НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І
ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ПОГОДЖЕНО	**ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ**
Декан факультету	Завідувач кафедри
Інформаційних технологій	Комп'ютерних систем, мереж та кібербезпеки
_____ Болбот І.М., д.тех.н, проф.	_____ Касаткін Д.Ю., к.п.н., доц.
підпис ПІБ, вчене звання і ступінь	підпис ПІБ, вчене звання і ступінь
«___»_____2024 р.	«___»_____2024 р.

МАГІСТЕРСЬКА РОБОТА

На тему: «Дослідження комп'ютерної системи для телекомунікаційних технологій, реалізованої на основі засобів Cisco»

Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма _____

Орієнтація освітньої програми _____

Керівник дипломної роботи: _____ / Сагун А.В. /
підпис ПІБ

Виконав: _____ / Шведов Д.В. /
підпис ПІБ

КИЇВ-2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки
_____/ Касаткін Д.Ю., к.п.н., доц. /
підпис ПІБ, вчене звання і ступінь
«__» _____ 20__ р.

З А В Д А Н Н Я

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ РОБОТИ СТУДЕНТУ

Шведов Дмитро Володимирович
(прізвище, ім'я, по батькові)

Спеціальність (напрям підготовки): комп'ютерна інженерія_____
Освітня програма _____
Орієнтація освітньої програми _____

Тема магістерської роботи: «Дослідження комп'ютерної системи для телекомунікаційних технологій, реалізованої на основі засобів Cisco»_____
затверджена наказом ректора НУБіП України від "___" _____20__р. №_____
Термін подання завершеної роботи на кафедру _____
Вихідні дані до магістерської роботи _____
_____
_____
_____
_____
Перелік питань, що підлягають дослідженню:

1. _____
2. _____
3. _____

Перелік графічного матеріалу (за потреби) _____
_____

Дата видачі завдання "_____"_____2023 р.

Керівник магістерської роботи _____ _Сагун А.В., к.т.н., доцент_____
(підпис) (прізвище та ініціали)

Завдання прийняв до виконання _____ ____Шведов Д.В.___
(підпис) (прізвище та ініціали студента)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз предметної області		Виконано
2	Проектування системи		Виконано
3	Реалізація системи		Виконано
4	Тестування системи		Виконано
5	Оформлення пояснювальної записки		Виконано
6	Оформлення графічного матеріалу		Виконано

Студент _____ **Д.В. Шведов**

(підпис) (ініціали та прізвище)

Керівник проекту (роботи) _____ **А.В. Сагун**

(підпис) (ініціали та прізвище)

РЕФЕРАТ

Пояснювальна записка: 66 сторінок, 42 рисунка, 14 таблиць, 15 джерел.

КОМП'ЮТЕРНА МЕРЕЖА, CISCO, EVE-NG, ROUTERS, SWITCHES

Мета – дослідження та розробка комп'ютерної системи на базі інструментаріїв Cisco та подальше порівняння змодельованої системи з існуючою.

Об'єкт – комп'ютерна мережа корпоративного призначення з нахилом на телекомунікаційні технології.

Предмет дослідження – аналіз програмних і апаратних засобів Cisco, що використовуються для створення мереж телекомунікацій а також побудова мережевої моделі за допомогою програмного забезпечення EVE-NG .

Проект складається з чотирьох розділів.

У першому розділі представлено огляд і аналіз предметної області. Описано область застосування, проведено аналіз мережних рішень і поставлені завдання для розробки.

У другому розділі розроблено проєкт комп'ютерної системи, яка використовує інструменти Cisco. Підібрано обладнання для мережі, як пасивне, так і активне. Підібрано кінцеві пристрої. Розроблено логічну схему мережі.

У третьому розділі реалізовано комп'ютерну систему на базі засобів Cisco. Налаштовано робоче середовище EVE-NG. Сконфігуровано комутатори та маршрутизатор Cisco. Налаштовано кінцеві пристрої.

У четвертому розділі було порівняно спроєктовану мережу з поточною мережею.

Результатом роботи є дослідження комп'ютерної системи для телекомунікаційних технологій, реалізованої на основі засобів Cisco.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

AD	–	Active Directory
DC	–	Контролер домену
DHCP	–	Протокол динамічної конфігурації
КС	–	Комп’ютерна система
ОС	–	Операційна система
OU	–	Organizational Units
VLAN	–	Віртуальна локальна комп'ютерна мережа
VM	–	Віртуальна машина
ПК	–	Персональний комп’ютер

ВСТУП

У сучасному світі телекомунікаційні технології займають ключову роль у розвитку інформаційного суспільства та забезпеченні ефективного функціонування різних галузей економіки. Високі темпи розвитку інтернету, мобільного зв'язку, а також широкосмугових мереж сприяють постійному зростанню обсягів переданих даних та потребують вдосконалення існуючих і впровадження нових рішень для забезпечення стабільної та безпечної передачі інформації.

Cisco Systems, яка протягом багатьох років була лідером у розробці та впровадженні мережевих рішень, є одним із ключових гравців на ринку телекомунікаційних технологій. Системи Cisco можуть ефективно задовольнити потреби як малих, так і великих компаній у телекомунікаційних послугах завдяки своїй масштабованості, надійності та безпеці, які роблять їх широко поширеними по всьому світу.

Унікальність теми дослідження полягає в тому, що для покращення якості та ефективності телекомунікаційних послуг необхідно вивчити та впровадити новітні технології на основі засобів Cisco. Зокрема, важливо дослідити можливості інтеграції комп’ютерних систем, які базуються на рішеннях Cisco, у існуючі інфраструктури підприємств. Крім того, важливо визначити переваги та недоліки цих рішень порівняно з іншими методами.

Мета дипломної роботи полягає в тому, щоб проаналізувати комп’ютерну систему телекомунікаційних технологій, яка використовує продукти Cisco, зосереджуючись на її дизайні, функціональних можливостях, безпеці та масштабованості. Для досягнення поставленої мети буде проведено теоретичне дослідження основних теоретичних питань побудови телекомунікаційних мереж, порівняння з іншими провідними технологіями та дослідження практичного впровадження систем Cisco у різних галузях.

Здатність забезпечувати високу надійність і безперервність роботи мереж є важливим компонентом комп’ютерних систем для телекомунікаційних технологій. Для великих компаній і державних установ це особливо важливо, оскільки вони потребують безперебійного доступу до інформації для виконання своїх завдань. Технології Cisco включають механізми відновлення після аварій, балансування навантаження та використання резервних каналів зв’язку для побудови мереж з високим рівнем відмовостійкості.

При використанні телекомунікаційних технологій безпека інформації є ще одним важливим фактором, який необхідно враховувати. Завдяки використанню сучасних протоколів шифрування, систем виявлення та запобігання вторгненням, а також засобів контролю доступу, продукти Cisco дозволяють забезпечувати високий рівень захисту даних. Це особливо важливо в умовах зростаючої кількості кіберзагроз, які загрожують конфіденційності.

Масштабованість мереж є ще одним важливим елементом, який визначає ефективність телеком-технологій. Засоби Cisco легко використовувати для розширення мережі, якщо потреба компанії в обробці даних зросте або географія діяльності зросте. Це гарантує, що мережеві рішення є гнучкими та адаптивними, що є важливим фактором для збереження конкурентоспроможності компанії на сучасному ринку.

1 ОГЛЯД ТА АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Опис області застосування

У сучасному світі телекомунікаційні технології є життєво важливими для підтримки ефективного та стійкого зв’язку між різними підприємствами, державними органами та приватними особами. Для передачі даних, голосу та відео телекомунікаційні системи використовують різні технології, від дротових і бездротових мереж до широкосмугових Інтернет-з’єднань.

Інтеграція різних технологій і рішень для максимізації ефективності та надійності зв’язку є важливим завданням у сфері телекомунікацій. У цьому контексті комп’ютерні системи, які забезпечують управління мережевими ресурсами, контроль доступу та захист даних, відіграють важливу роль. Cisco Systems є одним із провідних виробників таких рішень.

Багато сфер використовують системи Cisco, такі як корпоративні мережі, державні установи, освіта та охорона здоров’я. У їхній асортимент входять маршрутизатори, комутатори, бездротові точки доступу, мережеві захисні засоби та програмне забезпечення для управління мережами, а також різні продукти для побудови локальних і глобальних мереж.

Технології телекомунікації на основі засобів Cisco забезпечують надійність, масштабованість і високу продуктивність мереж. Вони забезпечують захист від кіберзагроз, оптимізують використання смуги пропускання та дозволяють ефективно керувати ресурсами. Інтеграція систем Cisco в телекомунікаційні інфраструктури гарантує безперебійну роботу та високу якість зв’язку.

Телекомунікаційні системи стають ще більш важливими в епоху цифрової трансформації, коли все більше процесів перемикаються на онлайн-середовище. Високі вимоги до сучасних мережевих рішень включають високу швидкість передачі даних, мінімальну затримку та максимальну доступність.

Завдяки своїм інноваціям і постійному вдосконаленню технології Cisco дозволяють створювати мережі, які відповідають цим вимогам.

Впровадження мереж на основі політики (PBN) і програмно-визначених мереж (SDN) є одним із основних напрямків розвитку телекомунікаційних технологій. Цей тип стратегій значно підвищує гнучкість і керованість мережевих інфраструктур, одночасно знижуючи витрати на експлуатацію та надаючи можливість швидко адаптуватися до змін умов. Cisco постійно розвиває ці технології та пропонує ринку передові рішення для створення сучасних мереж.

Забезпечення кібербезпеки в телекомунікаційних мережах також має вирішальне значення. Зі зростанням кількості кіберзагроз необхідні надійні рішення для захисту даних. Системи виявлення та запобігання вторгненням, засоби шифрування даних і контролі доступу — це лише деякі з рішень Cisco для захисту мереж від зовнішніх і внутрішніх загроз.

Cisco пропонує своїм клієнтам надійні, безпечні та високопродуктивні мережеві рішення, займаючись лідером на ринку телекомунікаційних технологій завдяки своїй інноваційній діяльності та багаторічному досвіду. Забезпечуючи постійний зв’язок і захист даних, ці технології підвищують продуктивність організацій.

1.2 Аналіз мережних рішень

Телекомунікаційні технології є життєво важливими для забезпечення ефективного та постійного зв’язку в різних сферах діяльності. В цьому підпункті буде розглянуто мережні рішення, які базуються на засобах Cisco, з оглядом їх основних характеристик, переваг і недоліків.

Маршрутизатори та комутатори Cisco є одними з найпоширеніших у сфері телекомунікаційних мереж. Маршрутизатори оптимізують використання смуги пропускання та забезпечують стабільність з'єднання, розподіляючи трафік між різними сегментами мережі. Забезпечуючи високу пропускну здатність і мінімальні затримки, комутатори відповідають за швидке та надійне передавання даних у локальних мережах.

Сучасні мережні рішення Cisco також включають бездротові точки доступу, що полегшує мобільність користувачів і дозволяє з'єднатися в місцях, де прокладання кабелів є складним або неможливим. Це особливо важливо для великих офісних будівель, складських приміщень і відкритих майданчиків.

Cisco пропонує широкий спектр рішень для забезпечення безпеки мереж у сфері захисту даних. Мережеві екрани, також відомі як файрволи, системи виявлення та запобігання вторгненням (IDS/IPS), засоби шифрування даних і системи контролю доступу належать до цієї категорії. Конфіденційність, цілісність і доступність даних, які забезпечують ці рішення, дозволяють захистити мережі від зовнішніх і внутрішніх загроз.

Програмно-визначені мережі (SDN) є ще одним важливим аспектом розвитку мережних технологій. Щоб відокремити керуючу плоскість від плоскості передачі даних, SDN дозволяє підвищити керованість і гнучкість мережевих інфраструктур. Це дозволяє керувати мережею з одного місця, що спрощує процес налаштування та оптимізації мережевих ресурсів.

Виявлення переваг і недоліків мережних рішень Cisco у порівнянні з іншими виробниками є важливою частиною аналізу. Основними перевагами продуктів Cisco є висока надійність, продуктивність і безпека, а також широка підтримка сучасних протоколів і стандартів. Недоліками також є висока вартість обладнання та складність налаштування, для якої потрібна висока кваліфікація персоналу.

Програмно-визначені мережі (SDN) — це сучасний метод управління телекомунікаційними мережами, який дозволяє підвищити керованість,

гнучкість і ефективність мережевої інфраструктури. Основним принципом SDN є відділення плоскості передачі даних від плоскості керування. За допомогою цього розділення програмне забезпечення можна використовувати для централізованого управління ресурсами мережі.

Ключовими елементами SDN є:

Контролер SDN: основна частина SDN, яка виконує функцію мозку мережі. Контролер контролює всі пристрої в мережі, приймає рішення щодо політики безпеки та маршрутизації трафіку. Він спрощує процес налаштування та моніторингу, а також забезпечує централізоване управління мережею. Контролери Cisco APIC-EM та OpenDaylight.

Пристрої мережі: маршрутизатори, комутатори та інші пристрої мережі, які можуть виконувати команди контролера SDN. Вони відповідають за передачу трафіку відповідно до політики, визначеної контролером.

Інтерфейси: API дозволяють взаємодіяти між контролерами SDN і мережевими пристроями. Команди можна передавати від контролера до мережевих пристроїв за допомогою API південного зв’язку, таких як OpenFlow. Інтерфейси північного зв’язку, також відомі як API північного зв’язку, дозволяють контролеру спілкуватися з додатками або сервісами, які працюють у мережі.

Переваги SDN включають:

Гнучкість: Швидке налаштування та перепланування мережі можливо без фізичних змін у топології.

Керованість: використання централізованого управління зменшує складність управління мережею та покращує контроль над нею.

Оптимізація ресурсів: SDN дозволяє оптимально використовувати мережеві ресурси, зменшуючи затримки та підвищуючи пропускну здатність.

Автоматизація: Централізоване управління може легко автоматизувати багато рутинних завдань, таких як оновлення політик безпеки або налаштування нових пристроїв.

Завдяки своїм перевагам і можливостям програмно-визначені мережі стають все більш популярними. SDN дозволяє організаціям створювати мережі, які більш адаптовані до сучасних бізнес-потреб.

Розглянемо пристрої мережі:

Маршрітизатори, також відомі як роутери, допомагають оптимізувати використання смуги пропускання та забезпечують стабільне з'єднання шляхом розподілу трафіку між різними сегментами мережі. Для визначення найкращого способу передавання даних вони використовують маршрутизаційні таблиці. Cisco ISR і Cisco ASR є популярними моделями маршрутизаторів Cisco, які пропонують широкий спектр функціональності, таких як підтримка VPN, якість послуг і багатошарова безпека.

Комутатори є важливою частиною локальних мереж (LAN), оскільки вони дозволяють передачі даних між пристроями в мережі швидко та надійно. Вони працюють на канальному рівні моделі відкритих систем (OSI), а трафік спрямовується до відповідних портів за допомогою таблиць MAC-адрес. Комутатори Cisco Catalyst і Nexus відомі своєю безпекою, масштабованістю та високою продуктивністю. Залежно від моделі вони підтримують різні швидкості передачі даних, включаючи 1 Gbps, 10 Gbps та більше.

У локальних мережах пристрої можна з'єднати за допомогою кабельних мереж, таких як UTP і STP. Найпоширенішими є кабелі категорії 5e, 6 і 6a, які забезпечують швидкості передачі даних до 1 Gbps і 10 Gbps відповідно. Вони мають вирішальне значення для створення мереж, які є надійними та стійкими.

SDI (Serial Digital Interface) і MDI (Media Dependent Interface) є двома типами кабелів, які використовуються в телекомунікаційних мережах. Тоді як MDI кабелі дозволяють підключати різні типи мережевого обладнання, SDI кабелі призначені для передачі цифрових відеосигналів високої якості. Передача даних на великі відстані з мінімальними затримками та високою швидкістю забезпечується оптичними волокнами, ще одним важливим компонентом телекомунікаційних мереж.

Точки доступу забезпечують користувачам бездротове підключення до мережі. Вони використовуються для розширення покриття мережі Wi-Fi, що дозволяє користувачам без кабелів підключатися до Інтернету. Продукти Cisco Aironet і Cisco Meraki підтримують найновіші стандарти бездротового зв'язку, такі як 802.11ac і 802.11ax (Wi-Fi 6), що гарантує швидкі та надійні зв'язки.

Мережеві адаптери: Мережеві адаптери, такі як PCIe карти та USB-адаптери, дозволяють кінцевим пристроям підключатися до мережі за допомогою дротового або бездротового підключення.

Фейєри (міжмережеві екрани): Фейєри захищають мережу від несанкціонованого доступу та кіберзагроз. Cisco пропонує низку продуктів ASA та Firepower, які можуть забезпечити захист мережі на кількох рівнях.

Концентратори VPN — це пристрої, які використовуються для створення захищених віртуальних приватних мереж (VPN), які дозволяють безпечно передавати інформацію між користувачами та віддаленими офісами.

Телефони VoIP — це пристрої, які можуть передавати голосові дані через IP-мережі, що зменшує витрати на телефонний зв'язок і забезпечує високу якість звуку.

Контролери бездротових мереж: це пристрої, які дозволяють керувати великими бездротовими мережами з одного місця, що дозволяє краще контролювати, моніторити та забезпечувати безпеку мережі.

Медіаконвертери: це пристрої, які дозволяють перетворювати сигнали з одного типу медіа (наприклад, мідних кабелів) на інший тип медіа (наприклад, оптичні волокна), що дозволяє мережам бути гнучкими та розширеними.

Ці компоненти та обладнання відіграють важливу роль у забезпеченні ефективного, надійного та безпечного функціонування телекомунікаційних мереж.

1.3 Постановка завдань для розробки

В проекті заплановано реалізувати мереже та побудувати схему зі всіма налаштуваннями мережевого обладнання на базі середовища EVE-NG.

Основна мета полягає у створенні стабільної, надійної та захищеної мережевої інфраструктури, що відповідатиме сучасним вимогам телекомунікаційних компаній та підприємств:

Спочатку буде проведено аналіз та обрано пристрої, мережні та кінцеві.

Наступним етапом буде спроєктовано логічну та фізичну схему мережі. Потрібно буде визначити топологію мережі, включаючи сегментацію мережі, розташування маршрутизаторів, комутаторів та інших пристроїв.

Логічна схема мережі — це важливий інструмент, який допомагає проектувати, розуміти та керувати мережею. Вона надає візуальне представлення структури мережі, включаючи всі пристрої та зв'язки між ними.

Фізична схема мережі — це візуальне представлення фізичного розташування та з'єднань між мережевими пристроями. Вона відіграє важливу роль у проектуванні, встановленні, управлінні та обслуговуванні мережі.

Наступним кроком буде встановлення та налаштування платформи EVE-NG для симуляції мережевої інфраструктури та завантаження та інтеграція образів мережевих пристроїв Cisco, включаючи маршрутизатори, комутатори, точки доступу та інше обладнання.

Після цього буде налаштовано основних мережевих функцій на маршрутизаторах Cisco, таких як маршрутизація, NAT, VPN, QoS та безпека. Налаштування комутаторів Cisco для забезпечення VLAN, STP, агрегації каналів та інших функцій комутації.

Наступним етапом буде впровадження інструментів моніторингу для відстеження стану мережі, виявлення проблем та їх своєчасного усунення.

Останнім етапом буде тестування мережі та підбивання підсумків з покращення роботи мережі.

2 ПРОЄКТУВАННЯ КОМП'ЮТЕРНОЇ СИСТЕМИ НА ОСНОВІ ЗАСОБІВ CISCO

2.1 Вибір активного мережевого обладнання

Для початку потрібно обрати маршрутизатор, для комп'ютерної системи для телекомунікаційних технологій.

На даний момент на ринку є велика кількість маршрутизаторів, які підходять для обчислювальних установок будь-якого розміру, від малих підприємств до великих організацій. Cisco є лідером у виробництві маршрутизаторів і є однією з провідних компаній у світі у сфері високих технологій. ASR і IRS є найпопулярнішими маршрутизаторами лінійки.

Маршрутизатор служб агрегації (ASR) (рис. 2.1) — це абревіатура від «маршрутизатор служб агрегації». Компанії та постачальники послуг, які мають високі вимоги до мережі, використовують CISCO ASR. Для збільшення пропускної здатності використовується Cisco ASR, який працює на операційній системі IOS XE. Cisco представила маршрутизатори ASR 900, ASR 1000 і ASR 9000 у своїй лінійці ASR.

Рисунок 2.1 – Маршрутизатор Cisco ASR

Уже тривалий час маршрутизатори для корпоративних мереж і провайдери Cisco ASR будуть доступні на ринку. Це оснащення призначено для виконання найскладніших завдань, оскільки ці продукти відрізняються високою продуктивністю та збільшеною відмовостійкістю.

Найбільш просунуту серію лінійки ASR, з раніше розглянутих, являє собою серія ASR 9000. Цей роутер є найдорожчим з представленої лінійки компанії. Ця серія надає клієнтам функції, з якими не зможе зрівнятися жоден інший маршрутизатор Cisco, можливості базової та граничної маршрутизації. Тим часом, решта маршрутизаторів серії ASR, здатні тільки на граничну маршрутизацію.

Integrated Service Router (ISR) (рис. 2.2) — пермін «інтегровані послуги» стосується способу організації комп'ютерної мережі, який гарантує високу якість обслуговування (QoS). Маршрутизатори серії ISR використовуються для з'єднання філій в організаціях малого та середнього розміру. Для забезпечення надійної та безпечної доступності філій дана серія використовує граничну маршрутизацію.

Рисунок 2.2 – Маршрутизатор Cisco ISR

Незважаючи на те, що маршрутизатори Cisco з сервісами агрегації та інтегровані маршрутизатори мають багато спільного, є кілька важливих відмінностей, які зрештою є більш важливими під час вирішення питання про купівлю маршрутизаторів Cisco ASR порівняно з маршрутизаторами ISR.

ISR Cisco: 1. для місць з обмеженою пропускною здатністю. 2: Цей ряд маршрутизаторів включає ISR 800, ISR 1900, ISR 2900, ISR 3900 і ISR 4000. 3: Це операційна система IOS.

Cisco ASR: для місць, які потребують великої пропускної здатності. 2: Операційна система IOS XE використовується. 3: ASR 900, ASR 1000 і ASR 9000 — це деякі з маршрутизаторів цієї серії.

Нижче, наведена таблиця порівняння цих двох лінійок (табл. 2.1):

Таблиця 2.1 – Порівняння лінійок Cisco ISR та ASR

	Серія Cisco ISR	Серія Cisco ASR
Використання	Cisco ISR розроблений спеціально для використання в невеликих мережах.	Cisco ASR розроблений спеціально для використання у великих мережах.
Операційна система	Серія ISR працює в системі Cisco IOS.	Серія ASR працює з системами Cisco IOS XE та XR.
Хмарний доступ	Cisco ISR має доступ до хмари.	Cisco ASR не має доступу до хмари.
Швидкість	Cisco ISR може обробляти швидкості до 10G.	Cisco ASR може працювати з швидкісними Ethernet-з'єднаннями, які досягають швидкості до 100G.
Щільність портів	Cisco ISR має нижчу щільність портів.	Cisco ASR має вищу щільність портів.

Тоді як маршрутизатори ISR призначені для мереж малого та середнього розміру, маршрутизатори ASR призначені для підприємств і постачальників послуг. Серія ISR займає менше місця, ніж серія ASR, оскільки вона розроблена для ситуацій, які потребують меншої кількості обчислювальних ресурсів. Оскільки серія ASR розроблена для великомасштабних додатків і організацій, вона пропонує додаткові функції та високий рівень продуктивності. Наприклад, маршрутизатори ASR підтримують 100G Ethernet, тоді як маршрутизатори ISR підтримують лише 10G. Крім того, серія ASR має більшу щільність портів. Маршрутизатори серії ASR 9000 є єдиними в своєму роді, які підтримують базову маршрутизацію.

Для роботи мережі достатньо функціоналу Cisco ISR, тому потрібно порівняти ISR 800, ISR 1900, ISR 2900, ISR 3900 та ISR 4000 (табл. 2.2):

Таблиця 2.2 – Порівняння маршрутизаторів Cisco ISR

Серія	Призначення	Операційна система	Пропускна здатність	Кількість портів	Доступ до хмари	Підтримка віртуалізації
Cisco ISR 800	Для невеликих офісів і філій	Cisco IOS	До 100 Мбіт/с	До 4 портів	Немає	Немає
Cisco ISR 1900	Для невеликих і середніх офісів	Cisco IOS	До 25-75 Мбіт/с	2-8 портів	Немає	Немає
Cisco ISR 2900	Для середніх офісів і філій	Cisco IOS	До 75-100 Мбіт/с	4-12 портів	Немає	Обмежена підтримка
Cisco ISR 3900	Для великих офісів і підприємств	Cisco IOS	До 250 Мбіт/с	8-20 портів	Немає	Часткова підтримка

Cisco ISR 4000	Для середніх і великих підприємств	Cisco IOS XE	До 1-2 Гбіт/с	8-88 портів	Є	Повна підтримка

Для виконання даного роду проєкту вистачить Cisco ISR 2900. Саме тому було обрано маршрутизатор Cisco 2911-V/K9 (рис. 2.3):

Рисунок 2.3 - Cisco 2911-V/K9

Маршрутизатор Cisco 2911-V/K9, який входить до серії ISR G2 (Integrated Services Routers Generation 2), розроблений для використання в середніх і великих мережах і може підтримувати послуги передачі даних, голосу та відео. Це надійне рішення для бізнесу, яке пропонує гнучкість, розширені функції маршрутизації, функціональність безпеки та високу продуктивність.

Має наступні характеристики (табл. 2.3):

Таблиця 2.3 – Характеристики Cisco 2911-V/K9

Тип маршрутизатора	Cisco Integrated Services Router (ISR)
Порти	3 порти Gigabit Ethernet, 1 порт для консолі, 1 порт для AUX
Кількість портів RJ45	3 порти RJ45 (Ethernet)

Наступним кроком буде вибір комутаторів.

Комутатор Cisco — це мережевий пристрій, розроблений Cisco Systems, який дозволяє з’єднати кілька пристроїв у локальній мережі (LAN) і контролювати трафік даних між ними. Комутатори працюють на канальному рівні (Layer 2) моделі Open Systems Interconnection (OSI). Однак комутатори рівня 3 також можуть виконувати деякі функції мережевого рівня (Layer 3). Ось повне пояснення:

1. Пересилання даних
    a. Рівень 2 (канальний рівень): Комутатори Cisco пересилають кадри даних на основі MAC-адрес (Media Access Control). Вони підтримують таблицю MAC-адрес для відстеження портів, пов'язаних з кожною MAC-адресою.
    b. Рівень 3 (мережевий рівень): Комутатори рівня 3 також маршрутизують пакети даних на основі IP-адрес, забезпечуючи міжмережеву маршрутизацію та зв'язок між різними підмережами.
2. Щільність портів: Комутатори Cisco поставляються з різними конфігураціями портів, від декількох портів у менших комутаторах до сотень портів у великих модульних комутаторах.
3. Підтримка VLAN: Віртуальні локальні мережі (VLAN) дозволяють мережевим адміністраторам сегментувати фізичну мережу на кілька логічних мереж, підвищуючи безпеку та продуктивність.

4. Якість обслуговування (QoS): Функції QoS дозволяють комутаторам надавати пріоритет певним типам трафіку, гарантуючи, що критичні додатки отримають необхідну пропускну здатність.
5. Живлення через Ethernet (PoE): Комутатори Cisco можуть подавати живлення на підключені пристрої, такі як IP-телефони, бездротові точки доступу і камери, усуваючи необхідність в окремих джерелах живлення для цих пристроїв.
6. Безпека: Комутатори Cisco пропонують розширені функції безпеки, включаючи списки контролю доступу (ACL), захист портів, аутентифікацію 802.1X і багато іншого для захисту мережі від несанкціонованого доступу і атак.
7. Керування: Комутаторами Cisco можна керувати через інтерфейс командного рядка (CLI), веб-інтерфейс або за допомогою програмного забезпечення для управління мережею Cisco, наприклад, Cisco DNA Center. Вони підтримують такі протоколи, як SNMP, NetFlow та інші для моніторингу та управління.
8. Резервування та надійність: Такі функції, як стекування, агрегація каналів та резервні джерела живлення, забезпечують високу доступність і надійність в корпоративних середовищах.
9. Масштабованість: Комутатори Cisco можна масштабувати від невеликих мереж до великих корпоративних мереж, використовуючи варіанти стекових комутаторів і модульних комутаторів на базі шасі, які дозволяють розширювати мережу в міру зростання вимог до неї.

Існують такі типи комутаторів Cisco:

1. Серія Cisco Catalyst: Включає серії Cisco Catalyst 9200, 9300, 9400, 9500: Широко використовуються в корпоративних мережах для рівнів доступу, розподілу та ядра.
2. Серія Cisco Nexus: включає серію Cisco Nexus 9000. Ці комутатори призначені для центрів обробки даних і забезпечують високу продуктивність, масштабованість і підтримку програмно-визначених

мереж (SDN) за допомогою Cisco ACI (Application Centric Infrastructure).

3. Серія Cisco Meraki: включає серію Cisco Meraki MS. Ці хмарні комутатори пропонують централізоване управління та ідеально підходять для розподілених мереж.

Для роботи цілком підійде серія комутаторів Cisco Catalyst. Отже, потрібно порівняти Cisco Catalyst 9200, 9300, 9400, 9500 (табл. 2.4):

Таблиця 2.4 – Порівняння комутаторів серії Cisco Catalyst

Серія	Призначення	Операційна система	Пропускна здатність	Архітектура	Кількість портів	Підтримка стекування	Підтримка віртуалізації
Cisco Catalyst 9200	Для середніх та малих підприємств	Cisco IOS XE	До 160 Гбіт/с	Фіксована	До 48 портів GE	Є (StackWise-80)	Немає
Cisco Catalyst 9300	Для корпоративних мереж і доступу в кампусах	Cisco IOS XE	До 480 Гбіт/с	Фіксована	До 48 портів GE або Multi-Gigabit	Є (StackWise-480)	Немає
Cisco Catalyst 9400	Для великих корпоративних мереж (модульний)	Cisco IOS XE	До 9 Тбіт/с (у шасі)	Модульна	До 384 портів GE або 10GE	Немає	Часткова підтримка

Cisco Catalyst 9500	Для агрегації і ядра кампусних мереж	Cisco IOS XE	До 6.4 Тбіт/с	Фіксована	До 40 портів 40GE або 100GE	Немає	Повна підтримка

Для виконання проєкту підійдуть комутатори Cisco Catalyst 9300. Отже, було обрано Cisco C9300-24P-A (рис.2.5):

Рисунок 2.5 - Cisco C9300-24P-A

Серія Catalyst 9300 включає комутатор Cisco C9300-24P-A, який розроблений для корпоративних мереж, які потребують високої швидкості та надійності. Ця модель підтримує живлення PoE+, що робить її ідеальною для підключення IP-телефонів, точок доступу та інших пристроїв, які потребують живлення по Ethernet.

Має наступні характеристики (табл. 2.5):

Таблиця 2.5 – Характеристики Cisco C9300-24P-A

Порти	24 порти Gigabit Ethernet (RJ45) з підтримкою PoE+; 4 порти для SFP uplink
Тип комутатора	Керований, Layer 2, корпоративний рівень
Кількість портів RJ45	24 порти RJ45
Додатково	Підтримка PoE+ (до 30 Вт на порт), можливість стекування до 8 комутаторів

2.2 Вибір кінцевих пристроїв

Для початку потрібно обрати стаціонарні ПК. В даному випадку вони будуть поділені на офісні, монтажні та дизайнерські станції.

Офісні станції потрібні для елементарної роботи за ПК, в даному випадку ц написання документів, перегляд та прослуховування відео і т.д. Для цього було обрано ПК PowerUp Core i5 6400/8 GB/SSD 256GB/Int Video (рис. 2.6):

Рисунок 2.6 – Офісний ПК PowerUp Core i5 6400/8 GB/SSD 256GB/Int Video

ПК має наступні характеристики (табл. 2.6):

Таблиця 2.6 – Характеристики ПК PowerUp Core i5 6400/8 GB/SSD 256GB/Int Video

Процесор	Core i5 6400
Кількість ядер / потоків	4/4
Відеокарта	int Video
Материнська плата	HP, Acer s1151
Оперативна пам'ять	DDR4 8 GB
HDD	No HDD
SSD	SSD 256GB
Блок живлення	400W
Корпус	MiniTower ATX

Наступним кроком буде вибір дизайнерських станцій. Їх основна задача це обробка ефектів та робота з графікою. Для дизайнерських станцій обрано ПК Expert PC Ultimate (рис. 2.7)

Рисунок 2.7 - Expert PC Ultimate

Даний ПК має наступні характеристики (табл. 2.7)

Таблиця 2.7 – Характеристики дизайнерського ПК Expert PC Ultimate

Модель центрального процесора	Ryzen 7 5700X
Об'єм ОЗП	32 ГБ
Об'єм накопичувача	1 ТБ
Модель графічного процесора	GeForce RTX 4060 Ti
Об'єм відео пам'яті	8 ГБ

Останнім кроком вибору стаціонарних ПК буде підбір монтажних станцій. Вони потрібні для якісної роботи з відео.

Для даного проєкту в якості монтажних ПК обрано ПК Cobra Gaming (рис. 2.8):

Рисунок 2.8 - Cobra Gaming

Даний ПК має наступні характеристики (табл.2.8):

Таблиця 2.8 – Характеристики Cobra Gaming

Модель центрального процесора	Ryzen 5 3600
Об'єм ОЗП	32 ГБ
Об'єм накопичувача	2 ТБ
Модель графічного процесора	GeForce RTX 4070
Об'єм відео пам'яті	12 ГБ

Останнім кроком буде вибір сервера для Active Directory. Для цього було обрано сервер Supermicro SYS-6029P-TR, він має наступні характеристики (табл.2.9):

Таблиця 2.9 – Характеристика Supermicro SYS-6029P-TR

Кількість U	2U
Тип сервера	Стійкові (Rack)
Процесор	Intel Xeon
Обсяг ОЗП	16 ГБ

Стійкий сервер Supermicro SYS-6029P-TR містить два потужні шестиядерних процесори Xeon Bronze від Intel. Ядро має тактову частоту 1,9 ГГц. Модель також оснащена планкою оперативної пам'яті об’ємом 16 Гб. Це все забезпечує хорошу роботу системи. Таким чином, сервер має хороші показники масштабованості та пропонує широкі можливості для апгрейда. Так, модель має чотири слота RAM, що дозволяє ОЗП. Підтримується 512 Гб оперативки.

Сервер має SSD накопичувач на 240 Гб. В ньому також є вісім гнізд для жорстких або твердотільних носіїв 2,5 дюйма. Також є слот U.2 NVMe. Модель також підтримує установку двох блоків живлення.

2.3 Проєктування логічної схеми мережі

В проєкті передбачено, що мережа складатиметься з 1 маршрутизатора Cisco 2911-V/K9, 4-х комутаторів Cisco C9300-24P-A, 2-х монтажних станцій Cobra Gaming, 3-х дизайнерських станцій Expert PC Ultimate, 35 офісних станцій PowerUp та 1 сервера Supermicro SYS-6029P-TR.

Відобразимо логічну схему мережі (рис. 2.9):

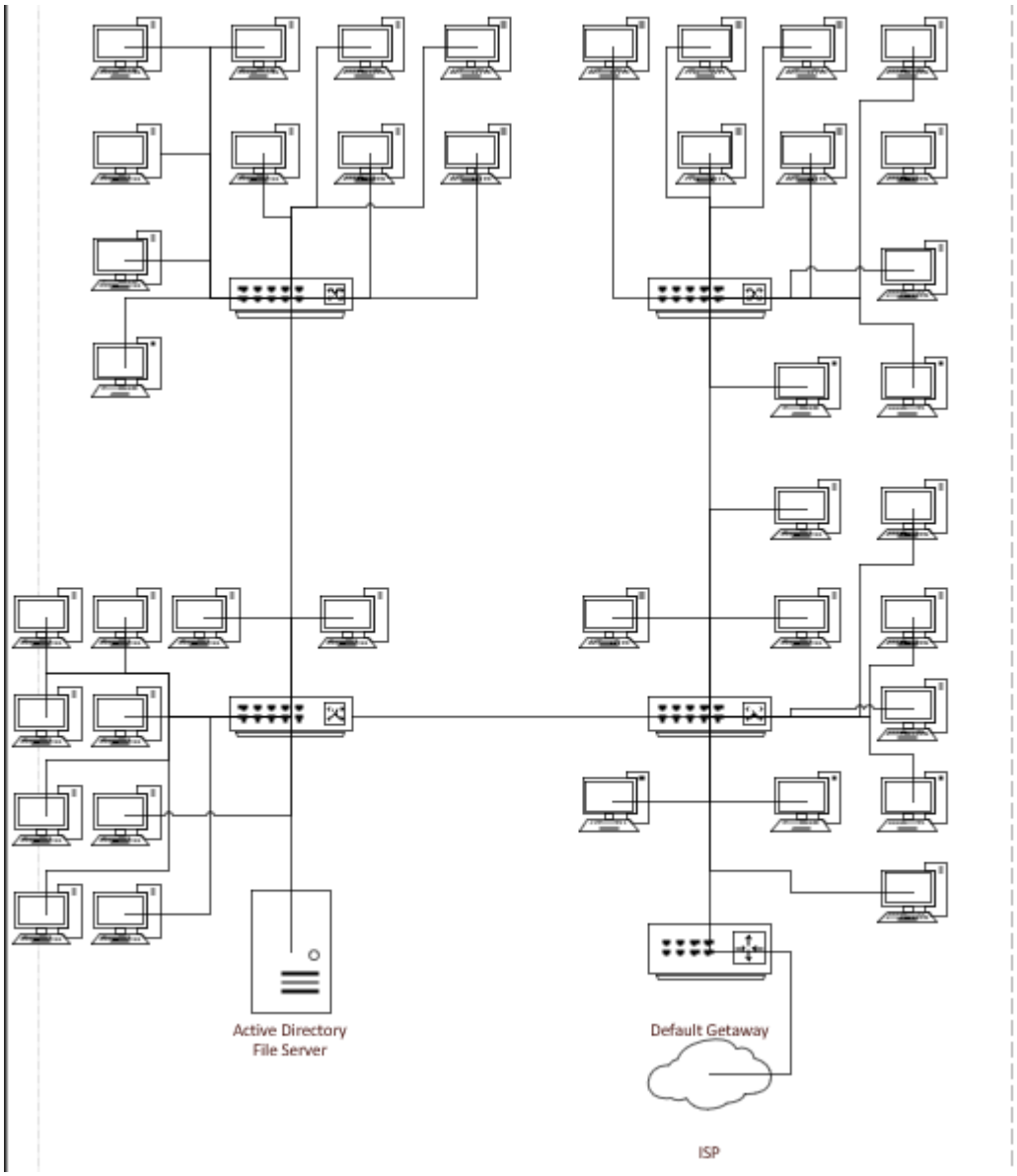

Рисунок 2.9 – Логічна схема мережі

Наступним кроком потрібно розділити мережу на VLAN-и. На підприємстві є 9 орг-юнітів:

- Дирекція – 5 ПК PowerUp;
- Бухгалтерський відділ – 4 ПК PowerUp;
- Юридичний відділ – 3 ПК PowerUp;
- ІТ-відділ – 1 ПК PowerUp;
- Відділ реклами – 4 ПК PowerUp;

- Відділ редакторів – 16 ПК PowerUp;
- Аналітичний відділ – 2 ПК PowerUp;
- Дизайнерський відділ – 3 ПК Expert PC Ultimate;
- Відділ режисерів – 2 ПК Cobra Gaming.

Кожен відділ буде ділитися на окремий VLAN/ Виходячи з цього маємо наступну таблицю VLAN-ів (табл. 2.10)

Таблиця 2.10 – Таблиця VLAN

№ VLAN	Ім’я VLAN	Примітка
10	dir	Дирекція
20	buh	Бухгалтерський відділ
30	law	Юридичний відділ
40	it	IT-відділ
50	adv	Відділ реклами
60	edit	Відділ редакторів
70	ana	Аналітичний відділ
80	diz	Дизайнерський відділ
90	film	Відділ режисерів
100	managment	Для керування мережевими пристроями

Маємо наступну схему VLAN (рис. 2.10):

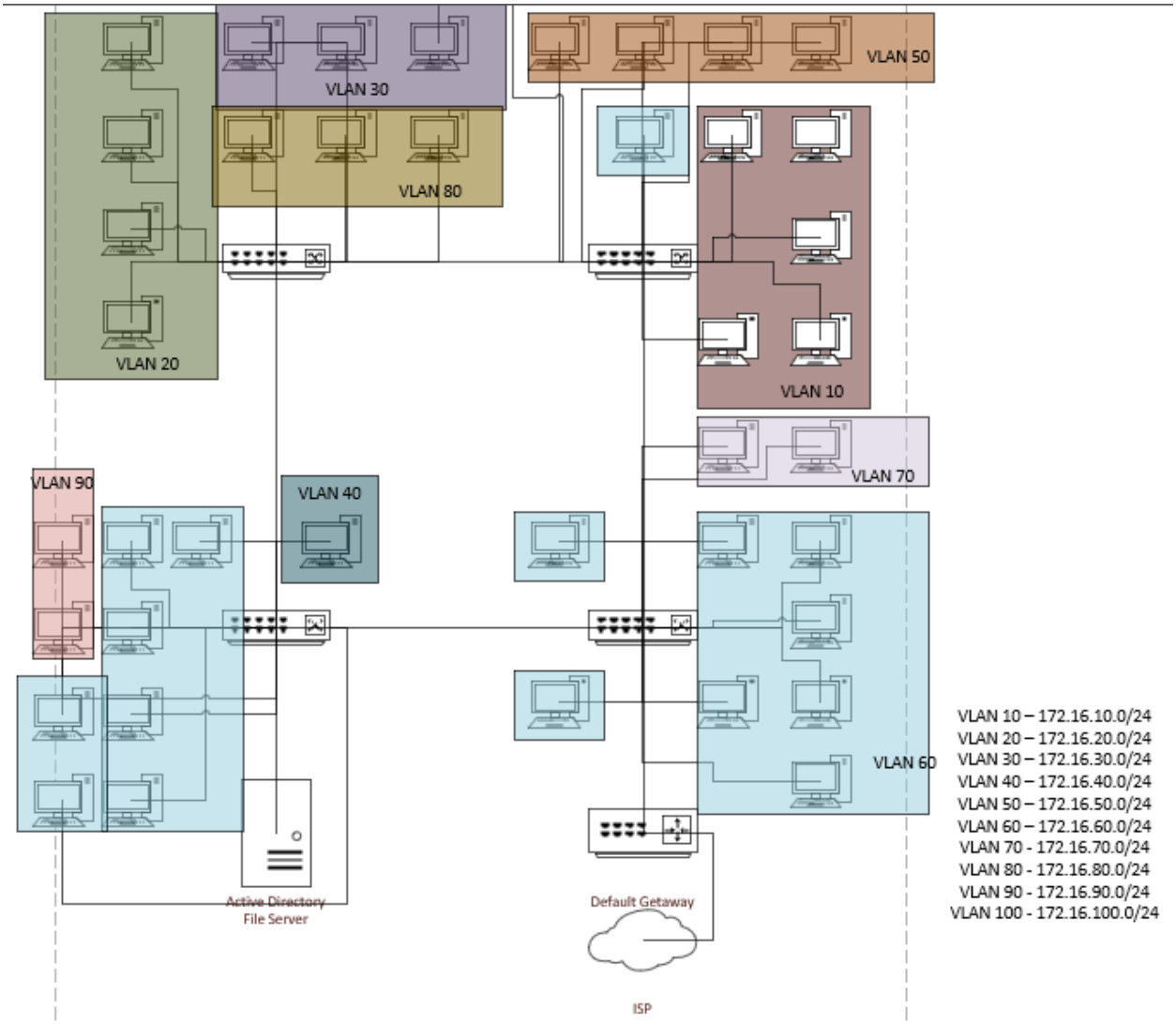

Рисунок 2.10 – Схема VLAN

Виходячи з картинки вище, маємо наступні підмережі (рис. 2.11):

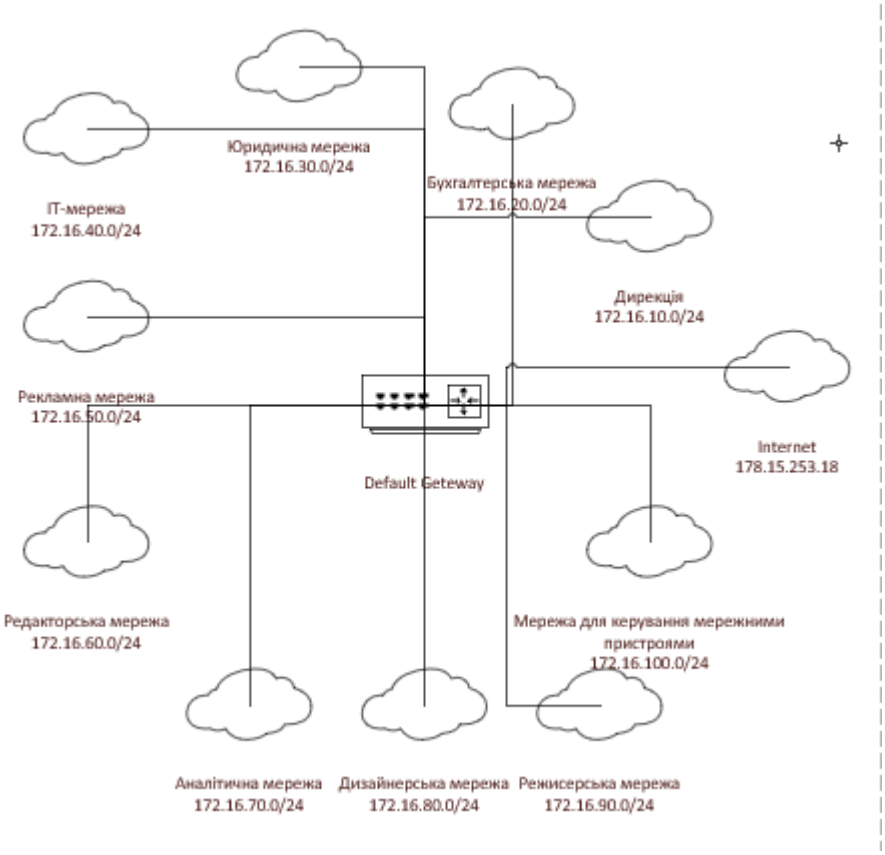

Рисунок 2.11 – Підмережі комп’ютерної системи

Отже, в ході другого етапу проєкту було створено логічну схему мережі, вона демонструє елементи або компоненти, з’єднані в мережі. До таких компонентів належать комп’ютери, факсимільні апарати, принтери, брандмауери, сервери тощо. Спосіб з’єднання одного з іншим представлено на схемі логічної топології мережі, оскільки вона розповідає, як логічно відбувається передача в цих інструментах у мережі. З іншого боку, схема мережі — це схема, яка показує саму мережу технічній команді, наприклад IT-адміністратору та кібербезпеці.

3 РЕАЛІЗАЦІЯ КОМП'ЮТЕРНОЇ СИСТЕМИ

3.1 Налаштування середовища для розробки

Для початку потрібно налаштувати середовище для розробки. У нас середовищем буде виступати EVE-NG всередині Google Cloud. Хмарні технології в останні роки набирають все більшої популярності. Це зрозуміло, оскільки вже довгий час все більше і більше в світі превалює тенденція виходу бізнесу в Інтернет простір. Це почалося навіть набагато раніше, ніж трапилася пандемія, але ми також не можемо ігнорувати впливу коронавірусу на цей тренд. Говорячи про міграцію в хмару, ми завжди думаємо про видатних гравців на вершині хмарних технологій і Google Cloud, безумовно, входить до їхнього числа.

Google Cloud – це набір сервісів, які можуть допомогти великим, середнім та малим підприємствам перейти на цифрові технології. Google Cloud Platform також є частиною Google Cloud, яка надає місце для розгортання та розміщення ваших веб-застосунків.

Google Cloud Platform (GCP) працює в інфраструктурі, ідентичній інфраструктурі продуктів Google для кінцевих користувачів. Він пропонує модульні послуги машинного навчання, зберігання та аналізу даних. ГКП доступний у багатьох країнах і регіонах по всьому світу, і він пропонує широкий спектр ресурсів, бібліотек і послуг, необхідних для розробки, розгортання та керування хмарними програмами.

EVE-NG — це сучасна платформа, яка використовується інженерами, адміністраторами та студентами для емуляції мережевих інфраструктур і тестування різних технологій. Він надає можливість створювати віртуальні середовища для навчання, тестування конфігурацій і моделювання реальних мережевих сценаріїв. Це дозволяє використовувати різноманітне мережеве обладнання для відтворення складних топологій.

Підтримка Cisco IOL (IOS on Linux) є важливою перевагою EVE-NG, оскільки вона дозволяє працювати з віртуальними образами Cisco без використання фізичного обладнання. Це робить платформу ідеальною для налаштування політик безпеки, тестування сценаріїв взаємодії пристроїв і моделювання мережевих рішень.

Використання Cisco IOL в EVE-NG є особливо важливим для цього проекту, оскільки це спрощує та ефективнить процес створення комп'ютерних систем. Це дозволяє створювати деталізовані мережеві середовища для тестування, перевірки конфігурації, навчання та відпрацювання сценаріїв відмови. Інтеграція Cisco IOL дозволяє використовувати всі переваги платформ Cisco, такі як управління доступом, потужні інструменти маршрутизації та гнучкість у налаштуванні.

Висока продуктивність і масштабованість платформи роблять її універсальним інструментом для розробки, навчання та експериментів у сфері телекомунікаційних технологій, дозволяючи моделювати навіть великі корпоративні мережі.

Для початку потрібно створити віртуальну машину EVE-NG (рис. 3.1):

Рисунок 3.1 – Створення віртуальної машини

Наступним кроком буде додавання образів в EVE-NG.

Спочатку потрібно завантажити образи Cisco IOL (рис. 3.2):

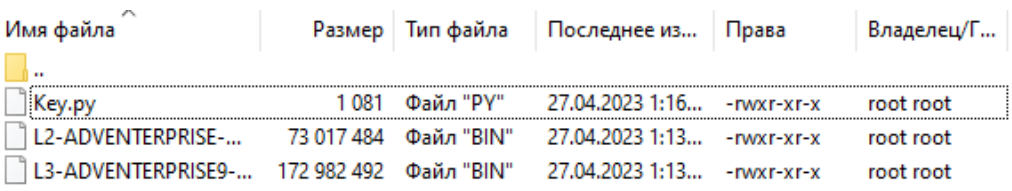

Рисунок 3.2 – Завантаження образів Cisco IOL в EVE-NG

Cisco IOL (IOS on Linux) — це емулятор мережного обладнання Cisco, який дозволяє використовувати Cisco IOS (Internetwork Operating System) на операційній системі Linux. З іншого боку, це модифікована версія Cisco IOU (IOS on Unix), адаптована для роботи на Linux. Cisco IOL використовується для навчання, тестування і симуляції мережевих конфігурацій без фізичного обладнання.

Наступним кроком буде додавання Windows 10 та Windows Server 2019.

Алгоритм дії складатиметься з того, що нам потрібно завантажити образи та створити віртуальний жорсткий диск (рис. 3.3):

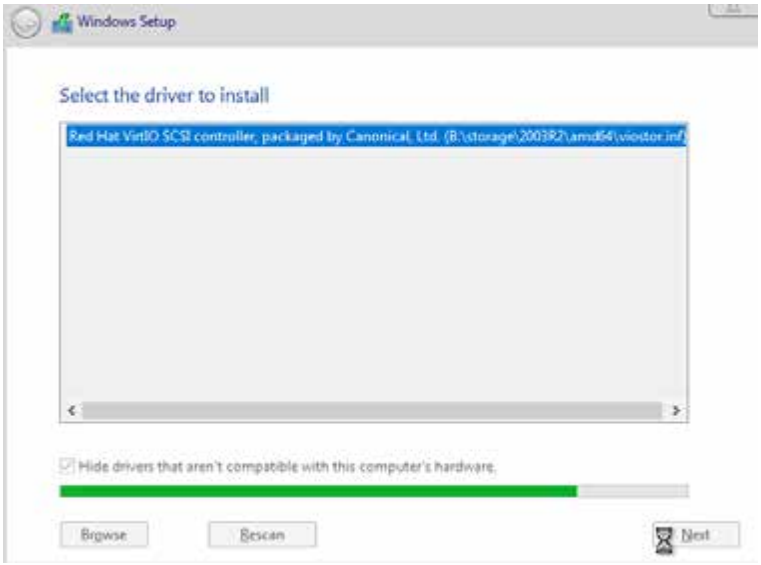

Рисунок 3.3 – Віртуальний жорсткий диск, приєднується до образу Windows 10

Також потрібно зберегти стан поточного віртуального диску та видалити sdrom.iso (рис. 3.4):

```
root@eve-ng:/opt/unetlab/tmp/0/e3abdcb3-0f7d-4738-94b0-1581900eb2c8/1# cd /opt/u
netlab/addons/qemu/win-10/
root@eve-ng:/opt/unetlab/addons/qemu/win-10# rm -f cdrom.iso
root@eve-ng:/opt/unetlab/addons/qemu/win-10#
```

Рисунок 3.4 – Видалення cdrom.iso

Аналогічні дії потрібно виконати з Windows Server 2019.

Після чого потрібно скласти логічну схему мережі (рис. 3.5):

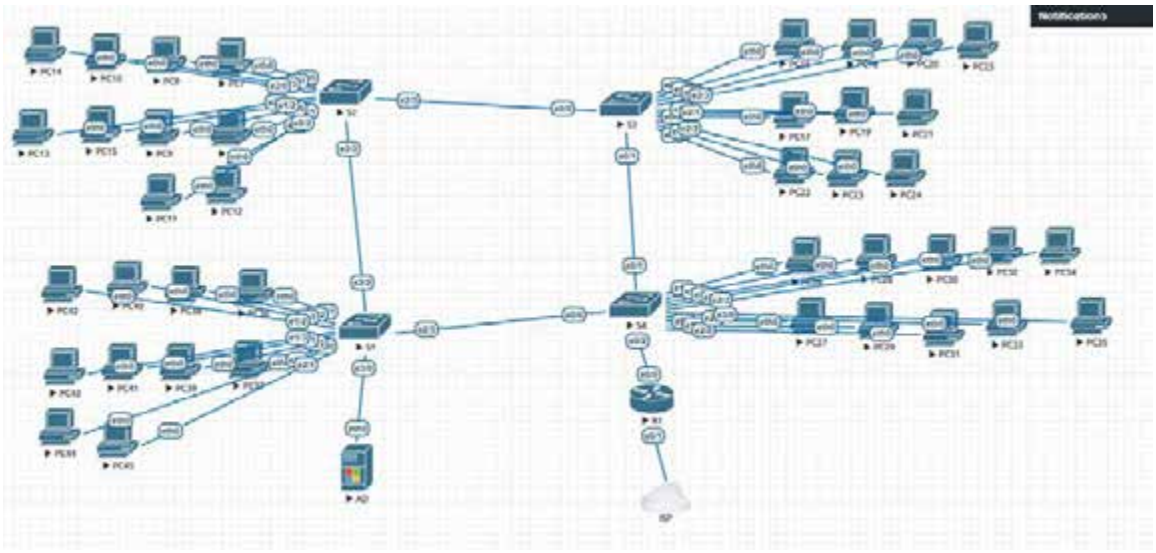

Рисунок 3.5 – Логічна схема мережі в середовищі EVE-NG

3.2 Налаштування комутаторів Cisco

Для початку потрібно налаштувати L2 комутатори Cisco.

Рівень мережевого комутатора визначає, де він знаходиться в мережевій моделі Open Systems Interconnection (OSI). Це визначає рівень інтелекту та функціональності пристрою, а також, що найважливіше для покупців, його ціну. Терміни Layer 2 і Layer 3 отримані з моделі Open System Interconnection (OSI), яка служить еталоном для опису та пояснення мережевих комунікацій. Прикладний рівень, рівень представлення, сеансовий рівень, транспортний рівень, мережевий рівень, канальний рівень і фізичний рівень складають модель Open Systems Interconnection (OSI). Рівень канального рівня знаходиться на рівні 2, а мережевий рівень знаходиться на рівні 3. Комутатори рівня 2 і 3 відповідно називають комутатори цих рівнях.

Комутатор L2 може обробляти фрейми, або кадри інформації, окрім електричних сигналів. Він використовує логіку фізичної адресації, яка базується на MAC-адресах передавальних і приймальних пристроїв.

Спочатку потрібно дати імена комутаторам та налаштувати на них паролі (рис. 3.6):

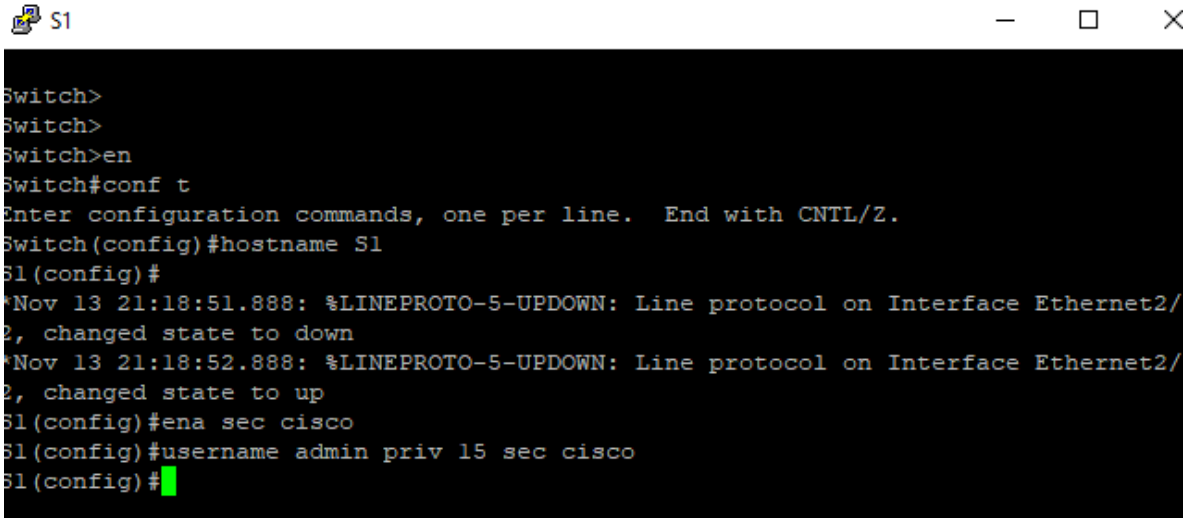

Рисунок 3.6 – Налаштування імена комутатора та паролів для входу

Налаштуємо авторизацію при підключенні до консолі (рис. 3.7):

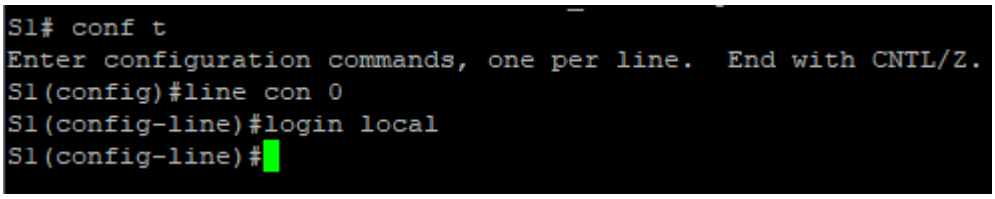

Рисунок 3.7 – Налаштування авторизації при підключенні до консолі для комутатора

Задаємо ip-адресу для керування пристроєм (рис. 3.8):

```
Sl(config-line)#int vlan 100
Sl(config-if)#
*Nov 13 21:25:20.992: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan100, c
hanged state to down
Sl(config-if)#ip add 172.16.100.10 255.255.255.0
Sl(config-if)#no sh
Sl(config-if)#
*Nov 13 21:26:20.567: %LINK-3-UPDOWN: Interface Vlan100, changed state to down
Sl(config-if)#ip default-geteway 172.16.100.1
```

Рисунок 3.8 – Задаємо ip-адресу для керування пристроєм

Налаштовуємо ssh на комутаторах (рис. 3.9):

```
Sl(config)#no ip dom
Sl(config)#no ip domain-
Sl(config)#no ip domain-loo
Sl(config)#no ip domain-lookup
Sl(config)#ip dom
Sl(config)#ip domain na
Sl(config)#ip domain name Sl
Sl(config)#ip ssh ver 2
Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
Sl(config)#cryp
Sl(config)#crypto key
Sl(config)#crypto key gen
Sl(config)#crypto key generate r
Sl(config)#crypto key generate rsa
The name for the keys will be: Sl.Sl
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

Sl(config)#
*Nov 13 21:32:31.794: %SSH-5-ENABLED: SSH 2.0 has been enabled
Sl(config)#line vty 0 15
                    ^
% Invalid input detected at '^' marker.

Sl(config)#line vty 0 ?
  <1-4>  Last Line number
  <cr>

Sl(config)#line vty 0 4
Sl(config-line)#tra
Sl(config-line)#transport in
Sl(config-line)#transport input ssh
Sl(config-line)#login local
Sl(config-line)#
```

Рисунок 3.8 – Налаштування ssh на комутаторах

Далі налаштуємо VTP. Сервером буде виступати S1 а інші комутатори – клієнти.

Протокол Cisco VTP (VLAN Trunking Protocol) автоматизує керування та поширення інформації про віртуальні локальні мережі (VLAN) у мережі комутатора. Він робить управління VLAN простішим, особливо в великих мережах із великою кількістю комутаторів.

Налаштуємо VTP-сервер (рис. 3.9):

```
S1(config)#vtp ver 2
S1(config)#vtp mode server
Device mode already VTP Server for VLANS.
S1(config)#vtp domain Shvedov
Changing VTP domain name from NULL to Shvedov
S1(config)#
*Nov 13 21:43:38.686: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to Shvedov.
S1(config)#vtp password cisco
Setting device VTP password to cisco
S1(config)#
```

Рисунок 3.9 – Налаштування VTP-сервера

Налаштовуємо VTP-клієнт (рис.3.10):

```
S2(config)#vtp ver 2
VTP version is already in V2.
S2(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
S2(config)#
*Nov 13 21:46:43.292: %SW_VLAN-4-VTP_USER_NOTIFICATION: VTP protocol user notifi
cation: MD5 digest checksum mismatch on receipt of equal revision summary on tru
nk: Et2/2

S2(config)#vtp dom Shvedov
Domain name already set to Shvedov.
S2(config)#vtp password cisco
Setting device VTP password to cisco
S2(config)#do wr
Building configuration...
Compressed configuration from 1114 bytes to 605 bytes[OK]
S2(config)#
```

Рисунок 3.10 – Налаштування VTP-клієнта

Далі потрібно створити VLANs на VTP-сервері (рис. 3.11):

```
Sl(config)#vlan 10
Sl(config-vlan)#name dir
Sl(config-vlan)#vlan 20
Sl(config-vlan)#name buh
Sl(config-vlan)#vlan 30
Sl(config-vlan)#name law
Sl(config-vlan)#vlan 40
Sl(config-vlan)#name it
Sl(config-vlan)#vlan 50
Sl(config-vlan)#name adv
Sl(config-vlan)#vlan 60
Sl(config-vlan)#name edit
Sl(config-vlan)#vlan 70
Sl(config-vlan)#name ana
Sl(config-vlan)#vlan 80
Sl(config-vlan)#name diz
Sl(config-vlan)#vlan 90
Sl(config-vlan)#name film
Sl(config-vlan)#vlan 100
Sl(config-vlan)#name managment
Sl(config-vlan)#
```

Рисунок 3.11 – Створення VLAN

VLAN, також відомий як Virtual Local Area Network, поділяє мережу на окремі сегменти. Ці сегменти працюють як окремі мережі, навіть якщо пристрої фізично підключені до одного комутатора. Використання VLAN дозволяє групувати пристрої за логічними ознаками (наприклад, за відділами або функціями) без залежності від фізичної інфраструктури, що покращує безпеку, керованість і продуктивність мережі.

VLAN потрібен для наступних цілей:

- Об'єднання в єдину мережу комп'ютерів, підключених до різних комутаторів;
- Поділ у різні підмережі комп'ютерів, підключених до одного комутатора;
- Поділ гостьової Wi-Fi мережі та Wi-Fi мережі підприємства.

Наступним кроком буде налаштування ACCESS та TRUNK-портів.

Типи портів на комутаторах Access і Trunk регулюють передачу даних між VLAN. Вони є важливою частиною управління трафіком VLAN у мережі.

Порт доступу, також відомий як ACCESS порт, може бути підключений лише до однієї VLAN і може передавати трафік для цієї VLAN без тегування.

Зазвичай комутатор підключається до кінцевих пристроїв, таких як комп’ютери, принтери та IP-телефони.

Як магістральний порт, trunk-порт може передавати трафік для кількох VLAN. Trunk-порти дозволяють комутаторам з’єднатися між собою або до маршрутизатора, щоб передавати трафік кількох VLAN.

Налаштуємо ACCESS-порти комутатора (рис. 3.12):

```
Sl(config-if)#int e0/1
Sl(config-if)#sw
Sl(config-if)#switchport mod
Sl(config-if)#switchport mode acc
Sl(config-if)#switchport mode access
Sl(config-if)#sw
Sl(config-if)#switchport acc
Sl(config-if)#switchport access vl
Sl(config-if)#switchport access vlan 40
Sl(config-if)#int e0/2
Sl(config-if)#sw
Sl(config-if)#switchport mod
Sl(config-if)#switchport mode acc
Sl(config-if)#switchport mode access
Sl(config-if)#sw
Sl(config-if)#switchport acc
Sl(config-if)#switchport access vl
Sl(config-if)#switchport access vlan 90
Sl(config-if)#int el/0
Sl(config-if)#switchport mode access
Sl(config-if)#switchport access vlan 90
Sl(config-if)#int range el/1-e3/0
                             ^
% Invalid input detected at '^' marker.

Sl(config)#int range el/1-3
Sl(config-if-range)#switchport mode access
Sl(config-if-range)#switchport access vlan 60
Sl(config-if-range)#do wr
Building configuration...
Compressed configuration from 1817 bytes to 1028 bytes[OK]
Sl(config-if-range)#int e3/0
Sl(config-if)#switchport mode access
Sl(config-if)#switchport access vlan 40
Sl(config-if)#do wr
Building configuration...
Compressed configuration from 1868 bytes to 1046 bytes[OK]
Sl(config-if)#
```

Рисунок 3.12 – Налаштування ACESS-портів комутатора

Налаштуємо TRUNK-порти (рис. 3.13):

```
Sl(config-if)#int e2/3
Sl(config-if)#switchport trunk encapsulation dotlq
Sl(config-if)#switchport mode trunk
Sl(config-if)#
```

Рисунок 3.13 – Налаштування TRUNK-портів комутатора

Ще одним етапом буде налаштування STP на комутаторах (рис. 3.14):

```
Sl(config)#spannin
Sl(config)#spanning-tree mo
Sl(config)#spanning-tree mode rap
Sl(config)#spanning-tree mode rapid-pvst
Sl(config)#
```

Рисунок 3.14 – Налаштовуємо STP на комутаторах

Для запобігання петлям у мережах Ethernet використовуються протоколи STP і RSTP. Вони забезпечують резервування шляхів і стабільну роботу мережі, автоматично організовуючи топологію комутаторів.

Протокол STP призначений для запобігання петлям у мережах із резервними шляхами. Множинне дублювання трафіку, перевантаження мережі та неправильне функціонування мережевих пристроїв – усе це результати використання петлів.

Далі задля безпеки налаштовуємо фільтрацію по MAC-адресі (рис. 3.15):

```
Sl(config-if)#int e0/1
Sl(config-if)#switchport port-security max 1
Sl(config-if)#switchport port-security mac-address sticky
Sl(config-if)#int e0/2
Sl(config-if)#switchport port-security max 1
Sl(config-if)#switchport port-security mac-address sticky
Sl(config-if)#int e1/0
Sl(config-if)#switchport port-security max 1
Sl(config-if)#switchport port-security mac-address sticky
Sl(config-if)#int e1/2
Sl(config-if)#switchport port-security max 1
Sl(config-if)#switchport port-security mac-address sticky
Sl(config-if)#int e1/3
Sl(config-if)#switchport port-security max 1
Sl(config-if)#switchport port-security mac-address sticky
Sl(config-if)#int e1/1
Sl(config-if)#switchport port-security max 1
Sl(config-if)#switchport port-security mac-address sticky
Sl(config-if)#int e0/3
Sl(config-if)#switchport port-security max 1
Sl(config-if)#switchport port-security mac-address sticky
Sl(config-if)#int e0/0
Sl(config-if)#switchport port-security max 1
Sl(config-if)#switchport port-security mac-address sticky
Sl(config-if)#int e2/0
Sl(config-if)#switchport port-security max 1
Sl(config-if)#switchport port-security mac-address sticky
Sl(config-if)#int e2/1
Sl(config-if)#switchport port-security max 1
Sl(config-if)#switchport port-security mac-address sticky
Sl(config-if)#int e3/0
Sl(config-if)#switchport port-security max 1
Sl(config-if)#switchport port-security mac-address sticky
Sl(config-if)#
```

Рисунок 3.15 – Налаштування фільтрації по MAC-адресі

Функція port security є функцією комутатора, яка дозволяє вказувати MAC-адреси хостів, яким дозволено передавати дані через порт. Якщо MAC-адреса відправника не вказана як дозволена, порт не передає пакети. Крім того, можна обмежити кількість MAC-адрес, дозволених для передачі трафіку через порт комутатора.

Використовується, щоб запобігти:

- несанкціоноване змінення мережевого пристрою MAC-адреси або підключення до мережі;
- атаки з метою переповнення таблиці комутації.

На даному етапі налаштування комутаторів завершено, далі буде налаштовано маршрутизатор.

3.3 Налаштування маршрутизатора Cisco

Першим етапом налаштуємо ім’я пристрою та паролі та налаштуємо SSH (рис. 3.16):

```
Router(config)#host
Router(config)#hostname R-1
R-1(config)#ip dom
R-1(config)#ip domain-n
R-1(config)#ip domain-name corpcisco.local
R-1(config)#crypto key generate rsa
The name for the keys will be: R-1.corpcisco.local
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 512
% Generating 512 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

R-1(config)#
*May  1 15:06:38.834:  RSA key size needs to be atleast 768 bits for ssh version
 2
R-1(config)#
*May  1 15:06:38.839: %SSH-5-ENABLED: SSH 1.5 has been enabled
R-1(config)#ip ssh version 2
Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
R-1(config)#ip ssh time-out 60
R-1(config)#ip ssh authentication-retries 2
R-1(config)#P4QQ
R-1#
*May  1 15:07:51.784: %SYS-5-CONFIG_I: Configured from console by console
R-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R-1(config)#line vty 0 4
R-1(config-line)#transport input ssh
R-1(config-line)#login local
R-1(config-line)#user
R-1(config-line)#usern
R-1(config-line)#username admin priviligate 15 secret Dm3Sh2!
                 ^
% Invalid input detected at '^' marker.

R-1(config-line)#exit
R-1(config)#user
R-1(config)#usern
R-1(config)#username admin pri
R-1(config)#username admin privilege 15 sec
R-1(config)#username admin privilege 15 secret Dm3Sh2!
```

Рисунок 3.16 – Налаштування паролів та SSH на маршрутизаторі

Далі налаштовуємо авторизацію для підключення до консолі (рис. 3.17):

```
R-1(config)#enable sec
R-1(config)#enable secret Dm3Sh2!
R-1(config)#line cons
R-1(config)#line console 0
R-1(config-line)#login local
R-1(config-line)#
```

Рисунок 3.17 – Налаштування підключення до консолі на маршрутизаторі

Наступним кроком буде налаштування VLAN на маршрутизаторі (рис. 3.18):

```
R1(config-if)#int e0/0.10
R1(config-subif)#enc
R1(config-subif)#encapsulation do
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip add
R1(config-subif)#ip address 172.16.10.1 255.255.255.0
R1(config-subif)#no sh
R1(config-subif)#int e0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 172.16.20.1 255.255.255.0
R1(config-subif)#int e0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 172.16.30.1 255.255.255.0
R1(config-subif)#int e0/0.40
R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#ip address 172.16.40.1 255.255.255.0
R1(config-subif)#int e0/0.50
R1(config-subif)#encapsulation dot1Q 50
R1(config-subif)#ip address 172.16.50.1 255.255.255.0
R1(config-subif)#int e0/0.60
R1(config-subif)#encapsulation dot1Q 60
R1(config-subif)#ip address 172.16.60.1 255.255.255.0
R1(config-subif)#int e0/0.70
R1(config-subif)#encapsulation dot1Q 70
R1(config-subif)#ip address 172.16.70.1 255.255.255.0
R1(config-subif)#int e0/0.80
R1(config-subif)#encapsulation dot1Q 80
R1(config-subif)#ip address 172.16.80.1 255.255.255.0
R1(config-subif)#int e0/0.90
R1(config-subif)#encapsulation dot1Q 90
R1(config-subif)#ip address 172.16.90.1 255.255.255.0
R1(config-subif)#int e0/0.100
R1(config-subif)#encapsulation dot1Q 100
R1(config-subif)#ip address 172.16.100.1 255.255.255.0
R1(config-subif)#do wr
Building configuration...
[OK]
R1(config-subif)#
```

Рисунок 3.18 – Налаштування VLAN на маршрутизаторі

Далі потрібно налаштувати DHCP-сервер на маршрутизаторі Cisco (рис 3.19):

```
R1(config)#ip dhcp pool DIR
R1(dhcp-config)#net
R1(dhcp-config)#netw
R1(dhcp-config)#network 172.16.10.0 255.255.255.0
R1(dhcp-config)#defaul
R1(dhcp-config)#default-router 172.16.10.1
R1(dhcp-config)#dns-server 172.16.10.1
R1(dhcp-config)#exit
R1(config)#ip dhcp pool BUH
R1(dhcp-config)#network 172.16.20.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.20.1
R1(dhcp-config)#dns-server 172.16.20.1
R1(dhcp-config)#exit
R1(config)#ip dhcp pool LAW
R1(dhcp-config)#network 172.16.30.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.30.1
R1(dhcp-config)#dns-server 172.16.30.1
R1(dhcp-config)#exit
R1(config)#ip dhcp pool IT
R1(dhcp-config)#network 172.16.40.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.40.1
R1(dhcp-config)#dns-server 172.16.40.1
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ADV
R1(dhcp-config)#network 172.16.50.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.50.1
R1(dhcp-config)#dns-server 172.16.50.1
R1(dhcp-config)#exit
R1(config)#ip dhcp pool EDIT
R1(dhcp-config)#network 172.16.60.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.50.1
R1(dhcp-config)#default-router 172.16.60.1
R1(dhcp-config)#NO default-router 172.16.50.1
R1(dhcp-config)#default-router 172.16.60.1
R1(dhcp-config)#dns-server 172.16.60.1
R1(dhcp-config)#exit
R1(config)#ip dhcp pool ANA
R1(dhcp-config)#network 172.16.70.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.70.1
R1(dhcp-config)#dns-server 172.16.70.1
R1(dhcp-config)#exit
R1(config)#ip dhcp pool DIZ
R1(dhcp-config)#network 172.16.80.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.80.1
R1(dhcp-config)#dns-server 172.16.80.1
R1(dhcp-config)#exit
R1(config)#ip dhcp pool FILM
R1(dhcp-config)#network 172.16.90.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.90.1
R1(dhcp-config)#dns-server 172.16.90.1
R1(dhcp-config)#exit
R1(config)#DO WR
```

Рисунок 3.19 – Налаштування DHCP-сервера на маршрутизаторі

DHCP (Dynamic Host Configuration Protocol) — це протокол мережі, який автоматизує процес надання пристроям у локальній мережі IP-адрес і інших параметрів мережі. DHCP усуває необхідність призначати IP-адреси кожного пристрою вручну, що значно спрощує управління налаштуваннями мережі.

Після підключення пристрою до мережі він надсилає запит на отримання IP-адреси. Після отримання цього запиту DHCP-сервер виділяє вільну IP-адресу з визначеного діапазону, а потім передає її пристрою.

Який алгоритм отримання IP-адреси:

- DISCOVER: клієнт надсилає запит на виявлення DHCP-сервера;
- OFFER: DHCP-сервер відповідає IP-адресою та іншими параметрами, такі як маски підмережі, шлюзи та DNS;
- REQUEST: Клієнт схвалює пропозицію та подає запит на підтвердження;
- ACK: Налаштування підтверджує DHCP-сервер, і клієнт може використовувати виділену IP-адресу.

Наступним кроком налаштуємо NAT. Для цього потрібно зробити налаштування всередині самої EVE-NG (рис. 3.20):

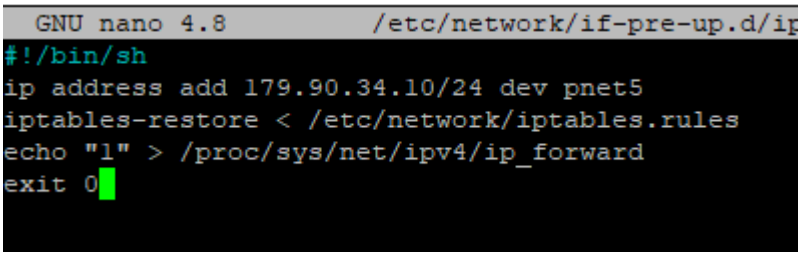

Рисунок 3.20 – Налаштування NAT всередині EVE-NG

Далі налаштовуємо NAT на маршрутизаторі (рис. 3.21):

```
Rl(config)#int e0/1
Rl(config-if)#no sh
Rl(config-if)#
*Nov 13 23:38:04.118: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*Nov 13 23:38:05.118: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
Rl(config-if)#ip add 179.90.34.9 255.255.255.0
Rl(config-if)#no sh
Rl(config-if)#ip route 0.0.0.0 0.0.0.0 179.90.34.9
%Invalid next hop address (it's this router)
Rl(config)#ip route 0.0.0.0 0.0.0.0 179.90.34.10
Rl(config)#ip nat outside
% Incomplete command.

Rl(config)#int e0/1
Rl(config-if)#ip nat out
Rl(config-if)#ip nat outside
Rl(config-if)#ip nat outside
*Nov 13 23:43:11.247: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, chan
ged state to up
Rl(config-if)#int e0/0.10
Rl(config-subif)#ip nat inside
Rl(config-subif)#int e0/0.20
Rl(config-subif)#ip nat inside
Rl(config-subif)#int e0/0.30
Rl(config-subif)#ip nat inside
Rl(config-subif)#int e0/0.40
Rl(config-subif)#ip nat inside
Rl(config-subif)#int e0/0.50
Rl(config-subif)#ip nat inside
Rl(config-subif)#int e0/0.60
Rl(config-subif)#ip nat inside
Rl(config-subif)#int e0/0.70
Rl(config-subif)#ip nat inside
Rl(config-subif)#int e0/0.80
Rl(config-subif)#ip nat inside
Rl(config-subif)#int e0/0.90
Rl(config-subif)#ip nat inside
Rl(config-subif)#exit
Rl(config)#ip access-list standa
Rl(config)#ip access-list standard NAT
Rl(config-std-nacl)#permit 172.16.10.0 0.0.0.255
Rl(config-std-nacl)#permit 172.16.20.0 0.0.0.255
Rl(config-std-nacl)#permit 172.16.30.0 0.0.0.255
Rl(config-std-nacl)#permit 172.16.40.0 0.0.0.255
Rl(config-std-nacl)#permit 172.16.50.0 0.0.0.255
Rl(config-std-nacl)#permit 172.16.60.0 0.0.0.255
Rl(config-std-nacl)#permit 172.16.70.0 0.0.0.255
Rl(config-std-nacl)#permit 172.16.80.0 0.0.0.255
Rl(config-std-nacl)#permit 172.16.90.0 0.0.0.255
Rl(config-std-nacl)#ip nat inside source list NAT interface e0/1 overload
Rl(config)#
```

Рисунок 3.21 – Налаштування NAT

NAT (Network Address Translation) - це технологія, що дає змогу перетворювати приватні IP-адреси пристроїв локальної мережі на публічну IP-адресу, з якою вони виходять в інтернет. Це дає змогу кільком пристроям використовувати одну зовнішню IP-адресу для доступу в мережу і допомагає економити IPv4-адреси.

3.4 Налаштування кінцевих пристроїв

Для початку налаштовується роль Active Directory на сервері Windows Server 2019 (рис. 3.22):

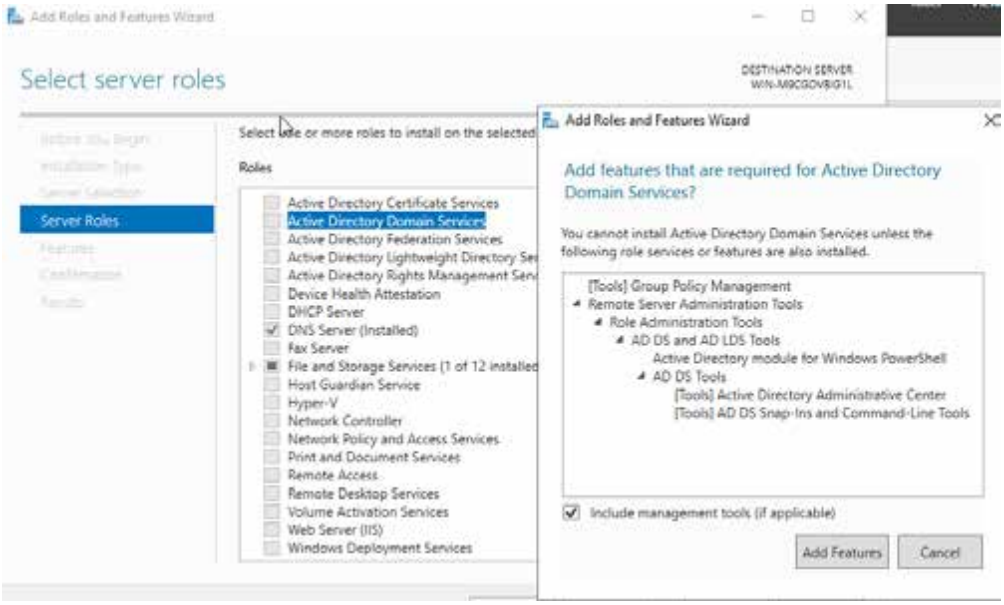

Рисунок 3.22 – Розгортання ролі Active Directory

Active Directory (AD) — це ієрархічна служба каталогу, розроблена Microsoft. У доменному середовищі Windows він використовується для організації та централізованого управління різними типами об’єктів, таких як комп’ютери, користувачі, сервери та принтери. В мережах Windows AD є основним компонентом управління та аутентифікації. Активна директорія тісно пов’язана з багатьма службами та додатками Microsoft, такими як DNS, DHCP і поштова служба Exchange Server. На відміну від workgroup, де на кожному комп’ютері зберігається власна база користувачів, користувач може увійти під своїм обліковим записом і паролем на будь-який комп’ютер у домені AD, оскільки всі облікові записи користувача зберігаються в одній базі AD.

AD складається з ієрархічних структур. Архітектура AD складається з наступних компонентів:

- Ліс AD (forest) - найвищий рівень ієрархії Active Directory. Він являє собою набір пов'язаних доменів, які поділяють загальну схему, структуру і глобальний каталог
- Домен - окрема область всередині лісу AD, зі своєю межею безпеки та реплікацією. Містить користувачів, комп'ютери, групи та інші об'єкти.
- Організаційна одиниця (OU) - контейнери всередині домену для логічного групування об'єктів (аналог - папки на диску). OU є точкою призначення GPO та делегування повноважень.
- Для встановлення домену Active Directory потрібно встановити роль Active Directory Domain Services (ADDS) на комп'ютері з Windows Server. Такий сервер називається контролер домену Active Directory (DC). У домені може бути один або кілька контролерів домену, залежно від потреб і розміру домену. Контролери домену виконують аутентифікацію користувачів і обслуговують запити на доступ до ресурсів мережі (використовується як logon server);
- На контролері домену зберігається база Active Directory (NTDS.DIT). Кожен контролер домену зберігає свою копію бази AD і реплікує нові/змінені даний з іншим DC.
- Сайт AD - об'єкти AD, що являють собою одну або кілька фізичних IP підмереж, пов'язаних швидкими каналами. Зазвичай сайти AD відображають фізичні географічні або логічні кордони у вашій корпоративній мережі. Клієнти виконують аутентифікацію, отримують політики з контролерів домену у своїх сайтах. У кожному сайті може бути один або кілька контролерів домену. Між сайтами можна налаштувати інтервали реплікації для зменшення навантаження на WAN канали.

- Global Catalog (GC) - ця роль може бути призначена будь-якому контролеру домену. Такий DC зберігатиме коротку інформацію про весь ліс і використовуватиметься для виконання пошуку й аутентифікації в різних доменах;
- Групові політики (GPO) - дають змогу адміністраторам налаштовувати параметри комп'ютерів і користувачів у мережі з використанням централізованих політик;
- Схема AD - визначає структуру та можливі атрибути об'єктів в Active Directory.

У рамках даного проєкту система Active Directory є важливим компонентом управління доступом, надаючи користувачам централізовану платформу для авторизації та аутентифікації. Це програмне забезпечення дозволяє перевіряти облікові дані кожного користувача, захищаючи їх від несанкціонованого доступу. Крім того, він встановлює рівні доступу відповідно до ролей і повноважень кожного користувача. Active Directory спрощує управління користувачами, ресурсами та політиками безпеки завдяки інтеграції з корпоративною інфраструктурою.

У додаток до функцій аутентифікації Active Directory надає адміністраторам багато можливостей, включаючи центральне управління обліковими записами та конфігурацію групових політик, які автоматизують налаштування доступу та поведінку користувачів у мережі. Це не лише зменшує вплив людського фактору на процеси безпеки, але й покращує робочі процеси, зменшуючи час, необхідний для виконання рутинних операцій.

Крім того, система легко інтегрується з іншими сервісами, такими як, файлові сховища та програми, що дозволяє користувачам отримувати безшовний доступ до ресурсів, які вони потребують. Навіть у великих компаніях із розгалуженою інфраструктурою Active Directory залишається ефективним рішенням завдяки можливості масштабування. Це гарантує стабільне функціонування, зручність для користувачів і високий рівень захисту корпоративних даних.

Після встановлення прописуємо назву домену (рис. 3.23):

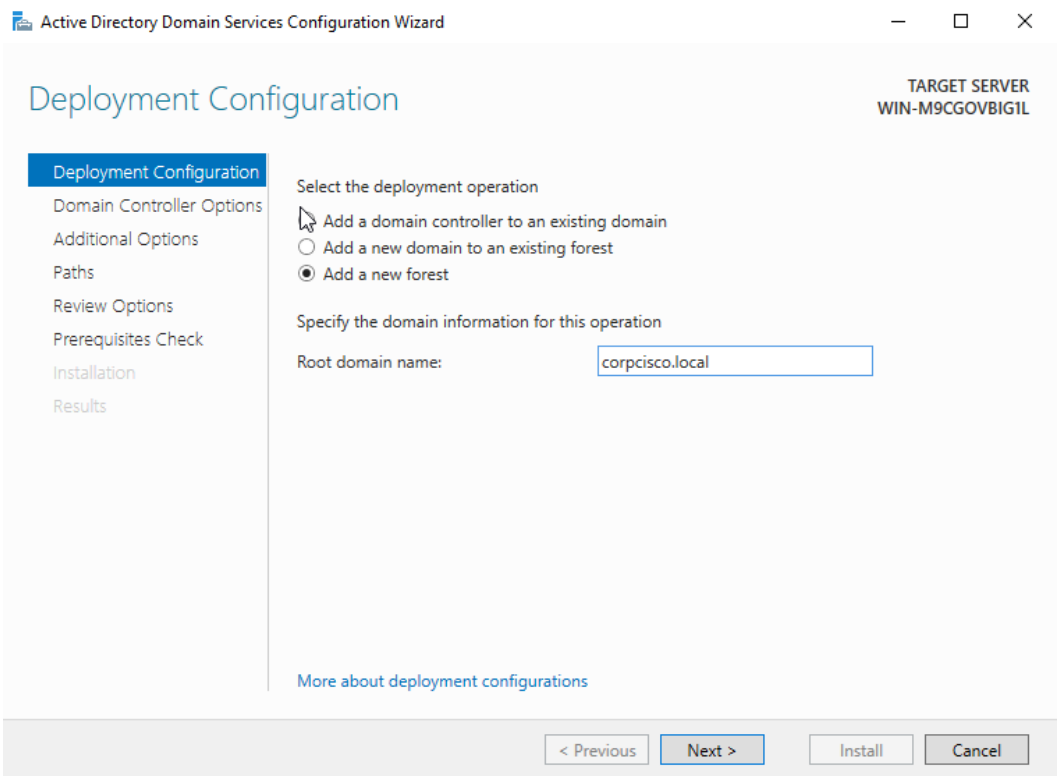

Рисунок 3.23 – Створення домену

Після встановлення ролі Active Directory на сервер Windows Server 2019 можна створити користувачів (рис. 3.24):

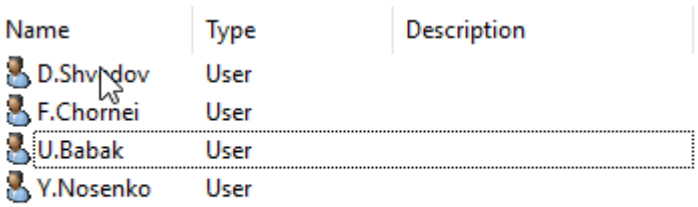

Рисунок 3.24 – Створення користувачів в Active Directory

Далі налаштуємо наш сервер ще як файлову шару, щоб можна було там зберігати файли (рис. 3.25):

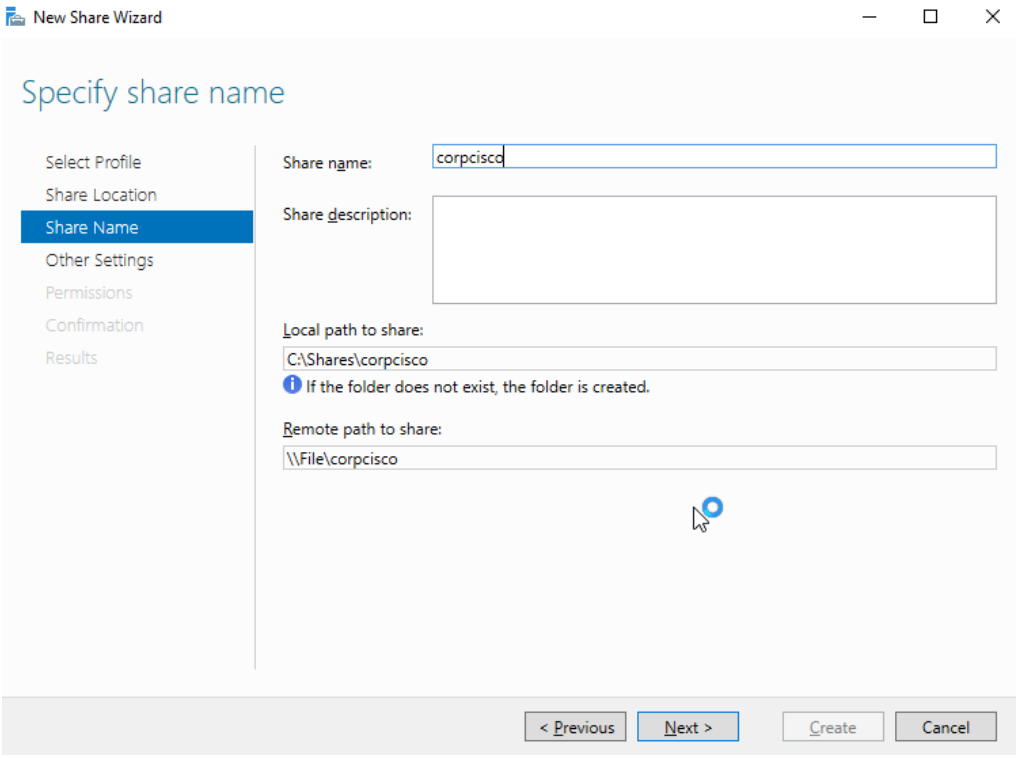

Рисунок 3.25 – Створення файлової шари

Файлові шари потрібні насамперед, для централізованого зберігання даних, а не на комп'ютерах користувачів гарантує, що важливі дані зберігаються навіть у разі несправності обладнання. Можливість звільнити місце на комп'ютерах користувачів і спростити роботу з великими файлами.

Далі можна створити групову політику на Active Directory, яка буде «мапити» мережеву папку користувачам. Для цього спочатку потрібно створити папку, і створити групову політику, для приєднання папки (рис.3.26):

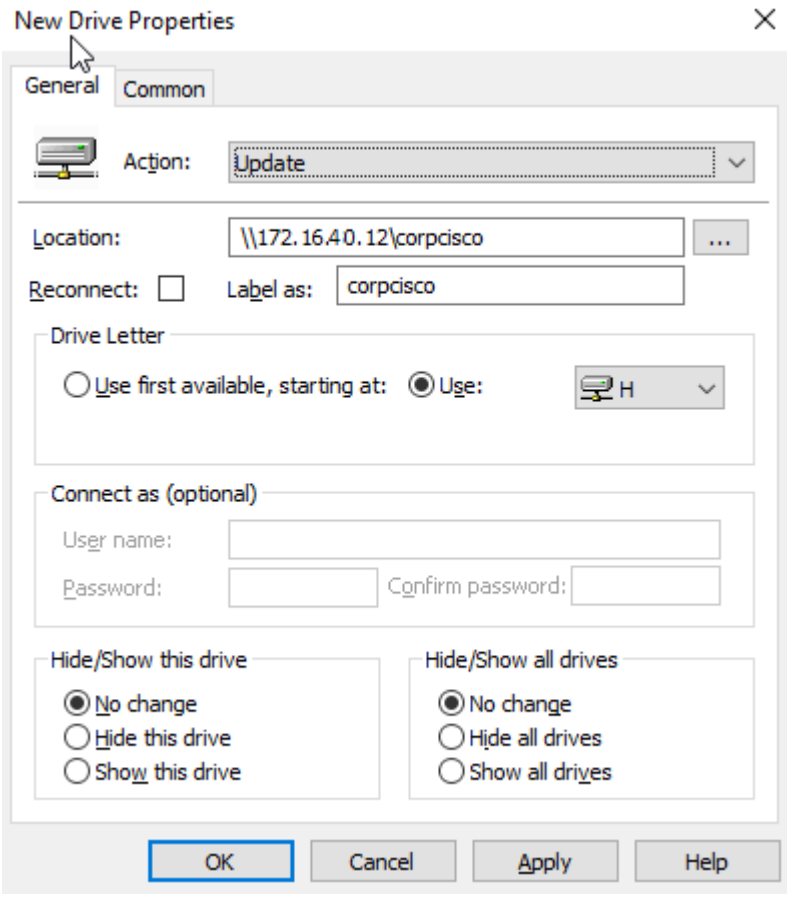

Рисунок 3.26 – Налаштування групової політики для приєднання папки користувачам

Наступним кроком є введення стаціонарних ПК в домен (рис. 3.27):

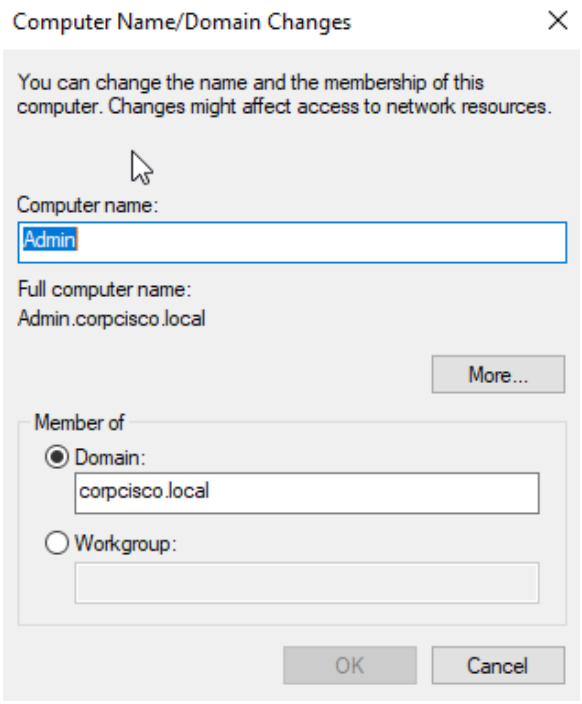

Рисунок 3.27 – Введення ПК в домен

Також потрібно зазначити, що для стаціонарних ПК потрібно закупити:

- 40 ліцензій Office 365 для роботи з файлами;
- 5 пакетів Adobe, 3 для дизайнерів та 2 для режисерів.

Ще однією задачею буде перевірити як відпрацьовує групова політика, стосовно приєднання мережевої папки (рис. 3.28):

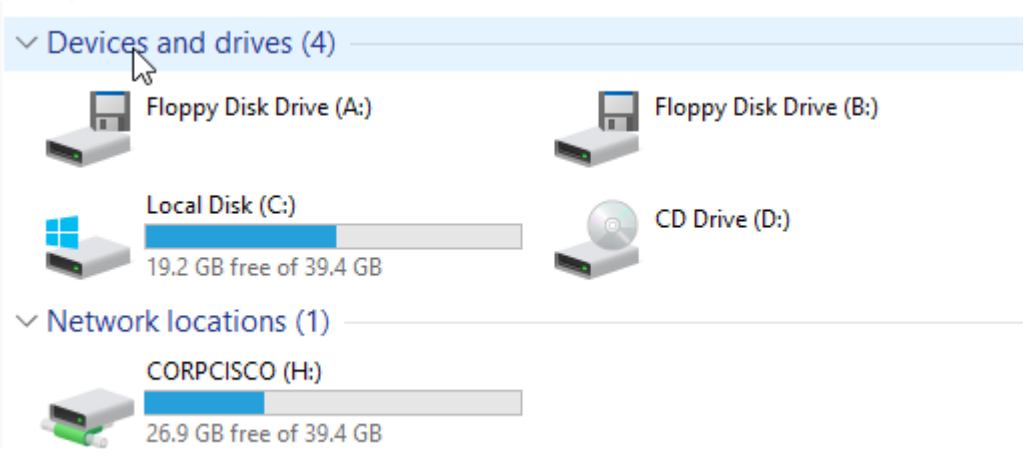

Рисунок 3.28 – Приєднання мережевої папки до доменного користувача

На цьому налаштування кінцевих пристроїв мережі завершено.

4 ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ОТРИМАНИХ РЕЗУЛЬТАТІВ

4.1 Огляд поточного стану мережі

Даний проєкт був запланований в якості розширення локальної мережі підприємства, на поточний стан система має наступну мережу (рис.4.1):

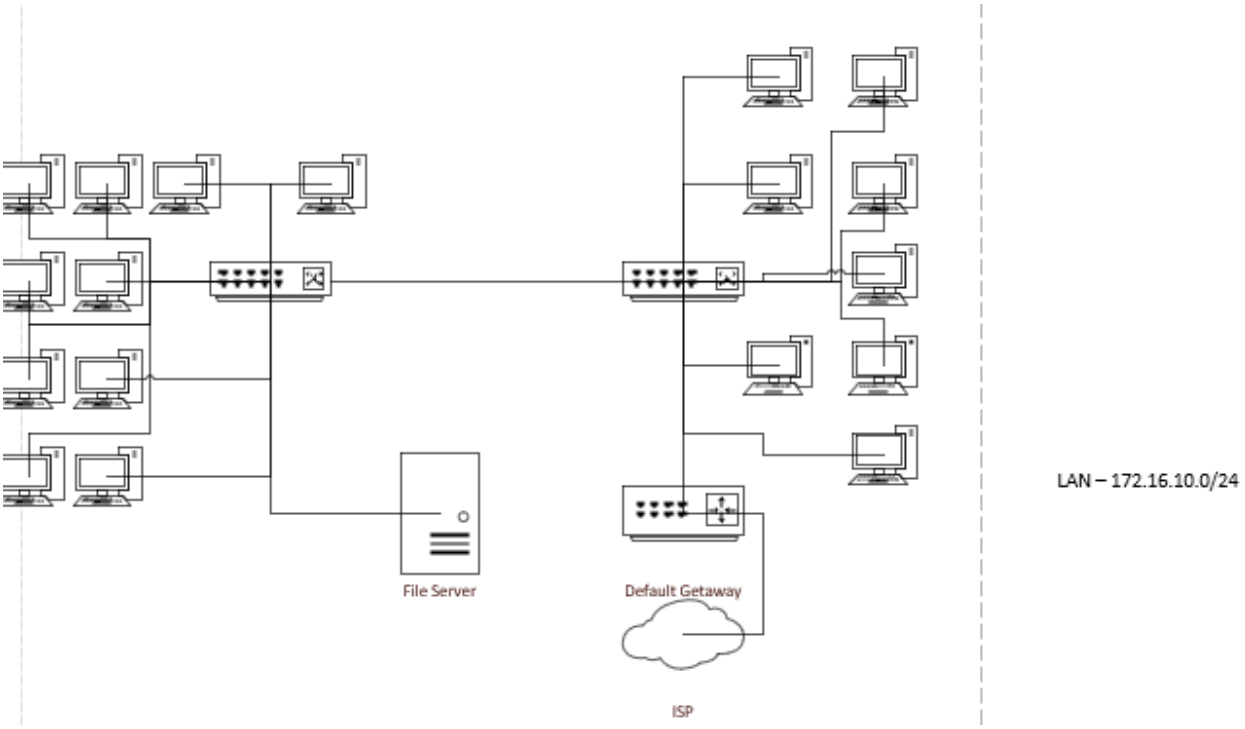

Рисунок 4.1 – Поточний стан мережі підприємства

Мережа підприємства складається з 18 ПК:

- Дирекція - 5 ПК;
- Бухгалтерський відділ – 2 ПК;
- Юридичний відділ – 1 ПК;
- ІТ-відділ – 1 ПК;
- Відділ реклами – 2 ПК;
- Відділ редакторів – 5 ПК;
- Дизайнерський відділ – 1 ПК;

- Відділ режисерів – 1 ПК.

Експлуатувалися комутатори D-Link DGS-1024D (рис. 4.2):

Рисунок 4.2 – Комутатор D-Link DGS-1024D

Некерований комутатор DGS-1024D з 24 портами 10/100/1000Base-T призначено для використання в мережах SOHO і підприємств малого та середнього бізнесу (SMB). Має наступні характеристики (табл. 4.1):

Таблиця 4.1 – Характеристики комутатора D-Link DGS-1024D

Порти	1 Гбіт/с
Тип комутатора	Некерований
Кількість портів RJ45	24
Додатково	Кріплення в стійку

В якості маршрутизатора використовувався маршрутизатор TP-Link TL-R470T+ (рис. 4.3):

Рисунок 4.3 – Маршрутизатор TP-Link TL-R470T+

Пристрій з балансуванням навантаження TL-R470T+ є високопродуктивним і стабільним, що дозволяє економити гроші, організовуючи мережу в таких місцях, як Інтернет-кафе та невеликі офіси. Вкладені в нього гроші швидко окупляться! Крім того, за допомогою цього пристрою можна уникнути витрат на мережеве обладнання. TL-R470T+ має три змінні порти WAN/LAN, що дозволяє йому мати до чотирьох портів WAN, що задовольняє різні вимоги до підключення до Інтернету через один пристрій. Ви будете користуватися стабільною мережею з широкими можливостями Ethernet-підключення завдяки надійному міжмережевому екрану, методам балансування навантаження та функції пріоритезації даних. Пристрій можна легко і просто налаштувати за допомогою веб-утиліти, яка проста та зрозуміла для будь-якого користувача.

Має наступні характеристики (табл. 4.2):

Таблиця 4.2 – Характеристики маршрутизатора TP-Link TL-R470T+

Тип маршрутизатора	Дротовий
Порти	100 Мбіт/с
Кількість портів RJ45	5
Форм-фактор	Настільний

Також мережа мала тільки файловий сервер, DNS-сервером виступав маршрутизатор.

4.2 Порівняння поточної та спроєктованої мережі

Найперше, на що варто звернути увагу, те, що локальна мережа була поділена на VLAN. Поділ мережі на віртуальні локальні мережі (VLAN) мають багато важливих переваг, що роблять їх важливою практикою для покращення продуктивності, безпеки та керованості мережі:

- VLAN дозволяє окремити кілька пристроїв одна від одної. Це обмежує можливість несанкціонованого доступу до даних по мережі та захищає дані, розділяючи їх за рівнями доступу. Наприклад, користувачам гостьової мережі може бути обмежений доступ, щоб вони не могли отримати доступ до ресурсів компанії. В даному проєкті розмежовано VLAN по орг.юнітам, що в майбутньому можна буде обмежити доступ одних від інших;
- Кожен VLAN має власний багатомовний домен. Це означає, що широкомовні пакети, які потребують ресурсів мережі, поширюються лише в межах конкретного VLAN, а не на всю мережу. Це покращує продуктивність і знижує навантаження на мережу;

- Піділ мережі VLAN дозволяє адміністраторам групувати та керувати пристроями незалежно від їхнього фізичного розташування. Наприклад, в проєкті відділ редакторів розбитий на декілька комутаторів;
- VLAN дає змогу застосувати пріоритетність трафіку для різних служб. Наприклад, можна виділити окремий VLAN для IP-телефонії та налаштувати пріоритети так, щоб трафік дзвінків передавався з мінімальними затримками. В проєкті це не застосовувалося, але може бути використано, у випадку необхідності;
- VLAN забезпечує гнучкість під час зміни мережевої структури: пристрої можна переміщати, не змінюючи фізичні під'єднання, тільки змінюючи їхню приналежність до VLAN. Це також дає змогу простіше масштабувати мережу під час додавання нових пристроїв або користувачів;
- Використання VLAN дозволяє створювати політики безпеки на рівні VLAN, а не на окремих пристроях, що полегшує управління правилами безпеки та полегшує виконання вимог щодо інформаційної безпеки.

Іншою характерною особливістю являється порівняння характеристик комутаторів (табл. 4.3):

Таблиця 4.3 – Порівняння комутаторів D-Link DGS-1024D та Cisco C9300-24P-A

	D-Link DGS-1024D	Cisco C9300-24P-A
Порти	1 Гбіт/с	24 порти Gigabit Ethernet (RJ45) з підтримкою PoE+; 4 порти для SFP uplink
Тип комутатора	Некерований	Керований, Layer 2, корпоративний рівень
Кількість портів RJ45	24	24 порти RJ45

Продовження таблиці 4.3

Додатково	Кріплення в стійку	Підтримка PoE+ (до 30 Вт на порт), можливість стекування до 8 комутаторів

Головною відмінністю в межах проєкту являється те, що D-Link DGS-1024D є некерованим комутатором, через що логічно неможливо розділити мережу на VLANs з такими комутаторами.

Другою не менш важливою відмінністю являється роздільна здатність портів комутаторів, D-Link DGS-1024D має роздільну здатність портів 1 1 Гбіт/с в той час як Cisco C9300-24P-A має порти 10 Гбіт/с.

Наступним етапом буде порівняння маршрутизаторів TP-Link TL-R470T+ та Cisco 2911-V/K9 (табл. 4.4)

Таблиця 4.4 – Порівняння маршрутизаторів TP-Link TL-R470T+ та Cisco 2911-V/K9

	TP-Link TL-R470T+	Cisco 2911-V/K9
Тип маршрутизатора	Дротовий	Дротовий
Порти	100 Мбіт/с	3 порти Gigabit Ethernet, 1 порт для консолі, 1 порт для AUX
Кількість портів RJ45	5	3 порти RJ45 (Ethernet)
Форм-фактор	Настільний	Стійковий

Першою і основною перевагою Cisco 2911-V/K9 над TP-Link TL-R470T+ є роздільна здатність портів. В той час як TP-Link TL-R470T+ має роздільну здатність портів 100 Мбіт/с, Cisco 2911-V/K9 має роздільну здатність Ethernet-портів 10 10 Гбіт/с.

Ще однією перевагою є те, що Cisco 2911-V/K9 можливо закріпити в стійку, в той час як TP-Link TL-R470T+ - ні.

Ще однією особливістю покращення, є наявність сервера з Active Directory, що дає змогу централізовано керувати мережею, що є дуже зручним інструментом.

Отже, було проведено порівняльну характеристику поточної та спроєктованої мереж, де визначено, що спроєктована мережа має ряд переваг.

ВИСНОВКИ

Отже, в роботі «Дослідження комп'ютерної системи для телекомунікаційних технологій, реалізованої на основі засобів Cisco» було виконано наступні задачі.

Перший розділ було присвячено огляду та аналізу предметної області. Здійснено опис області застосування, проаналізовано мережні рішення, та постановлені завдання для розробки.

У другому розділі описано проєктування комп’ютерної системи на основі засобів Cisco. Було обрано активне мережевого обладнання, також були обрані кінцеві пристрої. Було спроєктовано логічну схему мережі.

У третьому розділі виконано реалізацію комп’ютерної системи. Налаштовано середовище для розробки, Налаштовано комутатори та маршрутизатор Cisco. Також налаштовано кінцеві пристрої.

В четвертому розділі була здійснена порівняльна характеристика отриманих результатів. Проведено огляд поточного стану мережі та проведено порівняння поточної та спроєктованої мережі, в ході якої виявилося, що спроєктована мережа має ряд переваг, як от поділення мережі на VLAN, адміністрування мережі за допомогою Active Directory та ін.

ПЕРЕЛІК ПОСИЛАНЬ

1. 8 Steps to Configure Your Network Switch - Cisco [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/how-to-setup-network-switch.html
2. How to configure Cisco switch in 11 steps| ManageEngine Network Configuration Manager [Електронний ресурс] – Режим доступу: https://www.manageengine.com/network-configuration-manager/configure-cisco-switch.html
3. Basic Router Configuration – Cisco [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/routers/access/800M/software/800MSCG/routconf.html
4. How to Configure a Cisco Router in 10 Steps - PyNet Labs [Електронний ресурс] – Режим доступу: https://www.pynetlabs.com/how-do-i-configure-a-cisco-router/
5. Configure DHCP Server Cisco | ManageEngine [Електронний ресурс] – Режим доступу: https://www.manageengine.com/network-configuration-manager/configlets/configure-dhcp-server-cisco.html
6. How to configure VLAN and inter-VLAN Routing in Packet Tracer | by Madan Adhikari | Medium [Електронний ресурс] – Режим доступу: https://medium.com/@minwork/how-to-configure-vlan-and-inter-vlan-routing-in-packet-tracer-427e7fdf6bb5
7. Installing and Configuring Active Directory – Windows Server 2016 · ReadAndExecute [Електронний ресурс] – Режим доступу: https://www.readandexecute.com/how-to/server-2016/active-directory/how-to-server-2016installing-active-directory-server-2016/
8. Windows Server 2016 : File Server : Install : Server World [Електронний ресурс] – Режим доступу: https://www.server-world.info/en/note?os=Windows_Server_2016&p=smb&f=3

9. Ознайомтеся з логічною мережевою схемою та її прикладами [Електронний ресурс] – Режим доступу: https://www.mindonmap.com/uk/blog/logical-network-diagram/
10. SYS-6029P-TR - Сервер Supermicro SYS-6029P-TR купити в Києві, Дніпрі по кращій ціні! EServer [Електронний ресурс] – Режим доступу: https://e-server.com.ua/uk/aktivne-obladnannja/serveri/serveri-stijkovi-rack/server-supermicro-sys-6029p-tr-detail
11. Офісний ПК PowerUp #41 Core i5 6400/8 GB/SSD 240 GB/Int Video [Електронний ресурс] – Режим доступу: https://powerup.ua/ofysnyi-pk-powerup-41-core-i5-6500-8-gb-ssd-240-gb-int-video/?gad_source=1&gclid=Cj0KCQiA0MG5BhD1ARIsAEcZtwQY8dVM3xDtj7AaQTI1aglyEz6FxlNiXaKT4wX1wgtn6e98PEXH7UgaArkKEALw_wcB
12. DGS-1024D - Комутатор D-Link DGS-1024D купити в Києві, Дніпрі по кращій ціні! EServer [Електронний ресурс] – Режим доступу: https://e-server.com.ua/uk/aktivne-obladnannja/komutatori/nekerovani-komutatori/komutator-d-link-dgs-1024d-detail
13. TL-R470T+ - Мультисервісний маршрутизатор TP-Link TL-R470T+ купити в Києві, Дніпрі по кращій ціні! EServer [Електронний ресурс] – Режим доступу: https://e-server.com.ua/uk/aktivne-obladnannja/marshrutizatori/multiservisnij-marshrutizator-tp-link-tl-r470t-1xfe-lan-3xfe-lan-wan-1xfe-wan-detail?srsltid=AfmBOor6Jv0wjy7dpt6bjaNdrqVjcYrlwQeQ3Jq9-es5SvSXZEWChUGO
14. Коммутатор Cisco C9300-24P-A [Електронний ресурс] – Режим доступу: https://xn--h1aemkx.com.ua/switch/cisco-catalyst-9300/kommutator-cisco-c9300-24p-a
15. Маршрутизатор Cisco 2911-V/K9 [Електронний ресурс] – Режим доступу: https://xn--h1aemkx.com.ua/router/cisco-2900-series/marshrutizator-cisco-2911-v-k9