

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 забезпечення безпеки мережі будівельної компанії»

Виконав

студент 4-го курсу, групи КБ-1

спеціальності 125 «Кібербезпека»

 Музичук А. А.

Керівник,

доцент кафедри КІ та КБ, к.т.н., доцент

 Пулеко І. В.

Рецензент

старший викладач кафедри КІ та КБ,

 Філіпов В.О.

Житомир – 2021

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки

_____ Єфіменко А. А.

«12» квітня 2021 р.

ЗАВДАННЯ

на випускн у кваліфікаційну роботу

Студента **Музичука Артура Анатолійовича**

Тема роботи: **Проект забезпечення безпеки мережі будівельної компанії**
затверджена Наказом по університету від «12» квітня 2021 р. № 134/С

Термін здачі студентом закінченої роботи – «22» червня 2021р.

Вихідні дані для роботи:

1. Логічна топологія мережі
2. Маршрутизатори Cisco
3. Комутатори Cisco
4. Операційні системи Cisco IOS, Windows 10
5. Графічний симулятор мереж GNS3

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	25.05.21	25.05.21
2	Єфіменко А.А.	04.06.21	04.06.21
3	Єфіменко А.А.	14.06.21	14.06.21

Керівник _____ Пулеко І. В.

Календарний план

№ з/п	Назва етапів курсового проекту	Строк виконання етапів проекту	Примітки
1	Постановка задачі	15.05.2021	Виконано
2	Опрацювання літературних джерел	25.05.2021	Виконано
3	Проектування проекту	01.06.2021- 02.06.2021	Виконано
4	Налагодження обладнання	05.06.2021- 10.06.2021	Виконано
5	Написання пояснювальної записки	11.06.2021- 20.06.2021	Виконано
6	Захист		Виконано

Студент  Музичук А.А.

Керівник  Пулеко І. В.

АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра містить проект забезпечення безпеки мережі будівельної компанії, пояснювальну записку та ілюстративний матеріал до нього. Пояснювальна записка до випускної роботи містить 61 сторінку, 38 ілюстрацій та 4 таблиці.

Метою кваліфікаційної роботи є підвищення рівня захищеності мережі будівельної компанії.

Визначена мета передбачає вирішення таких **завдань**:

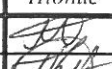
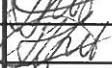
- аналізу існуючих загроз мережевих з'єднань;
- формування основних вимог до захисту мережевих з'єднань;
- проектування топології комп'ютерної мережі та розробки системи адресації;
- вибору та налаштування обладнання для організації роботи мережі.

Об'єктом дослідження є – процес забезпечення безпеки комп'ютерної мережі.

Предмет дослідження – процес створення захищеної мережі будівельної компанії. Для розуміння технологій захисту, шифрування та передачі даних в мережі, зображено структурну схему офісу типової будівельної організації.

Практична значимість роботи полягає в розробці і налаштуванні проекту комп'ютерної мережі будівельної компанії.

КЛЮЧОВІ СЛОВА: МЕРЕЖА, БЕЗПЕКА, VPN, КОРИСТУВАЧІ.

Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Музичук А.А.			«Проект забезпечення безпеки мережі будівельної компанії» Пояснювальна записка	Літ.	Арк.	Аркушів
Перевір.		Пудеко І.В.						
Керівник		Пудеко І.В.				«Житомирська політехніка» ФІКТ зр. КБ – І		
Н. контр.		Філіпов В.О.						
Зав. каф		Єфіменко А.А.						

ABSTRACT

The bachelor's thesis contains a project to ensure the security of the construction company's network, an explanatory note and illustrative material to it. The explanatory note to the final work contains 61 pages, 38 illustrations and 4 tables.

The purpose of the qualification work is to increase the level of security of the construction company's network.

The defined purpose involves solving the following tasks:

- analysis of existing threats to network connections;
- formation of basic requirements for protection of network connections;
- design of computer network topology and development of addressing system;
- selection and configuration of equipment for the organization of the network.

The object of research is the process of ensuring the security of a computer network.

The subject of research is the process of creating a secure network of a construction company. To understand the technologies of protection, encryption and data transmission in the network, the structural diagram of the office of a typical construction organization is shown.

The practical significance of the work lies in the development and configuration of the computer network project of the construction company.

KEY WORDS: NETWORK, SECURITY, VPN, USERS.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		2

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	4
ВСТУП	5
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ БЕЗПЕКИ МЕРЕЖІ	7
1.1 Актуальність захисту мереж	7
1.2 Існуючі загрози мережових з'єднань.....	11
1.3 Основні вимоги до захисту мережових з'єднань	15
Висновки до розділу 1.	19
РОЗДІЛ 2. ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ.....	20
2.1. Вибір топології мережі	20
2.2. Вибір обладнання для передавання інформації в мережі.....	27
2.3. Розробка загальної структури мережі	30
2.4. Вибір технології VPN та протоколу маршрутизації для мережі	34
2.5. Розробка схеми адресації мережі	39
Висновки до розділу 2.	41
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ОБЛАДНАННЯ.....	42
3.1 Вибір обладнання для організації роботи мережі	42
3.2 Вибір ПЗ, налагодження маршрутизації та безпеки пристроїв мережі	49
3.3. Перевірка працездатності мережі	55
Висновки до розділу 3	60
ВИСНОВКИ.....	61
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	62
Додатки	64

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		3

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

VPN – Virtual Private Network - віртуальна приватна мережа

ПК – Персональний комп'ютер

NAT- Network address translation

OSPF - Open Shortest Path First

IP – Internet Protocol

ISAKMP – Internet Security Association and Key Management Protocol - Інтернет протокол асоціацій безпеки та керування ключами

WAN - широкосмугова мережа

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		4

ВСТУП

Крадіжки та дрібні злочини, такі як вандалізм, завжди переслідували будівельну галузь. Поєднання цінного портативного обладнання та тимчасових місць може зробити будівельні фірми та будівельні об'єкти привабливими об'єктами для злодіїв. Фізична крадіжка машин, обладнання та матеріалів може коштувати бізнесу чималих грошей.

Однак протягом останніх років будівельна галузь зіткнулася з новою загрозою. Деякі люди, які працюють у цій галузі, можуть не вважати будівництво об'єктом високого ризику, коли йдеться про кіберзлочинність, порівняно з такими сферами, як фінанси та роздрібна торгівля. Однак справа в тому, що цей порівняно новий вид злочину зараз загрожує кожному виду бізнесу, включаючи малий бізнес та будівельні фірми. Це також означає, що кібербезпеку в будівництві слід сприймати так само серйозно, як і фізичну безпеку.

Ці злочини залишають за собою незліченну кількість жертв. Інформація, що дозволяє ідентифікувати особу, що витікала в результаті недавніх порушень даних, є гарячим товаром у даркнеті для інших злочинців, які прагнуть продовжити цикл шкоди, заподіяної нічим не підозрюючим споживачам.

Тим часом, компанії, які зазнали порушення, можуть очікувати безліч викликів: значні штрафи, судові розгляди, втрата довіри споживачів. Опитування показало, що 81% споживачів припинять взаємодіяти з брендом в Інтернеті після порушення даних, тоді як більше половини малих підприємств, які зазнали порушення даних, очікують припинення бізнесу протягом шести місяців після зазначеного порушення.

Оскільки будівельна галузь рухається вперед, швидко застосовуючи нові технології майже щодня, ризики стають все більш поширеними. Щоб переконатися, що офіси та будівельні майданчики захищені від злодіїв. Зараз оцифровка будівельної галузі означає, що обробляються, зберігаються та

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		5

передаються величезні обсяги важливих даних, включаючи моделі будівель, документи, креслення та персональні дані.

Метою кваліфікаційної роботи є підвищення рівня захищеності мережі будівельної компанії.

Визначена мета передбачає вирішення таких **завдань**:

- аналізу існуючих загроз мережевих з'єднань;
- формування основних вимог до захисту мережевих з'єднань;
- проектування топології комп'ютерної мережі та розробки системи адресації;
- вибору та налаштування обладнання для організації роботи мережі.

Об'єктом дослідження є – процес забезпечення безпеки комп'ютерної мережі.

Предмет дослідження – процес створення захищеної мережі будівельної компанії. Для розуміння технологій захисту, шифрування та передачі даних в мережі, зображено структурну схему офісу типової будівельної організації.

Практична значимість роботи полягає в розробці і налаштуванні проекту комп'ютерної мережі будівельної компанії.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		6

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ БЕЗПЕКИ МЕРЕЖІ

1.1 Актуальність захисту мереж

Кібербезпека - це не те, що традиційно асоціюється з будівельною галуззю. Незалежно від того, займаєтесь ви будівельною галуззю, чи ні, ви, мабуть, будете знати, що загрози кібербезпеки зростають, причому найгірші випадки виходять у ЗМІ з тривожною регулярністю. Проблеми нижчого профілю, що зачіпають дрібні компанії, рідко публікують заголовки, які можуть спокусити вас помилково уявити, що порушення даних стосується лише великих корпорацій. Однак у звіті про розслідування порушень даних Verizon (DBIR) зазначається, що 43% кібератак у 2019 році були спрямовані на малий бізнес [3].

Оскільки будівельна галузь рухається вперед, швидко застосовуючи нові технології майже щодня, ризики стають все більш поширеними. Це не просто випадок, щоб переконатися, що офіси та будівельні майданчики захищені від злодіїв. Зараз оцифровка будівельної галузі означає, що обробляються, зберігаються та передаються величезні обсяги високочутливих даних, включаючи моделі будівель, документи, креслення та персональні дані [3]. Промислові процеси все більше будуються на програмних системах і покладаються на доступність цих систем, щоб забезпечити швидкий зв'язок та аудиторські записи. Збої та порушення даних можуть мати серйозні наслідки. Серед них: переривання бізнесу та збитки або дохід; час і продуктивність; стабільність роботи; і власний капітал бренду.

Збільшення дуже чутливих даних вимагало більше уваги та дій. За даними уряду, проаналізованими Spescops Software, будівельна галузь після багаторічного відставання збільшила витрати на кібербезпеку на 188% у 2018-19-19 роках. Збільшення витрат є позитивною новиною, але врешті-решт добре продумана стратегія зменшення ризику є ключовим фактором мінімізації впливу[3].

Безпека мережі - це комбінація кроків, які запобігають несанкціонованому доступу. Після того, як мережа захищена, користувачі та підключені пристрої

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		7

можуть працювати без порушення даних. Однак у добре захищеній мережі можуть застосовуватися деякі обмеження. Для впровадження мережевої безпеки спеціалісти мережі використовують дуже складні стратегії за допомогою апаратного та програмного забезпечення. Загалом, кожна організація повинна мати спеціальну особу, людей або компанію (залежно від масштабу), яка б займалася їх мережевою безпекою.

На сьогодні порушення комп'ютерної безпеки є звичним явищем і це трапляється по всьому світу щодня. Деякі є незначними з невеликою втратою даних або грошей, але досить багато з них є великими або навіть катастрофічними.

Хакери постійно шукають нові вразливості для того щоб проникнути в систему. Коли мережа не є захищеною, інформація про приватних осіб, організацію або навіть уряд може бути викритою або використаною проти когось[3].

Для сучасного бізнесу оцифрування більше не є конкурентною перевагою - це необхідність. Оскільки все більше компаній переживають цифрову трансформацію, безпека цифрової інфраструктури повинна бути на першому місці серед пріоритетів кожного оператора.

Безпечні та надійні мережі захищають не лише організаційні інтереси та операції, а й будь-якого клієнта або клієнта, який обмінюється інформацією з організацією, крім широкої громадськості.[5] і якщо захист інформації не є достатньою причиною для інвестування в мережеву безпеку, враховуйте вартість: за даними Solarwinds MSP, загальна вартість боротьби зі збитками, заподіяними кіберзлочинністю, до 2021 року, за оцінками, сягає 6 трлн. доларів.

Безпека мережі вже давно є життєво важливим процесом у кожній організації, щоб ефективно забезпечити, щоб жодна стороння сторона не могла будь-яким способом пошкодити свою мережу та ресурси. У міру просування індустрії еволюціонував також спосіб організації моніторингу своїх мереж. Комп'ютери, планшети та мобільні телефони, які ви маєте сьогодні, мають автоматичне оновлення програмного забезпечення [6]. Оскільки організації стають більш

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		8

зв'язаними та залежними від даних, вони стають вразливішими до загроз, які можуть серйозно пошкодити їх мережі. Безпека мережі важлива, оскільки:

- Формує довіру;
- Зменшує ризик;
- Захищає приватну інформацію;
- Уможлиблює більш сучасне робоче місце;
- Економія грошей;
- Економія часу;
- Покращує роботу;
- Підвищує відповідність;
- Мінімізує катастрофічні події даних;

Безпека для великих систем означає безпеку для всіх. Безпека мережі підвищує довіру клієнтів та споживачів, а також захищає ваш бізнес від репутації та законних наслідків порушення безпеки.

Правильне рішення мережевої безпеки допоможе бізнесу дотримуватися ділових та державних норм, а також мінімізує діловий та фінансовий вплив порушення, якщо воно все ж відбудеться[3].

Клієнти покладаються на організацію, щоб захистити їх конфіденційну інформацію. Бізнес також покладається на той самий захист. Безпека мережі забезпечує захист інформації та даних, що передаються в мережі.

Починаючи від дозволу співробітникам безпечно працювати з будь-якого місця за допомогою VPN, до заохочення співпраці із захищеним доступом до мережі, мережева безпека надає можливості для майбутнього роботи. Ефективна мережева безпека також забезпечує безліч рівнів безпеки, які можна масштабувати відповідно бізнесу.

Ризикувати незахищеною мережею може означати втрату бізнесу, штрафні санкції, судові збори, ділові штрафи та багато іншого - потенційний кошмар для прибутку.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		9

Багато людей вважають, що робота з підкріплення захисту ІТ-системи займає більше часу і є більш складною, ніж робота з їх виправлення. Це не може бути далі від істини. Будь-які збої в роботі даних або ІТ – тіньова діяльність безпосередньо знизять продуктивність, послуги та майбутнє зростання бізнесу.

Мережа, яка є більш безпечною та впорядкованою, є більш продуктивною, ефективнішою та керованішою.

Сьогодні в більшості галузей промисловості існує якась форма регуляторного органу, що встановлює правила та керівні принципи кібербезпеки. Поліпшення безпеки мережі посилює зусилля щодо дотримання вимог.

Це повторює, що надійна система мережевої безпеки, що використовує ряд стратегій, є найкращою практикою з першого дня.

Якщо не забезпечити безпеку мережі бізнесу це може дати такі наслідки:

- Перерваний бізнес;
- Втрата даних;
- Штрафи та юридичні наслідки;
- Загальна втрата бізнесу;

Навіть невеликі кібератаки можуть зірвати бізнес, як зазвичай, ризикуючи всім, починаючи від фінансової інформації та перерваної інвентаризації і закінчуючи цифровим відключенням.

Втрата ділового обличчя, мабуть, найменше з ваших турбот під час кібератаки. Конфіденційність споживачів та агентство порушено, а також ваші відповідні ділові дані та конфіденційну інформацію.

Окрім належного звітування про глибину та ширину кібератаки, ваш бізнес може зіткнутися з певними штрафами, передбаченими урядом, за "неправильне використання", а також втратити відповідність чи стандартні сертифікації.

Мало споживачів довірятимуть компанії, резюме якої запламоване цифровим безгосподарним управлінням[3]. Це безпосередньо впливає на ваш результат і здатність залишатися відкритим.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		10

1.2 Існуючі загрози мережових з'єднань

Кіберзлочинність є зростаючою загрозою у всьому світі. Наприклад, у Німеччині спецслужби попереджали, що зростаючі кібератаки - це "бомби із затримкою часу", які загрожують критичній інфраструктурі, а також комерційним інтересам [15]. Існує ряд різних видів кібератак та інших загроз, які можуть поставити під загрозу вразливу будівельну фірму або партнера. До них належать, але не обмежуються:

1) Зловмисне програмне забезпечення буває різних форм, але віруси, хробаки та інші типи призначені для заподіяння шкоди вашим системам та даним. Іноді це може бути спроба вилучити гроші з жертви - наприклад, за допомогою програми-вимагателя - тоді як інші типи шкідливих програм можуть бути чисто зловмисними[16]. Прикладами зловмисного ПЗ є:

- Вірус - вони можуть повторювати себе, підключаючись до програм або файлів на головному комп'ютері, таких як пісні, відео тощо, а потім вони подорожують по Інтернету. Вірус Среерг вперше був виявлений на ARPANET. Прикладами є файловий вірус, макровірус, вірус завантажувального сектора, вірус стелс тощо.

- Хробаки – вони також самовідтворюються за своєю природою, але вони не підключаються до програми на головному комп'ютері. Найбільша різниця між вірусом та хробаками полягає в тому, що останні знають мережу. Вони можуть легко переходити з одного комп'ютера на інший, якщо мережа доступна, і на цільовій машині вони не завдадуть великої шкоди, вони, наприклад, споживають місце на жорсткому диску, тим самим сповільнюючи роботу комп'ютера.

- Троян – концепт трояна абсолютно відрізняється від вірусів та хробаків. Назва Троян походить від історії «Троянський кінь» у грецькій міфології, що пояснює, як греки змогли увійти до укріпленого міста Троя, заховавши своїх солдатів у великому дерев'яному коні, подарованому троянцям. Троянці дуже

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		11

любили коней і сліпо довіряли дару. Вночі солдати вийшли і напали на місто зсередини.

Їх мета полягає в тому, щоб приховати себе всередині програмного забезпечення, яке здається легітимним, і коли це програмне забезпечення буде запущено або інстальовано, вони виконують своє завдання або викрасти інформацію, або будь-яку іншу мету, для якої вони призначені.

2) Вимагальна програма - цей спеціалізований тип шкідливого програмного забезпечення шифрує та «блокує» критично важливі системи та дані, при цьому кіберзлочинці вимагають «викупу», щоб звільнити їх. Цей тип нападів зростає, і за останні пару років були деякі гучні випадки, такі як атака WannaCry, спрямована на NHS у Великобританії, іспанський телекомунікаційний гігант Telefonica та інші організації по всьому світу.

3) Фішинг. Схеми фішингу бувають різних форм, хоча їх центральна мета одна і та ж - змусити реальну людину передавати конфіденційну інформацію. Ця інформація може мати критичне значення для бізнесу, наприклад, мережеві паролі або особисті дані, такі як електронні листи, номери соціального страхування, банківські рахунки та історія хвороби. Фішинг-операції часто є більш успішними, ніж інші типи злому даних, оскільки вони використовують людський «дотик», щоб отримати те, що їм потрібно. Фішинг-хакери часто надсилають повідомлення та інформацію про кадри так, ніби вони надходять із надійного джерела. Вони можуть навіть виглядати як електронні листи від людей, яких ви знаєте, або послуги, якими ви користуєтесь, наприклад, від вашого колеги чи банку, із посиланнями, які спрямовують вас на непомітний веб-сайт. Звідти хакер може імплантувати шкідливе програмне забезпечення на ваш комп'ютер або запросити точну інформацію, яку вони шукають - і все одно прикидаючись кимось, кого ви знаєте.

4) Атаки паролем. Злом паролів користувачів може дати кіберзлочинцям безперешкодний доступ до важливих даних та систем.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		12

5) DDoS може використовуватися для збою веб-сайту або порушення дійсних користувачів у доступі до мереж та систем. Зазвичай це робиться шляхом бомбардування сайту або системи зайвими запитами.

6) Викрадення сесії - це коли хтось користується Інтернетом, їх перегляд та запити класифікуються за допомогою унікального ідентифікатора сеансу. Цей ідентифікатор сеансу - це те, що дозволяє працювати в Інтернеті, оскільки він передає сусідні сервери, ким ви є і що ви вимагаєте від них. Потім ці сервери доставляють цю інформацію назад на ваш пристрій, і ви продовжуєте гуглити, робити покупки, надсилати електронні листи та обмінюватися повідомленнями, як зазвичай. Викрадення сесії, по суті, є як муха на стіні ваших унікальних сеансів. Ідентифікатор, який пов'язує ваш пристрій із сусіднім сервером, більше не є приватним, і хакери можуть видавати себе за ваш комп'ютер або мобільний телефон, викрадати інформацію про запит, а потім отримувати доступ до інших даних на інших серверах. Це складна форма злому, яка може призвести до величезної та різкої втрати даних.

7) Атаки грубої сили на відміну від інших атак даних які намагаються обдурити користувачів або проникнути через захист системи, хакерські що використовують стратегію грубої сили, зазвичай завалюють мережу різними спробами спроб і помилок паролів. Багато хто використовує спеціальне програмне забезпечення, яке може спробувати сотні комбінацій паролів за хвилину, пришвидшивши їх злом і надаючи їм доступ до даних всієї мережі через одну точку входу.

Порушення даних трапляються, коли зовнішня організація може проникнути у ваші цифрові канали та отримати доступ до вашої конфіденційної інформації. Потім ця організація виконує ряд завдань, що скалічують, від викрадення та видалення інформації про клієнтів до вимагання грошей на викуп в обмін на відсутність довгострокових пошкоджень мережі.

Порушення даних, як правило, починаються одним із двох способів:

- Соціальні атаки;

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		13

- Мережеві атаки;

Розглянемо кожен із способів.

Під час соціальної атаки хакери або запрограмовані боти можуть спамувати ваших співробітників, як правило, електронною поштою або прихованим відвідуванням веб-сайту. Вони спробують переконати ваших співробітників видавати паролі та логіни, натискати посилання, відкривати файл або завантажувати матеріали, що видаються безпечними та важливими для бізнесу. Якщо все буде зроблено, хакер може встановити пряму точку входу у вашу мережу, як ви передали їм ключ від вхідних дверей.

Під час мережевої атаки кваліфікований хакер може досліджувати слабкі місця у захисті вашої мережі, такі як слабкі паролі, застарілі операційні системи або навіть неефективне антивірусне програмне забезпечення. Потім вони можуть пройти тунель через такі слабкі місця, щоб висадити віруси або безпосередньо вкрасти інформацію. Найгірші мережеві атаки можуть спричинити невизначений ризик вилучення даних, який вимагатиме повного оновлення системи.

Хоча це загальний процес порушення даних під час кібератаки, існують й інші причини значної втрати даних, включаючи випадкові або зловмисні пошкодження даних, відключення електроенергії та людських помилок при видаленні файлів.

Ось деякі загальні джерела кіберзагроз:

- 1) Злочинні групи
- 2) Хакери
- 3) Терористичні групи
- 4) Хактивісти
- 5) Зловмисні інсайдери
- 6) Корпоративні шпигуни

Злочинні угруповання прагнуть проникнути в системи або мережі з метою отримання фінансової вигоди. Ці групи використовують фішинг, спам, шпигунське

		Музичук А.А.				Арк.
						14
Змн.	Арк.	№ докум.	Підпис	Дата		

та шкідливе програмне забезпечення для викрадення особистих даних, шахрайства в Інтернеті та вимагання системи.

Хакери вивчають різні кібер-методи, щоб зламати захист та використати вразливості в комп'ютерній системі або мережі. Їх спонукає особиста вигода, помста, переслідування, фінансова вигода та політична активність. Хакери розробляють нові типи погроз для хвилювання викликів або хвастощів у хакерській спільноті.

Терористи проводять кібератаки, щоб знищити, проникнути або використати критичну інфраструктуру, щоб загрожувати національній безпеці, компрометувати військову техніку, порушувати економіку та спричиняти масові жертви.

Хакісти проводять кібератаки на підтримку політичних причин, а не фінансових вигод. Вони націлені на галузі, організації чи осіб, які не відповідають їхнім політичним ідеям та порядку денному.

Інсайдери можуть включати співробітників, сторонніх продавців, підрядників або інших ділових партнерів, які мають законний доступ до активів підприємства, але зловживають цим доступом для викрадення або знищення інформації для отримання фінансової або особистої вигоди.

Корпоративні шпигуни проводять промисловий чи діловий шпигунство, щоб отримати прибуток або зірвати бізнес конкурента, атакуючи критичну інфраструктуру, викрадаючи комерційну таємницю та отримуючи доступ.

1.3 Основні вимоги до захисту мережевих з'єднань

Безпека мережі є життєво важливою для захисту даних та інформації клієнта, забезпечення спільних даних у безпеці та забезпечення надійного доступу та роботи мережі, а також захисту від кіберзагроз. Добре розроблене мережеве рішення безпеки зменшує накладні витрати та захищає організації від дорогих втрат, які виникають внаслідок порушення даних або іншого інциденту безпеки. Забезпечення законного доступу до систем, програм та даних дозволяє здійснювати ділові операції та надавати послуги та продукти споживачам [5].

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		15

Існує багато рівнів, на які слід звертати увагу при вирішенні питань безпеки мережі в організації. Атаки можуть відбуватися на будь-якому рівні в моделі рівнів мережевої безпеки, тому обладнання, програмне забезпечення та політика мережевої безпеки повинні бути розроблені з урахуванням кожної області [6].

Безпека мережі, як правило, складається з трьох різних елементів управління: фізичного, технічного та адміністративного. Ось короткий опис різних типів мережевої безпеки:

- Фізична безпека мережі
- Технічна безпека мережі
- Безпека адміністративної мережі

Ось короткий опис того, як працює кожен тип мережевої безпеки:

Контроль фізичної безпеки призначений для запобігання несанкціонованому персоналу отримати фізичний доступ до мережевих компонентів, таких як маршрутизатори, кабельні шафи тощо. Контрольований доступ, такий як замки, біометрична автентифікація та інші пристрої, необхідний у будь-якій організації.

Технічні засоби контролю захищають дані, які зберігаються в мережі або передаються через мережу, в неї або поза нею. Захист подвійний; їй потрібно захищати дані та системи від несанкціонованого персоналу, а також захищати від зловмисної діяльності працівників.

Адміністративний контроль безпеки складається з політик та процесів безпеки, які контролюють поведінку користувачів, включаючи спосіб автентифікації користувачів, рівень їх доступу, а також те, як члени ІТ-персоналу впроваджують зміни в інфраструктуру.

Види захистів мережевої безпеки :

- Брандмауери. Вони контролюють вхідний та вихідний трафік у мережах заздалегідь визначеними правилами безпеки. Брандмауери утримують недоброзичливий трафік і є необхідною частиною щоденних обчислень. Мережева безпека значною мірою покладається на брандмауери, особливо на брандмауери наступного покоління, які зосереджуються на блокуванні шкідливого програмного

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		16

забезпечення та атак на рівні програм. Захищає організацію від цілого ряду шкідливого програмного забезпечення, включаючи віруси, програми-вимагателі, хробаків та троянські програми[16]. Найкраще програмне забезпечення не тільки сканує файли при вході в мережу, але й постійно сканує та відстежує файли.

-Сегментація мережі - визначає межі між сегментами мережі, де активи всередині групи мають спільну функцію, ризик або роль в організації. Наприклад, шлюз по периметру сегментує мережу компанії з Інтернету. Потенційні загрози поза мережею запобігаються, гарантуючи, що конфіденційні дані організації залишаються всередині. Організації можуть піти далі, визначивши додаткові внутрішні межі в межах своєї мережі, що може забезпечити покращений захист та контроль доступу.

-Контроль доступу визначає людей або групи та пристрої, які мають доступ до мережевих додатків та систем, тим самим відмовляючи несанкціонованому доступу та, можливо, погрозам. Інтеграція з продуктами управління ідентифікацією та доступом (IAM) може чітко ідентифікувати користувача та політику контролю доступу на основі ролей (RBAC), що гарантує авторизованому доступу особи та пристрою до об'єкта.

-Віддалений доступ VPN забезпечує віддалений та безпечний доступ до мережі компанії для окремих хостів або клієнтів, таких як телекомунікатори, користувачі мобільних пристроїв та споживачі екстрамережі[19]. На кожному хості зазвичай завантажується програмне забезпечення клієнта VPN або використовується веб-клієнт. Конфіденційність та цілісність конфіденційної інформації забезпечується за допомогою багатофакторної автентифікації, сканування відповідності кінцевій точці та шифрування всіх переданих даних.

-Zero Trust Network Access (ZTNA) - модель безпеки з нульовою довірою стверджує, що користувач повинен мати лише той доступ та дозволи, які потрібні йому для виконання своєї ролі. Це зовсім інший підхід від підходу, що надається традиційними рішеннями безпеки, такими як VPN, які надають користувачеві повний доступ до цільової мережі. Доступ до нульової мережі (ZTNA), також

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		17

відомий як програмно-визначений периметр (SDP), дозволяє детальний доступ до програм організації від користувачів, яким потрібен цей доступ для виконання своїх обов'язків.

-Безпека електронної пошти - розуміються будь-які процеси, продукти та послуги, призначені для захисту ваших облікових записів електронної пошти та вмісту електронної пошти, захищених від зовнішніх загроз. Більшість постачальників послуг електронної пошти мають вбудовані функції захисту електронної пошти, призначені для захисту вас, але їх може бути недостатньо, щоб перешкодити злочинцям отримати доступ до вашої інформації.

-Запобігання втраті даних (DLP) - це методологія кібербезпеки, яка поєднує технології та найкращі практики для запобігання викриттю конфіденційної інформації за межами організації, особливо регламентованих даних, таких як особиста інформація (PII) та відповідні дані: HIPAA, SOX, PCI DSS тощо

-Системи запобігання проникненню (IPS) можуть виявляти або запобігати атакам мережевої безпеки, таким як атаки грубої сили, атаки відмови в обслуговуванні (DoS) та використання відомих вразливих місць. Вразливість - це слабкість, наприклад, в програмній системі, а експлойт - це атака, яка використовує цю вразливість для отримання контролю над цією системою. Коли оголошено про експлойт, зловмисники часто мають можливість скористатися цією вразливістю до того, як застосувати виправлення безпеки. У цих випадках для швидкого блокування цих атак може бути використана Система запобігання проникненню.

-Гіпермасштабна мережева безпека - це здатність архітектури масштабуватися належним чином, оскільки до системи додається підвищений попит. Це рішення включає швидке розгортання та масштабування вгору чи вниз, щоб задовольнити зміни у вимогах безпеки мережі. Завдяки тісній інтеграції мережевих та обчислювальних ресурсів у програмно визначену систему, можна повністю використати всі апаратні ресурси, доступні в кластерному рішенні.

-Безпека хмарної мережі. Програми та робочі навантаження більше не розміщуються виключно локально в локальному центрі обробки даних. Захист

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		18

сучасного центру обробки даних вимагає більшої гнучкості та інновацій, щоб не відставати від міграції робочих навантажень додатків до хмари. Програмно-визначені мережеві (SDN) та програмно-визначені широкосмугові (SD-WAN) рішення дозволяють рішення мережевої безпеки в приватних, загальнодоступних, гібридних та хмарних розгортаннях Firewall-as-a-Service (FWaaS).

1.4 Висновки до розділу 1

Під час написання першого розділу було проаналізовано актуальність захисту мереж та їх місце в будівельних компаніях, її важливість та наслідки того якщо не буде забезпечено її. Проаналізували існуючі загрози мережевих з'єднань, їх види та джерела. Переглянуто основні вимоги до захисту мережі, типи безпеки та види захистів мережевої безпеки.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		19

РОЗДІЛ 2. ПРОЕКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ

2.1. Вибір топології мережі

Мережеві топології є одним з основних будівельних блоків для передачі даних. Вони описують, як мережеві сутності безпосередньо взаємопов'язані між собою, і таким чином визначають, як може протікати інформація. Така структура зв'язків вузлів може будуватися на різних шарах, що призводить до фізичної або логічної топології. Перший буде побудований при підключенні пристроїв фізичним середовищем. Поверх цієї структури обмін даними можна організувати через мережу та прикладний рівень, створюючи логічну або накладену топологію[11].

Фізична топологія та її можливості визначаються активними мережевими пристроями та носіями, такими як тип (и) кабелю, рівень контролю або бажана стійкість до несправностей.

На відміну від цього, логічна топологія - це спосіб дії сигналів на мережевий носій або спосіб передачі даних через мережу від одного пристрою до іншого без урахування фізичного взаємозв'язку пристроїв. Логічна топологія мережі не обов'язково така ж, як її фізична топологія. Наприклад, оригінальна вита пара Ethernet з використанням багаторазових концентраторів була логічною топологією шини з фізичним розташуванням топології зірки. Також Token Ring є логічною топологією кільця, але з'єднана як фізична топологія зірки з модуля доступу до медіа. Логічна класифікація мережевих топологій, як правило, дотримується тих самих класифікацій, що і у фізичній класифікації мережевих топологій, але описує шлях, який проходять дані між використовуваними вузлами, на відміну від фактичних фізичних зв'язків між вузлами.

Логічні топології, як правило, визначаються мережевими протоколами, на відміну від того, що визначаються фізичним розташуванням кабелів, проводів та мережевих пристроїв або потоком електричних або оптичних сигналів, хоча в багатьох випадках шляхи, якими проходять сигнали між вузлами, можуть тісно відповідати логічному потоку даних, отже, домовленість про використання

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		20

термінів логічна топологія та сигнальна топологія взаємозамінні. Логічні топології можуть бути динамічно переналаштовані за допомогою спеціальних типів обладнання, таких як маршрутизатори та комутатори.

Основними топологіями мережі є:

- Point-to-point
- Шина
- Зірка
- Кільцева або кругова
- Сітка
- Дерево
- Гібридна

Топологія Point-to-point - це найпростіша топологія, яка з'єднує два вузли безпосередньо разом із загальним зв'язком. Вся пропускна здатність загальної лінії зв'язку зарезервована для передачі між цими двома вузлами[11]. Точкові з'єднання використовують фактичну довжину дроту або кабелю для з'єднання двох кінців, але можливі й інші варіанти, такі як супутникові канали або мікрохвильові печі.

Змінюючи телевізійні канали за допомогою пульта дистанційного керування, ви встановлюєте точковий зв'язок між пультом дистанційного керування та системою управління телевізором.

Передача даних у топології "точка-точка" може здійснюватися по всій мережі різними способами: у симплексному, повнодуплексному або напівдуплексному.

- У симплексному режимі зв'язку сигнал протікає в одному напрямку, і лише один вузол передає, а інший приймає.
- У напівдуплексному режимі зв'язку кожен вузол може передавати та приймати, але не одночасно.
- У повнодуплексному режимі зв'язку обидві станції одночасно передають і приймають.

Топологія шини, також зветься лінійною топологією, може бути навіть конкретно цілковитою топологією, під час якої кожен комп'ютер і мережевий

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		21

пристрій підключаються як мінімум до одного кабелю або магістралі. Загалом, термін стосується того, як розпізнаються різні пристрої під час роботи в мережі. розраховуючи на якусь мережеву карту, для їх з'єднання використовується коаксіальний або мережевий кабель RJ-45.

Топологія шини несе передані дані по кабелю. оскільки дані потрапляють до кожного вузла, вузол перевіряє адресу призначення (MAC / IP-адресу), щоб визначити, чи відповідає вона їх адресі. Якщо адреса не збігається з вузлом, то вузол більше нічого не робить. Але якщо адреси вузла збігаються з адресами, що містяться в даних, тоді вони обробляються на основі знань. У шині зв'язок між вузлами здійснюється за допомогою передового мережевого кабелю.

Переваги топології шини:

- Це найпростіша топологія мережі для лінійного підключення периферійних пристроїв або комп'ютерів.
- Працює дуже ефективно, коли є невелика мережа.
- Легко підключити або видалити пристрої в цій мережі, не впливаючи на будь-який інший пристрій.
- Дуже економічно вигідне порівняно з іншою топологією мережі, тобто сіткою та зіркою
- Легко зрозуміти топологію.
- Легко розширити, з'єднавши два кабелі.

Недоліки топології шини:

- Топологія шини не підходить для великих мереж.
- Усунення неполадок з окремими проблемами пристрою дуже важке.
- Додаткові пристрої сповільнюють роботу мережі.
- Якщо основний кабель пошкоджений, вся мережа виходить з ладу або розпадається на дві частини.
- Втрата пакетів велика.
- Ця топологія мережі дуже повільна в порівнянні з іншими топологіями.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		22

Топологія зірка. У мережах із топологією зірка кожен хост або клієнт підключений до центрального хабу (комутатора, маршрутизатора, сервера) за допомогою з'єднання точка-точка. Весь трафік, який проходить через мережу, проходить через центральний хаб. Він виконує роль маршрутизатора сигналів. Топологія зірка вважається найпростішою топологією для проектування та реалізації. Перевагою топології зірки є простота додавання додаткових вузлів. Основним недоліком топології зірки є те, що концентратор являє собою одну точку відмови, хоча цей «пристрій» зазвичай дублюється. Зірка займає більше кабелю, ніж, наприклад, шина, але перевага полягає в тому, що якщо кабель вийде з ладу, буде збитий лише один вузол. Якщо один пристрій хоче надіслати дані на інший пристрій, це спочатку надіслати інформацію до хабу, а потім він передає ці дані до призначеного пристрою.

Переваги топології зірки:

- Вона надійна - якщо один кабель або пристрій вийде з ладу, тоді всі інші все одно працюватимуть;
- Є високоефективним, оскільки не може статися зіткнення даних;
- Менш дорога, оскільки кожному пристрою потрібен лише один порт вводу-виводу і бажає бути підключеним до хабу за допомогою однієї лінії зв'язку;
- Легке виявлення несправностей, оскільки посилення часто легко ідентифікувати;
- Відсутність перебоїв у роботі мережі під час підключення або видалення пристроїв;
- Для кожного пристрою потрібен лише один порт, тобто для підключення до хабу;

Недоліки топології зірки:

- Потребує більше кабелів, ніж лінійна шина;
- Якщо підключення мережевого пристрою (мережевого комутатора) не вдається, підключені вузли вимикаються і не можуть брати участь у мережевому зв'язку;

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		23

- Дорожча, ніж топологія лінійної шини, через значення підключаючих пристроїв (мережевих комутаторів);
- Якщо хаб падає, все падає, жоден з пристроїв не може працювати без його.
- Хаб вимагає більше ресурсів та регулярного обслуговування, оскільки це центральна система зірки;
- Потрібне додаткове обладнання (концентратори або комутатори), що збільшує вартість;
- Продуктивність визначається одним хабом;

Кільцева топологія - мережева топологія, яка налаштована круговим способом, коли дані об'їжджають кільце в одному напрямку, а кожен пристрій на кільці діє як ретранслятор, щоб підтримувати сигнал сильним під час руху. Кожен пристрій включає приймач вхідного сигналу та передавач для передачі даних на наступний пристрій у кільці. Коли пристрій надсилає дані, він повинен подорожувати по кожному пристрою на кільці, поки не досягне місця призначення. Кожен вузол є критичною ланкою.

У цій топології пакети здійснюють перехід від одного пристрою до іншого, поки вони не досягнуть потрібного пункту призначення. У цьому випадку передача даних є односпрямованою, але вона також може бути двонаправленою, маючи 2 з'єднання між кожним вузлом мережі, що називається подвійною топологією кільця.

Використовується в локальних мережах та глобальних мережах залежно від карти мережі в комп'ютері.

Переваги кільцевої топології:

- Дані рухаються в одному напрямку, що зменшує ймовірність зіткнення пакетів.
- Завдяки наявності маркера передачі продуктивність кільцевої топології стає кращою, ніж топологія шини при інтенсивному русі.
- Рівний доступ до ресурсів.
- Немає потреби в сервері для контролю зв'язку між вузлами в топології.
- Дешево встановлювати та розширювати.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		24

- Мінімальне зіткнення.
- У цій топології додаткові робочі станції можуть бути додані після, не впливаючи на продуктивність мережі.
- Швидкість передачі даних дуже висока
- Легкий в управлінні.
- Кільцева мережа надзвичайно впорядкована, де кожен пристрій має доступ до маркера і, отже, можливість передавати.

Недоліки кільцевої топології:

- Через односпрямоване кільце пакет даних (маркер) повинен проходити через усі вузли.
- Повна залежність від одного кабелю.
- Продуктивність вона повільніша порівняно з топологією шини
- Це дорого.
- Якщо одна робоча станція вимикається, це впливає на всю мережу або, якщо вузол перестає працювати, вся мережа падає.
- Додавання та видалення будь-якого вузла під час роботи в мережі є складним завданням і може спричинити проблеми в роботі мережі.
- Для того щоб всі комп'ютери могли спілкуватися між собою, вони повинні бути ввімкненими.

Топологія сітки - у цій топології всі комп'ютери з'єднані між собою під час мережі. Кожен комп'ютер не тільки передає власні сигнали, але й передає дані з інших комп'ютерів. Вузли підключені до будь-якого іншого повністю за допомогою виділеного посилення, під час якого інформація переходить від вузлів до вузлів. Кожен вузол має точкове з'єднання з протилежним вузлом. З'єднання всередині сітки часто проводові або бездротові.

Топологія сітки використовує одну з двох схем, що називаються повною та частковою.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		25

У повній всі вузли в мережі пов'язані між собою. Повна сітка забезпечує чудове резервування, але оскільки вона надзвичайно дорога у реалізації, вона зазвичай зарезервована для магістральних мереж.

Часткова є більш практичною в порівнянні з повною сіткою. У частково з'єднаній сітці не потрібно, щоб усі вузли були з'єднані між собою під час мережі. Периферійні мережі з'єднуються за допомогою часткової сітки та працюють із повномасштабною магістраллю в тандемі.

Переваги топології сітки:

- Помилка одного пристрою не призведе до розриву мережі.
- Немає проблем з дорожнім рухом, оскільки для кожного комп'ютера існує виділена точка для посилянь.
- Ця топологія забезпечує безліч шляхів для досягнення успіху в пункті призначення та тонни надмірностей.
- Це забезпечує високу конфіденційність та безпеку.
- Передача даних є більш послідовною, оскільки відмова не порушує її процесів.
- Додавання нових пристроїв не порушить передачу даних.

Недоліки топології сітки:

- Це дорого в порівнянні з протилежними топологіями мережі, тобто топологією зірка, шина, точка-точка.
- Надзвичайно складне втсановлення.
- Потреба в енергії вища, оскільки всі вузли повинні постійно залишатися активними та розподіляти навантаження.
- Вартість впровадження сітки перевищує інші варіанти.
- Існує високий ризик надмірних з'єднань.
- Кожен вузол вимагає додаткових витрат на комунальні послуги, про які слід подумати.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		26

Після розгляду варіантів топлогій та їх переваг і не доліків було вирішено використати для дипломного проекту топлогію зірка. Так як вона є надійною, високоефективною та в ній легко виявити несправності.

2.2. Вибір обладнання для передавання інформації в мережі

Кабель - це носій, за допомогою якого інформація зазвичай переміщується від одного мережевого пристрою до іншого. Існує кілька типів кабелів, які зазвичай використовуються в локальних мережах. У деяких випадках мережа використовуватиме лише один тип кабелю, інші мережі використовуватимуть різні типи кабелів. Тип кабелю, вибраний для мережі, залежить від топології мережі, протоколу та розміру[1]. Розуміння характеристик різних типів кабелів та їх співвідношення з іншими аспектами мережі є необхідним для розвитку успішної мережі.

Який би тип мережі не використовувався, певний тип мережевого носія завжди необхідний для передачі сигналів між комп'ютерами. У мережах використовуються два типи носіїв: носії на основі кабелю, такі як кручена пара, та типи носіїв, пов'язані з бездротовими мережами, такі як радіохвилі.

У мережах, що використовують кабельні носії інформації, існує три основних варіанти:

- Вита пара
- Коаксіальний
- Волоконно-оптичний

Вита пара і коаксіальний кабель використовують мідний дріт для електронної проводки сигналів; волоконно-оптичний кабель використовує скляний або пластиковий провідник і передає сигнали як світло.

Кабелі з витою парою існують дуже давно. Спочатку вони були створені для передачі голосу і широко використовувалися для телефонної комунікації. Сьогодні,

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		27

крім телефонного зв'язку, вита пара є найбільш широко використовуваним середовищем для роботи в мережі.

Популярність витой пари можна пояснити тим, що вона легша, гнучкіша і простіша в монтажі, ніж коаксіальний або волоконно-оптичний кабель. Також дешевші, ніж інші засоби масової інформації, і можуть досягти більшої швидкості, ніж конкуренти. Ці фактори роблять кручену пару ідеальним рішенням для більшості мережевих середовищ.

Коаксіальний кабель зазвичай використовується кабельними операторами, телефонними компаніями та провайдерами Інтернету по всьому світу для передачі даних, відео та голосового зв'язку клієнтам. Він також широко використовувався в будинках.

Він існує довгий час як технологія (з початку 20 століття) і має безліч особливих переваг для надійної та точної передачі.

Він також має обмеження, через які в деяких випадках приходить його замінювати волоконно-оптичним кабелем або, іноді, бездротовими сигналами.

Запорукою успіху коаксіального кабелю стала екранована конструкція, яка дозволяє мідному сердечнику кабелю швидко передавати дані, не піддаючись перешкодам або пошкодженню чинниками навколишнього середовища. Коаксіальний кабель сконструйований таким чином, щоб додати опір загасанню (втрата сили сигналу, коли сигнал проходить через відстань), перехресні перешкоди (погіршення сигналу, спричинене сигналами від інших кабелів, що проходять поруч з ним), та ЕМІ. Три найпоширеніші розміри кабелів - RG-6, RG-11 та RG-59.

Світ телекомунікацій швидко переходить від мідних дротових мереж до волоконної оптики. Оптичне волокно - це дуже тонка нитка чистого скла, яка діє як провідник для світла на великі відстані. Він використовує принцип, відомий як повне внутрішнє відображення. Волоконно-оптичний кабель насправді складається з двох шарів скла: серцевини, яка несе власне світловий сигнал, і оболонки, яка являє собою шар скла, що оточує серцевину. Облицювання має нижчий показник

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		28

заломлення, ніж серцевина. Це спричиняє повне внутрішнє відображення всередині ядра. Більшість волокон працюють дуплексними парами: одне волокно використовується для передачі, а друге - для прийому. Але можна надіслати обидва сигнали через одну нитку. Існує два основних типи волоконно-оптичних кабелів: одномодовий волоконний (SMF) і багатомодовий волоконний (MMF). Різниця в основному полягає в розмірі серцевини. MMF має набагато ширше ядро, що дозволяє поширюватися безлічі режимів (або "променів") світла. SMF має дуже вузьке ядро, яке дозволяє поширюватися лише одному режиму світла.

Переваги волоконно-оптичних кабелів:

- Вони мають практично необмежену інформацію;
- Вони мають високу пропускну здатність (дуже широка смуга пропускання, ТГц або Тбіт / с);
- Вони мають дуже низькі втрати при передачі;
- Вони не розсіюють тепло;
- Вони несприйнятливі до перехресних розмов та електромагнітних перешкод;

Серед переглянутих типів кабелів вибір є 2 типи які можуть підійти для майбутньої мережі – це коаксіальний та волоконно-оптичний кабелі. Порівняймо їхні переваги та в чому їх різниця.

Обидва ці типи кабелів можуть бути використані для передачі відео, аудіо та інших форм даних, і обидва можуть запропонувати певні переваги та недоліки у налаштуванні мережі.

Рішення, що найкраще підходить для ситуації, залежить від відстані з'єднання та обсягу даних, які надсилаються. Волоконно-оптичні кабелі несуть сигнал на кілька миль, перш ніж потрібен ретранслятор. Втрати сигналу вищі в коаксіальному кабелі, тому слід використовувати його на менші відстані. Волоконно-оптичні кабелі несуть набагато більше інформації. Волоконно-оптичний кабель також значно дорожчий. Волоконно-оптичні кабелі зустрічаються рідше в побутових умовах, ніж коаксіальні кабелі.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		29

Коаксіальні кабелі прості в монтажі і дуже довговічні. Оскільки волокно має вищу та швидшу передачу даних, ніж коаксіальне, їх найкраще використовувати для професійних мереж, таких як ті, що знаходяться в бізнес-містечку чи університеті. Якщо ви працюєте над домашньою установкою або мережею передачі даних середньої ємності, то вам, мабуть, було б краще дотримуватися коаксіального кабелю.

Багато сучасних компаній використовують кабельні з'єднання для своїх широкосмугових послуг у бізнесі. Найбільшим недоліком кабельного Інтернету є коливання швидкості. Звертаючись до оптоволоконного Інтернету та кабельного Інтернету, послуга кабельного Інтернету, як правило, ділиться серед багатьох абонентів. Це означає, що якщо в кабельному регіоні є велика кількість користувачів, які одночасно використовують Інтернет-програми, що використовують інтенсивну пропускну здатність, швидкість кожного може коливатися в межах від 100% до 25% від обіцяної швидкості.

Що стосується вартості волокна проти коаксіального волокна, волокно зазвичай набагато дорожче.

Так як мережа яка буде створена є мережею будівельної компанії з багатьма офісами на відстані для яких буде потрібна велика швидкість передачі даних та надійність, було вирішено використовувати волоконно-оптичний кабель.

2.3. Розробка загальної структури мережі

При проектуванні мережі було вирішено розділити мережу на головний офіс та офіси працівників компанії.

Головний офіс складається з 1 маршрутизатора, 1 комутаторів із кінцевим обладнанням та 5 робочих станцій (більшість мереж будуть використовувати VPCS для зменшення навантаження).

А офіси працівників складатимуться з 1 маршрутизатора, 1 комутатора з кінцевим обладнанням та 10 робочих станцій (більшість мереж будуть використовувати VPCS для зменшення навантаження). Таких офісів буде 8.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		30

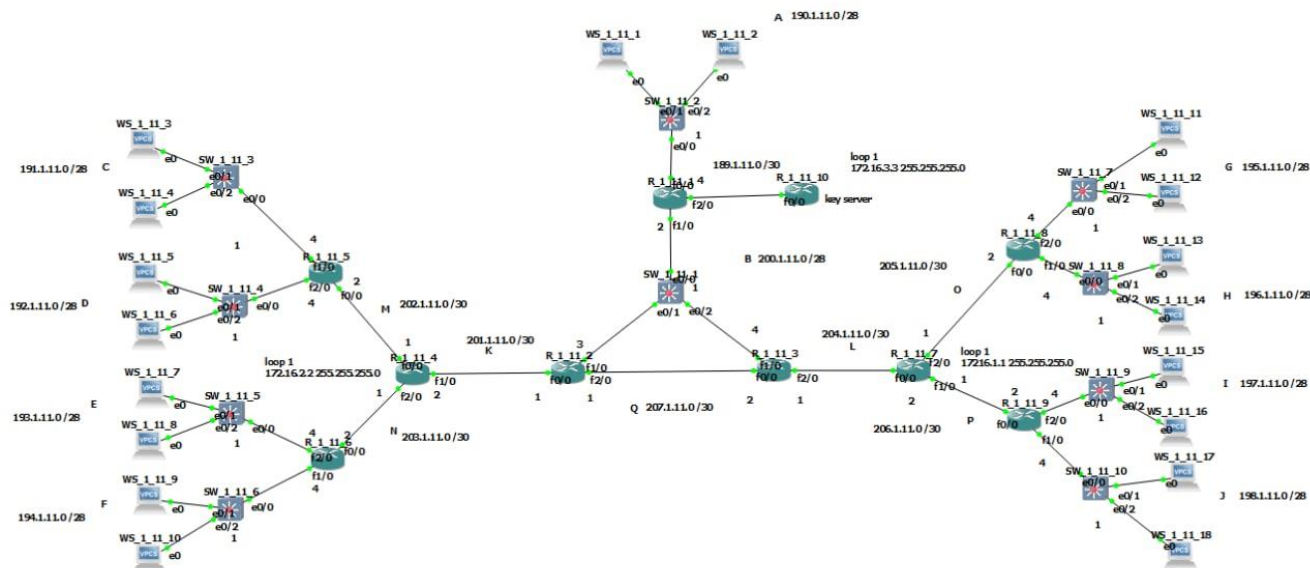


Рисунок 2.1 – Загальна топологія мережі

Загалом у мережі використано 9 маршрутизаторів, 10 комутаторів. Мережа складається з 16 підмереж.

Розглянемо кожну підмережу.

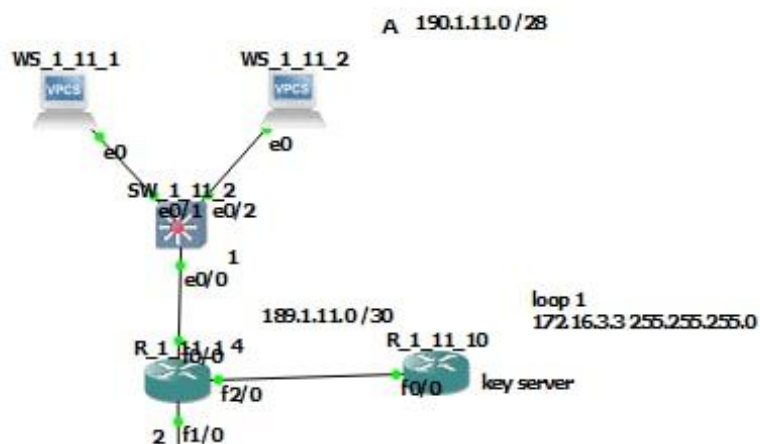


Рисунок 2.2 – Підмережа А та Key Server

Підмережа А складається з одного комутатора SW_1_11_2 на 16 портів до якого підключено 5 робочих станцій. Також він підключений до маршрутизатора R_1_11_1. Всі з'єднання у цій підмережі виконано за допомогою технології виті пари Ethernet та FastEthernet.

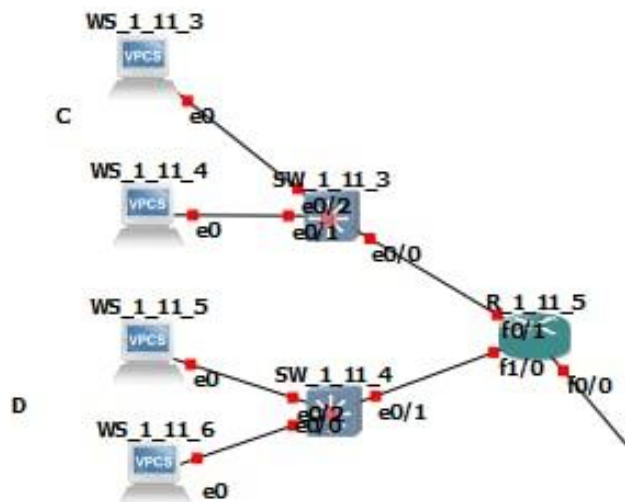


Рисунок 2.3 – Підмережа C та D

З маршрутизатора R_1_11_5 виходить дві підмережі C та D.

Підмережа C складається із одного комутатора на 16 портів до яких підключено 10 робочих станцій та один порт задіяний для підключення до маршрутизатора R_1_11_5.

Підмережа D складається із одного комутатора на 16 портів до яких підключено 12 робочих станцій та один порт задіяний для підключення до маршрутизатора R_1_11_5.

Всі з'єднання у цих підмережах виконано за допомогою технології витої пари Ethernet та FastEthernet.

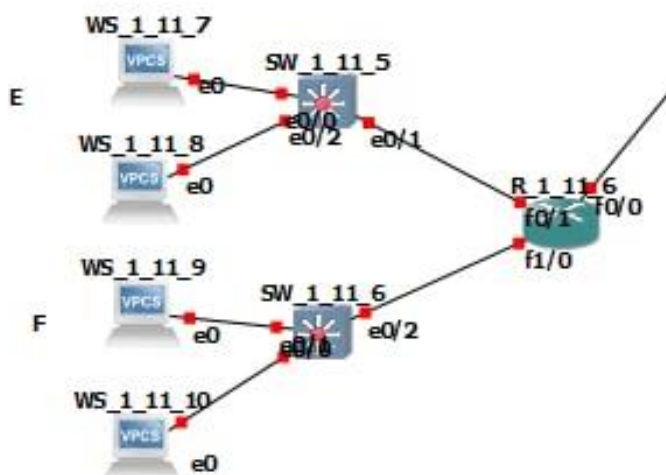


Рисунок 2.4 – Підмережа E, F

		Музичук А.А.			Арк.
					32
Змн.	Арк.	№ докум.	Підпис	Дата	

З маршрутизатора R_1_11_6 виходить дві підмережі Е та F.

Підмережа Е складається із одного комутатора на 16 портів до яких підключено 11 робочих станцій та один порт задіяний для підключення до маршрутизатора R_1_11_6.

Підмережа F складається із одного комутатора на 16 портів до яких підключено 10 робочих станцій та один порт задіяний для підключення до маршрутизатора R_1_11_6.

Всі з'єднання у цих підмережах виконано за допомогою технології витвої пари Ethernet та FastEthernet.

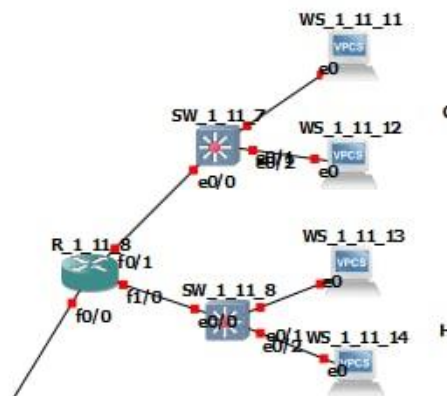


Рисунок 2.5 – Підмережа G, H

З маршрутизатора R_1_11_8 виходить дві підмережі G та H.

Підмережа G складається із одного комутатора на 16 портів до яких підключено 10 робочих станцій та один порт задіяний для підключення до маршрутизатора R_1_11_8.

Підмережа H складається із одного комутатора на 16 портів до яких підключено 10 робочих станцій та один порт задіяний для підключення до маршрутизатора R_1_11_8.

Всі з'єднання у цих підмережах виконано за допомогою технології витвої пари Ethernet та FastEthernet.

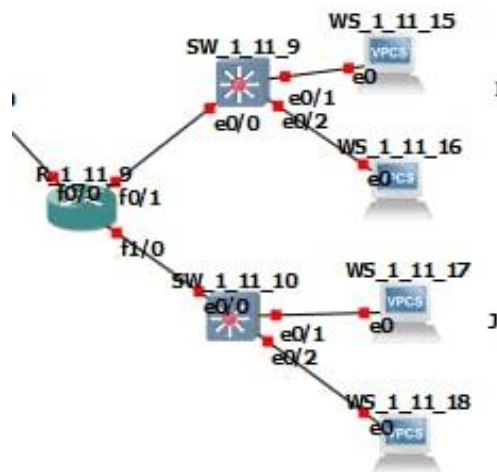


Рисунок 2.6 – Підмережа I, J

З маршрутизатора R_1_11_9 виходить дві підмережі I та J.

Підмережа I складається із одного комутатора на 16 портів до яких підключено 12 робочих станцій та один порт задіяний для підключення до маршрутизатора R_1_11_9.

Підмережа J складається із одного комутатора на 16 портів до яких підключено 10 робочих станцій та один порт задіяний для підключення до маршрутизатора R_1_11_9.

Всі з'єднання у цих підмережах виконано за допомогою технології витвої пари Ethernet та FastEthernet.

2.4. Вибір технології VPN та протоколу маршрутизації для мережі

Віртуальну приватну мережу (VPN) можна визначити як спосіб забезпечення безпечного спілкування між членами групи за допомогою використання загальнодоступної телекомунікаційної інфраструктури, збереження конфіденційності через використання протоколу тунелювання та процедур безпеки. Існує багато різних рішень VPN, і просто вирішити, яке з них вибрати, може бути складно, оскільки всі вони мають переваги та недоліки[19]. VPN можна класифікувати як безпечні або надійні VPN, клієнтські або веб-VPN, VPN на базі клієнта або постачальника, або зовнішні або внутрішні VPN. Ці категорії часто

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		34

перекривають одна одну. Для того, щоб вирішити, які рішення VPN вибрати для різних частин інфраструктури підприємства, обраним рішенням повинно бути те, яке найкраще відповідає вимогам підприємства.

Раніше організації або підприємства фізично встановлювали лінії на великі відстані, щоб забезпечити безпечну передачу даних. Однак ця система непрактична для кожного підприємства та повсякденних користувачів через вартість, простір та час, необхідні для таких установок. В останні роки, з експоненціальним зростанням Інтернету, ландшафт телекомунікацій докорінно змінився, і Інтернет став частиною майже всіх аспектів розвиненого світу, включаючи освіту, банківську справу, бізнес та політику. За останні два десятиліття громадський Інтернет виявився вразливим для зловмисників, які шукають конфіденційну інформацію. Найновішим рішенням цієї проблеми стала віртуальна приватна мережа на основі IP (IPVPN). Віртуальну приватну мережу (VPN) можна визначити як спосіб забезпечення безпечного зв'язку між членами групи за допомогою використання загальнодоступної телекомунікаційної інфраструктури, збереження конфіденційності за допомогою протоколу тунелювання та процедур безпеки. Системи VPN надають користувачам ілюзію повністю приватної мережі. Віртуальну приватну мережу IP (IPVPN) можна визначити як реалізацію VPN, яка використовує загальнодоступні або спільні ресурси мережі IP для емуляції характеристик приватної мережі на основі IP. Основною метою VPN є надання підприємствам тих самих можливостей, або навіть кращих, як у приватних мережах, але з набагато меншими витратами.

Віртуальна приватна мережа (VPN) - це з'єднання, яке забезпечує безпечне приватне спілкування через незахищену мережу, таку як загальнодоступна мережа. Як правило, VPN забезпечує з'єднання між мережевими пристроями. Термін "приватний" означає, що весь трафік всередині VPN зашифрований, а ресурси розподіляються лише між уповноваженими групами користувачів і контролюються різними рівнями контролю доступу. Термін "віртуальна" означає, що VPN виглядає як приватна мережа з точки зору користувача і складається з віртуальної топології,

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		35

що управляється незалежно, хоча основна мережа є спільною для всіх, хто використовує мережу. Крім того, VPN дешева, оскільки вона зазвичай використовує загальнодоступну мережу замість дорогого орендованого каналу послуг.

Спочатку VPN був пов'язаний з мережами Frame Relay. Компанії використовували виділені лінії та послуги рівня 2, такі як Frame Relay, щоб з'єднати свої вузли з посиланнями, якими вони володіли. Кадрові ретрансляційні мережі вважаються безпечними, оскільки трафік клієнтів буде передаватися заздалегідь визначеним шляхом (Постійний віртуальний контур). Однак, із швидким розвитком мережі IP, VPN почала мігрувати зі звичайного ретранслятора рівня 2 до мережі на базі IP рівня.

VPN можна класифікувати різними способами.

За протоколами. Для встановлення з'єднання і клієнт, і сервер повинні використовувати один і той же протокол VPN:

- Протокол тунелювання точки до точки (PPTP). PPTP - це стандартний протокол тунелювання, розроблений PPTP Forum, який складається з Microsoft та деяких інших постачальників віддаленого доступу.
- Протокол тунелювання другого рівня (L2TP). L2TP - це комбінація PPTP та переадресації другого рівня (L2F), розроблена IETF.
- Захист протоколу Інтернету (IPSec). IPSec - це структура відкритих стандартів IETF, спрямованих на захист трафіку на мережевому рівні.
- Шар захищеного сокета (SSL). SSL - це протокол вищого рівня безпеки, розроблений Netscape. SSL зазвичай використовується з HTTP для забезпечення безпечного перегляду веб-сторінок, що називається HTTPS.
- Комутація міток з декількома протоколами (MPLS). MPLS - це технологія комутації пакетів яка розроблена завдяки численним попереднім технологіям, таким як "Перемикання міток" Cisco та "ARIS" IBM. Ідея полягає в тому, що маленька мітка або стек міток вставляється між лінією даних та заголовками мережевого рівня для прийняття ефективних рішень щодо маршрутизації.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		36

За топологією:

- Peer to Peer VPN встановлює захищений тунель між двома комп'ютерами через загальнодоступні мережі. IP-адреса буде присвоєна кожному кінці тунелю, щоб два комп'ютери могли спілкуватися один з одним так, ніби вони з'єднані фізичним кабелем Ethernet.
- Site to Site VPN. Встановлює захищений тунель між двома мережами через загальнодоступний Інтернет, де кінцевими точками тунелю є концентратор VPN та сервер VPN. Ці VPN шифрують лише трафік між концентраторами VPN та серверами VPN, а будь-який трафік поза кінцевими точками тунелю не захищений. VPN від сайту до сайту широко використовується між головним офісом компанії та віддаленим офісом.
- Client to Server VPN. Клієнт-сервер VPN встановлює захищений тунель між клієнтом VPN і певною мережею через загальнодоступні мережі. Клієнт VPN може підключатися до всіх комп'ютерів у певній мережі. Однак, на відміну від Peer to Peer VPN, клієнт-сервер VPN шифрує лише трафік між клієнтом VPN та сервером VPN а трафік між сервером VPN та іншими комп'ютерами у певній мережі не захищений.

Серед багатьох технологій VPN вибір було зупинено на 2 варіантах: EasyVPN та GetVPN.

EasyVPN використовує клієнтський протокол Unity, який дозволяє визначати більшість параметрів IPSec VPN на шлюзі IPSec, який також є сервером EasyVPN. Коли клієнт EasyVPN ініціює тунельне підключення IPSec, сервер EasyVPN передає політики IPSec та інші атрибути, необхідні для формування тунелю IPSec, до клієнта EasyVPN і створює відповідне тунельне з'єднання IPSec.

Тунель на клієнті EasyVPN може бути ініційований автоматично або вручну, або він може бути викликаний трафіком, залежно від конфігурації або типу використовуваного клієнта EasyVPN. На клієнті EasyVPN потрібна мінімальна конфігурація.

EasyVPN забезпечує наступний загальний процес конфігурації:

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		37

- Easy VPN Переговори про параметри тунелю: У EasyVPN це можна зробити за допомогою алгоритмів шифрування, терміну служби SA тощо.
- Легка автентифікація користувачів VPN: у програмі Easy VPN це може передбачати перевірку облікових даних користувача за допомогою XAUTH.
- Автоматична конфігурація Easy VPN: у програмі EasyVPN її можна виконати, натискаючи такі атрибути, як IP-адреса, DNS, WIN тощо, використовуючи MODECFG.

GETVPN називається груповим зашифрованим транспортним VPN; це позбавляє від необхідності компромісу між мережевою розвідкою та конфіденційністю даних у приватних середовищах глобальної мережі. GET VPN спрощує надання та управління VPN. GET VPN визначає нову категорію VPN, яка не використовує тунелі.

Отже, GETVPN не є технологією VPN від точки до точки для підключення до віддалених локацій. GDOI - це протокол управління груповими ключами, який використовується для надання набору ключів IPSec групі пристроїв IOS, які називаються Group Members (GM), які хочуть безпечно спілкуватися, тобто GDOI запускається між GM та сервером ключів (KS). Ці ключі періодично оновлюються на всіх пристроях за допомогою процесу, який називається rekey.

За допомогою GETVPN:

- Можливо спрощувати миттєвий зв'язок між гілками та забезпечувати низьку затримку та тремтіння, дозволяючи постійний прямий зв'язок між сайтами, не вимагаючи транспорту через центральний хаб.
- Можливо максимізувати свою мережеву безпеку, і вона забезпечує шифрування мереж MPLS, зберігаючи при цьому мережевий інтелект, такий як з'єднання з повною мережею, природний шлях маршрутизації та якість обслуговування (QoS).
- Можливо можете дотримуватися державного законодавства та законів про конфіденційність, і це допомагає вам дотримуватися вимог безпеки та внутрішнього регулювання, шифруючи весь трафік глобальної мережі.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		38

- Також GETVPN надасть вам гнучкість управління та усуне складне однорангове керування ключами за допомогою групових ключів шифрування. Після порівняння технологій VPN було вирішено використати в майбутній мережі GetVPN.

Протоколом маршрутизації для мережі було вирішено використати OSPF.

OSPF - це протокол внутрішнього шлюзу (IGP), який направляє пакети в рамках однієї автономної системи (AS). OSPF використовує інформацію про стан зв'язку для прийняття рішень про маршрутизацію, роблячи обчислення маршруту, використовуючи алгоритм найменшого шляху (SPF) (також званий алгоритмом Дейкстри)[12]. Кожен маршрутизатор, на якому запущено OSPF, заповнює оголошення стану зв'язку по всій АС або області, яка містить інформацію про підключені до цього маршрутизатора інтерфейси та метрики маршрутизації. Кожен маршрутизатор використовує інформацію в цих оголошеннях про стан зв'язку, щоб розрахувати шлях із найменшими витратами до кожної мережі та створити таблицю маршрутизації для протоколу.

2.5. Розробка схеми адресації мережі

Для мережі процес розподілу адрес по діапазону відбувався таким чином, щоб використати мінімальну кількість IP-адрес, забезпечивши при цьому потреби підключених вузлів.

Розподіл адрес :

SW_1_11_1 – R_1_11_1 – 200.1.11.2 /28

SW_1_11_1 – R_1_11_2 – 200.1.11.3 /28

SW_1_11_1 – R_1_11_3 – 200.1.11.4 /28

R_1_11_2 – R_1_11_4 – 201.1.11.0/30

R_1_11_3 – R_1_11_7 – 204.1.11.0/30

R_1_11_7 – R_1_11_8 – 205.1.11.0/30

R_1_11_7 – R_1_11_9 – 206.1.11.0/30

R_1_11_4 – R_1_11_5 – 202.1.11.0/30

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		39

R_1_11_4 – R_1_11_6 – 203.1.11.0/30

Розподіл адрес для зв'язку між маршрутизаторами та підмережами:

R_1_11_1 – SW_1_11_2 – 190.1.11.0/28

R_1_11_5 – SW_1_11_3 – 191.1.11.0/28

R_1_11_5 – SW_1_11_4 – 192.1.11.0/28

R_1_11_6 – SW_1_11_5 – 193.1.11.0/28

R_1_11_6 – SW_1_11_6 – 194.1.11.0/28

R_1_11_8 – SW_1_11_7 – 195.1.11.0/28

R_1_11_8 – SW_1_11_8 – 196.1.11.0/28

R_1_11_9 – SW_1_11_9 – 197.1.11.0/28

R_1_11_9 – SW_1_11_10 – 198.1.11.0/28

Розрахунок IP адрес для підмереж наведені у наступних таблицях

Таблиця 2.1 – Адресація підмережі А

Призначення	IP-адреса
Адреса мережі	190.1.11.0
Маска мережі	255.255.255.240
Інвертована маска	0.0.0.15
Мінімальна адреса	190.1.11.1
Максимальна адреса	190.1.11.14
Широкомовна адреса	190.1.11.15
Шлюз по замовчуванню	190.1.11.1
Діапазон адрес комутаторів	190.1.11.1
Діапазон адрес майбутніх ПК	190.1.11.2 - 190.1.11.3 - 190.1.11.14
Діапазон вільних адрес	190.1.11.4

Таблиця 2.2 – Адресація підмережі С

Призначення	IP-адреса
Адреса мережі	191.1.11.0
Маска мережі	255.255.255.240
Інвертована маска	0.0.0.15
Мінімальна адреса	191.1.11.1
Максимальна адреса	191.1.11.14
Широкомовна адреса	191.1.11.15
Шлюз по замовчуванню	191.1.11.1
Діапазон адрес комутаторів	191.1.11.1
Діапазон адрес майбутніх ПК	191.1.11.2 - 191.1.11.3 - 191.1.11.14
Діапазон вільних адрес	191.1.11.4

Висновки до розділу 2

В другому розділі було розглянуто види топологій, їх переваги та недоліки, а також обрано кращий варіант для майбутньої мережі. Було вибрано обладнання для передавання інформації в мережі, види кабелів, їх переваги та обрано кращий для мережі. Також було розроблено загальний вид мережі, кількість маршрутизаторів, комутаторів та ПК. Також було вибрано технологію VPN, а саме GetVPN та протокол маршрутизації OSPF для мережі. І в останньому підрозділі було розроблено схему адресації мережі, , забезпечивши при цьому потреби підключених вузлів.

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ОБЛАДНАННЯ

3.1 Вибір обладнання для організації роботи мережі

Так як під час проектування мережі було вирішено задля надання більшої безпеки передачі даних використати GetVPN, а так як ця технологія є розробкою компанії Cisco, було вирішено використовувати їхню продукцію для побудови мережі.

Cisco Systems, Inc. є провідним світовим постачальником комп'ютерних мережевих продуктів, систем та послуг. Продуктова лінійка компанії включає маршрутизатори, комутатори, пристрої віддаленого доступу, перекладачі протоколів, пристрої Інтернет-послуг, а також програмне забезпечення для управління мережами та мережею, кожна з яких поєднує географічно розподілені локальні мережі (LAN), глобальні мережі (WAN) та сам Інтернет. Cisco обслуговує три основні сегменти ринку: великі організації - включаючи корпорації, урядові структури, комунальні підприємства та освітні установи - потребують складних мережевих рішень, які, як правило, об'єднують кілька місць; постачальники послуг, включаючи постачальників доступу до Інтернету, телефонних та кабельних компаній та постачальників бездротового зв'язку; та малий та середній бізнес, потреби яких включають експлуатаційні мережі, підключення до Інтернету та / або зв'язок з діловими партнерами. Компанія дедалі більше розвиває досвід у галузі волоконно-оптичних мереж, а також супутній досвід мультисервісних мереж, які пропонують відео- та голосові можливості на додаток до традиційних можливостей передачі даних.

Комутація - це інтегрована мережева технологія, що використовується в кампусах, філіях та центрах обробки даних. Комутатори використовуються всередині будівель в локальних мережах (LAN) і на великі відстані в широкомасштабних мережах (WAN). Комутаційні продукти компанії пропонують різні форми підключення до кінцевих користувачів, робочих станцій, IP-телефонів, бездротових точок доступу та серверів, а також функціонують як агрегатори в

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		42

локальних та глобальних мережах. У його комутаційних системах використовується декілька технологій, включаючи Ethernet, Power over Ethernet, Fibre Channel over Ethernet (FCoE), пакетну передачу через синхронну оптичну мережу та багатопроTOCOLьна комутація за мітками. Багато комутаторів компанії розроблені для підтримки інтегрованого набору розширених служб, що дозволяє організаціям бути більш ефективними, використовуючи один комутатор для декількох мережевих функцій, а не кілька комутаторів для виконання тих самих функцій.

Модульні комутатори з фіксованою конфігурацією також включають продукти, такі як оптичні модулі, які спільно використовуються на різних платформах продуктів. Його портфоліо комутацій також включає віртуальні комутатори та відповідні пропозиції. Ці продукти забезпечують функцію перемикання для віртуальних машин і призначені для роботи з віртуальними службами для оптимізації безпеки та поведінки додатків. Компанія Cisco ACI складається з комутаторів Cisco Nexus серії 9000, вдосконаленого програмованого контролера переривань Cisco (APIC), що супроводжує централізовану функцію управління політикою, інтегровану фізичну та віртуальну інфраструктуру та відкриту екосистему постачальників мереж, зберігання, управління та оркестровки.

Центр обробки даних. Уніфікована обчислювальна система Cisco (UCS) дає можливість ІТ, поєднуючи обчислювальну, мережеву та інфраструктуру зберігання з управлінням та віртуалізацією. Її архітектура забезпечує пули керованої політикою компонованої інфраструктури, яку клієнти можуть оптимізувати для традиційних робочих навантажень, аналітики даних та власних хмарних додатків, все в операційному середовищі з відкритим інтерфейсом прикладних програм (API) для сумісності та автоматизації.

Безпека. Портфоліо продуктів та послуг компанії, розроблене для розробки, пропонує рішення, яке збирає та передає інформацію з координованим акцентом на загрози в усьому континуумі атак - до, під час та після атаки. Ці рішення включають безпеку мережі та центрів обробки даних, вдосконалений захист від загроз, безпеку

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		43

Інтернету та електронної пошти, доступ та політику, уніфіковане управління загрозами та консультації, інтеграцію та керовані послуги. Категорія безпеки включає рішення брандмауера наступного покоління (NGFW), орієнтоване на загрози. Компанія інтегрувала своє рішення FirePOWER Services (NGIPS Sourcefire) у свій асортимент удосконалених пристроїв безпеки (ASA) для створення рішень NGFW, орієнтованих на загрози. Він також включає кілька апаратних платформ, які також можуть бути включені за допомогою служб FirePOWER, такі як ASA 5506-X, 5508-X, 5516-X, 5506H та FirePOWER 9300.

Отже, для мережі було вирішено використати продукти саме цієї компанії. А саме модель маршрутизатора ISR4451 та комутатор CISCO C9300-24T-A . Але через обмеження програмного забезпечення в якому буде налаштовуватися та складатися мережа буде використано більш старіші моделі маршрутизаторів та комутаторів.

Маршрутизатор інтегрованих служб Cisco 4451, названий ISR4451-X, який підтримує 2 слоти розширеного сервісного модуля (SM-X), забезпечує загальну пропускну здатність від 1 Гбіт / с до 2 Гбіт / с. Цей маршрутизатор також підтримує два типи DDRM, площину передачі даних та площину управління / обслуговування, що полегшує адміністратору управління маршрутизатором.



Рисунок 3.1 – Маршрутизатор Cisco 4451

Маршрутизатор Cisco ISR4451-X / K9 підтримує всю функціональність рівня L7, надаючи замовникам призначені для користувача послуги найвищої якості, високу масштабованість архітектури, захист інвестицій і мінімальні витрати на установку.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		44

Маршрутизатор Cisco 4451-X може забезпечити підтримку PoE завдяки 2 з 4-х портів SFP / RJ-45 на передній частині корпусу. Так само роутер оснащений 3 NIM слотами, 1 SM слотом, 8 Гб flash-пам'яті, 2 Гб оперативної пам'яті (Data Plane), 4 Гб оперативної пам'яті (Control Plane), Integrated Services Card (ISC) слотом на материнській платі для PVDM4-модулів з високими характеристиками DSP для сервісів голосу і відео.

В маршрутизатор Cisco 4451-X можна встановити серверні модулі Cisco Unified Computing System E-серії, це дозволить об'єднувати і резервувати ресурси і сервіси на рівні локальної мережі. Серверні модулі дають можливість запускати програмні компоненти (такі як Cloud Connector) для спільної роботи з хмарними сервісами на основі вбудованих апаратних ресурсів.

Особливості:

- Багатоядерна процесорна архітектура з використанням операційної системи IOS-XE, що динамічно адаптується;
- Поділ трафіку даних, контролю і сервісів (data, control, service plane) для забезпечення максимальної продуктивності і захисту сервісів в разі збою;
- Збільшення продуктивності (до 1 Гбіт / с з включеними сервісами) і розширення можливостей за допомогою гнучкої системи ліцензування функцій;
- Широкий вибір опціонально модулів для різних типів підключень: T1 / E1, T3 / E3, Gigabit Ethernet;
- Вбудована платформа віртуалізації для інтеграції сервісів і функцій

Детальнішу інформацію буде наведено в таблиці 3.1 .

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		45

Таблиця 3.1 – Характеристики маршрутизатора Cisco 4451

Інтерфейси	5 мережевих інтерфейсів 4x10 / 100/1000 Combo SFP Gigabit Ethernet 1x10 / 100/1000 Management
Flash пам'ять	8GB max 32GB
DRAM Control plane пам'ять	4GB max 16GB
DRAM Data Plane пам'ять	2GB max 2GB
Слоти розширення	3 NIM, 1 SM
Підтримка нового голосового процесора	PVDM4
Ліцензії	Немає встановлених ліцензій, при замовленні обов'язково IP BASE, опціонально SEC, UC і APP (DATA + WAAS)
Додаткові функції	Продуктивність в постачанні 1Gbps з включеними сервісами Розширення продуктивності за допомогою ліцензії Performance до 2Gbps Архітектура з розділенням Control Plane і Data Plane Підтримка ACL, SSHv2 і інших механізмів безпеки
Форм-фактор	Модульний, для монтажу в 19 " комутаційний шафа, 1U

Комутатори лінійки Cisco Catalyst - інтелектуальні і гнучкі мережеві рішення з характеристиками фіксованою конфігурації, широкою лінійкою модулів для вирішення питань із забезпеченням коректної роботи локальної мережі. Мережеві комунікатори дозволяють максимально спростити експлуатацію IT-інфраструктури, гарантують безпеку бізнес-процесів, забезпечують безперебійне функціонування мережі.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		46



Рисунок 3.2 - Комутатор CISCO C9300-24T-A

Нові комутатори Cisco Catalyst 9300 серії реалізує конвергенцію Інтернету речей з провідним в індустрії рівнем масштабованості, забезпечують до 384 портів з потужністю до 60 Вт для UPOE, а також POE + і PoE, високу безпеку, підтримку протоколу AVB і стандарту IEEE +1588, аналіз сервісів і класифікацію для додатків Інтернету речей.

Комутатори Cisco Catalyst 9300 забезпечують інтелектуальний, простий і максимально безпечний доступ за допомогою інтегрованого контролера бездротової мережі. Вони можуть працювати в умовах високої щільності за стандартом 802.11ac другої хвилі (48 точок доступу) і при цьому відрізняються компактністю (форм-фактор 1 RU).

Основні переваги серії 9300:

- Висока масштабіруемость з точками доступу Wave2;
- Інтелектуальне управління живленням за допомогою технології Cisco StackPower;
- Процесор Intel x86;
- Розширений функціонал безпеки.
- Підтримка подвійного стека для розподілу IPv4 / IPv6;
- Новітня операційна система Cisco IOS XE;

Технічні характеристики комутатора Cisco C9300-24T-A наведено в таблиці 3.2:

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		47

Таблиця 3.2 - Технічні характеристики комутатора Cisco C9300-24T-A

Тип	Фіксований доступ
Рівень комутатора	3+ рівень
Порти доступу Ethernet	24 x GE RJ-45
MPPS	154,76 MPPS
Матриця комутації	104 Гбіт / с
Таблиця MAC адрес	32000 MAC адрес
Максимальний VLAN ID	4000
Протоколи VLAN	802.1Q/VLAN
Стекування	StackWise-480/9
Робота в кластері	Да
Пам'ять FLASH	16 Гб
Обсяг ОЗУ	8 Гб
Потужність номінальна / максимальна	350 Ватт
Основне джерело струму	AC 100-240В
Габаритні розміри, см	4,4 x 44,5 x 44,5
Тип Cisco IOS	Network Advantage

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		48

3.2 Вибір ПЗ, налагодження маршрутизації та безпеки пристроїв мережі

Програмним забезпеченням для проектування та налаштування мережі було вибрано GNS3.

GNS3 - це графічний симулятор мережі, що дозволяє емулювати складні мережі. Спочатку розроблений як інструмент для мереж Cisco, GNS3 (скорочення від Graphical Network Simulator) перетворився на симулятор мереж із багатьма постачальниками. GNS3 поєднує в собі найкращі можливості існуючого програмного забезпечення для емуляції в інтерфейсі графічного інтерфейсу і дозволяє створювати необмежену кількість сценаріїв маршрутизації та комутації Cisco. Оскільки справжнє вивчення маршрутизації та комутації вимагає певної практики - і знову ж таки, більшість людей та компаній не можуть дозволити собі інвестувати у все обладнання, необхідне для тестування десятків різних сценаріїв - GNS3 є життєздатним варіантом.

Першим, що було налаштовано в мережі це адресація інтерфейсів маршрутизаторів та комутаторів.

```
R_1_11_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1_11_1(config)#int f0/0
R_1_11_1(config-if)#ip address 190.1.11.4 255.255.255.240
R_1_11_1(config-if)#no sh
R_1_11_1(config-if)#
*Mar  1 00:47:05.843: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:47:06.843: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R_1_11_1(config-if)#ex
R_1_11_1(config)#int f1/0
R_1_11_1(config-if)#ip address 200.1.11.2 255.255.255.240
R_1_11_1(config-if)#no sh
R_1_11_1(config-if)#ex
R_1_11_1(config)#
*Mar  1 00:51:44.211: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Mar  1 00:51:45.211: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R_1_11_1(config)#
```

Рисунок 3.3 – Налаштування адресації на маршрутизаторі R_1_11_1

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		49

```

IOU1(config)#hostname SW_1_11_1
SW_1_11_1(config)#int vlan1
SW_1_11_1(config-if)#ip address 200.1.11.1 255.255.255.240
SW_1_11_1(config-if)#no sh
SW_1_11_1(config-if)#ex
SW_1_11_1(config)#
*Jun 16 09:34:17.910: %LINK-3-UPDOWN: Interface Vlan1, changed state to down
SW_1_11_1(config)#

```

Рисунок 3.4 - Налаштування адресації на комутаторі SW_1_11_1

Налаштування інших маршрутизаторів та комутаторів аналогічне, лістинги конфігурацій наведені у додатках.

Приклади налаштування протоколу OSPF:

```

R_1_11_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1_11_1(config)#router ospf 1
R_1_11_1(config-router)#network 190.1.11.4 0.0.0.15 area 0
R_1_11_1(config-router)#network 200.1.11.2 0.0.0.15 area 0
R_1_11_1(config-router)#
R_1_11_1(config-router)#ex
R_1_11_1(config)#

```

Рисунок 3.5 – Налаштування протоколу OSPF на R_1_11_1

```

R_1_11_3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1_11_3(config)#router ospf 1
R_1_11_3(config-router)#network 200.1.11.4 0.0.0.15 area 0
R_1_11_3(config-router)#network 207.1.11.2 0.0.0.3 area 0
R_1_11_3(config-router)#network 207.1.11.2 0.0.0.3 area 0
*Jun 16 16:32:34.275: %OSPF-5-ADJCHG: Process 1, Nbr 207.1.11.1 on FastEthernet0
/0 from LOADING to FULL, Loading Done
R_1_11_3(config-router)#network 204.1.11.1 0.0.0.3 area 0
R_1_11_3(config-router)#ex
R_1_11_3(config)#

```

Рисунок 3.6 – Налаштування протоколу OSPF на R_1_11_3

Аналогічно до маршрутизаторів R_1_11_1 та R_1_11_3 налаштовуються всі інші роутери. Лістинги конфігурацій наведені у додатках.

Для безпеки кожного з роутерів було вирішено провести налаштування локальної авторизації та аутентифікації на пристроях.

		Музичук А.А.				Арк.
						50
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R_1_11_1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R_1_11_1(config)#enable password adminpass
R_1_11_1(config)#line console 0
R_1_11_1(config-line)#password mypass1
R_1_11_1(config-line)#login
R_1_11_1(config-line)#exit
R_1_11_1(config)#line aux 0
R_1_11_1(config-line)#password mypass2
R_1_11_1(config-line)#login
R_1_11_1(config-line)#exit
R_1_11_1(config)#line vty 0 15
R_1_11_1(config-line)#password mypass3
R_1_11_1(config-line)#login
R_1_11_1(config-line)#exit
R_1_11_1(config)#

```

Рисунок 3.7 – Налаштування локальної авторизації та аутентифікації на R_1_11_1

Приклад налаштування технології Port Security на комутаторі SW_1_11_2.

Коли через комутатор проходять Ethernet-фрейми, він заповнює таблицю MAC адрес використовуючи адресу відправника, який вказаний в цих фреймах. Максимальний розмір цієї таблиці обмежений, заповнити її зломисникові не так складно, як здається, досить використовувати спеціальний софт, який буде генерувати безліч фреймів з випадковими зворотними адресами. Навіщо це може знадобитися? У разі переповнення таблиці MAC адрес, комутатор може почати діяти як хаб - тобто розсилати всі отримані фрейми на всі порти. Наступна дія зломисника - запустити сніффер, програму для перегляду всіх вхідних пакетів, а так як комутатор у нас знаходиться в режимі паніки, то всі пакети, що проходять через нього в тому ж VLAN-е, що і порт зломисника буде видно атакуючому. Для того щоб уникнути подібної ситуації слід заздалегідь подбати про те, щоб на всіх комутаторах працював port security.

У чому полягає суть цієї функції: тим чи іншим способом, для кожного порту обмежується список (або кількість) MAC адрес, які на ньому можуть з'являтися, якщо на порту помічено занадто багато адрес, то порт гаситься. Таким чином, ідея з генеруванням фреймів з випадковими зворотними адресами, як не важко помітити, досить швидко провалиться.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		51

Існує два способи введення обмежень на MAC адреси:

- Статичний - коли адміністратор перераховує, які адреси дозволені
- Динамічний - коли адміністратор вказує, скільки адрес дозволено, а комутатор навчається, запам'ятовуючи, які адреси зараз звертаються через вказаний порт

```
SW_1_11_2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW_1_11_2(config)#int e0/1
SW_1_11_2(config-if)#switchport mode access
SW_1_11_2(config-if)#switchport port-security
SW_1_11_2(config-if)#switchport port-security mac-address 00:50:79:66:68:00
SW_1_11_2(config-if)#switchport port-security violation shutdown
SW_1_11_2(config-if)#storm-control broadcast level 50
^
% Invalid input detected at '^' marker.

SW_1_11_2(config-if)#storm-control broadcast?
% Unrecognized command
SW_1_11_2(config-if)#storm-control?
% Unrecognized command
SW_1_11_2(config-if)#ex
SW_1_11_2(config)#int e0/2
SW_1_11_2(config-if)#switchport mode access
SW_1_11_2(config-if)#switchport port-security
SW_1_11_2(config-if)#switchport port-security mac-address 00:50:79:66:68:01
SW_1_11_2(config-if)#switchport port-security violation shutdown
SW_1_11_2(config-if)#ex
SW_1_11_2(config)#ex
% Ambiguous command: "ex"
SW_1_11_2(config)#end
```

Рисунок 3.8 - Налаштування технології Port Security на комутаторі SW_1_11_2

Налаштування протоколу CDP на маршрутизаторі R_1_11_1 та комутаторі SW_1_11_2.

CDP - це власний протокол рівня 2 компанії Cisco. Він використовується для обміну інформацією з іншим безпосередньо підключеним обладнанням Cisco, таким як операційна система та IP-адреса. Ця інформація буде передаватися між підключеними пристроями. Це допомагає усувати несправності, дозволяючи адміністраторам намітити спосіб підключення пристроїв Cisco між собою.

```
R_1_11_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1_11_1(config)#cdp timer 30
R_1_11_1(config)#cdp holdtime 90
R_1_11_1(config)#cdp advertise-v2
R_1_11_1(config)#cdp run
R_1_11_1(config)#ex
R_1_11_1#sh
```

Рисунок 3.9 - Налаштування протоколу CDP на маршрутизаторі R_1_11_1

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		52

```

SW_1_11_2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW_1_11_2(config)#cdp timer 30
SW_1_11_2(config)#cdp holdtime 90
SW_1_11_2(config)#cdp advertise-v2
SW_1_11_2(config)#cdp run
SW_1_11_2(config)#ex
% Ambiguous command: "ex"
SW_1_11_2(config)#end

```

Рисунок 3.10 - Налаштування протоколу CDP на комутаторі SW_1_11_2

Приклад налаштування технології GETVPN на маршрутизаторах.

Налаштування сервера ключів KS (R_1_11_10) :

```

R_1_11_10#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1_11_10(config)#crypto isakmp policy 10
R_1_11_10(config-isakmp)#encryption aes 256
R_1_11_10(config-isakmp)#authentication pre-share
R_1_11_10(config-isakmp)#group 2
R_1_11_10(config-isakmp)#exut
^
% Invalid input detected at '^' marker.

R_1_11_10(config-isakmp)#exit
R_1_11_10(config)#crypto isakmp key vpn address 201.1.11.2
R_1_11_10(config)#crypto isakmp key vpn address 204.1.11.2
R_1_11_10(config)#

```

Рисунок 3.11 – Налаштування crypto isakmp policy

```

R_1_11_10(config)#access-list 150 permit ip 172.16.0.0 0.0.255.255 172.16.0.0 $

```

Рисунок 3.12 – Створення ACL

```

R_1_11_10(config)#crypto ipsec transform-set tset esp-aes esp-md5-hmac
R_1_11_10(cfg-crypto-trans)#exit
R_1_11_10(config)#crypto ipsec profile GET-PROF
R_1_11_10(ipsec-profile)#set transform-set tset
R_1_11_10(ipsec-profile)#set security-association lifetime seconds 3600
R_1_11_10(ipsec-profile)#exit
R_1_11_10(config)#

```

Рисунок 3.13 – Створення ipsec профілю

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		53

```

R_1_11_10(config)#crypto gdoi group GET-GROUP
R_1_11_10(config-gdoi-group)#identity number 100
R_1_11_10(config-gdoi-group)#server local
R_1_11_10(gdoi-local-server)#
*Jun 17 18:51:40.843: %CRYPTO-6-GDOI_ON_OFF: GDOI is ON
R_1_11_10(gdoi-local-server)#sa ipsec 1
R_1_11_10(gdoi-sa-ipsec)#profile GET-PROF
R_1_11_10(gdoi-sa-ipsec)#match address ipv4 150
R_1_11_10(gdoi-sa-ipsec)#exit
R_1_11_10(gdoi-local-server)#address ipv4 172.16.3.3
R_1_11_10(gdoi-local-server)#exit
R_1_11_10(config-gdoi-group)#

```

Рисунок 3.14 – Створення gdoi групи

```

R_1_11_4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1_11_4(config)#crypto isakmp policy 10
R_1_11_4(config-isakmp)#encryption aes 256
R_1_11_4(config-isakmp)#authentication pre-share
R_1_11_4(config-isakmp)#group 2
R_1_11_4(config-isakmp)#crypto isakmp key vpn address 172.16.3.3
R_1_11_4(config)#crypto gdoi group GET-GROUP
R_1_11_4(config-gdoi-group)#identity number 100
R_1_11_4(config-gdoi-group)#server address ipv4 172.16.3.3
R_1_11_4(config-gdoi-group)#crypto map cmap 10 gdoi
% NOTE: This new crypto map will remain disabled until a valid
group has been configured.
R_1_11_4(config-crypto-map)#set group GET-GROUP
R_1_11_4(config-crypto-map)#crypto map cmap
^
% Invalid input detected at '^' marker.

R_1_11_4(config-crypto-map)#ex
R_1_11_4(config)#int f1/0
R_1_11_4(config-if)#crypto map cmap
R_1_11_4(config-if)#
*Jun 17 19:14:02.558: %CRYPTO-5-GM_REGSTER: Start registration to KS 172.16.3.3
for group GET-GROUP using address 201.1.11.2
R_1_11_4(config-if)#ex
*Jun 17 19:14:02.590: %CRYPTO-6-GDOI_ON_OFF: GDOI is ON
R_1_11_4(config-if)#ex
R_1_11_4(config)#

```

Рисунок 3.15 – Налаштування GETVPN на R_1_11_4

```

R_1_11_7#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1_11_7(config)#crypto isakmp policy 10
R_1_11_7(config-isakmp)#encryption aes 256
R_1_11_7(config-isakmp)#authentication pre-share
R_1_11_7(config-isakmp)#group 2
R_1_11_7(config-isakmp)#crypto isakmp key vpn address 172.16.3.3
R_1_11_7(config)#crypto gdoi group GET-GROUP
R_1_11_7(config-gdoi-group)#identity number 100
R_1_11_7(config-gdoi-group)#server address ipv4 172.16.3.3
R_1_11_7(config-gdoi-group)#crypto map cmap 10 gdoi
% NOTE: This new crypto map will remain disabled until a valid
group has been configured.
R_1_11_7(config-crypto-map)#set group GET-GROUP
R_1_11_7(config-crypto-map)#ex
R_1_11_7(config)#int f0/0
R_1_11_7(config-if)#crypto map cmap
R_1_11_7(config-if)#
*Jun 17 19:20:39.738: %CRYPTO-5-GM_REGSTER: Start registration to KS 172.16.3.3
for group GET-GROUP using address 204.1.11.2
R_1_11_7(config-if)#
*Jun 17 19:20:39.774: %CRYPTO-6-GDOI_ON_OFF: GDOI is ON
R_1_11_7(config-if)#ex
R_1_11_7(config)#

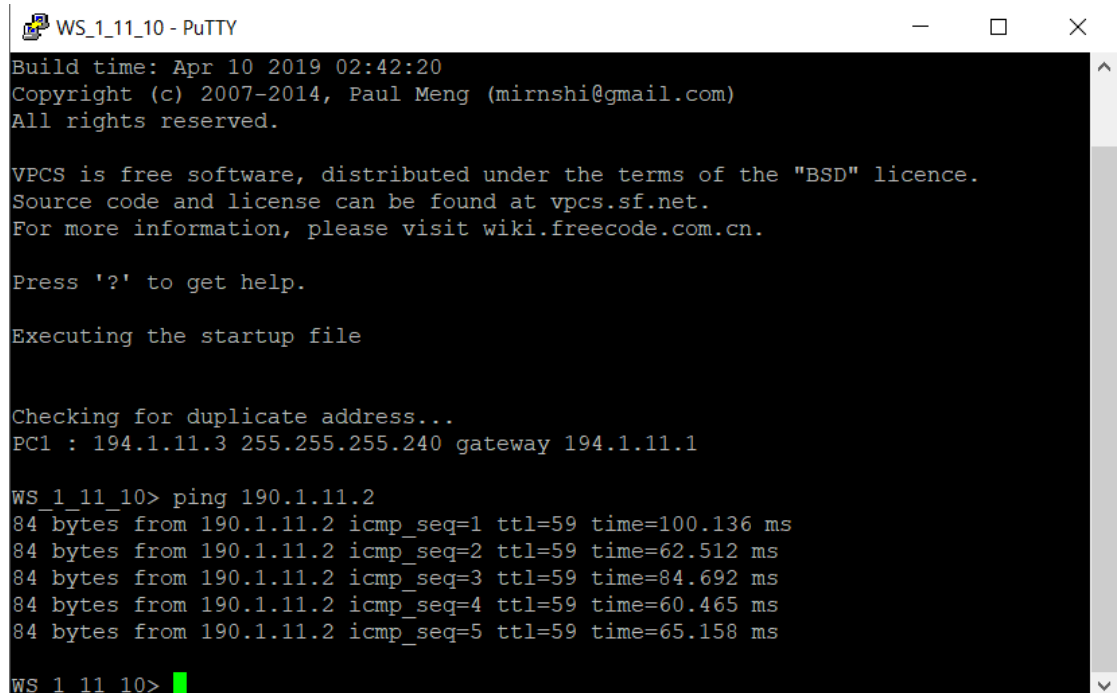
```

Рисунок 3.16 - Налаштування GETVPN на R_1_11_7

		Музичук А.А.				Арк.
						54
Змн.	Арк.	№ докум.	Підпис	Дата		

3.3. Перевірка працездатності мережі

Перше, що потрібно перевірити це наявність зв'язку між кінцевими пристроями та шлях передачі пакету.



```
WS_1_11_10 - PuTTY
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC1 : 194.1.11.3 255.255.255.240 gateway 194.1.11.1

WS_1_11_10> ping 190.1.11.2
84 bytes from 190.1.11.2 icmp_seq=1 ttl=59 time=100.136 ms
84 bytes from 190.1.11.2 icmp_seq=2 ttl=59 time=62.512 ms
84 bytes from 190.1.11.2 icmp_seq=3 ttl=59 time=84.692 ms
84 bytes from 190.1.11.2 icmp_seq=4 ttl=59 time=60.465 ms
84 bytes from 190.1.11.2 icmp_seq=5 ttl=59 time=65.158 ms

WS_1_11_10>
```

Рисунок 3.17 – Перевірка зв'язку між WS_1_11_10 та WS_1_11_1



```
WS_1_11_3> trace 190.1.11.2
trace to 190.1.11.2, 8 hops max, press Ctrl+C to stop
 1  191.1.11.1    0.694 ms   0.823 ms   0.963 ms
 2  190.1.11.2    0.625 ms   7.616 ms  4294967.236 ms
 3  191.1.11.4    7.735 ms  12.418 ms  10.220 ms
 4  202.1.11.1    9.754 ms  21.754 ms  10.739 ms
 5  201.1.11.1   20.578 ms  20.896 ms  21.130 ms
 6  200.1.11.2   21.097 ms   *
 7  190.1.11.2    0.682 ms  60.967 ms   *
 8  190.1.11.2    0.881 ms  55.143 ms   *
```

Рисунок 3.18 – Виконання команди trace на WS_1_11_3

Переглянемо таблицю маршрутизації на роутері R_1_11_2 :

```

R_1_11_2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    207.1.11.0/30 is subnetted, 1 subnets
C       207.1.11.0 is directly connected, FastEthernet2/0
    204.1.11.0/30 is subnetted, 1 subnets
O       204.1.11.0 [110/2] via 207.1.11.2, 00:00:08, FastEthernet2/0
    201.1.11.0/30 is subnetted, 1 subnets
C       201.1.11.0 is directly connected, FastEthernet0/0
    200.1.11.0/28 is subnetted, 1 subnets
C       200.1.11.0 is directly connected, FastEthernet1/0
R_1_11_2#

```

Рисунок 3.19 – Виконання команди show ip route на R_1_11_2

Перевірка налаштування локальної авторизації та аутентифікації на R_1_11_1

```

User Access Verification

Password:
Password:
R_1_11_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1_11_1(config)#

```

Рисунок 3.20 – Вхід в маршрутизатор за допомогою паролю

```

line con 0
 exec-timeout 0 0
 privilege level 15
 password mypass1
 logging synchronous
 login
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 password mypass2
 logging synchronous
 login
 stopbits 1
line vty 0 4
 password mypass3
 login
line vty 5 15
 password mypass3
 login
!
end
R_1_11_1#

```

Рисунок 3.21 – Перегляд налаштувань на маршрутизаторі R_1_11_1

		Музичук А.А.				Арк.
						56
Змн.	Арк.	№ докум.	Підпис	Дата		

Перевірка налаштування технології Port Security на комутаторі SW_1_11_2.

```
SW_1_11_2#show
*Jun 17 11:42:55.634: %SYS-5-CONFIG_I: Configured from console by console
SW_1_11_2#show port-security
Secure Port    MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
          (Count)          (Count)          (Count)
-----
      Et0/1             1             1              0          Shutdown
      Et0/2             1             1              0          Shutdown
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 4096
SW_1_11_2#
```

Рисунок 3.22 – Виконання команди show port-security на SW_1_11_2

```
SW_1_11_2#show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
      (mins)
-----
      1    0050.7966.6800    SecureConfigured    Et0/1     -
      1    0050.7966.6801    SecureConfigured    Et0/2     -
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 4096
SW_1_11_2#show port-security interface ethernet 0/1
Port Security      : Enabled
Port Status        : Secure-up
Violation Mode     : Shutdown
Aging Time         : 0 mins
Aging Type         : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0050.7966.6800:1
Security Violation Count : 0
```

Рисунок 3.23 - Виконання команди show port-security address на SW_1_11_2

Перевірка налаштування протоколу CDP на маршрутизаторі R_1_11_1 та комутаторі SW_1_11_2.

```
R_1_11_1#show cdp
Global CDP information:
    Sending CDP packets every 30 seconds
    Sending a holdtime value of 90 seconds
    Sending CDPv2 advertisements is enabled
R_1_11_1#
```

Рисунок 3.24 - Виконання команди show cdp на маршрутизаторі R_1_11_1

```

R_1_11_1#show cdp interface
FastEthernet0/0 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 30 seconds
  Holdtime is 90 seconds
FastEthernet1/0 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 30 seconds
  Holdtime is 90 seconds
FastEthernet2/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 30 seconds
  Holdtime is 90 seconds
FastEthernet3/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 30 seconds
  Holdtime is 90 seconds

```

Рисунок 3.25 - Виконання команди show cdp interface на маршрутизаторі R_1_11_1

```

SW_1_11_2#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID         Local Intrfce   Holdtme    Capability Platform Port ID
R_1_11_1          Eth 0/0         68         R          7206VXR   Fas 0/0

Total cdp entries displayed : 1

```

Рисунок 3.26 - Виконання команди show cdp neighbors на комутаторі SW_1_11_2

```

SW_1_11_2#show cdp entry R_1_11_1
-----
Device ID: R_1_11_1
Entry address(es):
  IP address: 190.1.11.4
Platform: Cisco 7206VXR, Capabilities: Router
Interface: Ethernet0/0, Port ID (outgoing port): FastEthernet0/0
Holdtime : 60 sec

Version :
Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 12.4(24)T2,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Mon 19-Oct-09 22:53 by prod_rel_team

advertisement version: 2
Duplex: half

```

Рисунок 3.27 - Виконання команди show cdp entry на комутаторі SW_1_11_2

		Музичук А.А.				Арк.
						58
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW_1_11_2#show cdp traffic
CDP counters :
    Total packets output: 3667, Input: 200
    Hdr syntax: 0, Chksum error: 0, Encaps failed: 0
    No memory: 0, Invalid packet: 0,
    CDP version 1 advertisements output: 0, Input: 0
    CDP version 2 advertisements output: 3667, Input: 200
SW_1_11_2#

```

Рисунок 3.28 - Виконання команди show cdp traffic на комутаторі
SW_1_11_2

Перевірка працездатності налаштованого GetVPN.

```

R_1_11_4#ping 204.1.11.2 source 172.16.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 204.1.11.2, timeout is 2 seconds:
Packet sent with a source address of 172.16.2.2
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/33/44 ms

```

Рисунок 3.29 - Перевірка зв'язку

```

protected vrf: (none)
local ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)
current_peer 0.0.0.0 port 848
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

```

Рисунок 3.30 – Перевірка шифрування пакетів

```

R_1_11_4#show crypto ISAKMP SA
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
172.16.3.3    201.1.11.2    GDOI_IDLE      1001 ACTIVE

IPv6 Crypto ISAKMP SA

```

Рисунок 3.31 - Виконання команди show crypto isakmp sa на маршрутизаторі
R_1_11_4 для перевірки тунелю

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		59

```

R_1_11_4#trace 172.16.2.2

Type escape sequence to abort.
Tracing the route to 172.16.2.2

  0  1 172.16.2.2 4 msec 0 msec 4 msec
R_1_11_4#

```

Рисунок 3.32 - Перевірка передачі трафіку на R_1_11_4

Висновки до розділу 3

В останньому розділі було розглянуто та вибрано обладнання для мережі. Було проаналізовано та вибрано новітнє обладнання яке буде краще підходити для мережі. Також розібрали головні характеристики маршрутизатора Cisco 4451 та комутатора CISCO C9300-24T-A. Також як основним ПЗ для проектування мережі було вибрано GNS3. Було налаштовано IP-адресацію в мережі, протокол маршрутизації OSPF, налаштовано локальну авторизацію та аутентифікацію, технологію Port Security на комутаторах, технологію CDP на маршрутизаторах та комутаторах, а також технологію GetVPN. Після налаштування було виконано перевірку працездатності мережі.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		60

ВИСНОВКИ

Під час виконання випускної роботи бакалавра було спроектовано та реалізовано проект забезпечення безпеки мережі будівельної компанії та було виконано наступні завдання:

В першому розділі було проаналізовано актуальність захисту мереж та їх місце в будівельних компаніях, її важливість та наслідки того якщо не буде забезпечено її. Проаналізували існуючі загрози мережових з'єднань, їх види та джерела. Переглянуто основні вимоги до захисту мережі, типи безпеки та види захистів мережевої безпеки.

В другому розділі було розглянуто види топологій, їх переваги та недоліки, а також обрано кращий варіант для майбутньої мережі. Було вибрано обладнання для передавання інформації в мережі, види кабелів, їх переваги та обрано кращий для мережі. Також було розроблено загальний вид мережі, кількість маршрутизаторів, комутаторів та ПК. Також було вибрано технологію VPN, а саме GetVPN та протокол маршрутизації OSPF для мережі. І в останньому підрозділі було розроблено схему адресації мережі, забезпечивши при цьому потреби підключених вузлів.

В третьому розділі було розглянуто та вибрано обладнання для мережі. Було проаналізовано та вибрано новітнє обладнання яке буде краще підходити для мережі. Також розібрали головні характеристики маршрутизатора Cisco 4451 та комутатора CISCO C9300-24T-A. Також як основним ПЗ для проектування мережі було вибрано GNS3. Було налаштовано IP-адресацію в мережі, протокол маршрутизації OSPF, налаштовано локальну авторизацію та аутентифікацію, технологію Port Security на комутаторах, технологію CDP на маршрутизаторах та комутаторах, а також технологію GetVPN. Після налаштування було виконано перевірку працездатності мережі.

В майбутньому можливо розширити структуру мережі та налаштувати додаткові функції для її безпеки.

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		61

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cabling, Connectors and Ethernet Standarts [Електронний ресурс], - Режим доступу:
https://access.itxlearning.com/data/cmdata/NETPLUSN10004/Books/ec2_netplus004c02.pdf
2. J. M. Kizza - Computer Network Security / Joseph Migga Kizza – М.: Springer, 2005 – 535 стр.
3. Information Security in the Construction Industry — What You Need to Know [Електронний ресурс], - Режим доступу:
<https://www.viewpoint.com/blog/information-security-in-the-construction-industry-what-you-need-to-know>
4. Richard Deal- The Complete Cisco VPN Configuration Guide/ Richard Deal– М.: Cisco Press, 2005 - 1032 стр.
5. Network Security Baseline [Електронний ресурс], - Режим доступу:
<https://paper.bobylive.com/Security/Cisco-secure-baseline-handbooks.pdf>
6. What is Network Security? [Електронний ресурс], - Режим доступу:
<https://www.paloaltonetworks.com/cyberpedia/what-is-network-security>
7. W. Stallings - Network Security Essentials / William Stallings - М.: Pearson India, 2016 - 464 стр.
8. J. Michael Stewart - Network Security, Firewalls, and VPNs / J. Michael Stewart, Denise Kinsey М.: Jones & Bartlett Learning, 2020 - 481 стр.
9. What Is an Access Control List [Електронний ресурс], - Режим доступу:
<https://www.imperva.com/learn/data-security/access-control-list-acl/>
10. Y. Bhaiji - Network Security Technologies and Solutions / Yusuf Bhaiji - М.: Cisco Press, 2016 - 840 ст.
11. What is network topology and types of network topology? [Електронний ресурс], - Режим доступу: <https://afteracademy.com/blog/what-is-network-topology-and-types-of-network-topology>

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		62

12. Open Shortest Path First (OSPF) [Електронний ресурс], - Режим доступу:
<https://www.cisco.com/c/en/us/products/ios-nx-os-software/open-shortest-path-first-ospf/index.html>
13. A. Colton - OSPF for Cisco Routers / Andrew Colton - М.: Rocket Science, 2003 - 252 ст.
14. Н. Andrea - Cisco VPN Configuration Guide: Step-By-Step Configuration of Cisco VPNs for ASA and Routers / Harris Andrea - М.: CreateSpace Independent Publishing Platform, 2014 - 260 ст.
15. What Is Network Security [Електронний ресурс], - Режим доступу:
<https://www.cisco.com/c/en/us/products/security/what-is-network-security.html>
16. What Is Network Security: Its Types And Management [Електронний ресурс], - Режим доступу: <https://www.softwaretestinghelp.com/network-security/>
17. GETVPN Troubleshoot Guide [Електронний ресурс], - Режим доступу:
<https://www.cisco.com/c/en/us/support/docs/security/group-encrypted-transport-vpn/118125-technote-getvpn-00.html>
18. Cisco Group Encrypted Transport VPN [Електронний ресурс], - Режим доступу: <https://www.zsis.hr/UserDocsImages/Sigurnost/pdfs/GETVPN.pdf>
19. VPN protocols explained and compared [Електронний ресурс], - Режим доступу: <https://www.comparitech.com/vpn/protocols/>
20. Configuring Port Security [Електронний ресурс], - Режим доступу:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.pdf

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		63

Додатки

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		64

Адресація підмереж

Таблиця 1 - Адресація підмережі В

Призначення	IP-адреса
Адреса мережі	200.1.11.0
Маска мережі	255.255.255.240
Інвертована маска	0.0.0.15
Мінімальна адреса	200.1.11.1
Максимальна адреса	200.1.11.14
Широкомовна адреса	200.1.11.15
Шлюз по замовчуванню	200.1.11.1
Діапазон адрес комутаторів	200.1.11.1
Діапазон вільних адрес	200.1.11.5 - 200.1.11.14

Таблиця 2 - Адресація підмережі D

Призначення	IP-адреса
Адреса мережі	192.1.11.0
Маска мережі	255.255.255.240
Інвертована маска	0.0.0.15
Мінімальна адреса	192.1.11.1
Максимальна адреса	192.1.11.14
Широкомовна адреса	192.1.11.15
Шлюз по замовчуванню	192.1.11.1
Діапазон адрес комутаторів	192.1.11.1
Діапазон адрес майбутніх ПК	192.1.11.2 - 192.1.11.3 - 192.1.11.14
Діапазон вільних адрес	192.1.11.4

Таблиця 3 - Адресація підмережі Е

Призначення	ІР-адреса
Адреса мережі	193.1.11.0
Маска мережі	255.255.255.240
Інвертована маска	0.0.0.15
Мінімальна адреса	193.1.11.1
Максимальна адреса	193.1.11.14
Широкомовна адреса	193.1.11.15
Шлюз по замовчуванню	193.1.11.1
Діапазон адрес комутаторів	193.1.11.1
Діапазон адрес майбутніх ПК	193.1.11.2 - 193.1.11.3 - 193.1.11.14
Діапазон вільних адрес	193.1.11.4

Таблиця 4 - Адресація підмережі F

Призначення	ІР-адреса
Адреса мережі	194.1.11.0
Маска мережі	255.255.255.240
Інвертована маска	0.0.0.15
Мінімальна адреса	194.1.11.1
Максимальна адреса	194.1.11.14
Широкомовна адреса	194.1.11.15
Шлюз по замовчуванню	194.1.11.1
Діапазон адрес комутаторів	194.1.11.1
Діапазон адрес майбутніх ПК	194.1.11.2 - 194.1.11.3 - 194.1.11.14
Діапазон вільних адрес	194.1.11.4

Таблиця 5 - Адресація підмережі G

Призначення	IP-адреса
Адреса мережі	195.1.11.0
Маска мережі	255.255.255.240
Інвертована маска	0.0.0.15
Мінімальна адреса	195.1.11.1
Максимальна адреса	195.1.11.14
Широкомовна адреса	195.1.11.15
Шлюз по замовчуванню	195.1.11.1
Діапазон адрес комутаторів	195.1.11.1
Діапазон адрес майбутніх ПК	195.1.11.2 - 195.1.11.3 - 195.1.11.14
Діапазон вільних адрес	195.1.11.4

Таблиця 6 - Адресація підмережі H

Призначення	IP-адреса
Адреса мережі	196.1.11.0
Маска мережі	255.255.255.240
Інвертована маска	0.0.0.15
Мінімальна адреса	196.1.11.1
Максимальна адреса	196.1.11.14
Широкомовна адреса	196.1.11.15
Шлюз по замовчуванню	196.1.11.1
Діапазон адрес комутаторів	196.1.11.1
Діапазон адрес майбутніх ПК	196.1.11.2 - 196.1.11.3 - 196.1.11.14
Діапазон вільних адрес	196.1.11.4

Таблиця 7 - Адресація підмережі І

Призначення	IP-адреса
Адреса мережі	197.1.11.0
Маска мережі	255.255.255.240
Інвертована маска	0.0.0.15
Мінімальна адреса	197.1.11.1
Максимальна адреса	197.1.11.14
Широкомовна адреса	197.1.11.15
Шлюз по замовчуванню	197.1.11.1
Діапазон адрес комутаторів	197.1.11.1
Діапазон адрес майбутніх ПК	197.1.11.2 - 197.1.11.3 - 197.1.11.14
Діапазон вільних адрес	197.1.11.4

Таблиця 8 - Адресація підмережі J

Призначення	IP-адреса
Адреса мережі	198.1.11.0
Маска мережі	255.255.255.240
Інвертована маска	0.0.0.15
Мінімальна адреса	198.1.11.1
Максимальна адреса	198.1.11.14
Широкомовна адреса	198.1.11.15
Шлюз по замовчуванню	198.1.11.1
Діапазон адрес комутаторів	198.1.11.1
Діапазон адрес майбутніх ПК	198.1.11.2 - 198.1.11.3 - 198.1.11.14
Діапазон вільних адрес	198.1.11.4

Таблиця 9 - Адресація підмережі К

Призначення	IP-адреса
Адреса мережі	201.1.11.0
Маска мережі	255.255.255.252
Інвертована маска	0.0.0.3
Мінімальна адреса	201.1.11.1
Максимальна адреса	201.1.11.2
Широкомовна адреса	201.1.11.3
Діапазон вільних адрес	201.1.11.1-201.1.11.2

Таблиця 10 - Адресація підмережі М

Призначення	IP-адреса
Адреса мережі	202.1.11.0
Маска мережі	255.255.255.252
Інвертована маска	0.0.0.3
Мінімальна адреса	202.1.11.1
Максимальна адреса	202.1.11.2
Широкомовна адреса	202.1.11.3
Діапазон вільних адрес	202.1.11.1-202.1.11.2

Таблиця 11 - Адресація підмережі N

Призначення	IP-адреса
Адреса мережі	203.1.11.0
Маска мережі	255.255.255.252
Інвертована маска	0.0.0.3
Мінімальна адреса	203.1.11.1
Максимальна адреса	203.1.11.2
Широкомовна адреса	203.1.11.3
Діапазон вільних адрес	203.1.11.1-203.1.11.2

Таблиця 12 - Адресація підмережі L

Призначення	IP-адреса
Адреса мережі	204.1.11.0
Маска мережі	255.255.255.252
Інвертована маска	0.0.0.3
Мінімальна адреса	204.1.11.1
Максимальна адреса	204.1.11.2
Широкомовна адреса	204.1.11.3
Діапазон вільних адрес	204.1.11.1-204.1.11.2

Таблиця 13 - Адресація підмережі O

Призначення	IP-адреса
Адреса мережі	205.1.11.0
Маска мережі	255.255.255.252
Інвертована маска	0.0.0.3
Мінімальна адреса	205.1.11.1
Максимальна адреса	205.1.11.2
Широкомовна адреса	205.1.11.3
Діапазон вільних адрес	205.1.11.1-205.1.11.2

Таблиця 14 - Адресація підмережі P

Призначення	IP-адреса
Адреса мережі	206.1.11.0
Маска мережі	255.255.255.252
Інвертована маска	0.0.0.3
Мінімальна адреса	206.1.11.1
Максимальна адреса	206.1.11.2
Широкомовна адреса	206.1.11.3
Діапазон вільних адрес	206.1.11.1-206.1.11.2

Конфігураційні файли пристроїв мережі

R_1_11_1
R_1_11_1#show run
Building configuration...

Current configuration : 1492 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_1_11_1
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable password adminpass
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
archive
 log config
 hidekeys
!
ip tcp synwait-time 5
!
interface Loopback1
 no ip address
!
interface FastEthernet0/0
 ip address 190.1.11.4 255.255.255.240
 duplex half
!
interface FastEthernet1/0
 ip address 200.1.11.2 255.255.255.240
 duplex half
!

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		71

```

interface FastEthernet2/0
ip address 189.1.11.2 255.255.255.252
duplex half
!
interface FastEthernet3/0
no ip address
shutdown
duplex half
!
router ospf 1
log-adjacency-changes
network 189.1.11.0 0.0.0.3 area 0
network 190.1.11.0 0.0.0.15 area 0
network 200.1.11.0 0.0.0.15 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
!
no cdp log mismatch duplex
cdp timer 30
cdp holdtime 90
!
control-plane
!
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
password mypass1
logging synchronous
login
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
password mypass2
logging synchronous
login
stopbits 1
line vty 0 4
password mypass3
login
line vty 5 15
password mypass3
login
!
end

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		72

```

R_1_11_10
R_1_11_10#show run
Building configuration...

Current configuration : 1678 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_1_11_10
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key VPN address 201.1.11.2
crypto isakmp key VPN address 204.1.11.2
!
crypto ipsec transform-set tset esp-aes esp-md5-hmac
!
crypto ipsec profile GET-PROF
 set transform-set tset
!
crypto gdoi group GET-GROUP
 identity number 100
 server local
 rekey retransmit 10 number 2
 sa ipsec 1
 profile GET-PROF

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		73

```

match address ipv4 150
replay counter window-size 64
address ipv4 172.16.3.3
!
crypto map cmap 10 gdoi
set group GET-GROUP
!
ip tcp synwait-time 5
!
interface Loopback1
ip address 172.16.3.3 255.255.255.0
!
interface FastEthernet0/0
ip address 189.1.11.1 255.255.255.252
duplex half
crypto map cmap
!
router ospf 1
log-adjacency-changes
network 189.1.11.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
access-list 150 permit ip 172.16.0.0 0.0.255.255 172.16.0.0 0.0.255.255
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
shutdown
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
End

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		74

```

R_1_11_2
R_1_11_2#show run
Building configuration...

Current configuration : 1358 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_1_11_2
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 ip address 201.1.11.1 255.255.255.252
 duplex half
!
interface FastEthernet1/0
 ip address 200.1.11.3 255.255.255.240
 duplex half
!
interface FastEthernet2/0
 ip address 207.1.11.1 255.255.255.252
 duplex half
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex half

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		75

```

!
interface FastEthernet4/0
  no ip address
  shutdown
  duplex half
!
router ospf 1
  log-adjacency-changes
  network 200.1.11.0 0.0.0.15 area 0
  network 201.1.11.0 0.0.0.3 area 0
  network 207.1.11.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
  shutdown
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  login
!
End

R_1_11_3
R_1_11_3#show run
Building configuration...

Current configuration : 1358 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		76

```

hostname R_1_11_3
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 ip address 207.1.11.2 255.255.255.252
 duplex half
!
interface FastEthernet1/0
 ip address 200.1.11.4 255.255.255.240
 duplex half
!
interface FastEthernet2/0
 ip address 204.1.11.1 255.255.255.252
 duplex half
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex half
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex half
!
router ospf 1
 log-adjacency-changes
 network 200.1.11.0 0.0.0.15 area 0
 network 204.1.11.0 0.0.0.3 area 0
 network 207.1.11.0 0.0.0.3 area 0
!

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		77

```

ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
shutdown
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
end

```

```

R_1_11_4
R_1_11_4#show run
Building configuration...

```

```

Current configuration : 1682 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_1_11_4
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		78

```

!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key VPN address 172.16.3.3
!
!
crypto gdoi group GET-GROUP
 identity number 100
 server address ipv4 172.16.3.3
!
crypto map cmap 10 gdoi
 set group GET-GROUP
!
ip tcp synwait-time 5
!
interface Loopback1
 ip address 172.16.2.2 255.255.255.0
!
interface FastEthernet0/0
 ip address 202.1.11.1 255.255.255.252
 duplex half
!
interface FastEthernet1/0
 ip address 201.1.11.2 255.255.255.252
 duplex half
 crypto map cmap
!
interface FastEthernet2/0
 ip address 203.1.11.1 255.255.255.252
 duplex half
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex half
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex half

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		79

```

!
router ospf 1
 log-adjacency-changes
 network 201.1.11.0 0.0.0.3 area 0
 network 202.1.11.0 0.0.0.3 area 0
 network 203.1.11.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
end

R_1_11_5
R_1_11_5#show run
Building configuration...

Current configuration : 1359 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_1_11_5
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		80

```

!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 ip address 202.1.11.2 255.255.255.252
 duplex half
!
interface FastEthernet1/0
 ip address 191.1.11.4 255.255.255.240
 duplex half
!
interface FastEthernet2/0
 ip address 192.1.11.4 255.255.255.240
 duplex half
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex half
!
interface FastEthernet4/0
 no ip address
 shutdown
 duplex half
!
router ospf 1
 log-adjacency-changes
 network 191.1.11.0 0.0.0.15 area 0
 network 192.1.11.0 0.0.0.15 area 0
 network 202.1.11.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		81

control-plane

!

gatekeeper

shutdown

!

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line aux 0

exec-timeout 0 0

privilege level 15

logging synchronous

stopbits 1

line vty 0 4

login

!

end

R_1_11_6

R_1_11_6#show run

Building configuration...

Current configuration : 1359 bytes

!

upgrade fpd auto

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R_1_11_6

!

boot-start-marker

boot-end-marker

!

logging message-counter syslog

!

no aaa new-model

ip source-route

no ip icmp rate-limit unreachable

ip cef

!

no ip domain lookup

no ipv6 cef

!

multilink bundle-name authenticated

!

archive

log config

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		82

```

hidekeys
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
ip address 203.1.11.2 255.255.255.252
duplex half
!
interface FastEthernet1/0
ip address 194.1.11.4 255.255.255.240
duplex half
!
interface FastEthernet2/0
ip address 193.1.11.4 255.255.255.240
duplex half
!
interface FastEthernet3/0
no ip address
shutdown
duplex half
!
interface FastEthernet4/0
no ip address
shutdown
duplex half
!
router ospf 1
log-adjacency-changes
network 193.1.11.0 0.0.0.15 area 0
network 194.1.11.0 0.0.0.15 area 0
network 203.1.11.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
shutdown
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		83

```

logging synchronous
stopbits 1
line vty 0 4
login
!
end

```

```

R_1_11_7
R_1_11_7#show run
Building configuration...

```

```

Current configuration : 1682 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_1_11_7
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
archive
log config
hidekeys
!
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 2
crypto isakmp key VPN address 172.16.3.3
!
!
crypto gdoi group GET-GROUP
identity number 100
server address ipv4 172.16.3.3

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		84

```

crypto map cmap 10 gdoi
  set group GET-GROUP
!
ip tcp synwait-time 5
!
interface Loopback1
  ip address 172.16.1.1 255.255.255.0
!
interface FastEthernet0/0
  ip address 204.1.11.2 255.255.255.252
  duplex half
  crypto map cmap
!
interface FastEthernet1/0
  ip address 206.1.11.1 255.255.255.252
  duplex half
!
interface FastEthernet2/0
  ip address 205.1.11.1 255.255.255.252
  duplex half
!
interface FastEthernet3/0
  no ip address
  shutdown
  duplex half
!
interface FastEthernet4/0
  no ip address
  shutdown
  duplex half
!
router ospf 1
  log-adjacency-changes
  network 204.1.11.0 0.0.0.3 area 0
  network 205.1.11.0 0.0.0.3 area 0
  network 206.1.11.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
  shutdown
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		85

```

stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
end

```

```

R_1_11_8
R_1_11_8#show run
Building configuration...

```

```

Current configuration : 1425 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_1_11_8
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
archive
log config
hidekeys
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
ip address 205.1.11.2 255.255.255.252
duplex half
!
interface FastEthernet1/0

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		86

```

ip address 196.1.11.4 255.255.255.240
duplex half
!
interface FastEthernet2/0
ip address 195.1.11.4 255.255.255.240
duplex half
!
interface FastEthernet3/0
no ip address
shutdown
duplex half
!
interface FastEthernet4/0
no ip address
shutdown
duplex half
!
interface FastEthernet5/0
no ip address
shutdown
duplex half
!
router ospf 1
log-adjacency-changes
network 195.1.11.0 0.0.0.15 area 0
network 196.1.11.0 0.0.0.15 area 0
network 205.1.11.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
gatekeeper
shutdown
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
end

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		87

```

R_1_11_9
R_1_11_9#show run
Building configuration...

Current configuration : 1359 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_1_11_9
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
archive
log config
hidekeys
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 ip address 206.1.11.2 255.255.255.252
 duplex half
!
interface FastEthernet1/0
 ip address 198.1.11.4 255.255.255.240
 duplex half
!
interface FastEthernet2/0
 ip address 197.1.11.4 255.255.255.240
 duplex half
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex half

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		88

```

!
interface FastEthernet4/0
  no ip address
  shutdown
  duplex half
!
router ospf 1
  log-adjacency-changes
  network 197.1.11.0 0.0.0.15 area 0
  network 198.1.11.0 0.0.0.15 area 0
  network 206.1.11.0 0.0.0.3 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
!
control-plane
!
gatekeeper
shutdown
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  login
!
end

```

		Музичук А.А.				Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		89