Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи ступеня бакалавра
(бакалавра, спеціаліста, магістра)

студента Солдатов Ярослав Олександрович
(ПІБ)

академічної групи 123-18ск-1
(шифр)

спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

на тему «Комп'ютерна система фітнес клубу «Спортлайф» з розробкою підсистеми збору поточної конфігурації з пристрою Cisco IOS-XE»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	ас. Панферова Я.В.			
розділів:				
апаратний розділ	доц. Ткаченко С.М.			
розрахунок мережі	ас. Панферова Я.В.			
програмне забезпечення	ас. Бешта Л.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2021

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій та
комп'ютерної інженерії
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

« » _____ 2021 року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студента Солдатов Я.О. **академічної групи** 123-18ск-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

на тему «Комп'ютерна система фітнес клубу «Спортлайф» з розробкою підсистеми збору поточної конфігурації з пристрою Cisco IOS-XE» затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.2021 № 317-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати завдання, конкретизувати предмет та мету роботи	18.05.2021
Технічні вимоги до комп'ютерної системи	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до розробки комп'ютерної системи	25.05.2021
Спеціальна частина	Розв'язати завдання з розробки комп'ютерної системи фітнес клубу «Спортлайф» з розробкою підсистеми збору поточної конфігурації з пристрою Cisco IOS-XE в репозиторії GitHub	04.06.2021

Завдання видано _____ ас. Панферова Я.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі 19.04.2021

Дата подання до екзаменаційної комісії 17.06.2021

Прийнято до виконання _____ Солдатов Я.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 59 с., 16 рис., 7 табл., 1 додатку, 10 джерел.

Об’єкт розробки: корпоративна мережа фітнес клубу «Sport Life»

Мета кваліфікаційної роботи: створення комп’ютерної системи фітнес клубу «Sport Life» з розробкою підсистеми збору поточної конфігурації з пристрою Cisco IOS-XE та збереження у репозиторії GitHub.

Спеціальна частина містить наступні підрозділи: розробка апаратної частини, де представлене обґрунтування вибору топології та технологій, зроблено вибір технічних засобів, розроблена структурна схема та можливості панелі управління Meraki Dashboard.

В розділі «Розробка комп’ютерної системи та перевірка її налаштувань» отримані дані від точок доступу Meraki інструментом API. Розроблена схема мережі реалізована у вигляді моделі на базі симулятора Cisco Packet Tracer і перевірена її робота.

MERAKI, API, CISCO, МЕРЕЖА, ФІТНЕС-КЛУБ, GIT, NETMIKO

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ і ТЕРМІНІВ

КС − комп’ютерна система

СКВ − система контролю версіями

ЛОМ − локальна обчислювальна мережа

API – прикладни́й програ́мний інтерфе́йс

VLSM – маски підмережі змінної довжини (англ. Variable Length Subnet Mask);

DHCP – протокол динамічного налаштування вузла (англ. Dynamic Host Configuration Protocol);

ВСТУП

В наш час не можливо уявити будь-яке підприємство без телекомунікаційних та інформаційних мереж. Досить швидко розвилася сфера надання послуг, тому мережі що забезпечують передачу даних та безперервність їх роботи є пріоритетною вимогою. Тому на сам перед слід зосередитись на підтримці нових сервісів, пристроїв і користувачів, а головне надійний захист від сучасних кіберзагроз. Не є винятком і мережа фітнес-клубів “Sport Life”.

Актуальність даної теми полягає в впровадженні досить гнучкої системи управління інфраструктурою мережі компанії, а саме введення певних даних що будуть включати в собі: хто, коли, куди заходив і кількість переданих даних.

Для виконання поставленого завдання існують мережеві рішення, також їх набори, які керуються через інтернет та забезпечують єдине джерело управління інфраструктурою і пристроями. Досить добрим рішенням будуть технології компанії Meraki, які здатні забезпечувати Wi-Fi, комутацію, безпеку та управління мережею за допомогою мобільних з використанням центральної хмарної платформи. Завдяки цієї платформи розширюються можливості IT-відділів надаючи їм здатність швидко та ефективно реагувати на зміни та оперативно вирішувати поставлені завдання.

Метою роботи є надання високоякісних послуг клієнтам фітнес-клубу “Sport Life” за рахунок побудови сучасної та надійної комп’ютерної системи.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАДАЧІ

1.1 Характеристика галузі та умов застосування системи, що проектується

Фітнес клуби – місця які включають в себе різні спортивні та тренажерні зали для підтримання та покращення фізичної форми осіб що відвідують їх за відповідну плату відповідно до вибраного тарифу.

«Спортлайф» - мережа фітнес-клубів що функціонує на даний момент. Діяльність компанії спрямована на створення глобальної мережі відповідних залів що будуть базуватися на світових стандартах. На сьогоднішній день мережа володіє досить великою кількістю фітнес-клубів, магазинів як спортивного одягу так відповідного спорядження, а також соляріями по всьому світі. Згідно з офіційними даними по Україні відкрито понад 65 фітнес-клубів, але це ще не кінець, так як розвиток та розростання мережі не зупинився. Для підвищення комфорту клієнтів, а також підвищення відвідування мережі, кожен клуб повинен забезпечуватися обчислювальною локальною мережею для забезпечення кожного відвідувача безкоштовним доступом до Wi-Fi.

Кожен з фітнес-клубів є широко профільним, що поділяються на такі зони: кардіо, вільних ваг, хамерів, тренажерів, стрейчінгу, аква та лаунж зони. Також заняття проводяться відповідно до вікових груп відвідувачів.

1.2 Організаційна структура КС

Фітнес клуб включає в себе ряд технічних та адміністративних відділів. Окремо слід виділити тренажерний зал, басейн, дитячий клуб та групові програми. В цих відділах працюють інструктори, які проводять персональні тренування та групові заняття і підпорядковуються менеджерам даних підрозділів.

До адміністративних відділів відноситься: відділ сервісу, відділ продажів, відділ служби безпеки, центральна рецепція клубу

(адміністрація), дирекція та бухгалтерія. До технічних відноситься: відділ технічної експлуатації та відділ клінінгу.

Відділ сервісу працює з діючими членами клубу, основна задача відділу – вирішення конфліктних ситуацій, робота зі скаргами і побажанням клієнтів, продовження абонементів діючих клієнтів, інформування клієнтів про актуальні акції. У відділі працюють сервіс-менеджери, які підпорядковані старшому сервіс-менеджеру.

Відділ продажів працює з потенційними клієнтами, його основна задача – продаж абонементів новим клієнтам. У відділі працюють сейл-менеджери (менеджери з продажів), які підпорядковані старшому сейл-менеджеру.

Служба безпеки клубу контролює роботу всіх підрозділів клубу, забезпечує порядок і безпеку клієнтів в клубі, фіксує факти порушень клубних правил. Співробітник служби безпеки підпорядковується старшому співробітнику зміни, а старший співробітник в свою чергу – начальнику служби безпеки.

Центральна рецепція клубу займається реєстрацією візиту клієнта до клубу, оформленням платних та безкоштовних послуг, забезпечує взаємодію всіх підрозділ між собою. Адміністратор центральної рецепції підпорядковується старшому адміністратору.

До дирекції відноситься фітнес-директор та його асистент, яким підпорядковані усі структурні підрозділи клубу, крім служби безпеки. Дирекція контролює роботу всіх структурних підрозділів, відповідає за матеріальне забезпечення клубу, виконання планів з надання послуг.

У відділі технічної експлуатації працюють інженери з експлуатації, основна задача, яких – підтримання належного функціонування усіх систем та обладнання клубу. Інженери з експлуатації підпорядковані управляючому.

Співробітники відділу клінінгу забезпечують підтримання чистоти та забезпечення дотримання санітарно-гігієнічних норм на території клубу. Співробітники клінінгу підпорядковані клінінг-менджеру.

Організаційна структура фітнес клубу «Спортлайф» наведена на рисунку 1.1.

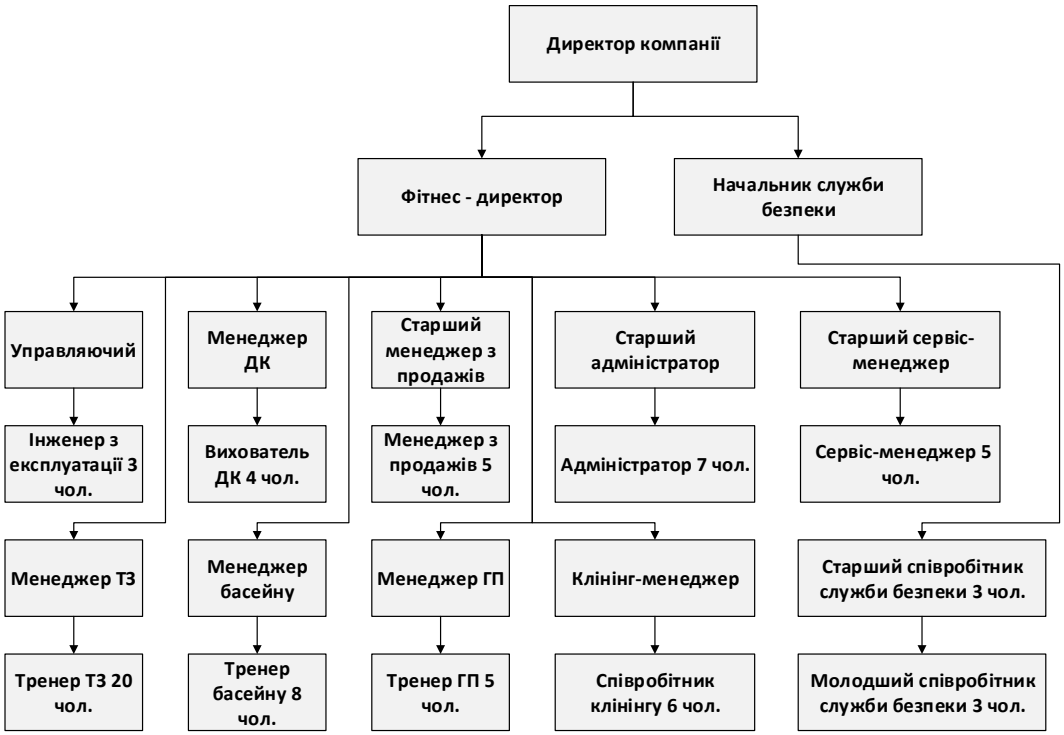

Схема організаційної структури фітнес клубу «Спортлайф»

1.3 Організація обчислювальної мережі КС «Спортлайф»

В мережі фітнес-центрів «Спортлайф» впроваджено архітектуру Meraki. Обладнання повинно розміщуватися в серверній, а пристрої Meraki повинні підключитися до хмари з використанням шифрування SSL.

Дане рішення досить сильно спрощує роботу адміністраторів, оскільки воно є єдиною точкою управління, консолідуючи всі засоби автоматизації та моніторингу. Також якщо зв’язок з хмарою буде втрачено, робота мережі не зупиниться.

Оскільки використовується шифрований канал зв’язку з хмарою, то безпека гарантується. Також для підключення використовується подвійна аутентифікація.

Дана архітектура виключає необхідність використання апаратних контролерів і комплексів управління.

Комутатори ядра серії Catalyst 3650 постачаються з операційною системою Cisco IOS-XE. Cisco IOS XE − це оновлений варіант IOS, що запускається в 64х бітовому віртуалізованому середовищі, де сама ОС, драйвери, додаткові програмні компоненти та модулі працюють в окремих один від одного процесах. Це відчутно підвищує відмовостійкість і спрощує обслуговування даної ОС.

1.4 Infrastructure as Code

Інфраструктура − це ресурси, які потрібні для підтримки коду. Водночас дехто може уявити серверні стійки, світчі та зміїне кубло кабелів... Але це вчорашній день. Сьогодні 99% проєктів живе в «хмарах». Тобто ресурси — це віртуальні машини, контейнери, load balancers.

Отже, усі хмарні ресурси − це інше програмне забезпечення, яке виконується на комп’ютерах нашого хмарного провайдера.

Infrastructure as Code − це спосіб постачання та керування обчислювальними та мережевими ресурсами методом їх опису у вигляді програмного коду, на відміну від налаштовування необхідного обладнання власноруч чи з допомогою інтерактивних інструментів [3].

1.5 Завдання і мета роботи

Завдання даної кваліфікаційної роботи – створення комп’ютерної системи фітнес клубу “ Спортлайф” та автоматизація збору та збереження поточної конфігурації мережного обладнання в репозиторії GitHub.

Мета даної кваліфікаційної роботи – підвищення ефективності КС за допомогою розроблення, покрашення та збереження підсистеми збору конфігурацій з заданого пристрою, а саме Cisco IOS-XE в репозиторії GitHub.

Реалізація даного проекту забезпечить підвищення ефективності збору та збереження конфігурацій, що в свою чергу покраще процеси роботи комп’ютерної системи та більш реалізує політику роботи з клієнтами.

Для досягнення поставленої мети було сформовано такі завдання:

– обґрунтувати вибір топології мережі і технологій;

– розробити специфікацію апаратних засобів КС;

– розробити структурну схему комплексу технічних засобів КС;

– побудувати модель в Packet Tracer та перевірити її роботу.

– дослідити можливості репозиторії Git;

– робити скрипт для резервного копіювання поточної конфігурації комутаторів ядра Catalyst 3650 в репозиторії Git з відслідковуванням версій.

2 ТЕХНІЧНІ ВИМОГИ ДО КОМП‘ЮТЕРНОЇ СИСТЕМИ

2.1 Вимоги до системи в цілому

2.1.1 Вимоги до структури і функціонування системи

Технологічний комплекс даних підрозділів складається з центрального серверу, на якому наявна клієнтська база клубу, автоматизованих робочих місць менеджерів та адміністраторів, а також мережевого обладнання стандарту Ethernet. Робочі місця співробітників оснащені персональними комп’ютерами та зчитувачами клієнтських карток, які підключені до локальної комп’ютерної мережі фітнес клубу і мають доступ до мережі Інтернет. Менеджери з продажів додають нових клієнтів до бази даних, а сервіс-менеджери та адміністратори використовують існуючу базу для роботи.

Комутатори ядра і контролер бездротової мережі Meraki будуть розташовуватися в серверному приміщенні, Всі бездротові точки повинні використовувати технологію PoE+. Комутатори ядра Catalyst 3650 розраховані на підключення серверного обладнання зі швидкістю не менше 10Гбіт/с. Всі комутатори доступу повинні підтримувати PoE+ на всіх портах для можливості гнучкої комутації і підключення як комп'ютерів, так і точок доступу. Всі комутатори повинні підтримувати технології стекування, для спрощення конфігурації і підвищення надійності мережі. Всі комутатори повинні мати резервовані блоки живлення. Кожна комутаційна кімната повинна підключатися до серверної двома сполуками зі швидкістю 10Гбіт / с кожен.

2.1.2 Вимоги до складу технічних засобів системи

Бездротова мережа побудована на продуктах Cisco з управлінням з хмарної платформи Meraki .

Вимоги до хмарно-керованих точок доступу:

– самоконфігурація, розгортання за принципом «включай і працюй»;

– протоколи 802.11ac і 802.11n MIMO з підтримкою до трьох просторових потоків для голосу і відео;

– інтегрована безпека підприємства і гостьовий доступ;

– виділене радіо для безпеки і оптимізації RF з інтегрованим аналізом спектра;

– інтегрована система виявлення і запобігання вторгнень (WIDS/WIPS);

– самонавчальний механізм аналізу трафіку з урахуванням додатків;

– гнучкий механізм групової політики для створення і застосування політик з урахуванням додатків по мережі, типу пристрою і кінцевого користувачева;

– адміністрування на основі ролей і автоматичні, заплановані оновлення прошивки, що надаються через Інтернет;

– попередженнями на електронну пошту чи текстові повідомлення про збої живлення, простоях або зміни конфігурації;

– привабливий дизайн і компактні розміри.

Технічне забезпечення системи повинно максимально і найбільш ефективним чином використовувати існуючі технічні засоби.

Активне мережеве обладнання комп'ютерної мережі забезпечує:

– високошвидкісний обмін даними між розеткою підключення обладнання і/або серверами за технологією Ethernet (Fast Ethernet, Gigabit Ethernet) та Wi-Fi 802.11n частотою 2,4 та 5 ГГц;

– ефективну роботу всіх складових елементів локальної обчислювальної мережі ЛОМ (АРМ, серверів, принтерів і т.п.).

2.1.3 Вимоги до пропускної здатності інформаційних каналів

Повинно використовувати віту пару категорії 5е, який нараховує чотири пари, використовується при конструюванні мережі 100/1000 Мбіт/с. Коли взаємодіють дві пар, швидкість передачі - 100Мбіт/с, якщо використовують всі чотири пари – 1000Мбіт/с. Частотна полоса 100 МГц.

Бездротова мережа забезпечувати пропускну здатність не менше 600 Мбіт/с.

2.1.4 Вимоги до надійності

Безперебійна робота серверного обладнання (24х7х365). У разі повного відключення електроенергії система повинна функціонувати протягом 60 хв.

Безперебійна робота локальної мережі, комутаційних шаф, де знаходиться активне мережеве обладнання. У разі повного відключення електроенергії мережа повинна функціонувати протягом 30 хв.

2.1.5 Вимоги до ергономіки та технічної естетики

Елементи комп'ютерної мережі мають бути промарковані. Маркування має бути нанесено :

– на обох кінцях кабелю;

– на телекомунікаційних розетках;

– на комутаційних панелях;

Кожне автоматизоване робоче місце повинно складатися з інформаційної розетки RJ-45 в кількості 2 штуки.

Нумерація розеток наноситься на креслення розташування робочих місць. Кожен порт RJ-45 повинен бути промаркований номером кімнати і через «.» номером порту у кімнаті.

Зовнішній вигляд коробів та аксесуарів повинен гармоніювати з інтер'єром робочих місць.

2.1.6 Вимоги до захисту інформації від несанкціонованого доступу

Забезпечити можливість безпечного та захищеного віддаленого адміністрування через мережу Інтернет.

Забезпечити обмеження доступу до серверного обладнання з корпоративної мережі та мереж загального користування.

Забезпечити мережевий захист від вірусних атак, DDoS.

2.1.7 Вимоги до схоронності інформації при аваріях

Забезпечити резервне копіювання даних які підлягають довготривалому зберіганню (передбачити схему резервного копіювання в проекті).

2.1.8 Вимоги до захисту від впливу зовнішніх чинників

Всі кабельні з’єднання повинні знаходитися в кабель каналах для захисту від зовнішнього впливу.

2.1.9 Вимоги до патентної та ліцензійної чистоти

Рішення по створенню КС «Спортлайф» повинно відповідати вимогам по патентної чистоті згідно з чинним законодавством України і майнові права на надане програмне забезпечення визначаються відповідно до законодавства України.

2.1.10 Вимоги до стандартизації та уніфікації

Прі реалізації даного проекту повинні прийматися до керівництва діючі в Україні. .Обладнання має використовувати стандартні електричні стики, інтерфейси, технології та протоколи передачі даних. Технічні засоби системи, що підлягають обов'язковій сертифікації відповідно до чинного законодавства України, повинні мати відповідні сертифікати.

2.2 Вимоги до функцій, які виконує КС

Побудова єдиного інформаційного середовища фітнес-центру для забезпечення наступних функцій:

– управління мережним обладнанням з хмарної платформи Meraki;

– обчислювальними ресурсами для обробки інформаційних систем фітнес-клубу «Спортлайф»;

– ресурси системи зберігання даних для зберігання даних систем фітнес-клубу «Спортлайф»;

– інформаційними системами та користувачами загальними інфраструктурними сервісами (DHCP, DNS, друк і т.д.);

– інформаційних систем і користувачів службою каталогу;

– засобами віртуалізації серверів і надання послуг віртуалізації.

2.3 Вимоги до видів забезпечення

2.3.1 Вимоги до інформаційного забезпечення

В рамках будови КС «Спортлайф» вимоги до інформаційного забезпечення не пред’являлись.

2.3.2 Вимоги до лінгвистичного забезпечення

В рамках будови КС «Спортлайф» вимоги до інформаційного забезпечення не пред’являлись.

2.3.3 Вимоги до програмного забезпечення

Можливість резервного копіювання поточної робочої конфігурації мережних пристроїв в розподіленій системі контролю версій Git за запитом адміністратора системи.

Надати можливість багато поточного резервування.

Можливість відслідковування змінених блоків даних для зменшення часу резервного копіювання.

3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

3.1 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи

У фітнес клубі «Спортлайф» відповідно до його організаційної структури можна виділити 5 основних підмереж організації:

1) відділи роботи з клієнтами (далі LAN 1). Даний відділ виконує функції контролю за доступом, відео нагляд за дотриманням порядку та безпеки клієнтів клубу;

2) відділ служби безпеки та контроля доступу (далі LAN 2) – центральна рецепція, відділ продажів та відділ сервісу. Дані відділи тісно співпрацюють між собою і знаходяться поряд на вхідній групі клубу тому і будуть відноситись до однієї підмережі;

3) бухгалтерія (далі LAN 3);

4) офіс адміністрації клубу (далі LAN 4), знаходиться в службовій частині клубу. До нього входить дирекція клубу, менеджери басейну та тренажерного залу;

5) віддалена підмережа кураторів та дирекції (далі LAN 5), що знаходиться у місті Київ.

Для підмережі LAN 2 буде застосовано технологію агрегації каналів. Це пов'язано з тим, що у даній підмережі співпрацюють відділи, які займаються обслуговуванням клієнтів, де необхідне створення надійних каналів із забезпеченням високої пропускної здатності.

У підмережі LAN 4 будуть створені мережі VLAN. Це пов'язано з тим, що кількість робочих станцій різних відділів офісу невелика, і розділення на окремі підмережі декількох робочих станцій вимагає застосування додаткових маршрутизаторів, що є нераціональним. А використання VLAN дозволить на базі комутаторів розділити відділи офісу на окремі підмережі.

Для створення локальної комп’ютерної мережі фітнес клубу буде використано технологію Fast Ethernet. Обрана технологія забезпечує високу швидкість передачі даних (до 100 Мбіт/с), має високі показники надійності і щвидкодії, обладнання має відносно невисоку вартість.

Оскільки для ми вибрали архітектуру Meraki обладнання повинно розміщуватися в головному офісі, а пристрої повинні підключитися до хмари з використанням шифрування SSL. За допомогою панелі управління процес мережевого менеджменту в рази спрощується.

Дане рішення досить сильно спрощує роботу адміністраторів, оскільки воно є єдиною точкою управління, консолідуючи всі засоби автоматизації та моніторингу. Також якщо зв’язок з хмарою буде втрачено, робота мережі не зупиниться.

Оскільки використовується шифрований канал зв’язку з хмарою, то безпека гарантується. Також для підключення використовується подвійна аутентифікація.

Дана архітектура виключає необхідність використання апаратних контролерів і комплексів управління.

Для вибору структурної схеми потрібно враховувати всі поставлені перед системою вимоги та що б вона задовольняла кількісний склад технічних засобів. Також потрібно враховувати узгодження структури з топологічними особливостями об’єкту розробки и найголовніше, структура повинна бути доцільно продуктивною. Структурну схему комплексу технічних засобів комп’ютерної системи зображено на рисунку 3.1.

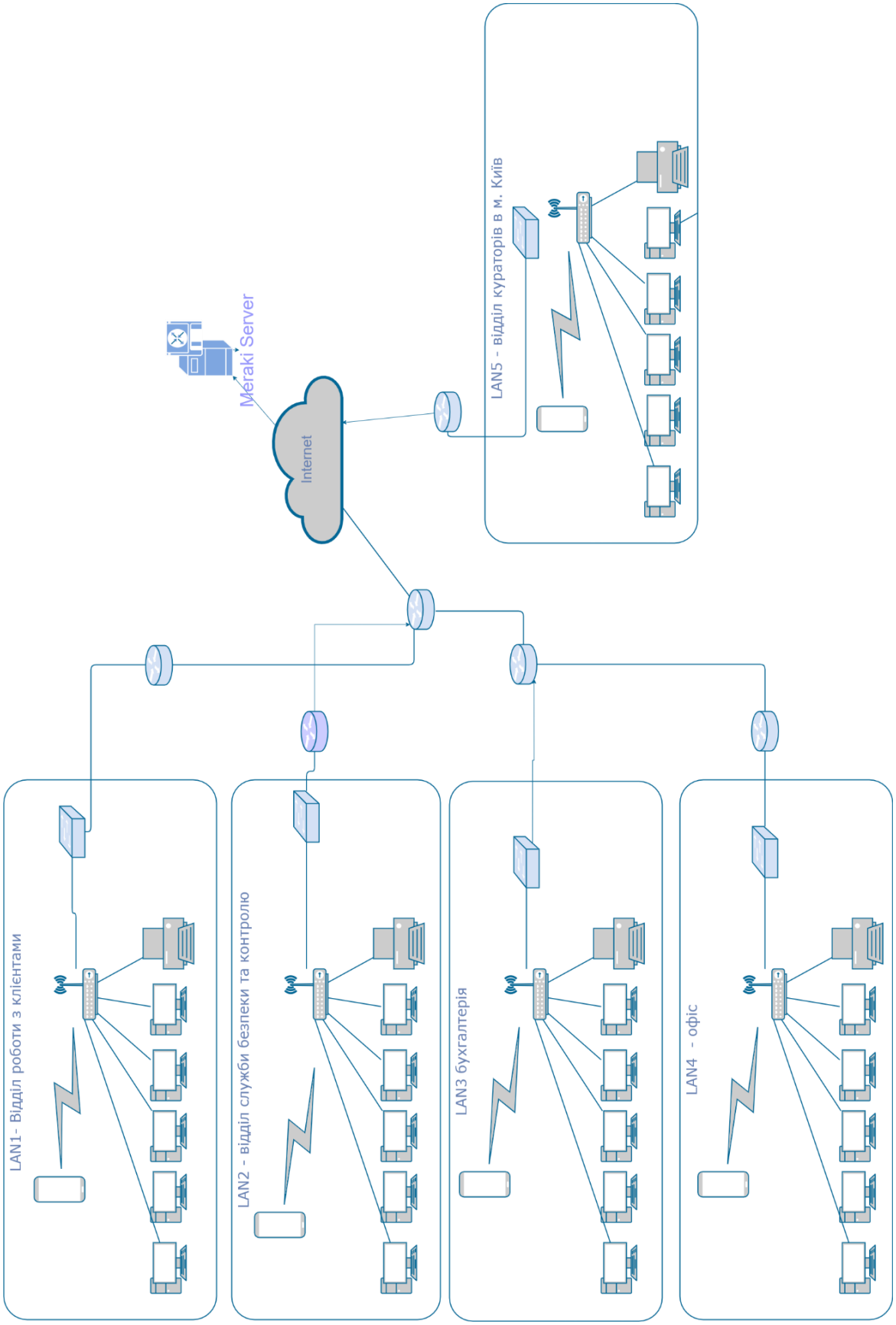

Рисунок 3.1 − Структурна схема комплексу технічних засобів системи

Компанія Cisco надає архітектуру Meraki з панеллю керування що значно підвищує продуктивність адміністрування і роботи мереж за допомогою хмарних збережень.

3.2 Розробка специфікацій апаратних засобів КС

Відповідно до поставлених вимог було обрано наступне обладнання:

– маршрутизатор Cisco 2911 – для реалізації маршрутизації між підмережами організації та реалізації доступу до мережі Інтернет (рис. 3.2;

– комутатор Cisco 3650-24 TT – для реалізації комутації в підмережах організаці (рис.3.3)ї;

– сервер Dell PowerEdge T30 – для організації DNS-серверу – сервер для трансляції імен сайтів в IP-адреси; TFTP-серверу – для зберігання конфігураційних файлів мережевого обладнання організації; HTTP-серверу – для реалізації сайту.

– Meraki MR34 для бездротового підключення (рис.3.4).

Рисунок 3.2 − Маршрутизатор Cisco 2911

Рисунок 3.3 − Комутатор Cisco 3650-24 TT

Рисунок 3.4 − Wi-Fi точка доступа Cisco Meraki MR34

В таблиці 3.1 надана специффікафія обраного обладання та його кількість.

Таблиця 3.1 – Специфікація апаратних засобів

Найменування обладнання	Характеристики	К-ть, шт.
Cisco 2911	Підтримувані стандарти – Ethernet, Fast Ethernet, Gigabit Ethernet; кількість слотів EHWIC – 4; пам’ять DDR2 ECC DRAM – 512 Мбайт; Compact Flash – 256 Мбайт; зовнішні слоти Flash-пам’яті USB 2.0 – 2; консольний порт USB – 1; вхідна напруга живлення - від 100 до 240 В ~; частота вхідної змінної напруги – 47 – 63 Гц; максимальна споживана потужність – 250 Вт.	7
Найменування обладнання	Характеристики	К-ть, шт.
Cisco 3650-24 TT	Кількість портів RJ-45 – 26; підтримувані стандарти Ethernet, Fast Ethernet – 24 порти, Gigabit Ethernet – 2 порти; максимальна пропускна здатність 10,1 Гбіт/с; об’єм пам’яті ОЗП – 64 Мб; об’єм флеш пам’яті – 32 Мб; Максимальне число записів таблиці MAC-адрес – 8192; Максимальна кількість VLAN – 64; Списки доступу – до 512; Вхідна напруга живлення - від 100 до 240 В ~; максимальна споживана потужність – 45 Вт.	9
Meraki MR34	3 радіо: 2,4 і 5 ГГц, дводіапазонні WIDS / WIPS 3-потік 802.11ac і 802.11n, до 1,75 Гбіт 1 × 100 / 1000Base-T Ethernet (RJ45) 48V DC 802.3at / 802.3af PoE 1 × DC power connector (5mm x 2.1mm, center positive	1
Dell PowerEdge T30	Процесор – чотирьох ядерний Intel Xeon Quad-Core E3-1225 v5 (3.3 - 3.7 ГГц); Об’єм пам’яті ОЗП – 8 Гб, Пам'ять HDD – 1 Тб; споживана потужність – до 300 Вт; підтримуваний стандарт комп’ютерних мереж – Gigabit Ethernet;	3

3.3 Розрахунок характеристик вихідного трафіку комп'ютерної мережі

Для проектованої комп'ютерної системи було розраховано основні характеристик для вихідного трафіку в найбільшому сегменті мережі підприємства за умови, що послугами одночасно користуються 100% користувачів.

Розраховано такі параметри як: коефіцієнт зайнятості обслуговуючого маршрутизатора, завантаження каналу передачі даних маршрутизатора, середня затримку кадру, середню довжину черги, середній час перебування пакета в черзі, пропускна здатність каналу.

Для розрахунку приймається модель ділянки мережі як модель СМО M/M/1 [8].

Проектні дані:

- кількість вузлів в найбільшій мережі: 115;
- середня інтенсивність трафіку: μ=105 (кадрів/с);
- середня довжина повідомлення: l=600 байт;
- вимоги до затримки передачі пакету – ≤5 мс.

Згідно кількості вузлів (115) для їх підключення на рівні розподілу обрано комутатор Cisco Catalyst 3750 серії. (1 шт.), на рівні доступу комутатор Cisco Catalyst 2960 24 10/100 (5 шт.).

Вихідний трафік пересилається на маршрутизатор в лінію з пропускною здатністю 100Мбіт/с.

Для того, щоб комутатор рівня розподілу не був перенасичений, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Розрахунок проведено з врахуванням того, що послугами одночасно користуються 100% користувачів. Середня інтенсивність трафіку μ=105 (кадрів/с), а середня довжина повідомлення – 600 байт.

Розрахунок пропускної здатності мережі на рівні доступу допускаючи, що послугами одночасно користуються 100% користувачів виконується за формулою 3.1.

$$P_{р.д}= \mu \times l \times n \times 8=105 \times 600 \times 24 \times 8= 12{,}1 \text{ (Мбіт/с)}, \quad (3.1)$$

де n – кількість портів в комутаторі рівня доступу.

Пропускна здатність мережі на рівні розподілу розраховується наступним чином. Так як до одного комутатора рівня розподілу підходять 4 комутатори рівня доступу, а загальна кількість користувачів дорівнює 115, то пропускна здатність мережі на рівні розподілу розраховується за формулою 3.2.

$$P_{р.р}= \mu \times l \times N \times 8=105 \times 600 \times 115 \times 8= 57{,}96 \text{ (Мбіт/с)}, \quad (3.2)$$

де N - кількість вузлів в найбільшій мережі.

Отримані при розрахунку результати не перевищують задані параметри мережі. Отже, перевантажень на обраному обладнанні не буде.

Комутатор рівня розподілу пересилає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 100Мбіт/с.

Загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{вих}=100\ 000\ 000/(600*8)=20834 \text{ пакетів/с};$$

Оскільки кожне джерело генерує в середньому 105 пакетів/с, то обмеження на приєднанням до комутатора рівня розподілу становить:

$$N=20834/105=198 \text{ джерел.}$$

Що задовольняє умовам мережі на 115 робочих станцій.

Кожна з 115 робочих станцій посилає потік заявок з інтенсивністю 105 кадрів/с. Інтенсивність вихідного трафіку від всіх користувачів розраховується за формулою 3.3.

$$\lambda = N \times \mu = 115 \times 105=12075 \text{ (пакетів/с)}; \quad (3.3)$$

Коефіцієнт затримки на рівні розподілу, тобто показник завантаженості вихідного каналу зв'язку, який впливає на час очікування в черзі розраховується за формулою 3.4.

$$\rho = \frac{\lambda}{\mu_{вих}} = \frac{9450}{20834} = 0{,}58; \quad (3.4)$$

Коефіцієнт зайнятості комутатора рівня розподілу розраховується за формулою 3.5.

$$r = \frac{\rho}{1-\rho} = \frac{0,58}{1-0,58} = 1,38 \quad (3.5)$$

Середня затримка кадру, пов’язана з чергою M/M/1,розраховується за формулою 3.6.

$$T = \frac{1}{(\mu-\lambda)} = \frac{1}{20834-12075} = 1,14 \text{ мкс}; \quad (3.6)$$

Середня довжина черги розраховується за формулою 3.7.

$$\mathcal{L}_{чер} = \frac{\rho^2}{1-\rho} = \frac{0,58^2}{1-0,58} = 0,8; \quad (3.7)$$

В даному випадку середня довжина черги визначає, що в системі на обслуговуванні менше 1 пакету, що свідчить про те, що система працює з великим запасом по продуктивності.

Середній час перебування пакета в черзі розраховується за формулою 3.8.

$$T_{чер} = \frac{\mathcal{L}_{чер}}{\lambda} = \frac{0,8}{12075} = 0,66 \text{ мкс}; \quad (3.8)$$

Це значення менше необхідного значення ≤5 мс, що задовольняє поставленим вимогам.

Пропускна здатність каналу розраховується за формулою 3.9.

$$b = \lambda \times l = 12075 * 600 * 8 = 57960000 \text{ біт/с} = 57,96 \text{ Мбіт/с}; \quad (3.9)$$

Що задовольняє пропускній здатності вихідного каналу в 100Мбіт/с.

4 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

4.1 Розробка моделі комп'ютерної системи

Для налаштування IP-адрес на кінцевих пристроях були використані можливості графічного інтерфейсу цих пристроїв, наданих можливостями системи. Налаштування маршрутизаторів та комутаторів виконувалось за допомогою командного рядка.

Відповідно до організаційної структури фітнес клубу та вимогам розташування пристроїв за допомогою програмного забезпечення Cisco Packet Tracer модель була розроблена мережі організації, яка зображена на рисунку 4.1.

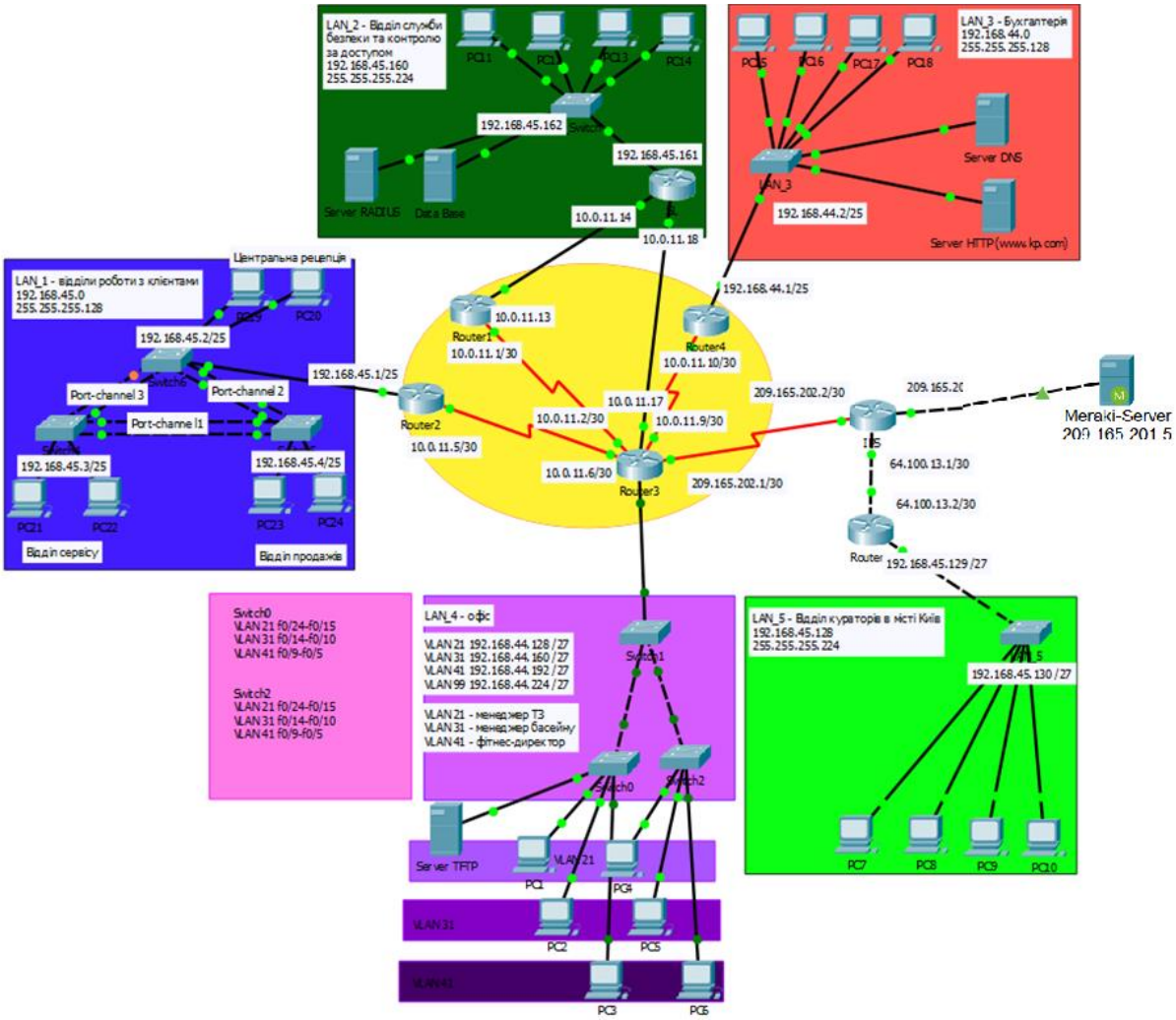

Рисунок 4.1 – Побудована модель комп'ютерної мережі фітнес клубу «Спортлайф»

4.2 Розрахунок схеми адресації корпоративної мережі

Для проектованої комп'ютерної мережі необхідно розробити адресацію з врахуванням наступних вимог до мережі: використовувати блок приватних IP-адрес 192.168.44.0/22 (255.255.252.0), та врахувати кількість вузлів у різних сегментах мережі згідно таблиці 4.1, мережу, в якій містяться VLAN-мережі, розрахувати виходячи з вимог згідно таблиці 4.2. Також необхідно провести розрахунок схеми IP-адресації послідовних каналів між маршрутизаторами з діапазону 10.0.11.0/24.

Таблиця 4.1 – Кількість вузлів в різних підмережах

LAN1	LAN2	LAN3	LAN4	LAN5
74	22	115	80	30

Таблиця 4.2 – Список мереж VLAN

Номер VLAN	Ім'я VLAN	Примітка
1	Default	Не використовується
21	Gym_administration	Для адміністрації ТЗ
31	Basin_administration	Для адміністрації басейну
41	Club_management	Для дирекції клубу
99	Management	Для управління пристроями
100	Native	Власна мережа

Розробка схеми адресації здійснюється за допомогою методу VLSM. VLSM (variable length subnet masks) – мережеві маски змінної довжини, що використовуються у безкласовій маршрутизації. VLSM дозволяє використання більш ніж однієї мережевої маски в межах одного адресного простору. VLSM максимізує використання адресного простору і його використовують для сегментування сегментованих локальних мереж.

Для розрахунку IP адресації спочатку визначається кількість мереж. Згідно з структурної схеми необхідно розділити вихідний пул IP-адрес 192.168.44.0/22 на 5 мереж (LAN 1-5). Спочатку необхідно визначити кількість біт необхідних для визначення п'яти мереж. Для визначення п'яти мереж необхідно 3 біти (2^3=8), оскільки при використанні 2 біт вихідну

мережу можна розділити лише на 4 підмережі (2^2=4). Далі необхідно упорядкувати мережі за кількістю необхідних IP-адрес. Найбільша мережа LAN3 повинна бути розрахована на 115 IP-адрес. Відповідно необхідна кількість біт для отримання необхідної кількості IP-адрес – 7 (2^7=128). Важливо зазначити, що із загальної кількості IP-адрес на визначення вузлів (хостів) відводиться на 2 менше, оскільки перша адреса визначає адресу мережі (у хостовій частині лише нулі), а остання визначає адресу широкомовної розсилки (у хостовій частині лише одиниці).

Таким чином розрахунок IP-адрес методом VLSM для мережі LAN 3 має вигляд:

192.168. 0010 11|**00.0**|000 0000

Символами "| |" виділена частина IP-адреси, що визначає мережеву частину адреси. Маска підмережі – 25 одиниць (255.255.255.128). Адреса підмережі – 192.168.44.0/25, перша допустима адреса підмережі визначається як значення 1 в наймолодшому біті IP-адреси у хостовій (вузловій) частині – 192.168.44.0|**000 0001**| (192.168.44.1). Остання допустима адреса визначається, як значення одиниць в усіх розрядах хостової частини окрім наймолодшого – 192.168.44.0|**111 1110**| (192.168.44.126). Широкомовна адреса визначається як усі одиниці в усіх розрядах хостової частини IP-адреси - 192.168.44.0|**111 1111**| (192.168.44.127).

Розрахунок IP-адрес методом VLSM для мережі LAN 4:

Необхідна кількість IP-адрес – 80, відповідно для виділення необхідна кількість біт для визначення вузлів теж 7.

Частину адреси, що визначає підмережу необхідно збільшити на 1, додавши 1 до молодшого біта: 192.168. 0010 11|**00.1**|000 0000

Таким чином адреса підмережі LAN 1 – 192.168.44.128 /25;

Але виходячи із умов завдання підмережа LAN1 повинна складатися із 4 мереж VLAN (21,31,41,99), необхідно розрахувати її розділення.

Розрахунок IP-адрес методом VLSM для мережі VLAN 21:

Для створення чотирьох мереж VLAN з підмережі 192.168.44.128 /25 необхідно 2 біти, таким чином маска – /27 (255.255.255.224):

– адреса підмережі: 192.168.44.1|**00**|0 0000 (192.168.44.128 /27);

– перша допустима адреса: 192.168.44.1|**00**|**0 0001** (192.168.44.129);

– остання допустима адреса: 192.168.44.1|**00**|**1 1110** (192.168.44.158);

– адреса широкомовної розсилки: 192.168.44.1|**00**|**1 1111** (192.168.44.159).

Розрахунок IP-адрес методом VLSM для мережі VLAN 31:

– адреса підмережі: 192.168.44.1|**01**|**0 0000** (192.168.44.160 /27);

– перша допустима адреса: 192.168.44. 1|**01**|**0 0001** (192.168.44.161);

– остання допустима адреса: 192.168.44.1|**01**|**1 1110** (192.168.44.190);

– адреса широкомовної розсилки: 192.168.44.1|**01**|**1 1111** **(**192.168.44.191).

Розрахунок IP-адрес методом VLSM для мережі VLAN 41:

– адреса підмережі: 192.168.44.1|**10**|0 0000 (192.168.44.192);

– перша допустима адреса: 192.168.44.1|**10**|**0 0001** (192.168.44.193);

– остання допустима адреса: 192.168.44.1|**10**|**1 1110** (192.168.44.222);

– адреса широкомовної розсилки: 192.168.44.1|**10**|**1 1110**1 (192.168.44.223).

Розрахунок IP-адрес методом VLSM для мережі VLAN 99:

– адреса підмережі: 192.168.44.1|**11**|0 0000 (192.168.44.224/27);

– перша допустима адреса: 192.168.44.1|**11**|0 0001 (192.168.44.225);

– остання допустима адреса: 192.168.44.1|**11**|1 1110 (192.168.44.254);

– адреса широкомовної розсилки: 192.168.44.1|**11**|1 1111 (192.168.44.225).

У таблиці 4.3 наведено розрахунок схеми IP-адресації мереж VLAN в мережі LAN4.

Таблиця 4.3 – Схема IP-адресації мереж VLAN в мережі LAN4

Мережа	Розмір	Адреса	Маска	Десяткова маска	Діапазон адрес	Адреса широкомовної розсилки
VLAN 21	30	192.168.44.128	/27	255.255.255.224	192.168.44.129 - 192.168.44.158	192.168.44.159
VLAN 31	30	192.168.44.160	/27	255.255.255.224	192.168.44.161 - 192.168.44.190	192.168.44.191
VLAN 41	30	192.168.44.192	/27	255.255.255.224	192.168.44.193 - 192.168.44.222	192.168.44.223
VLAN 99	30	192.168.44.224	/27	255.255.255.224	192.168.44.225 - 192.168.44.254	192.168.44.255

Розрахунок IP-адрес методом VLSM для підмережі LAN1:

Необхідна кількість IP-адрес – 80, відповідно для виділення необхідна кількість біт для визначення вузлів теж 7.

адреса підмережі: 192.168. 0010 11|**01.0**|000 0000 (192.168.45.0 /25);

– перша допустима адреса: 192.168. 0010 11|**01.0**|**000 0001** (192.168.45.1);

– остання допустима адреса: 192.168. 0010 11|**01.0**|**111 1110** (192.168.45.126);

– адреса широкомовної розсилки: 192.168. 0010 11|**01.0**|**111 1111** (192.168.45.127).

Розрахунок IP-адрес методом VLSM для підмережі LAN5:

Необхідна кількість IP-адрес – 30, відповідно для виділення необхідна кількість біт для визначення вузлі – 5 (2^5= 32).

Частину адреси, що визначає підмережу необхідно збільшити на 1 біт: 192.168. 0010 11|**01.1**|000 0000.

– адреса підмережі: 192.168.45.128 /27;

– перша допустима адреса: 192.168.45**.** |**100**|**0 0001** (192.168.45.129);

– остання допустима адреса: 192.168.45**.** |**100**|**1 1110** (192.168.45.158);

– адреса широкомовної розсилки: 192.168.45**.** |**100**|**1 1110** (192.168.45.159);

Розрахунок IP-адрес методом VLSM для підмережі LAN2:

Необхідна кількість IP-адрес –22, відповідно для виділення необхідна кількість біт для визначення вузлів теж 5.

Частину адреси, що визначає підмережу необхідно збільшити на 1 біт: 192.168.45**. |101|0 0000**.

– адреса підмережі: 192.168.45.160 /27;

– перша допустима адреса: 192.168.45**. |101|0 0001** (192.168.45.161);

– остання допустима адреса: 192.168.45**. |101|1 1110** (192.168.45.190);

– адреса широкомовної розсилки: 192.168.45**. |101|1 1110** (192.168.45.191).

Розрахована схема IP-адресації мереж зведена у таблицю 4.4.

Таблиця 4.4 − Схема IP-адресації мереж

Мережа	Виділений розмір	Адреса	Маска	Десяткова маска	Діапазон адрес	Адреса широкомовної розсилки
LAN3	126	192.168.44.0	/25	255.255.255.128	192.168.44.1 - 192.168.44.126	192.168.44.127
LAN4	126	192.168.44.128	/25	255.255.255.128	192.168.44.129 - 192.168.44.254	192.168.44.255
VLAN21	30	192.168.44.128	/27	255.255.255.224	192.168.44.129 - 192.168.44.158	192.168.44.159
VLAN31	30	192.168.44.160	/27	255.255.255.224	192.168.44.161 - 192.168.44.190	192.168.44.191
VLAN41	30	192.168.44.192	/27	255.255.255.224	192.168.44.193 - 192.168.44.222	192.168.44.223
VLAN99	30	192.168.44.224	/27	255.255.255.224	192.168.44.225 - 192.168.44.254	192.168.44.255
LAN1	126	192.168.45.0	/25	255.255.255.128	192.168.45.1 - 192.168.45.126	192.168.45.127
LAN5	30	192.168.45.128	/27	255.255.255.224	192.168.45.129 - 192.168.45.158	192.168.45.159
LAN2	30	192.168.45.160	/27	255.255.255.224	192.168.45.161 - 192.168.45.190	192.168.45.191

Розрахунок схеми IP-адресації послідовних каналів між маршрутизаторами з діапазону 10.0.11.0/24 проводиться аналогічно. Виходячи із умов завдання необхідно розрахувати адресацію для п’яти каналів між маршрутизаторами. Відповідно кількість біт необхідних для

визначення мереж 2 (2^3=8), а кількість біт необхідних для адресації вузлів – 2 (2^2=4). Перша адреса – адреса підмережі, друга адреса – порт першого маршрутизатора, третя адреса – порт другого маршрутизатора, четверта адреса – адреса широкомовної розсилки у послідовному каналі.

Розрахунок каналу WAN 1:

– адреса каналу: 10.0.11.000|0**00**|00 (10.0.11.0 /30);

– перша допустима адреса: 192.168.13.000 |0**00**| **01** (10.0.11.1);

– остання допустима адреса: 192.168.13.000 |**000**|**10** (10.0.11.2);

– адреса широкомовної розсилки: 192.168.13.000|0**00**|**11** (10.0.11.3).

Розрахунок каналу WAN 2:

– адреса каналу: 10.0.11.0000 |**01**|00 (10.0.11.4 /30);

– перша допустима адреса: 192.168.13.000 |0**01**|**01** (10.0.11.5);

– остання допустима адреса: 192.168.13.000 |0**01**|**10** (10.0.11.6);

– адреса широкомовної розсилки: 192.168.13.000 |0**01**|**11** (10.0.11.7).

Розрахунок каналу WAN 3:

– адреса каналу: 10.0.11.000|0**10**|00 (10.0.11.8 /30);

– перша допустима адреса: 10.0.11.000 |0**10**|**01** (10.0.11.9);

– остання допустима адреса: 10.0.11.000 |0**10**|**10** (10.0.11.10);

– адреса широкомовної розсилки: 10.0.11.000 |0**10**|**11** (10.0.11.11).

Розрахунок каналу WAN 4:

– адреса каналу: 10.0.11.000 |0**11**|00 (10.0.11.12 /30);

– перша допустима адреса: 10.0.11.000 |0**11**|**01** (10.0.11.13);

– остання допустима адреса: 10.0.11.000 |0**11**|**10** (10.0.11.14);

– адреса широкомовної розсилки: 10.0.11.000 |0**11**|**11** (10.0.11.15).

Розрахунок каналу WAN 5:

– адреса каналу: 10.0.11.000|**100**|00 (10.0.11.16 /30);

– перша допустима адреса: 10.0.11.000|**100**|**01** (10.0.11.17);

– остання допустима адреса: 10.0.11.000|**100**|**10** (10.0.11.18);

– адреса широкомовної розсилки: 10.0.11.000|**100**|**11** (10.0.11.19).

Згідно із завданням послідовний канал між маршрутизаторами Router3 та IPS необхідно розрахувати із пулу 209.165.202.0 /30:

– адреса каналу: 209.165.202.0000 00|**00** (209.165.202.0/30);

– перша допустима адреса: 209.165.202.0000 00|**01** (209.165.202.1);

– остання допустима адреса: 209.165.202.0000 00|**10** (209.165.202.2);

– адреса широкомовної розсилки: 209.165.202.0000 00|**11** (209.165.202.3).

Згідно із завданням послідовний канал між маршрутизаторами Router0 та IPS необхідно розрахувати із пулу 64.100.13.0 /30:

– адреса каналу: 64.100.13.0000 00|**00** (64.100.13.0/30);

– перша допустима адреса: 64.100.13.0000 00|**01** (64.100.13.1/30);

– остання допустима адреса: 64.100.13.0000 00|**10** (64.100.13.2/30);

– адреса широкомовної розсилки: 64.100.13.0000 00|**11** (64.100.13.3/30).

Розрахована схема IP-адресації послідовних каналів зведена у таблицю 4.5.

Таблиця 4.5– Схема IP-адресації послідовних каналів

Мережа	Виділений	Адреса	Маска	Десяткова маска	Діапазон адрес	Адреса широкомовної розсилки
WAN1	2	10.0.11.0	/30	255.255.255.252	10.0.11.1 - 10.0.11.2	10.0.11.3
WAN2	2	10.0.11.4	/30	255.255.255.252	10.0.11.5 - 10.0.11.6	10.0.11.7
WAN3	2	10.0.11.8	/30	255.255.255.252	10.0.11.9 - 10.0.11.10	10.0.11.11
WAN4	2	10.0.11.12	/30	255.255.255.252	10.0.11.13- 10.0.11.14	10.0.11.15
WAN5	2	10.0.11.16	/30	255.255.255.252	10.0.11.17- 10.0.11.18	10.0.11.19
WAN6	2	209.165.202.0	/30	255.255.255.252	209.165.202.1 - 209.165.202.2	209.165.202.3
WAN7	2	64.100.13.0	/30	255.255.255.252	64.100.13.1 - 64.100.13.2	64.100.13.3

4.3 Розрахунок схеми адресації пристроїв

Схема адресації пристроїв розрахована з урахуванням наступних вимог:

− перші можливі для використання IP-адреси призначати інтерфейсам і підінтерфейсам маршрутизаторів у LAN;

− другі з можливих IP-адрес призначати комутаторам у LAN;

− серверам привласнено 21-шу доступну адресу в мережі;

− останні з використовуваних IP-адрес призначено вузлам;

− в мережах VLAN використовується адресація кінцевих пристроїв за протоколом DHCP.

У таблиці 4.6 наведено схему адресації пристроїв.

Таблиця 4.6 – Схема адресації пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
LAN1						
Switch4	fa0/1	192.168.45.2	255.255.255.128	192.168.45.1	1	Switch5: fa0/1
	fa0/2					Switch5: fa0/2
	fa0/3					Switch6: fa0/3
	fa0/4					Switch6: fa0/4
	fa0/24					PC21: fa0
	fa0/23					PC22: fa0
Switch5	fa0/1	192.168.45.3	255.255.255.128	192.168.45.1	1	Switch4: fa0/1
	fa0/2					Switch4: fa0/2
	fa0/3					Switch6: fa0/1
	fa0/4					Switch6: fa0/2
	fa0/24					PC19: fa0
	fa0/23					PC20: fa0
Switch6	fa0/1	192.168.45.4	255.255.255.128	192.168.45.1	1	Switch5: fa0/3
	fa0/2					Switch5: fa0/4
	fa0/3					Switch4: fa0/3
	fa0/4					Switch4: fa0/4
	fa0/24					PC24: fa0
	fa0/23					PC23: fa0
LAN2						
SL	fa0/24	192.168.45.162	255.255.255.224	192.168.45.161	1	PC11: fa0
	fa0/23					PC12: fa0
	fa0/22					PC13: fa0
	fa0/21					PC14: fa0
	gi0/2					SL: gi0/2
Radius	fa0	192.168.45.181	255.255.255.224	192.168.45.161	1	Switch_SL: fa0/1

Продовження таблиці 4.6

LAN3						
LAN_3	Gi0/1	192.168.44.2	255.255.255.128	192.168.44.1	1	Router4: Gi0/0
	fa0/23					PC15: fa0
	fa0/22					PC16: fa0
	fa0/21					PC17: fa0
	fa0/20					PC18: fa0
	fa0/1					HTTP: fa0
	fa0/2					DNS: fa0
HTTP	fa0	192.168.44.22	255.255.255.128	192.168.44.1	1	LAN_3: fa0/1
DNS	fa0	192.168.44.21	255.255.255.128	192.168.44.1	1	LAN_3: fa0/2
LAN4						
Switch1	Gi0/1	192.168.44.226	255.255.255.224	192.168.44.225	99	Router3: Gi0/1
	fa0/1					Switch0: fa0/1
	fa0/2					Switch2: fa0/1
	fa0/3					TFTP: fa0/1
Switch0	fa0/1	192.168.44.227	255.255.255.224	192.168.44.225	99	Switch1: fa0/1
	fa0/24					PC1: fa0
	fa0/14					PC2: fa0
	fa0/9					PC3: fa0
Switch0	fa0/1	192.168.44.227	255.255.255.224	192.168.44.225	99	Switch1: fa0/1
	fa0/24					PC1: fa0
	fa0/14					PC2: fa0
	fa0/9					PC3: fa0
Switch2	fa0/1	192.168.44.228	255.255.255.224	192.168.44.225	99	Switch1: fa0/2
	fa0/24					PC4: fa0
	fa0/14					PC5: fa0
	fa0/9					PC6: fa0
LAN5						
LAN_5	Gi0/1	192.168.45.130	255.255.255.224	192.168.45.129	1	Router0: Gi0/1
	fa0/24					PC7: fa0
	fa0/23					PC8: fa0
	fa0/22					PC9: fa0
	fa0/21					PC10: fa0
	fa0/1					Radius: fa0
TFTP	fa0	192.168.44.149	255.255.255.224	192.168.44.129	21	Switch0: fa0/16
Маршрутизатори						
Router0	Gi0/1	64.100.13.2	255.255.255.252	-	-	LAN_5: Gi0/1
	Gi0/0	192.168.45.129	255.255.255.224	-	-	IPS: Gi0/0
Router1	Gi0/0	10.0.11.13	255.255.255.252	-	-	SL: Gi0/0
	Se0/0/0	10.0.11.1	255.255.255.252	-	-	Router3: Se0/0/0
Router2	Gi0/1	192.168.45.1	255.255.255.128	-	-	Switch6: Gi0/1
	Se0/0/0	10.0.11.5	255.255.255.252	-	-	Router3: Se0/0/1

Продовження таблиці 4.6

Router3	Se0/0/1	10.0.11.6	255.255.255.252	-	-	Router2: Se0/0/0
	Se0/0/0	10.0.11.2	255.255.255.252	-	-	Router1: Se0/0/0
	Gig0/0/	10.0.11.17	255.255.255.252	-	-	SL: Gi0/1
	Se0/1/0	10.0.11.9	255.255.255.252	-	-	Router4: Se0/0/0
	Se0/1/1	209.165.202.1	255.255.255.252	-	-	IPS: Se0/0/0
	Gi0/1	-	-	-	-	Switch1: Gi0/1
	Gi0/1.21	192.168.44.129	255.255.255.224	-	21	-
	Gi0/1.31	192.168.44.161	255.255.255.224	-	31	-
	Gi0/1.41	192.168.44.193	255.255.255.224	-	41	-
	Gi0/1.99	192.168.44.225	255.255.255.224	-	99	-
IPS	Se0/0/0	209.165.202.2	255.255.255.252	-	-	Router3: Se0/1/1
	Gi0/0	64.100.13.1	255.255.255.252	-	-	Router0: Gi0/0
	Gi0/1	209.165.201.1	255.255.255.224	-	-	PC26: Fa0
Інші пристрої						
Meraki Server	Fa0	209.165.201.5	255.255.255.224	-	-	IPS: Gi0/1

4.4 Базове налаштування конфігурації пристроїв

Після увімкнення і успішного завантаження мережевого пристрою необхідно провести базове налаштування його конфігурації. Після завантаження пристрою користувач потрапляє у користувацький режим командного рядка Cisco. В даному режимі доступний лише обмежений перелік команд, виконання яких не може нашкодити функціонуванню пристрою. Наприклад, з цього режиму можна подивитися версію операційної системи командою show version або запустити команду ping. Для того щоб налаштовувати конфігурацію пристрою перш за все необхідно увійти в привілейований режим за допомогою команди «enable»:

пристрій>enable

У привілейованому режимі доступні команди перегляду конфігурації маршрутизатора, діагностики роботи.

Для конфігурування пристрою необхідно перейти до режиму глобальної конфігурації за допомогою команди «configure terminal»:

пристрій#configure terminal

Призначення імені для пристрою виконується задля зручності його ідентифікації поміж інших мережевих пристроїв:

пристрій(config)#hostname *Soldatov_пристрій*;

Для забезпечення базової безпеки мережевого обладнання від несанкціонованого доступу встановлюється пароль на консольну лінію – управління через безпосередньо підключений консольний кабель та пароль на telnet -лінію – віддалене управління.

пристрій(config)# line console 0

пристрій(config-line)# password cisco

пристрій(config-line)# login

пристрій(config-line)# exit

пристрій(config)# line vty 0 4

пристрій(config-line)# password cisco

пристрій(config-line)# login

пристрій(config-line)# exit

Призначення паролю на вхід до привілейованого режиму:

пристрій(config)#enable secret class

Команда service password-encryption дає програмну забезпечення IOS вказівку зашифрувати паролі, секрети CHAP і інші, аналогічні дані, які зберігаються в файлі конфігурації у відкритому вигляді:

пристрій(config)#service password-encryption

Банер MOTD (повідомлення дня) встановлюється для інформування користувачів, що намагаються підключитися до пристрою:

пристрій(config)#banner motd #Hello! This is *Soldatov_пристрій* #

Для адміністрування пристрою необхідно створити в локальній базі користувачів користувача з найвищим рівнем привілеїв та задати йому пароль:

пристрій(config)#username Soldatov.123-18sk privilege 15 secret admincisco

Для використання служби SSH, а також для дозволу «необізнаних доменних імен» задається домен за замовчуванням, ім’я якого – ім’я пристрою:

пристрій(config)#ip domain-name *Soldatov_пристрій*

Для шифрування даних створюється ключ RSA (криптографічний алгоритм з відкритим ключем) завдовжки 1024 біти:

пристрій(config)#crypto key generate rsa 1024

SSH (Secure Shell – «безпечна оболонка») – мережевий протокол прикладного рівня, що дозволяє здійснювати віддалене управління операційною системою і тунелювання TCP-з'єднань (наприклад, для передачі файлів), шифрує весь трафік, включаючи і паролі, що передаються. Тому для vty ліній необхідно встановити використання даного протоколу:

пристрій(config)#ip ssh version 2

пристрій(config)#line vty 0 4

пристрій(config)#login local

пристрій(config)#transport input ssh

пристрій(config)#exit

Для налаштування послідовних каналів між маршрутизаторами використовуються спеціальні DCE-інтерфейси. На DCE інтерфейсі одного з маршрутизаторів, що створюють послідовний канал, необхідно встановити значення тактової частоти синхронізації – 128000:

Soldatov_router(config)#interface s0/0/0

Soldatov_router(config-if)#clock rate 128000

Soldatov_router(config-if)#no shutdown

Soldatov_router(config)#exit

Необхідно відповідно до розробленої схеми адресації пристроїв налаштувати відповідні пристрої. На комутаторі необхідно обрати

інтерфейс VLAN1 і задати йому відповідну адресу та маску. На маршрутизаторі необхідно обрати відповідний фізичний інтерфейс (Serial або Gigabit) та задати йому відповідну адресу та маску, а також увімкнути його. На кінцевих вузлах задається IP-адреса вузла, мережева маска та адреса DNS-сервера у разі ручного налаштування параметрів IP, або вказати використання служби DHCP.

4.5 Налаштування маршрутизації

Маршрутизація – процес визначення маршруту прямування інформації між мережами. Маршрутизатор приймає рішення, що базується на IP-адресі отримувача пакету. Для того, щоб переслати пакет далі, всі пристрої на шляху слідування використовують IP-адресу отримувача. Для прийняття правильного рішення маршрутизатор має знати напрямки і маршрути до віддалених мереж.

Існує два типи маршрутизації:

- статична маршрутизація – маршрути задаються вручну адміністратором;
- динамічна маршрутизація – маршрути обчислюються автоматично за допомогою протоколів динамічної маршрутизації – RIP, OSPF , EIGRP, IS-IS, BGP, HSRP, які отримують інформацію про топологію і стан каналів зв'язку від інших маршрутизаторів у мережі.

Оскільки статичні маршрути конфігуруються вручну, будь-які зміни мережної топології вимагають участі адміністратора для додавання і видалення статичних маршрутів відповідно до змін. У великих мережах підтримка таблиць маршрутизації вручну може вимагати величезних витрат часу адміністратора. У невеликих мережах це робити легше. Статична маршрутизація не має можливості масштабування, яку має динамічна маршрутизація через додаткові вимоги до налаштування і втручання адміністратора.

В проектованій мережі в якості протоколу динамічної маршрутизації буде використано протокол EIGRP – вдосконалений дистанційно-векторний протокол динамічної маршрутизації.

Налаштування маршрутизації в мережі починається зі створення процесу EIGRP, далі необхідно оголосити безпосередньо підключені мережі і відключити поширення оновлень маршрутизації на інтерфейси в локальні мережі.

Для VLAN мереж необхідно визначити сумарний маршрут. Сумарний маршрут визначається таким чином: адреса мережі це та частина адрес, що не відрізняється, а маска – це та частина мережевої адреси, яка відрізняється:

192.168.44.1|000 0000

192.168.44.1|010 0000

192.168.44.1|100 0000

192.168.44.1|110 0000

Відмінність адрес починається в сьомому біті першого байту адреси, тому мережева маска – /25, а адреса сумарного маршруту – 192.168.44.128.

Необхідно вимкнути автоматичне підсумовування маршрутів.

Для реалізації доступу до мережі Інтернет в мережі організації необхідно налаштувати маршрут за умовчанням на маршрутизаторі з прямим підключенням до інтернет-провайдера (ISP) і розповсюдити його через оновлення маршрутизації. Маршрут за замовчуванням – це мережевий шлюз на який пакет відправляється в тому випадку, якщо маршрут до мережі призначення пакета не відомий.

4.6 Налаштування мереж VLAN, параметрів безпеки комутаторів та адресації ПК в мережах VLAN

VLAN (Virtual Local Area Network) – група пристроїв, що мають можливість взаємодіяти між собою безпосередньо на канальному рівні, хоча фізично при цьому вони можуть бути підключені до різних мережевих

комутаторів. І навпаки, пристрої, що знаходяться в різних VLAN, невидимі один для одного на канальному рівні, навіть якщо вони підключені до одного комутатора, і зв'язок між цими пристроями можливий тільки на мережевому і більш високих рівнях.

Налаштування VLAN складається з наступних кроків:

1) Створити відповідні мережі VLAN і присвоїти кожній з них ім'я;

2) Переведення портів в режим доступу та призначення їм мережі VLAN;

3) Налаштування каналу в якості транкового. Вказання мережі native VLAN для транків 802.1Q без міток, список мереж VLAN, яким дозволено доступ до транкового каналу;

4) Налаштування маршрутизації між VLAN за допомогою інкапсуляції 802.1Q.

В мережах VLAN буде використана динамічна IP-адресація на основі протоколу DHCP.

DHCP (Dynamic Host Configuration Protocol – протокол динамічної конфігурації вузла) – це мережевий протокол, що дозволяє комп'ютерам автоматично отримувати такі параметри як IP-адресу, маску, адресу шлюзу, та адресу DNS-сервера, які необхідні для роботи в мережі TCP/IP.

Маршрутизатор Soldatov_Router_3 буде виконувати роль DHCP-сервера у мережі LAN 4. Для налаштування DHCP-сервера було виконано:

1) виключено адреси, які не повинні входити в відповідний пул;

2) створено пули, з відповідними іменами (pool-VLAN21, pool-VLAN31, pool-VLAN41);

3) задано діапазони адрес пулів та їх маски (для VLAN 21 – 192.168.44.129 - 192.168.44.158 /27, VLAN 31 – 192.168.44.161 - 192.168.44.190 /27, VLAN 41 – 192.168.44.193 - 192.168.44.222 /27);

4) задано адреси шлюзів за замовчуванням (для VLAN 21 – 192.168.44.129, VLAN 31 – 192.168.44.161, VLAN 41 – 192.168.44.193);

5) задано адресу DNS-серверу (192.168.44.21).

Так як в цій мережі знаходиться сервер, то для захисту конфіденційної та комерційної інформації налаштовано функцію безпеки портів на портах комутаторів, підключених до серверів. Налаштування виконано таким чином, щоб тільки двом унікальним пристроям був дозволений доступ до порту та MAC-адреси розпізнавались динамічно і додавались в поточну конфігурацію. Якщо було порушено систему безпеки з'явиться повідомлення, а порт залишиться увімкненим. Якщо на даному інтерфейсі одночасно з'явиться третя (невідома) MAC-адреса, то всі пакети з цієї адреси будуть відкидатися, при цьому відправляється оповіщення – syslog, SNMP trap, збільшується лічильник порушень безпеки.

4.7 Налаштування роботи Інтернет

Для того щоб надати робочим станціям мережі організації доступ до мережі Інтернет на прикордонному маршрутизаторі було налаштовано протокол NAT.

NAT (Network Address Translation) – трансляція мережевих адрес. Процедура зі зміни адрес в заголовках IP-пакетів при їх проходженні через маршрутизатор або інший пристрій. Основною метою використання NAT є економія кількості публічних IPv4-адрес. Використання NAT дозволяє застосовувати приватні адреси всередині мережі, перетворюючи їх в публічні тільки в разі потреби.

Пристроям всередині підприємства можуть присвоюватися приватні адреси, а самі пристрої можуть функціонувати з унікальними локальними адресами.

При необхідності відправки трафіку в іншу організацію або Інтернет (або отримання трафіку з іншої організації або Інтернету) прикордонний маршрутизатор перетворює адреси в унікальні публічні глобальні адреси.

Динамічний NAT. Метод динамічного перетворення мережевих адрес (динамічний NAT) використовує пул публічних адрес, які присвоюються в порядку живої черги.

Коли внутрішній пристрій запитує доступ до зовнішньої мережі, динамічний NAT привласнює доступний публічний IPv4-адрес з пулу.

Для динамічного NAT потрібна достатня кількість публічних адрес, доступних для загальної кількості одночасних сеансів користувачів.

4.8 Перевірка налаштувань маршрутизації

Для перевірки налаштувань маршрутизації із мережі LAN 1 до мережі LAN 3 за допомогою команди tracert було отримано маршрут слідування. Результати виконання команди наведені на рисунку 4.2.

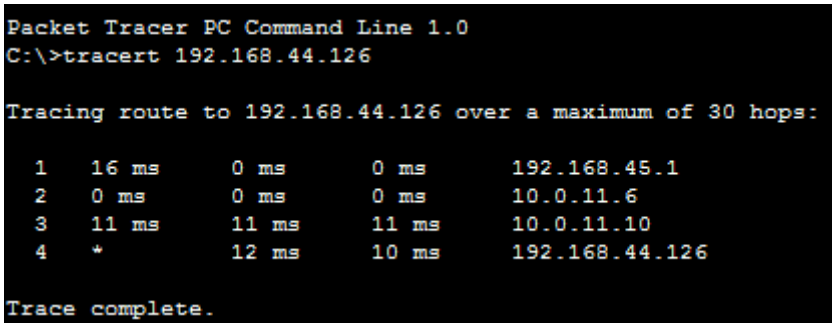

Рисунок 4.2 – Команда tracert між вузлами мережі LAN 1 і LAN 3

Про правильні налаштування маршрутизації свідчить наявність у таблиці маршрутизації маршрутизаторів, записів усіх мереж організації, отриманих за протоколом EIGRP. Таблиця маршрутизації центрального маршрутизатора Soldatov_Router_3 наведена на рисунку 4.3.

```
Gateway of last resort is 209.165.202.2 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
C       10.0.11.0/30 is directly connected, Serial0/0/0
L       10.0.11.2/32 is directly connected, Serial0/0/0
C       10.0.11.4/30 is directly connected, Serial0/0/1
L       10.0.11.6/32 is directly connected, Serial0/0/1
C       10.0.11.8/30 is directly connected, Serial0/1/0
L       10.0.11.9/32 is directly connected, Serial0/1/0
D       10.0.11.12/30 [90/3072] via 10.0.11.18, 04:37:31, GigabitEthernet0/0
C       10.0.11.16/30 is directly connected, GigabitEthernet0/0
L       10.0.11.17/32 is directly connected, GigabitEthernet0/0
     192.168.44.0/24 is variably subnetted, 10 subnets, 3 masks
D       192.168.44.0/25 [90/2170112] via 10.0.11.10, 04:37:24, Serial0/1/0
D       192.168.44.128/25 is a summary, 04:37:32, Null0
C       192.168.44.128/27 is directly connected, GigabitEthernet0/1.21
L       192.168.44.129/32 is directly connected, GigabitEthernet0/1.21
C       192.168.44.160/27 is directly connected, GigabitEthernet0/1.31
L       192.168.44.161/32 is directly connected, GigabitEthernet0/1.31
C       192.168.44.192/27 is directly connected, GigabitEthernet0/1.41
L       192.168.44.193/32 is directly connected, GigabitEthernet0/1.41
C       192.168.44.224/27 is directly connected, GigabitEthernet0/1.99
L       192.168.44.225/32 is directly connected, GigabitEthernet0/1.99
     192.168.45.0/24 is variably subnetted, 2 subnets, 2 masks
D       192.168.45.0/25 [90/2170112] via 10.0.11.5, 04:37:25, Serial0/0/1
D       192.168.45.160/27 [90/3072] via 10.0.11.18, 04:37:31, GigabitEthernet0/0
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.0/30 is directly connected, Serial0/1/1
L       209.165.202.1/32 is directly connected, Serial0/1/1
S*   0.0.0.0/0 [1/0] via 209.165.202.2
```

Рисунок 4.3 – Таблиця маршрутизації Soldatov_Router_3

4.9 Перевірка роботи DHCP

Про правильність налаштувань DHCP свідчить успішне отримання робочими станціями мережевих адрес із даного пулу, відповідна маска та адреса шлюзу за замовчуванням та DNS-сервера (див. рисунок 4.4).

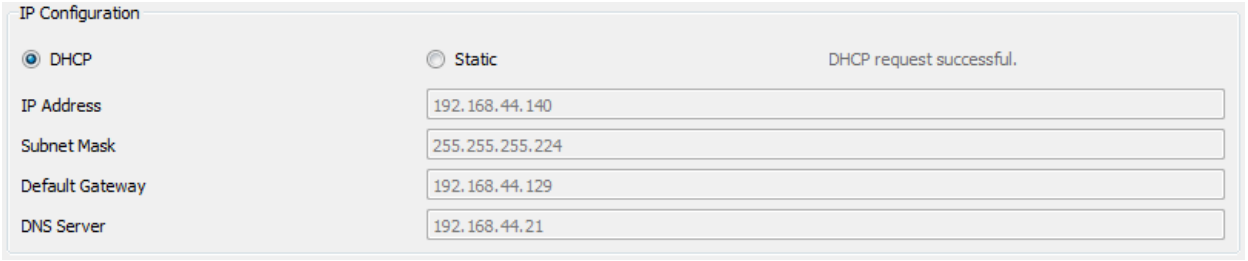

Рисунок 4.4 – Параметри IP-конфігурації вузла

4.10 Перевірка налаштувань VLAN

Для перевірки правильності налаштувань VLAN було згенеровано ICMP-пакет між вузлом 192.168.44.140 із VLAN 21 та вузлом 192.168.44.173

із VLAN 31 (рисунок 4.5). При проходженні дейтаграма через комутатор до кадру Ethernet II додається 802.1q Tag (рисунок 4.6), у полі TCI з'являється номер VLAN ($0x0015_{16}=21_{10}$) відправника, а після проходження кадру через маршрутизатор у полі TCI відображається номер VLAN ($0x001f_{16}=31_{10}$) отримувача.

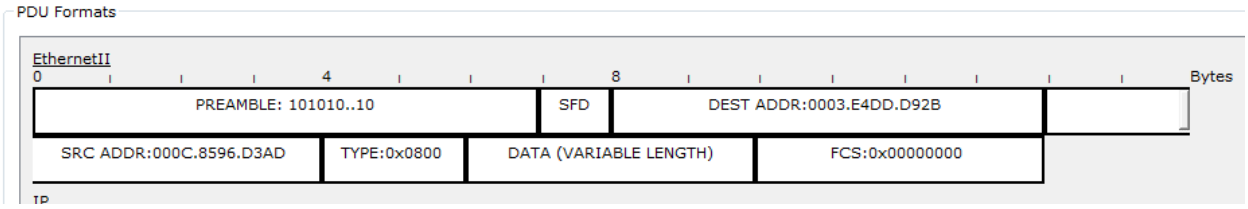

Рисунок 4.5 – Згенерована дейтаграма відправника

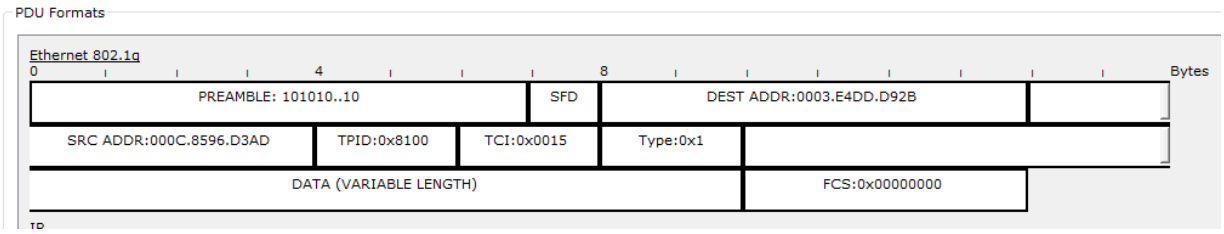

Рисунок 4.6 – Дейтаграма після проходження через комутатор

Правильність налаштування VLAN також перевірено командою show vlan brief (рисунок 4.7), де вказуються активні мережі VLAN, їх номера та імена, а також порти до яких вони відносяться.

```
Chernysh_Switch0_LAN_4#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/2, Fa0/3, Fa0/4, Gig0/1
                                                   Gig0/2
21   Gym_administration                  active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                   Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                   Fa0/23, Fa0/24
31   Basin_administration                active    Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                   Fa0/14
41   Club_management                     active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                   Fa0/9
99   Management                          active
100  Native                              active
1002 fddi-default                        active
1003 token-ring-default                  active
1004 fddinet-default                     active
1005 trnet-default                       active
```

Рисунок 4.7 – Налаштування VLAN на Soldatov_Switch0_LAN4

4.11 Перевірка налаштувань NAT

Для перевірки правильності роботи NAT було згенеровано ICMP-пакет між робочими станціями з різних підмереж організації до віддаленої мережі LAN 5. Про правильність налаштувань та роботи NAT свідчить таблиця NAT-перетворень маршрутизатора Soldatov_Router_3, яка наведена на рисунку 4.8.

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	209.165.202.7:1	192.168.44.125:1	192.168.45.158:1	192.168.45.158:1
icmp	209.165.202.7:2	192.168.44.125:2	192.168.45.158:2	192.168.45.158:2
icmp	209.165.202.7:3	192.168.44.125:3	192.168.45.158:3	192.168.45.158:3
icmp	209.165.202.7:4	192.168.44.125:4	192.168.45.158:4	192.168.45.158:4
icmp	209.165.202.8:1	192.168.44.126:1	192.168.45.155:1	192.168.45.155:1
icmp	209.165.202.8:2	192.168.44.126:2	192.168.45.155:2	192.168.45.155:2

Рисунок 4.8 – Таблиця NAT-перетворень на прикордонному маршрутизаторі Soldatov_Router_3

5 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КС

5.1 Призначення і область застосування програми КС

Сценарію Python, що виконує програмний збір поточної робочої конфігурації з пристрою Cisco IOS-XE і збереження конфігурації в репозиторії GitHub.

5.2 Обґрунтування технічних характеристик програм

5.2.1 Обґрунтування вибору системи контролю версій

Завдання кваліфікаційної роботи – розробити підсистему збору поточної конфігурації з пристрою Cisco IOS-XE.

Контроль версій, або так звана система контролю версій, - це спосіб управління змінами в наборі файлів для збереження історії цих змін.

Системи контролю версій (СКВ) зберігають основний набір файлів і історію змін в репозиторії, також відомому як репозиторій. Щоб внести зміни в файл, користувач повинен отримати робочу копію сховища в своїй локальній системі. Робоча копія - це особиста копія файлів, в яку вони можуть вносити зміни, не зачіпаючи інших. Деякі з переваг контролю версій:

– це забезпечує можливість спільної роботи - кілька людей можуть працювати над проектом (набором файлів) одночасно, не скасовуючи зміни один одного;

– підзвітність та прозорість - видно, хто які зміни вніс, коли і чому;

– можливість створювати нові функції незалежно, не зачіпаючи існуюче програмне забезпечення;

– файли можуть бути повернуті в разі помилки;

– файли зберігаються в репозиторії, тому будь-який пристрій може мати робочу копію.

На даний момент найпопулярнішою системою контролю версій є Git. Git − це реалізація розподіленої системи контролю версій з відкритим

вихідним кодом, яка в даний час є останньою тенденцією в розробці програмного забезпечення.

Переваги Git:

– легко вчитися;

– може обробляти всі типи проектів, в тому числі великі корпоративні проекти;

– має високу продуктивність;

– створено для спільних проектів;

– гнучкий;

– досить легкий;

– має всі переваги розподіленої системи контролю версій;

– безкоштовний.

На клієнтському комп'ютері повинен бути встановлений клієнт Git. Він доступний для MacOS, Windows і Linux/Unix. Хоча деякі клієнти Git поставляються з базовим графічним інтерфейсом, Git зосереджений на інтерфейсі командного рядка.

Одне з ключових відмінностей між Git і іншими системами контролю версій полягає в тому, що Git зберігає дані у вигляді знімків, а не відмінностей (різниці між поточним файлом і попередньою версією). Якщо файл не змінюється, Git використовує посилання на останній знімок в системі замість створення нового ідентичного знімка.

Концептуально, більшість СКВ зберігають інформацію як список файлових редагувань. Ці інші системи (CVS, Subversion, Perforce, Bazaar тощо) розглядають інформацію як список файлів та змін кожного з них протягом деякого часу (це зазвичай називають оснований на дельтах контроль версій).

Git не оброблює та не зберігає свої дані таким чином. Замість цього, Git сприймає свої дані радше як низку знімків мініатюрної файлової системи. У Git щоразу, як створювати коміт, тобто зберігати стан проекту, Git запам’ятовує як виглядають всі файли в той момент і зберігає посилання

на цей знімок. Для ефективності, якщо файли не змінилися, Git не зберігає файли знову, просто робить посилання на попередній ідентичний файл, котрий вже зберігається. Git вважає свої дані як потік знімків [11].

Це дуже важлива різниця між Git та майже всіма іншими СКВ. З цієї причини в Git було заново переосмислено майже кожен аспект контролю версій, які інші системи просто копіювали з попереднього покоління. Це зробило Git більш схожим на мініатюрну файлову систему з деякими неймовірно потужними вбудованими інструментами на додаток, а не просто СКВ [11].

Git складається з трійок - трьох етапів і трьох станів (рис.5.1).

Рисунок 5.1 − Стану файли в Git

В Git файли можуть перебувати в одному з трьох станів: зафіксованому, зміненому і підготовленому. «Зафіксований» означає, що файл вже збережено у локальній базі. До змінених відносяться файли, які змінилися, але ще не були зафіксовані. Підготовлені файли - це змінені файли, відмічені для включення в наступний коміт [11].

Таким чином, в проекті з використанням Git є три частини: каталог Git (Git directory), робочий каталог (working directory) і область підготовлених файлів (staging area).

Каталог Git це місце, де Git зберігає метадані та базу даних об'єктів вашого проекту. Це найбільш важлива частина Git. У кожного клієнта є повна копія сховища. Коли проект стає репозиторієм Git, створюється прихований каталог .git, який по суті є репозиторієм. Каталог .git містить метадані, такі як файли (стислі), фіксації та журнали (історія фіксації).

Робочий каталог − це витягнута з бази копія певної версії проекту. Це папка, видима в файлової системі. Ці файли можна змінювати, і зміни видно тільки користувачеві клієнта. Якщо файлова система клієнта буде пошкоджена, ці зміни будуть втрачені, але основний репозиторій залишиться недоторканим.

Область підготовлених файлів − це звичайний файл, зазвичай зберігається в каталозі Git, який містить інформацію про те, що повинно увійти в наступний коміт. Проміжна область зберігає інформацію про те, що користувач хоче додати/поновити/видалити в репозиторії. Користувачеві не потрібно додавати всі свої змінені файли в сліпок/репо; вони можуть вибирати певні файли. Хоча це називається областю, на самому ділі це просто індексний файл, розташований в каталозі .git.

Стандартний робочий процес з використанням Git виглядає приблизно так:

1. Змінюються файли в робочому каталозі.

2.Підготовлюються файли, додаючи їх зліпки в область підготовлених файлів.

3. Робиться коміт. При цьому зліпки з області підготовлених файлів зберігаються в каталог Git.

Якщо робоча версія файлу збігається з версією в каталозі Git, файл вважається зафіксованим. Якщо файл змінений, але доданий в область підготовлених даних, він підготовлений. Якщо ж файл змінився після вивантаження з БД, але не був підготовлений, то він вважається зміненим.

5.2.2 GitHub

Робота з проектами з використанням Git часто асоціюється з GitHub, але Git і GitHub - це не одне і те ж. Git - це реалізація розподіленого управління версіями і інтерфейс командного рядка. GitHub - це сервіс, що надається Microsoft, який реалізує сервіс хостингу сховища з Git.

Крім забезпечення розподіленого контролю версій і функцій управління вихідним кодом Git, GitHub також надає додаткові функції, такі як:

– огляд коду;

– документація;

– управління проектом;

– відстеження помилок;

– запити функцію

Щоб власники проектів могли управляти таким розрізненими сценаріями, GitHub ввів концепцію «пул реквест». Запит на витягування − це спосіб формалізації запиту з боку учасника на перевірку змін, таких як новий код, зміни існуючого коду і т. Д., В гілки учасника для включення в основну або інші кураторів гілки проекту. Ідіома запиту на витягування тепер повсюдно реалізована в сервісах хостингу Git.

GitHub − не єдина служба хостингу репозиторіїв, що використовує Git, інші включають Gitlab і Bitbucket.

5.2.3 Початкове налаштування Git

До Git входить утиліта що має назву git config, яка дозволяє отримати чи встановити параметри, що контролюють усіма аспектами того, як Git виглядає чи працює. Ці параметри можуть бути збережені в трьох різних місцях в системах Linux [11].

Файл /etc/gitconfig містить значення для кожного користувача в системі і всіх їхніх репозиторіїв. Коли передається опція --system при виконанні git config, параметри читаються та пишуться з цього файлу. (Це

системний файл конфігурації, відповідно, потрібен доступ адміністратора чи суперкористувача, щоб змінювати його.)

Файл ~/.gitconfig або ~/.config/git/config зберігає значення саме користувача. Можна налаштувати Git читати і писати в цей файл, вказуючи опцію --global.

Файл config у каталозі Git (тобто .git/config) у тому репозиторії, який використовуєтеся в даний момент, зберігає налаштування конкретного репозиторія.

Кожен рівень має пріоритет над налаштуваннями в попередньому рівні, тобто параметри в .git/config перевизначають параметри в /etc/gitconfig.

У системах Windows, Git шукає файл .gitconfig в каталозі $HOME (C:\Users\$USER для більшості користувачів). Він також все одно шукає файл /etc/gitconfig, хоча відносно кореня MSys, котрий знаходиться там, де встановлено Git у Windows системі [11].

5.3 Опис розробленої програми КС

5.3.1 Загальні відомості

Сценарій, написаний на мові Python, що виконує програмний збір поточної робочої конфігурації з пристрою Cisco IOS-XE і збереження конфігурації в репозиторії Git.

Мета застосунку – виконання резервного копіювання поточної конфігурації пристрою по запиту адміністратора системи.

5.3.2 Функціональне призначення

Функції, які виконує застосунок:

- авторизація та підключення користувача до пристрою;
- зберігання файлу поточної конфігурації пристрою в Git.

5.3.3 Опис логічної структури програми

На рис. 5.2 зображено діаграму робочого процесу збереження конфігурації в репозиторії GitHub.

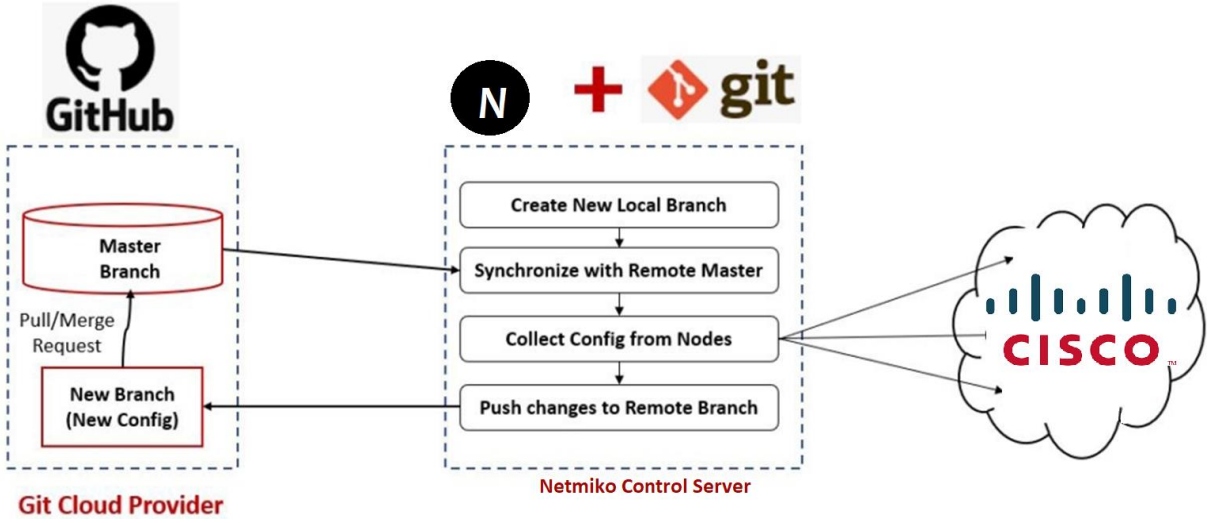

Рисунок 5.2 – Діаграма робочого процесу збереження конфігурації в репозиторії GitHub

Для підключення до пристрою ми будемо використовувати функції імпортованої бібліотеки Netmiko. Netmiko - це бібліотека SSH Python з підтримкою декількох вендорів, яка спрощує процес підключення до мережевих пристроїв через SSH. Ця бібліотека додає специфічну логіку виробника до paramiko, яка є де-факто SSH бібліотекою в Python [10].

Netmiko може бути встановлений через менеджер пакетів Python - pip.

```
$ Pip3 install netmiko
```

При ініціалізації програми першим чином надаються деталі підключення Cisco IOS-XE, а саме ти пристрою, IP-адреса та логін і пароль користувача.

Потім надаються дані сховища Git, а саме посилання на нього.

Для підключення до пристрою ми використовуємо ConnectHandler, якому передаємо свої дані підключення. Для підключення до пристрою та посилається команда show run для збереження результату в змінній `device_config`.

Відключаємось від пристрою для звільнення ресурсів.

Створюється тимчасова директорі в Git та клонується в неї репозиторій. Замінюються файли новим конфігураційним файлом і фіксуються всі зміни в Git (рис. 5.3).

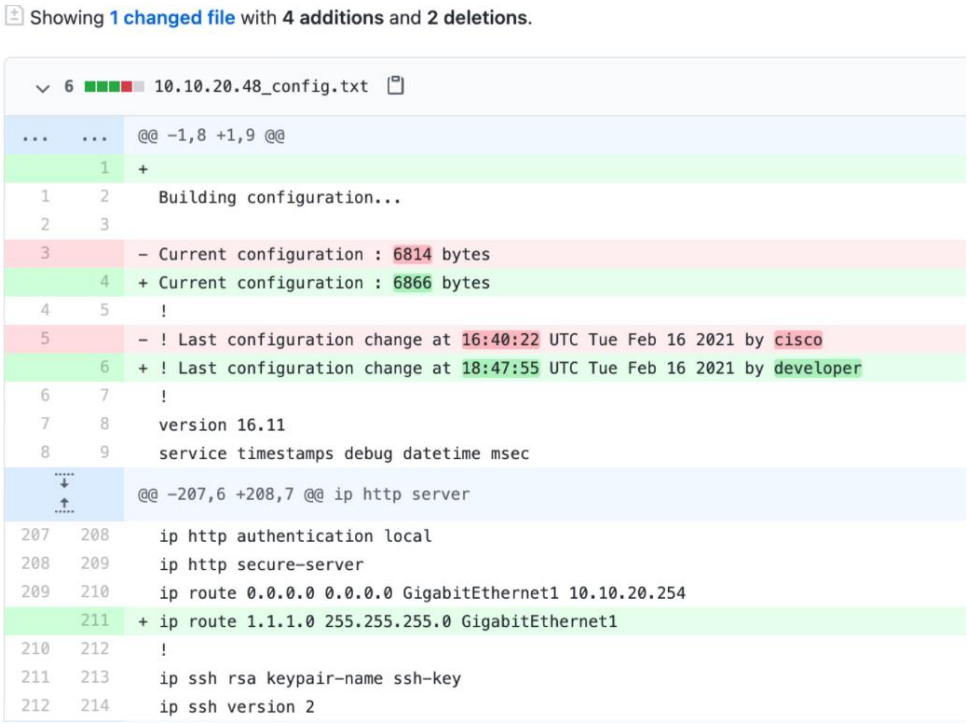

Рисунок 5.2 – Збережений файл в репозиторії GitHub

5.3.4 Використовувані технічні засоби

Під час розробки були використані наступні інструменти:

– Python 3.9.0;

– Git, встановлений на ПК;

– віддалений репозиторій Git;

– термінал, сумісний с Bash;

– доступ до пристрою IOS-XE.

5.3.5 Виклик і завантаження програми

Скрипт Python cisco_iosxe_to_git.py запускається безпосередньо в екземплярі терміналу, використовуючи subprocess.

5.3.6 Вхідні і вихідні дані

Вхідними даними є деталі підключення до пристрою Cisco IOS-XE, а саме:

– host – IP-адреса пристрою Cisco IOS-XE;

– username – логін адміністратора;

– password – пароль адміністратора.

Вихідними даними є новий комміт Git, який відстежить зміни між новою конфігурацією і старою.

6 ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ СИСТЕМІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Будь-яке розміщене рішення Git, таке як GitHub, GitLab або BitBucket. Git Repo, має бути приватним Repo, а доступ до цього приватного Repo повинен регулюватися ключами доступу SSH. Інший підхід полягає у використанні приватного екземпляра GitLab або BitBucket у мережі замість розміщеного рішення, доступного в Інтернеті, це на випадок, якщо вимоги до несанкціонованого доступу будуть більш жорстким.

ВИСНОВКИ

У даній кваліфікаційній роботі ми створили комп’ютерну систему мережі фітнес-клубів “Sport Life” з детальною розробкою підсистеми збору конфігурацій з використанням пристрою Cisco IOS-XE і збереження конфігурацій у репозиторії GitHub.

Практична цінність даної роботи полягає в впровадженні модернізації не лише в одному фітнес-центрі, а в загалом по всій мережі філіалів по Україні. За допомогою даної технології керування можливо здійснювати з будь якого місця через веб-браузерну панель, а також розробникам на дасть змогу використовувати розширенні можливості, сервіси да дані платформи в формі відкритих API-інтерфейсів, також на сам перед це полегшить збір та збереження конфігурацій.

Розробка комп’ютерної мережі виконана відповідно до завдання на кваліфікаційну роботу бакалавра.

Розроблена схема мережі реалізована у вигляді моделі на базі симулятора Cisco Packet Tracer з перевіркою її працездатності. Також був написаний програмний код для отримання коректної інформації з пристроїв.

Переваги даного проекту:

- централізоване управління без апаратного чи програмного контролера;
- підтримання інструментів керованого вирішення проблем та задач;
- дуже прості і швидкі розгортання оновлень;
- охоплення всієї мережі;
- зниження витрат на впровадження та обслуговування ;
- полегшення системи збору та збереження конфігурацій.

ПЕРЕЛІК ПОСИЛАНЬ

1. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання курсового проекту студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, Я.В. Панферова, Л.В. Бешта; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – 28 с.
2. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 1. – 60 с.
3. https://dou.ua/lenta/articles/infrastructure-as-code/
4. https://developer.cisco.com (дата звернення 09.06.2021)
5. https://devnetsandbox.cisco.com (дата звернення 09.06.2021)
6. https://www.netacad.com (дата звернення 09.06.2021)
7. https://sandboxdnac.cisco.com (дата звернення 09.06.2021
8. (https://uk.wikipedia.org/wiki/Прикладний_програмний_інтерфейс)
9. https://documentation.meraki.com/Architectures_and_Best_Practices/MX_and_MS_Basic_Recommended_Layer_3_Topology
10. https://github.com/ktbyers/netmiko
11. https://chamber.ua/wp-content/uploads/2019/12/progit_v2.1.2.pdf

ДОДАТОК А

Текст програми збору поточної робочої конфігурації з пристрою Cisco IOS-XE і збереження конфігурації в репозиторії GitHub