

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи освітнього ступеня «бакалавр»
за спеціальністю 122 «Комп'ютерні науки»
(освітня програма «Комп'ютерна графіка та розробка ігор»)
на тему:

«Підсистема захисту гетерогенної мережі організації на базі
протоколу маршрутизації EIGRP»

Виконала студентка групи КН-20-1
Наговерко Юлія Юріївна

Керівник роботи:
Кузьменко Олександр Вікторович

Рецензент:
Граф Марина Сергіївна

Житомир 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК

ЗАТВЕРДЖУЮ
Завідувач кафедри комп'ютерних наук
Марина ГРАФ
«25» січня 2024 р.

ЗАВДАННЯ

на кваліфікаційну роботу освітнього ступеня «бакалавр»
за спеціальністю 122 «Комп'ютерні науки»
(освітня програма «Комп'ютерна графіка та розробка ігор»)

Здобувач вищої освіти: Наговерко Юлія Юріївна

Керівник роботи: Кузьменко Олександр Вікторович

Тема роботи: «Підсистема захисту гетерогенної мережі організації на базі протоколу маршрутизації EIGRP»

затверджена наказом закладу вищої освіти від «25» січня 2024 р., №22/с

Термін здачі студентом закінченої роботи – «05» Червня 2024 р.

Вихідні дані для роботи:

Об'єктом дослідження є процес налаштування віддалених робочих столів і захисту комп'ютерної мережі від зловмисників.

Предметом дослідження є методи і засоби використання віддалених підключень та інших засобів для забезпечення захисту гетерогенної мережі.

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Кузьменко О.В.	5 березня 2024	30 березня 2024
2	Кузьменко О.В.	7 квітня 2024	28 квітня 2024
3	Кузьменко О.В.	4 травня 2024	20 травня 2024

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	2 лютого 2024 – 5 березня 2024	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо організації гетерогенної мережі	6 березня 2024 – 11 березня 2024	Виконано
3	Аналіз технологій захисту мережі за допомогою налаштувань на маршрутизаторах CISCO	12 березня 2024 – 18 березня 2024	Виконано
4	Аналіз можливостей мережного обладнання Cisco для гетерогенності мережі	19 березня 2024 – 25 березня 2024	Виконано
5	Розробка загального проекту мережі організації	26 березня 2024 – 1 квітня 2024	Виконано
6	Проектування мережі та вибір обладнання для її реалізації	2 квітня 2024 – 7 квітня 2024	Виконано
7	Проектування таблиці маршрутизації	8 квітня 2024 – 14 квітня 2024	Виконано
8	Проектування сценарію тестування мережі	16 квітня 2024 – 21 квітня 2024	Виконано
9	Базове налагодження пристроїв мережі	22 квітня 2024 – 25 квітня 2024	Виконано
10	Налагодження гетерогенної мережі	27 квітня 2024 – 6 травня 2024	Виконано
11	Тестування роботи гетерогенної мережі	7 травня 2024 – 11 травня 2024	Виконано
12	Аналіз результатів тестування	13 травня 2024 – 20 травня 2024	Виконано
13	Написання пояснювальної записки	21 травня 2024 – 30 травня 2024	Виконано
14	Підготовка презентації та виступу	1 червня 2024 – 9 червня 2024	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	11 червня 2024 – 17 червня 2024	Виконано
16	Захист	18 червня 2024	Виконано

Здобувач вищої освіти Наговерко Ю.Ю.

Керівник Кузьменко О.В.

РЕФЕРАТ

Кваліфікаційна робота складається з проекту гетерогенної мережі з можливістю віддалених робочих столів на базі протоколу EIGRP та пояснювальної записки до нього. Пояснювальна записка містить 69 сторінок, 52 ілюстрації та 9 таблиць.

Дипломний проект присвячений розробці гетерогенної мережі з можливістю віддалених робочих столів на базі протоколу EIGRP. Метою проекту буде надійність, ефективність та захищеність комп'ютерної мережі. Наша мережа має забезпечувати безперервний обмін даними та постійний зв'язок з віддаленими робочими столами. Також для захисту на маршрутизаторах буде налаштовано користувачів з різними рівнями привілеїв для різних типів доступу.

Дипломний проект 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 проекту. В додатках буде вказано конфігурації маршрутизаторів та комутаторів мережі.

КЛЮЧОВІ СЛОВА: ЗАХИСТ, КОМП'ЮТЕРНА МЕРЕЖА, ГЕТЕРОГЕННА МЕРЕЖІ, ВІДДАЛЕНІ РОБОЧІ СТОЛИ, CISCO.

					КН.КР.Б – 122 – 24 – ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата	Підсистема захисту гетерогенної мережі організації на базі протоколу маршрутизації EIGR	Літ.	Арк.	Аркушів
Розроб.		Ю.Ю. Наговерко						
Керівник		О. В. Кузьменко					4	61
Рецензент.		М.С.Граф				Житомирська політехніка, група КН-20-1		
Н.контр.								
Зав. каф.		М.С. Граф						

ABSTRACT

The qualification work consists of a project for a heterogeneous network with remote desktop capabilities based on the EIGRP protocol, accompanied by an explanatory note. The explanatory note includes 69 pages, 52 illustrations, and 9 tables.

The diploma project is dedicated to the development of a heterogeneous network with remote desktop capabilities based on the EIGRP protocol. The goal of the project is to ensure the reliability, efficiency, and security of the computer network. Our network should provide continuous data exchange and constant connectivity with remote desktops. Additionally, to enhance security, routers will be configured with users having different privilege levels for various types of access.

The diploma project will consist of three sections, which will include the development of the logical and physical structure of the network, the selection of network equipment and software, a network configuration scenario, and project testing. The appendices will contain the configurations of the network's routers and switches.

KEYWORDS: SECURITY, COMPUTER NETWORK, HETEROGENEOUS NETWORK, REMOTE DESKTOPS, CISCO.

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

РЕФЕРАТ	4
ABSTRACT.....	5
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	7
ВСТУП.....	8
РОЗДІЛ 1 ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ ГЕТЕРОГЕННОЇ МЕРЕЖІ З ВІДДАЛЕНИМИ РОБОЧИМИ СТОЛАМИ ТА ВИМОГИ ДО НЕЇ	10
1.1 Особливості побудови гетерогенної мережі.....	10
1.2 Теоретичні відомості щодо Active directory.....	11
1.3 Протокол маршрутизації EIGRP	13
1.4. Протокол DHCP.....	17
РОЗДІЛ 2 ПРОЕКТУВАННЯ ГЕТЕРОГЕННОЇ МЕРЕЖІ З МОЖЛИВІСТЮ ВІДДАЛЕНИХ РОБОЧИХ СТОЛІВ	22
2.1 Принципи роботи мережі.....	22
2.2 Розробка логічної структури мережі	25
2.3 Проект підсистеми, вибір обладнання та програмного забезпечення... ..	30
РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ДОСЛІДЖЕННЯ ПРОЕКТУ ПІДСИСТЕМИ ЗАХИСТУ ГЕТЕРОГЕННОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ З МОЖЛИВІСТЮ ВІДДАЛЕНИХ ПІДКЛЮЧЕНЬ НА БАЗІ ПРОТОКОЛУ МАРШРУТИЗАЦІЇ EIGRP.	35
3.1 Налаштування мережі	36
3.2 Тестування підсистеми захисту гетерогенної мережі організації з можливістю віддалених підключень на базі протоколу маршрутизації EIGRP	46
3.3 Аналіз результатів тестування.....	54
ВИСНОВКИ	57
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	60
ДОДАТКИ	63

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПЗ – програмне забезпечення

ПК – персональний комп'ютер

КМ – комп'ютерна мережі

ОС – операційна система

GNS3 – Graphical Network Simulator-3

AD – Active directory

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. У сучасному світі жодна організація не зможе ефективно та швидко функціонувати без комп'ютерних мереж. Ефективне управління мережею значною мірою залежить від правильного налаштування та складання коректної схеми маршрутизації. Крім того, для різних завдань не завжди підходить одна операційна система, і часто виникає потреба у використанні інших систем через вимоги різного програмного забезпечення.

Створення комп'ютерної мережі для різних організацій, компаній та підприємств є досить трудомістким процесом, який вимагає значних затрат часу та сконцентрованості для забезпечення правильної та злагодженої роботи всієї системи. Кожна компанія зазвичай має в своєму розпорядженні кілька комутаторів, маршрутизаторів, робочих станцій і серверів.

Оскільки комп'ютерна мережа буде використовуватися системою робочих станцій, призначених для людей з різним рівнем доступу, доцільно використовувати можливість віддалених робочих столів. Робочі станції користувачів з вищим рівнем доступу до бази даних клієнтів чи іншої важливої інформації можуть виходити з ладу. Щоб не витратити час на відновлення їх роботи або надання доступу з інших робочих станцій, доцільніше використовувати віддалений доступ з будь-якого ПК в мережі. При цьому дані для здійснення такого підключення слід надавати тільки тим користувачам, які мають повноваження для роботи з важливими даними на віддаленому сервері чи робочій станції.

Оскільки мережа буде складатися з великої кількості пристроїв, доцільним стане налаштування динамічної IP-адресації. Це дозволить швидко реагувати на вихід техніки з ладу або підключення нових робочих станцій. Крім того, варто встановити різні рівні привілеїв доступу для співробітників, адже не можна дозволяти всім користувачам використовувати всі можливості комп'ютерної мережі. Лише одна-дві особи матимуть доступ до всіх налаштувань комутаторів, маршрутизаторів, серверів і робочих станцій, а також відповідатимуть за формування звітів і

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						8
Змн.	Арк.	№ докум.	Підпис	Дата		

загальний стан пристроїв. Для моніторингу роботи та внесення змін у конфігураційні файли комунікаційних пристроїв мережі важливо налаштувати можливість віддаленого доступу до них за допомогою протоколів SSH чи Telnet.

Оскільки будь-яка система може привернути увагу зломисників або конкурентів, необхідно забезпечити захист даних організації. Нашу систему слід захистити або мінімізувати збитки від зловмисного впливу за допомогою різних засобів захисту від компанії CISCO, оскільки під час налаштування мережі будуть використовуватися комутатори та маршрутизатори саме цієї фірми.

Для практичної реалізації підсистеми буде використовуватися графічний симулятор GNS3. Для забезпечення гетерогенності мережі будуть використовуватися різні версії операційних систем Windows та Linux.

Метою кваліфікаційної роботи є розробка проекту гетерогенної мережі з можливостями віддалених робочих столів з використанням протоколу EIGRP.

Встановлена мета створює наступні завдання:

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

Об'єктом дослідження є процес налаштування віддалених робочих столів і захисту комп'ютерної мережі від зломисників.

Предметом дослідження є методи і засоби використання віддалених підключень та інших засобів для забезпечення захисту гетерогенної мережі.

В процесі виконання кваліфікаційної роботи був розроблений проект підсистеми захисту гетерогенної мережі під управлінням протоколу EIGRP.

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ЗАГАЛЬНІ ХАРАКТЕРИСТИКИ ГЕТЕРОГЕННОЇ МЕРЕЖІ З ВІДДАЛЕНИМИ РОБОЧИМИ СТОЛАМИ ТА ВИМОГИ ДО НЕЇ

1.1 Особливості побудови гетерогенної мережі

Гетерогенна мережа з віддаленими робочими столами використовується для з'єднання декількох локальних мереж (LAN) на невеликій території, надаючи можливість працювати з віддаленими мережами через віддалені робочі столи. Метою створення гетерогенної мережі є забезпечення доступу до ресурсів усіх робочих станцій як у локальних мережах, так і у віддалених мережах.

До основних компонентів гетерогенної мережі будуть відноситися:

- робочі станції під управлінням різних ОС (Windows, Linux);
- комутатори;
- маршрутизатори;
- програмне забезпечення мережі.

У гетерогенній мережі використовується два види робочих станцій:

1. Клієнтська станція - отримує доступ до інших робочих станцій через мережу і забезпечує віддалений доступ до головної робочої станції.
2. Головна станція (сервер) - містить всі основні ресурси мережі і доступна лише користувачам, яким надано відповідні права доступу.[1].

Мережа може бути одноранговою або з виділеним сервером, залежно від типу робочих станцій, які в ній використовуються. Розглянемо переваги та недоліки кожного типу мереж.

В одноранговій комп'ютерній мережі відсутній центральний вузол для зберігання даних, управління мережею та забезпечення взаємодії між робочими станціями. Мережеві завдання розподіляються між усіма пристроями. Кожен комп'ютер може виконувати як функції сервера, так і клієнта, приймаючи та обробляючи дані й запити від інших робочих станцій, а також відправляючи свої дані та запити до інших пристроїв.

До переваг однорангової комп'ютерної мережі належать:

- висока надійність;

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						10
Змн.	Арк.	№ докум.	Підпис	Дата		

- низька вартість.

Основними недоліками є:

- складність керування мережею, через відсутність центрального вузла для збору даних;
- складність в забезпеченні захисту інформації, оскільки налаштування будуть проводитися на всіх комутаторах, маршрутизаторах, робочих станціях окремо;
- залежність продуктивності від кількості пристроїв: працездатність, швидкість, ефективність роботи мережі напряму залежатимуть від кількості пристроїв та робочих станцій в мережі.

У комп'ютерній мережі з виділеним сервером вже присутня робоча станція, яка виступає в ролі сервера. Ця станція відповідає за функції збереження, керування, обробки даних та інші необхідні операції. Крім того, цей сервер призначений для використання всіма іншими робочими станціями у мережі.

Серед переваг можна відзначити наступне:

- збільшена швидкість обробки інформації завдяки централізованому серверу, через який проходять всі дані;
- підвищена надійність системи захисту інформації;
- відсутність обмежень у кількості робочих станцій, які можуть бути підключені до мережі;
- простота адміністрування та управління системою.

До недоліків можна віднести:

- значні витрати, оскільки одна з робочих станцій буде використана як сервер;
- швидкість та ефективність системи будуть залежати від потужності самого сервера.

1.2 Теоретичні відомості щодо Active directory

Active Directory - це рішення від компанії Microsoft, яке є надійним та легким у налаштуванні. Воно дозволяє об'єднати всю мережу, що може

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						11
Змн.	Арк.	№ докум.	Підпис	Дата		

складатися з різних пристроїв, разом з інформацією про користувачів та інші дані в одну систему. У нашому випадку Active Directory виконуватиме роль сервера у невеликій мережі, забезпечуючи функції DHCP, DNS-сервера та моніторингу цієї мережі.

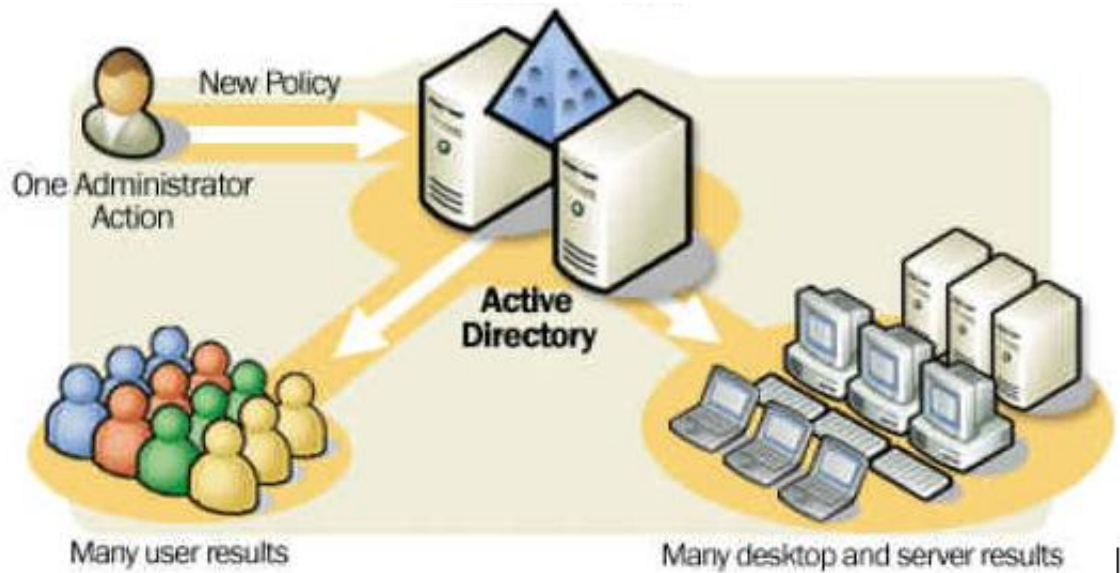


Рис.1.1. Принцип роботи Active directory в нашій системи

Ще однією перевагою Active Directory є зручне керування політиками. Це дозволяє розділити всіх користувачів на різні групи та надавати їм специфічні права на користування системою. У випадку політик у Active Directory існують прості рішення:

- Можливість змінювати та налаштовувати існуючі політики. Оскільки всі політики зберігаються в одній базі, зміни в одній політиці автоматично застосовуються до всієї системи.

- При створенні нового користувача і його включенні до однієї з груп, налаштування політик для цієї групи автоматично застосовуються й до нового користувача.

Active Directory також сприяє підвищенню захисту всієї мережі, оскільки всі дані зберігаються на контролерах доступу, які мають високий рівень захисту від зовнішнього доступу.

Компанія Microsoft інтегрувала в Active Directory можливість додавання сторонніх продуктів від інших компаній, що дозволяє організувати всі

пристрої та сервери в одну цілісну систему. До таких продуктів відносяться, наприклад:

- 1С;
- ІР-телефонія;
- віддалені робочі столи (Remote Desktop Gateway), які будуть використані в даному дипломному проєкті.[2].

Однією з особливостей AD є те, що всі дані та весь трафік проходять через сервер. Якщо цей сервер вийде з ладу, наприклад, у випадку відключення електропостачання в організації, то вся система та інші робочі станції стануть недоступними. Тому потрібно мати можливість додати один або декілька резервних серверів, які автоматично приймуть на себе роботу з такими ж налаштуваннями у разі відключення основного сервера. Додатково, якщо вийде з ладу вся система та всі резервні сервери, необхідно забезпечити регулярне резервне копіювання даних системи для швидкого відновлення її працездатності.

З усього вищезазначеного можна зробити висновок, що служба AD сильно впливає на роботу всієї системи. Тому, якщо потрібно правильно та коректно налаштувати систему організації, важливо залучати кваліфікованих спеціалістів, які допоможуть налаштувати AD та сервер в цілому для максимальної надійності та працездатності.

1.3 Протокол маршрутизації EIGRP

Протокол EIGRP (Enhanced Interior Gateway Routing Protocol) представляє собою вдосконалений внутрішній протокол маршрутизації, який застосовується в різних топологіях та мережах. Його належно налаштований екземпляр масштабується ефективно та забезпечує швидкий обмін даними з мінімальним обсягом мережевого трафіку. Принцип роботи протоколу відображено на рисунку 1.2.

Основні переваги протоколу EIGRP перед іншими включають:

- Ефективне використання мережевих ресурсів у звичайних умовах, оскільки лише hello-пакети передаються в стабільній мережі.

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						13
Змн.	Арк.	№ докум.	Підпис	Дата		

- При зміні топології розповсюджуються лише зміни в таблиці маршрутизації, а не вся таблиця. Це зменшує загальне навантаження мережі.
- Мінімізація часу конвергенції для змін в топології мережі.

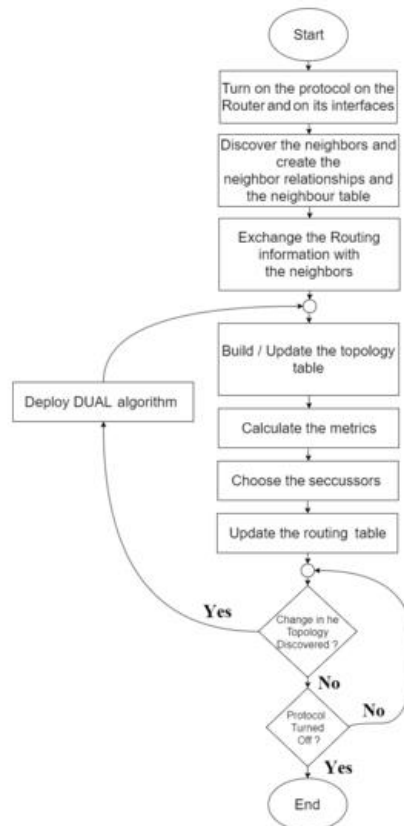


Рис. 1.2. Принцип роботи протоколу EIGRP

Розберемо дію протоколу EIGRP за допомогою схеми, представленої на рисунку 1.3.

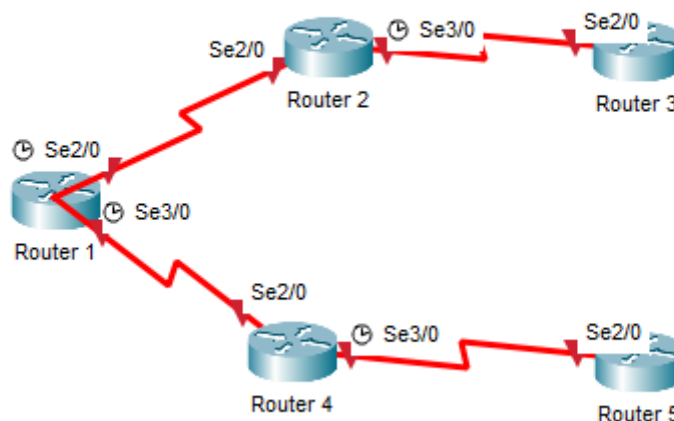


Рис. 1.3. Мережа для представлення протоколу EIGRP

Протокол EIGRP зберігає таблицю маршрутизації після кожного оновлення даних на маршрутизаторі та його сусідах. Він періодично запитує у сусідніх пристроях, чи вони володіють інформацією про інші мережі або додаткові маршрутизатори. На рисунку 1.2 показано мережу, де другий маршрутизатор володіє інформацією про своїх сусідів (перший та третій маршрутизатори). При необхідності передати дані до п'ятого маршрутизатора, другий маршрутизатор запам'ятовує шлях через перший. Якщо перший маршрутизатор виходить з ладу, другий маршрутизатор швидко переорієнтується та використовує топологію мережі для пошуку іншого можливого шляху до п'ятого маршрутизатора. [3].

Із цих пояснень можна зрозуміти наступне:

- Усі оновлення інформації про маршрутизацію отримуються за допомогою обміну даними з сусідніми маршрутизаторами.
- Якщо будь-який маршрут видаляється з таблиці топології мережі на одному маршрутизаторі, він також видаляється на інших маршрутизаторах.
- При втраті маршруту в таблиці маршрутизації запускається процес пошуку альтернативного маршруту до втраченої адреси.

Для передачі інформації про таблицю маршрутизації протокол EIGRP використовує не періодичне, адже оновлення відбувається тільки у випадку змін у маршрутах. Головним недоліком цього протоколу є неможливість точно визначити, коли певний маршрут стає недоступним. Тому кожні 5 або 60 секунд (залежно від пропускної здатності каналу) протокол EIGRP відправляє hello-пакети. Швидкість відправлення hello-пакетів називається інтервалом привітання і може бути налаштована за допомогою команди `ip hello-interval eigrp`. Крім того, існує параметр часу утримування, що вказує, як довго маршрутизатор буде вважати сусідній пристрій увімкненим, не отримуючи від нього hello-пакетів. Час утримування зазвичай дорівнює трьом інтервалам hello-пакетів (відповідно 15 та 180 секунд). Для зміни цього параметру використовується команда `ip hold-time eigrp`. При зміні інтервалу

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						15
Змн.	Арк.	№ докум.	Підпис	Дата		

hello-пакетів час утримування не змінюється автоматично, це потрібно робити окремо.

Якщо два маршрутизатори, налаштовані на протокол маршрутизації EIGRP, матимуть різний інтервал hello-пакетів та час утримування, вони все одно зможуть працювати разом.

Протокол EIGRP може підтримувати необмежену кількість сусідів, проте фактична можливість залежить від різних характеристик пристрою, таких як:

- обсяг доступної пам'яті;
- швидкість обробки інформації;
- обсяг переданої та отриманої інформації;
- складність топології мережі;
- стабільність мережевого з'єднання.

У протоколі EIGRP використовується відмінна від протоколів RIP та IGRP підхід до зберігання даних та забезпечення працездатності. Замість однієї таблиці маршрутизації, у EIGRP формується друга таблиця, відома як таблиця топології, на основі якої встановлюються маршрути для всіх пристроїв.

Для отримання інформації щодо формату таблиці топології мережі можна використати команду `show ip eigrp topology`. Ця таблиця міститиме дані, необхідні для побудови набору відстаней та векторів для кожної досяжної мережі, включаючи:

- найнижчу пропускну здатність каналів;
- загальну кількість затримок;
- надійність і завантаженість маршруту;
- найкоротша, допустима та оголошена відстань;
- джерело маршруту.

Протокол EIGRP використовує два основних параметри для розрахунку показників маршрутизації: мінімальну пропускну здатність та загальну

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						16
Змн.	Арк.	№ докум.	Підпис	Дата		

затримку. Незважаючи на це, можна налаштувати й інші метрики, але це може призвести до появи "петель" в мережі.

1.4. Протокол DHCP

Протокол DHCP є ключовим у великих мережах, де присутність багатьох робочих станцій. Його основне завдання - автоматичне налаштування параметрів мережевого адаптера. Налаштування DHCP може бути здійснене на маршрутизаторах Cisco або на серверах.[4].

Маршрутизатор може виконувати не лише роль DHCP сервера, але і функцію DHCP клієнта. Налаштування DHCP виявиться корисним, якщо вже наявний якийсь маршрутизатор, а мережу потрібно розширити за рахунок додавання нових пристроїв, таких як робочі станції, принтери, IP-телефони та інші. Тоді можна використати маршрутизатор для автоматичної настройки параметрів, щоб пристрої могли працювати самостійно, без втручання системного адміністратора.

Протокол DHCP дозволяє автоматично налаштовувати такі основні параметри:

- IP-адресу;
- маску мережі;
- основний шлюз;
- ім'я домену;
- DNS сервер. [5].

Давайте розглянемо процес отримання клієнтом даних від DHCP сервера більш детально. Спочатку робоча станція створює та відправляє широкомовний пакет, що складається з декількох фреймів. На другому рівні фрейму буде вказано MAC-адресу відправника (нашої робочої станції) та MAC-адресу отримувача у форматі аааа.аааа.аааа. Третій рівень фрейму буде містити IP-адресу відправника, проте оскільки її ще не відомо, ця частина буде порожньою. Такий пакет називається "DHCP discover".

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						17
Змн.	Арк.	№ докум.	Підпис	Дата		

Перший пакет отримують всі пристрої. Сервери DHCP, яких може бути кілька в мережі, збирають всю інформацію щодо DHCP і відправляють у зворотному напрямку необхідні дані, такі як IP-адреса, маска мережі, основний шлюз, ім'я домену, DNS сервер. При цьому на DHCP-сервері зарезервовується відповідна IP-адреса та виділяється на певний час (lease time). Пакет з усіма даними відправляється вже на нову адресу (DHCP offer).

Оскільки ми розглядаємо можливість наявності кількох DHCP серверів, клієнт обирає той, що відповідає найшвидше, і вже на нього відправляє із зазначенням своєї MAC-адреси та отриманої IP-адреси підтвердження всіх параметрів (DHCP request).

Після цього DHCP сервер зарезервовує відповідну IP-адресу для клієнта на певний час, оскільки до цього моменту вона була виділена, але не зарезервована. Після цього зазначена адреса і всі дані остаточно закріплюються за клієнтом. Тепер, після закріплення, сервер відправляє клієнту повідомлення, що клієнт успішно доданий до мережі (DHCP Acknowledge). Після цього клієнт починає коректну роботу. Формат повідомлення DHCP наведено у табл.1.1.

Таблиця 1.1

Формат DHCP пакету

Dynamic Host Configuration Protocol (DHCP)				
Бітове зміщення	0-15		16-31	
0	Код операції	Тип адреси на канальному рівні	Довжина апаратної адреси	Кількість переходів
32	ID операції			
64	Час операції		Flags	
96	Клієнтська IP-адреса			
128	IP-адреса яку пропонує сервер			
160	IP-адреса Серверу			

196	IP-адреса за замовчуванням
228+	MAC-адреса клієнту
	Ім'я домену або хосту
	Файл завантаження
	Додаткові налаштування

Давайте розглянемо кожен елемент у цьому пакеті:

1. OpCode - це код операції, який вказує на тип DHCP-пакету. Якщо йому присвоєно значення 0x01, це означає, що повідомлення є запитом від клієнта до серверу, а якщо 0x02 – відповіддю DHCP-сервера.

2. Hardware type - це тип адреси на канальному рівні.

3. Hardware length – це довжина апаратної адреси в байтах.

4. Transaction ID - це ID операції. Коли клієнт починає процес отримання IP-адреси, він генерує це значення, щоб сервер не переплутав конкретний процес цього клієнта з іншим.

5. Seconds elapsed (час операції) - це витрачений час в секундах. Рахується з початку отримання IP-адреси.

6. Flags – це спеціальні параметри для DHCP.

7. Client IP- це клієнтська IP-адреса. Це поле заповнюється тільки якщо DHCP-клієнт вже має якусь адресу. В інших випадках відправляється пустим.

8. Your IP – це адреса, яку пропонує DHCP-сервер.

9. Server IP– це IP-адреса серверу.

10. Gateway IP - це IP-адреса за замовчуванням. Застосовується тільки коли DHCP-сервер працює в режимі DHCP Relay Agent.

11. Client Hardware address – це MAC-адреса клієнту. Це поле заповнюється тільки тоді, коли на канальному рівні використовується Ethernet.

12. Server Host Name - це ім'я домену або хосту. Це поле заповнюється тільки тоді, коли у сервера є ім'я домену або хосту.

13. Boot file - це файл завантаження. Це поле заповнюється тільки якщо DHCP-сервер роздає назву файлу для завантаження.

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						19
Змн.	Арк.	№ докум.	Підпис	Дата		

14. Options - це додаткові налаштування. Це поле заповнюється, якщо задаються інші додаткові опції.

Сервер може назначити IP-адресу одним з трьох основних способів:

1. Статичний розподіл - подібний до ручного введення адреси на кожному комп'ютері. Однак відмінність полягає в тому, що системний адміністратор задає необхідні відповідності IP для MAC-адрес клієнтів безпосередньо на DHCP-сервері. IP-адреса залишається при клієнті навіть після виходу або переходу до іншої мережі.

2. Автоматичний розподіл - сервер закріплює IP з області за кожним клієнтом назавжди, тобто термін оренди необмежений.

3. Динамічний розподіл - DHCP-сервер назначає адресу з області на визначений проміжок часу. Цей підхід доцільний, якщо число доступних IP-адрес обмежено. IP призначається кожній станції при підключенні до мережі і повертається до області, як тільки клієнт її звільняє. У такому випадку IP може відрізнятись при кожному підключенні, але зазвичай призначається попередньо виданий.

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						20
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновки до розділу 1

Після аналізу особливостей гетерогенних мереж було виявлено основні принципи побудови схеми та методи її захисту. Наше завдання полягає в розробці підсистеми для гетерогенної мережі з можливістю віддаленого доступу до робочих станцій.

Варто розглянути можливість встановлення Active Directory на сервері Windows 10. Крім того, ми вибрали протокол маршрутизації EIGRP та протокол DHCP для автоматизації процесу підключення нових пристроїв.

Для обладнання ми вирішили скористатися виробником CISCO, оскільки на їхніх пристроях можна налаштувати всі обрані протоколи та технології. Для створення саме гетерогенної мережі будемо використовувати симулятор GNS3, що дозволить забезпечити взаємодію комунікаційних пристроїв та віртуальних машин з обраними операційними системами.

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						21
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЕКТУВАННЯ ГЕТЕРОГЕННОЇ МЕРЕЖІ З МОЖЛИВІСТЮ ВІДДАЛЕНИХ РОБОЧИХ СТОЛІВ

2.1 Принципи роботи мережі

При розробці мережі необхідно відразу логічно її структурувати. Ця підсистема складатиметься з декількох локальних мереж (LAN) та окремої підмережі з сервером на базі Windows 10 Server. [6].

При створенні цієї мережі необхідно виконати наступні вимоги:

- Створення підмережі з сервером, на якому буде налаштовано Active Directory.
- Використання різних операційних систем для забезпечення гетерогенності мережі.
- Забезпечення можливості роботи на віддалених робочих станціях.
- Автоматичне отримання IP-адрес (DHCP) для кожної підмережі.
- Захист підсистеми від дій злоумисників, конкурентів та недбалості власних працівників.

Оскільки проектування схеми передбачає використання великої кількості різних робочих станцій з різними ОС, важливо забезпечити достатню кількість IP-адрес. Необхідно налаштувати протокол DHCP для автоматизації процесу IP-адресації, враховуючи можливість додавання та виходу з ладу деяких робочих станцій. Для цього буде створено шість підмереж з різними DHCP-серверами та різними ОС. (табл. 2.1).

Розподіл на підмережі здійснюватиметься за допомогою DHCP-серверів на базі маршрутизаторів. Окремі підмережі будуть налаштовані для забезпечення зв'язку між маршрутизаторами рівня ядра. Також необхідно розробити IP-топологію мережі. Враховуючи значну кількість підмереж, внутрішню адресацію забезпечуватиме протокол динамічного налаштування вузлів. Детальні параметри адресації наведено в табл. 2.2.

Таблиця 2.1

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						22
Змн.	Арк.	№ докум.	Підпис	Дата		

Розподілення на підмережі пристроїв мережі

Назва мережі	Кількість робочих станцій	DHCP-сервер
LAN A	3 робочі станції і сервер (Можливість додавання робочих станцій)	Сервер під керуванням Windows 10 Server
LAN B	2 робочі станції (Можливість додавання робочих станцій)	Маршрутизатор
LAN C	3 робочі станції (Можливість додавання робочих станцій)	Маршрутизатор
LAN D	2 робочі станції (Можливість додавання робочих станцій)	Маршрутизатор
LAN E	3 робочі станції (Можливість додавання робочих станцій)	Маршрутизатор
LAN F	3 робочі станції (Можливість додавання робочих станцій)	Маршрутизатор

Таблиця 2.2

Параметри адресації мережі

Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Підмережа А				
Комутатор SW_6	Vlan 1	192.168.1.210	255.255.255.0	/24
Робоча станція WM_10	E0	DHCP	255.255.255.0	/24
Робоча станція WM_11	E0	DHCP	255.255.255.0	/24
Робоча станція WM_Win_10_server	E0	192.168.1.1	255.255.255.0	/24
Робоча станція WM_Win_XP	E0	DHCP	255.255.255.0	/24

...

Продовження таблиці 2.2

Підмережа В				
Комутатор SW_2	Vlan 1	192.168.2.210	255.255.255.0	/24
Робоча станція WM_9	E0	DHCP	255.255.255.0	/24
Робоча станція WM_Win_8_Lite	E0	DHCP	255.255.255.0	/24
Підмережа С				
Комутатор SW_1	Vlan 1	192.168.3.210	255.255.255.0	/24
Робоча станція WM_6	E0	DHCP	255.255.255.0	/24
Робоча станція WM_7	E0	DHCP	255.255.255.0	/24
Робоча станція WM_Ubuntu	E0	DHCP	255.255.255.0	/24
Підмережа D				
Комутатор SW_4	Vlan 1	192.168.4.210	255.255.255.0	/24
Робоча станція WM_8	E0	DHCP	255.255.255.0	/24
Робоча станція WM_Win_7	E0	DHCP	255.255.255.0	/24
Підмережа Е				
Комутатор SW_3	Vlan 1	192.168.5.210	255.255.255.0	/24
Робоча станція WM_4	E0	DHCP	255.255.255.0	/24
Робоча станція WM_Tinycore	E0	DHCP	255.255.255.0	/24
Робоча станція WM_5	E0	DHCP	255.255.255.0	/24
Підмережа F				
Комутатор SW_5	Vlan 1	192.168.6.210	255.255.255.0	/24
Робоча станція WM_1	E0	DHCP	255.255.255.0	/24
Робоча станція WM_2	E0	DHCP	255.255.255.0	/24
Робоча станція WM_3	E0	DHCP	255.255.255.0	/24
Ядро мережі				
Маршрутизатор R_1	E0/0	192.1.1.2	255.255.255.252	/30
	E0/1	DHCP	255.255.255.0	/24
	E0/2	192.168.5.1	255.255.255.0	/24
	E0/3	192.3.3.1	255.255.255.252	/30
Маршрутизатор R_2	E0/0	192.1.1.1	255.255.255.252	/30
	E0/1	192.168.1.2	255.255.255.0	/24
	E0/2	192.4.4.1	255.255.255.252	/30
	E0/3	192.168.3.1	255.255.255.0	/24
Маршрутизатор R_3	E0/0	192.168.4.1	255.255.255.0	/24
	E0/1	192.3.3.2	255.255.255.252	/30
	E0/2	192.2.2.2	255.255.255.252	/30
	E0/3	192.168.6.1	255.255.255.0	/24
Маршрутизатор R_4	E0/0	192.168.2.1	255.255.255.0	/24
	E0/1	192.2.2.1	255.255.255.252	/30
	E0/2	192.4.4.2	255.255.255.252	/30
	E0/3	DHCP	255.255.255.0	/24

2.2 Розробка логічної структури мережі

У цій схемі буде використано трирівневу ієрархічну модель мережі, оскільки вона є надійною та високопродуктивною. Мережа складатиметься з трьох рівнів: ядра, розподілу та доступу.[7].

Перевагами такої структури є:

1. Масштабованість – можливість вдосконалювати систему в майбутньому.
2. Швидке усунення неполадок та швидке і просте управління – за допомогою протоколу SSH[8] і віддалених робочих столів
3. Надійність – наявність резервних пристроїв, які можуть замінити основні у разі їхнього виходу з ладу.
4. Швидка працездатність – ієрархічна структура забезпечує високу пропускну здатність.

Розглянемо кожен з рівнів окремо.

Рівень ядра відповідає за швидке транспортування даних між пристроями рівня розподілу, тобто між комутаторами мережі. На цьому рівні зазвичай використовують дорогі пристрої високого класу, і за можливості – високопродуктивні комутатори.

Рівень розподілу знаходиться між рівнем ядра та рівнем доступу. Його завданням є забезпечення маршрутизації мережі та зв'язування рівнів ядра і доступу. Також на цьому рівні здійснюється фільтрація за допомогою ACLs та PBR. Основним завданням є зменшення навантаження на мережу.

Рівень доступу зазвичай складається з комутаторів і точок доступу, які дозволяють підключатися до робочих станцій, принтерів, IP-телефонів, серверів тощо. Найчастіше тут використовуються комутатори другого рівня через їх меншу вартість. Загальний вигляд розробленої схеми разом із зазначенням вищевказаних рівнів наведено на рисунку 2.1.

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						25
Змн.	Арк.	№ докум.	Підпис	Дата		

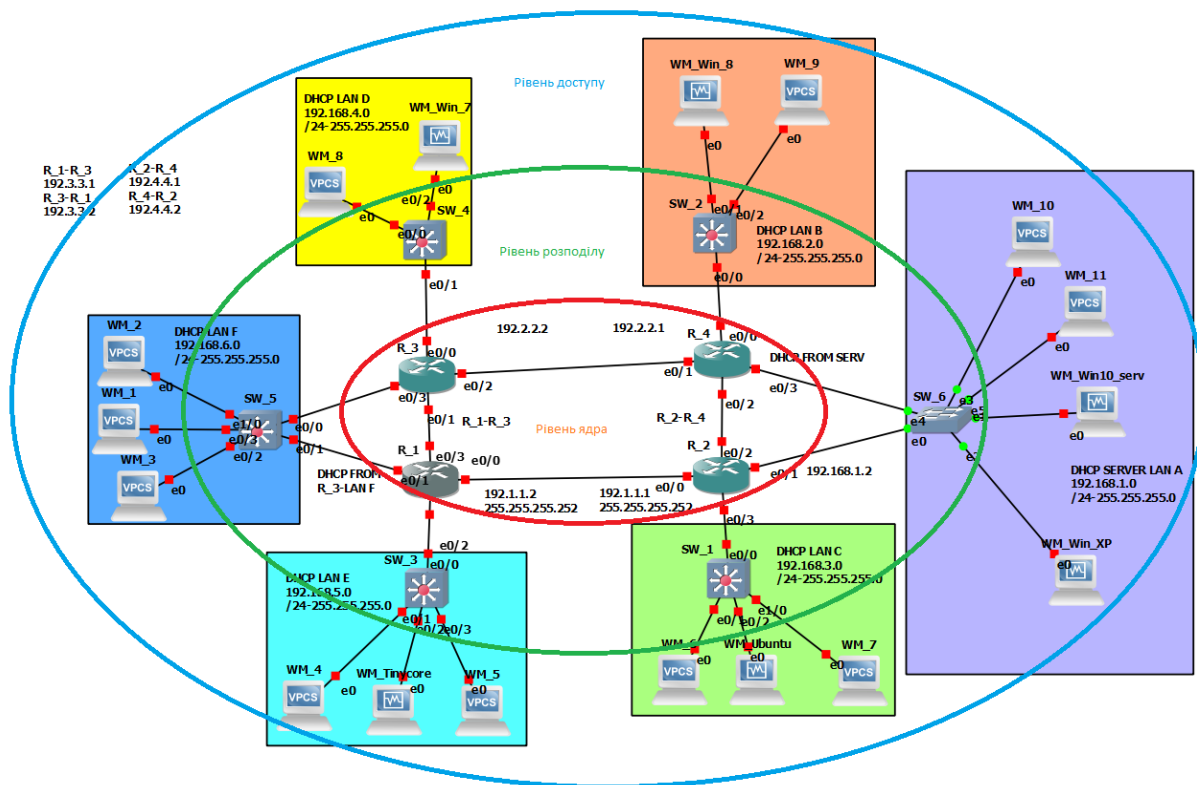


Рис.2.1. Трирівнева ієрархічна модель мережі

Детально розглянемо кожен з підмереж окремо. Зовнішній вигляд всіх LAN наведено на рисунках 2.2-2.7, пристрої, що входять до складу підмереж, зазначені в табл. 2.4-2.9.

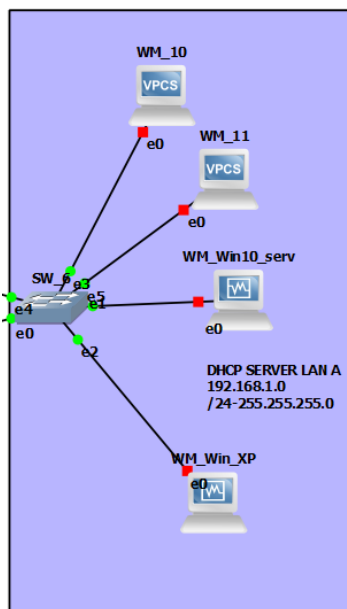


Рис.2.2. Локальна мережа LAN A

Змн.	Арк.	№ докум.	Підпис	Дата

Таблиця 2.4

Пристрої, що входять до складу LAN А

Робочі станції	Дві VPCS та робоча станція під управлінням ОС Windows XP
Комутатори	Один комутатор SW_6
Сервер	Один сервер від управлінням ОС Windows 10 server

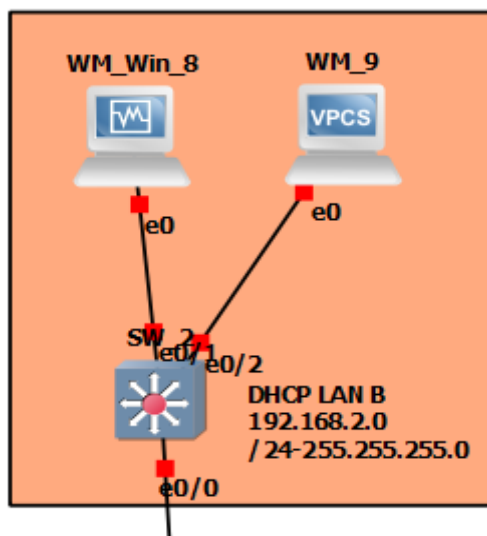


Рис.2.3. Локальна мережа LAN В

Таблиця 2.5

Пристрої, що входять до складу LAN В

Робочі станції	Дві робочі станції одна VPCS друга під управлінням ОС Windows 8 Lite
Комутатор	Комутатор другого рівня (образ i86bi-linux-l2-adventerprise-15.1b.bin)

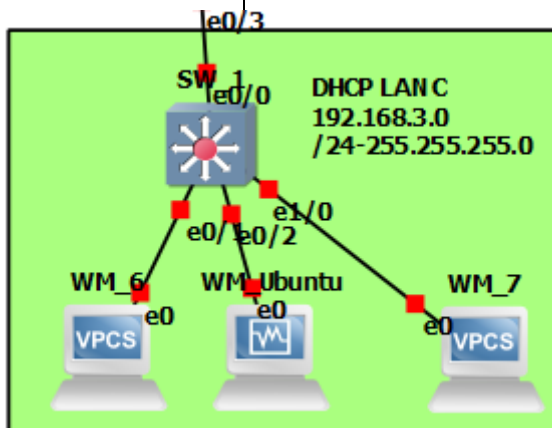


Рис.2.4. Локальна мережа LAN С

Таблиця 2.6

Пристрої, що входять до складу LAN C

Робочі станції	Три робочі станції дві VPCS третя під управлінням ОС Ubuntu
Комутатор	Комутатор другого рівня (образ i86bi-linux-l2-adventerprise-15.1b.bin)

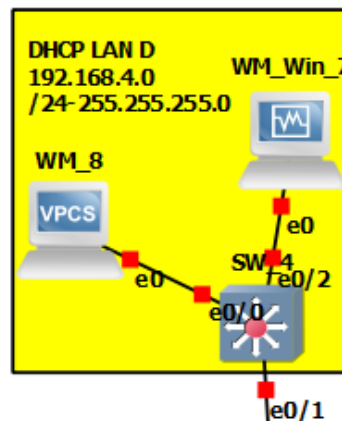


Рис.2.5. Локальна мережа LAN D

Таблиця 2.7

Пристрої, що входять до складу LAN D

Робочі станції	Дві робочі станції одна VPCS друга під управлінням ОС Windows 7
Комутатор	Комутатор другого рівня (образ i86bi-linux-l2-adventerprise-15.1b.bin)

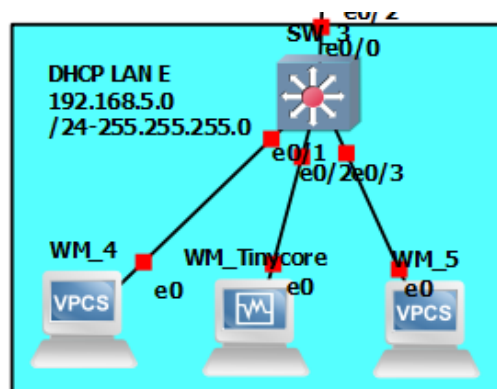


Рис.2.6. Локальна мережа LAN E

Пристрої, що входять до складу LAN E

Робочі станції	Три робочі станції дві VPCS третя під управлінням ОС Tinycore
Комутатор	Комутатор другого рівня (образ i86bi-linux-l2-adventerprise-15.1b.bin)

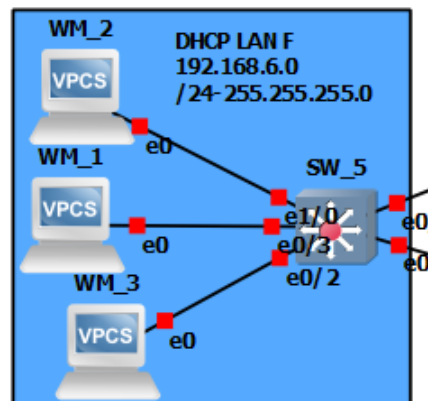


Рис.2.7. Локальна мережа LAN F

Пристрої, що входять до складу LAN F

Робочі станції	Три робочі станції під управлінням VPCS
Комутатор	Комутатор другого рівня (образ i86bi-linux-l2-adventerprise-15.1b.bin)

Окремо виділимо рівень ядра, що складається з чотирьох маршрутизаторів (i86bi-linux-l3-adventerprisek9-15.2.2.03T.bin). Його зовнішній вигляд відображає рисунок 2.8.

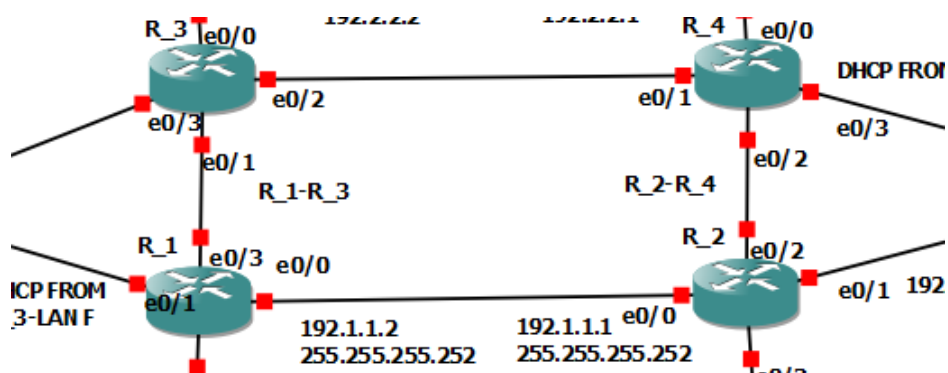


Рис.2.8. Рівень ядра

Проектована гетерогенна мережа створюється для організації або компанії, тому необхідно забезпечити її максимальну працездатність. Щоб прискорити відновлення доступу до мережі з робочих станцій у разі їхнього виходу з ладу або додавання нових, маршрутизатори будуть виконувати функції DHCP-серверів для кожної з підмереж.

Для стабільної роботи всієї мережі буде використано протокол зв'язку EIGRP, який є досить надійним. У разі проблем із зв'язком він швидко повідомляє інші пристрої в мережі та знаходить альтернативні шляхи до потрібного пристрою.

2.3 Проект підсистеми, вибір обладнання та програмного забезпечення.

Відповідно до потреб, що зазначені вище, сформовано такі вимоги до програмно-апаратного забезпечення:

1. Використання Windows 10 Server для налаштувань Active Directory.
2. Вибір наступних операційних систем: Windows XP[9], Windows 7[10], Windows 8 Lite[11], Ubuntu[12], Tinycore.
3. Висока надійність серверу.
4. Наявність віддаленого доступу до робочих станцій.
5. Наявність віддаленого захищеного доступу до пристроїв за допомогою SSH.

Захищеність мережі буде забезпечуватися: паролем доступом до маршрутизаторів, налаштуванням різних рівнів привілеї, захистом за допомогою DHCP-snooping, хешуванням md5[13], налаштуванням довірених портів за допомогою Port security[14].

Для реалізації схеми будемо використовувати обладнання фірми CISCO. Основними перевагами CISCO перед іншими компаніями є:

1. Надійність обладнання: Компанія CISCO перевірена часом і мільйонами одиниць інформаційного трафіку. Вона використовує тільки якісні компоненти та матеріали, починаючи від корпусу приладу і закінчуючи системою охолодження.

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						30
Змн.	Арк.	№ докум.	Підпис	Дата		

2. Широкий асортимент: CISCO пропонує великий вибір пристроїв, що підходять як для малих компаній та бізнесів, так і для інтернет-провайдерів та великих корпорацій. [15].
3. Гнучкість налаштувань: Один пристрій CISCO може виконувати різноманітні завдання, такі як маршрутизація, комутація, налаштування сервера, голосові сервіси, та захист від різних типів атак. Зазвичай, лише кілька команд достатні для додаткових функцій, що усуває потребу в придбанні додаткових пристроїв.
4. Високий рівень підтримки: Вся необхідна інформація щодо налаштування пристроїв CISCO доступна на офіційному сайті CISCO.COM. Системні адміністратори можуть знайти детальні описи моделей, їх характеристики та повну документацію щодо налаштування різних функцій.
5. Розширена гарантія: CISCO пропонує гарантії на всі свої пристрої, включаючи старі моделі, на будь-який термін. У випадку несправності пристрою, компанія забезпечує повну заміну пристрою або його частини протягом 4-8 годин, що є критично важливим для великих компаній. [16].

Отже, можна зробити висновок, що пристрої компанії CISCO є надзвичайно гнучкими в налаштуваннях і надійними, що робить їх ідеальними як для великих корпорацій, так і для невеликих бізнесів. Тому ми будемо використовувати образи маршрутизатора серії 4000[17] (рис.2.9) та комутатора 9300 [18](рис.2.10).

Для розробки моделі комп'ютерної гетерогенної мережі з можливістю віддалених робочих столів будемо користуватися програмою GNS3. Додатково використовується програма VirtualBox, а також WireShark для перевірки трафіку в нашій мережі.



Рис.2.9.Маршрутизатор останньої серії (Cisco 4000 Series Integrated Services Routers)



Рис. 2.10.Комутатор останньої серії (Cisco Catalyst серії 9300)

GNS3 (Graphical Network Simulator) - це графічний симулятор мережі, який дозволяє створювати, тестувати та захищати мережі безпосередньо на комп'ютері. Його основною перевагою є можливість розробки гетерогенних мереж за допомогою додавання різних типів обладнання з різними образами, такими як Cisco, Juniper, Mikrotik, CheckPoint і багато інших. Це означає, що GNS3 дозволяє запускати операційні системи різних виробників безпосередньо в одній системі. Наприклад, додавши маршрутизатор Cisco в GNS3, ви запускаєте реальну операційну систему Cisco IOS, що надає повноцінний функціонал маршрутизатора Cisco.

Основна перевага GNS3 полягає в тому, що він відтворює всі можливості пристроїв, надаючи доступ до всіх команд, які працюють на реальному обладнанні. Це робить його цінним інструментом для розробки та тестування мереж. На відміну від Cisco Packet Tracer, який не підтримує всі команди і не може демонструвати гетерогенність мережі. [19].

GNS3 дозволяє додавати та налаштовувати повноцінні робочі станції та сервери. У відмінність від Cisco Packet Tracer, де кінцевими пристроями є обмежені робочі станції з невеликим функціоналом, GNS3 дозволяє

використовувати різні операційні системи, такі як Windows XP, Windows 7, Linux Ubuntu та інші. Також, якщо потрібно додати сервер, можна використовувати, наприклад, Windows 10 Server. Це дозволяє створювати реалістичні мережі та навіть під'єднувати їх до реальних мереж Інтернету. Не менш важливою перевагою є те, що GNS3 є безкоштовним.

Однак найбільшим недоліком GNS3 є неможливість додавання повноцінних комутаторів. Замість цього, користувачам потрібно використовувати стандартний комутатор, що постачається разом з GNS3. Це через те, що реальні комутатори мають мікросхеми ASIC, які неможливо відтворити в симуляторах на звичайних комп'ютерах. ASIC мікросхеми забезпечують високу продуктивність та обробку пакетів, тому їх відсутність у симуляторі може бути обмеженням.

Однак симуляція реальних пристроїв та операційних систем має ще один недолік - високі вимоги до параметрів та ресурсів комп'ютера, на якому працює GNS3. Наприклад, для створення гетерогенної мережі потрібно запускати декілька віртуальних машин з операційними системами Windows та Linux. Проте, навіть для запуску лише однієї машини під керуванням Windows 10, потрібно мати щонайменше 4 гігабайти оперативної пам'яті.

VirtualBox - це програма для віртуалізації різних операційних систем, яка, що дуже важливо, працює майже на всіх платформах, таких як Windows, Linux, macOS та інші. VirtualBox має єдиний формат образів для віртуалізації, тому, наприклад, віртуальна машина з операційною системою Linux може бути переміщена з Windows і працювати без помилок. [20].

VirtualBox має кілька переваг. По-перше, він має дуже зрозумілий та дружелюбний інтерфейс, що робить його легким у використанні для користувачів на будь-якому рівні. Крім того, програма підтримує широкий спектр форматів образів, що означає, що ви можете встановити не лише операційні системи, але й образи маршрутизаторів, таких як Mikrotik, і використовувати їх у GNS3.

VirtualBox працює на основі віртуалізації різних операційних систем. Це означає, що після створення віртуальної мережі ви можете встановити практично будь-яку операційну систему і працювати на ній так, ніби це звичайний комп'ютер.

Можливості VirtualBox:

- запускати кілька віртуальних машин одночасно;
- налаштовувати параметри та кількість ресурсів основного комп'ютера для кожної віртуальної машини окремо;
- експортувати та імпортувати готові образи віртуальних машин;
- "заморожувати" стан віртуальної машини, щоб зменшити витрати ресурсів на машини, які тимчасово не використовуються;
- обмінюватися даними через спільні папки та файли між основним комп'ютером і віртуальними машинами, а також між самими віртуальними машинами;
- робити скріншоти та записувати відео з екрану віртуальних машин.

Wireshark — надзвичайно потужна програма для аналізу та перехоплення мережевого трафіку. Це програмне забезпечення доступне на операційних системах Linux, Windows, NetBSD, Mac OS та інших. Воно необхідне для детального аналізу трафіку. Крім того, якщо виникають проблеми, наприклад, з протоколом маршрутизації, Wireshark допомагає визначити причину проблеми та знайти місце втрати пакетів. [21].

Висновки до розділу 2

Було спроектовано підсистему гетерогенної мережі, що складається з шести локальних підмереж та маршрутизаторів рівня ядра. Обґрунтовано необхідність використання трирівневої ієрархічної моделі. Сформовано таблицю параметрів інтерфейсів та адресації пристроїв мережі.

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

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						35
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 НАЛАШТУВАННЯ ТА ДОСЛІДЖЕННЯ ПІДСИСТЕМИ ЗАХИСТУ ГЕТЕРОГЕННОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ З МОЖЛИВІСТЮ ВІДДАЛЕНИХ ПІДКЛЮЧЕНЬ НА БАЗІ ПРОТОКОЛУ МАРШРУТИЗАЦІЇ EIGRP.

3.1 Налаштування мережі

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

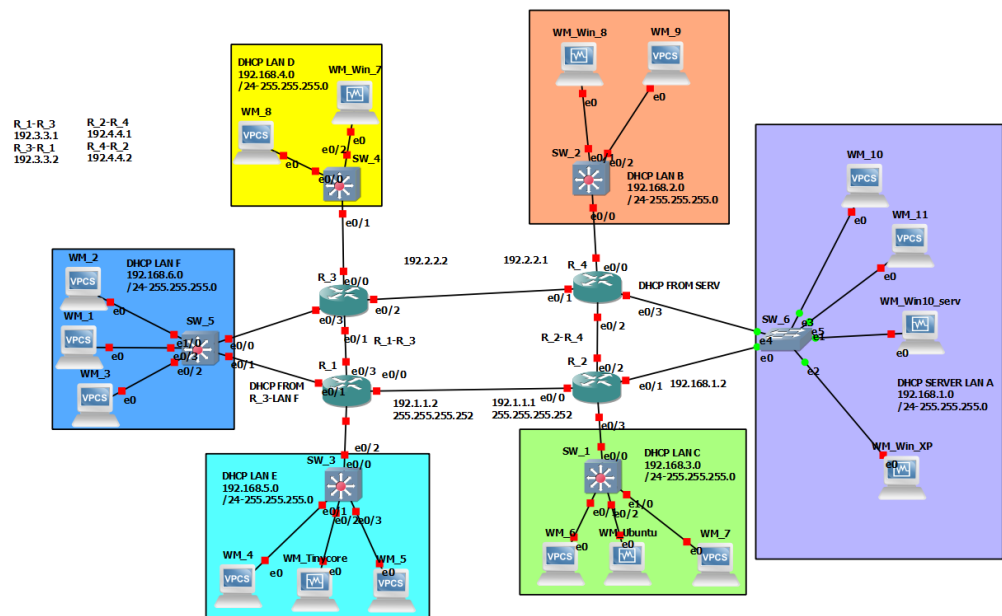


Рис. 3.1 Повна схема мережі

Далі налаштуємо Active directory на базі Windows 10 Server. Перед цим проведемо стандартні мережеві налаштування для серверу(рис.3.2-3.4).

Имя компьютера, имя домена и параметры рабочей группы

Имя компьютера: Server_WIN10

Полное имя: Server_WIN10

Описание: Server_WIN10

Рабочая группа: WORKGROUP

Изменить параметры

Рис. 3.2. Встановлення всіх служб для роботи серверу

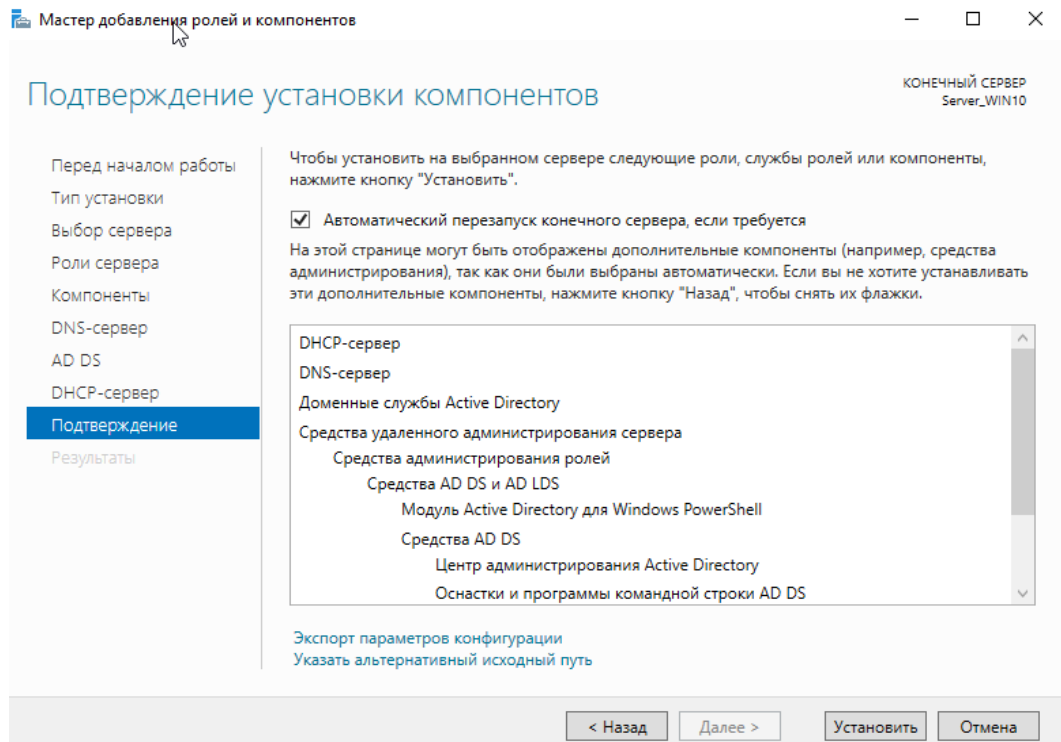


Рис. 3.3. Встановлення всіх служб для роботи серверу

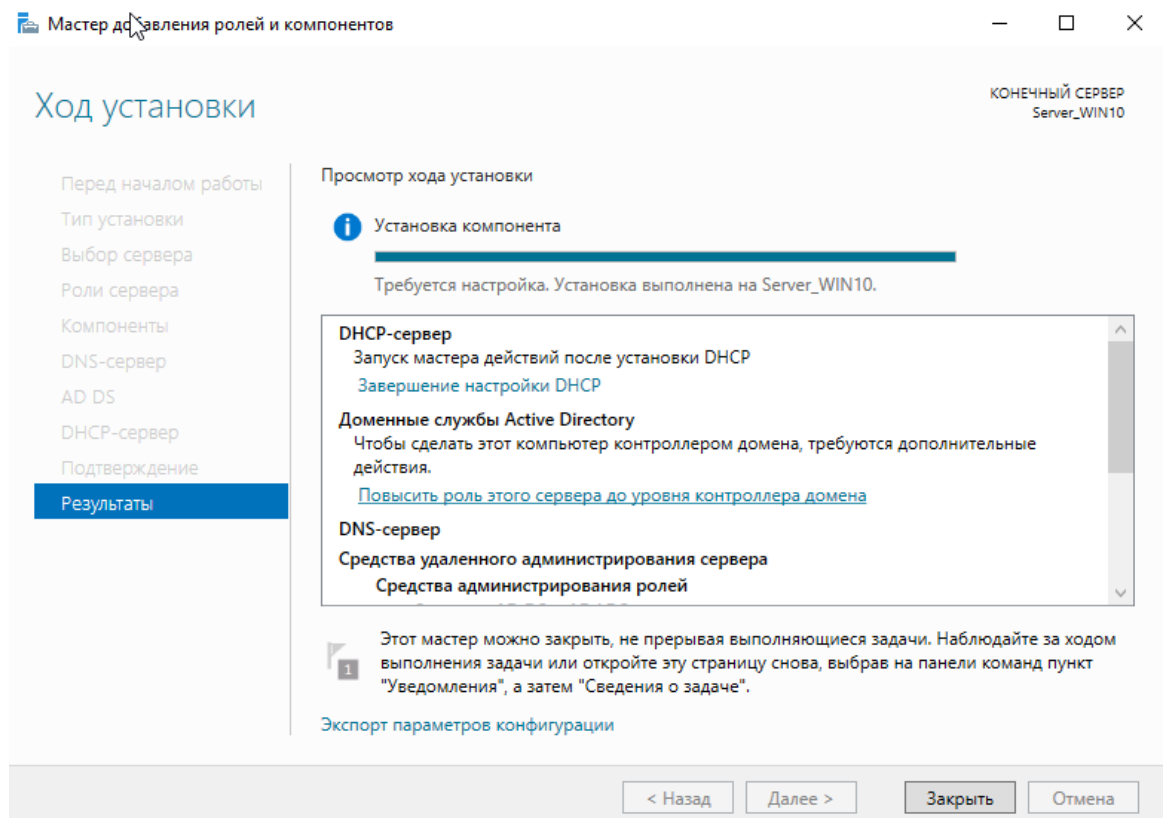


Рис. 3.4. Встановлення всіх служб для роботи серверу

Після встановлення служб DHCP, DNS та AD на сервері, необхідно налаштувати кожну службу окремо для забезпечення їх коректної

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						37
Змн.	Арк.	№ докум.	Підпис	Дата		

роботи. Спершу налаштовується доменна служба Active Directory для створення домену мережі, щоб пристрої, які використовуватимуть цей домен, могли приймати та виконувати всі групові політики, налаштовані на сервері.(рис.3.5-3.7).

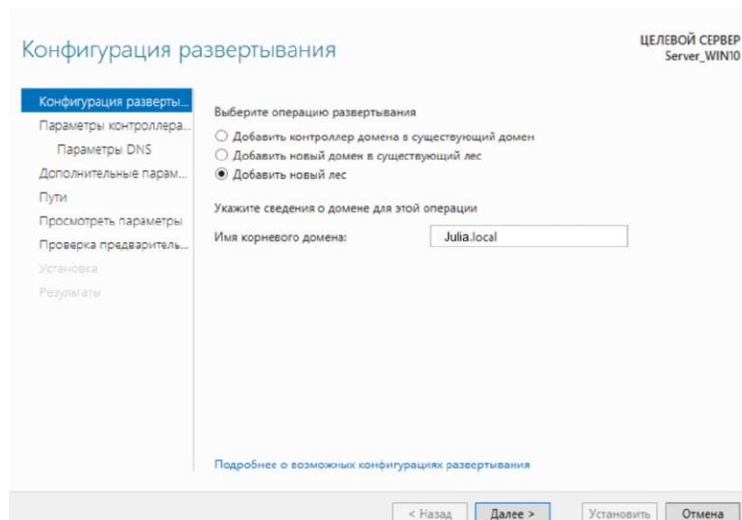


Рис. 3.5. Налаштування служби Active Directory

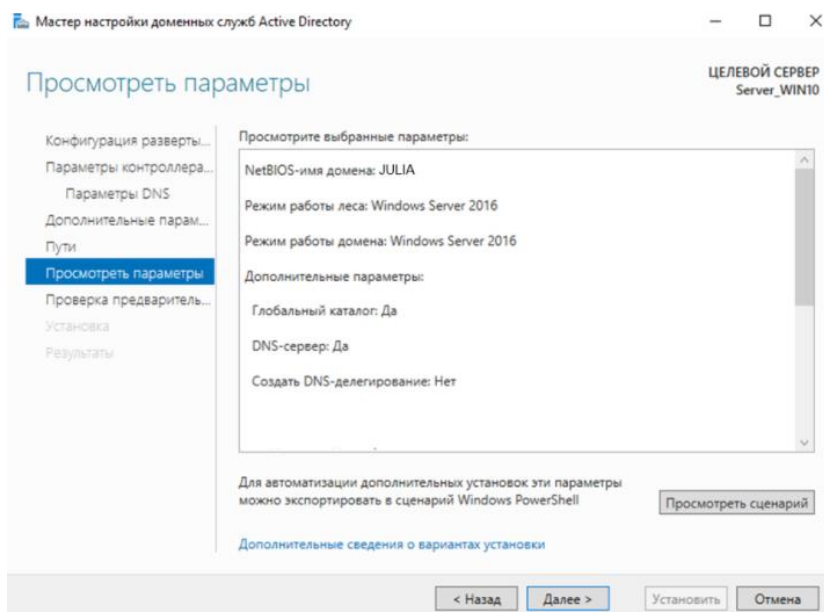


Рис. 3.6. Налаштування служби Active Directory

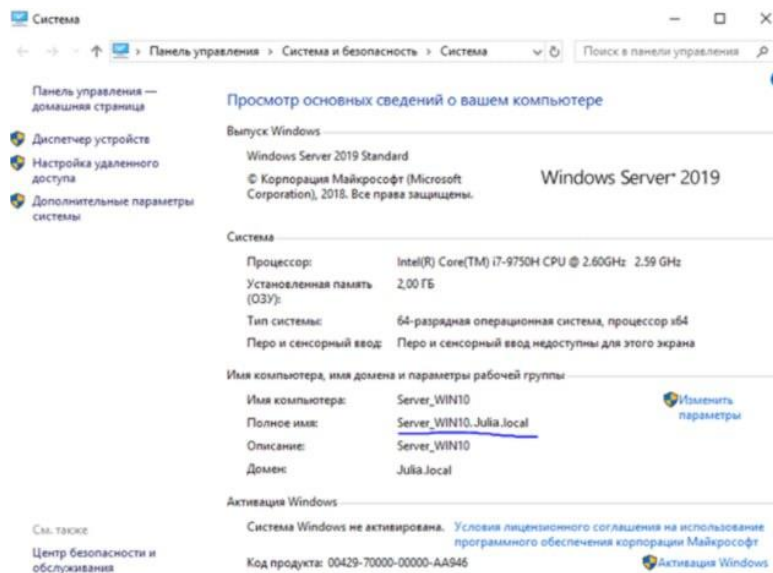


Рис. 3.7. Налаштування служби Active Directory

Як бачимо, після перезавантаження серверу створився домен під назвою Julia.local та до повного ім'я серверу додалася назва домену.

Також налаштуємо сервер DHCP на Windows 10 Server для майбутнього масштабування мережі та спрощення підключення локальних робочих станцій. (рис.3.8-3.9).

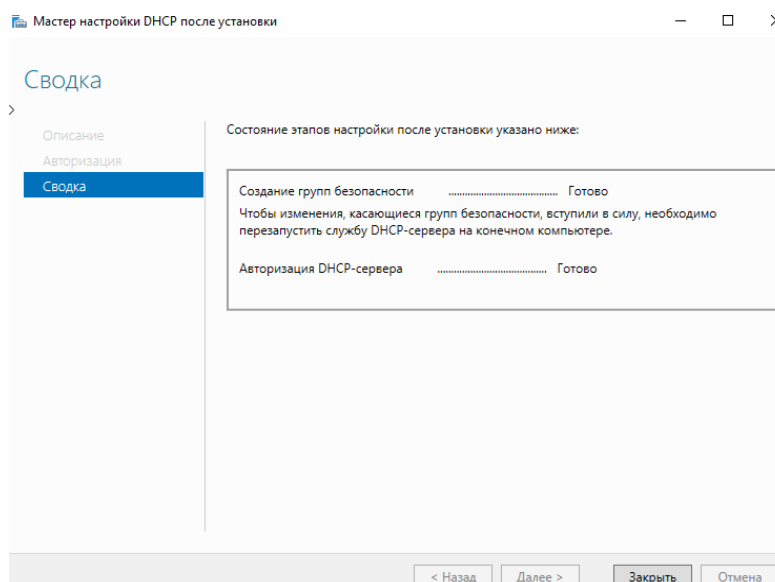


Рис. 3.8. Налаштування служби DHCP

Мастер создания области

Добавление исключений и задержка

Исключения являются адресами или диапазонами адресов, которые исключаются из распределения DHCP-сервером. Задержка определяет время, на которое будет задержана передача сообщения DHCP OFFER с сервера.

Введите диапазон IP-адресов, который необходимо исключить. Если вы хотите исключить один адрес, введите его только в поле "Начальный IP-адрес".

Начальный IP-адрес: Конечный IP-адрес:

Исключаемый диапазон адресов:

192.168.1.1-192.168.1.20	Удалить
192.168.1.90-192.168.1.100	

Задержка подсети в миллисекундах:

Рис. 3.9. Налаштування служби DHCP

Додатково налаштуємо DNS на сервері, оскільки він виконує дві основні функції: зберігання даних про IP-адреси домену та кешування інших ресурсів сервера. (рис.3.10-3.11).

Мастер создания новой зоны

Область репликации зоны, интегрированной в Active Directory

Вы можете указать, каким образом следует реплицировать данные DNS в вашей сети.

Укажите, каким образом вы хотите реплицировать информацию зоны:

☐ Для всех DNS-серверов, работающих на контроллерах домена в этом лесу: julia.local

☒ Для всех DNS-серверов, работающих на контроллерах домена в этом домене: julia.local

☐ Для всех контроллеров домена в этом домене (для совместимости с Windows 2000): julia.local

☐ На все контроллеры домена, указанные в области данного раздела каталога:

Рис. 3.10. Налаштування служби DNS

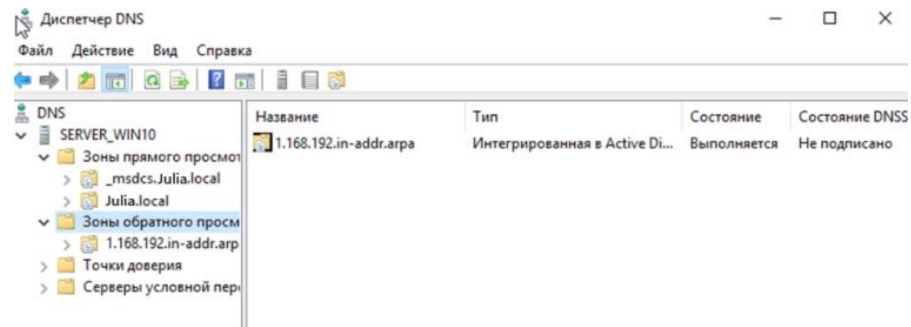


Рис. 3.11. Налаштування служби DNS

Після проведених налаштувань на Windows 10 Server, налаштуємо IP-адресацію на всіх маршрутизаторах. На рисунку 3.12 наведено лістинг налаштування адресації на R_1. На інших пристроях мережі воно проводиться аналогічно.

```
R_1 - PuTTY
*Apr 24 08:26:24.309: %LINK-5-CHANGED: Interface Serial2/0, changed state to administratively down
*Apr 24 08:26:24.309: %LINK-5-CHANGED: Interface Serial2/1, changed state to administratively down
R_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1(config)#int e0/0
R_1(config-if)#ip add 192.1.1.2 255.255.255.252
R_1(config-if)#no shut
R_1(config-if)#exit
*Apr 24 08:54:35.837: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Apr 24 08:54:36.842: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
R_1(config-if)#ex
R_1(config)#int e0/2
R_1(config-if)#ip add 192.168.5.1 255.255.255.0
R_1(config-if)#no shut
R_1(config-if)#exit
R_1(config)#int
*Apr 24 08:55:01.251: %LINK-3-UPDOWN: Interface Ethernet0/2, changed state to up
*Apr 24 08:55:02.256: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2, changed state to up
R_1(config)#int e0/1
R_1(config-if)#ip add 192.168.6.1 255.255.255.0
R_1(config-if)#no shut
R_1(config-if)#exit
R_1(config)#int e0/3
*Apr 24 08:55:22.526: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*Apr 24 08:55:23.529: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
R_1(config)#int e0/3
R_1(config-if)#ip add 192.3.3.1 255.255.255.252
R_1(config-if)#no shut
R_1(config-if)#exit
R_1(config)#
*Apr 24 08:55:52.229: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to up
*Apr 24 08:55:53.236: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to up
R_1(config)#
```

Рис. 3.12. Налаштування IP-адресації на R_1

Тепер налаштуємо протокол маршрутизації для забезпечення зв'язку між маршрутизаторами, комутаторами та іншими пристроями. В нашому випадку це протокол EIGRP (рис.3.13)

```

R_1#copy running-config st
R_1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1(config)#router eigrp 1
R_1(config-router)#network 192.1.1.0
^
% Invalid input detected at '^' marker.
R_1(config-router)#network 192.1.1.0
R_1(config-router)#network 192.1.1.0
*Apr 24 09:06:24.221: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 192.1.1.1 (Ethernet0/0) is up: new adjacency
R_1(config-router)#network 192.168.5.0
R_1(config-router)#network 192.3.3.0
R_1(config-router)#network 192.168.6.0
R_1(config-router)#

```

Рис. 3.13. Налаштування протоколу EIGRP на R_1

Оскільки в нашій мережі використовується досить багато робочих станцій, то налаштуємо протокол DHCP на маршрутизаторах (рис.3.14).

```

R_1(config-if)#ip add 192.3.3.1 255.255.255.252
R_1(config-if)#no shut
R_1(config-if)#exit
R_1(config)#
*Apr 24 08:55:52.229: %LINK-3-UPDOWN: Interface Ethernet0/3, changed state to up
*Apr 24 08:55:53.236: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/3, changed state to up
R_1(config)#ip dhcp pool LAN_E
R_1(dhcp-config)#network 192.168.5.0 255.255.255.0
R_1(dhcp-config)#de
R_1(dhcp-config)#default-router 192.168.5.1
R_1(dhcp-config)#exit
R_1(config)#

```

Рис. 3.14. Налаштування протоколу DHCP на R_1

Для налаштування віддалених робочих столів в операційних системах Windows, починаючи з версії Windows XP, достатньо натиснути WIN+R і ввести команду mstsc.exe. Однак, для операційної системи Ubuntu необхідно встановити спеціальний додаток (Vinagre), щоб підключитися до віддалених робочих столів Windows. (рис.3.15).

```

Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  i965-va-driver intel-media-va-driver libavahi-gobject0 libccard0
  libgtk-vnc-2.0-0 libgvnc-1.0-0 libigdgmm11 libphodav-2.0-0
  libphodav-2.0-common libspice-client-glib-2.0-8 libspice-client-gtk-3.0-5
  libusbredirhost1 libusbredirparser1 libva-x11-2 libva2 mesa-va-drivers
  spice-client-glib-usb-acl-helper va-driver-all
Предлагаемые пакеты:
  i965-va-driver-shaders gstreamer1.0-libav gstreamer1.0-plugins-bad
Следующие НОВЫЕ пакеты будут установлены:
  i965-va-driver intel-media-va-driver libavahi-gobject0 libccard0
  libgtk-vnc-2.0-0 libgvnc-1.0-0 libigdgmm11 libphodav-2.0-0
  libphodav-2.0-common libspice-client-glib-2.0-8 libspice-client-gtk-3.0-5
  libusbredirhost1 libusbredirparser1 libva-x11-2 libva2 mesa-va-drivers
  spice-client-glib-usb-acl-helper va-driver-all vinagre
Обновлено 0 пакетов, установлено 19 новых пакетов, для удаления отмечено 0 паке
тов, и 91 пакетов не обновлено.
Необходимо скачать 7.346 кВ архивов.
После данной операции объем занятого дискового пространства возрастёт на 52,5 М
В.
Показать приложения [д/н]

```

Рис. 3.15. Встановлення додатку на ОС Ubuntu

Після налаштування маршрутизації та віддалених робочих столів необхідно налаштувати безпеку пристроїв. Спочатку захистимо наші маршрутизатори, створивши користувачів з різними рівнями доступу.(рис. 3.16-3.18).

```

R_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1(config)#privilege exec level 1 show running-config
R_1(config)#privilege exec level 1 show interface
R_1(config)#privilege exec level 1 show ip interface
R_1(config)#privilege exec level 1 show ip route
R_1(config)#username USER privilege 1 secret cisco
R_1(config)#line console 0
R_1(config-line)#login local
R_1(config-line)#exec-timeout 10
R_1(config-line)#exit
R_1(config)#exit
R_1#
*May  1 10:47:43.588: %SYS-5-CONFIG_I: Configured from console by admin on conso
le
R_1#

```

Рис. 3.16. Налаштування користувачів на R_1

```

R_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1(config)#privilege exec level 3 configure terminal
R_1(config)#privilege configure level 3 interface
R_1(config)#privilege interface level 3 description
R_1(config)#privilege interface level 3 shutdown
R_1(config)#privilege interface level 3 switchport mode
% Unknown command 'switchport mode'
R_1(config)#privilege exec level 3 show running-config
R_1(config)#privilege exec level 3 write memory
R_1(config)#username Nykyta privilege 3 secret 15032000
R_1(config)#line console 0
R_1(config-line)#login local
R_1(config-line)#exec-timeout 10
R_1(config-line)#exit
R_1(config)#end
R_1#exit

```

Рис. 3.17. Налаштування користувачів на R_1

```

R_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1(config)#banner login #=====
Enter TEXT message. End with the character '#'.
Device hostname -$(R_1)
Your connection is -$(line)
Enter Admin's LOGIN and Password
=====#
R_1(config)#username admin privilege 15 secret cisco
R_1(config)#line console 0
R_1(config-line)#login local
R_1(config-line)#exec-timeout 10
R_1(config-line)#end
R_1#
*May 1 10:23:13.016: %SYS-5-CONFIG_I: Configured from console by console
R_1#

```

Рис. 3.18. Налаштування користувачів на R_1

Додатково налаштуємо параметри захисту на комутаторах, оскільки в нашій мережі присутні різні DHCP-сервери. Якщо злоумисник зможе підключити свій DHCP-сервер, це може призвести до втрати даних, що зберігаються на робочих станціях. Тому ми налаштуємо функцію довіреного порту на комутаторах. (рис.3.19).

```

SW_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW_1(config)#int vlan 1
SW_1(config-if)#ip add 192.168.3.210 255.255.255.0
SW_1(config-if)#no shut
SW_1(config-if)#exit
SW_1(config)#
*May 1 18:26:55.909: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*May 1 18:26:56.910: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
SW_1(config)#ip dhcp snooping vlan 1
SW_1(config)#int e0/0
SW_1(config-if)#ip dhcp snooping trust
SW_1(config-if)#ip dhcp snooping limit rate 50
SW_1(config-if)#exit
SW_1(config)#no ip dhcp snooping information option
SW_1(config)#exit
SW_1#
*May 1 18:27:50.039: %SYS-5-CONFIG_I: Configured from console by console
SW_1#

```

Рис. 3.19. Налаштування довіреного порту на комутаторі SW_1

Також налаштуємо функцію PortSecurity на комутаторах (рис.3.20).

```

May 19 07:28:02.737: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0, changed state to up
May 19 07:28:02.748: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1, changed state to up
May 19 07:28:02.761: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet2, changed state to up
May 19 07:28:02.772: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet3, changed state to up
May 19 07:28:35.391: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
May 19 07:28:36.392: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
SW_1#QQ
SW_1#
SW_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW_1(config)#int range e0/0-3
SW_1(config-if-range)#switchport mode access
SW_1(config-if-range)#switchport port-security
SW_1(config-if-range)#switchport port-security maximum 100
SW_1(config-if-range)#switchport port-security mac-address sticky
SW_1(config-if-range)#end
SW_1#
May 19 07:38:51.336: %SYS-5-CONFIG_I: Configured from console by console
SW_1#

```

Рис. 3.20. Налаштування Port Security на комутаторі SW_1

Для хешування даних налаштуємо MD5 на маршрутизаторах (рис.3.21).

```

User Access Verification
Username: admin
Password:
R_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1(config)#key chain authEIGRP
R_1(config-keychain)#key 1
R_1(config-keychain-key)#key-string cisco12345
R_1(config-keychain-key)#int e0/3
R_1(config-if)#ip autn
R_1(config-if)#ip authentication mode eigrp 100 md5
^
% Invalid input detected at '^' marker.
R_1(config-if)#ip authentication mode eigrp 100 md5
R_1(config-if)#ip authentication key-chain eigrp 100 authEIGRP
R_1(config-if)#end
R_1#

```

Рис. 3.21. Налаштування хешування MD5 на маршрутизаторі R_1

Для можливості віддаленого налаштування маршрутизаторів та інших пристроїв ми налаштуємо захищений протокол віддаленого доступу SSH. (рис.3.22).

```

R_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1(config)#ip domain-name SSH
R_1(config)#crypto key generate rsa
The name for the keys will be: R_1.SSH
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
R_1(config)#
*May 15 09:25:50.343: %SSH-5-ENABLED: SSH 1.99 has been enabled
R_1(config)#line vty 0 4
R_1(config-line)#transport input ssh
R_1(config-line)#login local
R_1(config-line)#ip ssh ver
^
% Invalid input detected at '^' marker.
R_1(config-line)#ip ssh ver 2
R_1(config)#username R_1 privilege 15 pass ssh
R_1(config)#end

```

Рис. 3.22. Налаштування протоколу віддаленого доступу SSH

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						45
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2 Тестування підсистеми захисту гетерогенної мережі організації з можливістю віддалених підключень на базі протоколу маршрутизації EIGRP

Тестування підсистеми захисту гетерогенної мережі організації проводиться з метою перевірки налаштувань на відповідність поставленим завданням.

Перше, що потрібно зробити, це перевірити налаштування адресації сервера та наявність зв'язку між ним і пристроями мережі. (рис.3.23-3.26).

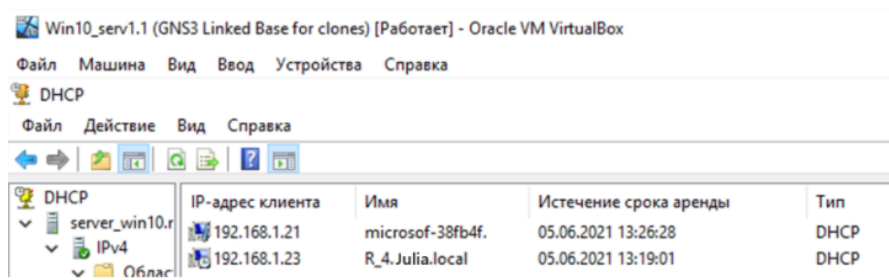


Рис. 3.23. Перевірка налаштувань серверу

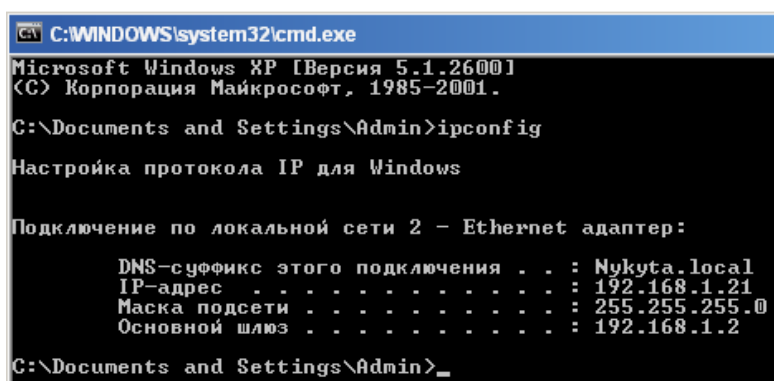


Рис. 3.24. Перевірка налаштувань серверу

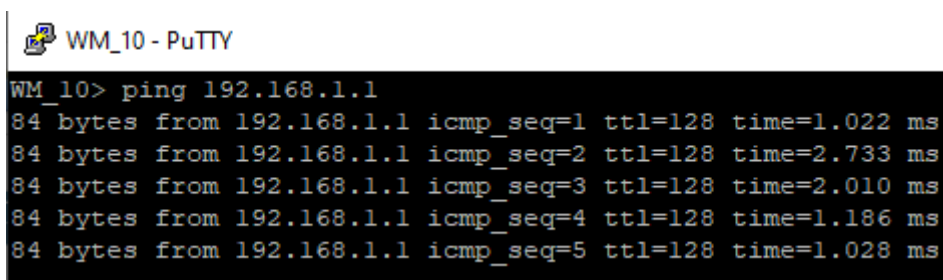


Рис. 3.25. Перевірка зв'язку з робочих станцій на серверу

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Admin>ping 192.168.1.1

Обмен пакетами с 192.168.1.1 по 32 байт:

Ответ от 192.168.1.1: число байт=32 время=1мс TTL=128
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=128
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=128
Ответ от 192.168.1.1: число байт=32 время=1мс TTL=128

Статистика Ping для 192.168.1.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
Приблизительное время приема-передачи в мс:
    Минимальное = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек

```

Рис. 3.26. Перевірка зв'язку з робочих станцій на серверу

Давайте перевіримо роботу інших DHCP-серверів, зокрема, чи вони надають адреси робочим станціям і чи виникають при цьому конфлікти. (рис.3.27-3.28).

```

tc@box:~$ dhclient
sh: dhclient: Permission denied
tc@box:~$ sudo dhclient
udhcpd (v1.19.0) started
Sending discover...
Sending select for 192.168.5.2...
Lease of 192.168.5.2 obtained, lease time 86400
deleting routers
route: SIOCDELRT: No such process
tc@box:~$

```

Рис. 3.27. Перевірка DHCP серверу

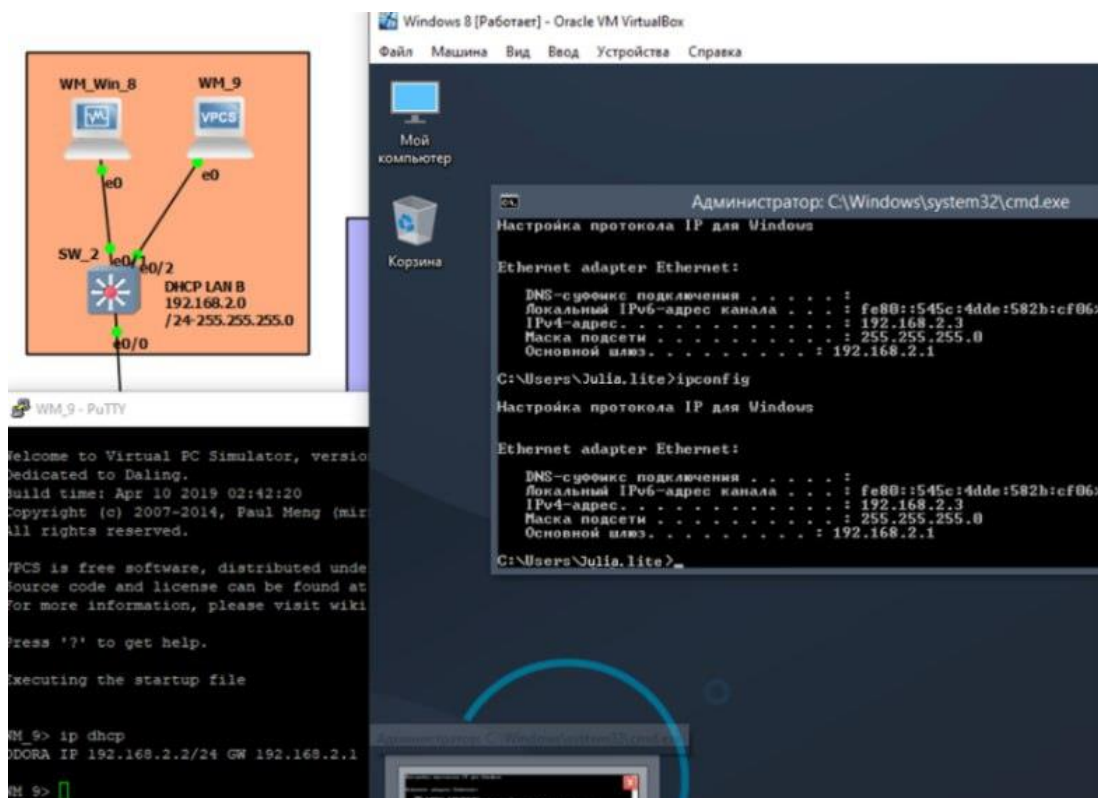


Рис. 3.28. Перевірка DHCP серверу

Тепер спробуємо зайти під користувачем admin на маршрутизаторі R_1 і перевіримо результат хешування у перехопленому повідомленні (рис.3.29-3.30).

```

net0/0) is up: new adjacency=====
Device hostname -$(R_1)
Your connection is -0
Enter Admin's LOGIN and Password
=====

User Access Verification

Username: admin
Password:
R_1#

```

Рис. 3.29. Перевірка налаштувань користувачів

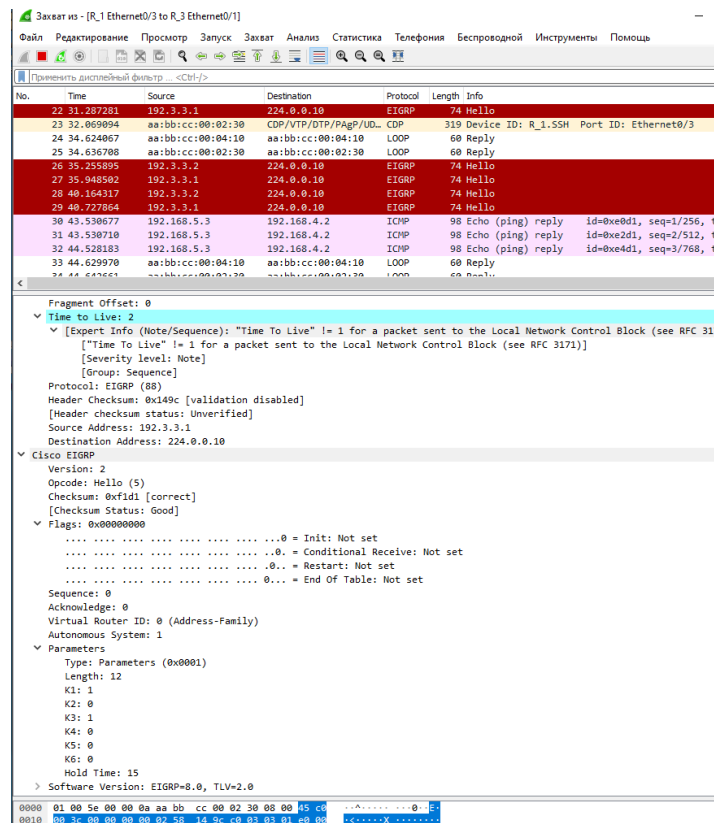


Рис. 3.30. Перевірка хешування MD5

Наступним кроком буде перевірка правильності налаштування SSH. Для цього ми спробуємо з маршрутизатора R_1 здійснити віддалене підключення до маршрутизатора R_3. (рис. 3.31-3.32).

```

R_1#SSH -l 192.3.3.2 R_3
Translating "R_3"

% Unknown command or computer name, or unable to find computer address
R_1#SSH -l R_3 192.3.3.2
=====
Device hostname -$(R_3)
Your connection is -$(lone)
Enter Admin's LOGIN adn Password
=====
Password:
R_3#

```

Рис. 3.31. Перевірка протоколу SSH

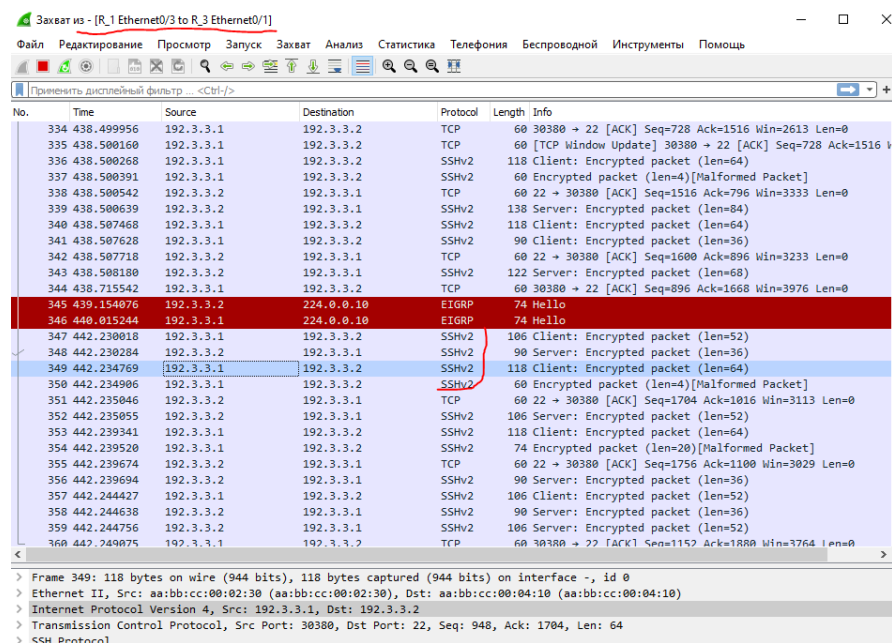


Рис. 3.32. Перевірка протоколу SSH

Тепер ми протестуємо протокол маршрутизації EIGRP, перевіривши зв'язок між віддаленими мережами. Для економії ресурсів ми запустимо лише Windows 10 Server та будемо перевіряти зв'язок з ним з робочих станцій в GNS3. Оскільки IP-адреса Windows 10 Server - 192.168.1.1, ми будемо відправляти пакети на цю адресу. (рис.3.33).

```

WM_9> ip dhcp
DORA IP 192.168.2.2/24 GW 192.168.2.1

WM_9> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=126 time=1.549 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=126 time=3.669 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=126 time=1.743 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=126 time=1.853 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=126 time=2.074 ms

WM_9>

```

Рис. 3.33. Перевірка зв'язку між LAN B та Windows 10 Server

Давайте перевіримо роботу віддалених робочих столів, підключившись з ОС Windows XP до Windows 7, а також з Ubuntu до Windows 10 Server. (рис.3.34-3.39).

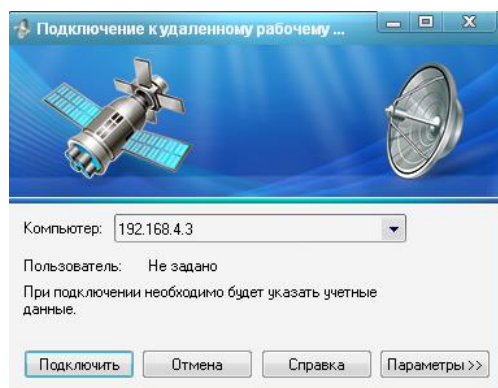


Рис. 3.34. Підключення до Windows 7 з робочої станції Windows XP

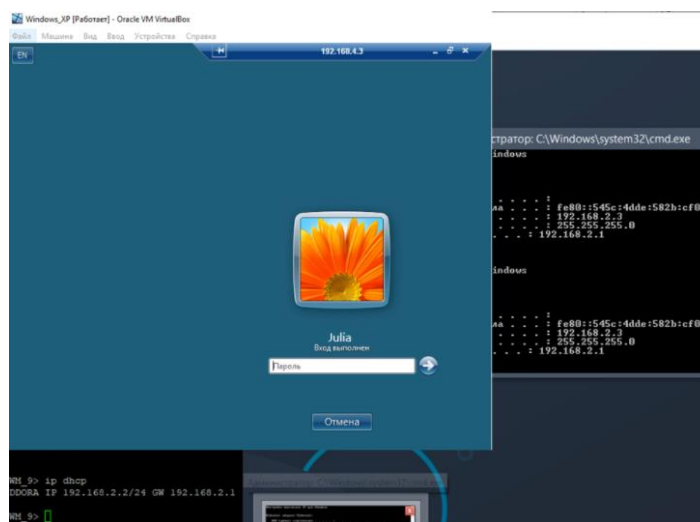


Рис. 3.35. Підключення до Windows 7 з робочої станції Windows XP

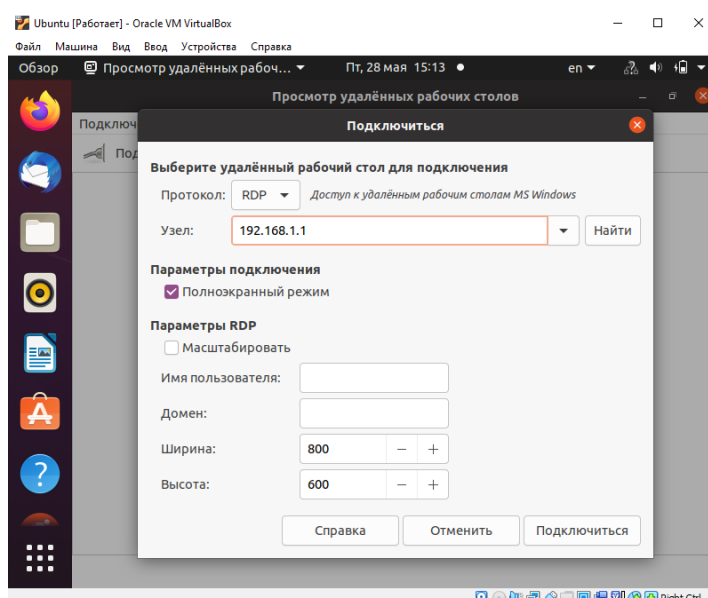


Рис. 3.36. Підключення до Windows 10 Server з робочої станції Ubuntu

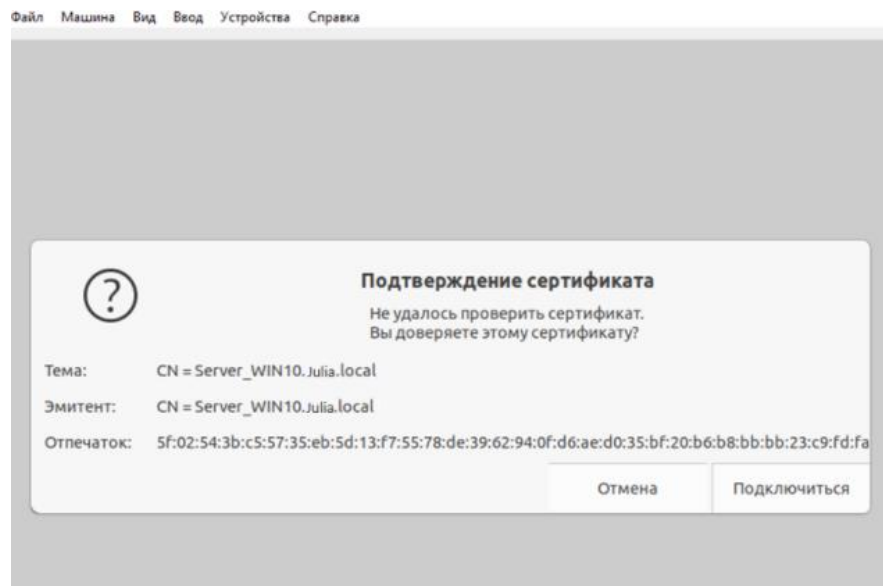


Рис. 3.37. Підключення до Windows 10 Server з робочої станції Ubuntu

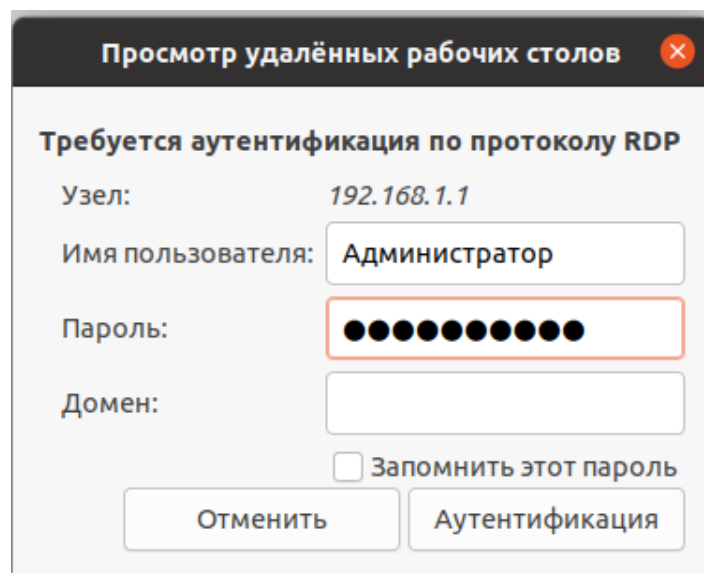


Рис. 3.38. Підключення до Windows 10 Server з робочої станції Ubuntu

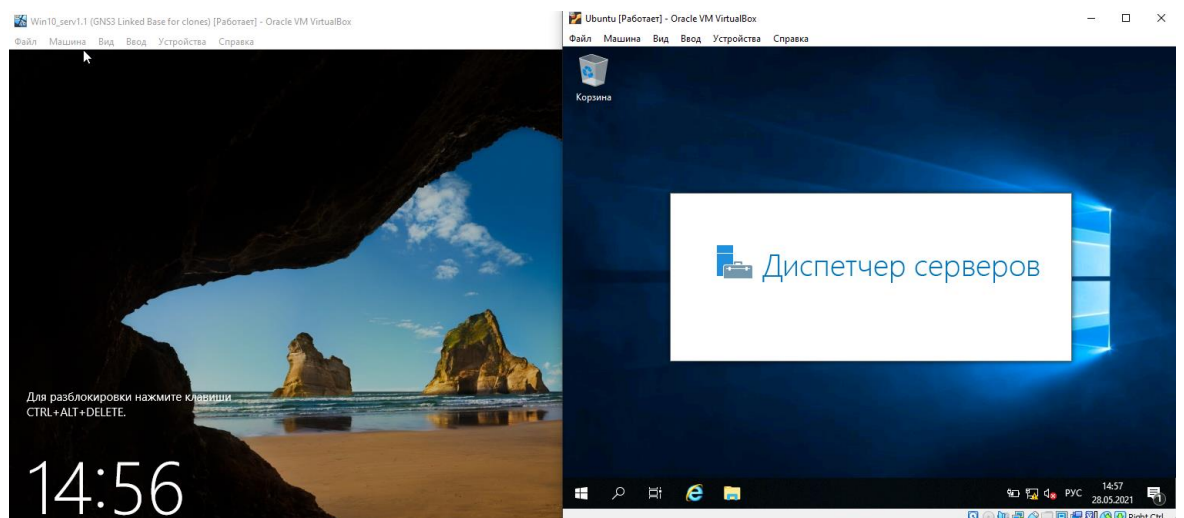


Рис. 3.39. Підключення до Windows 10 Server з робочої станції Ubuntu

Після всіх налаштувань захисту гетерогенної мережі ми повинні перевірити їх правильність. Оскільки раніше ми вже перевіряли налаштування щодо користувачів, тепер потрібно провести тестування налаштувань довіреного порту та хешування MD5.

Для перевірки налаштувань хешування MD5 використаємо аналізатор трафіку WireShark(рис.3.40-3.41).

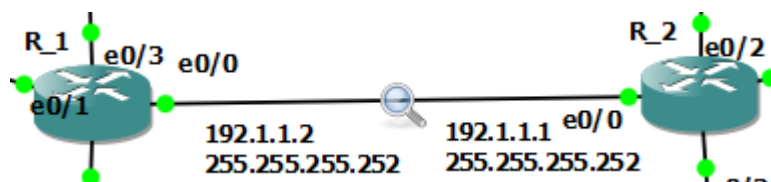


Рис. 3.40. Перевірка налаштувань MD5

69	85.420908	192.1.1.1	224.0.0.10	EIGRP	74
70	87.823732	192.1.1.2	224.0.0.10	EIGRP	74
71	89.734264	192.1.1.1	224.0.0.10	EIGRP	74
72	90.321165	aa:bb:cc:00:01:00	aa:bb:cc:00:01:00	LOOP	60
73	92.067398	aa:bb:cc:00:02:00	aa:bb:cc:00:02:00	LOOP	60
74	92.231957	192.1.1.2	224.0.0.10	EIGRP	74
75	94.277119	192.1.1.1	224.0.0.10	EIGRP	74
76	96.662682	192.1.1.2	224.0.0.10	EIGRP	74
77	98.702154	192.1.1.1	224.0.0.10	EIGRP	74
78	99.390143	aa:bb:cc:00:01:00	CDP/VTP/DTP/PAGP/UD...	CDP	319
79	100.328183	aa:bb:cc:00:01:00	aa:bb:cc:00:01:00	LOOP	60
80	101.011791	192.1.1.2	224.0.0.10	EIGRP	74
81	102.074588	aa:bb:cc:00:02:00	aa:bb:cc:00:02:00	LOOP	60
82	103.446325	192.1.1.1	224.0.0.10	EIGRP	74
83	105.842410	192.1.1.2	224.0.0.10	EIGRP	74
84	107.762555	192.1.1.1	224.0.0.10	EIGRP	74
85	109.329064	aa:bb:cc:00:02:00	CDP/VTP/DTP/PAGP/UD...	CDP	319
86	110.199419	192.1.1.2	224.0.0.10	EIGRP	74
87	110.332589	aa:bb:cc:00:01:00	aa:bb:cc:00:01:00	LOOP	60
88	112.079534	aa:bb:cc:00:02:00	aa:bb:cc:00:02:00	LOOP	60
89	112.277703	192.1.1.1	224.0.0.10	EIGRP	74

Opcode: Hello (5)	
Checksum: 0xf1d1 [correct]	
[Checksum Status: Good]	
> Flags: 0x00000000	
Sequence: 0	
Acknowledge: 0	
Virtual Router ID: 0 (Address-Family)	
Autonomous System: 1	
Parameters	
Type: Parameters (0x0001)	
Length: 12	
K1: 1	
K2: 0	
K3: 1	
K4: 0	
K5: 0	
K6: 0	
Hold Time: 15	

0000	01 00 5e 00 00 0a aa bb cc 00 02 00 08 00 45 c0	E
0010	00 3c 00 00 00 00 02 58 16 9d c0 01 01 02 e0 00	<.....X

Рис. 3.41. Перевірка налаштувань MD5

Тепер ми перевіримо налаштування довіреного порту. Оскільки ми маємо довірений інтерфейс саме на e0/0, то лише при підключенні до нього буде активний DHCP-сервер. Для цього створимо додатковий маршрутизатор і налаштуємо його як DHCP-сервер. (рис.3.42).

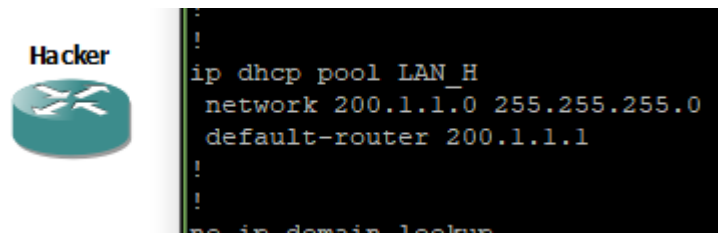


Рис. 3.42.Налаштування додаткового DHCP-серверу

Підключимо його до довіреного порту e0/0 і спробуємо отримати IP-адресу від нього (рис 3.43).

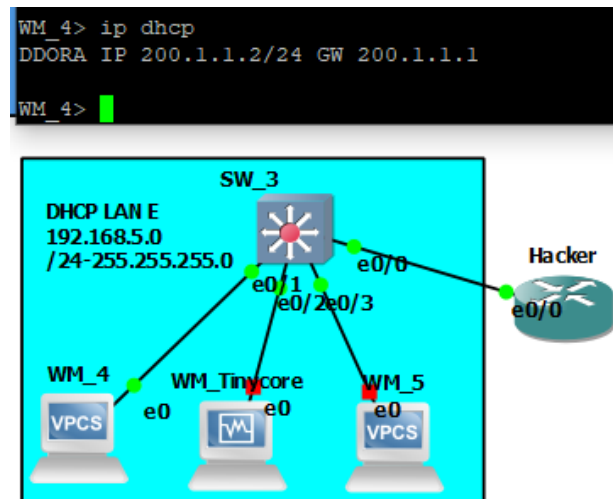


Рис. 3.43.Отримання IP-адреси від сервера-зловмисника

Як бачимо, саме через порт e0/0 ми отримаємо IP-адресу. Підключимо його тепер до будь-якого іншого порту (рис.3.44).

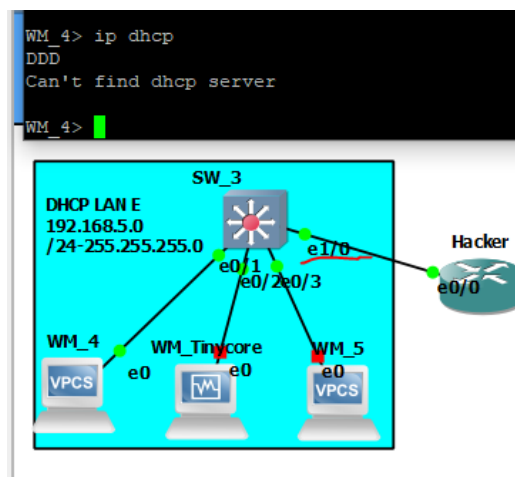


Рис. 3.44. Підключення сервера-зловмисника до недовіреного порту комутатору.

Як можна побачити, при підключенні до порту e1/0, який не є довіреним, комутатор не буде пропускати IP-адреси від серверу-зловмисника.

3.3 Аналіз результатів тестування

Всі раніше встановлені вимоги були успішно виконані, як і планувалося. У майбутньому ця мережа може бути розширена та вдосконалена для виконання нових завдань. Для цього є всі можливості. DHCP допоможе при додаванні нових робочих станцій та пристроїв, сервер буде використовуватися для налаштування нових пристроїв та їх моніторингу, а рівень ядра, з урахуванням використання маршрутизаторів від фірми Cisco, забезпечує гнучкість для майбутніх налаштувань.

Якщо в мережі будуть додаватися додаткові робочі станції з іншими операційними системами, які підтримують віддалені робочі столи, то комп'ютери зможуть взаємодіяти з ними. Це також стосується нових маршрутизаторів, якщо їх налаштовано з використанням протоколу SSH.

Щодо захисту, оскільки наша мережа використовує багато DHCP-серверів, захист портів буде важливим, оскільки зломиснику може вдалося підключитися до комутатора та надати свої IP-адреси, що може призвести до пошкодження мережі та втрати даних з робочих станцій та мережі загалом. Також захист на маршрутизаторах буде доцільним, якщо зломиснику вдасться прямо підключитися до маршрутизатора. Це може призвести до втрати даних, знищення пристроїв, підміни даних та інших негативних наслідків.

З логічної точки зору, найбільш оптимальним для підключення нових пристроїв буде LAN A, оскільки саме в цій мережі був встановлений та налаштований сервер, який працює під управлінням операційної системи Windows 10 Server. Це дає можливість використовувати автоматичну IP-адресацію та змінювати налаштування для всіх пристроїв, включаючи як нові, так і вже налаштовані, за допомогою зміни групових політик.

Ще однією перевагою цієї мережі є те, що на рівні ядра ми маємо 4 маршрутизатори, які взаємодіють між собою. У випадку виходу з ладу одного з них за допомогою протоколу EIGRP досить швидко встановлюється новий маршрут до потрібної мережі.

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						54
Змн.	Арк.	№ докум.	Підпис	Дата		

Одним з недоліків даної мережі є те, що чим більш професійне та якісне обладнання, тим воно дорожче. Наприклад, комутатори та маршрутизатори від компанії Cisco відомі своєю високою ціною через надійність, якість та гарантію на заміну пристрою або його компонентів у випадку неполадок в короткі терміни. Це може бути вигідно для великих компаній, де кожна хвилина коштує грошей.

Крім того, для налаштування та моніторингу стану пристроїв буде потрібно мати спеціаліста з глибокими знаннями цих пристроїв. Чим складніше та дорожче обладнання, тим вища буде заробітна плата такого працівника. Тому для невеликих компаній чи організацій мережа з використанням комутаторів та маршрутизаторів Cisco може бути не дуже вигідною.

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						55
Змн.	Арк.	№ докум.	Підпис	Дата		

Висновки до розділу 3

У цьому розділі було розглянуто основні налаштування всіх пристроїв даної мережі. Були налаштовані як статична, так і динамічна (DHCP) маршрутизація. Для полегшення використання та налаштування кожному пристрою було присвоєно особисту назву.

На маршрутизаторах було налаштовано протокол SSH для віддаленого доступу до них. На робочій станції, що працює під управлінням операційної системи Ubuntu, було встановлено програму для віддаленого керування робочими столами, які працюють під управлінням інших операційних систем.

Для забезпечення зв'язку між усіма підмережами схеми мережі було використано протокол маршрутизації EIGRP. Для забезпечення безпеки було налаштовано хешування MD5, довірені порти та створено користувачів з різними привілеями.

Також було проведено аналіз тестування та описано можливості масштабування та покращення мережі.

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						56
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У дипломному проекті була розроблена ієрархічна модель комп'ютерної гетерогенної мережі, яка базується на протоколі маршрутизації EIGRP. Для створення цієї мережі були використані технології від компанії Cisco. У процесі розробки були враховані всі вимоги до проекту, і була створена гетерогенна мережа, яка працює на основі протоколу EIGRP.

Початково був проведений аналіз та вибір наявних технологій для побудови сучасних гетерогенних мереж. Серед обраних технологій був графічний симулятор GNS3, операційні системи Windows, Linux, Tinycore, Ubuntu, служба Active Directory, протокол маршрутизації EIGRP, а також технології прикладного рівня, такі як SSH та DHCP.

Під час розробки мережі було встановлено, що в ній буде значна кількість робочих станцій, тому була створена топологія мережі. Для забезпечення масштабованості в майбутньому та зручності налаштування нових підключень робочих станцій та пристроїв було використано автоматичну видачу IP-адрес за допомогою протоколу DHCP. Для можливості віддаленого доступу як між робочими станціями, так і до пристроїв, був використаний захищений протокол SSH.

Далі була спроектована логічна ієрархічна модель комп'ютерної мережі з трьома рівнями: рівнем ядра, розподілу і доступу.

Це забезпечує можливість змін у мережі в майбутньому, зокрема масштабованість та надійність роботи. Комп'ютерна мережа складається з сімнадцяти робочих станцій, серед яких:

- один сервер, який працює під управлінням операційної системи Windows 10 Server;
- три робочі станції з операційними системами Windows XP, Windows 7, та Windows 8;
- дві робочі станції, на яких встановлені операційні системи TinyCore та Ubuntu;

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						57
Змн.	Арк.	№ докум.	Підпис	Дата		

- одинадцять робочих станцій, що використовують образи робочих станцій VPCS, створені в програмі GNS3.

Для масштабованості мережі в майбутньому використовувалися образи комутатора другого рівня з шістнадцятьма портами (образ i86bi-linux-l2-adventerprise-15.1b.bin), оскільки звичайний комутатор, який знаходиться в GNS3, неможливо налаштувати необхідним нам чином. Для ядра мережі використовувалися образи досить потужних та гнучких в налаштуванні маршрутизаторів третього рівня фірми CISCO (образ i86bi-linux-l3-adventerprisek9-15.2.2.03T.bin). Для сервера був обраний образ Windows 10 Server, на якому було повністю налаштовано функціонал Active Directory, DHCP, DNS та інші компоненти. Цей сервер також надає можливість встановлення орендованих адрес та назв комп'ютерів і пристроїв, що їх використовують. Більше того, користувач може переглянути заборонені IP-адреси. Завдяки редактору групових політик, можливо змінювати налаштування мережі, до якої підключений сервер, і всі ці зміни автоматично відображатимуться у налаштуваннях мережі сервера, що спрощує процес налаштування в даній мережі.

У третьому розділі було прийняте рішення щодо обладнання та програмного забезпечення. Обрані образи маршрутизаторів та комутаторів від компанії CISCO через їхню відому надійність та гнучкість у налаштуваннях. Також це обумовлено тим, що протокол EIGRP підтримується та використовується виключно фірмою CISCO, що ще раз підтверджує надійність системи. Програма для виконання дипломного проекту (GNS3) була обрана через те, що вона дозволяє створювати гетерогенні мережі за допомогою VirtualBox, яка, у свою чергу, дозволяє використовувати різні операційні системи, включаючи Windows, Linux, Ubuntu та Tinycore.

Було проведено налаштування пристроїв та аналізовано отримані результати, щоб сформулювати висновки щодо модернізації та покращення роботи. Розроблена мережа стала прототипом для реальної реалізації

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						58
Змн.	Арк.	№ докум.	Підпис	Дата		

проекту, а отримані конфігурації можуть бути використані для реального обладнання.

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						59
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гетерогенна комп'ютерна мережа [Електронний ресурс] – Режим доступу до ресурсу: [Гетерогенні комп'ютерні мережі — Вікіпедія \(wikipedia.org\)](#)
2. Active directory [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Active_Directory#:~:text=Active%20Directory%20%E2%80%94LDA P%2D%D1%81%D1%83%D0%BC%D1%96%D1%81%D0%BD%D0%B0%20%D1%80%D0%B5%D0%B0%D0%BB%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F,%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D1%85%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%20%D1%80%D0%BE%D0%B4%D0%B8%D0%BD%D0%B8%20Windows%20NT.
3. Протокол EIGRP [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/ru_ru/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html
4. Налаштування CISCO DHCP [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/hdhdcpv.html
5. DNS Server [Електронний ресурс] - Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/DNS-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80>
6. Windows 10 Server [Електронний ресурс] - Режим доступу до ресурсу: <https://www.microsoft.com/ru-ru/windows-server>
7. Ієрархічна модель мережі від Cisco [Електронний ресурс] - Режим доступу до ресурсу: <http://www.telesphera.net/blog/model-mereghi-vid-cisco.html>
8. Протокол SSH [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/SSH>
9. Windows XP [Електронний ресурс] - Режим доступу до ресурсу: 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. Windows 7 [Електронний ресурс] - Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Windows_7

11. Windows 8.1 [Електронний ресурс] - Режим доступу до ресурсу:
https://ru.wikipedia.org/wiki/Windows_8.1
12. Ubuntu [Електронний ресурс] - Режим доступу до ресурсу:
<https://en.wikipedia.org/wiki/Ubuntu>
13. Хешування MD5 [Електронний ресурс] – Режим доступу до ресурсу:
<https://uk.wikipedia.org/wiki/MD5>
14. 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
15. Cisco IOS - Privilege Levels [Електронний ресурс] - Режим доступу до ресурсу:
<https://learningnetwork.cisco.com/s/blogs/a0D3i000002eeWTEAY/cisco-ios-privilege-levels>
16. 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
17. Cisco Catalyst 2960-X - возможности и преимущества [Електронний ресурс] – Режим доступу до ресурсу:
http://stornet.ru/articles/cisco_catalyst_2960x_vozmojnosti_i_preimushhestva/
18. Cisco Catalyst 2960-X and 2960-XR Series Switches Data Sheet [Електронний ресурс] – Режим доступу до ресурсу:
https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/datasheet_c78-728232.html
19. GNS3 [Електронний ресурс] - Режим доступу до ресурсу:
<https://habr.com/ru/post/266503/>
20. VirtualBox [Електронний ресурс] - Режим доступу до ресурсу:
<https://www.virtualbox.org/>
21. Wireshark User Guide [Електронний ресурс] - Режим доступу до ресурсу:
https://www.wireshark.org/docs/wsug_html/

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						61
Змн.	Арк.	№ докум.	Підпис	Дата		

22. Wireshark [Електронний ресурс] - Режим доступу до ресурсу:
https://www.wireshark.org/docs/wsug_html_chunked/ChAdvExpert.html

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						62
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						63
Змн.	Арк.	№ докум.	Підпис	Дата		

Маршрутизатор R_1: базове
налаштування протоколу EIGRP та
DHCP

```
#show running-config

Building configuration...

Current configuration : 3111 bytes
!
version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!
hostname R_1

!
boot-start-marker

boot-end-marker

!

no aaa new-model

!
mmi polling-interval 60

no mmi auto-configure

no mmi pvc

mmi snmp-timeout 180

no ip icmp rate-limit unreachable

ip auth-proxy max-login-attempts 5

ip admission max-login-attempts 5

!

ip dhcp pool LAN_E

network 192.168.5.0 255.255.255.0
```

```
default-router 192.168.5.1

!

no ip domain lookup

ip domain name SSH

ip cef

no ipv6 cef

!

multilink bundle-name authenticated

!

key chain authEIGRP

key 1

key-string cisco12345

!

!

crypto pki token default removal timeout 0

!

!

username admin privilege 15 secret 5
$1$YMns$.9ehDuaRrigeN5SRVOolg0

username Julia privilege 10 secret 5
$1$Sw5n$VoU5TqAMhKHCSjyZRdAKy.

username USER secret 5
$1$4rAE$pAhEtbTOPnABs4ZNEsQuA.

username R_1 privilege 15 password 0 ssh

!

redundancy

!

!

ip tcp synwait-time 5

ip ssh version 2

!
```

interface Ethernet0/0	no ip address
ip address 192.1.1.2 255.255.255.252	shutdown
ip authentication mode eigrp 100 md5	serial restart-delay 0
ip authentication key-chain eigrp 100 authEIGRP	!
!	interface Serial2/1
interface Ethernet0/1	no ip address
ip address dhcp	shutdown
!	serial restart-delay 0
interface Ethernet0/2	!
ip address 192.168.5.1 255.255.255.0	interface Serial2/2
!	no ip address
interface Ethernet0/3	shutdown
ip address 192.3.3.1 255.255.255.252	serial restart-delay 0
!	!
interface Ethernet1/0	interface Serial2/3
no ip address	no ip address
shutdown	shutdown
!	serial restart-delay 0
interface Ethernet1/1	!
no ip address	interface Serial3/0
shutdown	no ip address
!	shutdown
interface Ethernet1/2	serial restart-delay 0
no ip address	!
shutdown	interface Serial3/1
!	no ip address
interface Ethernet1/3	shutdown
no ip address	serial restart-delay 0
shutdown	!
!	interface Serial3/2
interface Serial2/0	no ip address

```

shutdown
serial restart-delay 0
!
interface Serial3/3
no ip address
shutdown
serial restart-delay 0
!
!
router eigrp 1
network 192.1.1.0
network 192.3.3.0
network 192.168.5.0
network 192.168.6.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
privilege interface level 3 shutdown
privilege interface level 3 description
privilege configure level 3 interface
privilege exec level 3 write memory
privilege exec level 3 write
privilege exec level 3 configure terminal
privilege exec level 3 configure
privilege exec level 1 show ip route
privilege exec level 1 show ip interface
privilege exec level 1 show ip
privilege exec level 1 show running-config
privilege exec level 1 show interfaces
privilege exec level 1 show
banner
login
^C=====
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

```

Комутатор SW_1:
послідовність команд для
налаштування базової конфігурації

```
SW_1#show running-config

Building configuration...

Current configuration : 2177 bytes

!
version 15.1

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

service compress-config

!

hostname SW_1

!

boot-start-marker

boot-end-marker

!

logging discriminator EXCESS severity drops 6
msg-body drops EXCESSCOLL

logging buffered 50000

logging console discriminator EXCESS

!

no aaa new-model

no ip icmp rate-limit unreachable

!

ip cef

!

ip dhcp snooping vLAN 1

no ip dhcp snooping information option
```

```
no ip domain-lookup

no ipv6 cef

ipv6 multicast rpf use-bgp

spanning-tree mode pvst

spanning-tree extend system-id

!

vLAN internal allocation policy ascending

!

ip tcp synwait-time 5

!

interface Ethernet0/0

switchport mode access

switchport port-security maximum 100

switchport port-security

switchport port-security MAC-address sticky

switchport port-security MAC-address sticky
aabb.cc00.0130

duplex auto

ip dhcp snooping limit rate 50

ip dhcp snooping trust

!

interface Ethernet0/1

switchport mode access

switchport port-security maximum 100

switchport port-security

switchport port-security MAC-address sticky

duplex auto
```

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						67
Змн.	Арк.	№ докум.	Підпис	Дата		

!	duplex auto
interface Ethernet0/2	!
switchport mode access	interface Ethernet2/2
switchport port-security maximum 100	duplex auto
switchport port-security	!
switchport port-security MAC-address sticky	interface Ethernet2/3
duplex auto	duplex auto
!	!
interface Ethernet0/3	interface Ethernet3/0
switchport mode access	duplex auto
switchport port-security maximum 100	!
switchport port-security	interface Ethernet3/1
switchport port-security MAC-address sticky	duplex auto
duplex auto	!
!	interface Ethernet3/2
interface Ethernet1/0	duplex auto
duplex auto	!
!	interface Ethernet3/3
interface Ethernet1/1	duplex auto
duplex auto	!
!	interface VLAN1
interface Ethernet1/2	ip address 192.168.3.210 255.255.255.0
duplex auto	!
!	no ip http server
interface Ethernet1/3	!
duplex auto	control-pLANe
!	!
interface Ethernet2/0	line con 0
duplex auto	exec-timeout 0 0
!	privilege level 15
interface Ethernet2/1	logging synchronous

line aux 0

exec-timeout 0 0

privilege level 1

					КН.КР.Б – 122 – 24 – ПЗ	Арк.
						69
Змн.	Арк.	№ докум.	Підпис	Дата		

