнення *inter-VLAN routing* на багаторівневому комутаторі SwitchMain

Для обміну трафіком між мережами використовуються статичні маршрути або динамічні протоколи маршрутизації. Так як корпоративна мережа «зав'язана» на одному багаторівневому комутаторі, який вже маршрутизує VLAN між собою, то немає сенсу використовувати динамічні протоколи маршрутизації для внутрішньої мережі.

Але для рівня ядра слід налаштувати маршрутизацію. Для цього буде використаний протокол динамічної маршрутизації OSPF, налаштування якого наведено на рис. 3.12.

```
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
```

Рисунок 3.12 - Налаштування протоколу OSPF на маршрутизаторі RouterBackup

Вихід до мережі Інтернет буде здійснюватись за статичним маршрутом (рис. 3.13).

```
RouterInternet(config)#ip route 0.0.0.0 0.0.0.0 g0/2
RouterInternet(config)#
```

Рисунок 3.13 - Налаштування статичного маршруту на маршрутизаторі RouterInternet

3.2. Налагодження промислової мережі та її захисту

Після проведення базових налаштувань можна переходити до більш конкретних налаштувань, які потрібні для даної промислової мережі. Одною з важливих технологій є протокол маршрутизації мережевого рівня HSRP, що використовується для резервування шлюзу в Ethernet-мережах. Його налаштування показане на рис. 3.14

```
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
```

Рисунок 3.15 - Налаштування протоколу маршрутизації HSRP на маршрутизаторі RouterMain

Також були налаштовані маршрутизатори, що містять радіомодуль, тому виступають безпроводними точками доступу. Їх налаштування відрізняються від інших моделей маршрутизаторів (рис. 3.16-3.18).

Wireless-N Broadband Router

Firmware Version: v0.93.3

Setup

Setup

Wireless

Security

Access Restrictions

Applications & Gaming

Administration

Status

Basic Setup

DDNS

MAC Address Clone

Advanced Routing

Internet Setup

Internet Connection type

Automatic Configuration - DHCP

Optional Settings (required by some internet service providers)

Host Name:

Domain Name:

MTU:

Size: 1500

Network Setup

Router IP

IP Address:

192

168

1

1

Subnet Mask:

255.255.255.0

DHCP Server Settings

DHCP Server:

Enabled

Disabled

DHCP Reservation

Start IP Address:

192.168.1.

2

Maximum number of Users:

253

IP Address Range:

192.168.1. 2 - 254

Client Lease Time:

0

minutes (0 means one day)

Static DNS 1:

8

8

8

8

Static DNS 2:

0

0

0

0

Static DNS 3:

0

0

0

0

WINS:

0

0

0

0

Help...

Рисунок 3.16 -Налаштування внутрішньої та зовнішньої мережі на маршрутизаторі RouterWiFi1 відносно нього

Wireless-N Broadband Router

Firmware Version: v0.93.3

Wireless

Setup

Wireless

Security

Access Restrictions

Applications & Gaming

Administration

Status

Basic Wireless Settings

Wireless Security

Guest Network

Wireless MAC Filter

Advanced Wireless Settings

Basic Wireless Settings

Network Mode:

Mixed

Network Name (SSID):

Wi-Fi1

Radio Band:

Auto

Wide Channel:

Auto

Standard Channel:

1 - 2.412GHz

SSID Broadcast:

Enabled

Disabled

Help...

Рисунок 3.17 -Налаштування базових конфігурацій радіомодуля на маршрутизаторі RouterWiFi1

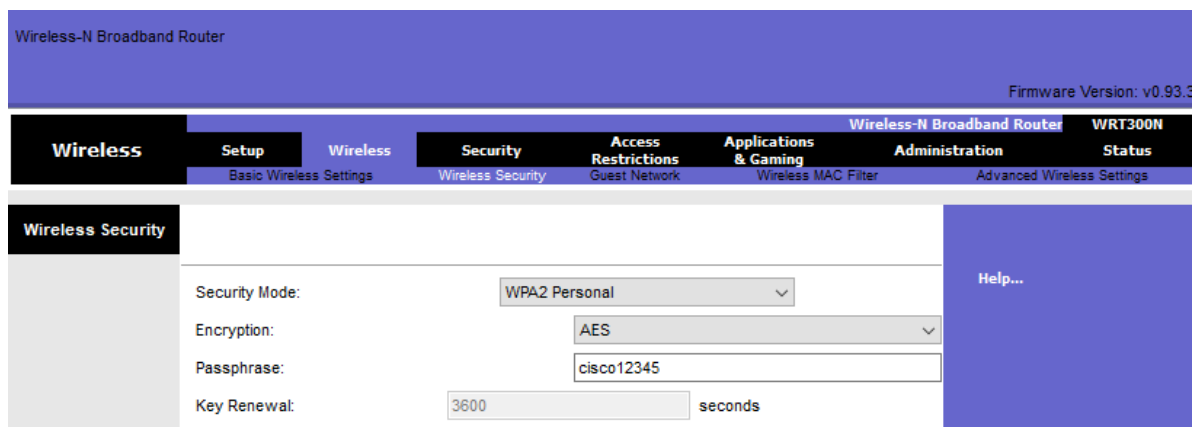


Рисунок 3.18 -Налаштування автентифікації на маршрутизаторі RouterWiFi1

Після цього можна підключити кінцеві пристрої до безпроводної мережі (рис. 3.19-3.20).

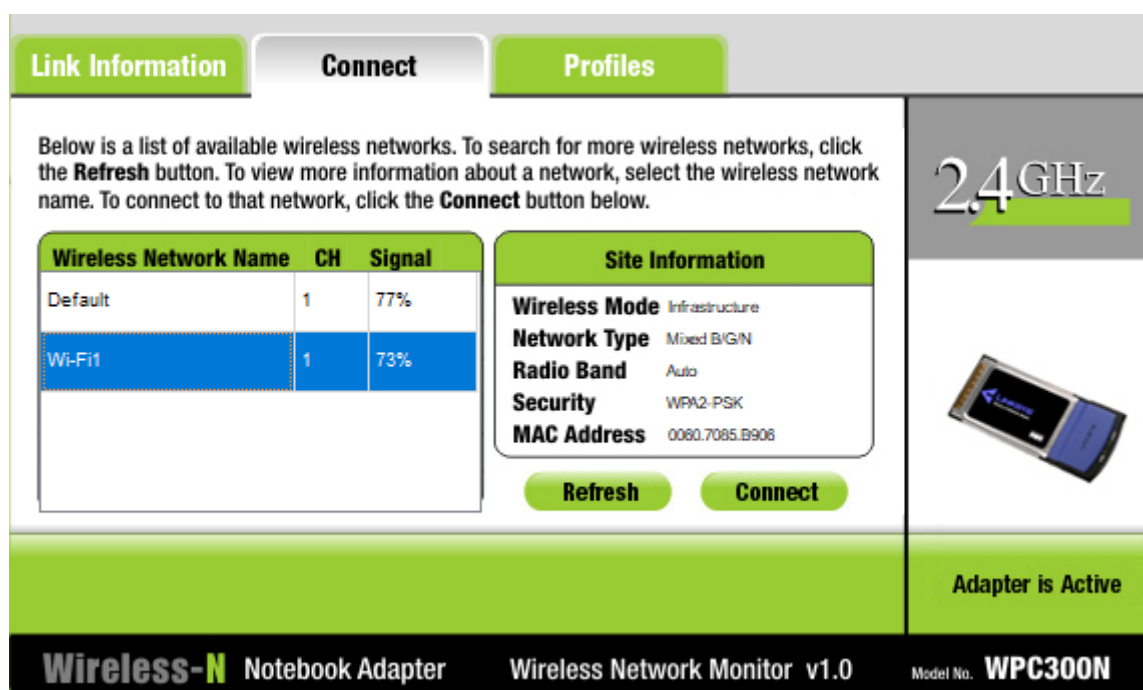


Рисунок 3.19 -Підключення кінцевого пристрою PC1-1 до бездротової мережі

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

cisco12345

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

Cancel

Connect

Рисунок 3.20 -Підключення кінцевого пристрою PC1-1до бездротової мережі

Physical
Config
Desktop
Programming
Attributes

GLOBAL

Settings

Algorithm Settings

INTERFACE

Wireless0

3G/4G Cell1

Bluetooth

Wireless0

Port Status ☒ On

Bandwidth 300 Mbps

MAC Address 0001.6407.8834

SSID Wi-Fi1

Authentication

☐ Disabled
☐ WEP

WEP Key

☐ WPA-PSK
☒ WPA2-PSK

PSK Pass Phrase cisco12345

☐ WPA
☐ WPA2

User ID

Password

☐ 802.1X

Method: MD5

User Name

Password

Encryption Type AES

IP Configuration

☒ DHCP
☐ Static

IP Address 192.168.1.3

Subnet Mask 255.255.255.0

Рисунок 3.21 -Підключення кінцевого пристрою Phone2до бездротової мережі

Тепер налаштуємо PortSecurityна комутаторах рівня доступу, тобто на портах, до яких будуть підключатися кінцеві вузли. PortSecurity – це функція каналного рівня, яка створена для запобігання несанкціонованій зміні MAC-

адреси мережевого підключення. Також, дана функція захищає комутатор від атак, які можуть бути спрямовані на переповнення таблиці MAC-адрес.

За допомогою PortSecurity можна обмежити (на каналному рівні) кількість підключень (MAC-адрес) на інтерфейсі, так само, при необхідності, ввести безпечні MAC-адреси вручну (статичні MAC-адреси). Приклад конфігурування буде наступним:

```
SwitchSecond(config)# intrangetafa0/23-24, fa0/1-2, gig0/2
```

```
SwitchSecond(config-if-range)#switchport port-security maximum 1
```

```
SwitchFirst(config-if-range)#switchport port-security mac-address sticky
```

```
SwitchFirst(config-if-range)#switchport port-security violation restrict
```

```
SwitchSecond(config-if-range)#switchport port-security aging type inactivity
```

```
SwitchSecond(config-if-range)#switchport port-security aging time 120
```

```
SwitchSecond(config-if-range)#switchport port-security
```

```
SwitchSecond(config-if-range)#exit
```

```
SwitchSecond(config)#
```

У налаштуваннях технології Port Security:

- «switchport port-security» означає, що включається Port Security на даному інтерфейсі;

- «switchport port-security maximum 1» говорить про те, що тільки 1 MAC адреса, може бути наявною на інтерфейсі одночасно для попередження підключення невідомих пристроїв.

- «switchport port-security violation restrict» вказує на режим реагування на порушення. Таким чином,

якщо на даному інтерфейсі одночасно з'явиться третя (невідома) MAC-адреса, то всі пакети з цієї адреси будуть відкидатися, при цьому відправляється повідомлення - syslog, SNMP trap, а також збільшується лічильник порушень (violation counter).

Далі налагодимо DHCP Snooping та IP Source Guard. IP Source Guard (Dynamic IP Lockdown) - функція комутатора, яка обмежує IP-трафік на

інтерфейсах 2го рівня, фільтруючи трафік на підставі таблиці прив'язок DHCPspooring і статичних відповідностей. Функція використовується для боротьби з IP-spoofingом.

У проєктованій мережі були застосовані типові команди для налаштування засобу IPSourceGuard, які виконуються по наступній схемі:

```
SwitchSecond(config)#int gig0/1
```

```
SwitchSecond(config-if)#ip dhcp snooping trust
```

```
SwitchSecond(config-if)#ex
```

```
SwitchSecond(config)#ip dhcp snooping
```

```
SwitchSecond(config)#int range fa0/23-24, fa0/1-2, gig0/2
```

```
SwitchSecond(config-if-range)#ip verify source port-security
```

```
SwitchSecond(config-if-range)#ex
```

Для доступу до відеокамер з серверу, камери та сервер були налаштовані наступним чином:

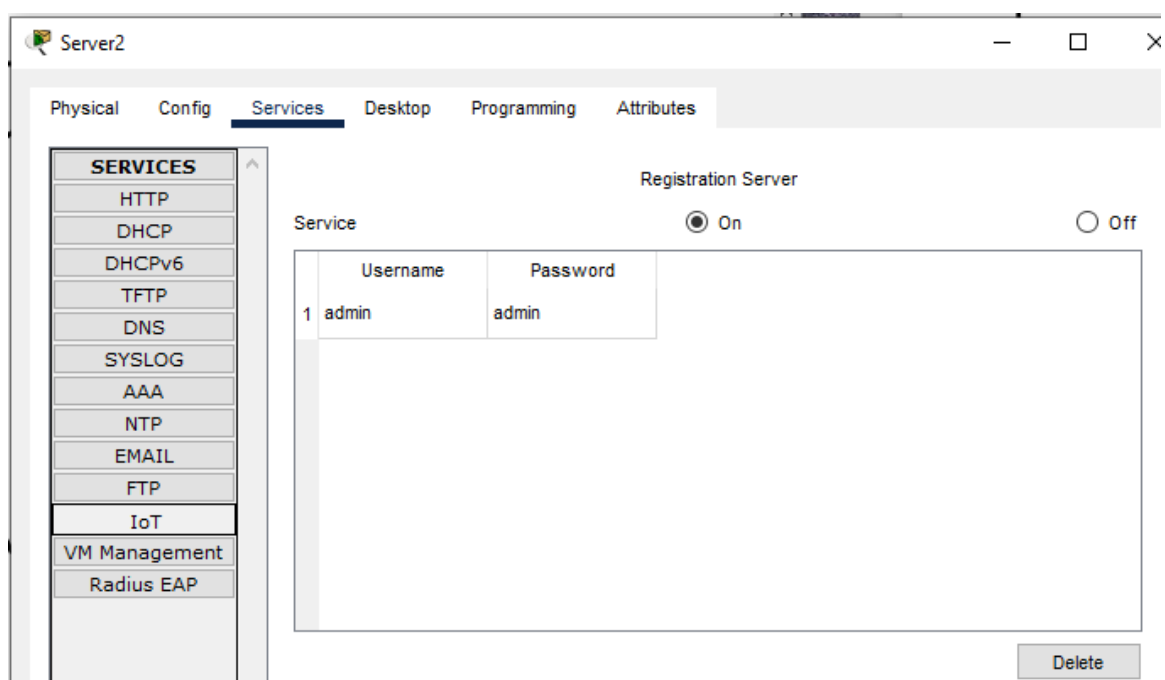


Рисунок 3.22 – Дозволення реєстрування на сервері

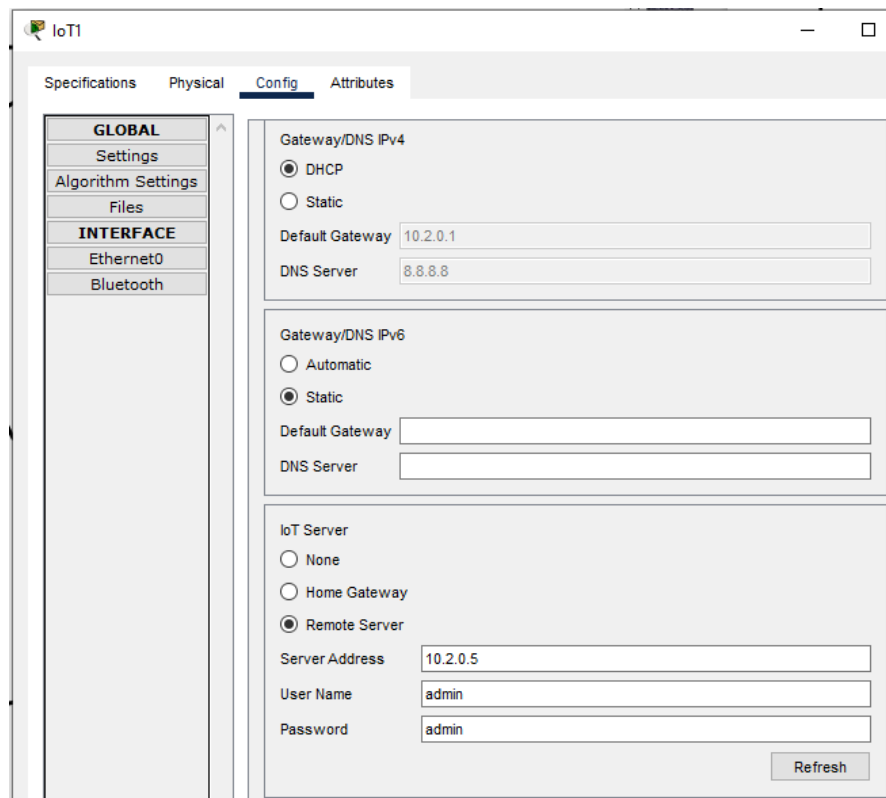


Рисунок 3.23 – Налаштування камери на роботу з сервером

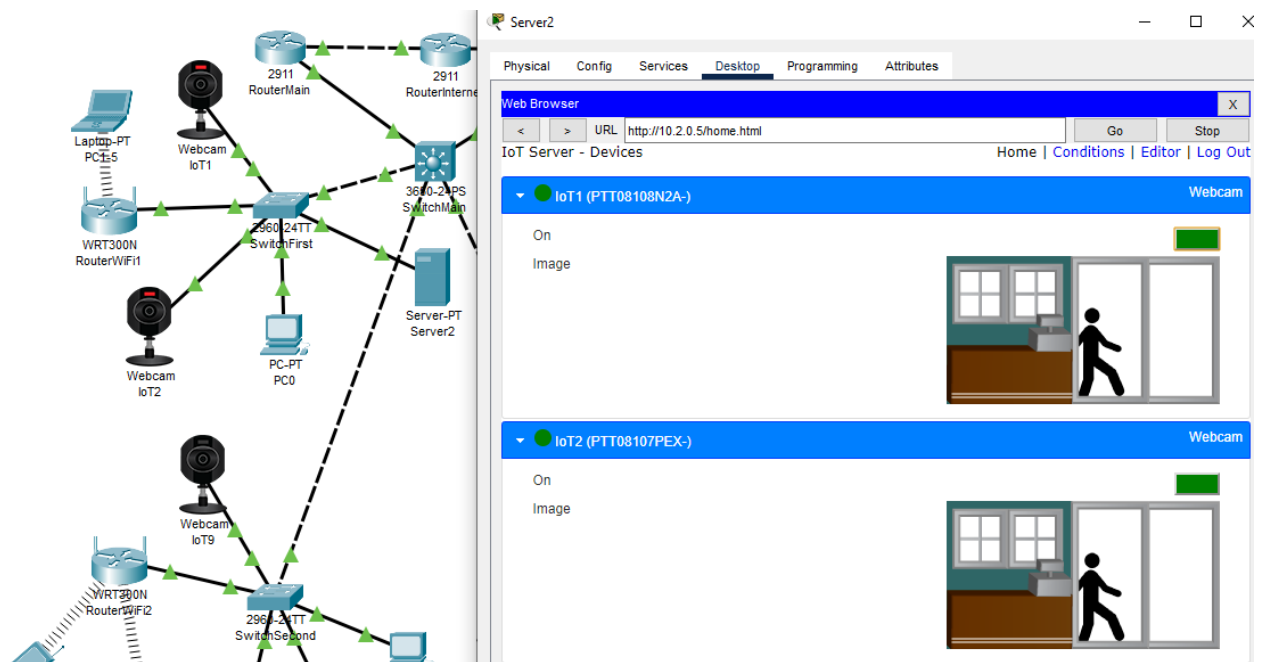


Рисунок 3.24 – Робота схеми за допомогою керування з сервера

Також були налагоджені сервери підприємства, а точніше сервіси HTTP/HTTPS, TFTP, SYSLOG таNTP (рис. 3.33-3.36).

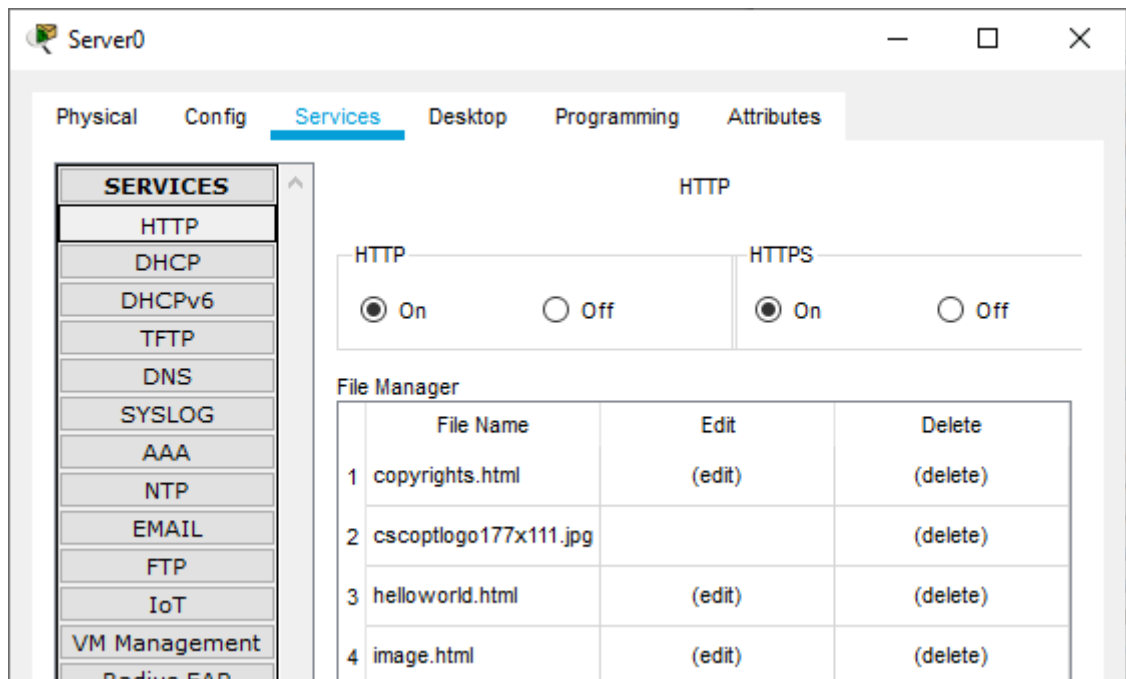


Рисунок 3.25 -Налагодження сервісів HTTP/HTTPS на сервері Server0

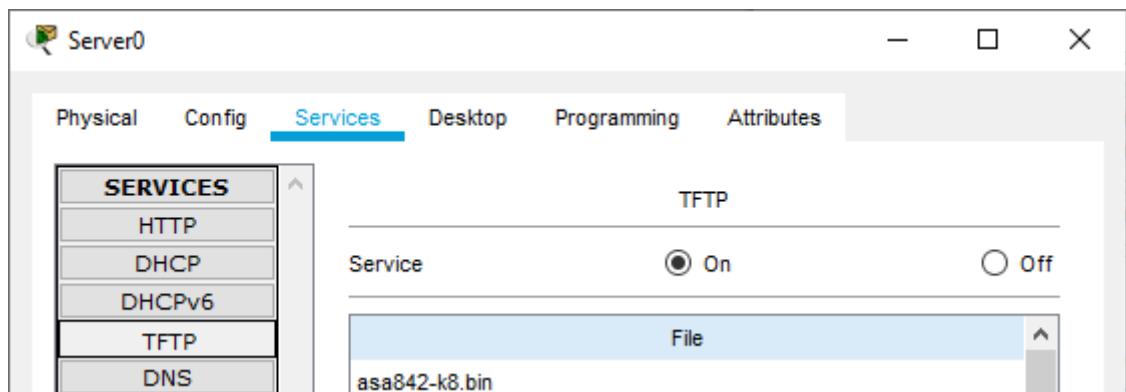


Рисунок 3.26-Налагодження сервісу TFTP на сервері Server0

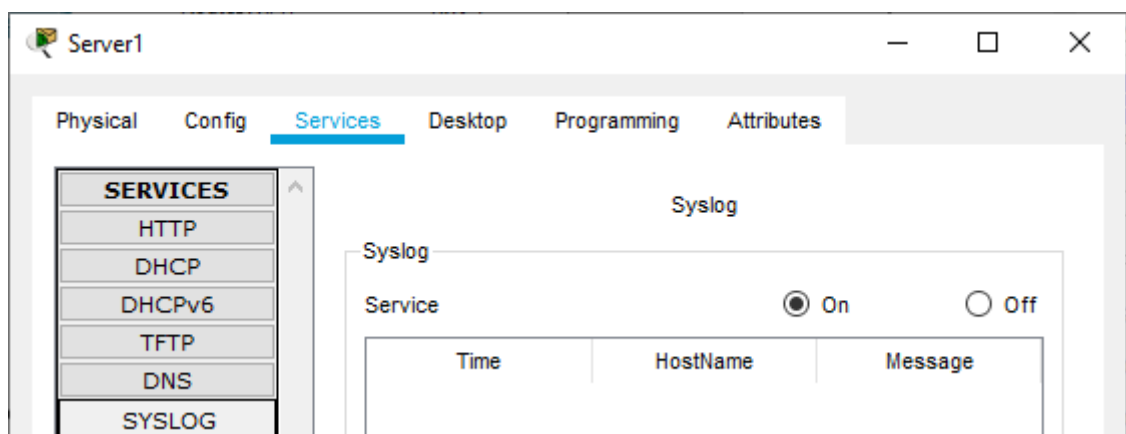


Рисунок 3.27 -Налагодження сервісу SYSLOG на сервері Server1

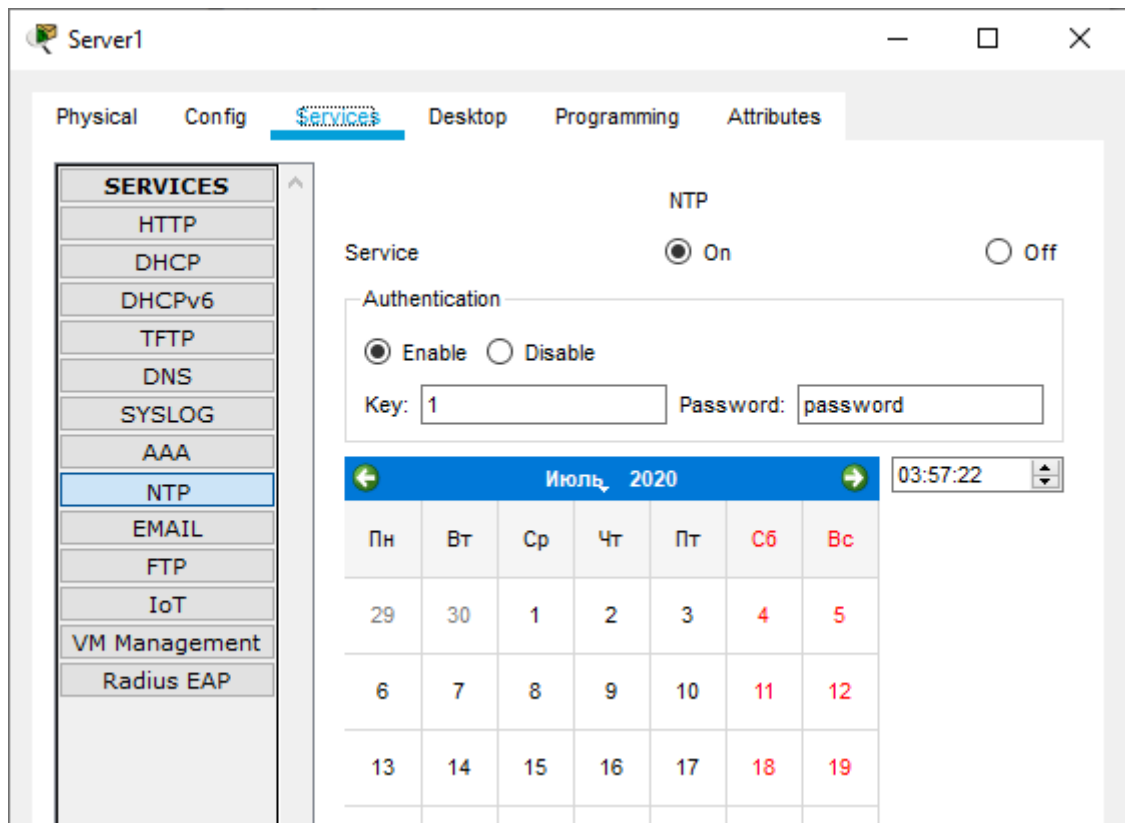


Рисунок 3.28 -Налагодження сервісу NTP на сервері Server1

Після того, як сервіси на серверах активовані, слід налаштувати ці сервіси на мережних пристроях. Першим з них є NTP – протокол системного часу. Він призначений для синхронізації дій в мережі. При налагодженні використовується автентифікація, визначається сервер, що є джерелом часу та параметри корегування часу. Налагодження є однотипним, як для маршрутизаторів, так і для комутаторів (рис. 3.29).

```
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#
*июл 30, 19:55:12.5555: %SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.29 - Налагодження сервісу NTP на комутаторі SwitchThird

```

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]
*изл 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

```

Рисунок 3.30 -Налагодження віддаленого підключення та користувачів на маршрутизаторі RouterInternet

Тепер налагодимо систему журналювання подій SYSLOG. Налагодження аналогічне для маршрутизаторів і комутаторів (рис. 3.31).

```

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. 3.31. Налагодження системи журналювання SYSLOG на маршрутизаторі RouterInternet

Також до проекту було додано приблизну схему роботи шлагбауму. У ролі шлагбауму виступають двері, у ролі контролера C-2000-2 – AccessPointPT (рисунок 3.32).

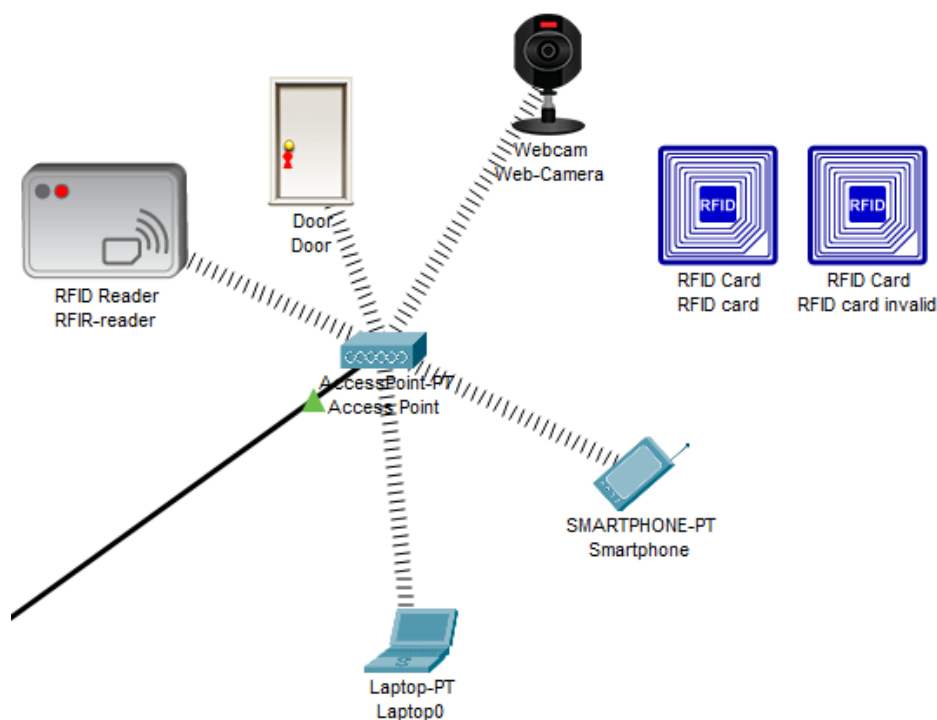


Рисунок 3.32 – Демонстрація підключених пристроїв до контролера

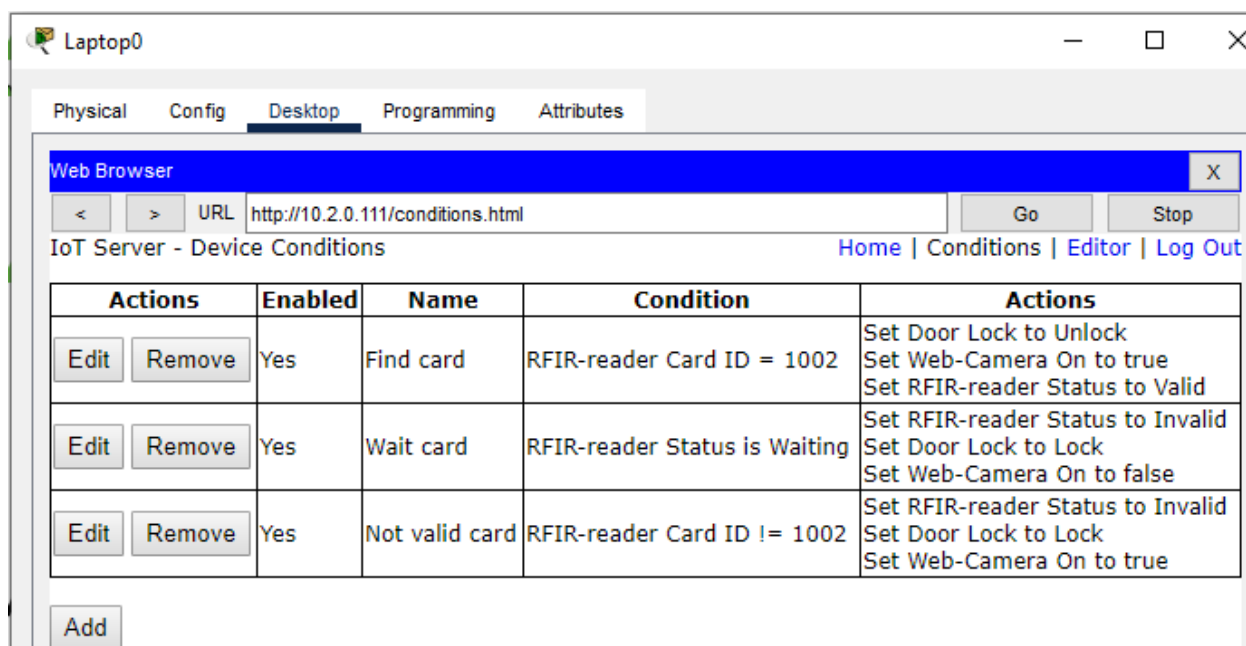


Рисунок 3.33 – Правила роботи пристроїв

3.3. Тестування налаштувань

Тестування налаштувань проводиться з метою перевірки їх коректності. Для перевірки будуть використовуватись різні діагностичні команди та візуальні відображення на кінцевих пристроях.

Проведемо перевірку на розділення на віртуальні підмережі з мережного обладнання офісів. Як видно на рис. 3.34, дане розділення існує, тому при необхідності є можливість обмеження проходження трафіку між ними за допомогою списків доступу.

```
SwitchMain#sh vlan
```

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
8 FOR_HSRP	active	Gig1/0/1, Gig1/0/2
101 Wi-Fil	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	

Рисунок 3.34 - Результат команди show vlan на комутаторі SwitchMain

Тепер перевіримо налаштування DHCP-серверу за допомогою нього самогорта кінцевого пристрою (рис. 3.35-3.36).

```

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        0001.97A0.138B   --                     Automatic
10.2.0.3        0060.4768.0B95   --                     Automatic
10.3.0.3        0001.423C.E72D   --                     Automatic
10.3.0.4        0001.42E3.8844   --                     Automatic
20.1.0.3        00D0.FF49.08E0   --                     Automatic
20.2.0.3        000A.F358.800C   --                     Automatic
20.2.0.4        0060.7041.98B9   --                     Automatic
25.5.0.6        0090.0CEE.139C   --                     Automatic
25.5.0.5        000D.BDA4.80C2   --                     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                 : 7
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 / 7 / 254

Pool LAN1-1 :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)          : 0 / 0
Total addresses                    : 254
Leased addresses                   : 2
Excluded addresses                 : 7
Pending event                      : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
10.2.0.1          10.2.0.1      - 10.2.0.254      2 / 7 / 254

Pool LAN1-2 :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)          : 0 / 0
Total addresses                    : 254
Leased addresses                   : 2
Excluded addresses                 : 7
Pending event                      : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
10.3.0.1          10.3.0.1      - 10.3.0.254      2 / 7 / 254

Pool Wi-Fi2 :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)          : 0 / 0
Total addresses                    : 254
Leased addresses                   : 1
Excluded addresses                 : 7
Pending event                      : none

```

Рисунок 3.35 - Результат виконання діагностичних команд show ipdhcpbindingта show ipdchppoolна багаторівневому комутаторі SwitchMain

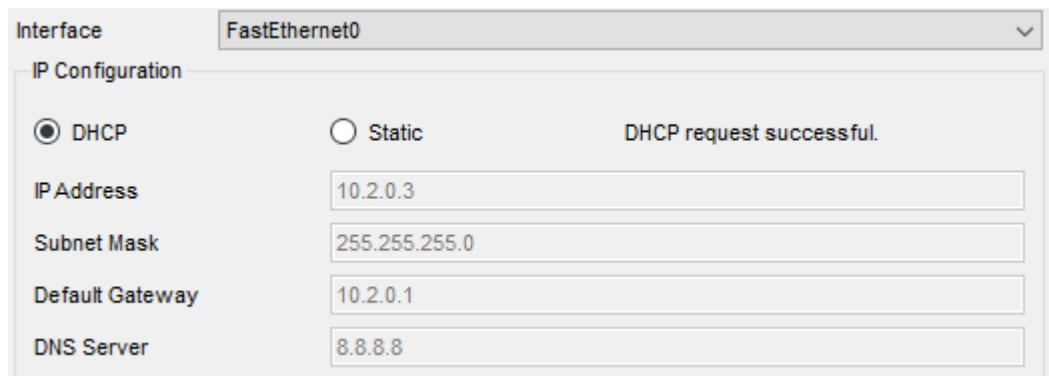


Рисунок 3.36 - Результат виконання DHCP-запиту на робочій станції PC1-1

Глобальну мережу Інтернет змодельовано за допомогою інтерфейса замикавання 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. 3.37).

```
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=6ms 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 = 6ms, Average = 1ms
```

Рисунок 3.37 - Результат тестування доступності мережі Інтернет на робочій станції PC1-1

Тепер з тої ж віртуальної машини перевіряється доступність двох сусідніх будівель підприємства. Як видно на рис. 3.38, у відповідь на команду *ping* <О н т е і п р и о д и т ь к і л ь к і с ь п е р е д а н и х б а й т т а ч а с з а т р и м к и – з н а ч и т ь з в ’ я з о к є.

```

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

```

Рисунок 3.38. Результат тестування доступності сусідніх будівель на робочій станції PC1-1

Перевіривши базові налаштування, перейдемо до тих, що потрібні для конкретного підприємства. Почнемо з HSRP – виведемо діагностичні команди, щодо HSRP на відповідних пристроях (рис. 3.39-3.40).

```

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

```

Рисунок 3.39 - 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

```

Рисунок 3.40 - Результат виконання діагностичних команд show standby та show standby brief на маршрутизаторі RouterBackup

Одним з важливих аспектів для даного підприємства є бездротова мережа Wi-Fi, тому наступною було перевірено саме її. На маршрутизаторах, на яких і налаштовувався бездротовий доступ, нажаль немає можливості вивести діагностичні команди, тому перевірку зроблено за допомогою перевірки налаштувань кінцевих пристроїв та їх доступність до мережі (рис. 3.41-3.42).

Interface: Wireless0	
IP Configuration	
☒ DHCP	☐ Static
DHCP request successful.	
IP Address	192.168.1.4
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	8.8.8.8

Рисунок 3.41 - Результат виконання DHCP-запиту на робочій станції PC1-1

```

C:\>ping 172.16.0.1

Pinging 172.16.0.1 with 32 bytes of data:

Request timed out.
Reply from 172.16.0.1: bytes=32 time=16ms TTL=252
Reply from 172.16.0.1: bytes=32 time=11ms TTL=252
Reply from 172.16.0.1: bytes=32 time=17ms TTL=252

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 17ms, Average = 14ms

```

Рисунок 3.42 - Результат тестування доступності мережі Інтернет на робочій станції PC1-1

Перейдемо до перевірки сервісів серверів. Першим перевіримо доступність HTTP/HTTPS(рис. 3.43).

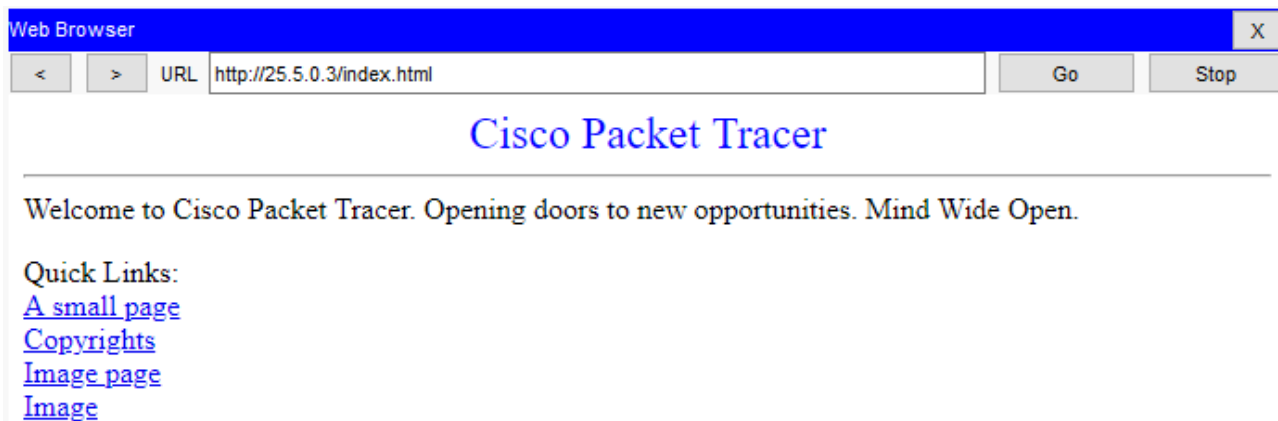


Рисунок 3.43 - Результат тестування доступності HTTP-серверу на робочій станції PC1-1

Тепер спробуємо скопіювати стартову конфігурацію пристрою на сервер, тим самим перевіривши TFTP(рис. 3.44-3.45).

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

Writing startup-config...!!
[OK - 4817 bytes]

4817 bytes copied in 0.001 secs (4817000 bytes/sec)
```

Рисунок 3.44 -Копіювання стартової конфігурації багаторівневого комутатора SwitchMainна TFTP-сервер

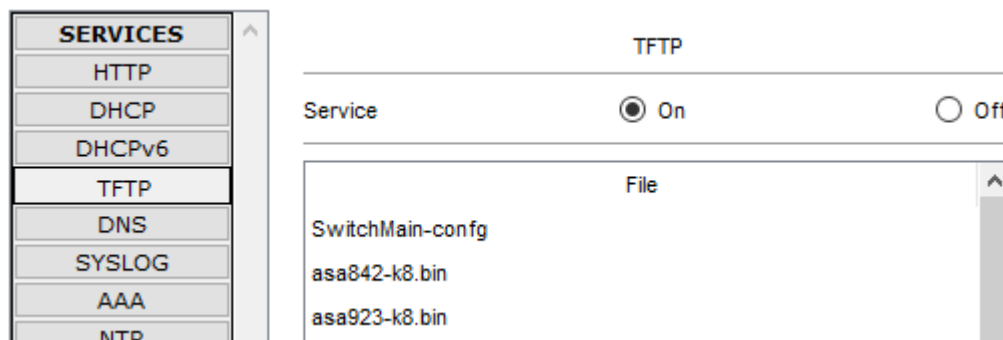


Рисунок 3.45 - Наявність скопійованого файлу стартової конфігурації багаторівневого комутатора SwitchMain на TFTP-сервері

Також на сервері перевіримо наявність повідомлень у журналі подій SYSLOG(рис. 3.46).

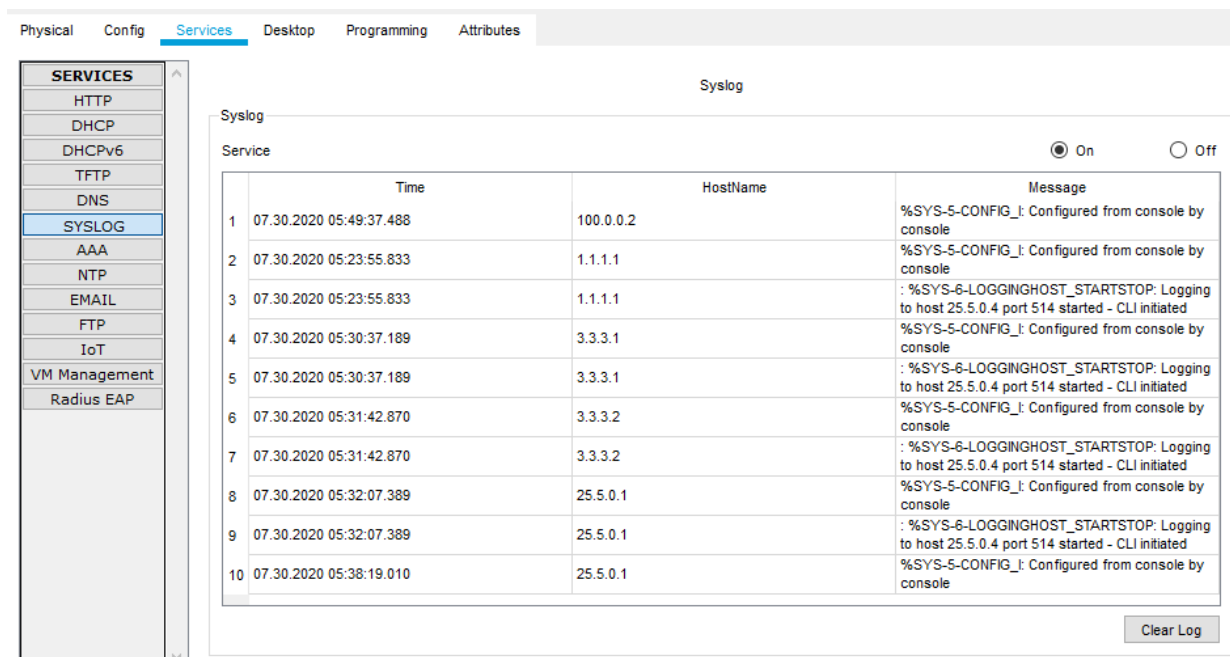


Рисунок 3.46 -Наявність записів в журналі подій SYSLOG

Останнім сервісом, що перевірятиметься є NTP. Його перевіримо за допомогою діагностичних команд (рис. 3.47-3.48).

```
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, - outlier, x falseticker, ~ configured
```

Рисунок 3.47 - Виконання діагностичних команд showclockdetail, showntpstatus та showntpassociations 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, - outlier, x falseticker, ~ configured
```

Рисунок 3.48 -Результат виконання діагностичних команд showclockdetail, showntpstatus та showntpassociations на маршрутизаторі RouterMain

Фізичний доступ до мережного обладнання перевіримо за допомогою консольного кабеля (рис. 3.49-3.50).

```

Connection to switch SwitchFirst For legal users only

User Access Verification

Username: adminer
Password:

SwitchFirst>en
Password:
SwitchFirst#
    
```

Рисунок 3.49 -Спроба фізичного підключення до комутатораSwitchFirst

```

Connection to router RouterMain For legal users only

User Access Verification

Username: adminer
Password:

RouterMain#
*июл 30, 19:59:13.5959: SEC_LOGIN-5-LOGIN_SUCCESS: Login Success
[user: adminer] [Source: 0.0.0.0] [localport: 0] at 19:59:13 UTC Чт
июл 30 2020
    
```

Рисунок 3.50 -Спроба фізичного підключення до маршрутизатораRouterMain

Далі слід перейти до перевірки віддаленого доступу. Його перевірятимемо за допомогою робочої станції PC1-1 (рис. 3.51-3.53).

Telnet / SSH Client

Session Options

Connection Type: SSH

Host Name or (IP address): 1.1.1.1

Username: adminer

Connect

Рисунок 3.51 - Під'єднання для віддаленого доступу з робочої станції PC1-1

SSH Client

Password:

Connection to router RouterInternet For legal users only

RouterInternet#

Рисунок 3.52 - Результат тестування доступності віддаленого доступу до маршрутизатора RouterInternet

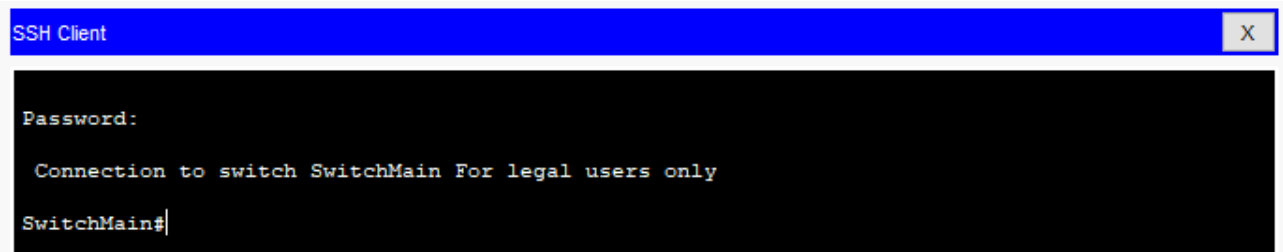


Рисунок 3.53 - Результат тестування доступності віддаленого доступу до комутатора SwitchMain

Як видно, при підключенні обладнання потребує авторизації користувача, що є одною з потреб безпеки.

Наступним кроком перевіримо захист інтерфейсів та захист від підміни DHCP-серверу.

```
SwitchSecond#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
              (Count)          (Count)          (Count)
-----
      Fa0/1      1          1          0      Restrict
      Fa0/2      1          1          0      Restrict
      Fa0/23     1          1          0      Restrict
      Fa0/24     1          1          0      Restrict
      Gig0/2     1          1          0      Restrict
-----

SwitchSecond#show mac address-table interface fa0/1
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
202     0060.47e3.dcdB    STATIC    Fa0/1
SwitchSecond#show mac address-table interface fa0/2
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
202     0030.a3e1.70dd    STATIC    Fa0/2
SwitchSecond#show mac address-table interface fa0/23
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
203     0040.0bc5.45e4    STATIC    Fa0/23
```

Рисунок 3.54 – Тестування PortSecurity

```
SwitchSecond#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----
GigabitEthernet0/1      yes         unlimited
SwitchSecond#
```

Рисунок 3.55 – Тестування DHCP Snooping

Наостанок перевіримо роботу шлагбауму (дверей), зчитувача та камери на правильну послідовність.

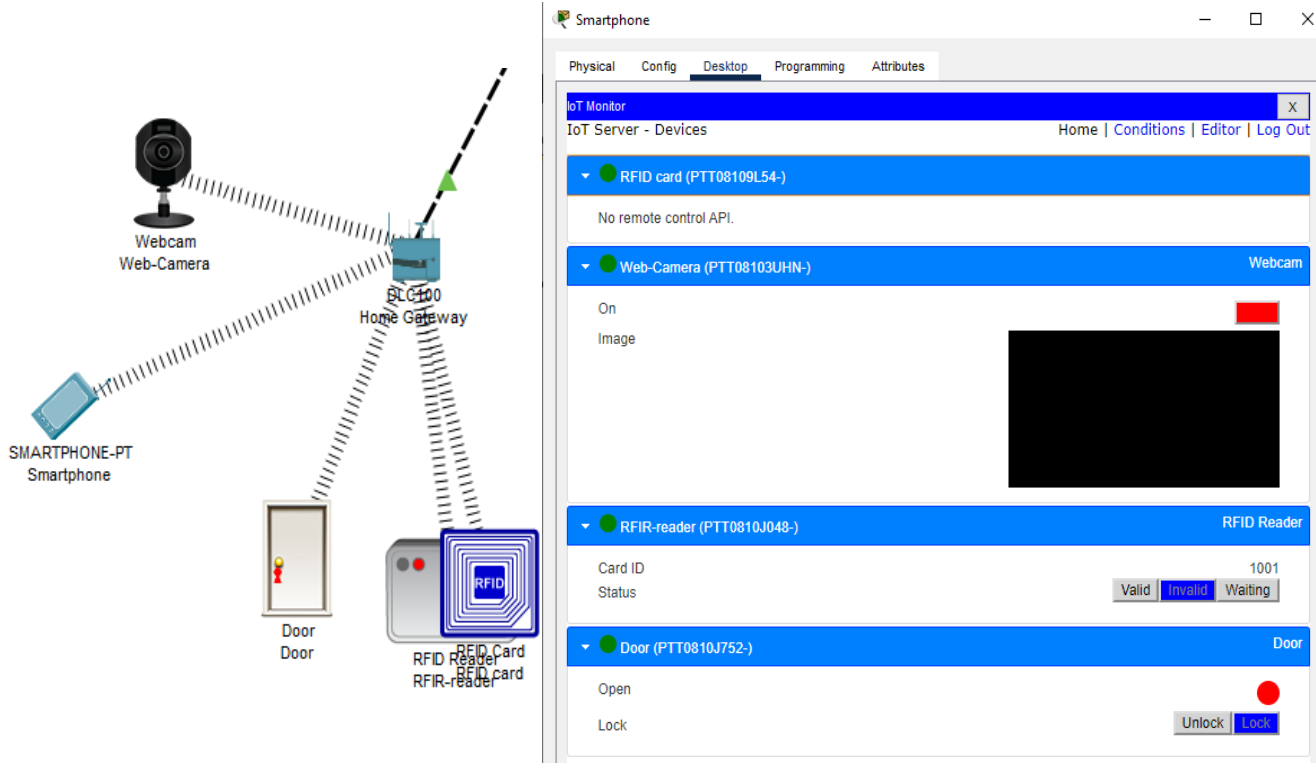
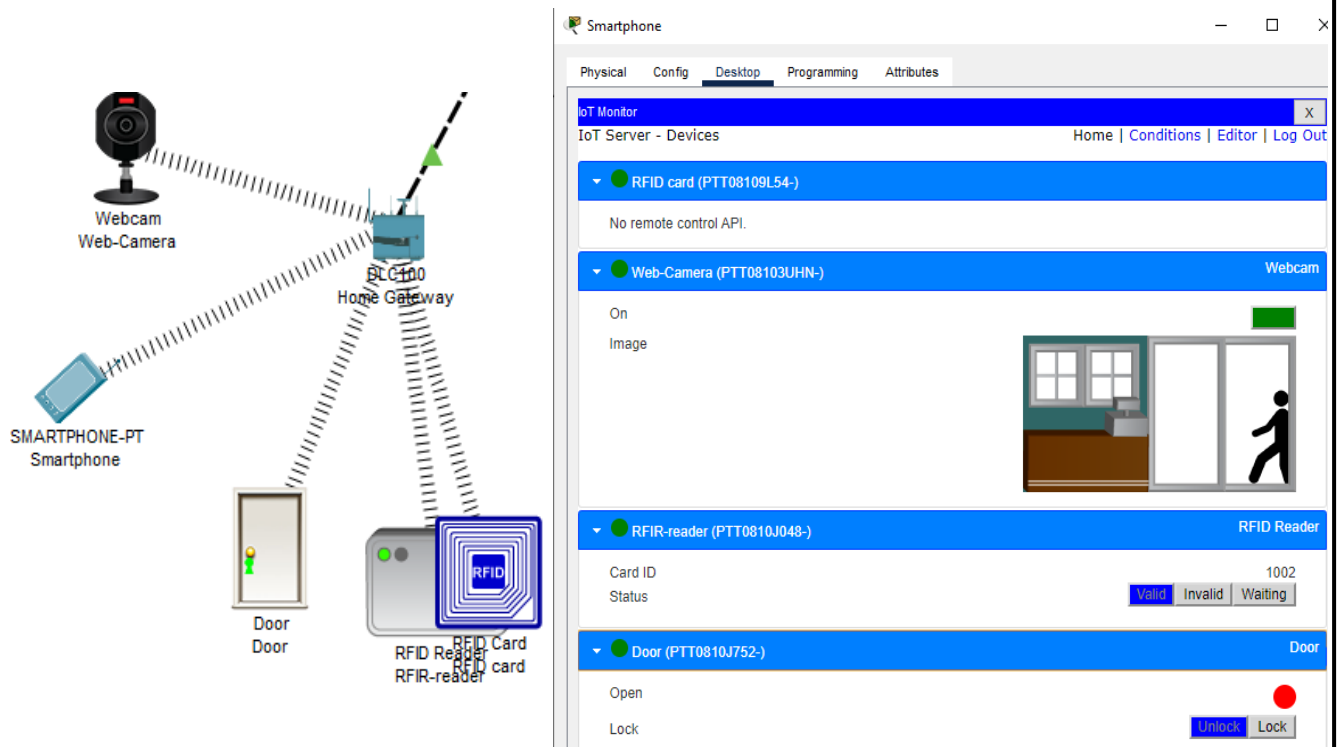


Рисунок 3.56 - Демонстрація піднесення невалідної карти



Рисункок 3.57 - Демонстрація піднесення валідної карти

Висновки до розділу 3

В даному розділі було наведено приклади налаштування основних процесів роботи мережі та їх детальний опис. Розглянуто реалізацію основних функцій необхідних для промислової мережі підприємства, таких як протокол резервування шлюзу HSRP, віртуальні приватні мережі, InterVLANrouting, парольний доступ до мережного обладнання та віддалений доступ з серверу до камер відеоспостереження, зчитувача карт і шлагбауму.

Налаштовано, досліджено та проаналізовано всю топологію мережі.

ВИСНОВКИ

Під час виконання випускної роботи бакалавра було вирішено актуальне завдання, а саме спроектовано та реалізовано систему відеоспостереження для підприємства.

В першому розділі було обґрунтовано необхідність розроблюваної системи відеоспостереження та висунуті вимоги до неї, були розглянуті та детально описані камери відеоспостереження. Дана система на сучасних підприємствах, як правило, використовується разом з СКУД. СКУД повинна формувати і видавати команди управління виконавчим пристроєм, автоматично і вручну розблоковувати турнікети для проходу при аварійних ситуаціях, з видачею сигналу «Тривога», передавати інформацію про стан системи на АРМи, вести облік часу перебування співробітників і відвідувачів.

Також в першому розділі обґрунтовано актуальність даної системи, описана сфера її використання, проаналізовані сучасні системи охорони та сучасні системи контролю і управління доступом.

В другому розділі був розроблений проект мережі промислового підприємства та схему розміщення камер відеоспостереження та мережевого обладнання за генпланом, обрано усі необхідні засоби для реалізації системи: виробника обладнання, конкретні моделі обладнання, методи та технології розподілу IP-адрес, методи захисту обладнання від зовнішнього зловмисного впливу, симулятор роботи з мережним обладнанням.

В третьому розділі було проведено налаштування основних процесів роботи мережі та їх детальний опис. Розглянуто реалізацію основних функцій необхідних для промислової мережі підприємства, таких як протокол резервування шлюзу HSRP, віртуальні приватні мережі, InterVLANrouting, парольний доступ до мережного обладнання та віддалений доступ з серверу до камер відеоспостереження, зчитувача карт і шлагбауму.

Налаштовано, досліджено та проаналізовано всю топологію мережі.

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

В подальшому дана система може бути розширена та масштабована за рахунок своєї ієрархії, модульності і гнучкості.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Технические системы охранной сигнализации Ворона В. А., Тихонов В.А. 2018 г.
2. Системы охранной, пожарной и охранно-пожарной сигнализации, В.Г. Сенилов 2011 г.
3. ПРОЕКТИРОВАНИЕ И ИССЛЕДОВАНИЕ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ В.А. Рыжова 2013г.
4. Анализ современных систем контроля и управления доступом А. Н. Фаткулин 2011 г.
5. Варнеев Николай. Системы охраны периметра -- задачи и проблема выбора. Компания «НИКИРЭТ» // БДИ. - 2006. - № 2 март-апрель // Электронна версія на сайті <http://articles.security-bridge.com/articles/104/11724/>.
6. Смирновский П., Смирновский И. Охрана периметров промышленных объектов. Курс лекций. Часть 1. Лекция 2. Охрана периметра - постановка задачи. Основная задача охраны периметра // Электронна версія на сайті <http://bre.ru/>.
7. Чікіткін В. Охорона периметра провідноволновими засобами // Алгоритм безпеки. - 2008. - №3. - С. 70 - 71.
8. Информационная безопасность в системах охранного видеонаблюдения [Электронный ресурс] – Режим доступа: <https://www.videomax-server.ru/support/articles/informatsionnaya-bezopasnost-v-sistemakh-okhrannogo-videonablyudeniya/>
9. Cisco Enterprise Campus Infrastructure. Best Practices Guide // Cisco Systems, Inc. – 2014. – С. 45.
10. Cisco Catalyst 4500E [Электронный ресурс] – Режим доступа до ресурсу: <https://altastor.ru/products/commutation/cisco/catalyst/4500e/>
11. 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/>

12. Cisco Catalyst 3850 [Електронний ресурс] – Режим доступу до ресурсу:
<https://www.cisco-parts.ru/catalog-cisco/cisco-campus-lan-switches-access/cisco-catalyst-3850/>
13. Cisco Catalyst 3650 [Електронний ресурс] – Режим доступу до ресурсу:
<https://lantorg.com/products/kommutator-cisco-catalyst-3650-24ts-sws-c3650-24ts->
14. 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/>
15. 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>
16. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ МАРШРУТИЗАЦІЇ МІЖ ВІРТУАЛЬНИМИ ЛОКАЛЬНИМИ МЕРЕЖАМИ У МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO [Електронний ресурс] – Режим доступу до ресурсу:
https://learn.ztu.edu.ua/pluginfile.php/64077/mod_resource/content/1/KM_KI_KB_LR-16-2019-2020_KI-3_KB-2-1_KB-2-2_KBK-19-1.pdf
17. 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
18. Configure InterVLAN Routing on Layer 3 Switches [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html>
19. 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

20. 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

21. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ ЗАСОБІВ ВІДДАЛЕНОГО ДОСТУПУ ТА АДМІНІСТРУВАННЯ [Електронний ресурс] – Режим доступу до ресурсу:

https://learn.ztu.edu.ua/pluginfile.php/60583/mod_resource/content/1/KM_KI_KB_LR-08-2019-2020_KI-3_KB-2-1_KB-2-2_KBK-19-1.pdf

22. Карты и RFID технология [Електронний ресурс] – Режим доступу: <https://credit-card.ru/articles/technology/rfid-cards.php>

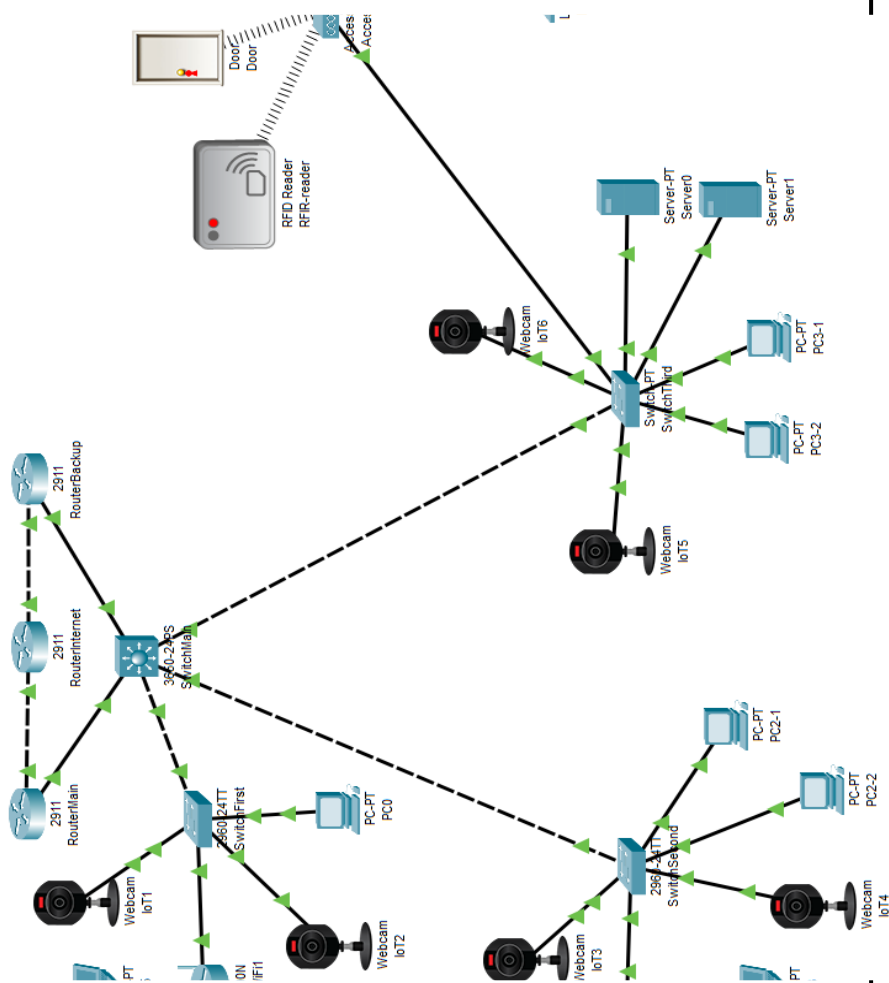
23. Implementation Of Smart Home By Using Packet Tracer [Електронний ресурс] – Режим доступу: <http://www.ijstr.org/final-print/feb2020/Implementation-Of-Smart-Home-By-Using-Packet-Tracer.pdf>

24. Системи відеоспостереження [Електронний ресурс] – Режим доступу: <https://infotel.ua/ua/videonabludenie/>

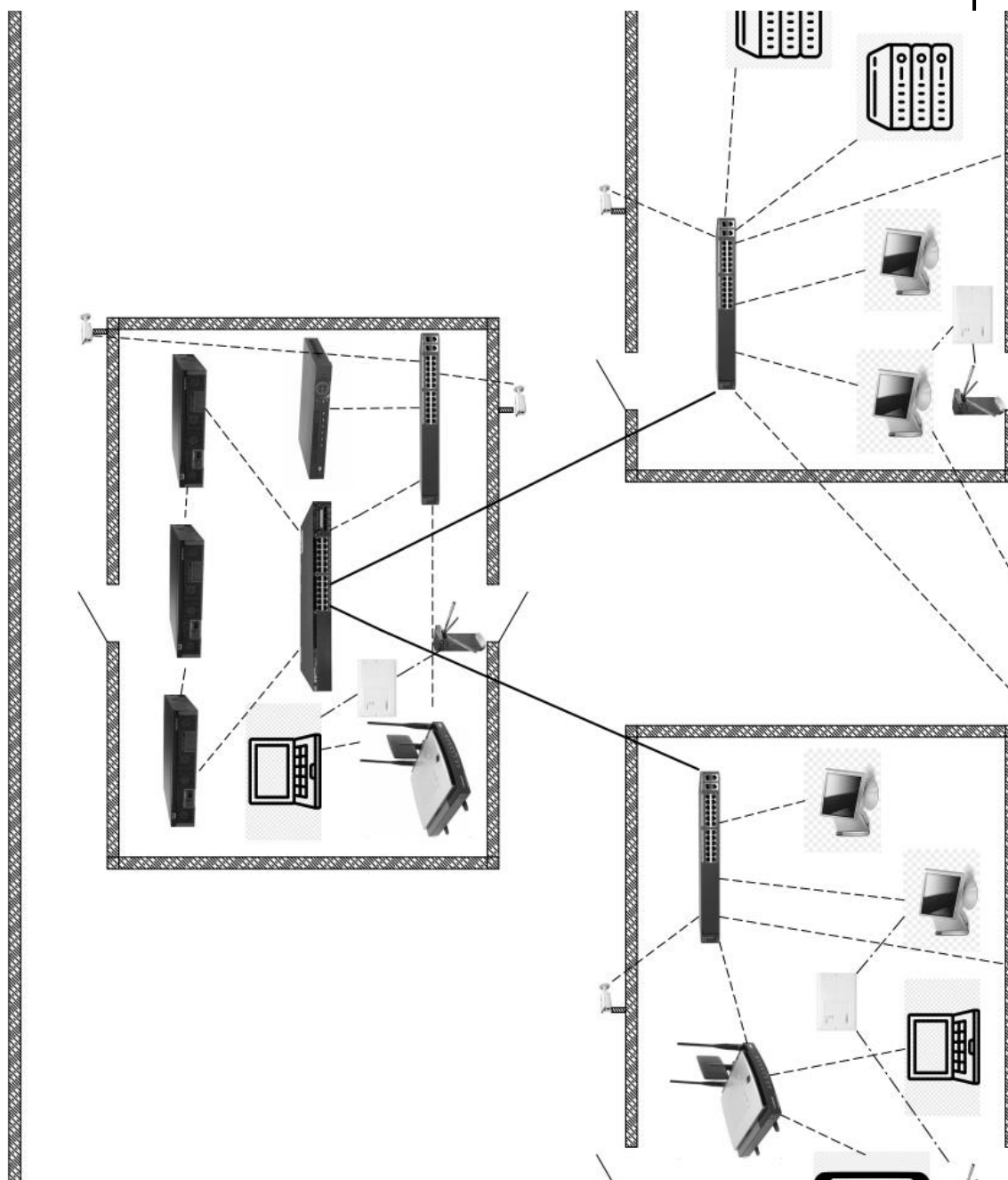
ДОДАТКИ

					КІК.КР.Б – 123 – 05 – ПЗ	
						91

Топологія мережі



Проект мережі підприємства



Лістинги конфігураційних файлів граничного маршрутизуючого обладнання

```

RouterInternet#sh run
Building configuration...

Current configuration : 1909 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
  no ip address
  duplex auto
  speed auto
  shutdown
!
interface Vlan1
  no ip address
  shutdown
!
router ospf 1
  log-adjacency-changes
  redistribute static
  passive-interface Loopback1
  network 1.1.1.0 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 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#sh run
Building configuration...

Current configuration : 1913 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 CISCO2911/K9 sn FTX15249OIZ-
!
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
!
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 1
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
!
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#sh run
Building configuration...

Current configuration : 1921 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 CISCO2911/K9 sn FTX1524WE52-
!
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
!
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
!
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

```

```

SwitchMain#sh run
Building configuration...

Current configuration : 4837 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 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 trunk encapsulation dot1q
  switchport mode trunk
!
interface GigabitEthernet1/0/4
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface GigabitEthernet1/0/5
  switchport trunk encapsulation dot1q
  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 : 3257 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
  mac-address 000c.8560.d101
  ip address 10.1.0.2 255.255.255.0
!
interface Vlan102
  mac-address 000c.8560.d102
  ip address 10.2.0.2 255.255.255.0
!
interface Vlan103
  mac-address 000c.8560.d103
  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 : 3261 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
  mac-address 000a.41c5.5401
  ip address 20.1.0.2 255.255.255.0
!
interface Vlan202
  mac-address 000a.41c5.5402
  ip address 20.2.0.2 255.255.255.0
!
interface Vlan203
  mac-address 000a.41c5.5403
  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 : 1368 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 Vlan1
    ip address 100.0.0.4 255.255.255.0
!
interface Vlan255
    mac-address 000c.cf7e.b001
    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

```