

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра на тему:
«Проект підсистеми захисту корпоративної мережі компанії на
базі обладнання Cisco»

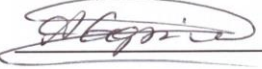
Виконав студент 4-го курсу, групи КБ-2
спеціальності 125 «Кібербезпека»

 Могильний Є.Л.

Керівник, професор кафедри КІ та КБ, д.т.н.,
доцент

 Воротніков В.В.

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

 Єфіменко А.А.

Житомир 2022

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

ЗАТВЕРДЖУЮ

Завідувач кафедри

комп'ютерної інженерії

та кібербезпеки

 Єфіменко А. А.

«01» березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента **Могильного Євгенія Леонідовича**

Тема роботи: **Проект підсистеми захисту корпоративної мережі компанії на базі обладнання Cisco**

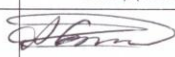
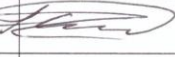
затверджена Наказом по університету від «01» березня 2022 р. № 128/С

Термін здачі студентом закінченої роботи – «10» червня 2022р.

Вихідні дані для роботи:

1. Фізична топологія мережі
2. Логічна топологія мережі
3. Маршрутизатори Cisco
4. Комутатори Cisco
5. Операційні системи Cisco IOS, Windows 7, Ubuntu, Linux.
6. Графічний симулятор мереж GNS3

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	/ Сугоняк І.І.	 1.03.22	 01.03.22
2	/ Сугоняк І.І.	 1.03.22	 01.03.22
3	/ Сугоняк І.І.	 1.03.22	 01.03.22

Керівник  Воротніков В.В.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	12 квітня 2022 – 13 квітня 2022	Виконано
2	Пошук літературних джерел для створення корпоративної мережі	14 квітня 2022 – 15 квітня 2022	Виконано
3	Аналіз протоколів захисту для маршрутизаторів CISCO	16 квітня 2022 – 17 квітня 2022	Виконано
4	Аналіз можливостей створення корпоративної мережі на базі обладнання Cisco	18 квітня 2022 – 20 квітня 2022	Виконано
5	Розробка проекту корпоративної мережі	20 квітня 2022 – 24 квітня 2022	Виконано
6	Вибір обладнання та початок реалізації проекту	25 квітня 2022 – 30 квітня 2022	Виконано
7	Проектування таблиці маршрутизації	1 травня 2022 – 4 травня 2022	Виконано
8	Узгодження тестування мережі	5 травня 2022 – 12 травня 2022	Виконано
9	Базове налагодження пристроїв мережі	13 травня 2022 – 17 травня 2022	Виконано
10	Налагодження корпоративної мережі	18 травня 2022 – 25 травня 2022	Виконано
11	Тестування на працездатність корпоративної мережі	26 травня 2022 – 29 травня 2022	Виконано
12	Аналіз результатів тестування	30 травня 2022 – 03 червня 2022	Виконано
13	Написання пояснювальної записки	04 червня 2022 – 08 червня 2022	Виконано
14	Підготовка презентації та виступу	09 червня 2022 – 15 червня 2022	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	20 червня 2022 – 22 червня 2022	Виконано
16	Захист	27 червня 2022	Виконано

Студент  Могильний Є.Л.

Керівник  Воротніков В.В.

РЕФЕРАТ

Кваліфікаційна робота складається з проєкту корпоративної мережі компанії на базі обладнання Cisco. Пояснювальна записка містить 58 сторінки, 33 ілюстрації та 5 таблиць.

Дипломний проєкт присвячений розробці корпоративної мережі компанії на базі обладнання Cisco. Метою проєкту буде надійність та захищеність. Мережа повинна забезпечити стабільний обмін даними та безпеку пристроїв, тому було створено користувачів для віддаленого доступу.

Дипломний проєкт буде складатися з трьох розділів, які включатимуть в себе розробку логічної та фізичної структури мережі, вибір мережевого обладнання та ПЗ, сценарій налаштування мережі та тестування проєкту. В додатках буде вказано конфігурації маршрутизаторів та комутаторів мережі.

КЛЮЧОВІ СЛОВА: ЗАХИСТ, КОМПЮТЕРНА МЕРЕЖА, КОРПОРАТИВНІ МЕРЕЖІ, RADIUS, CISCO.

					КБ.КВ.Б – 125 -22 -ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту корпоративної мережі компанії на базі обладнання Cisco Пояснювальна записка	Літ.	Арк.	Аркуші
Розроб.		Мозильний Є.Л.		10.06.22				
Керівник		Воротніков В.В.		20.06.22			4	61
Н. контр.		Ефіменко А.А.		20.06.22		Державний університет «Житомирська політехніка», група КБ-2		
Рецензент.		Ефіменко А.А.		20.06.22				
Зав. каф.		Ефіменко А. А.		20.06.22				

ABSTRACT

The qualification work consists of a project of the company's corporate network based on Cisco equipment. The explanatory note contains 63 pages, 52 illustrations and 9 tables.

The thesis project is devoted to the development of the company's corporate network based on Cisco equipment. The aim of the project will be reliability and security. The network must ensure stable data exchange and device security, so users have been created for remote access.

The thesis project will consist of three sections, which will include the development of logical and physical structure of the network, the choice of network equipment and software, network configuration scenario and project testing. The appendices will specify the configurations of routers and network switches.

KEY WORDS: SECURITY, COMPUTER NETWORK, ENTERPRISE NETWORK, RADIUS, CISCO.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

РЕФЕРАТ.....	4
ABSTRACT.....	5
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	7
ВСТУП.....	8
РОЗДІЛ 1 ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ КОРПОРАТИВНОЇ МЕРЕЖІ КОМПАНІЇ НА БАЗІ ОБЛАДНАННЯ CISCO.....	9
1.1 Особливості побудови корпоративної мережі.....	9
1.2 Протокол маршрутизації OSPF	10
1.3. Протокол DHCP.....	12
1.4. Протокол RADIUS	14
РОЗДІЛ 2 ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ВИБРАНИХ ПРОТОКОЛІВ НА БАЗІ ОБЛАДНАННЯ CISCO	18
2.1 Принципи роботи мережі.....	18
2.2 Розробка логічної структури мережі.....	22
2.3 Вибір обладнання та програмного забезпечення.	26
РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ДОСЛІДЖЕННЯ ПРОЄКТУ ПІДСИСТЕМИ КОРПОРАТИВНОЇ МЕРЕЖІ КОМПАНІЇ НА БАЗІ ОБЛАДНАННЯ CISCO.....	31
3.1 Налаштування мережі.....	31
3.2 Тестування підсистеми захисту корпоративної мережі компанії на базі обладнання Cisco.....	38
3.3 Аналіз результатів тестування.....	42
ВИСНОВКИ	44
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	45
ДОДАТКИ.....	47

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПЗ – програмне забезпечення

ПК – персональний комп'ютер

КМ – комп'ютерна мережі

ОС – операційна система

GNS3 – Graphical Network Simulator-3

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Корпоративна мережа використовується в світі дуже часто, її актуальності немає меж. Вона включає в себе тисячі найрізноманітніших компонентів: комп'ютери різних типів, мережеві адаптери, комутатори та маршрутизатори, кабельну систему. Основним завданням системи є - якнайкраще справлятися з обробкою потоків даних інформації, що циркулюють між співробітниками підприємства і дозволяла їм своєчасно та раціонально приймати рішення.

Корпоративна мережа, зазвичай, є територіально розподіленою, тобто об'єднує офіси, підрозділи та інші структури, що знаходяться на значному віддаленні один від одного. Також при проектуванні корпоративної мережі слід вживати всіх заходів для мінімізації обсягів даних, що передаються.

Для практичної реалізації підсистеми буде використовуватися графічний симулятор GNS3. Щоб забезпечити гетерогенність мережі використовуватимуться різні версії операційних систем Windows та Linux[13].

Метою кваліфікаційної роботи є розробка проєкту корпоративної мережі компанії на базі обладнання Cisco.

Встановлена мета створює наступні завдання:

- аналіз сучасних приладів;
- вибір структури мережі;
- вибір ПЗ для реалізації мережі;
- реалізація підсистеми захисту;

Об'єктом дослідження є здатність системи захистити дані від несанкціонованого доступу та забезпечити швидку передачу даних між пристроями.

Предметом дослідження є методи і засоби захисту корпоративної мережі за допомогою протоколів безпеки.

В процесі виконання кваліфікаційної роботи був розроблений проєкт підсистеми захисту корпоративної мережі компанії на базі обладнання Cisco.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ КОРПОРАТИВНОЇ МЕРЕЖІ КОМПАНІЇ НА БАЗІ ОБЛАДНАННЯ CISCO

1.1 Особливості побудови корпоративної мережі

Корпоративна мережа має великий обсяг пристроїв різного призначення, тому такі великі підсистеми потрібно розділити. Для цього використовується технологія VLAN. VLAN дозволяє зробити сегментацію локальної мережі на підмережі за функціональною ознакою незалежно від територіального розташування пристроїв. Тобто, пристрої однієї підмережі VLAN можуть бути підключені до різних комутаторів, віддалених один від одного. І навпаки, до одного комутатора можуть бути підключені пристрої, що належать до різних підмереж VLAN.

Пристрої з різних підмереж VLAN не можуть спілкуватися один з одним, що зменшує шанси зробити несанкціонований доступ до пристроїв системи. Зв'язок між різними підмережами можливий лише через маршрутизатор. Крім того, використання маршрутизатора дозволяє настроїти політики безпеки, які можуть бути застосовані відразу до всієї групи пристроїв, що належать до однієї підмережі.

Головні фактори які мають бути в корпоративній мережі:

- Продуктивність мережі – час реакції, пропускна спроможність, затримка передачі та варіація затримки передачі даних.
- Надійність – здатність мережі правильно працювати протягом тривалого часу.
- Безпека – здатність системи захистити дані від несанкціонованого доступу.
- Керованість мережі – можливість централізовано контролювати стан основних елементів мережі, виявляти та вирішувати проблеми, що виникають під час роботи мережі.
- Розширюваність – позначає ймовірність щодо легкого додавання окремих елементів мережі(користувачів, комп'ютерів, тощо)

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						9
Змн.	Арк.	№ докум.	Підпис	Дата		

– Масштабованість – означає, що мережа може нарощувати кількість вузлів і протяжність зв'язку у межах, у своїй ефективності мережі не погіршується.

– Прозорість – якість мережі приховувати від користувачів деталі свого внутрішнього пристрою, спрощуючи цим його роботу в мережі.

1.2 Протокол маршрутизації OSPF

OSPF (англ. Open Shortest Path First) - протокол динамічної маршрутизації. Заснований на технології відстеження стану каналу (link-state technology) і використовує для знаходження найкоротшого шляху.

Інформаційний обмін, який здійснюють маршрутизатори для визначення маршруту передачі всередині області, показаний на малюнку (Рис.1.1.) зеленими стрілками. Визначення маршруту та інформаційний обмін між областями в даному випадку проводиться через спеціальну центральну область – AREA 0. Використання такої схеми логічної побудови мережі дозволяє суттєво зменшити частку неінформативного трафіку, що передається каналами передачі даних між областями. Зокрема в цьому випадку каналами, що використовуються для передачі даних між областями, (червоний колір) не буде передаватися інформація про мережі, які мають суто локальне значення.

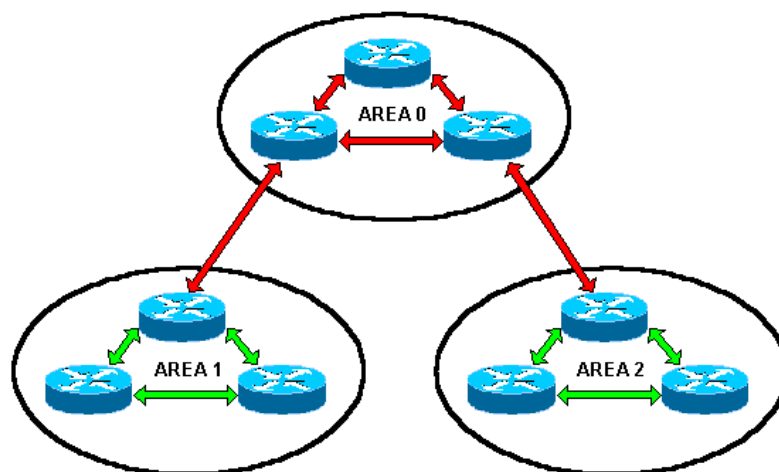


Рис.1.1. Модель маршрутизації

У разі використання протоколу маршрутизації OSPF допускається існування кількох маршрутів у напрямку деякого вузла мережі. У тому випадку, якщо ці маршрути забезпечують однакову якість передачі даних, інформаційний потік на адресу даного вузла може бути направлений по всіх цих каналах одночасно, що забезпечить суттєве збільшення швидкості передачі даних. Динамічне перерозподіл трафіку між паралельними каналами, яке виконується пропорційно до ступеня завантаженості цих каналів, називається Load balancing.

Розглянемо переваги OSPF:

- OSPF легко масштабується, тобто з дуже невеликою кількістю клопоту, ми можемо масштабувати його для використання в дуже великій мережі.
- Перший протокол відкритого найкоротшого шляху має повну підтримку підмереж.
- Використання привітних пакетів: OSPF надсилає невеликі привітні пакети для перевірки операцій зв'язку та ігнорує передачу великих таблиць.
- OSPF Підтримує тегування маршрутів: У OSPF маршрути можна позначати, щоб полегшити взаємодію з довільними значеннями.
- Маршрутизація: OSPF може маршрутизувати пакети залежно від їхнього типу службового поля.

Недоліки OSPF:

- OSPF - це інтенсивно використаний процесор протокол.
- Оскільки в ньому зберігається більше однієї копії інформації про маршрутизацію, вона споживає більше пам'яті.
- OSPF - це більш складний протокол для розуміння та вивчення порівняно з іншими Інтернет-протоколами.

У OSPF всі області повинні бути підключені до магістральної області. Якщо є розрив у безперервності магістралі або магістраль цілеспрямовано розділено, можна встановити віртуальний зв'язок. Двома кінцевими точками віртуального зв'язку є ABR. Віртуальне посилення має бути налаштовано в

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						11
Змн.	Арк.	№ докум.	Підпис	Дата		

обох маршрутизаторах. Інформація про конфігурацію в кожному маршрутизаторі складається з іншої віртуальної кінцевої точки (іншої ABR) і неосновної області, яку мають спільні два маршрутизатори (званої транзитною зоною). Зауважимо, що віртуальні посилення не можна налаштувати через заглушки області.

OSPF використовує найбільшу IP-адресу, налаштовану на інтерфейсах, як ідентифікатор маршрутизатора. Якщо інтерфейс, пов'язаний з цією IP-адресою, коли-небудь виходить з ладу, або якщо адреса видаляється, процес OSPF повинен перерахувати новий ідентифікатор маршрутизатора і повторно надіслати всю інформацію про маршрутизацію його інтерфейсів.

Якщо інтерфейс зворотного зв'язку налаштовано за допомогою IP-адреси, програмне забезпечення Cisco IOS використовуватиме цю IP-адресу як ідентифікатор маршрутизатора, навіть якщо інші інтерфейси мають більші IP-адреси. Оскільки інтерфейси зворотного зв'язку ніколи не вимикаються, досягається більша стабільність у таблиці маршрутизації.

OSPF автоматично віддає перевагу інтерфейсу петлі перед будь-яким іншим типом, і він вибирає найвищу IP-адресу серед усіх інтерфейсів зворотного зв'язку. Якщо інтерфейси зворотного зв'язку відсутні, вибирається найвища IP-адреса в маршрутизаторі. Ми не можемо вказати OSPF використовувати якийсь конкретний інтерфейс.

Спершу як протокол маршрутизації займає важливе місце в інтернет-інфраструктурі. Бути в змозі легко та швидко знайти найкоротший шлях допомагає зменшити непотрібне навантаження на мережу, а можливість знайти інший шлях у разі помилки на оптимальному рівні допомагає підвищити стабільність мережі.

1.3. Протокол DHCP

DHCP – протокол автоматизації призначення IP-адреси клієнту. Він широко використовується у сучасних мережах. Користувачам IP-адреси можуть бути призначені вручну, але це затратно за часом. Тож у 1993 року

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						12
Змн.	Арк.	№ докум.	Підпис	Дата		

розробили протокол DHCP. Він дозволив автоматизувати налаштування IP-адрес, спростити діагностику мережного з'єднання та отримання доступу з однієї підмережі до іншої.

При підключенні клієнта до мережі починається процес його ініціалізації. Користувальницький комп'ютер не має IP-адреси, тому надсилається повідомлення DHCPDISCOVER на всі пристрої в мережі. У тій же мережі обов'язково є DHCP server. Це може бути комутатор чи маршрутизатор.

Спочатку клієнт знаходиться в стані ініціалізації (INIT) і не має власної IP-адреси. Тому він відправляє широкомовне повідомлення DHCPDISCOVER на всі пристрої в локальній мережі. У тій же локальній мережі є DHCP-сервер. DHCP-сервер - це, наприклад, маршрутизатор або комутатор, існують також виділені DHCP-сервери.

Не завжди одну мережу обслуговує один DHCP-сервер, часто організації встановлюють відразу кілька. Сервер завжди слухає 67 порт, очікує широкомовне повідомлення від клієнта, а після його отримання відправляє пропозицію у відповідь — DHCPOFFER. Клієнт приймає повідомлення на 68 портів.

DHCP-сервер відповідає на пошук пропозицією, повідомляє IP, який може підійти клієнту. IP виділяються з області (SCOPE) доступних адрес, що задається адміністратором.

Якщо є адреси, які не повинні бути призначені DHCP-сервером, область можна обмежити, вказавши лише дозволені адреси. Наприклад, адміністратор може встановити діапазон використовуваних IP-адрес від 192.168.1.10 до 192.168.1.255.

Буває і так, що не всі доступні адреси мають бути призначені для клієнтів. Наприклад, адміністратор може виключити (exclude) діапазон 192.0.0.100 - 192.0.0.200 з використовуваної області. Таке обмеження називається винятком.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						13
Змн.	Арк.	№ докум.	Підпис	Дата		

DHCP виділяє доступні IP-адреси з області лише тимчасово, тому немає гарантії, що при наступному підключенні даного клієнта залишиться колишній IP. Але є можливість призначити будь-якому клієнту певний IP назавжди. Наприклад, забронювати 192.0.0.10 за комп'ютером системного адміністратора. Таке збереження IP окремих клієнтів називають резервацією (reservation).

DHCP має вразливість. Основна полягає у чотирьох кроках, необхідних для отримання IP. Процес DORA передбачає розсилку повідомлень широкомовного типу, коли перший DHCP-сервер, що відгукнувся, отримує можливість запропонувати IP зі своєї області. Якщо зломисник зможе використовувати свій сервер, який дасть найшвидшу відповідь клієнту, то в нього відкриється можливість отримати контроль над діями користувача в мережі та завдати істотних збитків.

Ще один проломом у безпеці - у тому, що DHCP використовує UDP-протокол. UDP – протокол обміну датаграмами без встановлення з'єднання, а отже, і без шифрування. Інформація, що передається по UDP, не захищена і може бути «підслухана», що також може бути використане зломисниками.

Третій недолік - знову ненадійність UDP, але іншого. UDP не забезпечує гарантії доставки інформації. Цей протокол допускає втрати та помилки, які можуть позначитися на роботі DHCP, зокрема при PXE-завантаженні.

1.4. Протокол RADIUS

RADIUS (Віддалена аутентифікація Dial-In Service) — стандарт IETF для AAA. Спочатку використовувався для розширення рівня 2 протоколу "точка-точка" (PPP) між кінцевими користувачами і сервером доступу до мережі (NAS), щоб передавати аутентифікований трафік з NAS на сервер AAA. Дайджести для аутентифікації та авторизації додаються до одного типу пакетів, а виставлення рахунків обробляється окремими процесами[10].

Cisco підтримує RADIUS відповідно до своєї парадигми безпеки автентифікації, авторизації та обліку (AAA). RADIUS можна використовувати

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						14
Змн.	Арк.	№ докум.	Підпис	Дата		

з іншими протоколами безпеки AAA, такими як TACACS+, Kerberos та локальний пошук імені користувача. Усі платформи Cisco підтримують RADIUS, але деякі функції, які підтримують RADIUS, доступні лише на певних платформах.

Використовувати RADIUS у таких мережових середовищах, де потрібна безпека доступу:

- Мережа з серверами доступу від кількох постачальників, кожен з яких підтримує RADIUS. Наприклад, сервер доступу від кількох постачальників використовує єдину базу даних безпеки на основі сервера RADIUS. У IP-мережі з серверами доступу кількох постачальників користувачі, які підключаються до телефонів, аутентифікуються через сервер RADIUS, налаштований для роботи із системою безпеки Kerberos.

- Додаток підтримує готові середовища мережевої безпеки з підтримкою RADIUS, наприклад системи контролю доступу за допомогою смарт-карт. В одному випадку RADIUS використовується з картками безпеки Enigma для автентифікації користувачів і надання доступу до мережових ресурсів.

- Мережа, яка вже використовує RADIUS. Ви можете додати пристрої Cisco RADIUS до своєї мережі. Це може бути вашим першим кроком у переході на сервер TACACS+.

- Користувач може отримати доступ до мережі лише для однієї послуги. Використовуючи RADIUS, ви можете контролювати доступ користувачів до одного хоста, однієї утиліти (наприклад, Telnet) або окремого протоколу (наприклад, PPP). Наприклад, коли користувач входить в систему, RADIUS ідентифікує користувача як уповноваженого ініціювати PPP з IP-адресою 10.2.3.4, і ініціює певний список доступу.

- Мережі, що вимагають обліку ресурсів. Ми можемо використовувати облік RADIUS незалежно від автентифікації або авторизації RADIUS. Функція обліку RADIUS дозволяє надсилати дані на початку та наприкінці служби, вказуючи на кількість ресурсів (таких як час, пакети та байти), використаних

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						15
Змн.	Арк.	№ докум.	Підпис	Дата		

під час сеансу. Провайдери можуть використовувати безкоштовні версії програмного забезпечення для контролю доступу та обліку RADIUS для особливих потреб безпеки та обліку.

– Підтримує мережі з попередньою автентифікацією. Використовуючи сервер RADIUS у вашій мережі, ми можете налаштувати попередню автентифікацію AAA та налаштувати профіль попередньої автентифікації. Попередня автентифікація дозволяє постачальникам послуг використовувати свої існуючі рішення RADIUS для кращого керування портами та ефективного керування використанням спільних ресурсів для надання різних угод про рівень обслуговування.

Після того, як ми визначили сервер RADIUS і визначили ключ автентифікації RADIUS, нам потрібно визначити список методів для автентифікації RADIUS. Оскільки AAA полегшує автентифікацію RADIUS, ми повинні ввести команду автентифікації aaa, вказуючи RADIUS як метод автентифікації.

Облік AAA дозволяє відстежувати доступ до послуг користувачів і кількість мережевих ресурсів, які вони споживають. Оскільки AAA полегшує облік RADIUS, ми повинні ввести команду aaa accounting, вказуючи RADIUS як метод обліку.

Авторизація AAA дозволяє встановити параметри, які обмежують доступ користувачів до мережі. Авторизація RADIUS забезпечує метод віддаленого контролю доступу, включаючи одноразову авторизацію або авторизацію для кожної служби, список облікових записів і профілів для кожного користувача, підтримку груп користувачів і підтримку IP, IPX, AppleTalk Remote Access (ARA) і віддалений вхід. Оскільки авторизація RADIUS надається AAA, ви повинні ввести команду авторизації aaa, вказуючи RADIUS як метод авторизації.

Сервери безпеки RADIUS ідентифікуються на основі їх імені хоста чи IP-адреси, імені хосту та конкретних номерів порту UDP або IP-адреси та конкретних номерів порту UDP. Комбінація IP-адреси та номера порту UDP

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						16
Змн.	Арк.	№ докум.	Підпис	Дата		

створює унікальний ідентифікатор, що дозволяє окремо визначати різні порти як хости RADIUS, що надають конкретну послугу AAA. Цей унікальний ідентифікатор дозволяє надсилати запити RADIUS на декілька портів UDP на сервері з однією IP-адресою. Якщо два різні записи хоста на одному сервері RADIUS налаштовано для однієї служби — наприклад, обліку — другий налаштований запис хосту діє як резервна копія для перемикання збоїв до першого. Якщо перший запис хосту не надає облікові послуги, сервер доступу до мережі намагається виконати другий запис хосту, налаштований на тому ж пристрої для облікових послуг.

Сервер RADIUS і пристрій Cisco використовують загальний секретний текстовий рядок для шифрування паролів та обміну відповідями. Щоб налаштувати RADIUS на використання команд безпеки AAA, ми повинні вказати хост, на якому запущено демон сервера RADIUS, і секретний текстовий рядок (ключ), який він спільно використовує з пристроєм.

Висновки до розділу 1

В результаті аналізу особливостей корпоративної мережі було визначено основні принципи побудови схеми та методи її захисту. Потрібно розробити підсистему корпоративної мережі з вищим рівнем безпеки.

Було обрано протокол маршрутизації OSPF та протокол DHCP для автоматичного призначення IP-адреси для пристроїв. Також RADIUS який буде контролювати доступ до хосту.

З обладнання будемо використовувати провідного виробника – CISCO, так як на пристроях даної фірми можна налаштувати всі обрані протоколи та технології. Для створення саме корпоративної мережі буде задіяний симулятор GNS3, який дозволить забезпечити взаємодію комунікаційних пристроїв та віртуальних машин з обраними операційними системами.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						17
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ВИБРАНИХ ПРОТОКОЛІВ НА БАЗІ ОБЛАДНАННЯ CISCO

2.1 Принципи роботи мережі

Так як корпоративна мережа складається з великої кількості пристроїв, то потрібно її розділити на LAN. VLAN поділяє підсистеми на окремі широкомовні домени. Це означає, що широкомовні повідомлення будуть отримувати лише пристрої, що знаходяться в одній мережі VLAN. Побудова системи з використанням технології VLAN дозволяє зменшити широкомовний трафік усередині мережі, тим самим знижується навантаження на мережеві пристрої та покращується продуктивність системи загалом.

В мережі буде використовуватися велика кількість пристроїв яким потрібно швидко надати IP-адреси, тому для цього використаємо протокол DHCP. Керувати буде маршрутизатор DHCPRouter.

В схемі буде багато підмереж, тому потрібно зробити IP-топологію. Для цього буде використано протокол OSPF. OSPF використовує найбільшу IP-адресу, налаштовану на інтерфейсах, як ідентифікатор маршрутизатора. Якщо інтерфейс, пов'язаний з цією IP-адресою, коли-небудь виходить з ладу, або якщо адреса видаляється, процес OSPF повинен перерахувати новий ідентифікатор маршрутизатора і повторно надіслати всю інформацію про маршрутизацію його інтерфейсів.

Також для швидкого доступу та налаштування пристроїв буде використано протокол RADIUS. Для його роботи потрібно провести налаштування аутентифікації AAA. Коротко, клієнт AAA відправляє вчені дані до сервера аутентифікації, і спираючись на його відповідь (або відсутність відповіді) приймає рішення про відмову або надання запиту. Відповідно до налаштованих політик AAA, пристрій запитує логін і пароль, після чого передає логін і хеш пароля RADIUS серверу.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						18
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 2.1

Розподілення на підмережі пристроїв мережі

Назва мережі	Кількість робочих станцій	DHCP-сервер
LAN10	1 робоча станція (Можливість додавання робочих станцій)	Сервер під керуванням Windows 10 Server
LAN20	1 робоча станція (Можливість додавання робочих станцій)	Маршрутизатор
LAN40	1 робоча станція (Можливість додавання робочих станцій)	Маршрутизатор
LAN50	1 робоча станція (Можливість додавання робочих станцій)	Маршрутизатор
LAN70	1 робоча станція (Можливість додавання робочих станцій)	Маршрутизатор
LAN80	1 робоча станція (Без можливості додавання робочих станцій)	Маршрутизатор

Таблиця 2.2

Адресація мережі

Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Підмережа А	-	192.168.1.0	255.255.255.0	/24
Підмережа В	-	192.168.2.0	255.255.255.0	/24
Підмережа С	-	192.168.3.0	255.255.255.0	/24
Підмережа D	-	192.168.4.0	255.255.255.0	/24
Підмережа E	-	192.168.5.0	255.255.255.0	/24
Підмережа 10	-	192.168.10.0	255.255.255.0	/24
Підмережа 20	-	192.168.20.0	255.255.255.0	/24
Підмережа 30	-	192.168.30.0	255.255.255.0	/24

Адресація мережі

Продовження таблиці 2.2

Підмережа 40	-	192.168.40.0	255.255.255.0	/24
Підмережа 50	-	192.168.50.0	255.255.255.0	/24
Підмережа 60	-	192.168.60.0	255.255.255.0	/24
Підмережа 70	-	192.168.70.0	255.255.255.0	/24
Підмережа 80	-	192.168.80.0	255.255.255.0	/24
Підмережа 90	-	192.168.90.0	255.255.255.0	/24
Інтернет підключення				
Маршрутизатор EDGERouter_1	e2/0	192.168.50.1	255.255.255.0	/24
	g1/0	192.168.2.1	255.255.255.0	/24
Маршрутизатор EDGERouter_2	g1/0	192.168.2.2	255.255.255.0	/24
	e2/1	192.168.3.8	255.255.255.0	/24
	e2/2	192.168.5.2	255.255.255.0	/24
Комутатор ServerSW	Vlan 3	192.168.3.5	255.255.255.0	/24
	Vlan 4	192.168.4.6	255.255.255.0	/24
Комутатор DMZSwitch	Vlan 5	192.168.5.1	255.255.255.0	/24
Server-Ubuntu	e0	192.168.5.3	255.255.255.0	/24
RADIUS	e0	192.168.3.6	255.255.255.0	/24
Комутатор Core1	Vlan 4	192.168.4.5	255.255.255.0	/24
Комутатор Core2	Vlan 4	192.168.4.3	255.255.255.0	/24
Комутатор Core 3	Vlan 3	192.168.3.2	255.255.255.0	/24
Комутатор Core 4	Vlan 4	192.168.4.2	255.255.255.0	/24

Адресація мережі

Продовження таблиці 2.2

DHCPRouter	e1/0	192.168.3.1	255.255.255.0	/24
	e1/1	192.168.4.1	255.255.255.0	/24
	e2/0	192.168.30.1	255.255.255.0	/24
	e2/1	192.168.60.1	255.255.255.0	/24
	e2/2	192.168.90.1	255.255.255.0	/24
Рівень доступу і розподілу				
Комутатор Dis1	Vlan 30	192.168.30.2	255.255.255.0	/24
	Vlan 10	192.168.10.1	255.255.255.0	/24
	Vlan 20	192.168.20.1	255.255.255.0	/24
Комутатор Dis2	Vlan 60	192.168.60.2	255.255.255.0	/24
	Vlan 40	192.168.40.1	255.255.255.0	/24
	Vlan 50	192.168.50.1	255.255.255.0	/24
Комутатор Dis3	Vlan 90	192.168.90.2	255.255.255.0	/24
	Vlan 70	192.168.70.1	255.255.255.0	/24
	Vlan 80	192.168.80.1	255.255.255.0	/24
Комутатор Асс1	Vlan 10	192.168.10.2	255.255.255.0	/24
Робоча станція PC1	e0	DHCP		
Комутатор Асс2	Vlan 20	192.168.20.2	255.255.255.0	/24
Робоча станція PC2	e0	DHCP		
Комутатор Асс3	Vlan 40	192.168.40.2	255.255.255.0	/24
Робоча станція PC3	e0	DHCP		

Адресація мережі

Продовження таблиці 2.2

Комутатор Асс4	Vlan 50	192.168.50.2	255.255.255.0	/24
Робоча станція PC4	e0	DHCP		
Комутатор Асс5	Vlan 70	192.168.70.2	255.255.255.0	/24
Робоча станція PC5	e0	DHCP		
Комутатор Асс6	Vlan 80	192.168.80.2	255.255.255.0	/24
Робоча станція ADMIN	e0	DHCP		

2.2 Розробка логічної структури мережі

В схемі використано корпоративну модель мережі яка забезпечить продуктивність, надійність мережі. В яку входить 5 рівнів: ядро з DHCP сервером, Data Center, DMZ, розподілу та доступу, а також інтернет з'єднання.

Ядро забезпечить швидку передачу даних між комутаторами. Також буде налаштовано DHCP сервер, який автоматично буде роздавати IP-адреси і інші параметри для пристроїв.

Data Center зберігає користувачів та паролі завдяки протоколу RADIUS. Також було додано комутатор L3 який буде підтримувати зв'язок з мережею.

Рівень розподілу забезпечить маршрутизацію мережі, також було налаштовано DHCP-relay для отримання IP-адреси між VLAN.

Загальний вигляд моделі наведено на рисунку 2.1.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						22
Змн.	Арк.	№ докум.	Підпис	Дата		

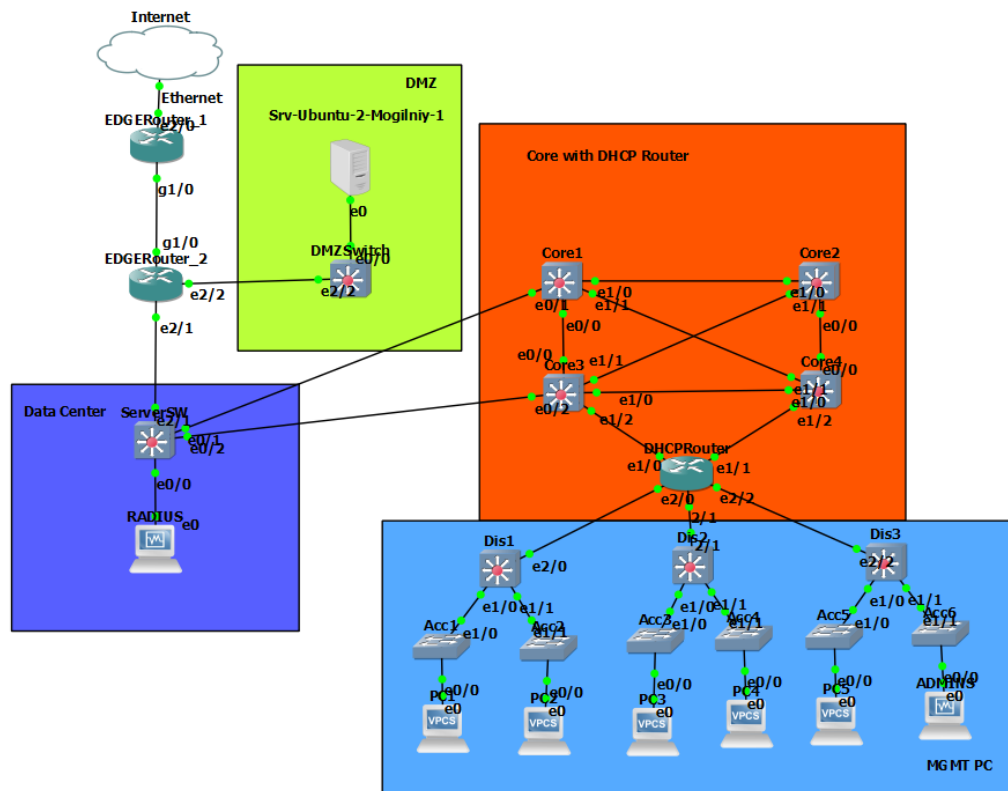


Рис.2.1. Корпоративна модель мережі

Для кращого розуміння моделі розглянемо всі рівні мережі окремо. Всі наведенні рівні знаходяться на рисунках (Рис2.2 – Рис.2.8).

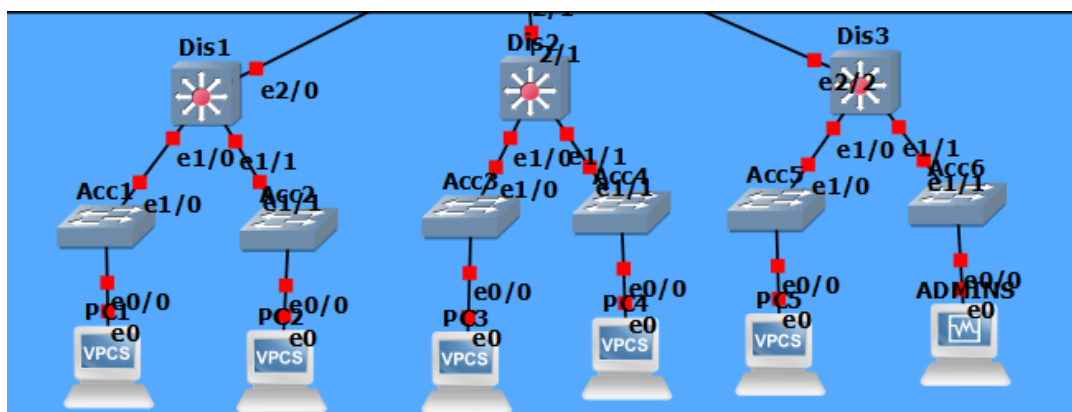


Рис.2.2. Рівні доступу та розподілу з робочими станціями

Таблиця 2.3

Рівні доступу та розподілу з робочими станціями

Комутатори	Switch L3 (i86bi-linux-l3-tpgen- ipbase-12.4.bin) Switch L2 (i86bi-linux-l2- adventerprisek9-15.1a.bin)
Робочі станції	Windows 7

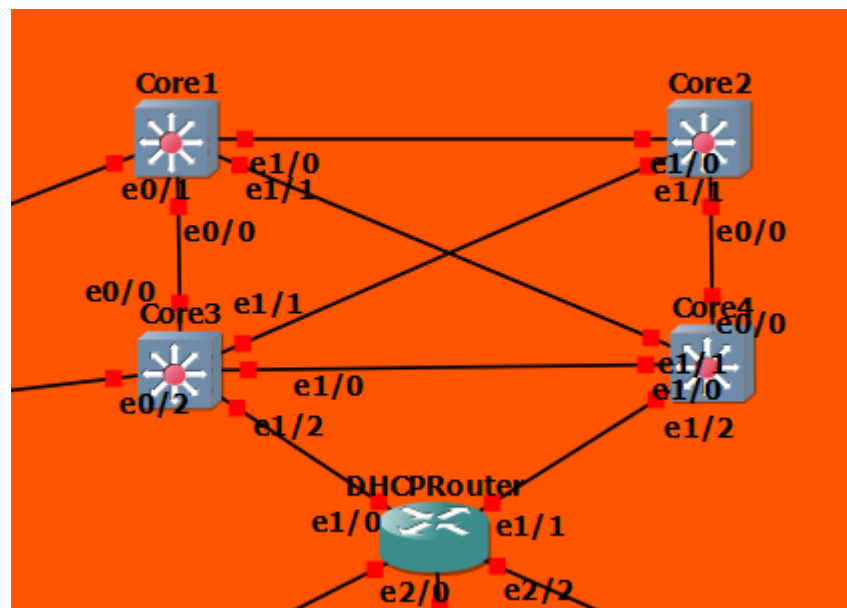


Рис.2.3. Ядро та DHCP-сервер

Таблиця 2.4

Ядро та DHCP-сервер

Комутатори	Switch L3 (i86bi-linux-l3-tpgen- ipbase-12.4.bin)
Маршрутизатори	c7200(c7200-adventerprisek9_sna- mz.150-1.M3.image)

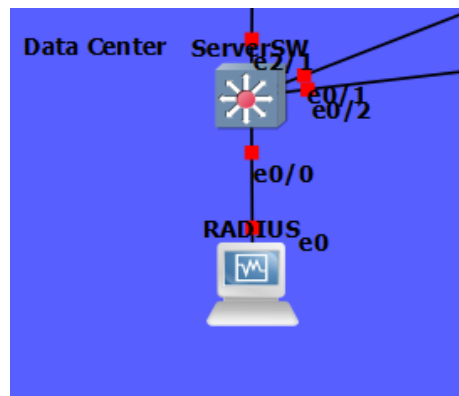


Рис.2.4. Data Center

Таблиця 2.5

Пристрої, що входять до складу Data Center

Комутатори	Switch L3 (i86bi-linux-l3-tpgen-ipbase-12.4.bin)
Робочі станції	RADIUS

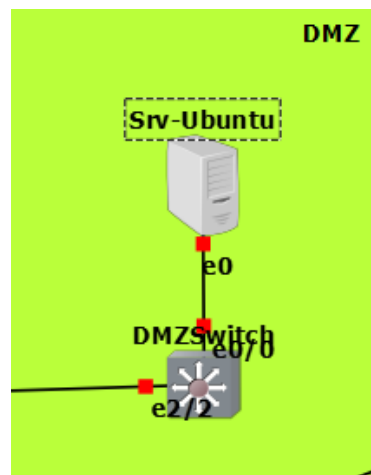


Рис.2.5. Модель DMZ

Таблиця 2.6

Пристрої моделі DMZ

Комутатори	Switch L3 (i86bi-linux-l3-tpgen-ipbase-12.4.bin)
Робочі станції	Ubuntu

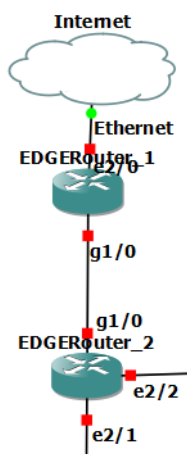


Рис.2.6. Інтернет з'єднання

Таблиця 2.7

Пристрої інтернет з'єднання

Маршрутизатори	c7200(c7200-adventerprisek9_sn- mz.150-1.M3.image)
----------------	---

2.3 Вибір обладнання та програмного забезпечення.

До потреб, що зазначені вище, було сформовані вимоги до програмного забезпечення:

- Налаштування DHCP сервера.
- Наявність захищеного доступу до робочих станцій.
- Сервер RADIUS.
- Списки доступу

Захищеність мережі буде забезпечуватися: доступом паролем та створенням користувачів за допомогою RADIUS, який буде зашифровувати паролі.

Для реалізації схеми будемо використовувати обладнання фірми CISCO. Основними напрямленнями CISCO є:

- Багатофункціональні маршрутизатори
- Потужні, розумні комутатори
- Пристрої активного захисту – ASA, ACE

- Системи запобігання вторгненням – IPS
- Системи централізованого бездротового доступу
- Уніфіковані комунікації (VoIP, відеоконференції, telepresence, системи керування дзвінками)
- Системи централізованого захисту хостів (CSA)
- Система контролю доступу (NAC)

Головне - cisco не зупиняється на досягнутому і «тримає ніс за вітром», вкладаючи гроші в перспективні напрямки та вигадуючи нові, наприклад, купуючи перспективні розробки та вбудовуючи їх у свої рішення.

Особливості обладнання CISCO є:

- Надійність - ламається все, питання лише коли. Надійність Cisco перевірена роками успішної експлуатації.
- Гнучкість - одне і те ж залізо, залежно від операційної системи та набивання модулями, може виконувати абсолютно різні функції: захисні, шлюза уніфікованих комунікацій, сервісні... А це означає, що якщо захочеться чогось нового, є великий шанс нічого не купувати, а просто набрати кілька команд.
- Взаємозалежність - різне залізо, що виконують різні функції, можуть залежати один від одного та керувати один одним. Це дозволяє зробити мережу живим організмом, а чи не набором розрізнених пристроїв.
- Налагодження - дуже важливо для налаштування та налаштувачів: найширші можливості пошуку несправностей, вбудовані практично у всі пристрої Cisco.
- Інтелектуальність - всі пристрої Cisco містять широкий спектр технологій, протоколів, ідеологій як стандартних, так і своїх власних, що дозволяють розширити можливості мережі.

Отже, можна зробити висновок, що прилади фірми CISCO є досить гнучкими з точки зору налаштувань і надійності як для великих корпорацій, так і для невеликих бізнесів. Тому ми будемо використовувати образи маршрутизатора серії 7200 (рис.2.7) та комутатора 9300 (рис.2.8).

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						27
Змн.	Арк.	№ докум.	Підпис	Дата		

Для створення моделі копоративної мережі будемо використовувати програму GNS3. Додатково використовується програма VirtualBox, а також WireShark для перевірки трафіку в нашій мережі.



Рис.2.7. Маршрутизатор серії (Cisco 7200)



Рис. 2.8. Комутатор серії (Cisco Catalyst серії 9300)

Graphical Network Simulator. Якщо перекласти дослівно – графічний симулятор мережі. Він дозволяє створювати різні мережеві топології прямо на вашому комп'ютері. Найчастіше GNS використовується як лабораторний стенд, де можна перевірити ту чи іншу технологію або схему[18].

Емулятор дозволяє створити модель комп'ютера або іншого пристрою та запускати всередині оригінальне програмне забезпечення. Емулюються всі основні компоненти пристрою, у тому числі процесор, пам'ять та пристрої введення/виводу. У випадку Cisco, емулятор створює модель маршрутизатора і запускає всередині реальну операційну систему Cisco IOS. Таким чином, ми отримуємо повнофункціональний маршрутизатор.

Перша і найголовніша причина чому саме GNS3 – повний функціонал емульованих пристроїв. Тобто, запустивши той самий маршрутизатор Cisco, нам будуть доступні практично всі функції, які працюють на реальному

маршрутизаторі. Якщо згадати Cisco Packet Tracer, то значної частини функціоналу недоступна, так як це лише симулятор.

Можливість побудови гетерогенних мереж. Мається на увазі, що ми можемо зібрати схему, де будуть не тільки пристрої Cisco, але і Juniper, Mikrotik, CheckPoint і т.д.

Додавання в мережу повноцінних робочих станцій та серверів. Знову ж таки, якщо згадати Cisco Packet Tracer, то там як кінцеві пристрої були доступні клієнтські комп'ютери або сервери з дуже обмеженим функціоналом. У GNS3 ми можемо додати повноцінний комп'ютер із Windows 7 або Ubuntu. Можемо використовувати у схемі Windows Server або RedHat. Робиться це за допомогою технологій віртуалізації (VirtualBox або VMWare) або підключивши GNS3 до реальної мережі. Таким чином ми можемо перевірити в лабораторній роботі встановлення VPN клієнта на робочу станцію, автентифікацію користувачів через сервер AAA, використовувати цей браузер при підключенні до цього Інтернету. Загалом, що завгодно, як у реальному житті.

VirtualBox – це програмне забезпечення, яке імітує справжній комп'ютер, що дає можливість користувачеві встановлювати, запускати та використовувати інші операційні системи, як звичайні програми. Такий собі комп'ютер у комп'ютері[19].

Віртуальна машина створює якесь ізольоване оточення на комп'ютері, яке складається з віртуальних компонентів реального ПК: жорсткого диска, відеокarti, оперативної пам'яті, різноманітних контролерів пристроїв тощо. Таким чином, встановлена в VirtualBox операційна система буде повністю впевнена, що вона працює на реальному залізі.

Способів застосування віртуальних машин є безліч. Розглянемо найпопулярніші серед звичайних користувачів:

– Ознайомлення з іншими операційними системами. Незалежно від того, яка операційна система встановлена на вашому комп'ютері, у VirtualBox можна встановити будь-яку з підтримуваних нею, а це безліч дистрибутивів

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						29
Змн.	Арк.	№ докум.	Підпис	Дата		

Linux, FreeBSD, MacOS, будь-яка з версій Windows, Android та інші. Не треба боятися того, що такою установкою ви зламаєте реальну систему, або видалить важливі дані - віртуальна машина працює ізольовано і ви можете експериментувати з нею як забажаєте. Коли вона вам буде більше не потрібна, просто видалить, і вона не залишить жодних слідів за собою;

– Ще один спосіб застосування VirtualBox – необхідність запуску програми, яка не працює у вашій основній ОС або її версії. Наприклад ви працюєте у Windows і вам знадобилася програма, яка доступна лише під Linux. Іноді єдиним виходом буде встановлення Linux у VirtualBox та використання потрібного ПЗ звідти. Детальна ситуація може бути, коли вам потрібна програма, що працює лише під старими версіями Windows;

– Тестування різного ПЗ. Може статися так, що вам знадобиться скористатися якоюсь програмою, або вам загалом часто доводиться тестувати різні програми, при цьому ви не особливо бажаєте засмічувати свою робочу машину. Знову ж таки, на допомогу прийде VirtualBox. Крім того, використовуючи віртуальну машину, ви можете не боятися заразити свій комп'ютер вірусами, навіть якщо таке станеться із запущеною у VirtualBox ОС.

Висновки до розділу 2

Спроекували модель підмережі, що складається з ядра, розподілу і доступу, DHCP сервера, інтернет з'єднання, RADIUS сервера. Також було сформовано таблиці розподілу мережі та адресацію.

Обрано пристрої, які будуть використовуватися на рівні ядра як найпотужніші. Описані можливості обладнання, які можуть бути застосовані для поставлених завдань. Також обґрунтовано вибір програмного забезпечення, зокрема симулятора, в якому буде створена мережа, та операційних систем, що будуть використовуватися для забезпечення гетерогенності мережі.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						30
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ДОСЛІДЖЕННЯ ПРОЄКТУ ПІДСИСТЕМИ КОРПОРАТИВНОЇ МЕРЕЖІ КОМПАНІЇ НА БАЗІ ОБЛАДНАННЯ CISCO.

3.1 Налаштування мережі

В даному пункті розглянуто основні налаштування пристроїв мережі. Спочатку повністю складемо схему, яку спроектували в попередньому розділі (рис.3.1).

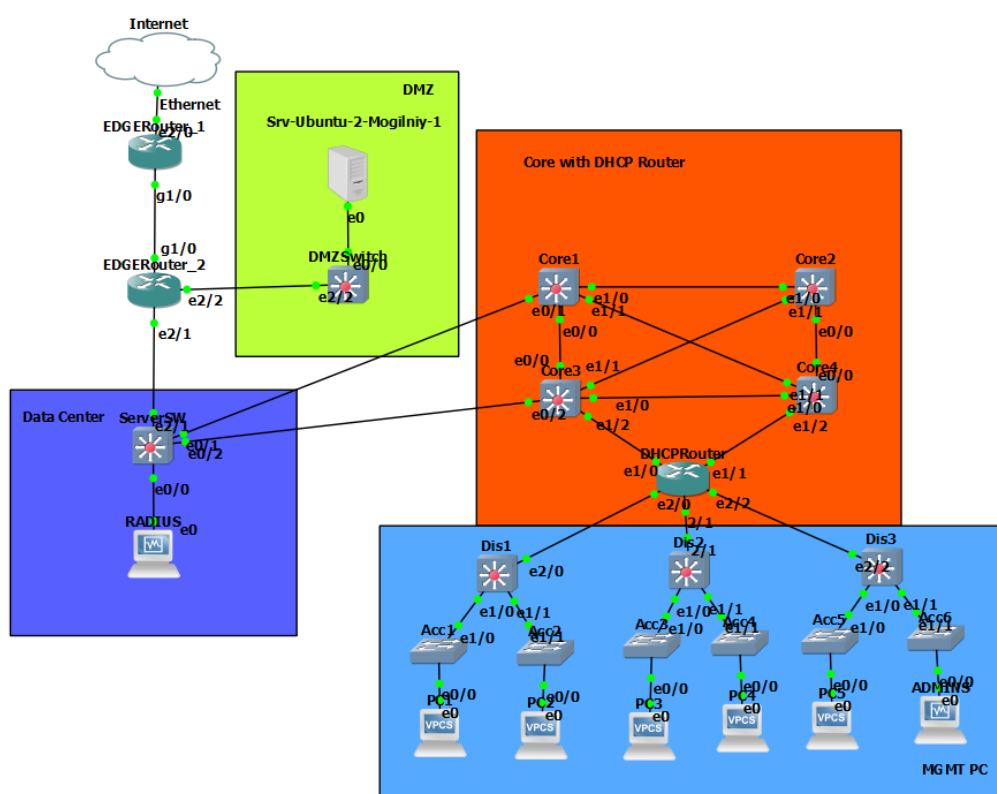


Рис. 3.1. Повна схема мережі

Для початку налаштуємо рівні розподілу та доступу. Для цього було використано протокол VLAN. Пристрої, що знаходяться у різних VLAN, будуть знаходитися у різних підмережах. Але водночас VLAN не прив'язаний до розташування пристроїв і тому пристрої, що знаходяться на відстані один від одного, все одно можуть бути в одному VLAN незалежно від розташування.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						31
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Acc1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Acc1(config)#vlan 10
Acc1(config-vlan)#name OFFICE_1
Acc1(config-vlan)#exit
Acc1(config)#int vlan 10
Acc1(config-if)#ip address 192.168.10.2 255.255.255.0
Acc1(config-if)#no shut
Acc1(config-if)#exit
Acc1(config)#int e1/0
Acc1(config-if)#switchport mode access
Acc1(config-if)#switchport access vlan 10
Acc1(config-if)#exit
Acc1(config)#int e0/0
Acc1(config-if)#switchport mode access
Acc1(config-if)#switchport access vlan 10
Acc1(config-if)#exit

```

Рис. 3.2. Налаштування VLAN на комутаторі доступу

На всіх інших комутаторах доступу налаштування виконувалося аналогічно.

Тепер потрібно провести налаштування комутатора розподілу та підключити його до комутатора доступу та DHCP сервера.

```

Dis1(config)#vlan 10
Dis1(config-vlan)#name OFFICE_1
Dis1(config-vlan)#exit
Dis1(config)#vlan 20
Dis1(config-vlan)#name OFFICE_2
Dis1(config-vlan)#exit
Dis1(config)#vlan 30
Dis1(config-vlan)#name DHCP_Router
Dis1(config-vlan)#exit
Dis1(config)#int vlan 30
Dis1(config-if)#ip address 192.168.30.2 255.255.255.0
Dis1(config-if)#no shut
Dis1(config-if)#int vlan 10
Dis1(config-if)#ip address 192.168.10.1 255.255.255.0
Dis1(config-if)#ip helper-address 192.168.30.1
Dis1(config-if)#no shut
Dis1(config-if)#exit
Dis1(config)#int vlan 20
Dis1(config-if)#ip address 192.168.20.1 255.255.255.0
Dis1(config-if)#ip helper-address 192.168.30.1
Dis1(config-if)#no shut
Dis1(config-if)#exit
Dis1(config)#int e1/0
Dis1(config-if)#description LINK_TO_ACC1
Dis1(config-if)#switchport mode access
Dis1(config-if)#switchport access vlan 10
Dis1(config-if)#no shut
Dis1(config-if)#exit
Dis1(config)#int e1/1
Dis1(config-if)#description LINK_TO_ACC2
Dis1(config-if)#switchport mode access
Dis1(config-if)#switchport access vlan 20
Dis1(config-if)#no shut
Dis1(config-if)#int e2/0
Dis1(config-if)#description LINK_TO_DHCPRROUTER
Dis1(config-if)#switchport mode access
Dis1(config-if)#switchport access vlan 30
Dis1(config-if)#no shut
Dis1(config-if)#exit

```

Рис. 3.3. Налаштування VLAN на комутаторі розподілу

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						32
Змн.	Арк.	№ докум.	Підпис	Дата		

Наступним кроком буде налаштування динамічної маршрутизації в якому використано протокол OSPF. Зупинимося на цьому трішки детальніше.

Командою `network` ми ставимо не ту мережу, що мовитиме наш маршрутизатор, ми визначаємо інтерфейси, що беруть участь у процесі.

Всі інтерфейси маршрутизатора, IP адреси яких потрапляють до налаштованого діапазону 192.168.10.0 0.0.0.255 (192.168.10.0-192.168.10.255), включатися до процесу. Це означає що з даних інтерфейсів будуть розсилатися Hello-повідомлення, через них встановлюватимуться відносини сусідства та відправлятимуться оновлення про топологію мережі.

```
Dis1(config)#router ospf 1
Dis1(config-router)#network 192.168.10.0 0.0.0.255 area 0
Dis1(config-router)#network 192.168.20.0 0.0.0.255 area 0
Dis1(config-router)#network 192.168.30.0 0.0.0.255 area 0
Dis1(config-router)#exit
Dis1(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.2
Dis1(config)#ip route 0.0.0.0 0.0.0.0 192.168.20.2
Dis1(config)#ip route 0.0.0.0 0.0.0.0 192.168.30.1
```

Рис. 3.4. Налаштування OSPF на комутаторі Dis1

Також виконаємо аналогічне налаштування маршрутизації на сервері DHCP.

```
DHCPRouter(config)#int e2/0
DHCPRouter(config-if)#ip address 192.168.30.1 255.255.255.0
DHCPRouter(config-if)#no shut
DHCPRouter(config-if)#exit
DHCPRouter(config)#int e2/1
DHCPRouter(config-if)#ip address 192.168.60.1 255.255.255.0
DHCPRouter(config-if)#no shut
DHCPRouter(config-if)#exit
DHCPRouter(config)#int e2/2
DHCPRouter(config-if)#ip address 192.168.90.1 255.255.255.0
DHCPRouter(config-if)#no shut
DHCPRouter(config-if)#exit
DHCPRouter(config)#int e1/0
DHCPRouter(config-if)#ip address 192.168.3.1 255.255.255.0
DHCPRouter(config-if)#no shut
DHCPRouter(config-if)#exit
DHCPRouter(config)#int e1/1
DHCPRouter(config-if)#ip address 192.168.4.1 255.255.255.0
DHCPRouter(config-if)#no shut
DHCPRouter(config-if)#exit
DHCPRouter(config)#router ospf 1
DHCPRouter(config-router)#network 192.168.10.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.20.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.30.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.40.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.50.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.60.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.70.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.80.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.90.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.3.0 0.0.0.255 area 0
DHCPRouter(config-router)#network 192.168.4.0 0.0.0.255 area 0
DHCPRouter(config-router)#exit
DHCPRouter(config)#ip route 0.0.0.0 0.0.0.0 192.168.30.2
DHCPRouter(config)#ip route 0.0.0.0 0.0.0.0 192.168.60.2
DHCPRouter(config)#ip route 0.0.0.0 0.0.0.0 192.168.90.2
DHCPRouter(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.2
DHCPRouter(config)#ip route 0.0.0.0 0.0.0.0 192.168.4.2
```

Рис.3.5. Налаштування DHCP-сервера

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						33
Змн.	Арк.	№ докум.	Підпис	Дата		

Перейдемо до налаштування DHCP протоколу. Який забезпечить автоматичне призначення IP-адреси до робочих станцій.

```
DHCPRouter(config)#ip dhcp pool OFFICE_1
DHCPRouter(dhcp-config)#network 192.168.10.0 255.255.255.0
DHCPRouter(dhcp-config)#default-router 192.168.10.1
DHCPRouter(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCPRouter(dhcp-config)#exit
DHCPRouter(config)#ip dhcp pool OFFICE_2
DHCPRouter(dhcp-config)#network 192.168.20.0 255.255.255.0
DHCPRouter(dhcp-config)#default-router 192.168.20.1
DHCPRouter(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCPRouter(dhcp-config)#exit
DHCPRouter(config)#ip dhcp pool OFFICE_3
DHCPRouter(dhcp-config)#network 192.168.40.0 255.255.255.0
DHCPRouter(dhcp-config)#default-router 192.168.40.1
DHCPRouter(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCPRouter(dhcp-config)#exit
DHCPRouter(config)#ip dhcp pool OFFICE_4
DHCPRouter(dhcp-config)#network 192.168.50.0 255.255.255.0
DHCPRouter(dhcp-config)#default-router 192.168.50.1
DHCPRouter(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCPRouter(dhcp-config)#exit
DHCPRouter(config)#ip dhcp pool OFFICE_5
DHCPRouter(dhcp-config)#network 192.168.70.0 255.255.255.0
DHCPRouter(dhcp-config)#default-router 192.168.70.1
DHCPRouter(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCPRouter(dhcp-config)#exit
DHCPRouter(config)#ip dhcp pool ADMINS
DHCPRouter(dhcp-config)#network 192.168.80.0 255.255.255.0
DHCPRouter(dhcp-config)#default-router 192.168.80.1
DHCPRouter(dhcp-config)#dns-server 8.8.8.8 8.8.4.4
DHCPRouter(dhcp-config)#exit
DHCPRouter(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
DHCPRouter(config)#ip dhcp excluded-address 192.168.20.1 192.168.20.10
DHCPRouter(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.10
DHCPRouter(config)#ip dhcp excluded-address 192.168.50.1 192.168.50.10
DHCPRouter(config)#ip dhcp excluded-address 192.168.70.1 192.168.70.10
DHCPRouter(config)#ip dhcp excluded-address 192.168.80.1 192.168.80.10
DHCPRouter(config)#
```

Рис.3.6. Налаштування DHCP-сервера протоколом DHCP

Ми наблизилися до ядра мережі. Ядро потрібно для швидкого транспортування пакетів по всій мережі, тому для його налаштування буде виконано маршрутизацію. Створимо 2 VLAN, один з яких буде головним, а другий запасний, на випадок якщо головний вийде з ладу і потребує ремонту.

```
Core1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Core1(config)#vlan 4
Core1(config-vlan)#exit
Core1(config)#int vlan 4
Core1(config-if)#ip address 192.168.4.5 255.255.255.0
Core1(config-if)#no shut
Core1(config-if)#exit
Core1(config)#int e1/1
Core1(config-if)#switchport mode access
Core1(config-if)#switchport access vlan 4
Core1(config-if)#exit
Core1(config)#int e1/0
Core1(config-if)#switchport mode access
Core1(config-if)#switchport access vlan 4
Core1(config-if)#exit
Core1(config)#int e0/1
Core1(config-if)#switchport mode access
Core1(config-if)#switchport access vlan 4
Core1(config-if)#exit
Core1(config)#router ospf 1
Core1(config-router)#network 192.168.4.0 0.0.0.255 area 0
Core1(config-router)#exit
Core1(config)#ip route 0.0.0.0 0.0.0.0 192.168.4.2
Core1(config)#ip route 0.0.0.0 0.0.0.0 192.168.4.6
Core1(config)#ip route 0.0.0.0 0.0.0.0 192.168.4.3
```

Рис.3.7. Налаштування ядра Core1

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						34
Змн.	Арк.	№ докум.	Підпис	Дата		

Перейдемо до інтернет-з'єднання яке дасть змогу мережі виходу до інтернету. В цьому нам допоможе NAT. NAT переводить приватні адреси у загальнодоступні. Це дозволяє пристрою з приватною адресою IPv4 звертатися до ресурсів за межами приватної мережі. NAT у поєднанні з приватними адресами IPv4 виявився корисним способом збереження загальнодоступних IPv4-адрес. Одна загальнодоступна IPv4-адреса може бути використана сотнями, навіть тисячами пристроїв, кожен з яких має приватну IPv4-адресу. NAT має додаткову перевагу, що полягає у додаванні ступеня конфіденційності та безпеки в мережу, оскільки він приховує внутрішні IPv4-адреси із зовнішніх мереж.

Маршрутизатори з підтримкою NAT можуть бути налаштовані з однією або декількома дійсними загальнодоступними IPv4-адресами. Ці загальнодоступні адреси називають пулом NAT. Коли пристрій із внутрішньої мережі надсилає трафік із мережі назовні, маршрутизатор з підтримкою NAT переводить внутрішній IPv4-адресу пристрою на загальнодоступну адресу з пулу NAT. Для зовнішніх пристроїв весь трафік, що входить і виходить з мережі, має загальнодоступну IPv4 адресу.

```
EDGERouter_1(config)#int e2/0
EDGERouter_1(config-if)#ip add
EDGERouter_1(config-if)#ip address 192.168.1.50 255.255.255.0
EDGERouter_1(config-if)#no shut
EDGERouter_1(config-if)#exit
EDGERouter_1(config)#
*Jun  5 16:48:47.471: %LINK-3-UPDOWN: Interface Ethernet2/0, changed state to up
*Jun  5 16:48:48.471: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2/0, changed state to up
EDGERouter_1(config)#int g1/0
EDGERouter_1(config-if)#ip add
EDGERouter_1(config-if)#ip address 192.168.2.1 255.255.255.0
EDGERouter_1(config-if)#no shut
EDGERouter_1(config-if)#ip
*Jun  5 16:49:25.671: %LINK-3-UPDOWN: Interface GigabitEthernet1/0, changed state to up
*Jun  5 16:49:26.671: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0, changed state to up
EDGERouter_1(config-if)#ip nat inside
*Jun  5 16:49:34.371: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to up
EDGERouter_1(config-if)#exit
EDGERouter_1(config)#int e2/0
EDGERouter_1(config-if)#ip nat outside
EDGERouter_1(config-if)#exit
EDGERouter_1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
EDGERouter_1(config)#acce
EDGERouter_1(config)#access-list 1 per
EDGERouter_1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
EDGERouter_1(config)#access-list 1 permit 192.168.20.0 0.0.0.255
EDGERouter_1(config)#access-list 1 permit 192.168.40.0 0.0.0.255
EDGERouter_1(config)#access-list 1 permit 192.168.50.0 0.0.0.255
EDGERouter_1(config)#access-list 1 permit 192.168.70.0 0.0.0.255
EDGERouter_1(config)#access-list 1 permit 192.168.80.0 0.0.0.255
EDGERouter_1(config)#access-list 1 permit 192.168.3.0 0.0.0.255
EDGERouter_1(config)#access-list 1 permit 192.168.4.0 0.0.0.255
EDGERouter_1(config)#s 192.168.1.51 192.168.1.100 netmask 255.255.255.0
EDGERouter_1(config)#ip nat inside source list 1 pool global-ips
EDGERouter_1(config)#router ospf 1
EDGERouter_1(config-router)#network 192.168.1.0 0.0.0.255 area 0
EDGERouter_1(config-router)#network 192.168.2.0 0.0.0.255 area 0
EDGERouter_1(config-router)#network 192.168.3.0 0.0.0.255 area 0
EDGERouter_1(config-router)#exit
```

Рис.3.8. Налаштування NAT та списків доступу

						Арк.
						35
Змн.	Арк.	№ докум.	Підпис	Дата	КБ.КВ.Б – 125 – 22 – ПЗ	

Для кращої безпеки мережі було налаштовано списки доступу. ACL – це універсальний та потужний механізм фільтрації. З їхньою допомогою можна визначити кого навішувати певні політики, але в кого ні, хто буде брати участь у деяких процесах, а хто ні, кого обмежуємо у швидкість до 56к, а кого до 56М.

Також потрібно налаштувати віддалений доступ до пристроїв. Для цього є 2 способів налаштування, ssh або telnet. Для цієї мережі використаємо SSHv2, тому що він створює захищений канал між пристроями. Тому перехопивши пакети зломисник не зможе дізнатися пароль та логін, бо він буде надійно зашифрований.

```
Acc2(config)#enable secret office2
Acc2(config)#username office2 privilege 15 secret rootnet
Acc2(config)#service password-encryption
Acc2(config)#banner exec c
Enter TEXT message. End with the character 'c'.
Acc2
Acc2(config)#ip domain-name marvelcs
Acc2(config)#crypto key generate rsa modulus 1024
The name for the keys will be: Acc2.marvelcs

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

Acc2(config)#ip ssh version 2
Acc2(config)#ip ssh time-out 15
Acc2(config)#ip ssh logging events
Acc2(config)#line vty 0 4
Acc2(config-line)#transport input ssh
Acc2(config-line)#transport output ssh
Acc2(config-line)#logging synchronous
Acc2(config-line)#login local
Acc2(config-line)#exec-timeout 5 0
Acc2(config-line)#exit
Acc2(config)#
*Jun  4 13:43:03.831: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Рис.3.9. Налаштування SSHv2

Наступним кроком буде налаштування серверу RADIUS. Для початку проведемо налаштування аутентифікації AAA, який дозволить використовувати RADIUS. Відповідно до налаштування політик AAA, пристрій запитує логін і пароль, після чого передає логін і хеш пароля RADIUS серверу.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						36
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ServerSW(config)#aaa ne
ServerSW(config)#aaa new-model
ServerSW(config)#aaa au
ServerSW(config)#aaa authe
ServerSW(config)#aaa authentication lo
ServerSW(config)#aaa authentication login def
ServerSW(config)#aaa authentication login default gr
ServerSW(config)#aaa authentication login default group ra
ServerSW(config)#aaa authentication login default group radius n
ServerSW(config)#aaa authentication login default group radius none
ServerSW(config)#rad
ServerSW(config)#radius se
ServerSW(config)#radius server TEST
ServerSW(config-radius-server)#address ipv4 192.168.3.11
ServerSW(config-radius-server)#key WinRadius
ServerSW(config-radius-server)#end

```

Рис.3.10. Налаштування аутентифікації AAA.

Перейдемо до налаштування RADIUS. В кладці «Властивості» змінимо режим сумісності на Windows 7 та поставимо галочку для відкривання програми від імені адміністратора.

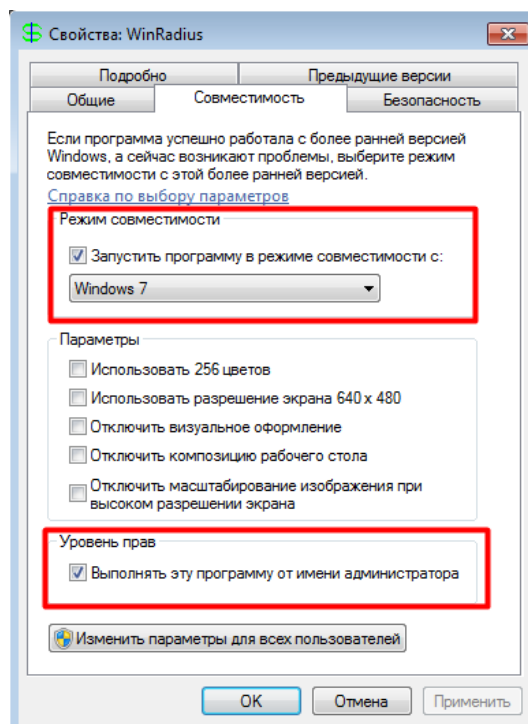


Рис.3.11. Зміна властивостей

Після запуску програми потрібно створити користувача, через який буде відбуватися підключення до пристроїв в мережі.

Рис.3.12. Створення користувача

Далі спробуємо підключитися до комутатора ServerSW через користувача який створили на минулому кроці.

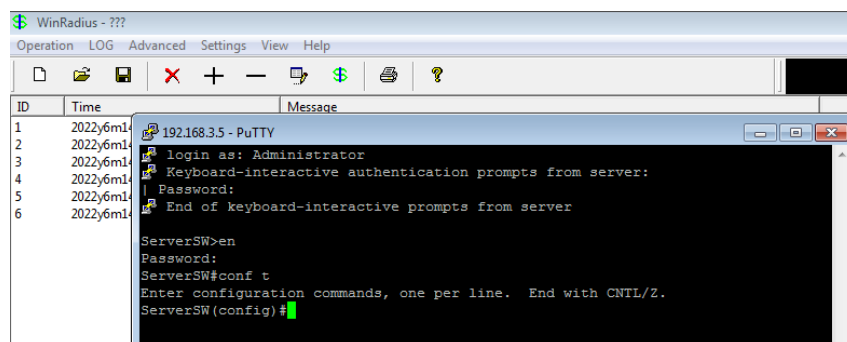


Рис.3.13. Вхід до обладнання

Як можна побачити (Рис.3.13) вхід був успішний, також ввели базові команди для перевірки працездатності.

3.2 Тестування підсистеми захисту корпоративної мережі компанії на базі обладнання Cisco.

Тестування підсистеми захисту корпоративної мережі компанії проводиться з метою перевірки налаштувань на відповідність поставленим завданням.

Для початку перевіримо правильність налаштування маршрутизації протоколу OSPF (Рис 3.14).

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						38
Змн.	Арк.	№ докум.	Підпис	Дата		

```
DHCPRouter#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.90.2	1	FULL/DR	00:00:37	192.168.90.2	Ethernet2/2
192.168.60.2	1	FULL/BDR	00:00:35	192.168.60.2	Ethernet2/1
192.168.30.2	1	FULL/BDR	00:00:33	192.168.30.2	Ethernet2/0
192.168.4.2	1	FULL/BDR	00:00:37	192.168.4.2	Ethernet1/1
192.168.3.2	1	FULL/BDR	00:00:30	192.168.3.2	Ethernet1/0

Рис. 3.14. Перевірка налаштувань OSPF

За допомогою Wireshark перевіримо розсилання Hello-повідомлення.

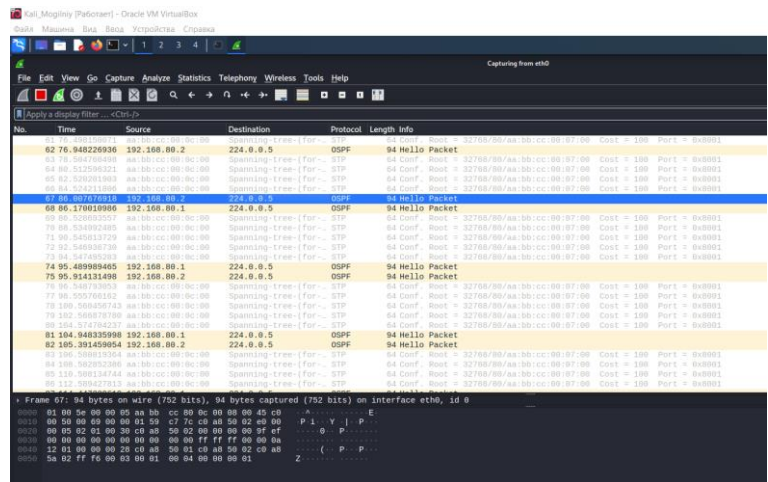


Рис. 3.15. Перевірка розсилання пакетів

Проведемо перевірку на працездатність мережі автоматично призначати IP-адреси робочим станція через DHCP (Рис.3.16 - Рис.3.19).

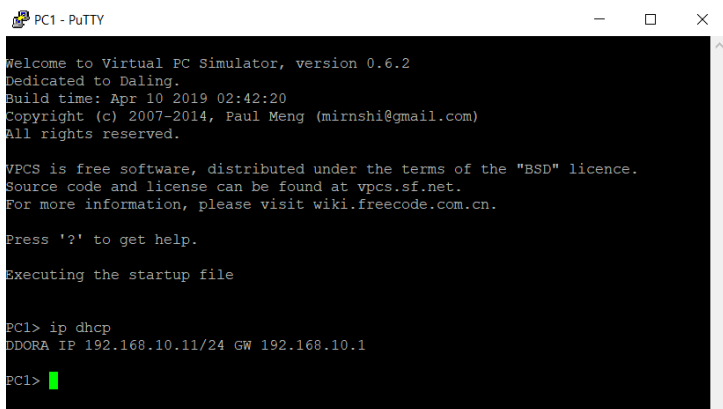


Рис. 3.16. Отримання DHCP-адреси

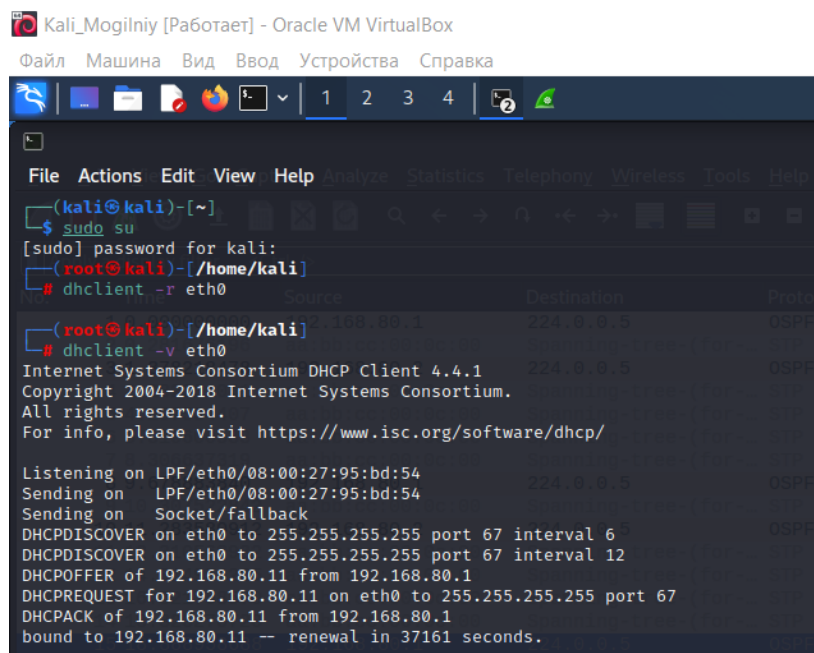


Рис. 3.17. Отримання DHCP-адреси

```

DHCPRouter#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/
                   Hardware address/
                   User name
192.168.10.11        0100.5079.6668.04
192.168.20.11        0100.5079.6668.00
192.168.40.11        0100.5079.6668.01
192.168.50.11        0100.5079.6668.02
192.168.70.11        0100.5079.6668.03
192.168.80.11        0108.0027.95d2.ee
                   Jun 06 2022 06:01 PM
                   Jun 06 2022 06:03 PM
                   Jun 06 2022 06:03 PM
                   Jun 06 2022 06:04 PM
                   Jun 06 2022 06:04 PM
                   Jun 06 2022 06:03 PM
                   Automatic
                   Automatic
                   Automatic
                   Automatic
                   Automatic
                   Automatic

```

Рис. 3.18. Перевірка підключення робочих станцій

```

DHCPRouter#show ip dhcp pool

Pool OFFICE_1 :
  Utilization mark (high/low)    : 100 / 0
  Subnet size (first/next)        : 0 / 0
  Total addresses                  : 254
  Leased addresses                 : 1
  Pending event                   : none
  1 subnet is currently in the pool :
    Current index  IP address range  Leased addresses
    192.168.10.12  192.168.10.1 - 192.168.10.254  1

Pool OFFICE_2 :
  Utilization mark (high/low)    : 100 / 0
  Subnet size (first/next)        : 0 / 0
  Total addresses                  : 254
  Leased addresses                 : 1
  Pending event                   : none
  1 subnet is currently in the pool :
    Current index  IP address range  Leased addresses
    192.168.20.12  192.168.20.1 - 192.168.20.254  1

Pool OFFICE_3 :
  Utilization mark (high/low)    : 100 / 0
  Subnet size (first/next)        : 0 / 0
  Total addresses                  : 254
  Leased addresses                 : 1
  Pending event                   : none
  1 subnet is currently in the pool :
    Current index  IP address range  Leased addresses
    192.168.40.12  192.168.40.1 - 192.168.40.254  1

Pool OFFICE_4 :
  Utilization mark (high/low)    : 100 / 0
  Subnet size (first/next)        : 0 / 0
  Total addresses                  : 254
  Leased addresses                 : 1
  Pending event                   : none
  1 subnet is currently in the pool :
    Current index  IP address range  Leased addresses
    192.168.50.12  192.168.50.1 - 192.168.50.254  1

```

Рис. 3.19. Перевірка пулів DHCP

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						40
Змн.	Арк.	№ докум.	Підпис	Дата		

Як ми бачимо всі робочі станції отримали свої IP-адреси, тому варто перевірити зв'язок між ними (Рис.3.20).

```

C:\Windows\system32\cmd.exe
C:\Users\admin>ping 192.168.10.11

Обмен пакетами с 192.168.10.11 по 32 байтами данных:
Ответ от 192.168.10.11: число байт=32 время=3021мс TTL=61
Ответ от 192.168.10.11: число байт=32 время=23мс TTL=61
Ответ от 192.168.10.11: число байт=32 время=18мс TTL=61
Ответ от 192.168.10.11: число байт=32 время=16мс TTL=61

Статистика Ping для 192.168.10.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
        Минимальное = 16мсек, Максимальное = 3021 мсек, Среднее = 769 мсек

C:\Users\admin>ping 192.168.40.11

Обмен пакетами с 192.168.40.11 по 32 байтами данных:
Ответ от 192.168.40.11: число байт=32 время=3020мс TTL=61
Ответ от 192.168.40.11: число байт=32 время=21мс TTL=61
Ответ от 192.168.40.11: число байт=32 время=17мс TTL=61
Ответ от 192.168.40.11: число байт=32 время=17мс TTL=61

Статистика Ping для 192.168.40.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
        Минимальное = 17мсек, Максимальное = 3020 мсек, Среднее = 768 мсек

C:\Users\admin>ping 192.168.70.11

Обмен пакетами с 192.168.70.11 по 32 байтами данных:
Ответ от 192.168.70.11: число байт=32 время=3023мс TTL=63
Ответ от 192.168.70.11: число байт=32 время=7мс TTL=63
Ответ от 192.168.70.11: число байт=32 время=4мс TTL=63
Ответ от 192.168.70.11: число байт=32 время=4мс TTL=63

Статистика Ping для 192.168.70.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
    Приблизительное время приема-передачи в мс:
        Минимальное = 4мсек, Максимальное = 3023 мсек, Среднее = 759 мсек

C:\Users\admin>
  
```

Рис. 3.20. Перевірка зв'язку між робочими станціями

Зробимо перевірку віддаленого доступу в мережі. Для цього спробуємо підключитися з ServerSW до Acc1 (Рис.3.21 – Рис.3.23).

```

ServerSW#ssh -l office1 192.168.10.2
Password:
A
Acc1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Acc1(config)#
  
```

Рис. 3.21. Перевірка зв'язку між робочими станціями

```

Acc1#
*Jun  5 15:20:20.179: %SSH-5-SSH2_SESSION: SSH2 Session request from 192.168.3.5
(tty = 0) using crypto cipher 'aes128-cbc', hmac 'hmac-sha1' Succeeded
Acc1#
*Jun  5 15:20:30.837: %SSH-5-SSH2_USERAUTH: User 'office1' authentication for SS
H2 Session from 192.168.3.5 (tty = 0) using crypto cipher 'aes128-cbc', hmac 'hm
ac-sha1' Succeeded
  
```

Рис. 3.22. Успішність підключення

```
(root@kali)-[/home/kali]
# ssh -l marvelcs 192.168.80.2
(marvelcs@192.168.80.2) Password:
(marvelcs@192.168.80.2) Password:

A
Acc6#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Acc6(config)#
```

Рис. 3.22. Підключення до пристроїв через Kali

Спробуємо перехватити SSH-пакети та отримати логіни та паролі(Рис.3.23).

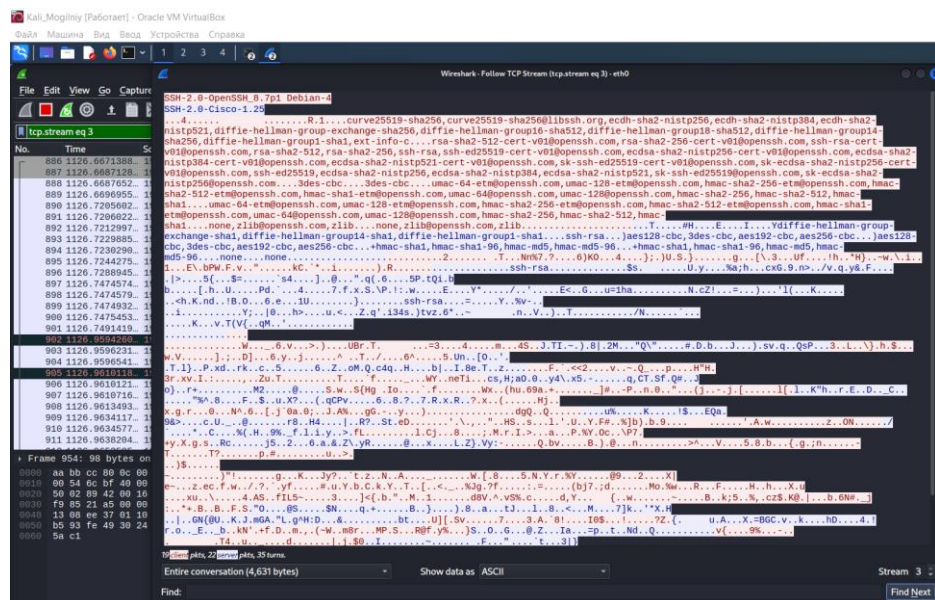


Рис. 3.23. Пакет SSH

Так як SSH має високий рівень шифрування, то паролі та логіни дізнатися не зможемо.

3.3 Аналіз результатів тестування

Як і планувалося, всі вимоги, які ставились раніше, були успішно виконані. В майбутньому дана мережа може бути збільшена та покращена під якісь певні завдання. Для цього є всі можливості. DHCP допоможе при встановленні нових робочих станцій та пристроїв, сервер - для налаштування нових приладів та моніторингу за ними, а рівень ядра, так як

використовуються маршрутизатори фірми CISCO, є досить гнучкий для майбутніх налаштувань.

Ще одна перевага мережі в тому, що на рівні ядра є 2 VLAN. Якщо один вийде з ладу, то інший візьме на себе контроль і продовжить виконувати роботу першого.

Висновки до розділу 3

В даному розділі було описано базові налаштування всіх пристроїв даної мережі. Була налаштована статична та динамічна (DHCP) маршрутизація. Для зручності використання та налаштування пристроїв було надано кожному особисту назву.

На маршрутизаторах було налаштовано протокол SSH для віддаленого доступу до них. Провели маршрутизацію за допомогою протоколу OSPF. Також завдяки RADIUS ми вдосконалили безпеку мережі захистивши її від несанкціонованого доступу, зашифрувавши паролі користувачів.

Було проведено аналіз тестування та описано можливості масштабування та покращення мережі.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						43
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У дипломному проекті була спроектована корпоративна модель комп'ютерної мережі на базі обладнання Cisco. При розробці були враховані всі вимоги до проекту.

Для початку було обрано існуючі технології для розробки мережі. Зокрема було обрано графічний емулятор GNS3, операційна система Windows 7 та 10, RADIUS, протоколи OSPF, DHCP, NAT, SSHv2, VLAN.

Так як корпоративна мережа складалася з великої кількості пристроїв, то ми її розділили на LAN. VLAN поділяє підсистеми на окремі ширококомовні домени. Це означає, що ширококомовні повідомлення будуть отримувати лише пристрої, що знаходяться в одній мережі VLAN. Побудова системи з використанням технології VLAN дозволила зменшити ширококомовний трафік усередині мережі, тим самим знизилася навантаження на мережеві пристрої та покращилася продуктивність системи загалом.

В схемі використано корпоративну модель мережі яка забезпечила продуктивність, надійність мережі. В яку входить 5 рівнів: ядро з DHCP сервером, Data Center, DMZ, розподілу та доступу, а також інтернет з'єднання.

Ядро забезпечило швидку передачу даних між комутаторами. Також було налаштовано DHCP сервер, який автоматично присвоїв IP-адреси і інші параметри для пристроїв.

Data Center зберіг користувачів та паролі завдяки протоколу RADIUS. Також було додано комутатор L3 який підтримував зв'язок з мережею.

Рівень розподілу забезпечив маршрутизацію мережі, також було налаштовано DHCP-relay для отримання IP-адреси між VLAN.

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						44
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Корпоративна мережа [Електронний ресурс] –
https://uk.wikipedia.org/wiki/Корпоративна_мережа
2. Все про NAT [Електронний ресурс] – <https://wiki.merionet.ru/seti/13/nat-na-palcah-hto-eto/>
3. Протокол OSFP [Електронний ресурс] – Режим доступу до ресурсу:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/xen-16/iro-xe-16-book/iro-cfg.html
4. Налаштування CISCO DHCP [Електронний ресурс] – Режим доступу до ресурсу: <https://study-ccna.com/configure-cisco-router-as-dhcp-server/>
5. DNS Server [Електронний ресурс] - <https://ru.wikipedia.org/wiki/DNS>
6. SSHv2 [Електронний ресурс] -
<https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html>
7. Ієрархічна модель мережі від Cisco [Електронний ресурс] -
<http://www.telesphera.net/blog/model-mereghi-vid-cisco.html>
8. Протокол SSH [Електронний ресурс] – <https://uk.wikipedia.org/wiki/SSH>
9. Windows XP [Електронний ресурс] -
https://en.wikipedia.org/wiki/Windows_XP#:~:text=Windows%20XP%20is%20an%20operating,NT%20family%20of%20operating%20systems.&text=It%20was%20Microsoft%27s%20operating%20system,Windows%20Vista%20in%20February%202007.
10. RADIUS [Електронний ресурс] - <https://uk.wikipedia.org/wiki/RADIUS>
11. Windows 7 [Електронний ресурс] -https://ru.wikipedia.org/wiki/Windows_7
12. Linux [Електронний ресурс] - <https://uk.wikipedia.org/wiki/Linux>
13. Ubuntu [Електронний ресурс] - <https://en.wikipedia.org/wiki/Ubuntu>
14. Хешування MD5 [Електронний ресурс] – <https://uk.wikipedia.org/wiki/MD5>
15. Налаштування CISCO port-security [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/switches/LAN/catalyst4000/8-2glx/configuration/guide/sec_port.html

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						45
Змн.	Арк.	№ докум.	Підпис	Дата		

16. Cisco IOS - Privilege Levels [Електронний ресурс] -
<https://learningnetwork.cisco.com/s/blogs/a0D3i000002eeWTEAY/cisco-ios-privilege-levels>

17. Керівництво CISCO по захисту пристроїв CISCO IOS [Електронний ресурс] – Режим доступу до ресурсу:
https://www.cisco.com/c/ru_ru/support/docs/ip/access-lists/13608-21.html#anc2

18. GNS3 [Електронний ресурс] - <https://habr.com/ru/post/266503/>

19. VirtualBox [Електронний ресурс] - <https://www.virtualbox.org/>

20. Wireshark User Guide [Електронний ресурс] -
https://www.wireshark.org/docs/wsug_html/

21. Wireshark [Електронний ресурс] -
https://www.wireshark.org/docs/wsug_html_chunked/ChAdvExpert.html

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						46
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						47
Змн.	Арк.	№ докум.	Підпис	Дата		

Комутатор Dis1

Dis1

Dis1#show running-config	!
Building configuration...	no ip domain-lookup
	no ipv6 cef
	ipv6 multicast rpf use-bgp
	!
	!
Current configuration : 2194 bytes	!
!	!
version 15.1	!
service timestamps debug datetime msec	!
service timestamps log datetime msec	!
no service password-encryption	spanning-tree mode pvst
service compress-config	spanning-tree extend system-id
!	!
hostname Dis1	!
!	!
boot-start-marker	!
boot-end-marker	vlan internal allocation policy ascending
!	!
!	ip tcp synwait-time 5
logging discriminator EXCESS severity drops 6	!
msg-body drops EXCESSCOLL	!
logging buffered 50000	!
logging console discriminator EXCESS	!
!	!
no aaa new-model	interface Ethernet0/0
no ip icmp rate-limit unreachable	duplex auto
!	!
ip cef	interface Ethernet0/1
!	duplex auto

!	interface Ethernet2/1
interface Ethernet0/2	duplex auto
duplex auto	!
!	interface Ethernet2/2
interface Ethernet0/3	duplex auto
duplex auto	!
!	interface Ethernet2/3
interface Ethernet1/0	duplex auto
description LINK_TO_ACC1	!
switchport access vlan 10	interface Ethernet3/0
switchport mode access	duplex auto
duplex auto	!
!	interface Ethernet3/1
interface Ethernet1/1	duplex auto
description LINK_TO_ACC2	!
switchport access vlan 20	interface Ethernet3/2
switchport mode access	duplex auto
duplex auto	!
!	interface Ethernet3/3
interface Ethernet1/2	duplex auto
duplex auto	!
!	interface Vlan1
interface Ethernet1/3	no ip address
duplex auto	shutdown
!	!
interface Ethernet2/0	interface Vlan10
description LINK_TO_DHCPROUTER	ip address 192.168.10.1 255.255.255.0
switchport access vlan 30	ip helper-address 192.168.30.1
switchport mode access	!
duplex auto	interface Vlan20
!	ip address 192.168.20.1 255.255.255.0

```

ip helper-address 192.168.30.1

!
interface Vlan30
ip address 192.168.30.2 255.255.255.0
!
router ospf 1
network 192.168.10.0 0.0.0.255 area 0
network 192.168.20.0 0.0.0.255 area 0
network 192.168.30.0 0.0.0.255 area 0
!
no ip http server
!
ip route 0.0.0.0 0.0.0.0 192.168.10.2
ip route 0.0.0.0 0.0.0.0 192.168.20.2
ip route 0.0.0.0 0.0.0.0 192.168.30.1
control-plane
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end
privilege exec level 1 show running-config
privilege exec level 1 show interfaces
privilege exec level 1 show

banner
login

Device hostname -(R_1)
Your connection is -(line)
Enter Admin's LOGIN and Password
=====^C
!
line con 0
privilege level 15
logging synchronous
login local
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login local
transport input ssh
!
End

```

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						50
Змн.	Арк.	№ докум.	Підпис	Дата		

Маршрутизатор DHCPRouter	!
DHCPRouter	!
	aaa session-id common
DHCPRouter#show running-config	!
Building configuration...	!
	!
Current configuration : 3899 bytes	ip source-route
!	no ip icmp rate-limit unreachable
! Last configuration change at 17:34:12 UTC Tue	ip cef
Jun 14 2022 by Administrator	!
!	!
upgrade fpd auto	ip dhcp excluded-address 192.168.10.1
version 15.0	192.168.10.10
service timestamps debug datetime msec	ip dhcp excluded-address 192.168.20.1
service timestamps log datetime msec	192.168.20.10
service password-encryption	ip dhcp excluded-address 192.168.40.1
!	192.168.40.10
hostname DHCPRouter	ip dhcp excluded-address 192.168.50.1
!	192.168.50.10
boot-start-marker	ip dhcp excluded-address 192.168.70.1
boot-end-marker	192.168.70.10
!	ip dhcp excluded-address 192.168.80.1
enable secret 5	192.168.80.10
\$1\$.BA\$Qi.HzKJm/CAV7JAdcFtNK1	ip dhcp excluded-address 192.168.3.1
!	192.168.3.10
aaa new-model	!
!	ip dhcp pool OFFICE_1
!	network 192.168.10.0 255.255.255.0
aaa authentication login default group radius none	default-router 192.168.10.1
!	dns-server 8.8.8.8 8.8.4.4
!	!
!	ip dhcp pool OFFICE_2

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						51
Змн.	Арк.	№ докум.	Підпис	Дата		

network 192.168.20.0 255.255.255.0	ip domain name marvelcs
default-router 192.168.20.1	no ipv6 cef
dns-server 8.8.8.8 8.8.4.4	!
!	multilink bundle-name authenticated
ip dhcp pool OFFICE_3	!
network 192.168.40.0 255.255.255.0	!
default-router 192.168.40.1	!
dns-server 8.8.8.8 8.8.4.4	!
!	!
ip dhcp pool OFFICE_4	!
network 192.168.50.0 255.255.255.0	!
default-router 192.168.50.1	!
dns-server 8.8.8.8 8.8.4.4	username dhcproute privilege 15 secret 5
!	\$1\$tyyR\$p6ZA1p3RyB2/JH16nmcsG/
ip dhcp pool OFFICE_5	!
network 192.168.70.0 255.255.255.0	redundancy
default-router 192.168.70.1	!
dns-server 8.8.8.8 8.8.4.4	!
!	ip tcp synwait-time 5
ip dhcp pool ADMINS	ip ssh time-out 15
network 192.168.80.0 255.255.255.0	ip ssh logging events
default-router 192.168.80.1	ip ssh version 2
dns-server 8.8.8.8 8.8.4.4	!
!	!
ip dhcp pool RADIUS	!
network 192.168.3.0 255.255.255.0	!
default-router 192.168.3.1	!
dns-server 8.8.8.8 8.8.4.4	!
!	!
!	!
no ip domain lookup	interface FastEthernet0/0

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						52
Змн.	Арк.	№ докум.	Підпис	Дата		

no ip address	!
shutdown	interface Ethernet2/1
duplex half	ip address 192.168.60.1 255.255.255.0
!	duplex half
!	!
interface Ethernet1/0	!
ip address 192.168.3.1 255.255.255.0	interface Ethernet2/2
duplex half	ip address 192.168.90.1 255.255.255.0
!	duplex half
!	!
interface Ethernet1/1	!
ip address 192.168.4.1 255.255.255.0	interface Ethernet2/3
duplex half	no ip address
!	shutdown
!	duplex half
interface Ethernet1/2	!
no ip address	!
shutdown	!
duplex half	router ospf 1
!	log-adjacency-changes
!	network 192.168.3.0 0.0.0.255 area 0
interface Ethernet1/3	network 192.168.4.0 0.0.0.255 area 0
no ip address	network 192.168.10.0 0.0.0.255 area 0
shutdown	network 192.168.20.0 0.0.0.255 area 0
duplex half	network 192.168.30.0 0.0.0.255 area 0
!	network 192.168.40.0 0.0.0.255 area 0
!	network 192.168.50.0 0.0.0.255 area 0
interface Ethernet2/0	network 192.168.60.0 0.0.0.255 area 0
ip address 192.168.30.1 255.255.255.0	network 192.168.70.0 0.0.0.255 area 0
duplex half	network 192.168.80.0 0.0.0.255 area 0
!	network 192.168.90.0 0.0.0.255 area 0

```

!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 0.0.0.0 0.0.0.0 192.168.30.2
ip route 0.0.0.0 0.0.0.0 192.168.60.2
ip route 0.0.0.0 0.0.0.0 192.168.90.2
ip route 0.0.0.0 0.0.0.0 192.168.3.2
ip route 0.0.0.0 0.0.0.0 192.168.4.2
!
no cdp log mismatch duplex
!
!
!
!
!
radius-server host 192.168.3.11 auth-port 1645
acct-port 1646 key 7 01240F0A690A0206345F
!
control-plane
!
!
!
!
!
!
!
gatekeeper
shutdown
!

```

```

banner exec ^C
DHCPRoute
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
exec-timeout 5 0
logging synchronous
transport input ssh
transport output ssh
!
end

```

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						54
Змн.	Арк.	№ докум.	Підпис	Дата		

Current configuration : 1955 bytes

!

upgrade fpd auto

version 15.0

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname EDGERouter_1

!

boot-start-marker

boot-end-marker

!

!

no aaa new-model

!

!

!

ip source-route

no ip icmp rate-limit unreachable

ip cef

!

!

!

Додаток В

Маршрутизатор EDGERouter_1

no ip domain lookup

EDGERouter_1

no ipv6 cef

!

EDGERouter_1#show running-config

multilink bundle-name authenticated

Building configuration...

!

!

					КБ.КВ.Б – 125 – 22 – ПЗ	Арк.
						55
Змн.	Арк.	№ докум.	Підпис	Дата		

!	!
!	interface Ethernet2/0
!	ip address 192.168.1.50 255.255.255.0
!	ip nat outside
!	ip virtual-reassembly
!	duplex half
!	!
redundancy	!
!	interface Ethernet2/1
!	no ip address
ip tcp synwait-time 5	shutdown
!	duplex half
!	!
!	!
!	interface Ethernet2/2
!	no ip address
!	shutdown
!	duplex half
!	!
interface FastEthernet0/0	!
no ip address	interface Ethernet2/3
shutdown	no ip address
duplex half	shutdown
!	duplex half
!	!
interface GigabitEthernet1/0	!
ip address 192.168.2.1 255.255.255.0	!
ip nat inside	router ospf 1
ip virtual-reassembly	log-adjacency-changes
negotiation auto	network 192.168.1.0 0.0.0.255 area 0
!	network 192.168.2.0 0.0.0.255 area 0

```

network 192.168.3.0 0.0.0.255 area 0
!
!
ip forward-protocol nd
!
no ip http server
gatekeeper
no ip http secure-server
shutdown
!
!
!
ip nat pool global-ips 192.168.1.51 192.168.1.100 netmask
255.255.255.0
line con 0
exec-timeout 0 0
ip nat inside source list 1 pool global-ips
privilege level 15
ip route 0.0.0.0 0.0.0.0 192.168.1.1
logging synchronous
!
stopbits 1
access-list 1 permit 192.168.10.0 0.0.0.255
line aux 0
access-list 1 permit 192.168.20.0 0.0.0.255
exec-timeout 0 0
access-list 1 permit 192.168.40.0 0.0.0.255
privilege level 15
access-list 1 permit 192.168.50.0 0.0.0.255
logging synchronous
access-list 1 permit 192.168.70.0 0.0.0.255
stopbits 1
access-list 1 permit 192.168.80.0 0.0.0.255
line vty 0 4
access-list 1 permit 192.168.3.0 0.0.0.255
login
access-list 1 permit 192.168.4.0 0.0.0.255
!
no cdp log mismatch duplex
end
!
!
!
!
!
!
!
control-plane
!
!
!
```

