

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

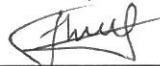
до випускної кваліфікаційної роботи бакалавра
на тему:

«Проект підсистеми захисту гетерогенної мережі організації з
можливістю віддалених підключень»

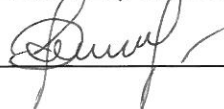
Виконав студент 4-го курсу, групи КБ-1
спеціальності 125 «Кібербезпека»

 Уваров М.С.

Керівник, ст. викладач кафедри КІ та КБ

 Покотило О.А.

Рецензент, ст. викладач кафедри КІ та КБ

 Байлюк Є.М.

Житомир 2021

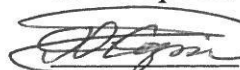
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри

комп'ютерної інженерії

та кібербезпеки

 Ефіменко А. А.

«12» квітня 2021 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента **Уварова Микити Сергійовича**

Тема роботи: **Проект підсистеми захисту гетерогенної мережі організації з
можливістю віддалених підключень**

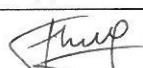
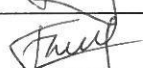
затверджена Наказом по університету від «12» Квітня 2021 р. № 134/С

Термін здачі студентом закінченої роботи – «15» Червня 2021р.

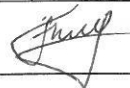
Вихідні дані для роботи:

1. Фізична топологія мережі
2. Логічна топологія мережі
3. Маршрутизатори Cisco
4. Комутатори Cisco
5. Операційні системи Cisco IOS, Windows XP, Windows 7, Ubuntu, Windows 8
Lite, Windows 10 Server
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	Покотило О.А.	 06.04.21	 06.04.21
2	Покотило О.А.	 06.04.21	 06.04.21
3	Покотило О.А.	 06.04.21	 06.04.21

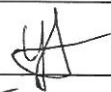
Керівник _____

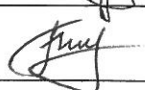


Покотило О.А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 квітня 2021 – 7 квітня 2021	Виконано
2	Пошук, огляд та аналіз літературних джерел щодо організації гетерогенної мережі	8 квітня 2021 – 11 квітня 2021	Виконано
3	Аналіз технологій захисту мережі за допомогою налаштувань на маршрутизаторах CISCO	12 квітня 2021 – 16 квітня 2021	Виконано
4	Аналіз можливостей мережного обладнання Cisco для гетерогенності мережі	17 квітня 2021 – 19 квітня 2021	Виконано
5	Розробка загального проекту мережі організації	20 квітня 2021 – 24 квітня 2021	Виконано
6	Проектування мережі та вибір обладнання для її реалізації	25 квітня 2021 – 30 квітня 2021	Виконано
7	Проектування таблиці маршрутизації	1 травня 2021 – 4 травня 2021	Виконано
8	Проектування сценарію тестування мережі	5 травня 2021 – 9 травня 2021	Виконано
9	Базове налагодження пристроїв мережі	10 травня 2021 – 13 травня 2021	Виконано
10	Налагодження гетерогенної мережі	14 травня 2021 – 18 травня 2021	Виконано
11	Тестування роботи гетерогенної мережі	19 травня 2021 – 22 травня 2021	Виконано
12	Аналіз результатів тестування	23 травня 2021 – 24 травня 2021	Виконано
13	Написання пояснювальної записки	25 травня 2021 – 29 травня 2021	Виконано
14	Підготовка презентації та виступу	30 травня 2021 – 31 травня 2021	Виконано
15	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	4 червня 2021 – 8 червня 2021	Виконано
16	Захист	18 червня 2021	Виконано

Студент  Уваров М.С.

Керівник  Покотило О.А.

РЕФЕРАТ

Кваліфікаційна робота складається з проекту гетерогенної мережі з можливістю віддалених робочих столів та пояснювальної записки до нього. Пояснювальна записка містить 63 сторінки, 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.

					КБ.КВ.Б – 125 -21 -ПЗ				
Зм.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту гетерогенної мережі організації з можливістю віддалених підключень	Літ.	Арк.	Аркушів	
Розроб.		Уваров М.С.		16.06.21				4	61
Керівник		Покотило О.А.		16.06.21					
Рецензент.		Байлюк Є.М.		16.06.21		Державний університет «Житомирська політехніка», група КБ-1			
Зав. каф.		Ефіменко А. А.		16.06.21					

ABSTRACT

The thesis consists of a heterogeneous network project with the possibility of remote desktops and an explanatory note to it. The explanatory note contains 63 pages, 52 illustrations and 9 tables. The thesis is devoted to the development of the heterogeneous network with the possibility of remote desktops based on the EIGRP protocol. The purpose of the project will be the reliability, efficiency and security of the computer network. (Our) network has to provide continuous data exchange and constant connection with remote desktops.

The thesis 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 setup scenario and project testing. The configuration of the routers and network switches will be indicated in the appendices.

KEY WORDS: SECURITY, COMPUTER NETWORK, HETEROGENEOUS NETWORKS, REMOTE DESKTOPS, CISCO.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

РЕФЕРАТ	Ошибка! Закладка не определена.
ABSTRACT	4
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	21
2.1 Принципи роботи мережі	21
2.2 Розробка логічної структури мережі.....	24
2.3 Проект підсистеми, вибір обладнання та програмного забезпечення...	29
РОЗДІЛ 3 ПРОЕКТ ПІДСИСТЕМИ ЗАХИСТУ ГЕТЕРОГЕННОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ З МОЖЛИВІСТЮ ВІДДАЛЕНИХ ПІДКЛЮЧЕНЬ.....	34
3.1 Налаштування мережі.....	34
3.2 Тестування підсистеми захисту гетерогенної мережі організації з можливістю віддалених підключень на базі протоколу маршрутизації EIGRP	44
3.3 Аналіз результатів тестування.....	52
ВИСНОВКИ.....	54
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	56
ДОДАТКИ.....	58

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

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. В сучасному світі без комп'ютерних мереж ні одна організація не зможе повноцінно та швидко функціонувати. Ефективність управління мережею комп'ютерів багато в чому залежить від правильності та грамотності її налаштування та складання коректної схеми маршрутизації. Також для різних завдань не завжди буде підходити одна операційна система. Іноді виникає необхідність використання інших систем у зв'язку з вимогами різних програмних забезпечень.

Створення комп'ютерної мережі для різних організацій, компаній, підприємств є досить трудомістким процесом, який вимагає багато затраченого часу та сконцентрованості для правильної та злагодженої роботи всієї системи разом. Кожна компанія зазвичай має в наявності в будь-якому випадку декілька комутаторів, маршрутизаторів, робочих станцій, серверів.

Оскільки комп'ютерна мережа буде використовуватися системою робочих станцій, що призначені для людей з різним рівнем доступу, то буде доцільно використовувати можливість віддалених робочих столів. Адже робочі станції користувачів з більшим рівнем доступу до бази даних клієнтів чи іншої важливої інформації також можуть виходити з ладу і для того, щоб не витрачати час для відновлювання їх роботи чи надання доступу з інших робочих станцій, доцільніше буде використовувати віддалений доступ з будь-якого ПК в мережі. При цьому надавати дані для здійснення такого підключення тільки тим користувачам, які безпосередньо мають повноваження для роботи з важливими даними на віддаленому сервері чи робочій станції.

Також оскільки мережа буде складатися з великої кількості пристроїв, доцільним стане налаштування динамічної IP-адресації, оскільки також час від часу техніка може виходити з ладу або виникне необхідність у підключенні нових робочих станцій. Крім того, не зайвим буде використовувати різні привілеї доступу для різних рівнів працівників, оскільки не можна дозволяти будь-кому використовувати всі можливості комп'ютерної мережі. Мати

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						8
Змн.	Арк.	№ докум.	Підпис	Дата		

доступ до всіх налаштувань комутаторів, маршрутизаторів, серверів та робочих станцій буде тільки одна-дві людини, які формуватимуть звіти та відповідатимуть за стан пристроїв в цілому. Для моніторингу роботи та внесення змін в конфігураційні файли комунікаційних пристроїв мережі важливим є налаштування можливості віддаленого доступу до них за допомогою протоколу SSH чи Telnet.

Так як будь-яка система може викликати інтерес у зловмисників чи конкурентів, виникає необхідність у забезпеченні захисту даних організації. Відповідно нашу систему потрібно буде також захистити або мінімізувати збитки від зловмисного впливу за допомогою різних можливостей захисту від компанії CISCO, так як комутатори та маршрутизатори саме цієї фірми будуть використані під час налаштування схеми.

Для практичної реалізації підсистеми буде використовуватися графічний симулятор GNS3. Щоб забезпечити гетерогенність мережі використовуватимуться 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 зловмисників.

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.

					КБ.КВ.Б – 125 – 21 – 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 між собою декількох LAN на невеликій території і надає можливість працювати з віддаленими мережами за допомогою віддалених робочих столів. Метою створення гетерогенної мережі є доступ до ресурсів всіх робочих станцій як і в LAN, так і в віддаленій мережі.

До основних компонентів гетерогенної мережі будуть відноситися:

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

В гетерогенній мережі використовується два види робочих станцій:

1. Клієнтська, яка буде отримувати через мережу доступ до інших робочих станцій і через віддалений доступ до головної робочої станції.
2. Головна(сервер), яка містить всі основні ресурси мережі і доступна лише користувачам, яким надано доступ[1].

Також мережа може бути одноранговою або з виділеним сервером, в залежності від того, який тип робочих станцій вона буде містити. Розглянемо всі переваги та недоліки таких мереж.

В одноранговій комп'ютерній мережі не буде якогось основного центру зберігання даних, керування мережею та забезпечення взаємодії між робочими станціями. Мережеве завдання буде розподілене між всіма пристроями. Кожний комп'ютер може виконувати як функції серверу, так і функції клієнта. Він може приймати та обробляти дані, запити від інших робочих станцій, а також відправляти свої дані та запити до інших пристроїв.

До переваг однорангової комп'ютерної мережі належать:

- висока надійність;

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						10
Змн.	Арк.	№ докум.	Підпис	Дата		

- низька вартість.

Основними недоліками є:

- складність керування мережею - через те що в мережі немає як такого основного центру збору даних;
- складність в забезпеченні захисту інформації, оскільки налаштування будуть проводитися на всіх комутаторах, маршрутизаторах, робочих станціях окремо;
- працездатність, швидкість, ефективність роботи мережі напряму залежатимуть від кількості пристроїв і робочих станцій в мережі.

В комп'ютерній мережі з виділеним сервером вже буде робоча станція (сервер), яка виконуватиме функції збереження, керування, обробки і т.д.. Також вона призначена для використання всіма робочими станціями мережі.

Серед переваг можна виділити наступні:

- висока швидкість обробки інформації, оскільки все буде проходити через єдиний сервер;
- більш надійна система захисту інформації;
- відсутність обмеження по числу робочих станцій;
- простота адміністрування та керування системою.

До недоліків можна віднести:

- досить високу вартість, оскільки одна із станцій буде виділятися на сервер;
- швидкість та ефективність всієї системи буде залежати від потужності самого серверу.

1.2 Теоретичні відомості щодо Active directory

Служба Active directory – це досить надійне та просте в налаштуванні рішення від компанії Microsoft, що дозволяє з'єднати всю мережу, яка може складатися з різних пристроїв, інформацію щодо користувачів та інше в одну систему. В нашому випадку Active directory буде виступати як сервер невеликої мережі з можливістю DHCP, DNS-серверу та моніторингу цієї мережі.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						11
Змн.	Арк.	№ докум.	Підпис	Дата		

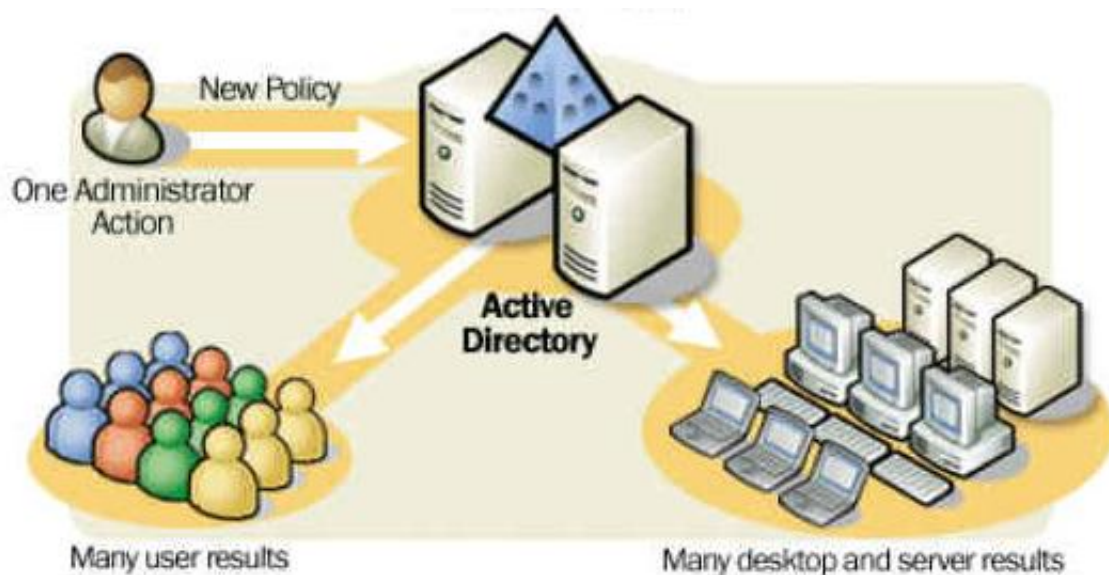


Рис.1.1. Принцип роботи Active directory в нашій системи

Ще однією перевагою Active directory є досить зручне керування політиками. За допомогою Active directory можна розділити всіх користувачів на різні групи і надавати їм особливі права на користування системою. Щодо політик в Active directory є досить прості рішення:

- змінення та налаштування вже існуючих політик. Оскільки всі політики зберігаються в одній базі, то якщо змінити налаштування однієї з них, всі зміни будуть також стосуватися та застосовуватися до всієї системи;
- при створенні нового користувача і присвоєння йому однієї з груп, всі налаштування щодо політик для даної групи будуть застосовуватися також для нового користувача.

Active directory також збільшує захист всієї мережі, оскільки всі дані зберігаються на контролерах доступу, які захищені 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 цілу систему, зокрема:

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

Особливістю AD є те, що всі дані та весь трафік будуть проходити через сервер, і якщо він вийде з ладу (наприклад, зникне світло в організації), то вся система та інші робочі станції будуть поза доступом. Тому потрібно мати можливість додати один чи декілька однакових серверів, які в випадку відключення основного автоматично почнуть працювати з такими ж налаштуваннями. Додатково, якщо з ладу вийде вся система і всі резервні сервери, потрібно забезпечити регулярне копіювання даних системи для швидкого відновлення її працездатності.

З цього всього можна зробити висновок, що служба AD досить сильно впливатиме на роботу всієї системи. І тому, якщо потрібно правильно, а головне - коректно налаштувати систему організації, важливо запрошувати 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) – це покращений внутрішній протокол маршрутизації. Він використовується в різних топологіях та мережах. Добре налаштований протокол EIGRP масштабується та забезпечує досить малий час обміну даними з мінімальним мережевим трафіком. Принцип роботи протоколу відображено на рисунку 1.2.

Основними перевагами протоколу EIGRP перед іншими є:

- невелике використання мережевих ресурсів під час нормальної роботи; тільки hello-пакети передаються в стабільній мережі;
- якщо відбувається зміна топології, розповсюджуються тільки зміни таблиці маршрутизації, а не повністю вся таблиця. Це зменшує загальне навантаження мережі;
- малий час конвергенції для змін в топології мережі.

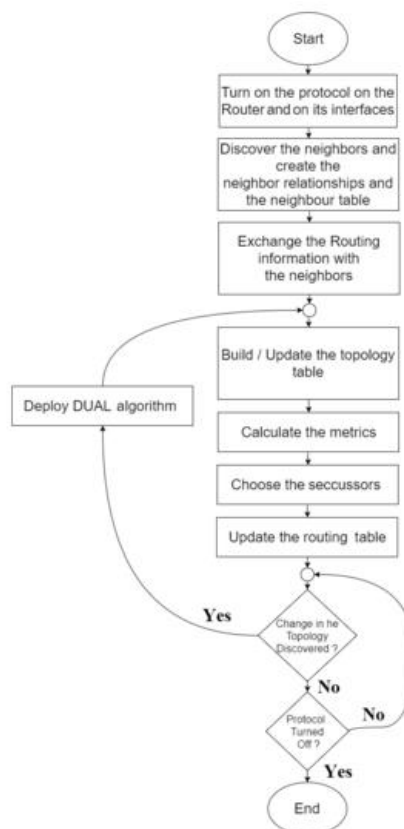


Рис. 1.2. Принцип роботи протоколу EIGRP

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

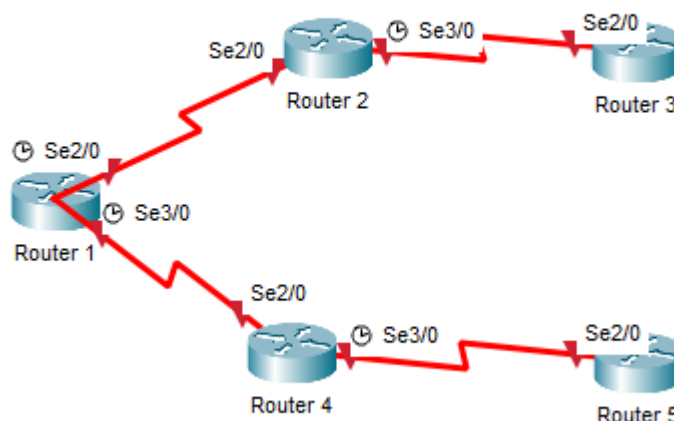


Рис. 1.3. Мережа для представлення протоколу EIGRP

Протокол EIGRP зберігає таблицю маршрутизації після кожного оновлення даних на маршрутизаторі та його сусідах. Він запитує, чи знає маршрутизатор ще якусь мережу чи додатковий маршрутизатор, шляхом

періодичного відправлення повідомлень сусіднім пристроям. В мережі, зображений на рисунку 1.2, другий маршрутизатор запам'ятовує та дає інформацію про своїх сусідів (перший та третій маршрутизатори). І якщо потрібно передати якісь дані до п'ятого маршрутизатора, то він запам'ятовує шлях через перший. Якщо ж і перший маршрутизатор виходить з ладу, то другий маршрутизатор одразу звертається до топології мережі в пошуках можливого шляху до п'ятого маршрутизатора[3].

З цих пояснень можна зрозуміти наступне:

- вся інформація стосовно оновлень отримується за допомогою даних сусідів маршрутизатора;
- якщо видаляється якийсь маршрут з таблиці топології мережі, то він видаляється також на інших маршрутизаторах;
- при втраті маршруту в таблиці маршрутизації запускається процес пошуку маршруту до втраченої адреси.

Для розповсюдження інформації щодо таблиці маршрутизації протокол EIGRP використовує неперіодичне оновлення таблиці маршрутизації, тобто пересилає оновлення тільки тоді, коли інформація стосовно маршрутів змінюється. Основним недоліком даного протоколу є те, що ми не можемо знати, коли заданий маршрут стає недоступним, і тому EIGRP кожних 5 або 60 секунд (в залежності від пропускної здатності каналу) посилає hello-пакети. Швидкість, з якою EIGRP відправляє hello-пакети, називається інтервалом привітання. Його можна налаштувати за допомогою команди `ip hello-interval eigrp`. Також є параметр час утримування, тобто час, протягом якого маршрутизатор вважатиме сусідній пристрій увімкненим, не отримуючи від нього hello-пакетів. Час утримування зазвичай дорівнює трьом інтервалам hello-пакетів (15 та 180 секунд відповідно). Для змінення даного параметру використовується команда `ip hold-time eigrp`. При введенні нового інтервалу hello-пакетів час утримання самостійно не змінюється, потрібно робити це власноруч.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						15
Змн.	Арк.	№ докум.	Підпис	Дата		

Якщо взяти два маршрутизатори, на яких налаштовано протокол маршрутизації EIGRP, і на них не будуть співпадати час hello-пакетів і час утримання, то все одно вони будуть працювати.

Кількість сусідів, яку підтримує протокол EIGRP, необмежена, але фактично залежить від наступних характеристик пристрою:

- об'єм пам'яті;
- швидкість обробки інформації ;
- кількість переданої та прийнятої інформації;
- складність топології;
- стабільність мережі.

В протоколі EIGRP замість таблиці маршрутизації, на відміну від протоколів RIP та IGRP, для зберігання всіх даних та для працездатності буде формуватися друга таблиця (таблиця топології), а вже на її основі буде встановлюватися маршрутизація всіх пристроїв.

Щоб дізнатися формат таблиці топології мережі, ми можемо виконати команду `show ip eigrp topology`. Таблиця топології буде містити відомості, потрібні для побудови набору відстаней і векторів для кожної досяжної мережі, включаючи:

- найнижчу пропускну здатність каналів;
- загальну кількість затримок;
- надійність і завантаженість шляху;
- найкоротшу, допустиму і оголошену відстань;
- джерело маршруту.

Протокол EIGRP для розрахунку показників маршрутизації використовує два параметри: мінімальну пропускну здатність та загальну затримку. Додатково можна налаштувати і інші метрики, але в такому випадку можуть з'являтися “петлі” в мережі.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						16
Змн.	Арк.	№ докум.	Підпис	Дата		

1.4. Протокол DHCP

Протокол DHCP необхідний для досить масштабних мереж для комфортної роботи з багатьма робочими станціями. Його головне завдання - проводити автоматичне налаштування параметрів мережевого адаптеру. DHCP налаштовується на базі маршрутизаторів CISCO чи на базі серверів[4].

Маршрутизатор не обов'язково має виступати як DHCP сервер. Він також може бути і DHCP клієнтом. Налаштування DHCP буде доцільним, якщо у нас вже є якийсь маршрутизатор, і до мережі потрібно додати декілька пристроїв (робочі станції, принтери, IP-телефони та інше). Тоді можна на ньому налаштувати автоматичну видачу параметрів, щоб пристрої вже самостійно, без участі системного адміністратора, могли функціонувати.

DHCP дозволяє автоматично налаштовувати такі основні параметри:

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

Розглянемо детальніше процес отримання клієнтом даних від DHCP серверу. Спочатку робоча станція створює та відправляє ширококомовний пакет, який складається з декількох фреймів. На другому рівні фрейму буде зазначено MAC-адресу відправника (нашої робочої станції) і MAC-адресу отримувача формату аaaa.аaaa.аaaa. Третій рівень фрейму міститиме IP-адресу відправника, але оскільки її ще не знаємо, ця частина буде пуста. Такий пакет називається "DHCP discover".

Перший пакет отримують всі пристрої. DHCP сервери, а їх може бути і декілька в мережі, збирають всю інформацію щодо DHCP і відправляють в зворотному напрямку необхідні дані, тобто IP-адресу, маску мережі, основний шлюз, ім'я домену, DNS сервер. При цьому на DHCP-сервері резервується

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						17
Змн.	Арк.	№ докум.	Підпис	Дата		

дана IP-адреса і виділяється на деякий час(lease time). Пакет з усіма даними відправляється вже на нову адресу (DHCP offer).

Оскільки ми розглядаємо можливість і декількох DHCP серверів, то клієнт буде обирати той, що йому швидше відповість, і вже на нього відправить із зазначенням своєї MAC-адреси та виданої йому IP-адреси підтвердження всіх параметрів, які він отримав (DHCP request).

Після цього DHCP сервер резервує за DHCP клієнтом дану IP-адресу на певний час, оскільки до цього моменту вона була вже виділена, але не зарезервована. І вже після цього зазначена адреса і всі дані остаточно закріплюються за клієнтом. Тепер, після закріплення, сервер відправляє клієнту повідомлення, що клієнт успішно доданий до його 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			

Розберемо кожний пункт в цьому пакеті:

1. OpCode - код операції. Перше поле 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 - тип адреси на каналному рівні.
3. Hardware length – довжина апаратної адреси в байтах
4. Transaction ID - ID операції. Коли клієнт починає процес отримання IP-адреси, він генерує це значення, щоб сервер не переплутав конкретний процес цього клієнта з іншим процесом.
5. Seconds elapsed (час операції) - витрачений час в секундах. Рахується з початку отримання IP-адреси.
6. Flags – спеціальні параметри для DHCP.
7. Client IP - клієнтська IP-адреса. Дане поле заповнюється тільки якщо DHCP-клієнт вже має якусь адресу. В інших випадках відправляється пустим.
8. Your IP – адреса, яку пропонує DHCP-сервер.
9. Server IP – IP-адреса серверу.
10. Gateway IP - IP-адреса за замовчуванням. Застосовується тільки коли DHCP-сервер працює в режимі DHCP Relay Agent.
11. Client Hardware address – MAC-адреса клієнту. Заповнюється тільки тоді, коли на каналному рівні використовується Ethernet.
12. Server Host Name - ім'я домену або хосту. Заповнюється тільки тоді, коли у сервера є ім'я домену або хосту.
13. Boot file - файл завантаження. Заповнюється тільки якщо DHCP-сервер роздає назву файлу для завантаження.
14. Options - додаткові налаштування. Заповнюється, якщо задаються інші додаткові опції.

Сервер назначає IP-адресу одним з трьох основних способів:

1. Статичний розподіл – схожий на введення адреси на кожному комп'ютері вручну. Відмінність в тому, що системний адміністратор задає

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						19
Змн.	Арк.	№ докум.	Підпис	Дата		

необхідні відповідності IP для MAC-адрес клієнтів на самому DHCP-сервері. IP залишиться за клієнтом навіть після виходу чи переходу до іншої мережі.

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

3. Динамічний розподіл – DHCP-сервер назначає адресу із області на визначений проміжок часу. Такий 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 відрізнятися при кожному підключенні, але зазвичай призначається попередньо виданий.

Висновки до розділу 1

В результаті аналізу особливостей гетерогенних мережі було визначено основні принципи побудови схеми та методи її захисту. Потрібно розробити підсистему гетерогенної мережі з можливістю віддалених робочих столів.

Було розглянуто можливість встановлення Active directory на Windows 10 Server. Крім того, обрано протокол маршрутизації EIGRP та протокол DHCP для автоматизації підключення нових пристроїв.

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

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						20
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЕКТУВАННЯ ГЕТЕРОГЕННОЇ МЕРЕЖІ 3 МОЖЛИВІСТЮ ВІДДАЛЕНИХ РОБОЧИХ СТОЛІВ

2.1 Принципи роботи мережі

При розробці мережі потрібно одразу логічно її структурувати. Дана підсистема буде складатися з декількох LAN та окремої підмережі з сервером на базі Windows 10 server[6].

При створенні даної мережі мають бути виконані наступні вимоги:

- створення підмережі з сервером, на якому буде налаштований Active Directory;
- використання різних операційних систем для гетерогенності мережі;
- забезпечення можливості працювати на віддалених робочих станціях;
- автоматичне отримання IP-адресації (DHCP) для кожної підмережі;
- захищеність підсистеми від дій зловмисників, конкурентів чи недбалості власних працівників.

Так як при проектуванні схеми буде використовувати досить багато різних робочих станцій з різними ОС, то при розробці мережі потрібно брати до уваги наявність великої кількості IP-адрес. Потрібно забезпечити налаштування протоколу DHCP для автоматизації процесу IP-адресації, оскільки деякі робочі станції можуть як додаватися, так і виходити з ладу. Для цього буде розроблено шість підмереж з різними DHCP-серверами та різними ОС (табл. 2.1).

Розподіл на підмережі буде здійснений за допомогою DHCP-серверів на базі маршрутизаторів. Окремі підмережі будуть налаштовані для зв'язку між маршрутизаторами рівня ядра.

Також потрібно розробити IP-топологию мережі. Оскільки в схемі буде досить багато підмереж, внутрішню адресацію забезпечуватиме протокол динамічного налаштування вузлів. Детальні параметри адресації наведено в табл. 2.2.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						21
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 2.1

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

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						23
Змн.	Арк.	№ докум.	Підпис	Дата		

2.2 Розробка логічної структури мережі

В даній схемі буде використана трирівнева ієрархічна модель мережі, оскільки вона є надійною та високопродуктивною. Дана мережа складатиметься з 3-х 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 – якщо з ладу виходить один із основних пристроїв то є запасний, який зможе виконувати його функції
4. Швидка працездатність – ієрархічна структура дає можливість високої пропускної здатності.

Розберемо кожен з рівнів окремо. Рівень ядра відповідає за швидке транспортування між пристроями рівня розподілу, тобто між комутаторами мережі. На рівні ядра найчастіше використовують досить дорогі пристрої високого класу, і, якщо є можливість - високопродуктивні комутатори.

Рівень розподілу знаходиться посередині між рівнем ядра та доступу. Завдання даного рівня - забезпечувати маршрутизацію мережі, а також зв'язувати рівень ядра та доступу. Також на цьому рівні йде фільтрація ACLs та PBR. Основним завданням також є зменшення навантаження на мережу.

Рівень доступу зазвичай складається з комутаторів і точок доступу, які в свою чергу, дають можливість підключатися до робочих станцій, принтерів, IP-телефонів, серверів тощо. Щодо вимог до комутаторів, це, найчастіше, комутатори другого рівня через їх меншу вартість.

Загальний вигляд розробленої схеми разом із зазначенням вищевказаних рівнів наведено на рисунку 2.1.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						24
Змн.	Арк.	№ докум.	Підпис	Дата		

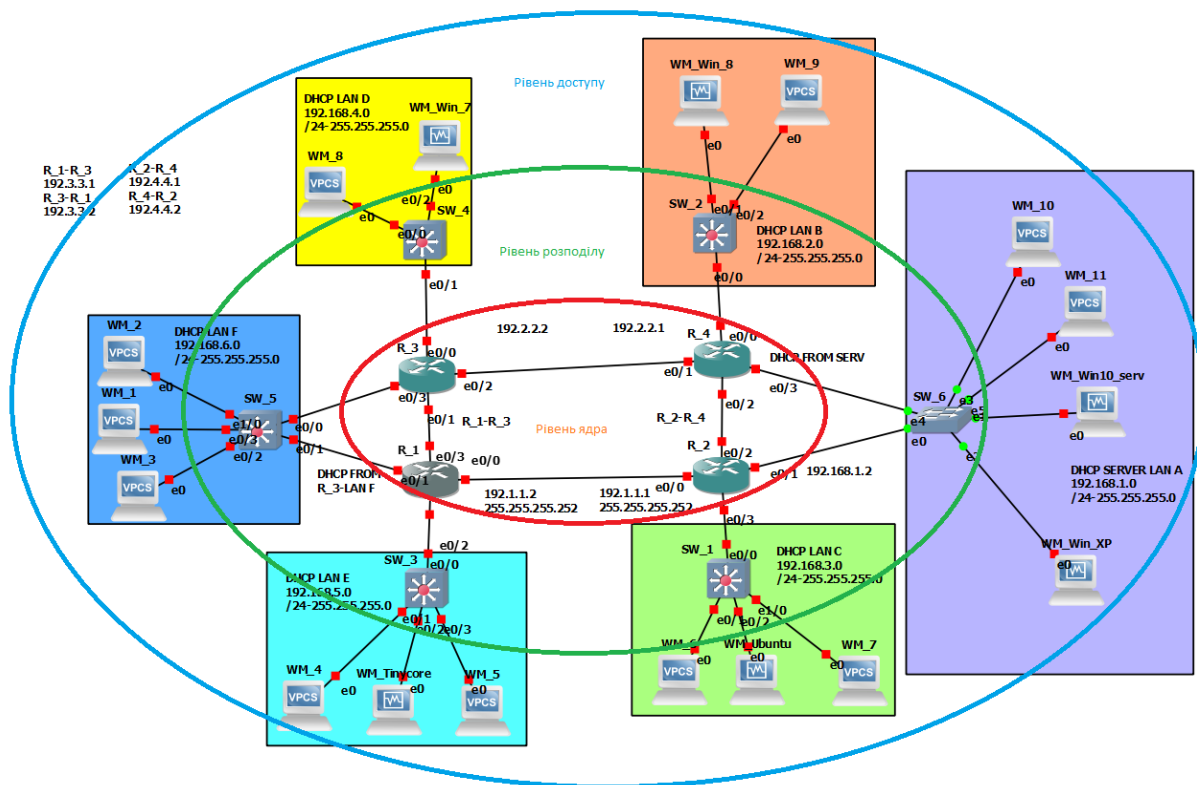


Рис.2.1. Трирівнева ієрархічна модель мережі

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.

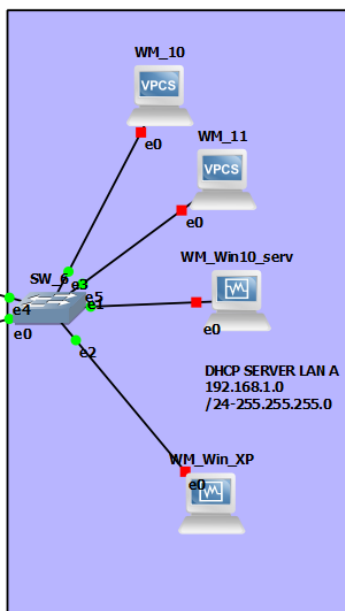


Рис.2.2. Локальна мережа LAN A

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

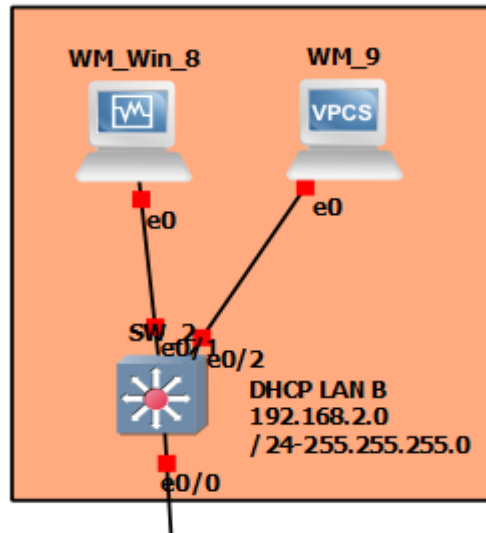


Рис.2.3. Локальна мережа LAN В

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)

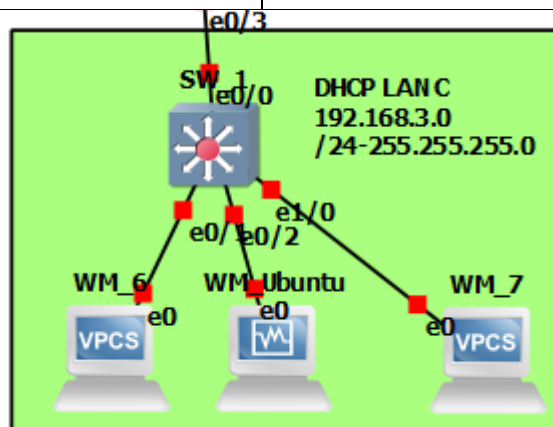


Рис.2.4. Локальна мережа LAN С

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)

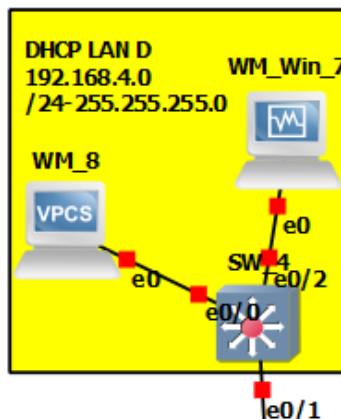


Рис.2.5. Локальна мережа LAN D

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)

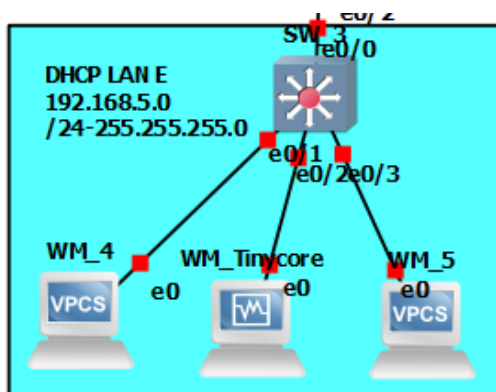


Рис.2.6. Локальна мережа LAN E

Таблиця 2.8

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)

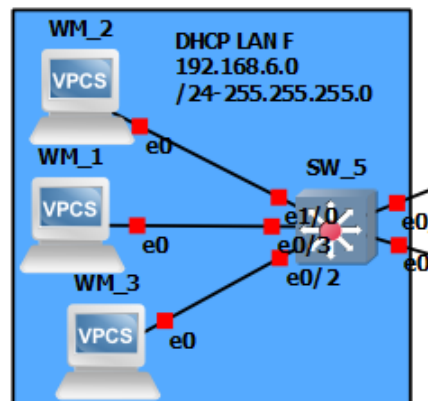


Рис.2.7. Локальна мережа LAN F

Таблиця 2.9

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.

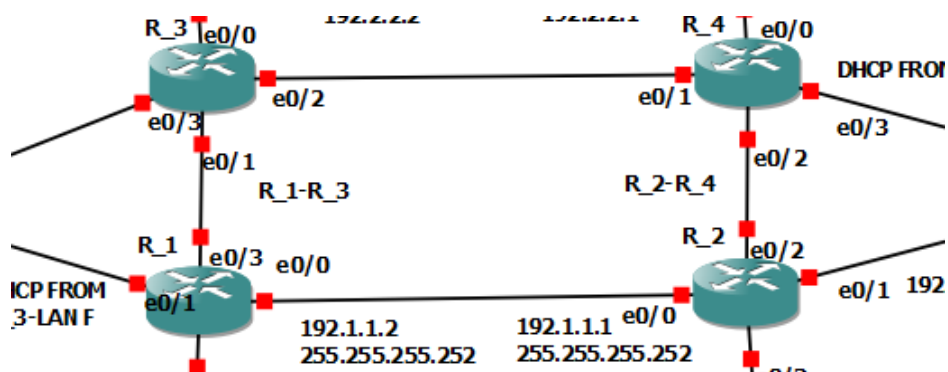


Рис.2.8. Рівень ядра

Проектована гетерогенна мережі створюється для організації чи компанії, тому потрібно забезпечити її максимальну працездатність. Для того, щоб пришвидшити процес відновлення доступу до мережі з робочих станцій при їхньому виході з ладу чи додавання нових робочих станцій, маршрутизатори будуть виступати саме як DHCP-сервера для кожної з підмереж.

Для нормалізування роботи всієї мережі буде використано протокол зв'язку EIGRP, оскільки він досить надійний, і при виникненні проблем із зв'язком досить швидко повідомляє про це 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 привілеїв, 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 роками і мільйонами трафіку інформації. Вона використовує лише якісні компоненти

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						29
Змн.	Арк.	№ докум.	Підпис	Дата		

та матеріали починаючи від корпусу приладу і закінчуючи системою охолодження.

2. CISCO пропонує досить великий вибір приладів – рішення для малих компаній, бізнесів, а також для провайдерів інтернету та великих корпорацій [15].

3. Можливість різного налаштування – навіть на базі одного приладу є можливість реалізувати різні завдання, наприклад, маршрутизацію, комутацію, налаштування сервера, голосові сервіси, захист від різних типів атак. Найчастіше вистачає буквально декілька команд для того, щоб прилад міг виконувати ще якусь додаткову роботу, і вже не буде потреби в придбанні додаткового пристрою.

4. Рівень підтримки пристроїв CISCO – якщо потрібна допомога в налаштуванні пристроїв CISCO, то вся інформація є на офіційному сайті компанії CISCO.COM. Там можна знайти все, що буде потрібно системному адміністратору для налагодження: від опису моделі та її характеристик до повної документації щодо налаштувань різних можливостей

5. Рівень гарантії пристроїв – компанія CISCO пропонує гарантії на будь-які прилади, в тому числі і старі, і майже на будь який термін. При покупці гарантії від CISCO, при несправності приладу компанія зробить повну заміну пристрою чи зламаной його частини протягом 4-8 годин. Для великих компаній, які користуються приладами CISCO, така гарантія є необхідною[16].

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 4000[17] (рис.2.9) та комутатора 9300 [18](рис.2.10).

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

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						30
Змн.	Арк.	№ докум.	Підпис	Дата		



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. Він дає можливість створювати різні мережі, проводити їх тестування, захищати і тощо прямо на комп'ютері. Головною перевагою є те, що GNS3 дозволяє розробляти саме гетерогенні мережі за рахунок додавання різного обладнання з різними образами, такими як Cisco, Juniper, Mikrotik, CheckPoint та ін. Тобто цей симулятор дає можливість запускати операційні системи різних виробників прямо в одній системі. Наприклад, при додаванні маршрутизатора Cisco в GNS3, запускається реальна операційна система Cisco IOS. Таким чином ми отримуємо повноцінний маршрутизатор Cisco. Тепер перерахуємо переваги та недоліки GNS3.

Головна перевага симулятора в тому, що він відтворює всі функції пристроїв. Тобто якщо додати маршрутизатор фірми Cisco, для нього будуть доступні всі команди, які працюватимуть і на реальному обладнанні, що дуже важливо. Якщо аналізувати Cisco Packet Tracer, то ця програма не підтримує всіх команд і не дає можливості продемонструвати гетерогенність мережі[19].

GNS3 дозволяє додавати та налаштовувати повноцінні робочі станції та сервери. Якщо розглядати Cisco Packet Tracer, то кінцевими пристроями

будуть звичайні робочі станції з невеликим пакетом можливостей і дуже обмеженим функціоналом. Така ж ситуація і з серверами. Щодо GNS3, ми можемо додавати повноцінні робочі станції під керуванням ОС Windows XP, Windows 7, Linux Ubuntu та інші. Якщо ж виникає необхідність додавання серверу, можливим є використання, наприклад, Windows 10 Server. Завдяки цьому реальним є навіть під'єднати всю мережу GNS3 то реальної мережі Інтернет. Крім того, також дуже важливим є те, що GNS3 взагалі безкоштовна.

Найбільший недолік GNS3 – це неможливість додавати повноцінні комутатори, тому потрібно користуватися саме стандартним комутатором від GNS3. Причиною є те, що в реальних комутаторах знаходяться ASIC мікросхеми, які неможливо відтворити в симуляторах на звичайних комп'ютерах. А комутатори мають таку велику передачу і обробку пакетів саме через ASIC мікросхеми.

Все ж таки симуляція реальних пристроїв та операційних систем тягне за собою ще один недолік – це великі потреби до параметрів та ресурсів комп'ютера, на якому буде працювати GNS3. Наприклад, для гетерогенної мережі потрібно декілька віртуальних машин під управлінням операційних систем Windows та Linux. Але для запуску тільки однієї машини під управлінням Windows 10 потрібно 4 Гігабайти оперативної пам'яті.

VirtualBox – це програма для віртуалізації різних операційних систем і, що дуже важливо, вона працює майже на всіх операційних системах Windows, Linux, MAC OS та ін. VirtualBox має однаковий формат образів для віртуалізації, і, якщо брати, наприклад, створення віртуальної машини під управлінням ОС Linux, вона може бути переміщена на Windows і працювати далі без помилок [20].

Перевагами VirtualBox є досить зрозумілий та дружелюбний інтерфейс. Також програма підтримує досить багато форматів образів, тобто крім операційних систем також можна встановити образ маршрутизатора (наприклад Mikrotik) і також використовувати в GNS3. VirtualBox працює на основі віртуалізації різних ОС. Після створення віртуальної мережі користувач

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						32
Змн.	Арк.	№ докум.	Підпис	Дата		

може встановити майже будь-яку ОС і працювати на ній, як на звичайному комп'ютері.

Можливості VirtualBox:

- запуск одразу декількох віртуальних машин;
- можливість налаштування параметрів та кількості ресурсів основного комп'ютера для кожної віртуальної машини;
- експорт та імпорт вже готових образів віртуальних машин;
- можливість “заморозити” стан віртуальної машини для зменшення втрати ресурсів на ту віртуальну машину, яка зараз не потрібна у використанні;
- можливість спільних папок та файлів для обміну даними як з основним комп'ютером, так і між віртуальними машинами;
- можливість робити скріншоти та захват відео з екрану віртуальних машин.

Wireshark – дуже потужна програма для аналізу та перехоплення мережевого трафіку. Дане ПЗ доступне на операційних системах Linux, Windows, NetBSD, MAC OS та ін. Ця програма потрібна для аналізу трафіку. Також, якщо щось виходить з ладу, наприклад, протокол маршрутизації, можна за допомогою Wireshark перевірити, в чому проблема і де втрачаються пакети[21].

Висновки до розділу 2

Була спроектована підсистема гетерогенної мережі, яка складається з 6 локальних підмереж та маршрутизаторів рівня ядра. Обґрунтовано необхідність використання трирівневої ієрархічної моделі. Сформовано таблицю параметрів інтерфейсів та адресації пристроїв мережі.

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 – 21 – ПЗ	Арк.
						33
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 ПРОЕКТ ПІДСИСТЕМИ ЗАХИСТУ ГЕТЕРОГЕННОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ З МОЖЛИВІСТЮ ВІДДАЛЕНИХ ПІДКЛЮЧЕНЬ.

3.1 Налаштування мережі

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

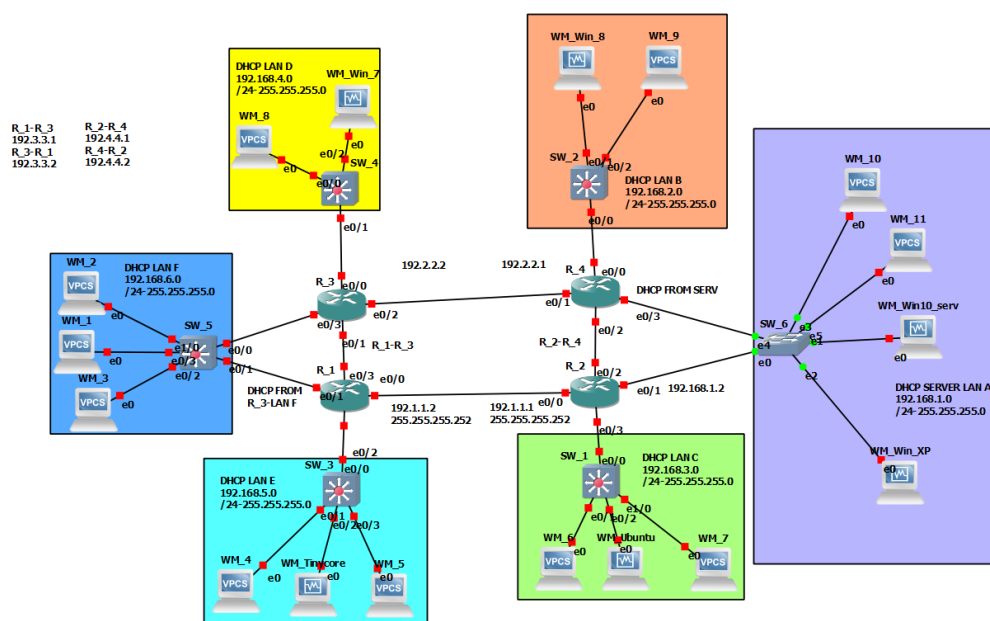


Рис. 3.1 Повна схема мережі

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

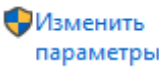
Имя компьютера:	Server_WIN10	
Полное имя:	Server_WIN10	
Описание:	Server_WIN10	
Рабочая группа:	WORKGROUP	

Рис. 3.2. Встановлення всіх служб для роботи серверу

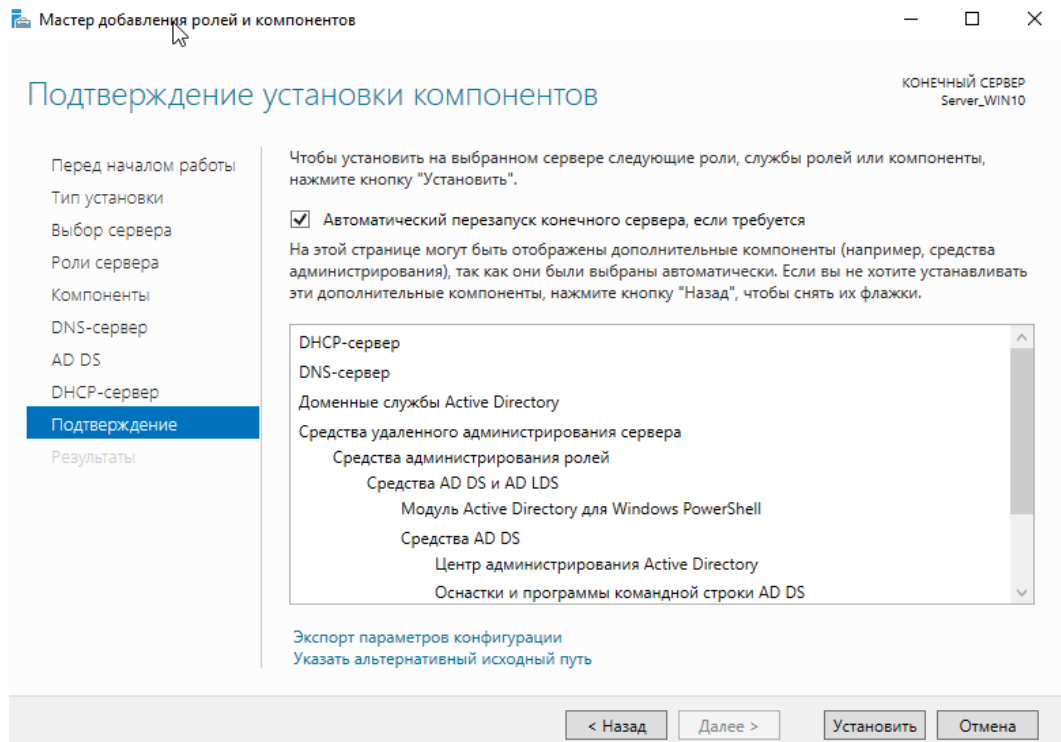


Рис. 3.3. Встановлення всіх служб для роботи серверу

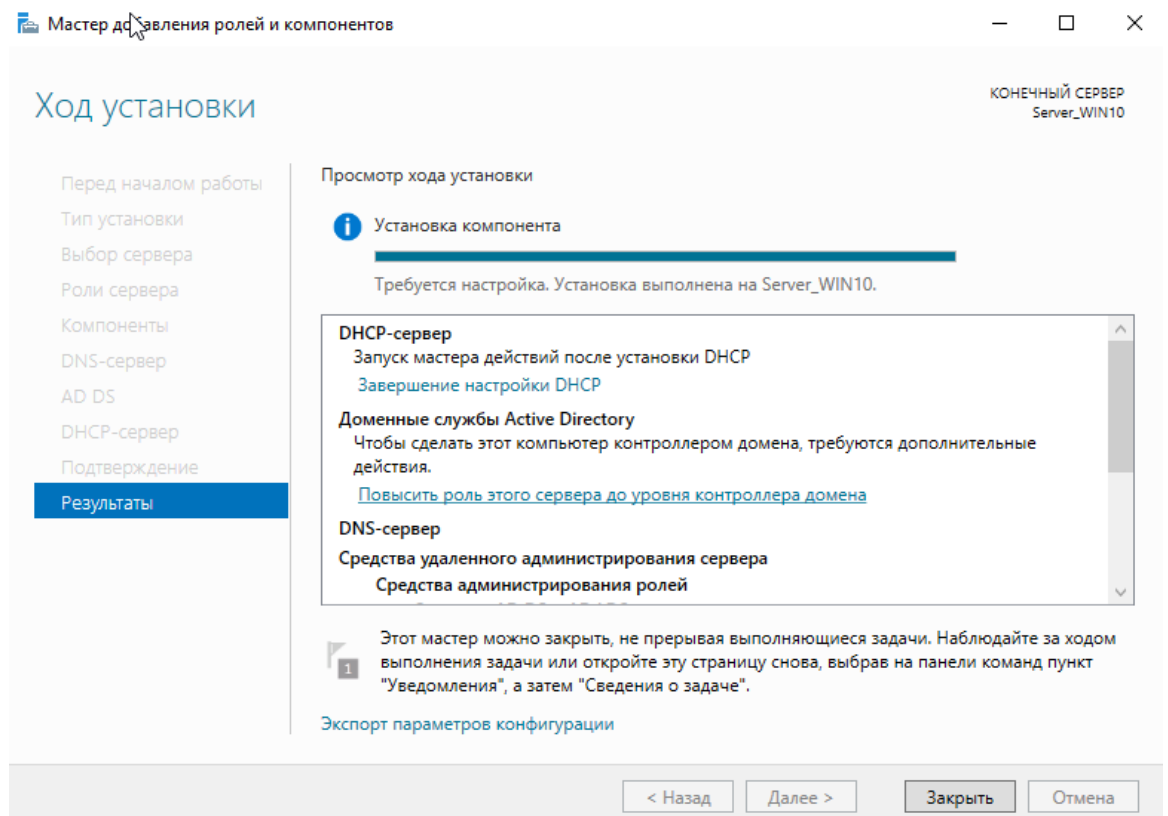


Рис. 3.4. Встановлення всіх служб для роботи серверу

Після встановлення на сервер служб DHCP, DNS, AD потрібно налаштувати кожну службу окремо для правильної роботи.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						35
Змн.	Арк.	№ докум.	Підпис	Дата		

Першою налаштовується сама доменна служба Active directory для створення домену мережі, щоб пристрої, які будуть використовувати цей домен, приймали та виконували всі групові політики, налаштовані на сервері (рис.3.5-3.7).

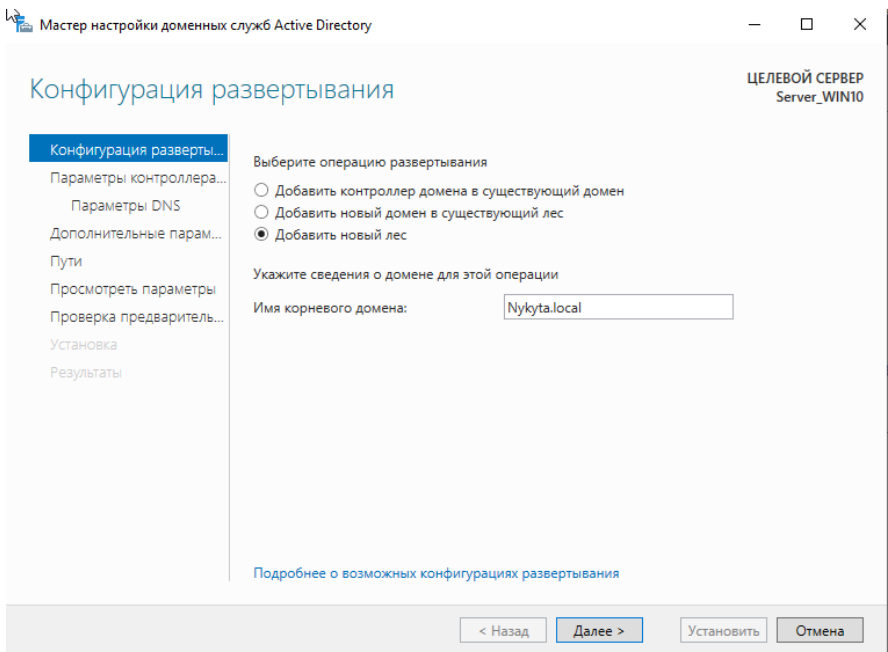


Рис. 3.5. Налаштування служби Active Directory

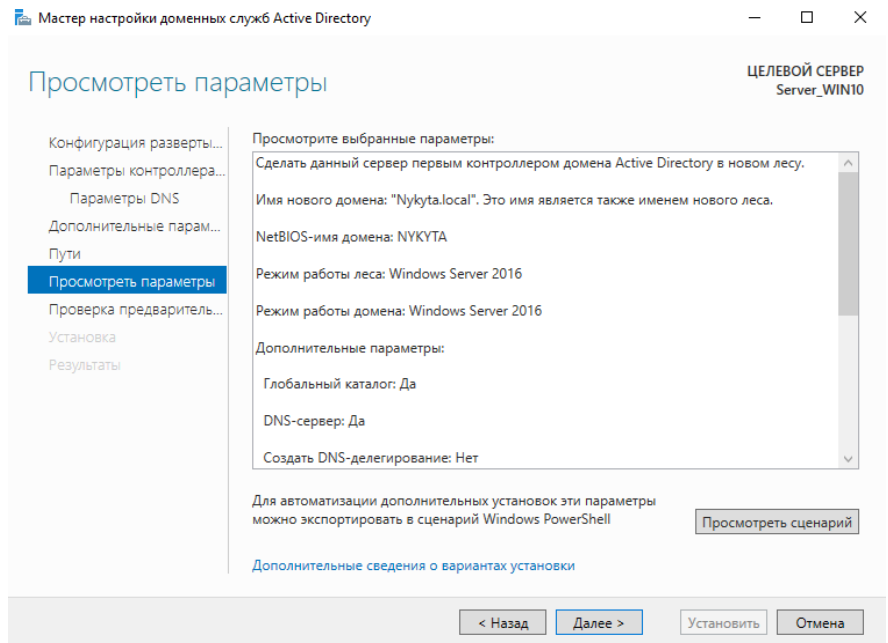


Рис. 3.6. Налаштування служби Active Directory

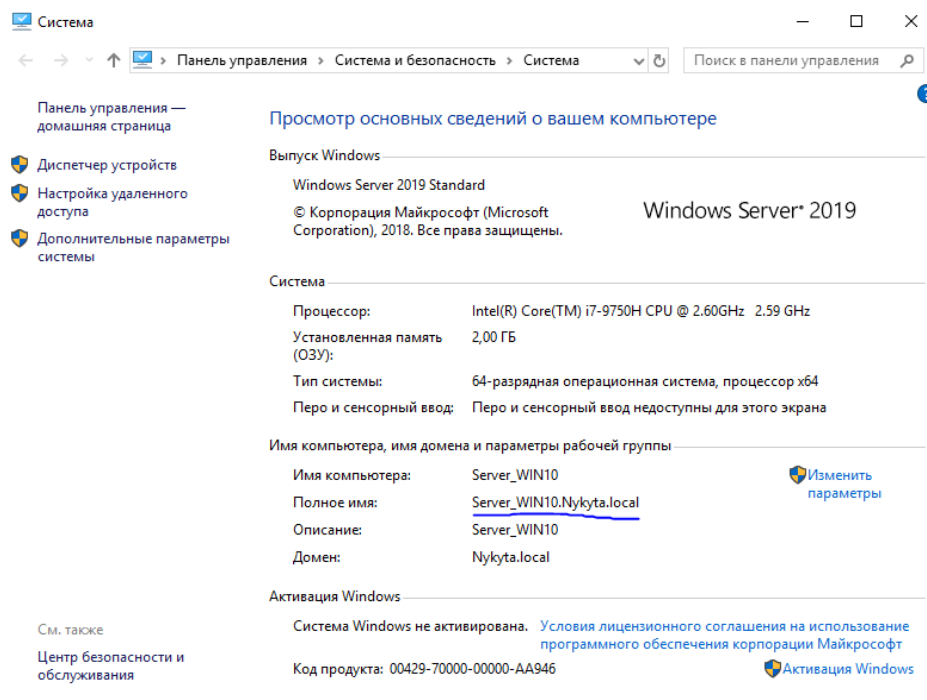


Рис. 3.7. Налаштування служби Active Directory

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

Налаштуємо також сервер DHCP на Windows 10 Server для масштабування мережі в майбутньому і для спрощення підключення локальних робочих станцій (рис.3.8-3.9).

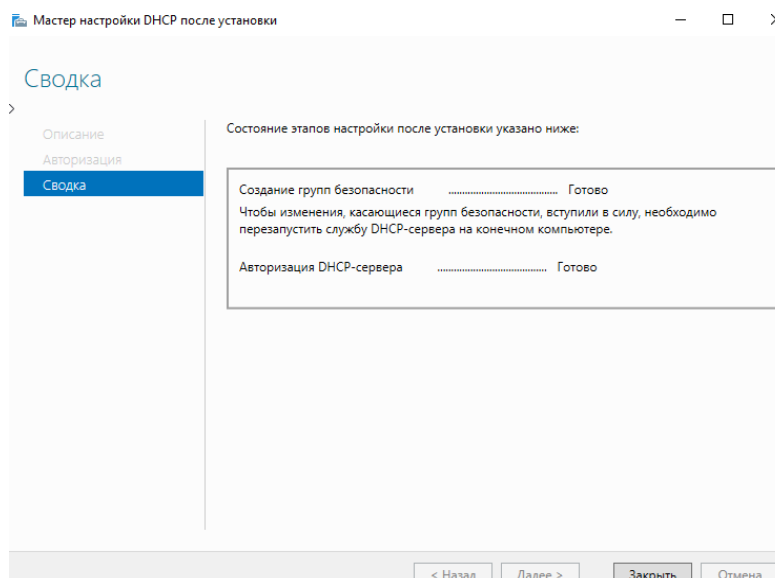


Рис. 3.8. Налаштування служби DHCP

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
192.168.1.90-192.168.1.100

Задержка подсети в миллисекундах:

< Назад

Рис. 3.9. Налаштування служби DHCP

Додатково також налаштуємо DNS на сервері, оскільки він потрібен для двох основних функцій: зберігання даних про конкретні IP-адреси домену та кешування інших ресурсів серверу (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: Nykyta.local

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

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

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

< Назад

Рис. 3.10. Налаштування служби DNS

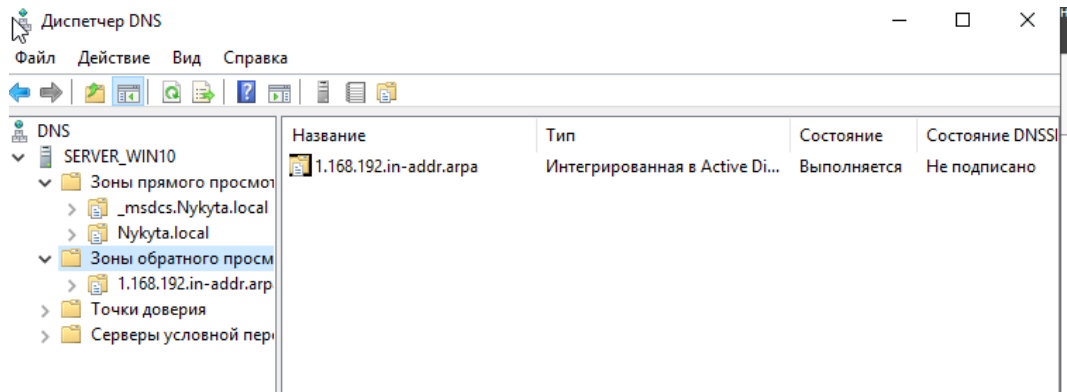


Рис. 3.11. Налаштування служби DNS

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 для зв'язку між маршрутизаторами, комутаторами та іншими приладами налаштуємо протокол маршрутизації. 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)#neetwork 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 таких ОС як Windows, починаючи з версії Windows XP, достатньо лише натиснути WIN+R та ввести команду mstsc.exe. Але для ОС Ubuntu потрібно встановити спеціальний додаток (Vinagre) для підключення до ОС Windows через віддалені робочі столи (рис.3.15).

```

nykyta@nykyta-VirtualBox:~$ sudo apt-get install vinagre
[sudo] пароль для nykyta:
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 libcacard0
  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 libcacard0
  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 объём занятого дискового пространства возрастёт на 52,5 М
В.
Хотите продолжить? [д/н]

```

Рис. 3.15. Встановлення додатку на ОС Ubuntu

Після налаштувань маршрутизації та віддалених робочих столів потрібно також налаштувати безпеку пристроїв. Для початку захистимо наші маршрутизатори за допомогою створення 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

І додатково налаштуємо параметри захисту на комутаторах, оскільки в нашій мережі досить багато DHCP-серверів. Якщо у злоумисника буде можливість підключити свій DHCP-сервер, то ми можемо втратити дані, які будуть знаходитися на робочих станціях. Тому 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

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						42
Змн.	Арк.	№ докум.	Підпис	Дата		

Також налаштуємо функцію Port Security 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 віддалено налаштовувати маршрутизатори та інші пристрої 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

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.

Для початку перевіriamo налаштування адресації серверу та наявність зв'язку між ним і пристроями мережі (рис.3.23-3.26).

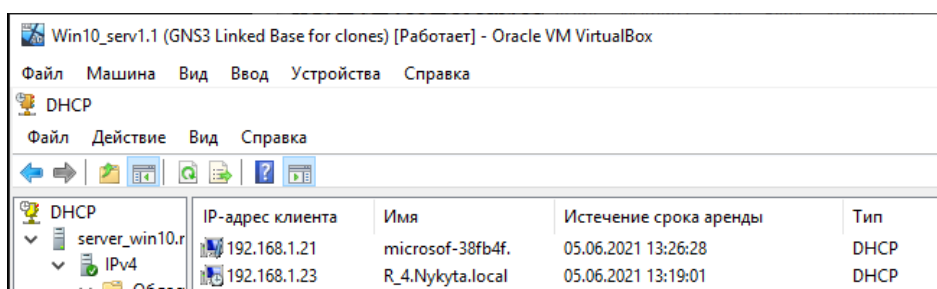


Рис. 3.23. Перевірка налаштувань серверу

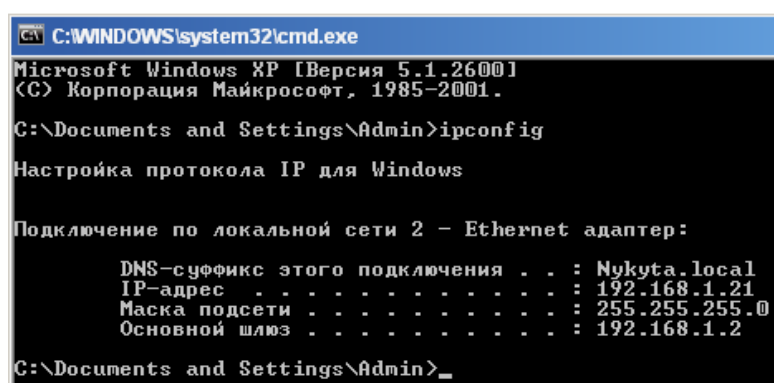


Рис. 3.24. Перевірка налаштувань серверу

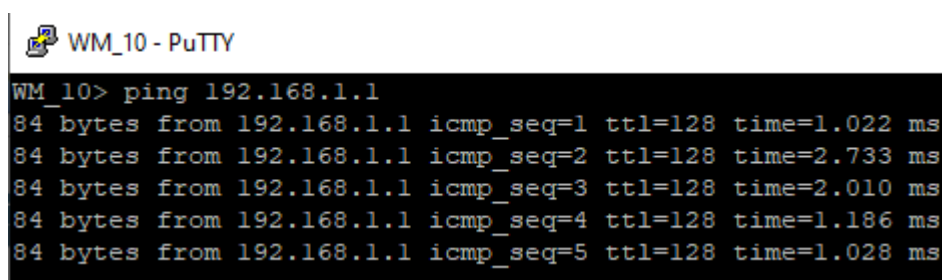


Рис. 3.25. Перевірка зв'язку з робочих станцій на серверу

```

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

Перевіримо роботу інших DHCP серверів, зокрема чи видають вони адреси робочим станціям і чи не виникає при цьому конфліктів (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

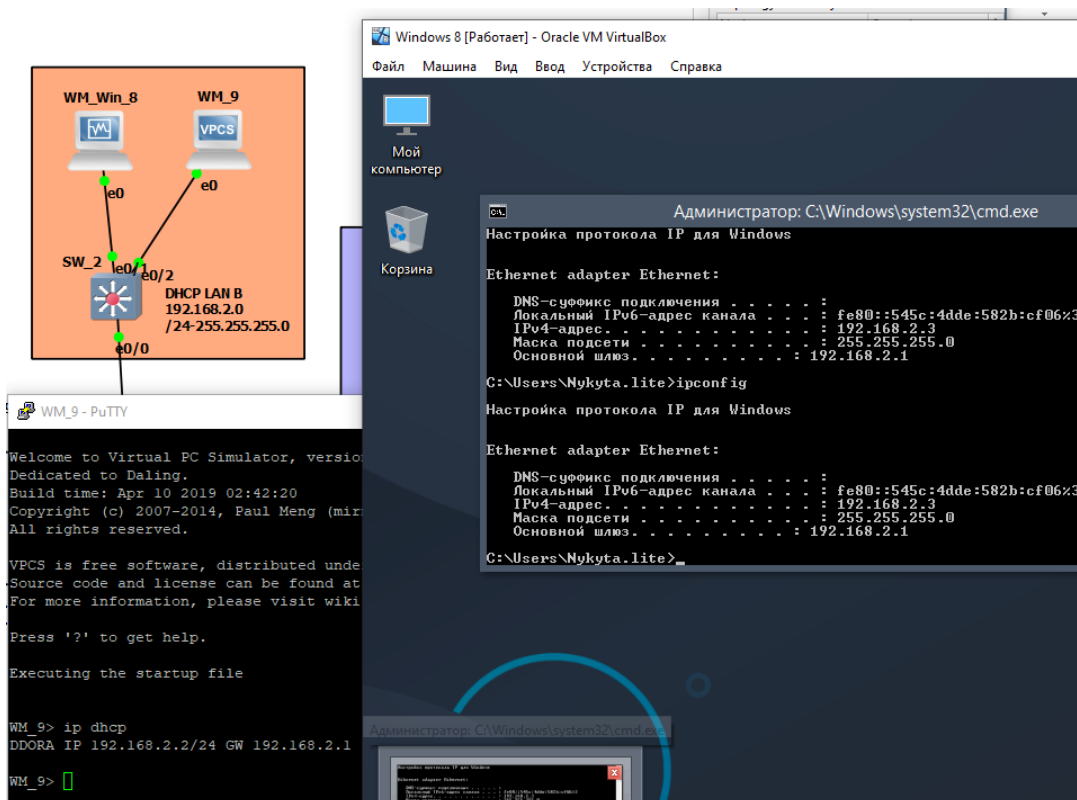


Рис. 3.28. Перевірка DHCP серверу

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

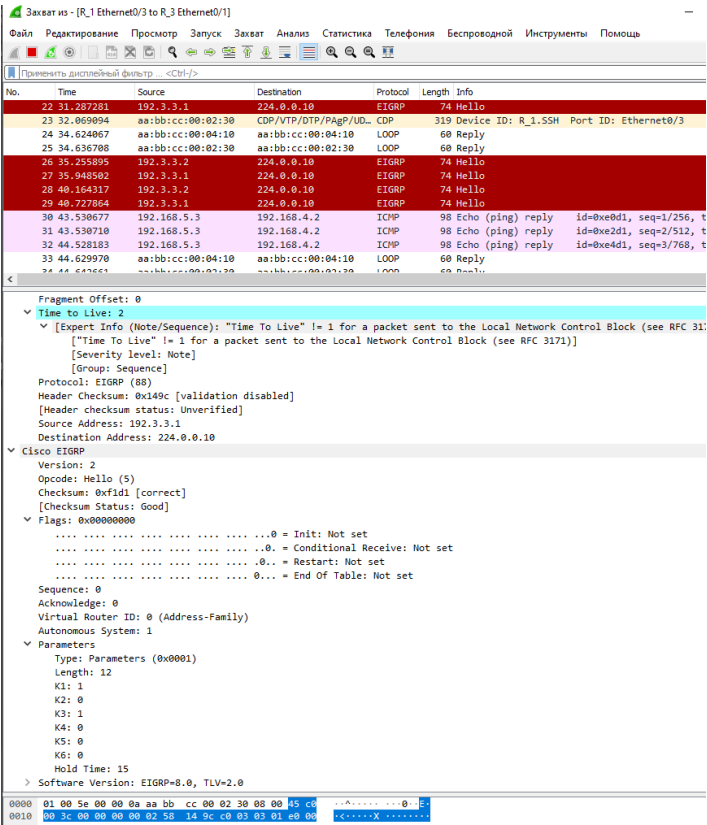


Рис. 3.30. Перевірка хешування MD5

Наступний крок – перевірка правильності налаштування SSH. Для цього спробуємо з маршрутизатора R_1 здійснити віддалене підключення до маршрутизатора R_3 (рис. 3.31-3.32).

```

R_1#SSH -1 192.3.3.2 R_3
Translating "R_3"

% Unknown command or computer name, or unable to find computer address
R_1#SSH -1 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

Захват из - [R_1 Ethernet0/3 to R_3 Ethernet0/1]

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр - <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
334	438.499956	192.3.3.1	192.3.3.2	TCP	60	30380 → 22 [ACK] Seq=728 Ack=1516 Win=2613 Len=0
335	438.500160	192.3.3.1	192.3.3.2	TCP	60	[TCP Window Update] 30380 → 22 [ACK] Seq=728 Ack=1516
336	438.500268	192.3.3.1	192.3.3.2	SSHv2	118	Client: Encrypted packet (len=64)
337	438.500391	192.3.3.1	192.3.3.2	SSHv2	60	Encrypted packet (len=4)[Malformed Packet]
338	438.500542	192.3.3.2	192.3.3.1	TCP	60	22 → 30380 [ACK] Seq=1516 Ack=796 Win=3333 Len=0
339	438.500639	192.3.3.2	192.3.3.1	SSHv2	138	Server: Encrypted packet (len=84)
340	438.507468	192.3.3.1	192.3.3.2	SSHv2	118	Client: Encrypted packet (len=64)
341	438.507628	192.3.3.1	192.3.3.2	SSHv2	90	Client: Encrypted packet (len=36)
342	438.507718	192.3.3.2	192.3.3.1	TCP	60	22 → 30380 [ACK] Seq=1600 Ack=896 Win=3233 Len=0
343	438.508180	192.3.3.2	192.3.3.1	SSHv2	122	Server: Encrypted packet (len=68)
344	438.715542	192.3.3.1	192.3.3.2	TCP	60	30380 → 22 [ACK] Seq=896 Ack=1668 Win=3976 Len=0
345	439.154076	192.3.3.2	224.0.0.10	EIGRP	74	Hello
346	440.015244	192.3.3.1	224.0.0.10	EIGRP	74	Hello
347	442.230018	192.3.3.1	192.3.3.2	SSHv2	106	Client: Encrypted packet (len=52)
348	442.230284	192.3.3.2	192.3.3.1	SSHv2	90	Server: Encrypted packet (len=36)
349	442.234769	192.3.3.1	192.3.3.2	SSHv2	118	Client: Encrypted packet (len=64)
350	442.234906	192.3.3.1	192.3.3.2	SSHv2	60	Encrypted packet (len=4)[Malformed Packet]
351	442.235046	192.3.3.2	192.3.3.1	TCP	60	22 → 30380 [ACK] Seq=1704 Ack=1016 Win=3113 Len=0
352	442.235055	192.3.3.2	192.3.3.1	SSHv2	106	Server: Encrypted packet (len=52)
353	442.239341	192.3.3.1	192.3.3.2	SSHv2	118	Client: Encrypted packet (len=64)
354	442.239520	192.3.3.1	192.3.3.2	SSHv2	74	Encrypted packet (len=20)[Malformed Packet]
355	442.239674	192.3.3.2	192.3.3.1	TCP	60	22 → 30380 [ACK] Seq=1756 Ack=1100 Win=3029 Len=0
356	442.239694	192.3.3.2	192.3.3.1	SSHv2	90	Server: Encrypted packet (len=36)
357	442.244427	192.3.3.1	192.3.3.2	SSHv2	106	Client: Encrypted packet (len=52)
358	442.244638	192.3.3.2	192.3.3.1	SSHv2	90	Server: Encrypted packet (len=36)
359	442.244756	192.3.3.2	192.3.3.1	SSHv2	106	Server: Encrypted packet (len=52)
360	442.244975	192.3.3.1	192.3.3.2	TCP	60	30380 → 22 [ACK] Seq=1152 Ack=1880 Win=3764 Len=0

< >

> Frame 349: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface -, id 0
 > Ethernet II, Src: aa:bb:cc:00:02:30 (aa:bb:cc:00:02:30), Dst: aa:bb:cc:00:04:10 (aa:bb:cc:00:04:10)
 > Internet Protocol Version 4, Src: 192.3.3.1, Dst: 192.3.3.2
 > Transmission Control Protocol, Src Port: 30380, Dst Port: 22, Seq: 948, Ack: 1704, Len: 64
 > SSH Protocol

Рис. 3.32. Перевірка протоколу SSH

Тепер протестуємо протокол маршрутизації EIGRP за допомогою перевірки зв'язку між віддаленими мережами. Для економії ресурсів запустимо лише Windows 10 Server та будемо перевіряти зв'язок з ним з робочих станцій GNS3. Оскільки IP Windows 10 Server 192.168.1.1, то 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

Перевіримо роботу віддалених робочих столів шляхом підключення з ОС Windows XP до Windows 7 та з Ubuntu до Windows 10 Server (рис.3.34-3.39).

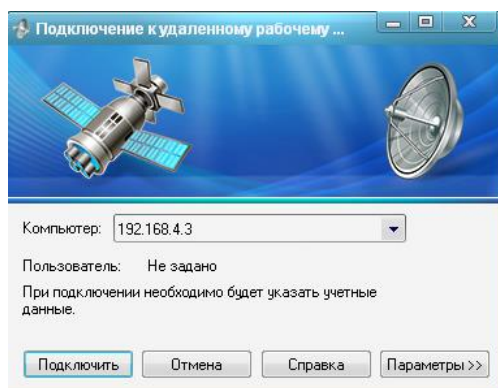


Рис. 3.34. Підключення до Windows 7 з робочої станції Windows XP

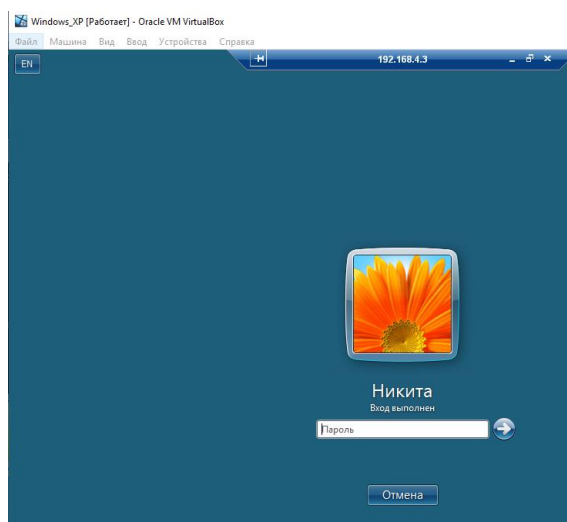


Рис. 3.35. Підключення до Windows 7 з робочої станції Windows XP

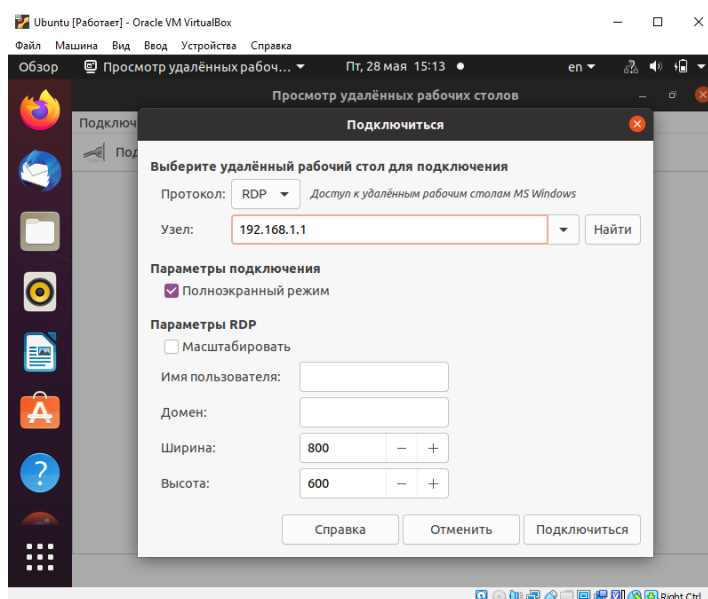


Рис. 3.36. Підключення до Windows 10 Server з робочої станції Ubuntu

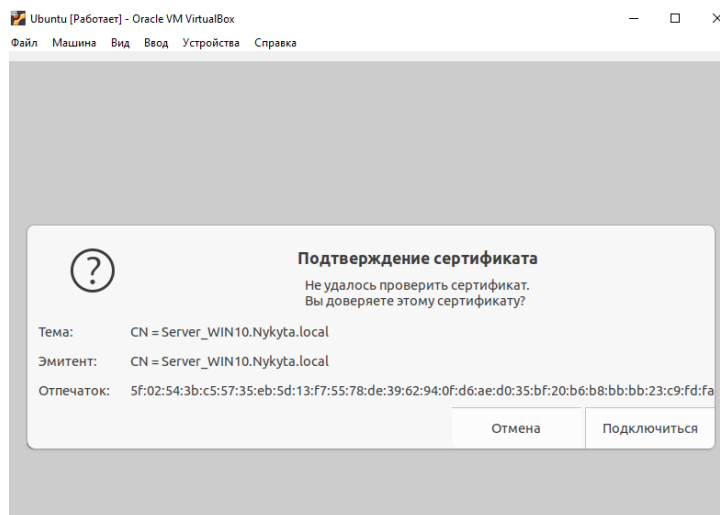


Рис. 3.37. Підключення до Windows 10 Server з робочої станції Ubuntu

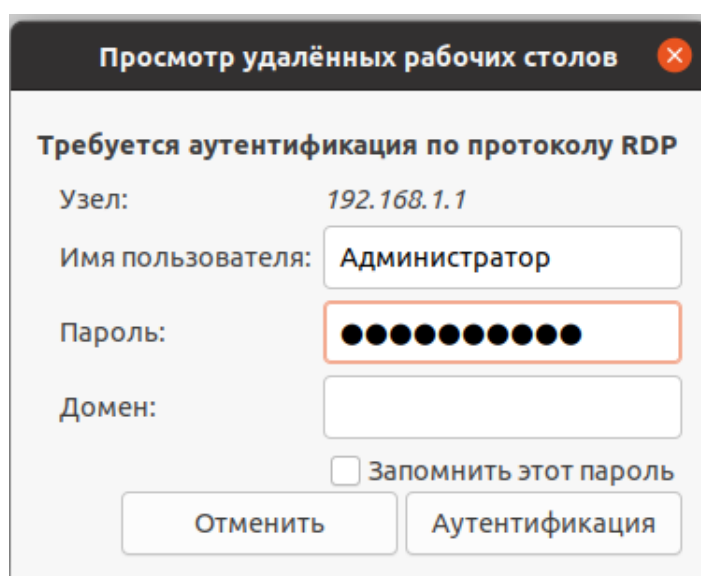


Рис. 3.38. Підключення до Windows 10 Server з робочої станції Ubuntu

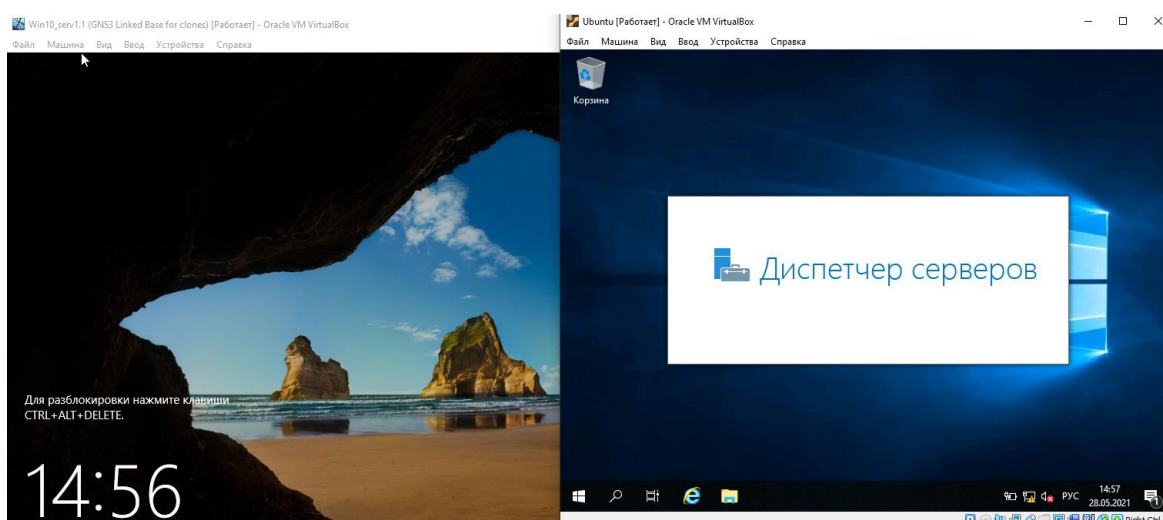


Рис. 3.39. Підключення до Windows 10 Server з робочої станції Ubuntu

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						49
Змн.	Арк.	№ докум.	Підпис	Дата		

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

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

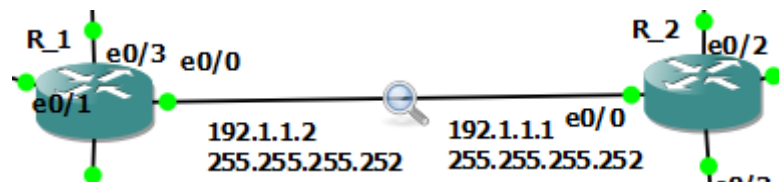


Рис. 3.40. Перевірка налаштувань MD5

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 02 58 16 9d c0 01 01 02 e0 00  <.....X
  
```

Всі готово к загрузке или захвату

Рис. 3.41. Перевірка налаштувань MD5

Тепер перевіримо налаштування довіреного порту. Оскільки у нас довірений інтерфейс налаштований саме на e0/0, то тільки при підключені до нього буде працювати DHCP-сервер. Створимо додатковий маршрутизатор і налаштуємо його як DHCP-сервер(рис.3.42).

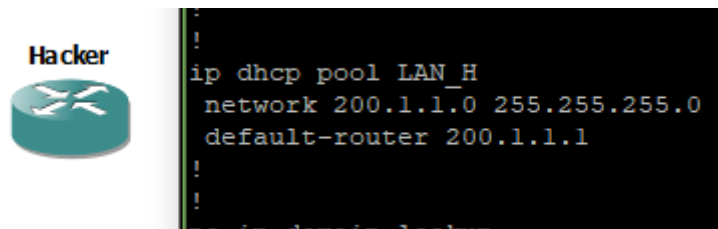


Рис. 3.42. Налаштування додаткового DHCP-серверу

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

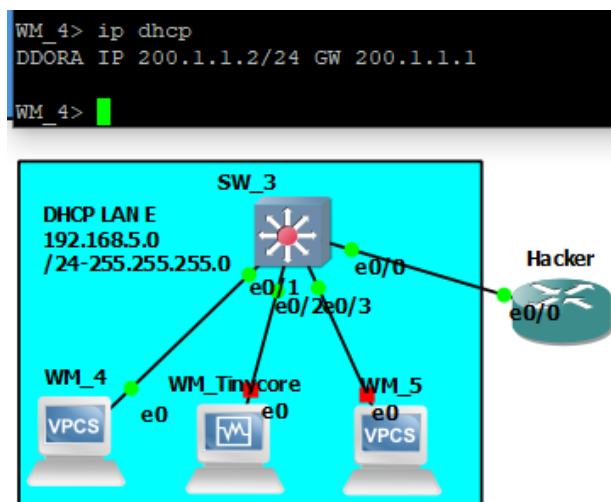


Рис. 3.43. Отримання IP-адреси від сервера-зловмисника

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

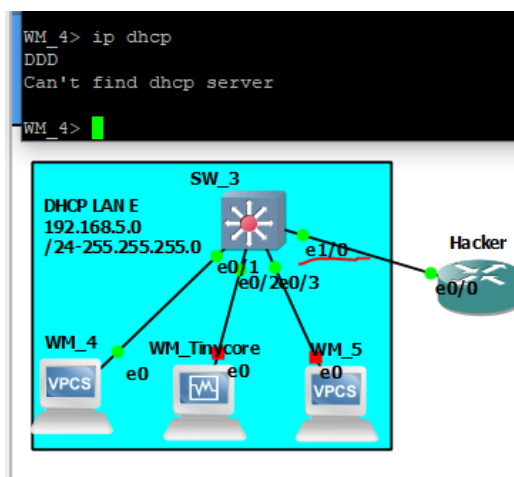


Рис. 3.44. Підключення сервера-зловмисника до недовіреного порту комутатора.

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

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.

Якщо в мережі будуть додаватися ще робочі станції з іншими операційними системами, і ці системи будуть підтримувати віддалені робочі столи, то комп'ютери зможуть взаємодіяти з ними. Також це стосується нових маршрутизаторів, якщо на них буде налаштовано протокол SSH.

Щодо захисту, оскільки наша мережа використовує досить багато DHCP серверів, в нагоді став захист портів, оскільки при бажанні зловмисник міг би приєднатися до комутатору та давати свої IP-адреси, що призвело б до пошкодження мережі та тягнуло б за собою втрату даних з робочих станцій та мережі в цілому. Також захист на маршрутизаторах буде доцільний, якщо у зловмисника вийде приєднатися до маршрутизатора напряму. Це може тягнути за собою як втрату даних, так і знищення пристрою, підміну даних та інше.

З точки зору логіки, найкращою для підключення нових приладів буде підмережа LAN A, оскільки саме в цій мережі було встановлено та налаштовано сервер під управлінням операційної системи Windows 10 Server, що в майбутньому дає змогу як автоматичної IP-адресації, так і змінення налаштувань для всіх (як нових, так і вже налаштованих) пристроїв за допомогою змінення групових політик.

Ще одна перевага мережі в тому, що на рівні ядра є 4 маршрутизатори, які з'єднані між собою і якщо один з них виходить з ладу, то за допомогою протоколу EIGRP досить швидко знаходиться новий маршрут до потрібної мережі.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						52
Змн.	Арк.	№ докум.	Підпис	Дата		

Щодо недоліків даної мережі, чим більш професійне та якісне обладнання, тим воно буде дорожче. Тобто комутатори та маршрутизатори від компанії CISCO є досить дорогими через їх надійність, якість, гарантію на заміну пристрою чи його компонентів при неполадках в малі строки, що досить вигідно великим компаніям, коли кожна хвилина коштує грошей. Також для налаштування та моніторингу стану приладів буде потрібно наймати працівника із знаннями цих пристроїв, тобто чим складніший та дорожчий пристрій, тим більше буде потрібна заробітна плата працівнику. Тому для невеликих компаній чи організацій мережа з використанням комутаторів та маршрутизаторів CISCO буде не вигідною.

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. На робочій станції під управлінням операційної системи Ubuntu було встановлено додаток для віддаленого керування робочими столами під управлінням інших операційних систем. Для зв'язку між всіма підмережами схеми було використано протокол маршрутизації EIGRP. Для захисту було налаштовано хешування MD5, довірені порти та користувачів з різними привілеями.

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

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						53
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У дипломному проекті була спроектована ієрархічна модель комп'ютерної гетерогенної мережі на базі протоколу маршрутизації EIGRP. Для побудови мережі використовувалися технології від компанії CISCO. При розробці були враховані всі вимоги до проекту і створено гетерогенну мережу на базі протоколу EIGRP.

Для початку було проведено аналіз та вибір існуючих технологій побудови сучасних гетерогенних мереж. Зокрема було обрано графічний симулятор GNS3, ОС Windows, Linux, Tinycore, Ubuntu, службу Active directory, протокол маршрутизації EIGRP, а також технології прикладного рівня SSH та DHCP.

На етапі розробки мережі було визначено, що комп'ютерна мережа міститиме досить багато робочих станцій, тому була розроблена топологія мережі. Щоб мережа використовувала досить багато IP-адрес для масштабованості в майбутньому і для комфорту налаштувань підключень нових робочих станцій та приладів було використано автоматичну видачу IP-адрес за допомогою DHCP. Для можливості віддаленого доступу не лише між робочими станціями, а також до приладів, використовувався захищений протокол SSH.

Далі було спроектовано логічну ієрархічну модель комп'ютерної мережі трьох рівнів, яка складається з рівнів ядра, розподілу і доступу.

Це дозволяє забезпечити зміни мережі в майбутньому – масштабованість та надійність роботи. Комп'ютерна мережі має в собі сімнадцять робочих станцій з яких:

- один сервер під управлінням Windows 10 Server;
- три робочих станції під управлінням Windows XP, Windows 7, Windows 8;
- дві робочі станції під управлінням TinyCore, Ubuntu;
- одинадцять робочих станцій під управлінням влаштованих в програму GNS3 образів робочих станцій VPCS.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						54
Змн.	Арк.	№ докум.	Підпис	Дата		

Для масштабованості мережі в майбутньому використовувалися образи комутатора другого рівня з шістнадцятьма портами (образ i86bi-linux-l2-adventerprise-15.1b.bin), адже 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 серверу було обрано образ Windows 10 Server та на ньому було повністю налаштовано Active Directory, DHCP, DNS, компоненти. Сервер також дає змогу зазначати орендовані адреси та назви комп'ютерів і пристроїв, які орендували їх. Також можна продивитися заборонені IP-адреси. За допомогою редактору групових політик є можливість змінити налаштування мережі, в якій знаходиться сервер, і таким чином всі зміни, які були вказані в них, застосовуються також і до мережі серверу, що спрощує налаштування в даній мережі.

В третьому розділі було обрано обладнання на програмне забезпечення. Образи маршрутизаторів та комутаторів обрані від компанії CISCO через їх надійність на гнучкість в налаштуваннях. Також ще через те, що протокол EIGRP підтримується і використовується тільки фірмою CISCO. Це ще раз доводить те, що система буде досить надійною. Програма, в якій виконувався дипломний проект (GNS3) була обрана через, те що вона дозволяє створити саме гетерогенну мережу за допомогою VirtualBox, яка, в свою чергу, дозволяє використовувати різні операційні системи, зокрема Windows, Linux, Ubuntu, Tinycore.

Проведено налаштування пристроїв та аналіз результатів, сформовано висновки стосовно модернізації та вдосконалення роботи. Реалізована мережа є готовим макетом реальної реалізації проекту, а конфігурації можуть застосовуватися для реального обладнання.

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						55
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гетерогенна комп'ютерна мережа [Електронний ресурс] – [Гетерогенні комп'ютерні мережі — Вікіпедія \(wikipedia.org\)](#)
2. Active directory [Електронний ресурс] – https://ru.wikipedia.org/wiki/Active_Directory
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/htdhcpsv.html
5. DNS Server [Електронний ресурс] - <https://ru.wikipedia.org/wiki/DNS>
6. Windows 10 Server [Електронний ресурс] - <https://www.microsoft.com/ru-ru/windows-server>
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. Windows 7 [Електронний ресурс] -https://ru.wikipedia.org/wiki/Windows_7
11. Windows 8.1 [Електронний ресурс] - https://ru.wikipedia.org/wiki/Windows_8.1
12. Ubuntu [Електронний ресурс] - <https://en.wikipedia.org/wiki/Ubuntu>
13. Хешування MD5 [Електронний ресурс] – <https://uk.wikipedia.org/wiki/MD5>

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						56
Змн.	Арк.	№ докум.	Підпис	Дата		

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] - <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://stor.net.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] - <https://habr.com/ru/post/266503/>
20. VirtualBox [Електронний ресурс] - <https://www.virtualbox.org/>
21. Wireshark User Guide [Електронний ресурс] - https://www.wireshark.org/docs/wsug_html/
22. Wireshark [Електронний ресурс] - https://www.wireshark.org/docs/wsug_html_chunked/ChAdvExpert.html

ДОДАТКИ

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						58
Змн.	Арк.	№ докум.	Підпис	Дата		

Маршрутизатор R_1

R_1

#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 Nykyta 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

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
no ip address	shutdown

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						60
Змн.	Арк.	№ докум.	Підпис	Дата		

```

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

SW_1

```

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
!
interface Ethernet0/2

```

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						62
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport mode access

switchport port-security maximum 100

switchport port-security

switchport port-security MAC-address sticky

duplex auto

!

interface Ethernet0/3

switchport mode access

switchport port-security maximum 100

switchport port-security

switchport port-security MAC-address sticky

duplex auto

!

interface Ethernet1/0

duplex auto

!

interface Ethernet1/1

duplex auto

!

interface Ethernet1/2

duplex auto

!

interface Ethernet1/3

duplex auto

!

interface Ethernet2/0

duplex auto

!

interface Ethernet2/1

duplex auto

!

interface Ethernet2/2

duplex auto

!

```

```

interface Ethernet2/3

duplex auto

!

interface Ethernet3/0

duplex auto

!

interface Ethernet3/1

duplex auto

!

interface Ethernet3/2

duplex auto

!

interface Ethernet3/3

duplex auto

!

interface VLAN1

ip address 192.168.3.210 255.255.255.0

!

no ip http server

!

control-pLANe

!

line con 0

exec-timeout 0 0

privilege level 15

logging synchronous

line aux 0

exec-timeout 0 0

privilege level 1

```

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						63
Змн.	Арк.	№ докум.	Підпис	Дата		

					КБ.КВ.Б – 125 – 21 – ПЗ	Арк.
						64
Змн.	Арк.	№ докум.	Підпис	Дата		