

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

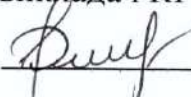
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту гетерогенної
мережі організації»

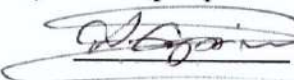
Виконав: студент 4-го курсу групи КБ-20-2
спеціальності 125 «Кібербезпека»

 Анастасія НЕСТЕРЧУК

Керівник старший викладач КІ та КБ

 Єлизавета ТРОКОЗ

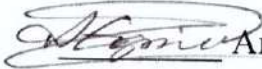
Рецензент завідувач кафедри КІ та КБ, к.т.н., доцент

 Андрій ЄФІМЕНКО

Державний університет «Житомирська політехніка»
Факультет інформаційно– комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Нестерчук Анастасія Володимирівна

Тема роботи: «Проект підсистеми захисту гетерогенної мережі організації»

затверджена Наказом університету від 5 березня 2024 р. № 98/с

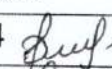
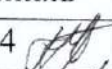
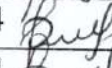
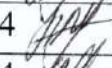
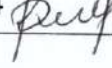
Термін здачі студентом закінченої роботи 26 червня 2024 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
вихідні дані для роботи;

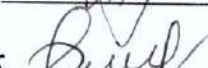
Обладнання та програмне забезпечення:

1. Топологія мережі.
2. Windows Server 2019
3. Ubuntu 20.04.6 LTS.
4. Windows 10.
5. Windows 7.

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єлизавета ТРОКОЗ	05.03.2024 	05.03.2024 
2	Єлизавета ТРОКОЗ	05.03.2024 	05.03.2024 
3	Єлизавета ТРОКОЗ	05.03.2024 	05.03.2024 

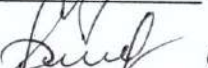
Студент  Анастасія НЕСТЕРЧУК

Керівник  Єлизавета ТРОКОЗ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	05.03.2024-05.03.2024	Виконано
2	Аналіз теоретичний аспектів гетерогенної мережі	04.04.2024-10.03.2024	Виконано
3	Аналіз вимог до системи захисту	11.03.2024-18.03.2024	Виконано
4	Вибір та обґрунтування методів і засобів захисту	19.03.2024-29.03.2024	Виконано
5	Проектування топології гетерогенної мережі	01.04.2024-12.04.2024	Виконано
6	Розробка схеми IP-адресації	13.04.2024-17.04.2024	Виконано
7	Вибір мережевого обладнання	18.04.2024-21.04.2024	Виконано
8	Налагодження мережевих пристроїв	22.04.2024-04.05.2024	Виконано
9	Перевірка роботи в мережі	05.05.2024-10.05.2024	Виконано
10	Оформлення пояснювальної записки	11.05.2024-23.06.2024	Виконано
11	Захист кваліфікаційної роботи	26.06.2024	Виконано

Студент  Анастасія НЕСТЕРЧУК

Керівник  Єлизавета ТРОКОЗ

АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра складається з пояснювальної записки до курсового проєкту, яка містить вступ, три розділи, висновки, список використаної літератури та додатки. Текстова частина викладена на 90 сторінках друкованого тексту. Пояснювальна записка включає 10 сторінок додатків. Список використаних джерел містить 15 найменування і займає 1 сторінку. В роботі наведено 89 рисунків та 3 таблиці. Загальний обсяг роботи – 100 сторінок.

Метою кваліфікаційної роботи є розробка проєкту підсистеми захисту гетерогенної мережі організації.

В роботі розглянуто теоретичні аспекти побудови та функціонування гетерогенних мереж. Проаналізовано використання протоколів і функцій захисту канального рівня, протоколу резервування шлюзу VRRP, стандарту відправки і реєстрації подій Syslog, протоколу аутентифікації та авторизації Radius, а також міжмережевих екранів. Розроблено топологію мережі та систему адресації, визначено необхідне обладнання та розроблено підсистему захисту. Налаштовано та протестовано систему захисту, результати відповідають поставленим вимогам.

Ключові слова: МЕРЕЖЕВА БЕЗПЕКА, ACTIVE DIRECTORY, RADIUS-SERVER, DHCP SNOOPING, PORT SECURITY, SYSLOG, ГЕТЕРОГЕННА МЕРЕЖА, КІБЕРЗАГРОЗИ, ІНФОРМАЦІЙНА БЕЗПЕКА.

					КІК.КР.Б – 125 – 19 – 24 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту гетерогенної мережі організації	Літ.	Арк.	Аркуші
Розроб.		Нестерчук А.В.		25.06				
Керівник		Трокоз Є.М.		25.06			4	100
Реценз.		Єфіменко А.А.		25.06		ФІКТ, Гр. КБ-20-2		
Н. контр.		Трокоз Є.М.		25.06				
Затверд.		Єфіменко А.А.		25.06				

ANNOTATION

The Bachelor's thesis consists of an explanatory note to the course project, which includes an introduction, three chapters, conclusions, a list of references, and appendices. The text part is presented on 89 pages of printed text. The explanatory note includes 10 pages of appendices. The list of references contains 15 titles and occupies 1 page. The work contains 89 figures and 3 tables. The total volume of the work is 99 pages.

The purpose of the thesis is to develop a project for the protection subsystem of the organization's heterogeneous network.

The work examines the theoretical aspects of building and functioning of heterogeneous networks. It analyzes the use of protocols and protection functions at the data link layer, the VRRP gateway redundancy protocol, the Syslog event sending and logging standard, the Radius authentication and authorization protocol, as well as firewalls. The network topology and addressing system were developed, necessary equipment was determined, and the protection subsystem was designed. The protection system was configured and tested, and the results meet the specified requirements.

Keywords: NETWORK SECURITY, ACTIVE DIRECTORY, RADIUS SERVER, DHCP SNOOPING, PORT SECURITY, SYSLOG, HETEROGENEOUS NETWORK, CYBER THREATS, INFORMATION SECURITY.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	7
РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ ГЕТЕРОГЕННИХ МЕРЕЖ.....	9
1.1 Гетерогенна мережа.....	9
1.2 Протоколи і функції захисту каналного рівня	11
1.3 Протокол резервування шлюзу VRRP	24
1.4 Стандарт відправки і реєстрації подій Syslog.....	27
1.5 Протокол аутентифікації та авторизації Radius.....	29
1.6 Міжмережевий екран.....	32
РОЗДІЛ 2 ТОПОЛОГІЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ.....	35
2.1 Побудова топології мережі	35
2.2 Вибір обладнання.....	37
2.3. Розробка схеми адресації мережі	42
2.4. Розробка підсистеми захисту гетерогенної мережі організації	46
РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ ГЕТЕРОГЕННОЇ МЕРЕЖІ.....	52
3.1 Базове налагодження пристроїв мережі	52
3.2 Налagodження Active Directory і робочих станцій	54
3.3 Налagodження підсистеми захисту	69
3.4 Тестування роботи підсистеми захисту мережі.....	82
ВИСНОВКИ.....	88
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	89
ДОДАТКИ.....	90

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD – Active Directory

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

STP – Spanning Tree Protocol

BPDU – Bridge Protocol Data Unit

IP – Internet Protocol

SSH – Secure Shell

OS – Operating System

ACL – Access Control List

VPN – Virtual Private Network

IPsec – Internet Protocol Security

MAC – Media Access Control

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Проєкт підсистеми захисту гетерогенної мережі організації обумовлена стрімким розвитком інформаційних технологій та збільшенням кількості кіберзагроз. У сучасних умовах організації стикаються з необхідністю захисту різнорідних мережевих середовищ, що включають різні типи обладнання, операційні системи та програмне забезпечення. Така різноманітність ускладнює забезпечення безпеки та вимагає комплексного підходу до захисту мережі. Зростаюча кількість кіберзагроз та постійне вдосконалення методів атак змушують організації постійно оновлювати та покращувати свої системи захисту. Важливість даного проєкту також підкріплюється необхідністю відповідності сучасним законодавчим нормам та стандартам безпеки, які вимагають від організацій забезпечення високого рівня захисту конфіденційної інформації. Ефективний захист гетерогенної мережі дозволяє уникнути значних фінансових втрат та підвищує довіру клієнтів і партнерів до організації. Таким чином, розробка підсистеми захисту гетерогенної мережі є надзвичайно актуальною та необхідною для забезпечення інформаційної безпеки в сучасному світі.

Метою кваліфікаційної роботи є розробка підсистеми захисту для гетерогенної мережі організації, яка забезпечить ефективний захист від кіберзагроз, підвищить рівень безпеки даних та відповідатиме сучасним стандартам інформаційної безпеки.

Об'єктом дослідження є процес проєктування топології гетерогенної мережі організації і розробка підсистеми захисту.

Предметом дослідження є методи, засоби та технології налаштування мережевих пристроїв, протоколи, функції та інструменти забезпечення захисту мережі та кінцевих користувачів від різних типів загроз.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ ГЕТЕРОГЕННИХ МЕРЕЖ

1.1 Гетерогенна мережа.

Гетерогенна комп'ютерна мережа – це мережа, яка об'єднує персональні комп'ютери та інші пристрої з різними операційними системами або протоколами передачі даних. Наприклад, локальна мережа, що включає комп'ютери під керуванням Microsoft Windows, Linux і MacOS, є гетерогенною. Цей термін також застосовується до бездротових мереж, які використовують різні технології для підключення. Наприклад, бездротова мережа, яка надає доступ через бездротову локальну мережу і може перемикатися на стільниковий зв'язок для забезпечення доступу, також називається гетерогенною мережею.

З семантичної точки зору важливо підкреслити, що термін "гетерогенні мережі" може мати різні значення в сфері бездротових телекомунікацій. Зокрема, він може позначати концепцію добре інтегрованої і всепроникної сумісності між різними протоколами, які застосовуються в різних зонах покриття (HetNet). В інших випадках цей термін може вказувати на нерівномірний просторовий розподіл користувачів або бездротових точок доступу (просторова неоднорідність). Таким чином, використання терміна "гетерогенні мережі" без відповідного контексту може призвести до непорозумінь у науковій літературі при рецензуванні роботи іншими фахівцями.

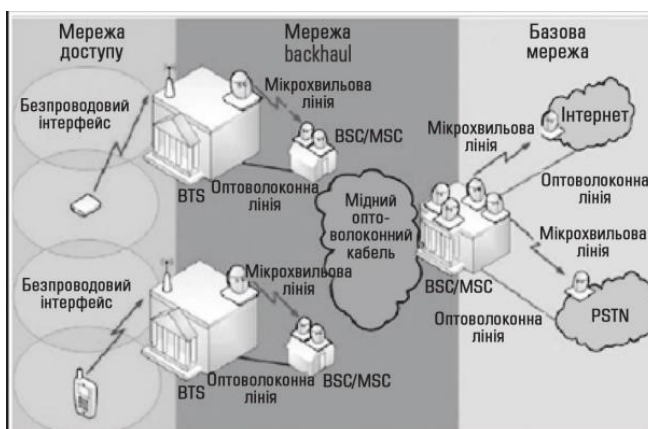


Рисунок 1.1 – Ієрархія мереж: мережа доступу, мережа backhaul і базова мережа

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

У різноманітних бездротових мережах, таких як WiFi, LTE, WiMax, UMTS, GPSR і інші, широко використовується технологія перемикання між різними точками доступу. Це необхідно для того, щоб користувач міг без перерви утримувати зв'язок під час руху в мережі з різними типами доступу. Ефективний алгоритм перемикання дозволяє автоматично переходити між різними точками доступу, забезпечуючи стабільний та надійний зв'язок для користувача. Також алгоритм прийняття рішень про перемикання мережі у гетерогенних безпроводних мережах може бути складним процесом, що базується на різних факторах та критеріях. Оцінка міцності сигналу, пропускної здатності, затримки, стабільності з'єднання та вартості передачі даних можуть бути важливими аспектами у виборі оптимальної мережі для перемикання.

- Збір інформації: Система збирає дані про міцність сигналу, пропускну здатність, затримку, стабільність з'єднання та вартість передачі даних кожної доступної мережі.
- Оцінка мереж: На основі зібраної інформації система оцінює кожен мережу за кожним з критеріїв.
- Визначення ваги критеріїв: Система визначає важливість кожного з критеріїв для конкретного користувача або сценарію використання.
- Ранжування мереж: Мережі ранжуються відповідно до їхньої загальної оцінки, яка обчислюється на основі ваг критеріїв.
- Прийняття рішення: Система вибирає мережу з найвищим рейтингом, яка найкращим чином відповідає потребам користувача або конкретному сценарію використання.
- Перемикання мережі: Якщо обрана мережа відрізняється від поточної, система автоматично здійснює перемикання на обрану мережу.
- Моніторинг: Після перемикання система продовжує моніторити якість з'єднання та можливість інших мереж для подальшого вирішення процесу перемикання.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

Будова гетерогенної мережі включає в себе різноманітні типи пристроїв та технологій, які взаємодіють між собою для забезпечення комунікації та обміну даними. Це можуть бути персональні комп'ютери, сервери, маршрутизатори, комутатори, мобільні пристрої, бездротові точки доступу тощо.

У гетерогенній мережі можуть використовуватися різні технології передачі даних, такі як Ethernet, Wi-Fi, Bluetooth, LTE, WiMax, UMTS, GSM, а також інші. Ці технології можуть використовуватися як окремо, так і у поєднанні одна з одною для створення ефективної та надійної мережі зв'язку.

Основні складові гетерогенної мережі включають в себе:

- Фізичні компоненти: Це пристрої та обладнання, які складають мережу, такі як комп'ютери, сервери, маршрутизатори, комутатори, кабелі, бездротові точки доступу тощо.
- Програмне забезпечення: Включає операційні системи, драйвери пристроїв, програми для управління та моніторингу мережі, а також програми застосування, які використовують мережеві ресурси.
- Протоколи комунікації: Це набір правил та стандартів, за якими пристрої обмінюються даними у мережі. Це можуть бути мережеві протоколи на різних рівнях моделі OSI, такі як TCP/IP, Ethernet, Wi-Fi, Bluetooth тощо.
- Мережеві сервіси та додатки: Це сервіси та програми, які використовуються для забезпечення певних функцій у мережі, таких як доступ до Інтернету, електронна пошта, файлообмін, друкування тощо[4].

Завдяки гнучкій будові та можливості інтеграції різноманітних технологій та пристроїв, гетерогенні мережі можуть забезпечити високий рівень доступності, надійності та ефективності у взаємодії користувачів та ресурсів.

1.2 Протоколи і функції захисту канального рівня

Модель OSI є еталонною та має повну назву "Основна еталонна модель для взаємоз'єднання відкритих систем" (Basic Reference Model Open Systems Interconnection model). Вона складається з семи рівнів. Спочатку розглянемо

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

загальну інформацію про модель, а потім перейдемо до розгляду окремих аспектів.

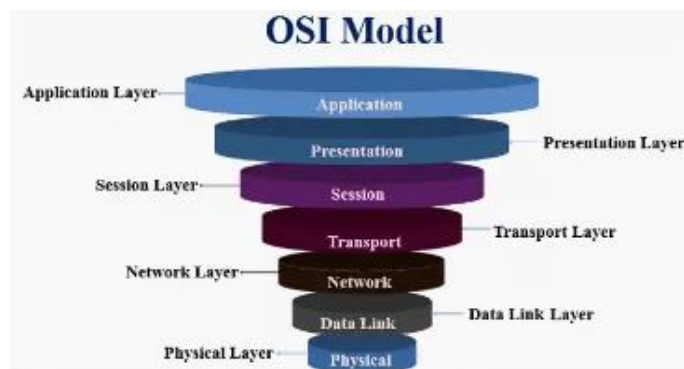


Рисунок 1.2 – Сім рівнів моделі OSI

Мережева модель OSI складається з семи рівнів, які розташовані ієрархічно від найвищого до найнижчого. Сьомий рівень є прикладним, а перший – фізичним.

У процесі передачі даних завжди беруть участь пристрій-відправник, пристрій-отримувач і самі дані, які необхідно передати та отримати. Для звичайного користувача це виглядає просто - потрібно відправити дані. Але всі процеси, які відбуваються під час передачі та отримання даних, детально описані семирівневою моделлю OSI.

На сьомому рівні інформація представлена у вигляді даних, а на першому у вигляді бітів. Процес, при якому інформація відправляється й перетворюється з даних на біти, називається інкапсуляцією. Зворотний процес, коли інформація, отримана у вигляді бітів на першому рівні, перетворюється на дані на сьомому рівні, називається декапсуляцією. На кожному з семи рівнів інформація представлена у вигляді блоків даних протоколу - PDU (Protocol Data Unit).

1-й рівень OSI - фізичний

На найнижчому рівні моделі OSI дані представлені у вигляді фізичних об'єктів - струму, світла або радіохвиль. Вони передаються через кабелі або за допомогою бездротових сигналів. Цей рівень працює з кабелями, контактами в роз'ємах, модуляцією сигналу, кодуванням одиниць та нулів та іншими

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

низькорівневими аспектами. По суті, перший рівень - це рівень дротів та фізичних методів передачі сигналу, з мінімальною абстракцією.

Найвідомішим протоколом фізичного рівня є Ethernet, який визначає, як сигнали кодуються і передаються через дроти. Крім Ethernet, існують також Bluetooth, Wi-Fi та ІЧ-порт, які містять інструкції для передачі даних.

2-й рівень OSI - каналний

Над фізичним рівнем знаходиться каналний рівень. Його завдання полягає в перевірці цілісності отриманих даних та виправленні помилок. Цей рівень є більш "розумним" порівняно з фізичним: він розуміє, що різні рівні напруги відповідають різним бітам, тобто нулям і одиницям. Крім того, каналний рівень здатний кодувати сигнали в біти і передавати їх далі.

Дані, отримані з фізичного рівня, діляться на фрейми або кадри. Кожен фрейм містить службову інформацію, наприклад, адреси відправника та одержувача, а також самі дані.

Лицьова сторона конверта - це MAC-адреса пристрою, який надіслав нам інформацію. Він потрібен, щоб ідентифікувати пристрої в локальній мережі, складається з 48 або 64 біт і виглядає приблизно так:

1d:85:25:11:b2:0a

Рисунок 1.3 – Запис MAC-адреси у шістнадцятковій системі числення

Канальний рівень не є таким простим - він поділяється на два підрівні:

- рівень керування логічним каналом (LLC - Logical Link Control);
- рівень керування доступом до середовища (MAC - Media Access Control).

Перший підрівень (LLC) необхідний для взаємодії з верхнім, мережевим рівнем, тоді як другий підрівень (MAC) забезпечує взаємодію з нижнім, фізичним рівнем. Пристрої каналного рівня, такі як комутатори та мости,

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

використовуються для передачі кадрів до відповідного адресата. До протоколів канального рівня належать PPP і CDP.

3-й рівень OSI – мережевий

Цей рівень відповідає за маршрутизацію даних у мережі між комп'ютерами. Тут вже з'являються такі терміни, як «маршрутизатори» та «IP-адреси».



Рисунок 1.4 – Маршрутизатор, який використовують Інтернет-провайдери

Маршрутизатори забезпечують комунікацію між різними мережами, використовуючи MAC-адреси для побудови маршруту від одного пристрою до іншого.

На мережному рівні дані представлені у формі пакетів, які схожі на кадри з канального рівня, але вони використовують інші адреси відправника та одержувача – IP-адреси.

Протокол ARP (Address Resolution Protocol) використовується для отримання IP-адреси обох пристроїв (відправника та одержувача). Він здатний конвертувати MAC-адреси в IP-адреси і навпаки.

4-й рівень OSI – транспортний

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

На цьому рівні мережі дійсно відбувається передача даних через мережу. Основні протоколи тут – TCP та UDP, які відповідають за те, як саме дані будуть передаватися.

TCP (Transmission Control Protocol) – це протокол, який гарантує доставку даних у коректному вигляді. Він дуже уважно стежить за кожним бітом інформації, але працює помітно повільніше за UDP.

Наприклад, при введенні логіна та пароля для входу в соціальну мережу дуже важливо, щоб всі символи досягли приймача в певній послідовності. Якщо які-небудь символи загубляться чи зміняться, авторизація може бути неможливою. Тому протокол TCP використовує різні методи перевірки, такі як контрольні суми, для забезпечення надійності передачі даних.

У протоколі TCP дані розбиваються на сегменти, кожен з яких є частиною пакету. Це допомагає передавати інформацію через мережу, враховуючи її пропускну здатність.

Наприклад, якщо ви передаєте дані з комп'ютера з пропускнуою здатністю 100 Мб/с на смартфон з пропускнуою здатністю 10 Мб/с, то дані будуть розділені так, щоб уникнути заторів у повільному пристрої.

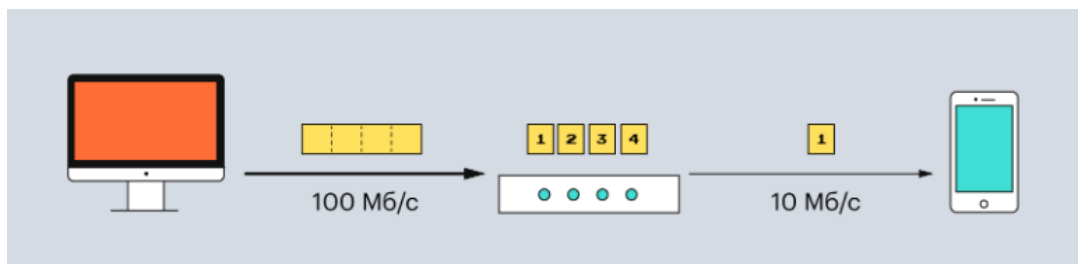


Рисунок 1.5 – Ось так дані поділяються на кілька сегментів, щоб протиснутися до мережі з пропускнуою здатністю 10 Мб/с

Сегментація є важливим аспектом для забезпечення надійності передачі даних. Розбиваючи великі пакети на менші сегменти, TCP знижує ризик втрати або помилкової доставки даних. Малі пакети також дозволяють відстежувати їх кількість і, у разі необхідності, запитувати невдалі сегменти від відправника ще раз, забезпечуючи таким чином надійність передачі.

У випадку UDP дані розділяються на датаграми, що подібне до пакетів, але автономні. Кожна датаграма містить усю необхідну інформацію для досягнення одержувача, тому вони не залежать від конкретної мережі та можуть бути доставлені різними маршрутами та в будь-якому порядку.

5-й рівень OSI – сеансовий

Починаючи з цього рівня і вище, дані вже мають звичайний вигляд, наприклад, знайомі нам файли у форматі JPEG або MP3. Мета мережі на цих рівнях – забезпечити представлення інформації у зрозумілій для людини формі і зробити її доступною для взаємодії користувача.

Сеансовий рівень керує з'єднаннями або сесіями. Типовим прикладом є виклик за допомогою Skype або Zoom. Коли ви телефонуєте іншій людині, між вашими комп'ютерами встановлюється з'єднання, через яке передаються аудіо та відео. Якщо це з'єднання буде розірвано, то ваш дзвінок перерветься.

На сеансовому рівні дуже важливо, щоб з'єднання було правильно встановлене і підтримувалось. Іншими словами, механізми протоколів повинні перевірити, що обидва співрозмовники мають потрібні кодеки і між пристроями присутній сигнал.

6-й рівень OSI – рівень подання даних

На рівні подання відбувається конвертування та зміна форматів даних, включаючи їх кодування та стиснення. Наприклад, отримані дані можуть бути перетворені у файл формату GIF або MP4. Цей процес також відбувається в зворотному напрямку, коли користувач надсилає файл іншій особі: дані спочатку конвертуються в біти, стискаються, а потім передаються на транспортний рівень.

Крім кодування та стиснення, на рівні подання дані можуть також шифруватися, якщо це необхідно.

7-й рівень OSI – прикладний

Останній рівень моделі OSI – це прикладний рівень. На цьому рівні розташовані мережеві служби, які допомагають користувачам без проблем переглядати інтернет.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

Прикладний рівень подібний до графічного інтерфейсу для всієї моделі OSI – він дозволяє користувачам взаємодіяти з іншими рівнями, навіть не усвідомлюючи цього. Цей інтерфейс називається мережевим[5].

Найпопулярніші з мережевих інтерфейсів включають HTTP, HTTPS, FTP та SMTP. А "пристрої" на цьому рівні це вже програми, такі як Zoom, Telegram, браузер.



Рисунок 1.6 – HTTP браузери запитують веб-сторінки та отримують у відповідь HTML-сторінки

Функції захисту на канальному рівні мережі включають:

- Контроль доступу до мережі (NAC): Визначення, які пристрої мають дозвіл на доступ до мережі на основі їхніх ідентифікаторів, наприклад, MAC-адреси.
- Керування ідентифікацією і аутентифікацією (IAM): Перевірка ідентичності користувачів і пристроїв, що намагаються отримати доступ до мережі, та перевірка їхніх прав доступу.
- Шифрування трафіку (VPN): Захист з'єднань між вузлами мережі шляхом застосування шифрування, щоб уникнути перехоплення інформації.
- Виявлення та запобігання атакам на мережевий рівень (IDS/IPS): Виявлення та блокування небажаних або зловмисних активностей, таких як спроби перехоплення даних або внесення змін до трафіку.
- Механізми захисту від втрати даних (L2TP): Захист від випадкової або навмисної втрати даних шляхом забезпечення їхнього надійного передавання через мережу.

Port Security.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

Port Security – це функція мережевих комутаторів, яка забезпечує захист портів від несанкціонованого доступу та підключення сторонніх пристроїв. Вона контролює і обмежує кількість MAC-адрес, які можуть використовувати конкретний порт на комутаторі.

Як працює Port Security:

❖ Налаштування кількості дозволених MAC-адрес:

Адміністратор мережі налаштовує максимальну кількість MAC-адрес, які можуть бути пов'язані з конкретним портом комутатора. Якщо ця кількість перевищується, комутатор може вжити заходів для захисту мережі.

❖ Динамічне навчання MAC-адрес:

Порт комутатора може динамічно вивчати MAC-адреси підключених пристроїв і зберігати їх у таблиці MAC-адрес. Це дозволяє контролювати, які пристрої підключені до порту.

❖ Статичне налаштування MAC-адрес:

Адміністратор може вручну налаштувати певні MAC-адреси, які дозволені на порту. Це забезпечує додатковий рівень безпеки, оскільки лише відомі і дозволені пристрої можуть підключатися.

Режими роботи Port Security:

- Protect: Перевищення кількості MAC-адрес просто ігнорується, нові MAC-адреси не вивчаються.
- Restrict: Перевищення кількості MAC-адрес блокує нові MAC-адреси і генерує повідомлення про помилку.
- Shutdown: Перевищення кількості MAC-адрес призводить до відключення порту, що вимагає втручання адміністратора для відновлення.

Повідомлення і логування:

При перевищенні дозволеної кількості MAC-адрес або спробі підключення несанкціонованого пристрою, комутатор може надсилати повідомлення адміністраторам та вести журнал подій для подальшого аналізу.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

Переваги використання Port Security:

- Підвищена безпека мережі: Запобігання несанкціонованим підключенням допомагає захистити мережу від внутрішніх загроз.
- Контроль доступу: Обмеження кількості MAC-адрес на порту дозволяє уникнути перевантаження і атак типу "MAC flooding".
- Простота налаштування: Інтерфейси управління комутаторами зазвичай пропонують зручні інструменти для налаштування Port Security.

Використання Port Security є важливим елементом у забезпеченні безпеки мережевої інфраструктури, особливо в організаціях з великою кількістю підключених пристроїв[6].

Dhcp snooping.

DHCP Snooping – це технологія безпеки рівня 2, призначена для захисту від атак з використанням протоколу DHCP. Наприклад, атаки з підменої DHCP-сервера в мережі або атаки DHCP starvation, які заставляють DHCP-сервер видаляти всі наявні на сервері адреси зломисника. DHCP Snooping передотворює несанкціоновані (мошенничні) DHCP-сервери, що пропонують IP-адресу DHCP-клієнтам. Функція DHCP Snooping виконує наступні дії:

- захистити клієнтів в мережі від отримання адреси від неавторизованого DHCP-сервера.
- регулювати які повідомлення протоколу DHCP відбрасувати, які перенаправляти і на які порти.

Для правильної роботи DHCP Snooping необхідно вказати, які порти комутатора будуть довіреними (довіреними), а які - нет (ненадійними, в подальшому - ненадежними):

- Ненадійні (Untrusted) – порти, до яких підключені клієнти. DHCP-відповіді, які надходять із цих портів відкидаються комутатором. Для ненадійних портів виконується ряд перевірок повідомлень DHCP і створюється база даних прив'язки DHCP (DHCP snooping binding database).

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

- Довірені (Trusted) – порти комутатора, до яких підключено інший комутатор або DHCP-сервер. DHCP-пакети, отримані з довірених портів, не відкидаються.

Як працює DHCP Snooping?

За замовчуванням комутатор відкидає DHCP-пакет, який прийшов на ненадійний порт, якщо:

- Надходить одне з повідомлень, що надсилає DHCP-сервер (DHCP OFFER, DHCP ACK, DHCP NAK або DHCP LEASE QUERY);
- Надходить повідомлення DHCP RELEASE або DHCP DECLINE, в якому міститься MAC-адреса з бази даних прив'язки DHCP, але інформація про інтерфейс у таблиці не збігається з інтерфейсом, на якому був отриманий пакет;
- У DHCP-пакеті, що прийшов, не збігаються MAC-адреса вказана в DHCP-запиті і MAC-адреса відправника;
- Надходить DHCP-пакет, в якому є опція 82.

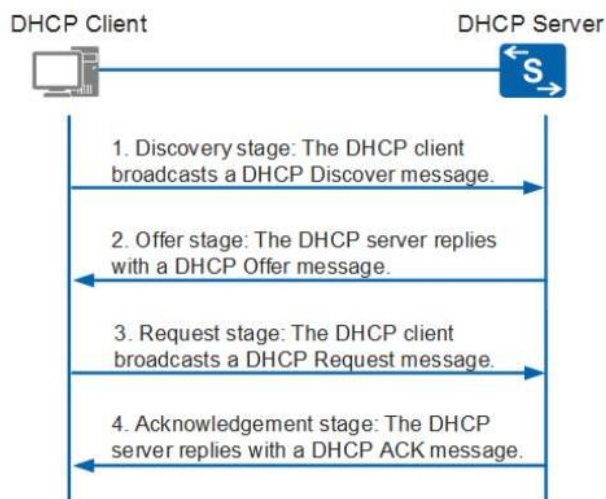


Рисунок 1.7 – Взаємодія з DHCP – сервером

DHCP Snooping зазвичай класифікує інтерфейси на комутаторі за двома категоріями: надійні ненадійні порти

Довірений порт – це порт або джерело, від якого повідомлення DHCP-сервера вважаються надійними. Ненадійний порт – це порт, від якого

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

повідомлення DHCP-сервера не є надійними. Коли активовано DHCP Snooping, повідомлення пропозиції DHCP можуть надсилатися тільки через довірені порти. Якщо ж вони надходять через ненадійні порти, то ці повідомлення будуть відкинуті.

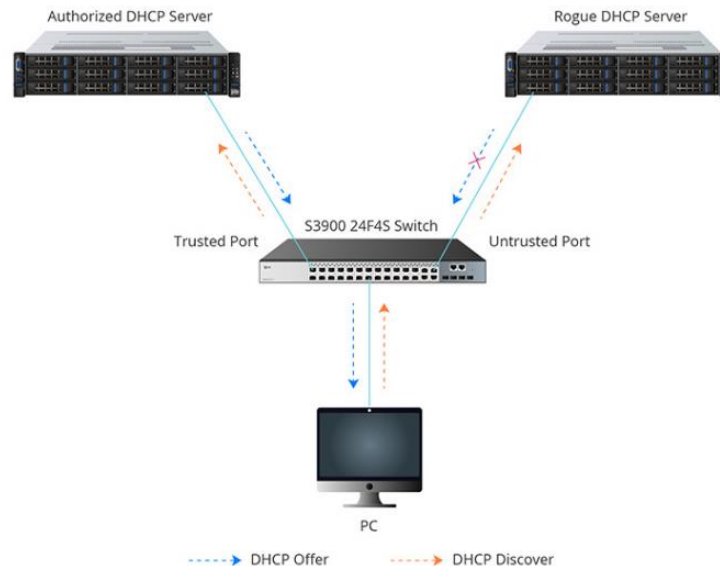


Рисунок 1.8 – Надійні та ненадійні проти

DHCP Snooping використовується тільки для провідних користувачів. Як функція безпеки рівня доступу, вона зазвичай активується на комутаторах, що мають порти доступу до VLAN, які використовують DHCP. При налаштуванні DHCP Snooping потрібно спочатку визначити довірені порти (порти, через які дозволені повідомлення DHCP-сервера), а потім увімкнути DHCP Snooping для відповідних VLAN, які необхідно захистити. Це можна зробити через інтерфейс командного рядка (CLI) або за допомогою веб-інтерфейсу[7].

BPDU guard і BPDU filter

У процесі проектування мережі важливо забезпечити надійну та ефективну топологію для підтримки безперебійної роботи та запобігання збоям. Spanning Tree Protocol (STP) є ключовою технологією в мережевій архітектурі, яка запобігає виникненню петель, що можуть призвести до мережових збоїв.

Для підвищення надійності STP використовуються інструменти BPDU Guard і BPDU Filter, які допомагають керувати блоками даних протоколу мосту

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

(BPDU) - повідомленнями, що обмінюються комутатори для підтримки топології STP.

Обидва інструменти, BPDU Guard і BPDU Filter, спрямовані на підвищення стабільності мережі, проте вони роблять це різними способами та підходять для різних мережевих умов.

BPDU Guard призначений для захисту мережі, негайно відключаючи порт, якщо він отримує BPDU. Це запобігає підключенню непередбачених або шкідливих пристроїв, які можуть порушити топологію STP.

BPDU Filter, з іншого боку, блокує передачу BPDU через порт, не беручи участі у топології STP. Це корисно в сценаріях, де необхідно запобігти участі певних портів у процесі обміну BPDU, зберігаючи при цьому їх роботу для інших мережевих функцій.

Операційні відмінності між BPDU Guard і BPDU Filter є суттєвими та вкрай важливими для розуміння мережевими інженерами під час впровадження заходів безпеки мережі. BPDU Guard має більш жорсткий підхід, забезпечуючи жорстке припинення потенційних проблем шляхом закриття портів, які отримують BPDU. Цей метод підходить для середовищ, де прийом BPDU означає явне порушення або помилку в конфігурації мережі.

На відміну від цього, фільтр BPDU пропонує більш гнучке рішення, запобігаючи надсиланню BPDU з порту або блокуючи вхідні BPDU. Це забезпечує більш плавну роботу в контрольованих середовищах, де топологія мережі є статичною, але де повна ізоляція від STP не потрібна.

Приклад 1: BPDU Guard у корпоративному середовищі

У великому корпоративному офісі BPDU Guard було розгорнуто на всіх комутаторах рівня доступу, підключених до робочих станцій співробітників. IT-відділ налаштував BPDU Guard для негайного відключення будь-якого порту, який отримав BPDU, ефективно запобігаючи потенційним збоям у мережі, спричиненим спробою несанкціонованого пристрою вплинути на топологію мережі.

Приклад 2: фільтр BPDU в центрі обробки даних

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

У середовищі центру обробки даних фільтр BPDU було застосовано до портів, що підключають сервери, які не беруть участь у STP. Завдяки фільтрації BPDU центр обробки даних гарантував, що порти сервера обходять процеси STP, зменшуючи затримку та покращуючи пропускну здатність даних, що є критичним у високопродуктивних обчислювальних середовищах.



Рисунок 1.9 – Порівняння BPDU Guard and BPDU Filter

Вибір між BPDU Guard і BPDU Filter залежить від кількох факторів, зокрема від розміру мережі, складності та конкретних вимог безпеки. Для мереж з високими потребами в безпеці та меншою складністю BPDU Guard може бути кращим вибором завдяки своїм простим заходам захисту. І навпаки, для мереж, де продуктивність є критичною, а зміни топології контролювані та мінімальні, фільтр BPDU може запропонувати необхідний баланс між безпекою та ефективністю.

Щоб ефективно застосувати ці інструменти, мережеві адміністратори повинні дотримуватися кількох найкращих практик:

- Уважно вивчіть компонування мережі перед впровадженням BPDU Guard або BPDU Filter.
- Регулярно оновлюйте та перевіряйте конфігурацію мережі, щоб уникнути випадкових збоїв.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

- Навчіть персонал наслідкам кожного налаштування та тому, як реагувати у випадку відключення портів або інших пов'язаних мережових подій[8].

1.3 Протокол резервування шлюзу VRRP

Virtual Router Redundancy Protocol (VRRP) є протоколом, який забезпечує автоматичне призначення доступного шлюзу для хостів у локальній мережі (LAN). Основна мета VRRP – підвищення доступності маршрутизаторів і запобігання збоїв у мережі через відмову шлюзу.

Основні характеристики VRRP

1 Резервування шлюзу:

- VRRP дозволяє створити групу маршрутизаторів, з яких один обирається головним (master), а інші - резервними (backup). Головний маршрутизатор відповідає за обробку трафіку, а резервні маршрутизатори чекають на випадок збою головного.

2 Простота налаштування:

- Хости налаштовуються на використання одного віртуального IP-адресу як шлюзу. VRRP керує перенаправленням цього IP-адресу до активного маршрутизатора в групі.

3 Підтримка безперебійної роботи:

- Якщо головний маршрутизатор стає недоступним, VRRP автоматично перенаправляє трафік до одного з резервних маршрутизаторів, мінімізуючи простой і забезпечуючи безперебійний доступ до мережових ресурсів.

Як працює VRRP

1 Група VRRP:

- Кожна група VRRP складається з одного віртуального IP-адресу та кількох маршрутизаторів, що належать до цієї групи.

2 Обрання головного маршрутизатора:

- Маршрутизатор з найвищим пріоритетом (за замовчуванням 100) стає головним. Пріоритет можна налаштувати, щоб визначити, який

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

маршрутизатор буде головним. У разі однакового пріоритету використовується IP-адреса як додатковий критерій.

3 Обмін повідомленнями:

- Головний маршрутизатор періодично надсилає повідомлення VRRP (advertisements) для інформування резервних маршрутизаторів про свій статус. Якщо резервний маршрутизатор не отримує ці повідомлення протягом певного часу (timeout), він вважає, що головний маршрутизатор недоступний, і бере на себе його роль.

4 Перенаправлення IP-адреси:

- Коли резервний маршрутизатор стає головним, він починає відповідати на ARP-запити для віртуального IP-адресу, перенаправляючи трафік через себе.

Преимущества VRRP

- Висока доступність: Автоматичне перемикання між маршрутизаторами забезпечує постійний доступ до мережі.
- Легкість налаштування: Віртуальний IP-адресу використовується як шлюз, що спрощує конфігурацію хостів.
- Гнучкість: Пріоритети можна налаштовувати, що дозволяє контролювати, який маршрутизатор буде головним.

VRRP є ефективним рішенням для підвищення надійності та безперебійності роботи мереж. Завдяки простоті налаштування та автоматичному перемиканню між маршрутизаторами, VRRP забезпечує високу доступність мережевих ресурсів, що є критичним для багатьох організацій.

Протокол VRRP (Virtual Router Redundancy Protocol) підтримує кілька способів автентифікації, які допомагають забезпечити безпеку обміну повідомленнями між маршрутизаторами в одній VRRP-групі. Ось основні способи автентифікації, які використовуються в VRRP:

1. Без автентифікації (No Authentication):

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

- У цьому режимі автентифікація взагалі не використовується. Це найпростіший і найменш безпечний варіант, оскільки повідомлення VRRP надсилаються і приймаються без будь-якої перевірки.

2. Проста текстова автентифікація (Simple Text Authentication):

- У цьому режимі використовується простий текстовий пароль для автентифікації повідомлень VRRP. Пароль передається у кожному VRRP-повідомленні у вигляді відкритого тексту.

- Основний недолік цього методу полягає в тому, що пароль передається незашифрованим, що робить його вразливим до перехоплення.

3. Автентифікація за допомогою MD5 (MD5 Authentication):

- Це більш безпечний метод автентифікації, в якому використовується алгоритм MD5 для створення хешу повідомлення. Хеш додається до кожного VRRP-повідомлення, що дозволяє маршрутизаторам перевіряти його автентичність.

- MD5 забезпечує більш високий рівень безпеки, оскільки хешування дозволяє перевірити цілісність повідомлення і переконатися, що воно не було змінено під час передачі.

Вибір методу автентифікації залежить від вимог до безпеки мережі та конкретних умов її експлуатації:

- Внутрішні мережі: У мережах, де безпека не є критичною, можна використовувати просту текстову автентифікацію або навіть обходитися без автентифікації.

- Зовнішні мережі або мережі з високими вимогами до безпеки: Рекомендується використовувати автентифікацію MD5 для забезпечення цілісності та автентичності повідомлень VRRP.

Забезпечення правильного налаштування автентифікації допомагає захистити мережу від потенційних атак і підвищує загальну надійність та безпеку мережевої інфраструктури[9].

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

1.4 Стандарт відправки і реєстрації подій Syslog

Syslog – це стандарт для обміну повідомленнями журналу в мережі комп'ютерів. Його використовують для збору різних видів логів та системних повідомлень з пристроїв і додатків. Ось основна інформація про Syslog:

- Syslog клієнт (або агент): Програма, яка генерує та надсилає повідомлення до Syslog сервера. Це можуть бути різні мережеві пристрої (маршрутизатори, комутатори), сервери, додатки і операційні системи.
- Syslog сервер (або демони): Програма, яка приймає повідомлення від Syslog клієнтів, зберігає їх у файл журналу або виконує інші дії з повідомленнями.
- Syslog повідомлення: Повідомлення, які містять інформацію про події, що відбуваються в системі або мережі.

Syslog повідомлення складається з кількох частин:

- PRI (Пріоритет): Визначає серйозність повідомлення та його об'єкт. Обчислюється як $8 * facility + severity$, де:
 - Facility: Вказує на тип програми або підсистеми, яка генерує повідомлення (напр., ядро, поштова система).
 - Severity: Вказує на рівень важливості події (від emergency до debug).
- HEADER (Заголовок): Містить позначку часу та ім'я хоста, з якого було відправлено повідомлення.
- MSG (Повідомлення): Містить власне текст повідомлення. Це може бути короткий опис події або більш детальна інформація про помилку.

Syslog визначає вісім рівнів важливості подій:

1. Emergency (0): Система непрацездатна.
2. Alert (1): Негайна дія необхідна.
3. Critical (2): Критичні умови.
4. Error (3): Помилки.
5. Warning (4): Попередження.
6. Notice (5): Повідомлення (нормальні, але значущі умови).
7. Informational (6): Інформаційні повідомлення.
8. Debug (7): Повідомлення для налагодження

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Syslog повідомлення передаються по мережі за допомогою протоколу UDP (порт 514), але також можуть використовувати TCP для забезпечення більшої надійності. Використання TCP або шифрування TLS може бути необхідним для підвищення безпеки передачі даних.

- Збір логів: Збирає журнали подій з різних пристроїв і додатків в централізоване місце для подальшого аналізу.
- Моніторинг: Використовується для моніторингу стану мережі та системи, виявлення проблем та інцидентів безпеки.
- Аналіз: Аналіз логів допомагає виявити проблеми в роботі системи, діагностувати збої та вживати необхідних заходів.
- Аудит: Журнали подій зберігають історію подій, що може бути корисним для аудиту та дотримання нормативних вимог.

Переваги Syslog

- Централізація логів: Полегшує керування логами з багатьох джерел.
- Масштабованість: Підтримує велику кількість пристроїв і додатків.
- Гнучкість: Легко налаштовується для збору потрібних даних.
- Стандартизація: Широко використовується стандарт, підтримуваний багатьма пристроями та програмами.

Недоліки Syslog

- Безпека: Передача логів по UDP не шифрується, що може бути ризиком для безпеки.
- Надійність: Використання UDP не гарантує доставку повідомлень, хоча TCP і TLS можуть вирішити цю проблему.
- Складність аналізу: Велика кількість логів може ускладнювати аналіз без спеціальних інструментів.

Syslog є важливим інструментом для адміністраторів мереж та систем, що дозволяє ефективно управляти логами та забезпечувати надійну роботу інфраструктури[10].

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

1.5 Протокол аутентифікації та авторизації Radius

RADIUS, що розшифровується як Remote Authentication Dial In User Service, є мережевим протоколом, який надає централізовані послуги з автентифікації, авторизації та обліку використання мережевих ресурсів. В англійській літературі ці три функції відомі під аббревіатурою AAA (Authentication, Authorization, Accounting).

Аутентифікація – це процес, який дозволяє ідентифікувати користувача за його даними, такими як логін (ім'я користувача, номер телефону тощо) та пароль.

Авторизація – це процес, під час якого визначаються повноваження ідентифікованого користувача на доступ до певних мережевих ресурсів.

Облік використаних мережевих ресурсів - термін, який сам по собі досить інформативний. Основними даними, що передаються за протоколом RADIUS, є обсяги вхідного та вихідного трафіку при передачі даних, а також тривалість розмови та набраний номер при використанні IP-телефонії. Окрім стандартних атрибутів (параметрів), визначених у протоколі, RADIUS також дозволяє виробникам обладнання використовувати власні атрибути, які в англійській літературі називаються Vendor Specific Attributes або VSA.

Наразі протокол RADIUS застосовується для забезпечення доступу до віртуальних приватних мереж (VPN), бездротових точок доступу (Wi-Fi), Ethernet комутаторів, DSL та інших типів мережевого доступу. Завдяки своїй відкритості, легкості впровадження та постійному вдосконаленню, RADIUS фактично став стандартом для віддаленої аутентифікації.

Аутентифікація та авторизація

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

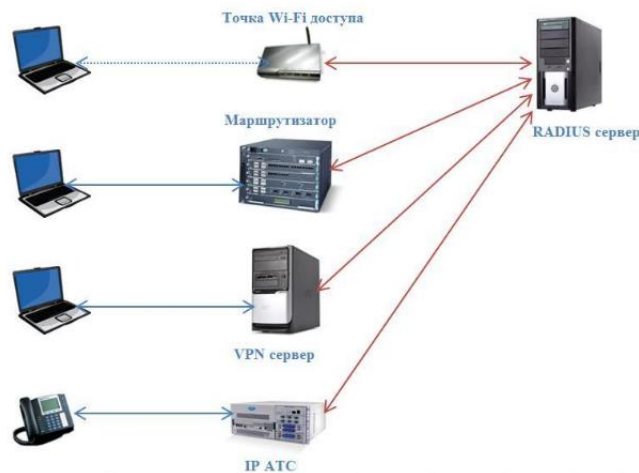


Рисунок 1.10 – Можливі варіанти NAS

Протокол RADIUS функціонує через інтерфейс між NAS, який діє як RADIUS клієнт, і RADIUS сервером – програмним забезпеченням, яке може бути встановлене на комп'ютері (сервері) або спеціалізованому пристрої. Отже, RADIUS сервер зазвичай не контактує безпосередньо з пристроєм користувача, а здійснює взаємодію через мережевий сервер доступу.

Користувач надсилає запит на мережевий сервер доступу для отримання доступу до певного мережевого ресурсу, використовуючи сертифікат доступу. Сертифікат надсилається на мережевий сервер доступу через протокол канального рівня, наприклад, Point-to-Point Protocol (PPP) у випадку комутованого доступу, або Digital Subscriber Line (DSL) у разі використання відповідних модемів тощо. Після цього NAS надсилає повідомлення запиту доступу на RADIUS сервер, яке називається RADIUS Access Request. Цей запит включає сертифікати доступу, які зазвичай представлені у вигляді імені користувача і пароля або сертифіката безпеки, отриманих від користувача. Крім того, запит може містити додаткові параметри, такі як мережеву адресу пристрою користувача, його телефонний номер, інформацію про фізичну адресу, з якої користувач взаємодіє з NAS.

RADIUS сервер перевіряє цю інформацію на коректність, використовуючи такі схеми автентифікації як PAP, CHAP та інші.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

PAP (Password Authentication Protocol) - це простий протокол аутентифікації, який застосовується для перевірки користувача на мережевому сервері доступу (NAS). PAP використовується протоколом PPP і підтримується майже всіма серверами доступу. Він передає незашифрований пароль через мережу, тому не забезпечує захисту. Зазвичай PAP застосовують, коли сервер не підтримує захищені протоколи, такі як CHAP, EAP тощо[11].

CHAP (Challenge Handshake Authentication Protocol) - широко поширений алгоритм автентифікації, що передбачає передачу не самого пароля користувача, а непрямих відомостей про нього. У разі використання CHAP сервер віддаленого доступу надсилає клієнтові рядок запиту. На основі цього рядка та пароля користувача клієнт обчислює хеш-код MD5 (Message Digest-5) та передає його серверу. Хеш-функція є алгоритмом одностороннього (необоротного) шифрування, оскільки значення хеш-функції для блоку даних легко обчислити, а визначити вихідний блок з хеш-коду з математичної точки зору неможливо за прийнятний час.

Протокол EAP (Extensible Authentication Protocol) (RFC 3748) забезпечує аутентифікацію для віддалених підключень, використовуючи різноманітні механізми перевірки. Точний метод аутентифікації погоджується між клієнтом віддаленого доступу та сервером, що виконує аутентифікацію (це може бути сервер віддаленого доступу або RADIUS сервер). За замовчуванням підтримуються протоколи EAP-TLS і MD5-Challenge (MD5-завдання). Додавання інших модулів EAP до сервера, що використовує маршрутизацію та віддалений доступ, дозволяє підтримувати додаткові методи EAP.

Сервер перевіряє ідентичність користувача, а також коректність додаткової інформації, яка може міститися у запиті: мережна адреса пристрою користувача, телефонний номер, стан рахунку, його привілеї при доступі до запитуваного мережного ресурсу.

За результатами перевірки RADIUS сервер надсилає NAS один із трьох типів відгуків:

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Access-Reject означає, що запит користувача є невірним. Сервер може додати текстове повідомлення до Access-Reject, яке може бути передане користувачу через клієнта. Інші атрибути (крім Proxy-State) не дозволені в Access-Reject.

Access-Challenge запитує додаткову інформацію від користувача, наприклад, другий пароль, PIN-код або номер картки. Ця відповідь також використовується для більш детального аутентифікаційного діалогу, коли захищений тунель встановлюється між пристроєм користувача та RADIUS сервером, щоб приховати сертифікати доступу від NAS.

Access-Accept означає, що користувач отримав дозвіл на доступ. Після аутентифікації RADIUS сервер перевіряє авторизацію на використання запитуваних ресурсів. Наприклад, користувачу може бути дозволено доступ через бездротову мережу, але заборонено підключення до VPN мережі[12].

1.6 Міжмережевий екран

Міжмережевий екран, брандмауер і файрвол – це терміни, що означають одне й те саме, але походять з різних мов. Вони представляють собою комбінацію апаратних та програмних засобів, які служать для фільтрації вхідного та вихідного трафіку, а також для захисту даних. Основною функцією міжмережевого екрану є фільтрація трафіку, що дозволяє забезпечити безпеку інформації.

Хакери постійно розробляють нові методи крадіжки персональних даних, а віруси поширюються все частіше. Це змушує організації шукати ефективніші методи захисту від кіберзагроз. У цьому контексті міжмережеві екрани стають все популярнішими.

Без брандмауера будь-який комп'ютер, підключений до Інтернету, швидко піддався б атакам вірусів і перестав би працювати. Локальна мережа великої компанії ще більш вразлива: якщо один комп'ютер заражається, вірус швидко поширюється на інші пристрої, що може паралізувати роботу всієї компанії, спричинити втрату даних і фінансові збитки.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

Міжмережевий екран є обов'язковим елементом у мережевій інфраструктурі будь-якого підприємства. Однією з його важливих функцій є захист від витоку конфіденційної інформації. Крім захисту, міжмережеві екрани також можуть вести журнал усіх подій і підозрілої активності, що відбувається в мережі.

Стандартні можливості Firewall:

- Фільтрація трафіку, блокування процесів, які вимагають доступ до системних або незахищених служб;
- Запобігання спробам несанкціонованого доступу до конфіденційної інформації та блокування спроб передачі захищених даних;
- Контроль доступу до пристроїв та портів мережі;
- Логування всіх мережевих активностей та ведення статистики;
- Видача повідомлень у разі виявлення підозрілих активностей та атак на мережу.

Одного міжмережевого екрану зазвичай недостатньо для забезпечення повного захисту від вірусів. Найкращу ефективність можна досягти, використовуючи його разом з іншими захисними програмними засобами, такими як антивірусні програми. Технології злому і перехоплення інформації розвиваються швидше, ніж засоби захисту, тому комплексний підхід до безпеки є найбільш надійним.

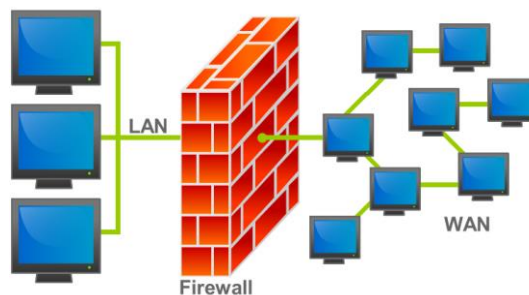


Рисунок 1.11 – Приклад міжмережевого екрану.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

Висновки до першого розділу:

У цьому розділі було розглянуто основні аспекти побудови і функціонування гетерогенних мереж, зокрема, різні протоколи і функції захисту, які застосовуються на канальному рівні. Обговорено такі важливі механізми безпеки, як Port Security, DHCP snooping, BPDU guard і BPDU filter, які забезпечують захист від різноманітних загроз і аномалій у мережевому трафіку. Також було розглянуто протокол резервування шлюзу VRRP, який підвищує надійність і доступність мережі, стандарт відправки і реєстрації подій Syslog, що дозволяє централізовано збирати і аналізувати логи, та протокол аутентифікації і авторизації Radius, який забезпечує надійний контроль доступу до мережевих ресурсів. Окремо було приділено увагу міжмережевим екранам, які є ключовими елементами захисту мережі від зовнішніх загроз. Всі ці компоненти разом утворюють комплексну систему захисту гетерогенної мережі, що дозволяє забезпечити її надійність і безпеку[1].

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

РОЗДІЛ 2. ТОПОЛОГІЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ

2.1 Побудова топології мережі

Успішна реалізація підсистеми захисту гетерогенної мережі організації починається з правильної побудови її топології. Топологія мережі визначає, як різні пристрої і сегменти мережі з'єднуються і взаємодіють один з одним. Для гетерогенних мереж, які включають різні типи пристроїв і операційних систем, особливо важливо мати добре сплановану топологію, яка забезпечує високу продуктивність, масштабованість і, головне, безпеку.

У цій роботі було розглянуто гетерогенну мережу, в якій буде використано 2 маршрутизатора: Mikrotik-1 та Mikrotik-2. Також будуть задіяні комутатори SW-1 та SW-4. Робочі станції будуть підключені до комутаторів SW – 3 і SW – 4. В даній мережі налаштовано доступ до Інтернет. На мережевих пристроях налаштовано синхронізацію часу через NTP, відправку даних про події з використанням Syslog та аутентифікацію з використанням Radius. На Windows Server буде налаштовано AD, DHCP-сервер, DNS-сервер, NTP-сервер, Syslog-сервер, Radius-сервер.

Інтернет-з'єднання забезпечує доступ до зовнішніх ресурсів і дозволяє організації взаємодіяти з партнерами, клієнтами та іншими зовнішніми суб'єктами. Підключення до Інтернету також є критичним для отримання оновлень безпеки і доступу до хмарних сервісів.

Робочі станції і сервери включають: Ubuntu, яка використовується на робочих станціях для завдань, які потребують стабільної та безпечної ОС з відкритим вихідним кодом; Windows 7, яка використовується на старих робочих станціях, що забезпечують продуктивність для певних додатків; Windows 10, яка є основною ОС для сучасних робочих станцій і забезпечує підтримку нових програм і сервісів; Windows Server, який використовується для централізованого управління мережею, зберігання даних, управління доступом і надання інших серверних функцій.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

Трирівнева топологія мережі складається з трьох основних рівнів: рівень доступу, рівень розподілу та рівень ядра. Кожен рівень виконує свою роль у забезпеченні ефективного і безпечного функціонування мережі.

Рівень доступу забезпечує підключення кінцевих пристроїв, таких як робочі станції, принтери та інші периферійні пристрої, до мережі. На цьому рівні використовуються комутатори Cisco. Основні завдання рівня доступу включають забезпечення фізичного підключення пристроїв, а також первинну обробку даних, таких як перевірка доступу та базова фільтрація трафіку. Рівень доступу також відповідає за надання базових мережевих сервісів, таких як VLAN, для сегментації мережі і підвищення безпеки.

Рівень розподілу є проміжним рівнем між рівнем доступу і рівнем ядра. Він забезпечує агрегацію трафіку, який надходить з рівня доступу, і його маршрутизацію до рівня ядра. На цьому рівні використовуються маршрутизатори MikroTik. Основні завдання рівня розподілу включають політику безпеки, такі як фільтрація трафіку за допомогою списків контролю доступу (ACL), маршрутизація між VLAN, а також забезпечення якості обслуговування (QoS) для критичних застосувань і сервісів. Рівень розподілу також відповідає за агрегацію трафіку і забезпечення надійності мережі за рахунок використання механізмів резервування і відмовостійкості.

Рівень ядра є основою мережі і відповідає за швидку та ефективну маршрутизацію трафіку між різними сегментами мережі. На цьому рівні використовуються потужні маршрутизатори, такі як MikroTik, які забезпечують високу продуктивність і надійність. Основні завдання рівня ядра включають маршрутизацію трафіку на великі відстані, забезпечення високої швидкості передачі даних і мінімальної затримки. Рівень ядра також відповідає за забезпечення відмовостійкості і безперебійної роботи мережі, використовуючи механізми резервування і балансування навантаження.

При проектуванні було використано трьохрівневу модель мережі. Ця модель має ієрархічну структуру і передбачає, що мережа має три залежних один

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

від одного рівні, це рівень ядра, рівень розподілу та рівень доступу, ця мережа представлена на рисунку нижче.

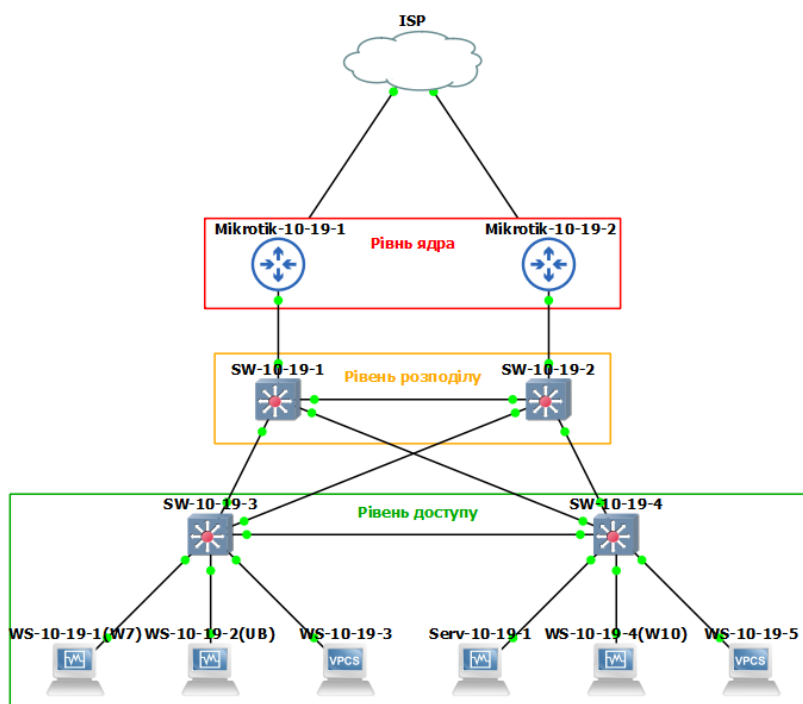


Рисунок 2.1 – Загальна топологія мережі

Рівень ядра складається з 2 маршрутизаторів Mikrotik, які з'єднані з ISP (англ. Internet Service Provider)

Рівень розподілу має 2 комутатори, що під'єднані до ядра мережі. З'єднання до ядра використано за допомогою технології Ethernet.

Рівень доступу має 2 комутатори, та підключені робочі станції, вони з'єднані між собою канальними зв'язками технології Ethernet.

2.2 Вибір обладнання

Мережа розроблена на обладнанні Cisco та Mikrotik. Нижче наведено характеристики обладнання, що буде використано в мережі.

MikroTik RouterBOARD 3011UiAS-RM – це високопродуктивний маршрутизатор серії RouterBOARD, який пропонує широкий спектр функцій для побудови складних мережеских рішень. Цей маршрутизатор підходить для використання як у малих і середніх бізнесах, так і в корпоративних мережах.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Пристрій оснащений процесором IPQ-8064 з архітектурою ARM 32bit, що має два ядра з частотою 1.4 ГГц. Оперативна пам'ять становить 1 ГБ, а зберігання даних реалізовано через 128 МБ NAND. Маршрутизатор має десять гігабітних Ethernet портів для швидкісного підключення та один SFP порт для підключення оптоволоконних модулів. Для підключення зовнішніх пристроїв передбачений USB 3.0 порт, а також слот для microSD карт для додаткового зберігання. Є серійний RJ45 консольний порт. Розмір пристрою становить 443 x 92 x 44 мм, що дозволяє встановлювати його в стандартну 19-дюймову стійку.

Живлення маршрутизатора здійснюється через 24V 1.5A адаптер, який входить в комплект. Підтримується вхідний PoE (Power over Ethernet) на портах 1-5 з напругою 18-57V. Максимальне споживання потужності пристрою становить 10 Вт.

MikroTik RouterBOARD 3011UiAS-RM підтримує широкий спектр мережевих протоколів і функцій. Серед них підтримка статичної та динамічної маршрутизації (OSPF, BGP, RIP), фільтрація пакетів, NAT, захист від DDoS атак. Для забезпечення безпечного з'єднання використовується підтримка різних типів VPN (PPTP, L2TP, IPSec, OpenVPN, GRE тунелі). Для управління трафіком передбачено пріоритезацію, управління пропускнуою здатністю і QoS. Підтримується також Hotspot сервер. Для мережевого моніторингу використовуються SNMP, NetFlow, sFlow, RADIUS. Додаткові функції включають DHCP сервер, DNS кешування, NTP клієнт/сервер і підтримку IPv6.

Пристрій працює на операційній системі RouterOS з ліцензією рівня 5, що забезпечує широкий спектр функцій та інструментів для управління і налаштування мережі. Управління маршрутизатором можна здійснювати через графічний інтерфейс Winbox, веб-інтерфейс Webfig або командний рядок (CLI).

MikroTik RB3011UiAS-RM ідеально підходить для створення центрального маршрутизатора в мережах малого та середнього бізнесу, корпоративних мереж із високими вимогами до продуктивності та безпеки, побудови надійних VPN-з'єднань між офісами, забезпечення гігабітного підключення до інтернету та внутрішньої мережі.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

Підключення до мережі здійснюється через Ethernet кабелі, підключені до гігабітних портів, або через SFP порт для оптоволоконного підключення. Живлення забезпечується адаптером або через PoE на портах 1-5. Для налаштування мережевих інтерфейсів, маршрутизації, брандмауера та інших функцій можна використовувати Winbox, Webfig або CLI.

MikroTik RouterBOARD 3011UiAS-RM – це потужний і гнучкий маршрутизатор, що забезпечує високу продуктивність і надійність, що робить його ідеальним вибором для різноманітних мережевих сценаріїв. Цей пристрій може легко впоратися з вимогами як невеликих офісних мереж, так і складних корпоративних інфраструктур[2].



Рисунок 2.2 – Високопродуктивний маршрутизатор RouterBOARD 3011UiAS

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

Таблиця 2.1

Характеристика маршрутизатора Mikrotik RouterBOARD 3011UiAS

Система	
Процесор:	IPQ-8064-0-519FCBGA-TR-01-0 dual core 1.4 GHz
RAM:	1 GB
Роз'єми:	10 × 10/100/1000 Mbit/s Ethernet RJ45 Auto-MDI/X 1 × SFP cage Gigabit Ethernet (Mini-GBIC; SFP модуль не поставляється) 1 × USB 3.0 type A 1 × Serial port RJ45
ОС:	MikroTik RouterOS Level 5
Інше	
Електроживлення:	Jack 10-30V DC; PoE in: 10-30V DC on Ether1 (Passive POE) PoE out: 24V 0.5A DC on Ether10 (Passive POE)
Споживання:	до 10 Вт
Розміри:	443 × 92 × 44 мм
Вага:	
Робоча температура:	від -30°C до +70°C

2. Комутатор Cisco WS-C2960-24-S

Cisco Catalyst WS-C2960-24-S – це модель комутатора серії Cisco Catalyst 2960, що призначена для забезпечення високої продуктивності та надійності в мережах малих і середніх підприємств, а також для побудови корпоративних мереж. Цей комутатор пропонує базові можливості для комутації на рівні 2

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

(Layer 2) і забезпечує необхідні функції для побудови ефективної та безпечної мережевої інфраструктури.

Cisco WS-C2960-24-S оснащений 24 портами Fast Ethernet (10/100 Мбіт/с), що забезпечують підключення пристроїв на швидкості 100 Мбіт/с. Додатково, комутатор має два комбіновані порти 10/100/1000 Ethernet або SFP (Small Form-Factor Pluggable), що дозволяють підключати гігабітні Ethernet кабелі або оптичні модулі для гігабітних з'єднань. Комутатор оснащений процесором з частотою 266 МГц і оперативною пам'яттю об'ємом 64 МБ DRAM, а також 32 МБ флеш-пам'яті для зберігання конфігурацій та операційної системи. Загальна пропускна здатність комутатора становить 16.8 Гбіт/с, а продуктивність досягає 6.6 мільйонів пакетів в секунду (pps).

Cisco WS-C2960-24-S має вбудований блок живлення з можливістю підключення до мережі змінного струму (AC) з напругою 100-240V. Споживана потужність комутатора становить приблизно 30 Вт. Розміри пристрою – 44.5 x 24.1 x 4.5 см (Ш x Г x В), вага – приблизно 3.6 кг.

Комутатор Cisco WS-C2960-24-S підтримує різноманітні мережеві протоколи і функції, що забезпечують надійну роботу і управління мережею. Серед них: підтримка до 255 VLAN (Virtual Local Area Network), що дозволяє сегментувати мережу для підвищення безпеки і управління трафіком; підтримка стандартного STP (Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol) і MSTP (Multiple Spanning Tree Protocol) для запобігання петель у мережі; функції управління пріоритетами трафіку (QoS – Quality of Service), що дозволяють оптимізувати роботу критично важливих додатків; функції безпеки, такі як ACL (Access Control Lists) для фільтрації трафіку, захист портів (Port Security), підтримка 802.1X для контролю доступу до мережі; мережевий моніторинг за допомогою SNMP (Simple Network Management Protocol), RMON (Remote Monitoring) і Syslog для моніторингу та управління мережею.

Cisco WS-C2960-24-S працює на базі операційної системи Cisco IOS, що забезпечує широкий спектр функцій для управління комутатором і налаштування мережі. Управління комутатором може здійснюватися через

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

командний рядок (CLI), веб-інтерфейс або засоби віддаленого управління, такі як Telnet або SSH. Комутатор також підтримує протокол Cisco Network Assistant (CNA) для централізованого управління і моніторингу.

Cisco WS-C2960-24-S є ідеальним вибором для мереж малих і середніх підприємств, де потрібна надійна і продуктивна комутація на рівні 2. Цей комутатор може використовуватися для підключення робочих станцій, серверів та інших мережевих пристроїв, забезпечуючи високу швидкість і надійність з'єднань. Він також підходить для побудови корпоративних мереж з високими вимогами до безпеки і управління трафіком. Підключення до мережі здійснюється через Fast Ethernet порти, а для гігабітних з'єднань можна використовувати комбіновані порти 10/100/1000 Ethernet або SFP. Живлення забезпечується через вбудований блок живлення, який підключається до мережі змінного струму[3].



Рисунок 2.3 – Комутатор Cisco WS-C2960-24-S

В ролі кінцевих робочих станцій будуть використовувати комп'ютери з ОС Windows 7, Windows 10, Ubuntu ці станції будуть працювати з мінімальними параметрами: 4-ядерний проц, 8ГБ ОЗУ, 256 ГБ HDD або SSD, мережевий інтерфейс 100Mbit. А в ролі сервера використовуватиметься комп'ютер з ОС Windows Server 2019 станція буде працювати мінімальними технічними параметрами: 8-ядерний проц, 16ГБ ОЗУ, 512 ГБ або більше HDD або SSD, мережевий інтерфейс 1000Mbit.

2.3. Розробка схеми адресації мережі

Розробка схеми адресації мережі є важливим аспектом при побудові гетерогенної мережі організації. Вона забезпечує унікальність кожного

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

пристрою в мережі, сприяє ефективному маршрутизації та управлінню мережевими ресурсами. В даному розділі буде розглянуто процес розробки схеми адресації мережі для організації, що включає різні типи пристроїв та операційних систем.

Адресація в мережі заснована на використанні IP-адрес. Існують два основні типи IP-адрес: IPv4 і IPv6. У нашій мережі буде використовуватися схема адресації IPv4, оскільки вона залишається більш поширеною і сумісною з більшістю обладнання та програмного забезпечення. Кожна IP-адреса складається з двох частин: мережевої частини і частини хоста. Маска підмережі визначає, яка частина адреси відноситься до мережі, а яка до хоста.

Для забезпечення ефективного управління та безпеки мережі необхідно розподілити IP-адреси між різними сегментами мережі. Основні сегменти включають: сервери, робочі станції, мережеве обладнання та гостьову мережу.

Для різних типів пристроїв використовуються різні методи призначення IP-адрес:

- Статична адресація: використовується для серверів, маршрутизаторів і комутаторів. Це забезпечує стабільність і прогнозованість адрес.
- Динамічна адресація: використовується для робочих станцій і гостьових пристроїв. Для цього використовується DHCP-сервер, який автоматично призначає IP-адреси з визначеного діапазону.

DHCP-сервер автоматично призначає IP-адреси пристроям у мережі. Він використовується для динамічної адресації робочих станцій і гостьових пристроїв. Налаштування DHCP-сервера включає визначення діапазону IP-адрес, які можуть бути виділені, а також інших параметрів мережі, таких як шлюз і DNS-сервери.

Після розробки схеми адресації необхідно налаштувати маршрутизатори і комутатори для підтримки розподілу адрес і маршрутизації трафіку між сегментами. Важливо також налаштувати політики безпеки, такі як фільтрація

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

трафіку і контроль доступу, для захисту мережі від несанкціонованого доступу і зловмисних дій.

Розробка схеми адресації мережі є важливим кроком у побудові надійної і безпечної гетерогенної мережі організації. Правильне планування і сегментація мережі дозволяють ефективно керувати ресурсами, забезпечують високу продуктивність і підвищують рівень безпеки. Використання статичної і динамічної адресації дозволяє гнучко керувати підключеннями і забезпечувати стабільну роботу критичних сервісів і пристроїв.

Для зв'язку між Mikrotik-1 та Mikrotik-2 з ISP використовується динамічна адресація зважаючи на отримані параметри від ISP.

Для локальної мережі буде залучено 1 адресу: 192.168.19.0/24

Маршрутизатори Mikrotik-1 та Mikrotik-2 будуть додані до групи резервування VRRP з метою покращення відмовостійкості мережі.

Таблиця 2.2

Параметри підключення пристроїв

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейса
ISP	Eth 0/0	Mikrotik-10-19-1	Eth 0
	Eth 0/1	Mikrotik-10-19-2	Eth 0
Маршрутизатор Mikrotik-10-19-1	Eth 0	ISP	Eth 0/0
	Eth 1	SW-10-19-1	Eth 3/3
Маршрутизатор Mikrotik-10-19-2	Eth 0	ISP	Eth 0/1
	Eth 1	SW-10-19-2	Eth 3/3
Комутатор SW-10-19-1	Eth 0/0	SW-10-19-3	Eth 3/3
	Eth 0/1	SW-10-19-4	Eth 3/2
	Eth 0/2	SW-10-19-2	Eth 0/2
	Eth 0/3	Mikrotik-10-19-1	Eth 3/3
Комутатор SW-10-19-2	Eth 0/0	SW-10-19-4	Eth 3/3
	Eth 0/1	SW-10-19-3	Eth 3/2
	Eth 0/2	SW-10-19-1	Eth 0/2
	Eth 0/3	Mikrotik-10-19-2	Eth 3/3

Параметри підключення пристроїв

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейса
Комутатор SW-10-19-3	Eth 0/1	Робоча станція WS-10-19-1	Eth 0
	Eth 0/2	Робоча станція WS-10-19-2	Eth 0
	Eth 0/3	Робоча станція WS-10-19-3	Eth 0
	Eth 3/1	SW-10-19-4	Eth 3/1
	Eth 3/2	SW-10-19-2	Eth 0/1
	Eth 3/3	SW-10-19-1	Eth 0/0
Комутатор SW-10-19-4	Eth 0/1	Сервер Serv-10-19-1	Eth 0
	Eth 0/2	Робоча станція WS-10-19-4	Eth 0
	Eth 0/3	Робоча станція WS-10-19-5	Eth 0
	Eth 3/1	SW-10-19-4	Eth 3/1
	Eth 3/2	SW-10-19-1	Eth 0/1
	Eth 3/3	SW-10-19-2	Eth 0/0

Здійсню розподіл адрес для локальних мереж. Для зручності результат наведений в таблиці 2.2.

Таблиця 2.3

Адресація локальної мережі

Призначення адрес	IP– address
Адреса мережі	192.168.19.0
Маска мережі	255.255.255.0(/24)
Мінімальна адреса	192.168.19.1
Шлюз за замовчуванням (1)	192.168.19.254
Призначені Windows Server (1)	192.168.19.251
Призначені комутаторам (4)	192.168.19.240 – 192.168.19.243
Діапазон адрес майбутніх пристроїв (30)	192.168.19.1 – 192.168.19.30
Діапазон вільних адрес (209)	192.168.19.31 – 192.168.19.239

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

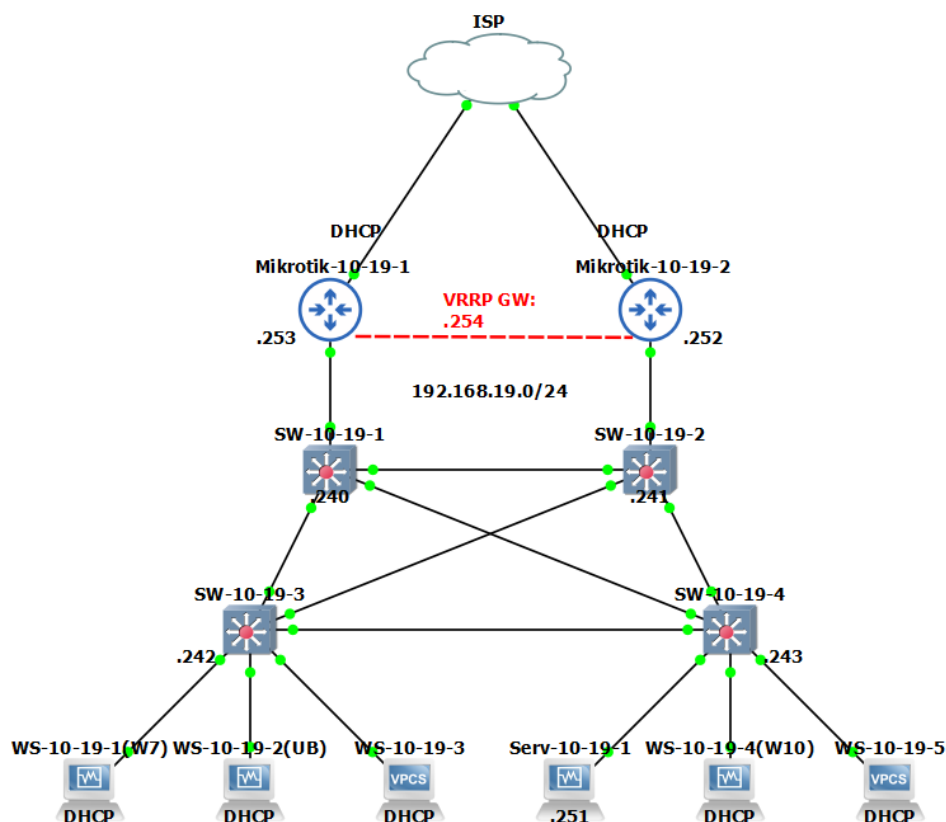


Рисунок 2.4 – Топологія мережі

2.4. Розробка підсистеми захисту гетерогенної мережі організації

Забезпечення безпеки гетерогенної мережі є одним із найважливіших аспектів управління інформаційними системами організації. Гетерогенна мережа включає різноманітні типи пристроїв і операційних систем, що ускладнює процес захисту. У цьому розділі буде розглянуто основні принципи і методи розробки підсистеми захисту гетерогенної мережі, що забезпечують захист від внутрішніх і зовнішніх загроз.

Першим етапом розробки підсистеми захисту є аналіз можливих загроз. Основні загрози для гетерогенної мережі включають зовнішні загрози (атаки з Інтернету, такі як DDoS-атаки, спроби несанкціонованого доступу, віруси і шкідливе програмне забезпечення), внутрішні загрози (несанкціонований доступ користувачів, витік даних, помилки конфігурації, а також шкідливі дії з боку співробітників) і вразливості систем (вразливості операційних систем і програмного забезпечення, неправильні налаштування мережевого обладнання).

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

Підсистема захисту гетерогенної мережі складається з декількох компонентів, кожен з яких відповідає за певний аспект захисту. Фаєрвол є першою лінією захисту від зовнішніх загроз. Він фільтрує вхідний і вихідний трафік, забезпечуючи доступ тільки для авторизованих користувачів і сервісів. Налаштування фаєрвола включає створення правил фільтрації трафіку і захист від DDoS-атак. IPS працює в тісному зв'язку з фаєрволом і забезпечує виявлення та запобігання загроз, які можуть пройти через фаєрвол. Налаштування IPS включає виявлення аномалій у трафіку і впровадження сигнатур атак.

VPN забезпечує безпечний віддалений доступ до мережі організації. Це особливо важливо для співробітників, які працюють віддалено або підключаються з зовнішніх мереж. Налаштування VPN включає створення тунелів шифрування і аутентифікацію користувачів. NAC забезпечує контроль доступу до мережі на основі політик безпеки організації. Налаштування NAC включає аутентифікацію і авторизацію користувачів, а також моніторинг пристроїв. Захист кінцевих точок включає заходи з захисту робочих станцій і серверів. Налаштування захисту кінцевих точок включає антивірусне програмне забезпечення, локальні брандмауери і систему управління патчами.

Система моніторингу і логування є важливою частиною підсистеми захисту, що забезпечує постійний контроль за станом мережі і виявлення потенційних загроз. Налаштування включає централізоване логування і моніторинг у режимі реального часу. Система резервного копіювання і відновлення даних забезпечує збереження критичних даних і можливість їх відновлення у випадку втрати. Налаштування включає регулярне резервне копіювання, зберігання резервних копій і план відновлення.

На комутаторах SW-1 – SW-5 налаштовано функції захисту Port Security, DHCP Snooping, BPDU guard і BPDU filter. Port Security обмежує кількість MAC-адрес на порту і блокує неавторизовані пристрої. DHCP Snooping захищає від атак типу DHCP Spoofing, фільтруючи підозрілі DHCP-повідомлення. BPDU guard і BPDU filter запобігають потенційним загрозам, пов'язаним із неправильним підключенням комутаторів і створенням петель у мережі.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

Mikrotik-1 та Mikrotik-2 додані до групи резервування VRRP з використанням аутентифікації типу «IP заголовок аутентифікації» (IP Authentication Header). VRRP забезпечує автоматичне перемикання на резервний маршрутизатор у разі виходу з ладу основного, підвищуючи надійність і доступність мережі. Для додаткового захисту на маршрутизаторах налаштовано певні правила Firewall, що контролюють вхідний і вихідний трафік.

На всіх мережевих пристроях налагоджено віддалений доступ по SSH, що забезпечує захищене підключення до обладнання для управління і моніторингу. Передача повідомлень до Syslog серверу дозволяє централізовано зберігати логи і проводити їх аналіз. Аутентифікація з використанням Radius забезпечує централізоване управління доступом до мережевих пристроїв і покращує безпеку шляхом використання єдиних облікових записів і політик.

На сервері Serv-1 (Windows Server 2019) налаштовано Active Directory (AD), Syslog сервер, Radius сервер, і створено облікові записи користувачів. Active Directory централізує управління користувачами і ресурсами, забезпечуючи зручне управління доступом і політиками безпеки. Syslog сервер збирає і зберігає логи з усіх мережевих пристроїв, що дозволяє проводити аналіз подій і виявляти потенційні загрози. Radius сервер забезпечує аутентифікацію користувачів і пристроїв, покращуючи безпеку і контроль доступу.

Всі робочі станції будуть залучені до домену «nesterchuk.net», і вхід виконуватиметься через заздалегідь створені облікові записи на Serv-1. Це забезпечує централізоване управління доступом до робочих станцій і ресурсів мережі, підвищуючи рівень безпеки і спрощуючи адміністрування.

Розробка підсистеми захисту гетерогенної мережі організації є критичним етапом для забезпечення безпеки і стабільної роботи мережі. Комплексний підхід, що включає використання фаєрволів, систем запобігання вторгнень, VPN, системи контролю доступу, захист кінцевих точок, моніторинг та логування, а також резервне копіювання і відновлення, дозволяє забезпечити високий рівень захисту від різноманітних загроз. Реалізація підсистеми захисту на кожному з

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

рівнів мережі забезпечує багаторівневий захист, що є необхідним для ефективного управління сучасними інформаційними системами.

Для посилення захисту мережі в рамках розробки підсистеми захисту гетерогенної мережі організації необхідно також впровадити додаткові методи і технології, що підвищують безпеку мережі та знижують ризики. До таких заходів можна віднести сегментацію мережі, застосування систем виявлення і реагування на інциденти, а також проведення регулярних аудитів безпеки.

Сегментація мережі є ефективним способом підвищення безпеки, оскільки вона дозволяє розділити мережу на окремі сегменти з різними рівнями доступу і політиками безпеки. Це зменшує поверхню атаки і ускладнює поширення загроз усередині мережі. Використання віртуальних локальних мереж (VLAN) дозволяє створювати логічно ізольовані сегменти, що покращує контроль доступу і підвищує безпеку. Наприклад, можна виділити окремі VLAN для фінансового відділу, технічної підтримки, адміністрації та гостей користувачів, забезпечуючи різні рівні доступу і захисту для кожної групи.

Впровадження систем виявлення і реагування на інциденти (IDR) є ключовим компонентом у забезпеченні оперативного виявлення і реагування на потенційні загрози. Такі системи включають в себе механізми моніторингу мережевого трафіку, аналізу поведінки користувачів і пристроїв, а також автоматичного виявлення аномалій і загроз. Важливим аспектом є інтеграція IDR з іншими компонентами підсистеми захисту, такими як фаєрволи і системи запобігання вторгнень, що дозволяє створювати комплексну систему захисту. Зокрема, можна використовувати рішення на базі SIEM (Security Information and Event Management), які збирають і аналізують дані з різних джерел, надаючи вичерпну картину про стан безпеки мережі і допомагаючи виявляти потенційні інциденти.

Регулярні аудити безпеки є важливою частиною процесу підтримки високого рівня захисту мережі. Вони дозволяють виявляти слабкі місця в конфігурації і налаштуваннях мережевих пристроїв, перевіряти відповідність політик безпеки актуальним загрозам і вимогам, а також оцінювати ефективність

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

впроваджених заходів захисту. Під час аудитів слід перевіряти всі компоненти мережі, включаючи маршрутизатори, комутатори, сервери і кінцеві точки, а також аналізувати журнали подій і повідомлення систем моніторингу.

Додатковим заходом захисту є навчання співробітників організації основам кібербезпеки. Людський фактор часто є найслабшою ланкою в системі захисту, тому важливо регулярно проводити навчання і тренінги для працівників, підвищуючи їх обізнаність про актуальні загрози і методи їх запобігання. Навчання повинно охоплювати такі аспекти, як безпечне використання паролів, розпізнавання фішингових атак, правила користування корпоративними ресурсами та реагування на підозрілі події.

Іншим важливим аспектом є використання сучасних технологій шифрування для захисту передаваних даних. Використання протоколів SSL/TLS для захисту веб-трафіку, шифрування електронної пошти і файлів, а також впровадження VPN для віддаленого доступу допомагає забезпечити конфіденційність і цілісність даних. Шифрування даних на кінцевих точках і серверних сховищах додатково захищає інформацію від несанкціонованого доступу у випадку фізичної крадіжки пристроїв.

Впровадження політики управління доступом на основі ролей (RBAC) дозволяє забезпечити гнучке і безпечне управління доступом до ресурсів мережі. Користувачі отримують доступ тільки до тих ресурсів, які необхідні для виконання їх робочих завдань, що знижує ризик несанкціонованого доступу і витоку даних. Управління доступом на основі ролей включає створення ролей з певними правами доступу, призначення ролей користувачам і регулярний перегляд та оновлення ролей відповідно до змін у організаційній структурі і вимогах безпеки.

Постійний моніторинг і аналіз мережевого трафіку є критично важливими для своєчасного виявлення і реагування на загрози. Використання спеціалізованих інструментів і технологій для аналізу трафіку, таких як мережеві аналізатори і системи виявлення вторгнень, допомагає швидко виявляти підозрілу активність і вживати необхідних заходів. Важливо також регулярно

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		50

оновлювати і вдосконалювати методи моніторингу, враховуючи нові загрози і методи атак.

Загалом, розробка підсистеми захисту гетерогенної мережі організації є комплексним і багатоступеневим процесом, що включає аналіз загроз, впровадження різноманітних технологій і рішень, а також постійний моніторинг і вдосконалення системи захисту. Використання сучасних технологій, регулярні аудити і навчання співробітників, а також впровадження політик і процедур управління безпекою дозволяють забезпечити високий рівень захисту мережі і ефективно протистояти актуальним загрозам.

Висновки до другого розділу:

У цьому розділі було висвітлено ключові аспекти проєктування і побудови гетерогенної мережі організації. Спочатку розглянуто питання побудови топології мережі, де було визначено оптимальне розташування і з'єднання мережевих пристроїв для забезпечення надійної і ефективної роботи. Далі проведено вибір обладнання, враховуючи вимоги до продуктивності, надійності та безпеки, що дозволило створити основу для побудови сучасної мережевої інфраструктури.

Розробка схеми адресації мережі включала планування і розподіл IP-адрес, що забезпечує унікальність і доступність кожного пристрою в мережі. Це дозволяє ефективно керувати мережевими ресурсами і забезпечує належний рівень контролю та управління трафіком.

Особливу увагу було приділено розробці підсистеми захисту гетерогенної мережі організації. Включено заходи щодо забезпечення безпеки на всіх рівнях мережі, використання сучасних технологій захисту і механізмів, таких як міжмережеві екрани, системи виявлення і запобігання вторгнень, шифрування, контроль доступу, а також моніторинг і логування подій. Комплексний підхід до безпеки дозволяє мінімізувати ризики і захистити мережу від внутрішніх і зовнішніх загроз, забезпечуючи стабільну і безпечну роботу інформаційних систем організації.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ ЗАХИСТУ ГЕТЕРОГЕННОЇ МЕРЕЖІ

3.1 Базове налагодження пристроїв мережі

Для того, щоб мережа правильно працювала, потрібно налаштувати все у правильному порядку, та ви користувати правильні параметри.

На початку налагодження зробили налаштування маршрутизатора MikroTik та комутатора Cisco через консоль PuTTY. Налаштування включають встановлення IP-адрес, налаштування NAT, VRRP та інші параметри, необхідні для забезпечення роботи пристроїв у мережі. Спочатку було змінено ім'я маршрутизаторів на "Mikrotik-10-19-1" та "Mikrotik-10-19-2". Це дозволяє легко ідентифікувати маршрутизатор в мережі та полегшує управління ним. До інтерфейсу ether2 було додано IP-адресу 192.168.19.253 з маскою підмережі /24 та 192.168.19.252 з маскою підмережі /24. Цей інтерфейс використовується для підключення до локальної мережі, і коментар "LINK-TO-LAN" був доданий для більшої ясності. Командою «ip dhcp-client» налаштовується робота DHCP-клієнту на ether1 завдяки чому маршрутизатори отримуватимуть динамічну адресу для виходу в Інтернет від провайдера (ISP). Після отримання динамічної адреси від провайдера маршрутизатори автоматично згенерують маршрут за замовчуванням для доступу трафіку локальної мережі до Інтернету. Для забезпечення коректної маршрутизації вихідного трафіку було додано правило NAT (Network Address Translation). Це правило дозволяє всім пристроям у підмережі 192.168.19.0/24 використовувати IP-адресу інтерфейсу ether1 для виходу в інтернет. Це досягається за допомогою маскування, який приховує внутрішні IP-адреси за зовнішньою адресою маршрутизатора. Щоб забезпечити високу доступність мережі, було налаштовано VRRP (Virtual Router Redundancy Protocol). На інтерфейсі ether2 було створено VRRP інтерфейс з ідентифікатором VRID 1 і пріоритетом 110. Використовується аутентифікація AH (Authentication Header) з паролем "vrrp-pas". До VRRP інтерфейсу була додана IP-адреса 192.168.19.254 з маскою підмережі /32 та коментарем "VRRP-GATEWAY". Це

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

дозволяє маршрутизатору виконувати роль резервного шлюзу у випадку відмови основного. Комутатор було налаштовано наступним чином: встановлено шлюз за замовчуванням 192.168.19.254, що дозволяє комутатору передавати трафік за межі локальної мережі. Налаштовано DNS сервер з IP-адресою 192.168.19.251 для забезпечення доменного імені. Встановлено доменне ім'я "nesterchuk.net" для комутатора. Увімкнено функцію DNS lookup, яка дозволяє комутатору переводити доменні імена в IP-адреси. Призначено IP-адресу 192.168.19.240 з маскою підмережі 255.255.255.0. Інтерфейс VLAN1 було активовано командою "no shut". Ці налаштування забезпечують базову функціональність мережевих пристроїв, включаючи маршрутизацію, трансляцію мережевих адрес, високу доступність та управління DNS. Це дозволяє створити стабільну та надійну мережеву інфраструктуру.

```

Mikrotik-10-19-1 - PuTTY
[admin@Mikrotik-10-19-1] > system identity set name=Mikrotik-10-19-1
[admin@Mikrotik-10-19-1] > ip address add interface=ether2 address=192.168.19.253/24 comment=LINK-TO-LAN
[admin@Mikrotik-10-19-1] > ip dhcp-client add interface=ether1 disabled=no
[admin@Mikrotik-10-19-1] > ip firewall nat add chain=srcnat src-address=192.168.19.0/24 out-interface=ether1 action=masquerade
  
```

Рисунок 3.1 – Налаштування ip адрес та NAT на Mikrotik 1

```

Mikrotik-10-19-2 - PuTTY
[admin@Mikrotik-10-19-2] > system identity set name=Mikrotik-10-19-2
[admin@Mikrotik-10-19-2] > ip address add interface=ether2 address=192.168.19.252/24 comment=LINK-TO-LAN
[admin@Mikrotik-10-19-2] > ip dhcp-client add interface=ether1 disabled=no
[admin@Mikrotik-10-19-2] > ip firewall nat add chain=srcnat src-address=192.168.19.0/24 out-interface=ether1 action=masquerade
  
```

Рисунок 3.2 – Налаштування ip адрес та NAT на Mikrotik 2

```

Mikrotik-10-19-1 - PuTTY
[admin@Mikrotik-10-19-1] > interface vrrp add interface=ether2 name=vrrp1 vrid=1 priority=110 version=2 authentication=ah password=vrrp-pas
[admin@Mikrotik-10-19-1] > ip address add address=192.168.19.254/32 interface=vrrp1 comment=VRRP-GATEWAY
  
```

Рисунок 3.3 – Налаштування VRRP на Mikrotik-1

```

Mikrotik-10-19-2 - PuTTY
[admin@Mikrotik-10-19-2] > interface vrrp add interface=ether2 name=vrrp1 vrid=1
9 priority=100 version=2 authentication=ah password=vrrp-pas
[admin@Mikrotik-10-19-2] > ip address add address=192.168.19.254/32 interface=vr
rp1 comment=VRRP-GATEWAY

```

Рисунок 3.4 – Налаштування VRRP на Mikrotik-2

```

SW-10-19-1 - PuTTY
SW-10-19-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW-10-19-1(config)#ip default-gateway 192.168.19.254
SW-10-19-1(config)#ip name-server 192.168.19.251
SW-10-19-1(config)#ip domain name nesterchuk.net
SW-10-19-1(config)#ip domain lookup
SW-10-19-1(config)#int vlan1
SW-10-19-1(config-if)#ip address 192.168.19.240 255.255.255.0
SW-10-19-1(config-if)#no shut

```

Рисунок 3.5 – Налаштування комутатора Cisco

3.2 Налагодження Active Directory і робочих станцій

Для початку ми налаштували сервер на використання статичної IP-адреси 192.168.19.251. Це забезпечує стабільний доступ до серверу та уникає можливих конфліктів з іншими пристроями в мережі.

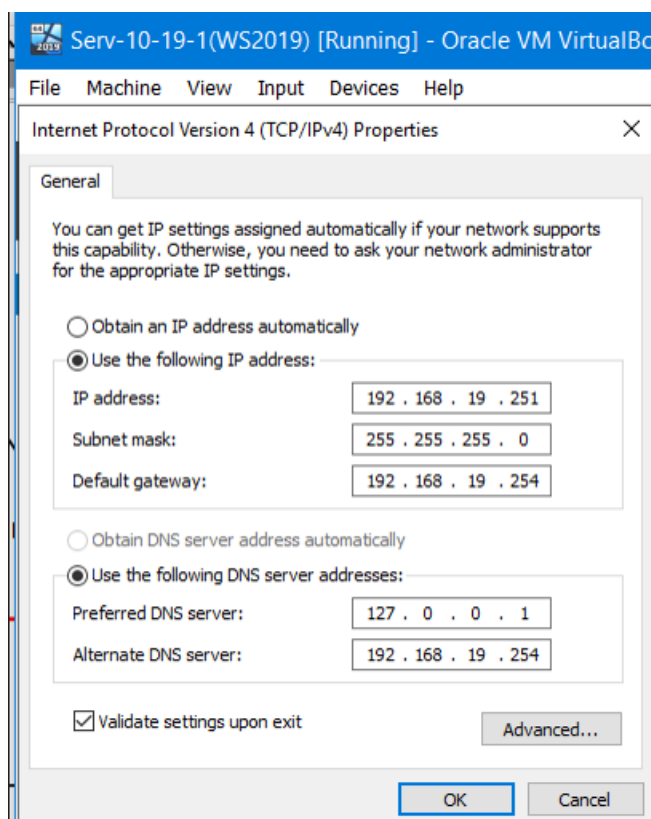


Рисунок 3.6 – Налаштування адреси

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

Наступним кроком було додавання необхідних ролей для сервера. Це включає в себе встановлення ролей Active Directory Domain Services (AD DS), DNS Server та DHCP Server.

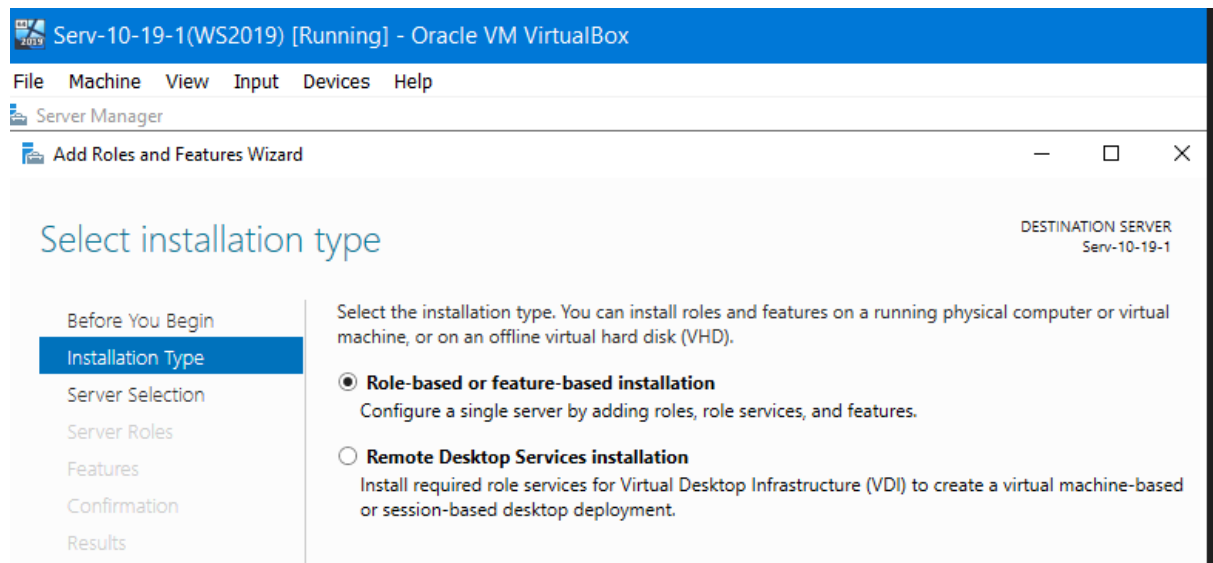


Рисунок 3.7 – Додавання ролей

У процесі додавання ролей ми обрали сервер, на якому будуть розгортатися ці ролі, забезпечуючи правильне функціонування домену та мережевих сервісів.

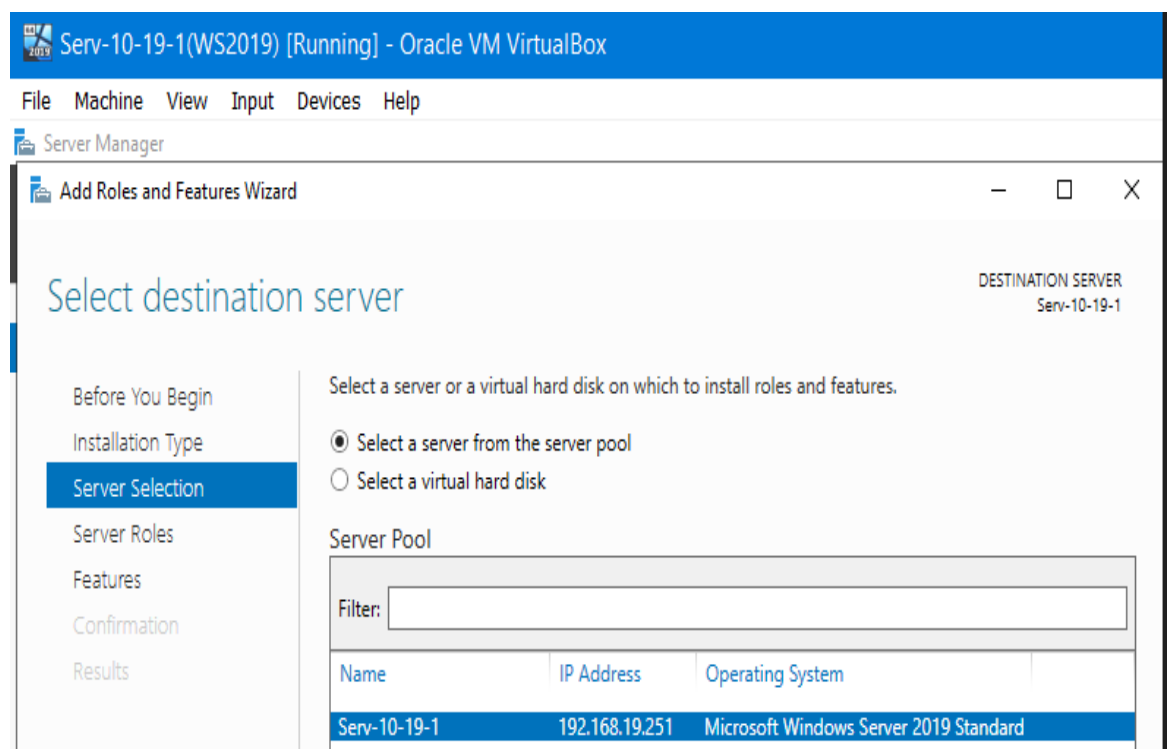


Рисунок 3.8 – Вибір сервера призначення

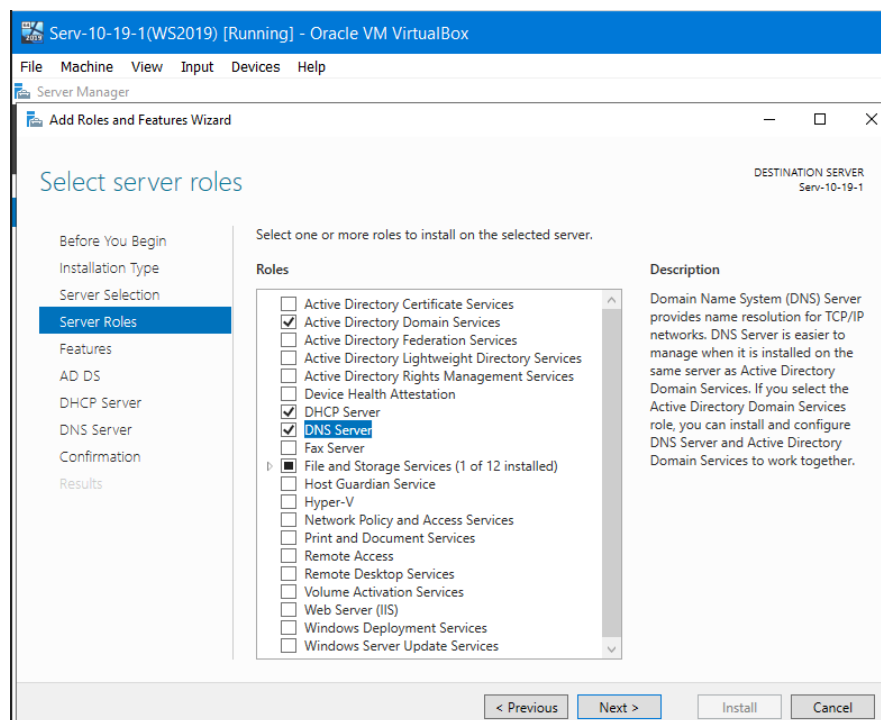


Рисунок 3.9 – Додавання ролей

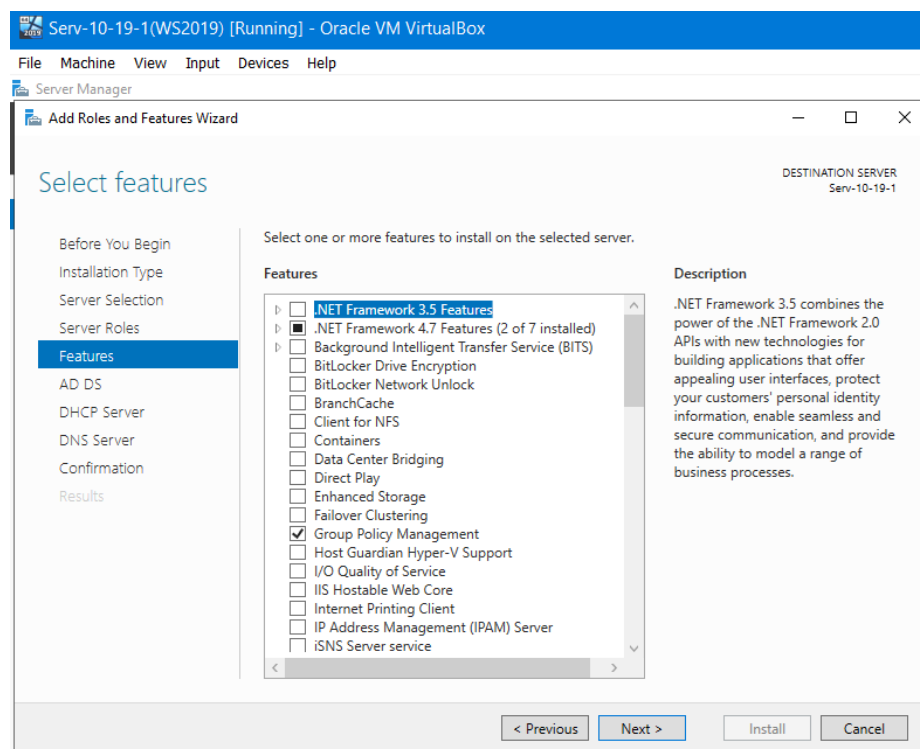


Рисунок 3.10 – Додавання ролей

Для налаштування домену було створено новий домен nesterchuk.net. Це дозволяє централізовано керувати користувачами, комп'ютерами та іншими ресурсами мережі.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

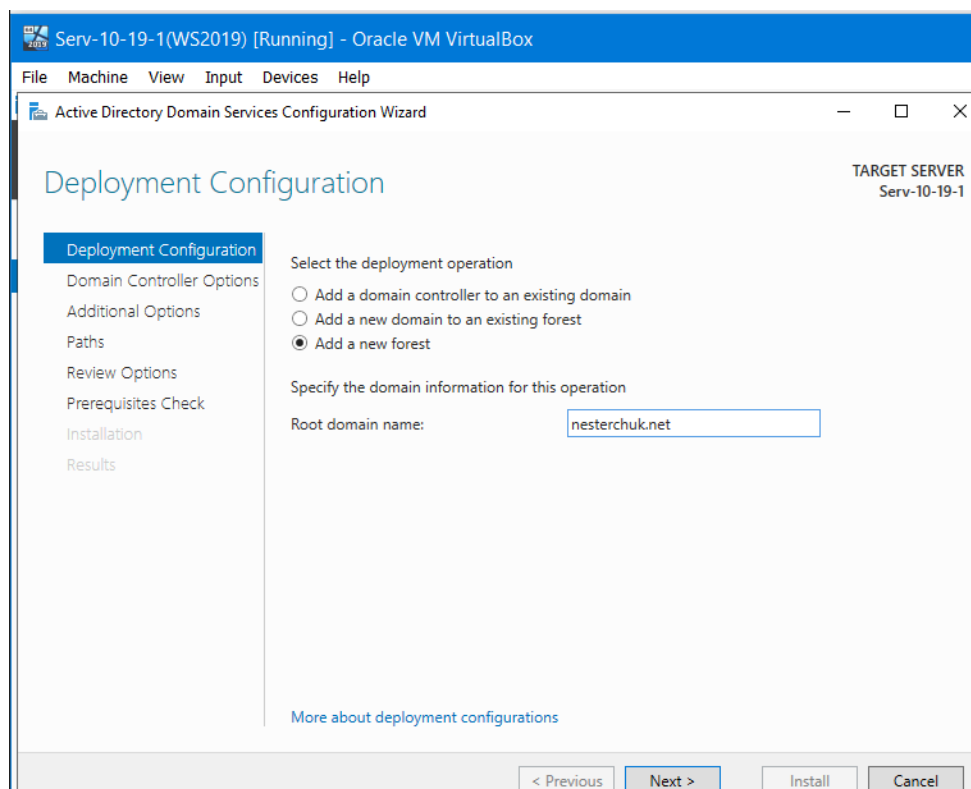


Рисунок 3.11 – Створення домену

Далі було створено область DHCP під назвою Lan_scope, що відповідає за автоматичний розподіл IP-адрес для клієнтських пристроїв в мережі.

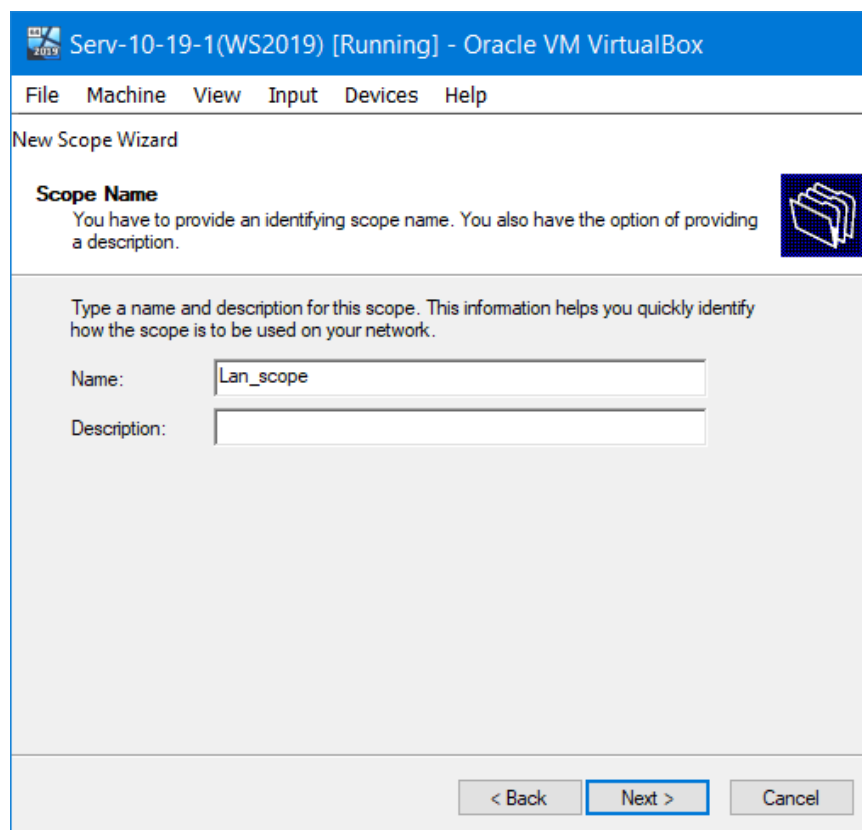


Рисунок 3.12 – Створення області Lan_scope

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

В межах області Lan_scope був визначений діапазон IP-адрес, які будуть надаватися клієнтським пристроям, наприклад, від 192.168.19.1 до 192.168.19.254.

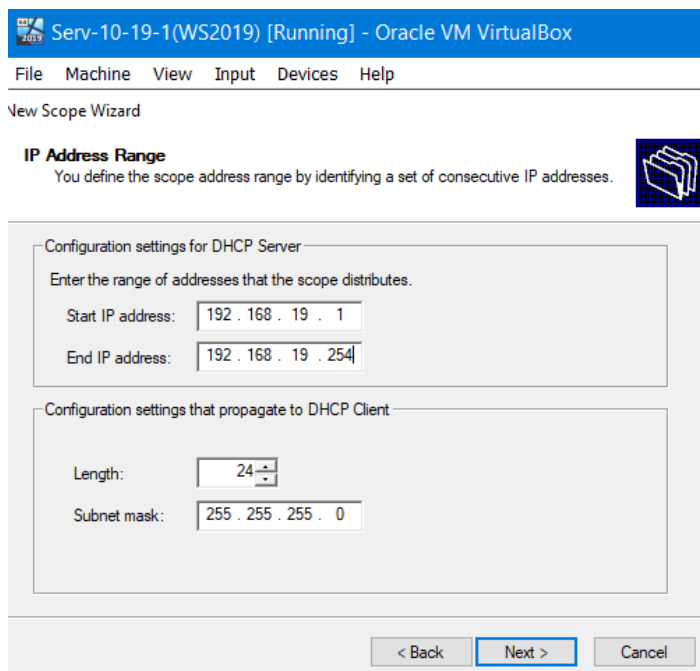


Рисунок 3.13 – Визначення діапазону роздачі адрес

З діапазону роздачі були виключені статичні IP-адреси, що використовуються сервером та іншими важливими пристроями 192.168.19.240-192.168.19.254 та 192.168.19.101-192.168.19.254.

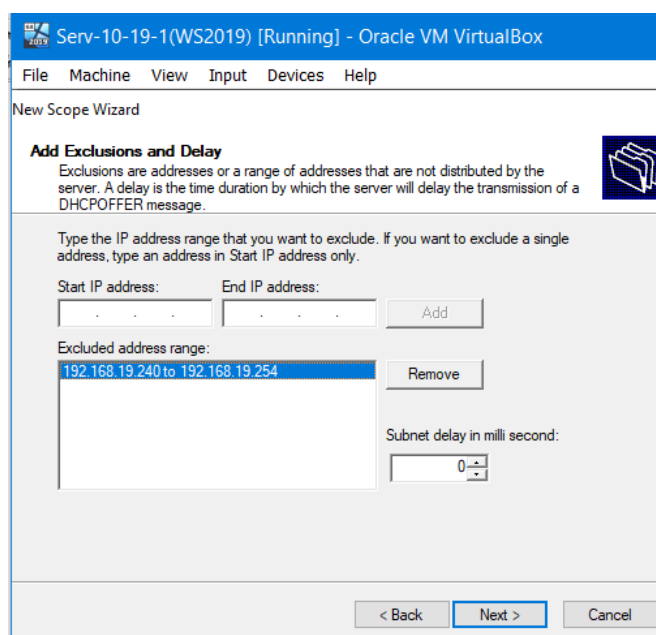


Рисунок 3.14 – Виключення статичних адрес з діапазону роздачі

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

Було налаштовано термін часу видачі IP-адрес (lease time) для клієнтів, 8 днів. Це забезпечує своєчасне оновлення адрес та зменшує ймовірність конфліктів.

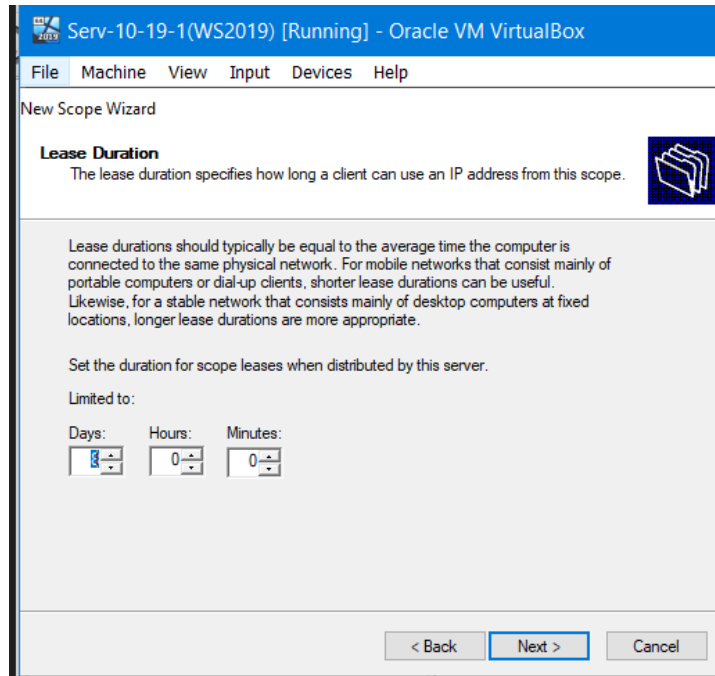


Рисунок 3.15 – Вибір терміну часу видачі адрес
В конфігурації DHCP було додано шлюз за замовчуванням (default gateway) з адресою 192.168.19.254, що забезпечує вихід в Інтернет.

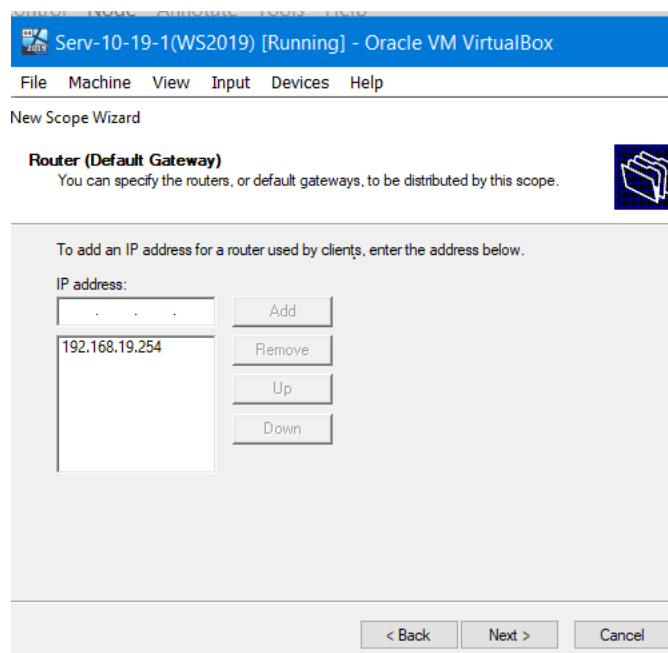


Рисунок 3.16 – Додавання адреси за замовчуванням

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

До конфігурації DHCP також були додані адреси DNS-серверів, що дозволяє клієнтам використовувати DNS для резолюції доменних імен. Основний DNS-сервер – 192.168.19.251.

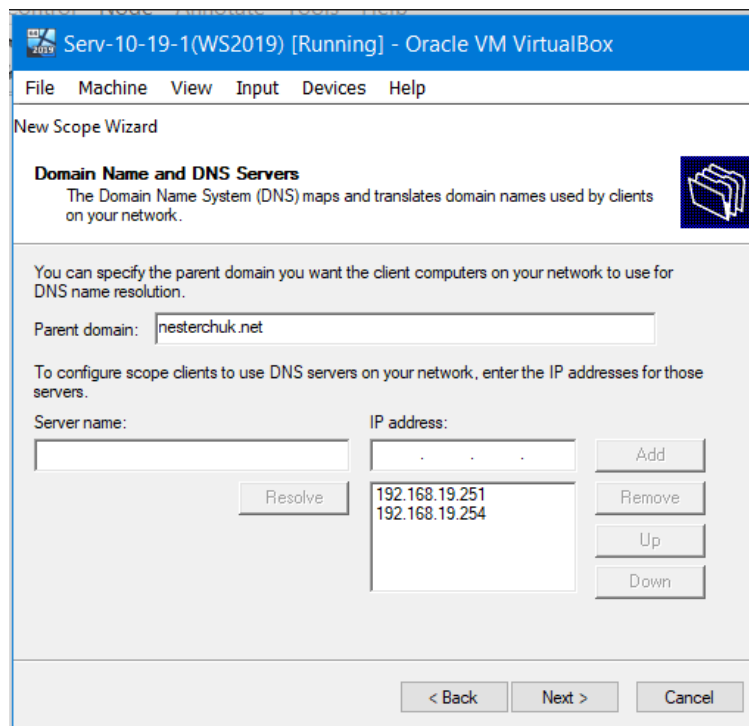


Рисунок 3.17 – Додання адрес DNS-серверів
Клієнтські станції (Windows 7, Windows 10, Ubuntu) були налаштовані на автоматичне отримання IP-адрес через DHCP.

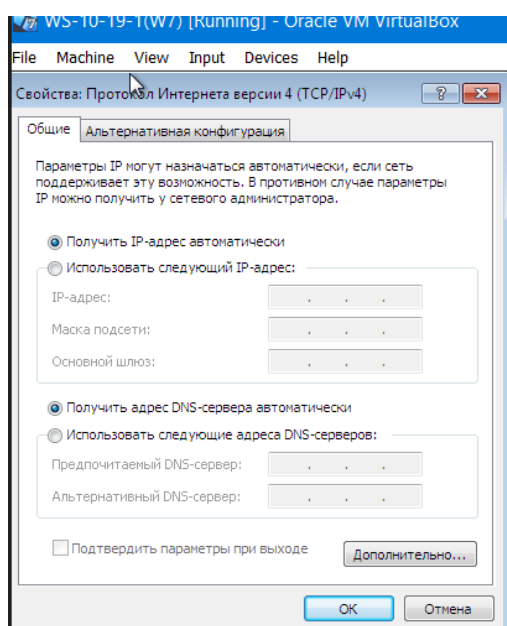


Рисунок 3.18 – Налаштування станції на автоматичне отримання адрес

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

Станцію з ОС Windows 7 було підключено до домену nesterchuk.net, що дозволяє використовувати централізоване управління користувачами та ресурсами.

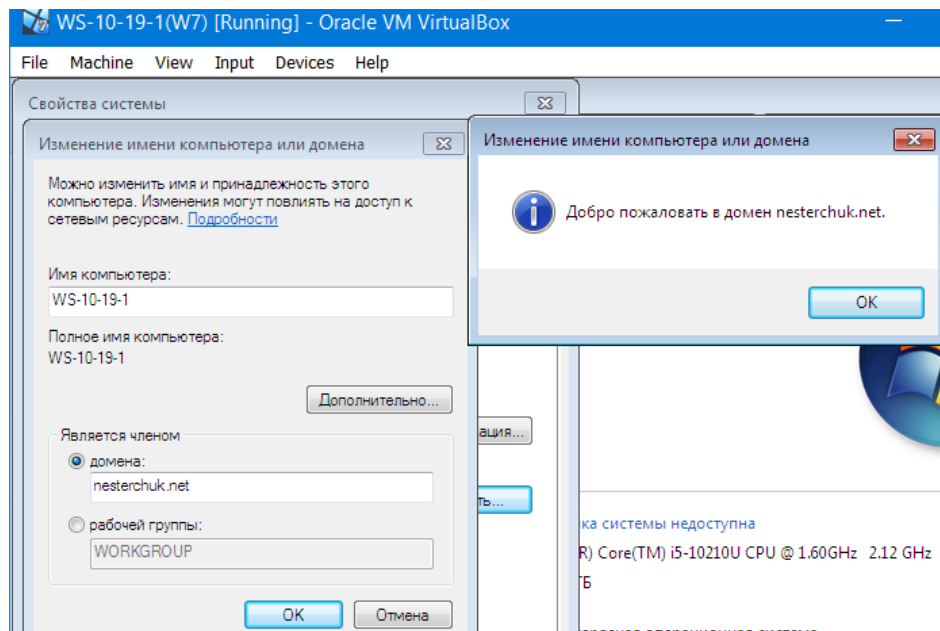


Рисунок 3.19 – Підключення станції з ОС Windows 7 до домену
Станцію Ubuntu було підключено до домену nesterchuk.net, що забезпечує уніфікований доступ до мережесих ресурсів.

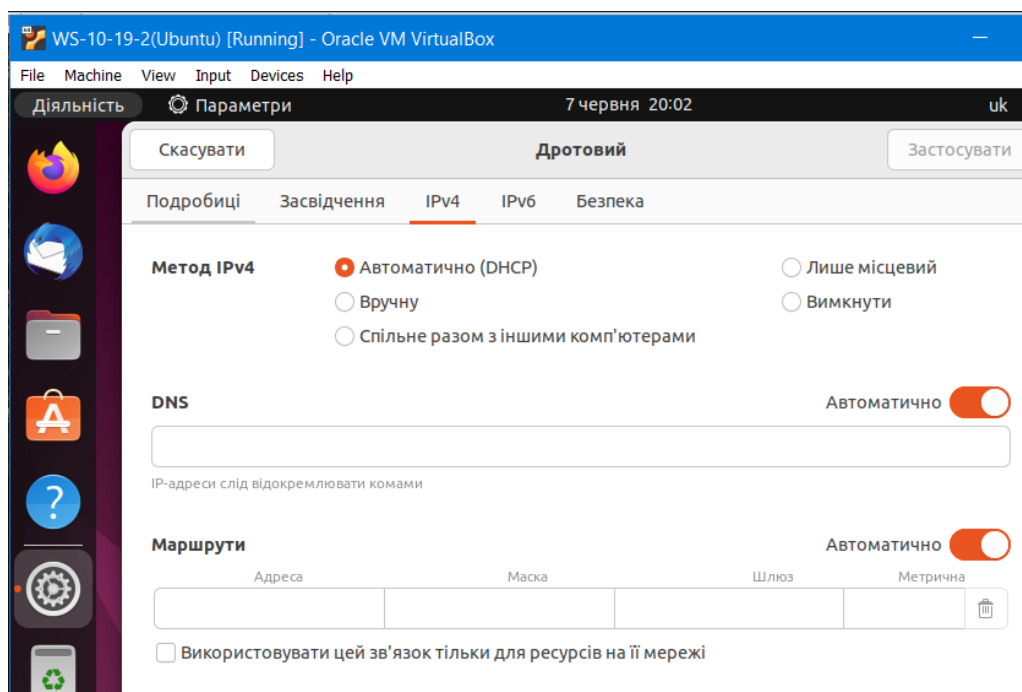


Рисунок 3.20 – Налаштування станції на автоматичне отримання адрес

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

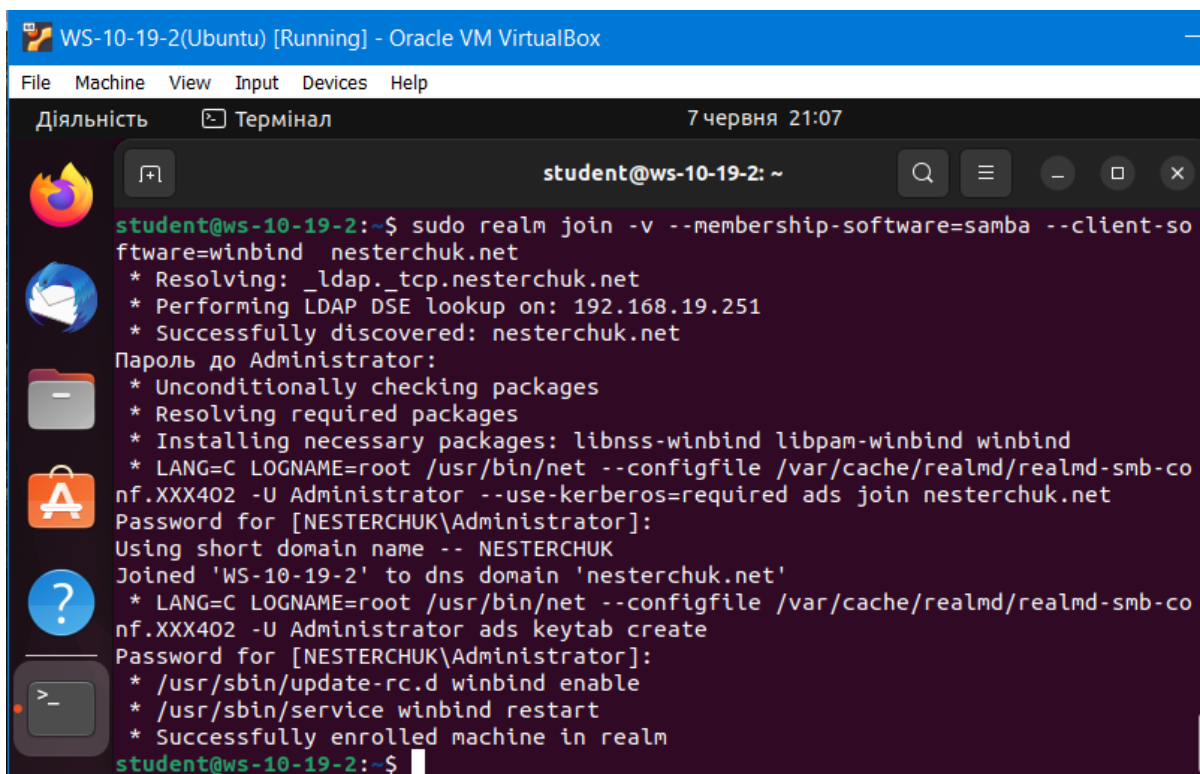


Рисунок 3.21 – Підключення до домену ubuntu

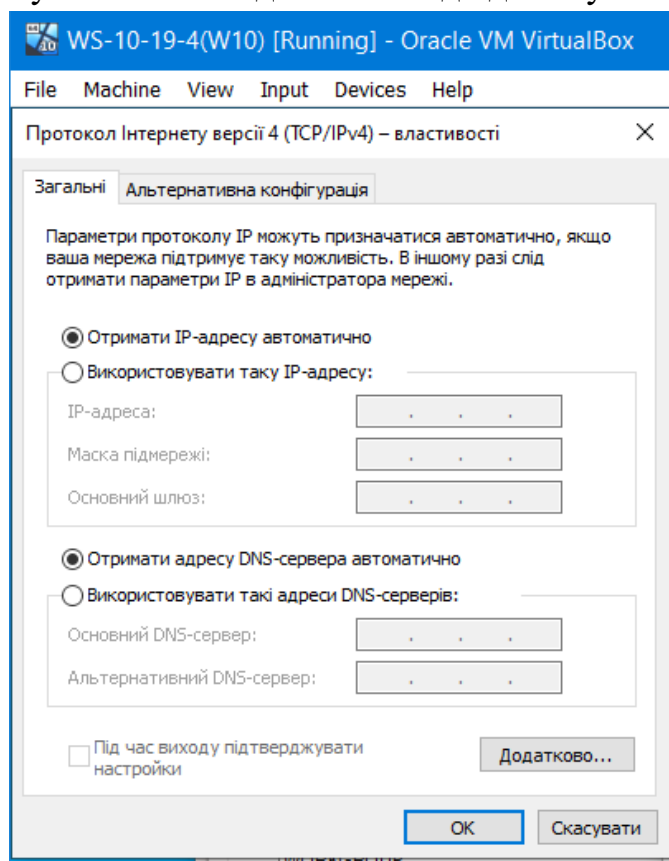


Рисунок 3.22 – Налаштування станції на автоматичне отримання адрес

Станцію з ОС Windows 10 також було підключено до домену nesterchuk.net, що дозволяє керувати нею з централізованого місця.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

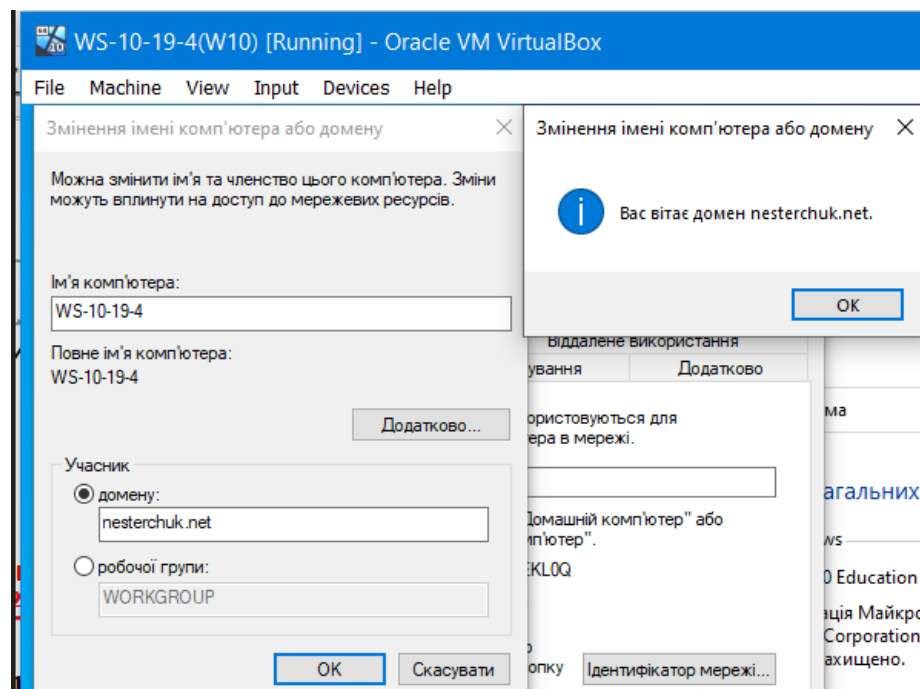


Рисунок 3.23 – Підключення станції з ОС Windows 10 до домену

Було створено необхідні DNS-записи для забезпечення правильного резолювання імен в домені nesterchuk.net.

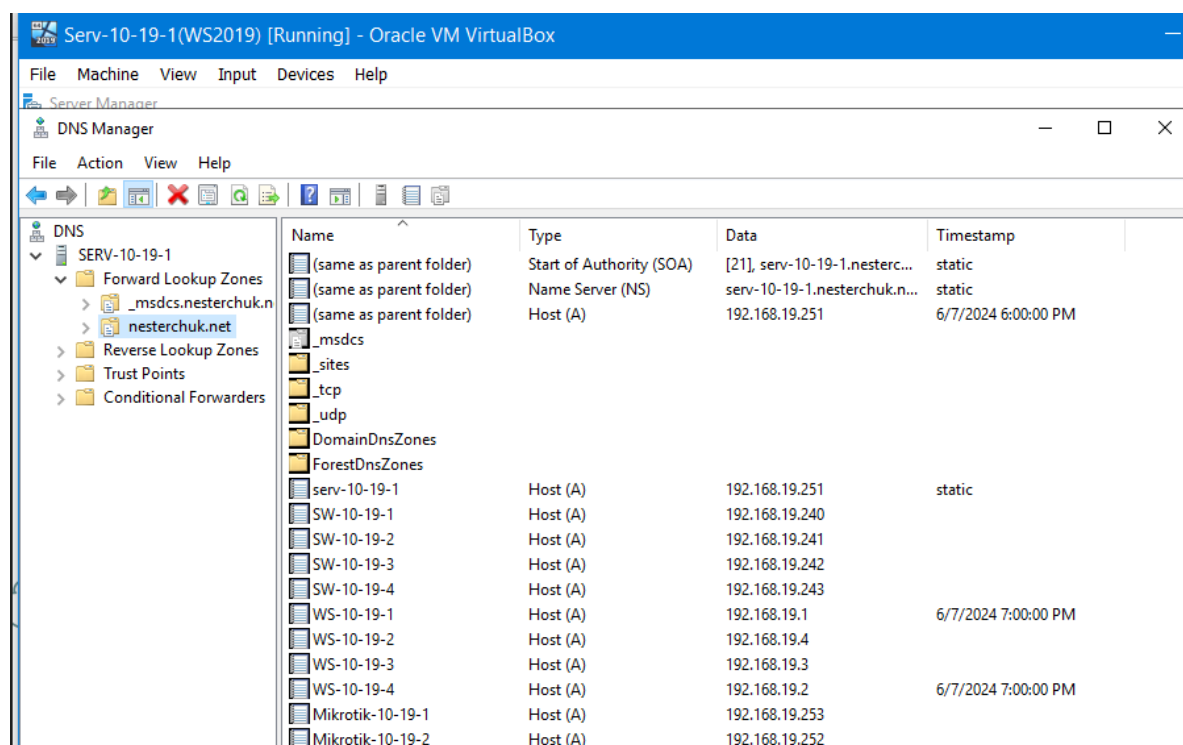


Рисунок 3.24 – Додання DNS-записів

Проведено перевірку всіх налаштувань для переконання, що всі пристрої коректно отримують IP-адреси та можуть підключатися до домену.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

```
WS-10-19-4(W10) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WS-10-19-4
Primary Dns Suffix . . . . . : nesterchuk.net
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : nesterchuk.net

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : nesterchuk.net
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-91-08-3D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a059:f1bc:393b:68af%6(Preferred)
IPv4 Address. . . . . : 192.168.19.2(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 7 червня 2024 р. 19:08:31
Lease Expires . . . . . : 15 червня 2024 р. 19:36:07
Default Gateway . . . . . : 192.168.19.254
DHCP Server . . . . . : 192.168.19.251
DHCPv6 IAID . . . . . : 101187623
DHCPv6 Client DUID. . . . . : 00-01-00-01-2D-EA-4F-30-08-00-27-91-08-3D
DNS Servers . . . . . : 192.168.19.251
                        192.168.19.254
NetBIOS over Tcpip. . . . . : Enabled
```

Рисунок 3.25 – Перевірка налаштувань

Перевірено наявність зв’язку з маршрутизатором Mikrotik та забезпечено вихід в Інтернет для всіх клієнтських станцій.

```
WS-10-19-4(W10) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: C:\Windows\system32\cmd.exe

Microsoft Windows [Version 10.0.18363.592]
(c) Корпорація Майкрософт (Microsoft Corporation), 2019. Усі права захищено.

C:\Users\Administrator>ping Mikrotik-10-19-1

Pinging Mikrotik-10-19-1.nesterchuk.net [192.168.19.253] with 32 bytes of data:
Reply from 192.168.19.253: bytes=32 time=2ms TTL=64
Reply from 192.168.19.253: bytes=32 time=2ms TTL=64
Reply from 192.168.19.253: bytes=32 time=1ms TTL=64
Reply from 192.168.19.253: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.19.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\Administrator>ping google.com

Pinging google.com [142.251.39.46] with 32 bytes of data:
Reply from 142.251.39.46: bytes=32 time=20ms TTL=115
Reply from 142.251.39.46: bytes=32 time=23ms TTL=115
Reply from 142.251.39.46: bytes=32 time=32ms TTL=115
Reply from 142.251.39.46: bytes=32 time=33ms TTL=115

Ping statistics for 142.251.39.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 33ms, Average = 27ms
```

Рисунок 3.26 – Перевірка наявності зв’язку з Mikrotik та з мережею Інтернет

Для синхронізації часу в мережі налаштовано NTP-сервер на контролері домену, що забезпечує точний час для всіх клієнтських пристроїв.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>w32tm /config /manualpeerlist:"ua.pool.ntp.org" /reliable:YES /update
The command completed successfully.

C:\Users\Administrator>net stop w32time
The Windows Time service is stopping.
The Windows Time service was stopped successfully.

C:\Users\Administrator>net start w32time
The Windows Time service is starting.
The Windows Time service was started successfully.

C:\Users\Administrator>w32tm /config /syncfromflags:domhier /reliable:YES /update
The command completed successfully.

C:\Users\Administrator>w32tm /query /peers
#Peers: 1

Peer:
State: Pending
Time Remaining: 889.1683606s
Mode: 0 (reserved)
Stratum: 0 (unspecified)
PeerPoll Interval: 0 (unspecified)
HostPoll Interval: 0 (unspecified)

```

Рисунок 3.27 – Налаштування роботи NTP сервера на контролері домену
Клієнтські станції з ОС Windows 10 були налаштовані на автоматичну
синхронізацію часу з NTP-сервером домену.

```

Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Administrator> w32tm /query /status
Leap Indicator: 0(no warning)
Stratum: 2 (secondary reference - syncd by (S)NTP)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0031699s
Root Dispersion: 19.6442356s
ReferenceId: 0xC0A813FB (source IP: 192.168.19.251)
Last Successful Sync Time: 08.06.2024 18:10:30
Source: Serv-10-19-1.nesterchuk.net
Poll Interval: 10 (1024s)

PS C:\Users\Administrator> w32tm /query /status /verbose
Leap Indicator: 0(no warning)
Stratum: 2 (secondary reference - syncd by (S)NTP)
Precision: -23 (119.209ns per tick)
Root Delay: 0.0031699s
Root Dispersion: 19.6442356s
ReferenceId: 0xC0A813FB (source IP: 192.168.19.251)
Last Successful Sync Time: 08.06.2024 18:10:30
Source: Serv-10-19-1.nesterchuk.net
Poll Interval: 10 (1024s)

Phase Offset: -1.8821602s
ClockRate: 0.0156250s
State Machine: 1 (Hold)
Time Source Flags: 8 (SignatureAuthenticated )
Server Role: 0 (None)
Last Sync Error: 0 (The command completed successfully.)
Time since Last Good Sync Time: 25.0503401s

```

Рисунок 3.28 – Налаштування NTP на ОС Windows 10

Аналогічно, клієнтські станції з ОС Ubuntu налаштовані на синхронізацію часу з NTP-сервером домену.

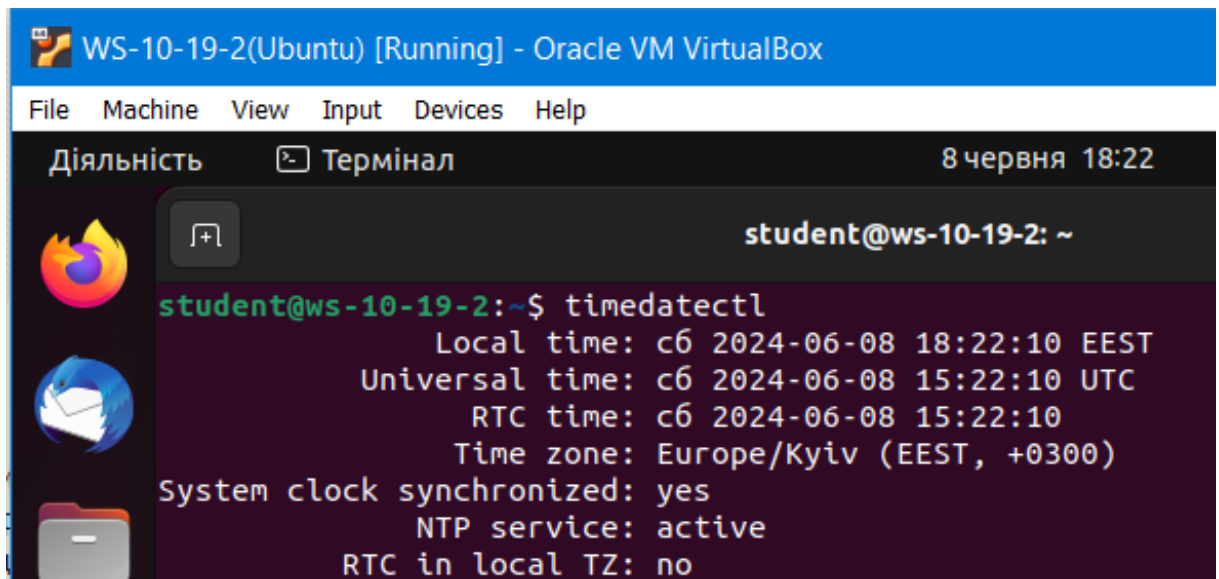


Рисунок 3.29 – Налаштування NTP на Ubuntu

Комутатор був налаштований на синхронізацію часу з NTP-сервером домену, що забезпечує правильний час для логування подій.

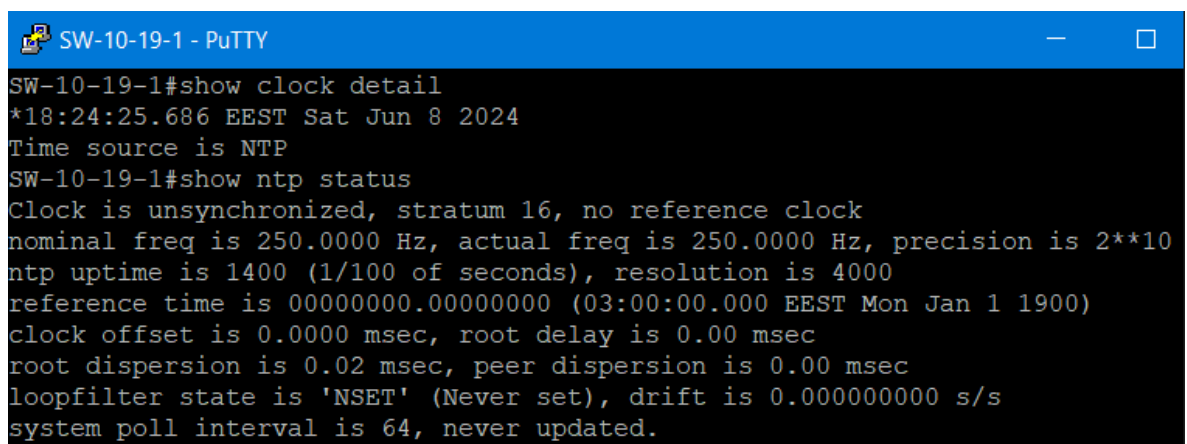


Рисунок 3.30 – Налаштування NTP на комутаторі.

Маршрутизатор Mikrotik також налаштований на синхронізацію часу з NTP-сервером, що забезпечує правильний час для всіх мережевих подій.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

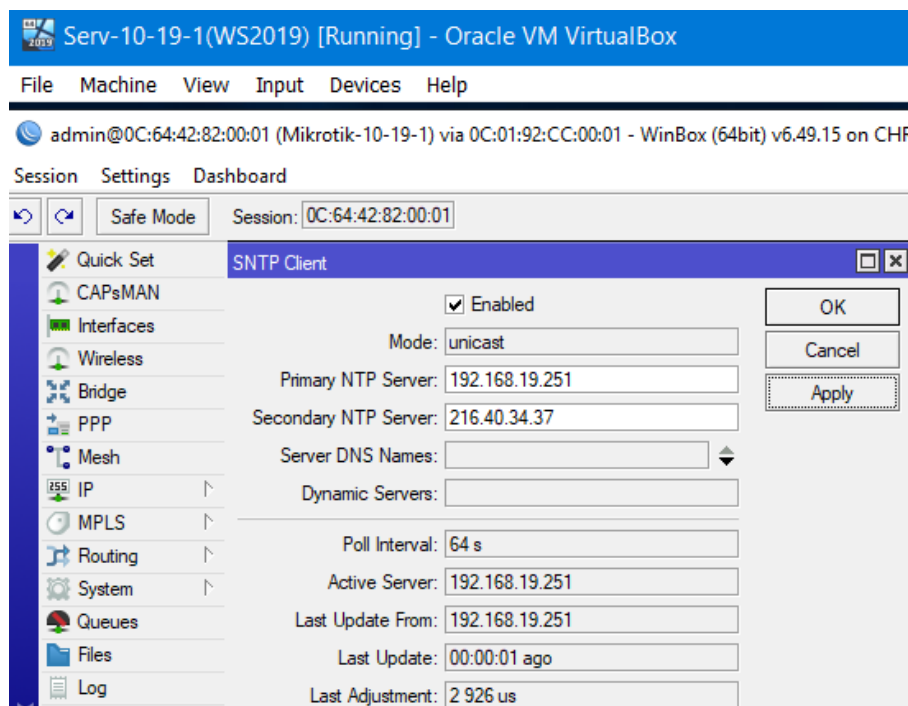


Рисунок 3.31 – Налаштування NTP на маршрутизаторі Mikrotik

Було створено нового користувача з іменем Анастасія Нестерчук у домені nesterchuk.net, що дозволяє їй підключатися до мережі та користуватися її ресурсами.

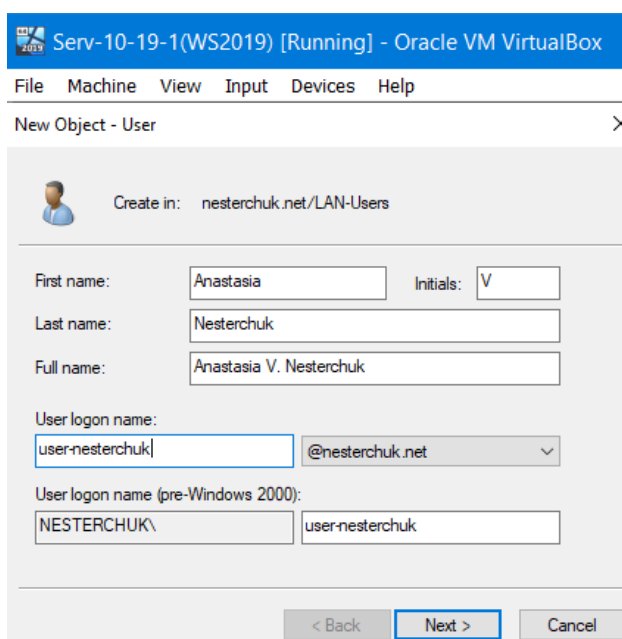


Рисунок 3.32 – Створення користувача

Для нового користувача user-nesterchuk був встановлений пароль, який забезпечує безпечний доступ до облікового запису.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

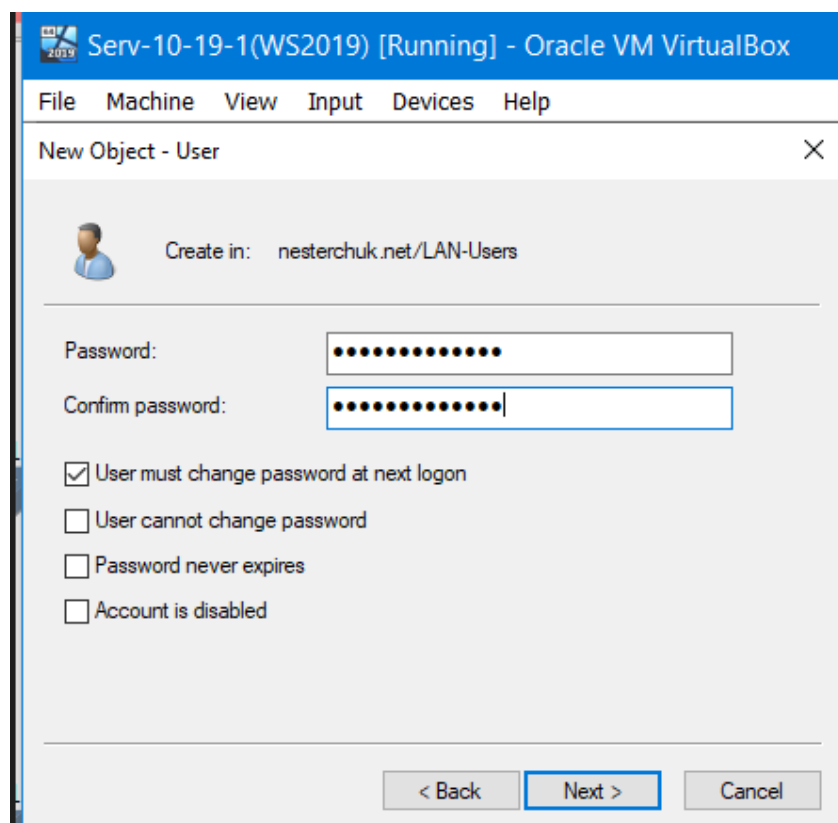


Рисунок 3.33 – Задання паролю

Перевірено можливість входу в систему під новим користувачем на різних клієнтських станціях для підтвердження коректності налаштувань та прав доступу.

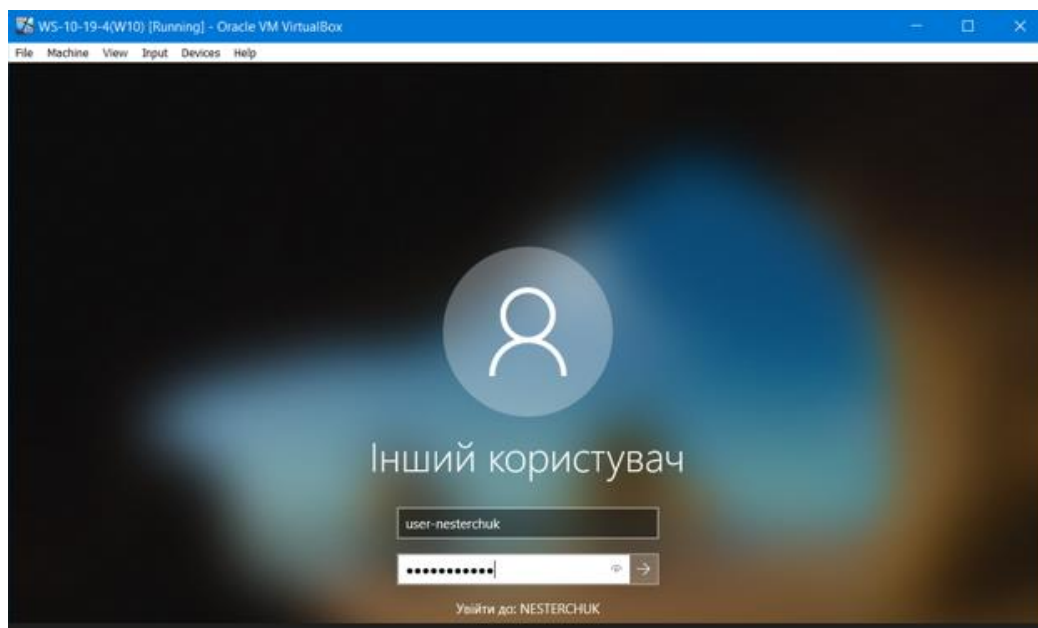


Рисунок 3.34 – Вхід в систему з використання облікових даних створеного користувача

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

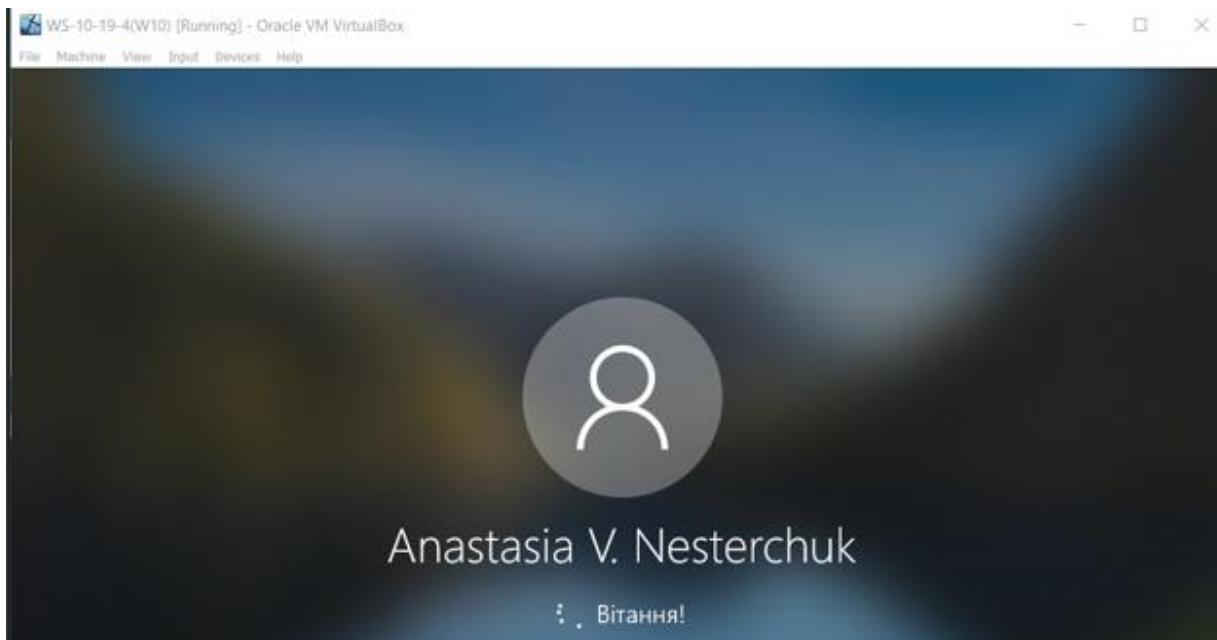


Рисунок 3.35 – Вхід в систему з використання облікових даних створеного користувача

3.3 Налагодження підсистеми захисту

Для забезпечення безпеки мережі важливо відключити всі незадіяні інтерфейси на комутаторі. Це допомагає запобігти несанкціонованим підключенням і можливим атакам на мережу.

```
SW-10-19-3 - PuTTY
SW-10-19-3(config)#vlan 1001
SW-10-19-3(config-vlan)#name UNUSED-VLAN
SW-10-19-3(config-vlan)#int range eth0/3, eth1/0-3, eth2/0-3, eth3/0
SW-10-19-3(config-if-range)#description UNUSED-PORT-VLAN1001
SW-10-19-3(config-if-range)#switchport mode access
SW-10-19-3(config-if-range)#switchport access vlan 1001
SW-10-19-3(config-if-range)#shutdown
```

Рисунок 3.36 – Відключення незадіяних інтерфейсів.

Наступним кроком є налаштування RADIUS-сервера для автентифікації мережеских клієнтів. Потрібно додати RADIUS-клієнтів, що включає в себе комутатори та маршрутизатори, які будуть використовувати цей сервер для автентифікації.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

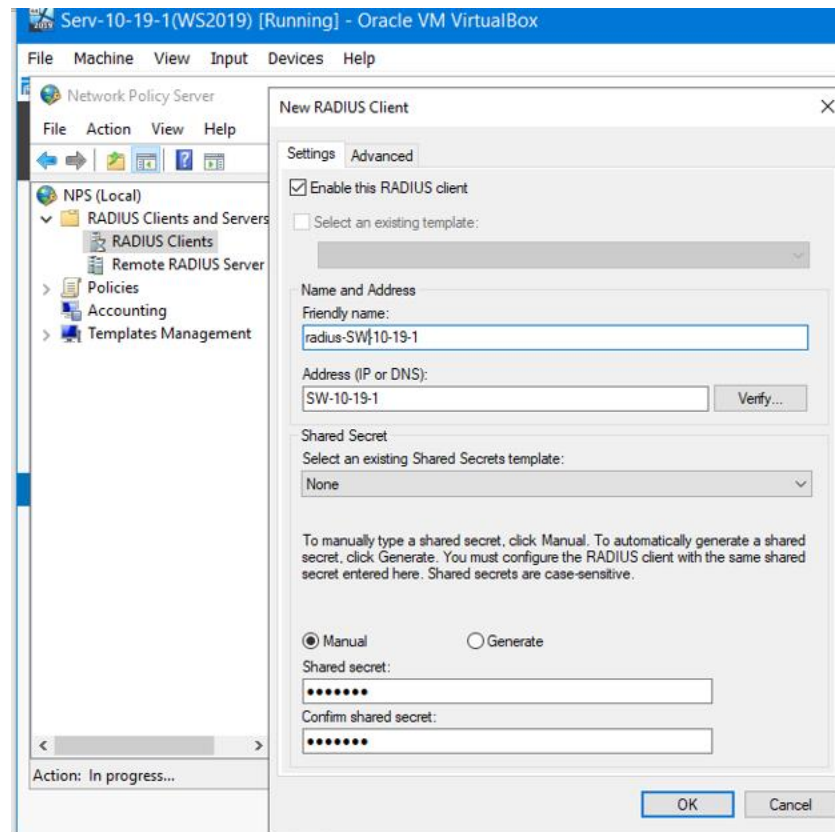


Рисунок 3.37 – Додання radius-клієнтів

Політики безпеки на RADIUS-сервері визначають, які параметри автентифікації та авторизації будуть використовуватися для різних клієнтів. Важливо налаштувати ці політики відповідно до вимог безпеки організації.

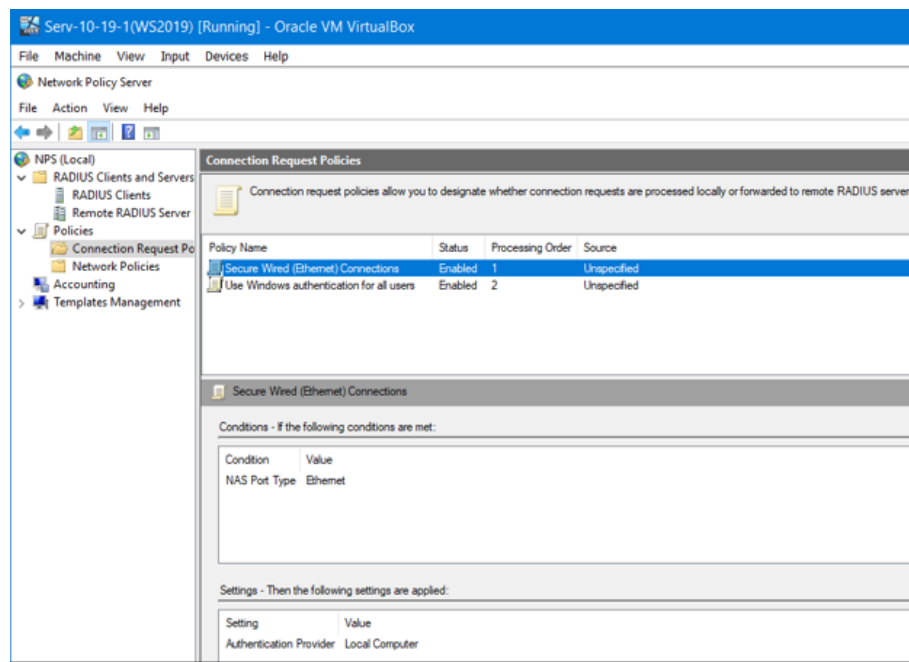


Рисунок 3.38 – Налаштування політик безпеки для Radius

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

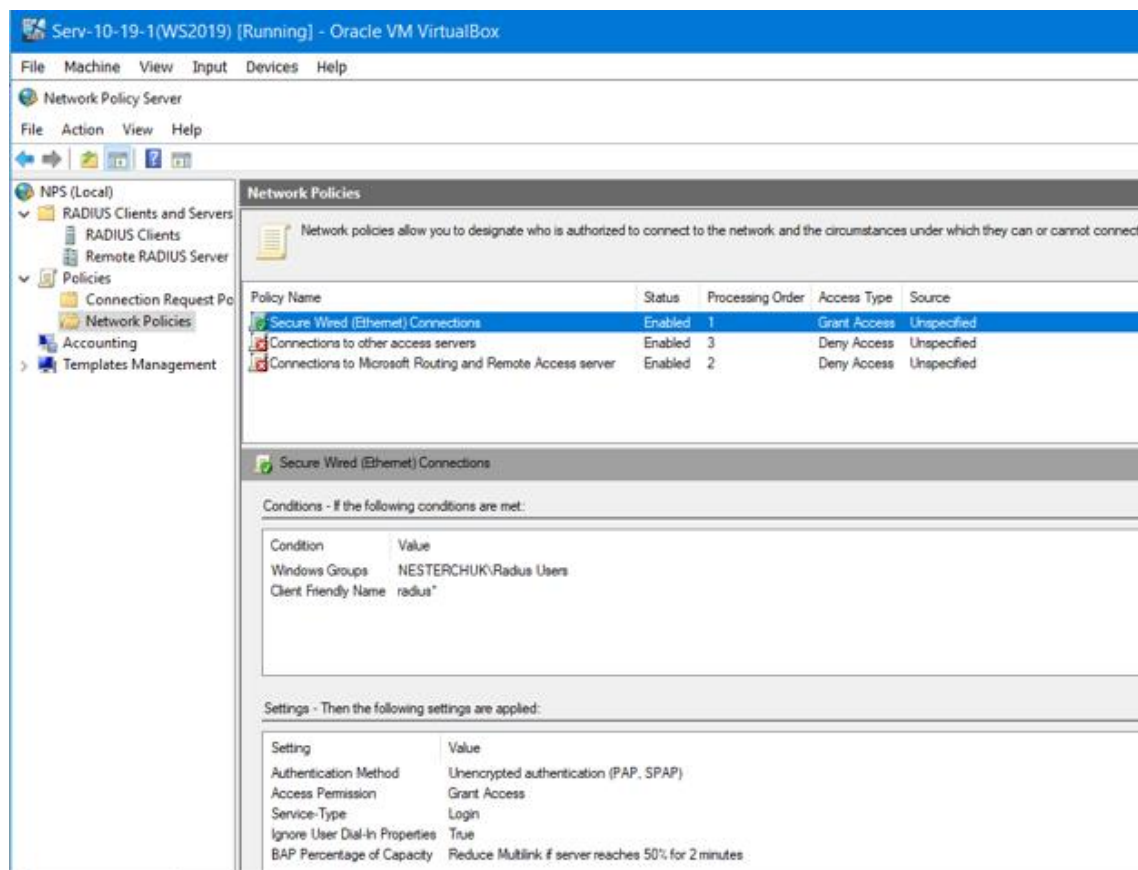


Рисунок 3.39 – Налаштування політик безпеки для Radius

На комутаторі потрібно налаштувати параметри для підключення до RADIUS-сервера. Це включає введення IP-адреси сервера, секретного ключа та інших необхідних налаштувань.

```

SW-10-19-1 - PuTTY
SW-10-19-1(config)#aaa new-model
SW-10-19-1(config)#username radius privilege 15 secret pass-rad
SW-10-19-1(config)#enable secret enable-pass
SW-10-19-1(config)#radius server Serv-10-19-1
SW-10-19-1(config-radius-server)#address ipv4 Serv-10-19-1 auth-port 1812 acct-port 1813
SW-10-19-1(config-radius-server)#key WinRadius
SW-10-19-1(config-radius-server)#exit
SW-10-19-1(config)#aaa authentication login default group radius local
SW-10-19-1(config)#aaa authorization exec default group radius local if-authenticated
SW-10-19-1(config)#line cons 0
SW-10-19-1(config-line)#login authentication default

```

Рисунок 3.40 – Налаштування Radius-клієнта на комутаторі

Аналогічно, потрібно налаштувати RADIUS-клієнта на маршрутизаторі Mikrotik. Це забезпечить централізовану автентифікацію для всіх мережевих пристроїв.

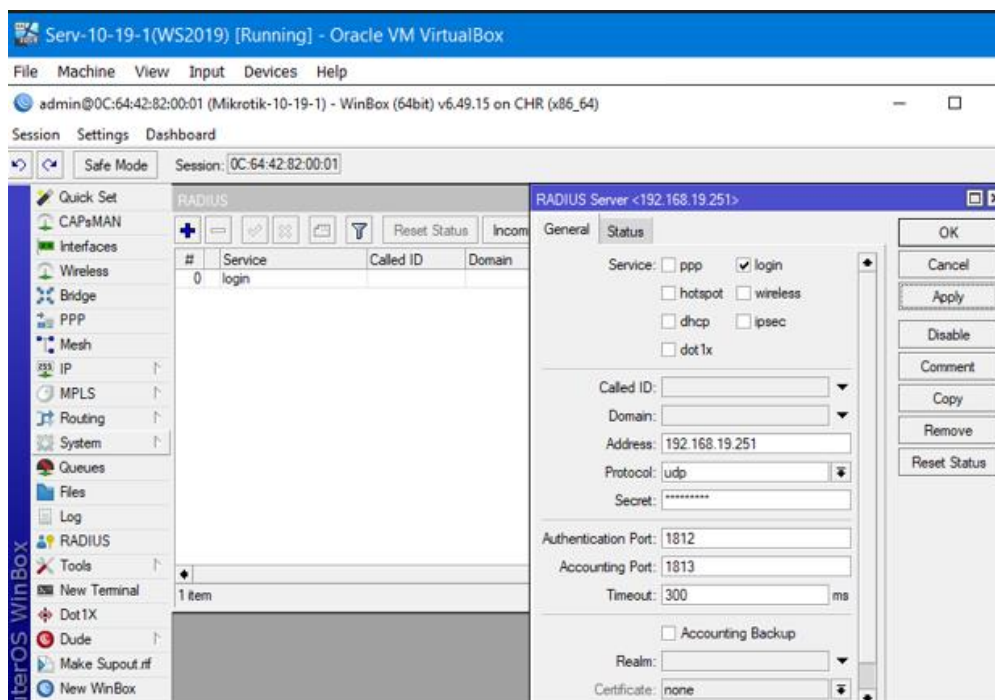


Рисунок 3.41 – Налаштування Radius-клієнта на Mikrotik

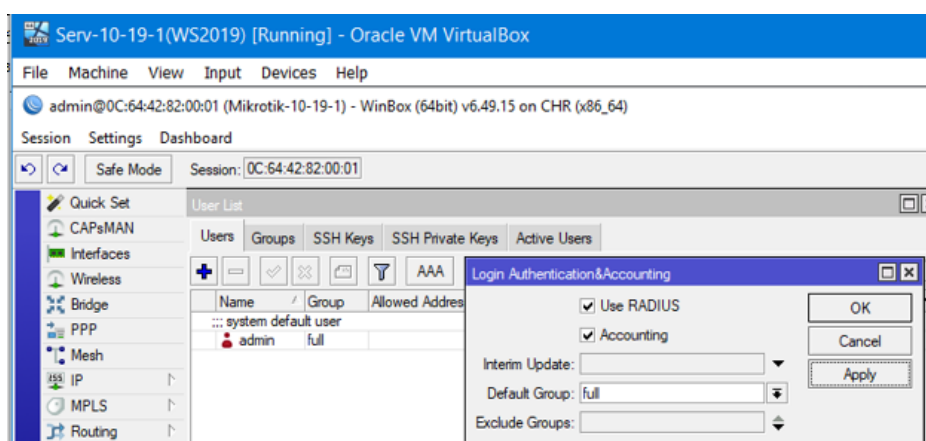


Рисунок 3.42 – Налаштування Radius-клієнта на Mikrotik

Після налаштування, необхідно перевірити, чи працює RADIUS-клієнт на комутаторі належним чином. Це можна зробити шляхом спроби автентифікації з різних пристроїв та перевірки логів на сервері.



Рисунок 3.43 – Перевірка роботи Radius-клієнта на комутаторі

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

Аналогічну перевірку проводимо для маршрутизатора Mikrotik. Переконайтеся, що всі налаштування виконані правильно і автентифікація проходить успішно.

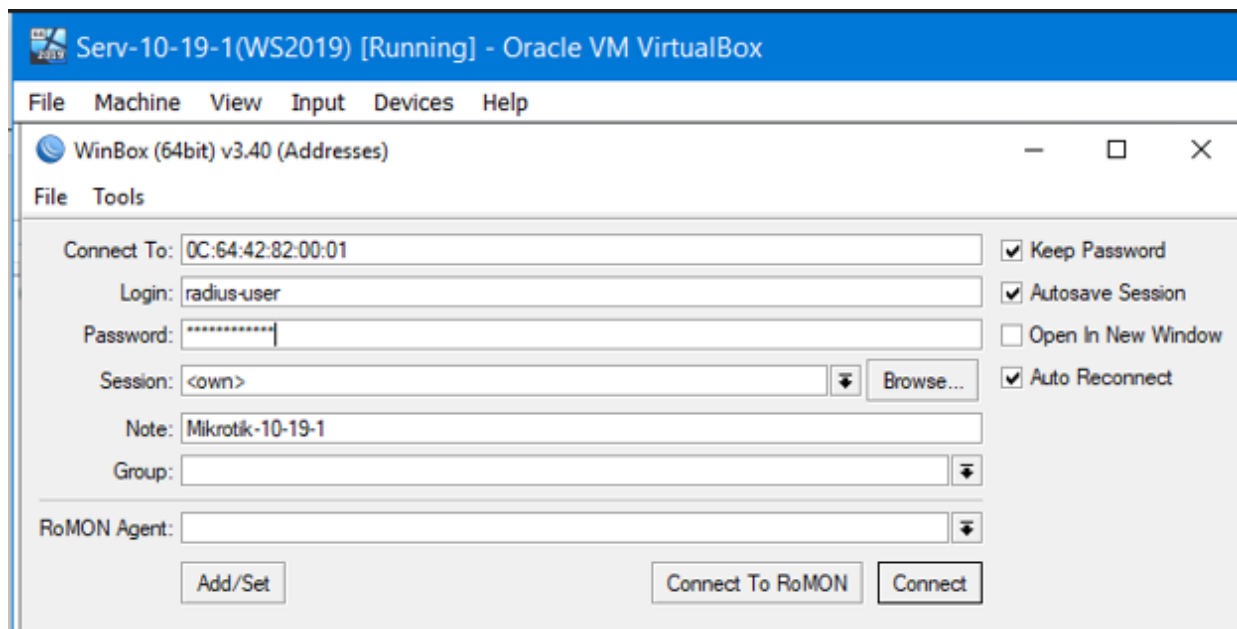


Рисунок 3.44 – Перевірка роботи Radius-клієнта на Mikrotik

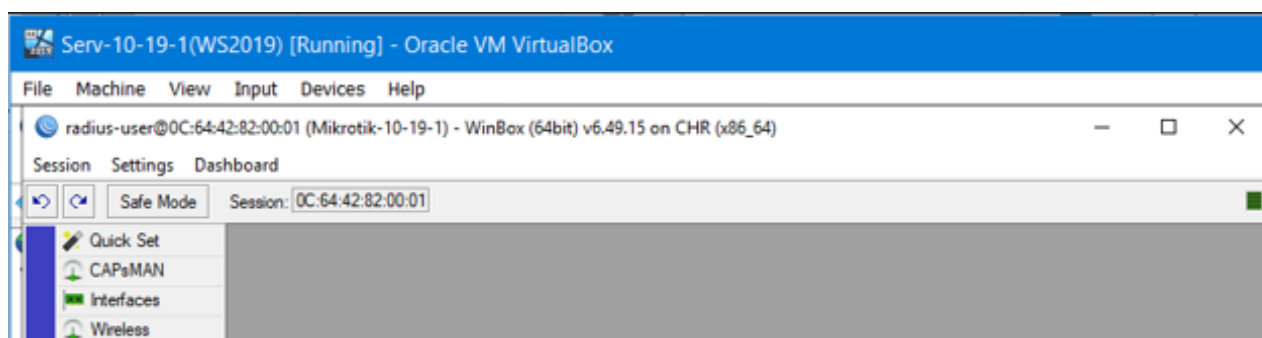


Рисунок 3.45 – Перевірка роботи Radius-клієнта на Mikrotik

Регулярна перевірка подій та логів на RADIUS-сервері допомагає виявити можливі проблеми з автентифікацією або спроби несанкціонованого доступу.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		73

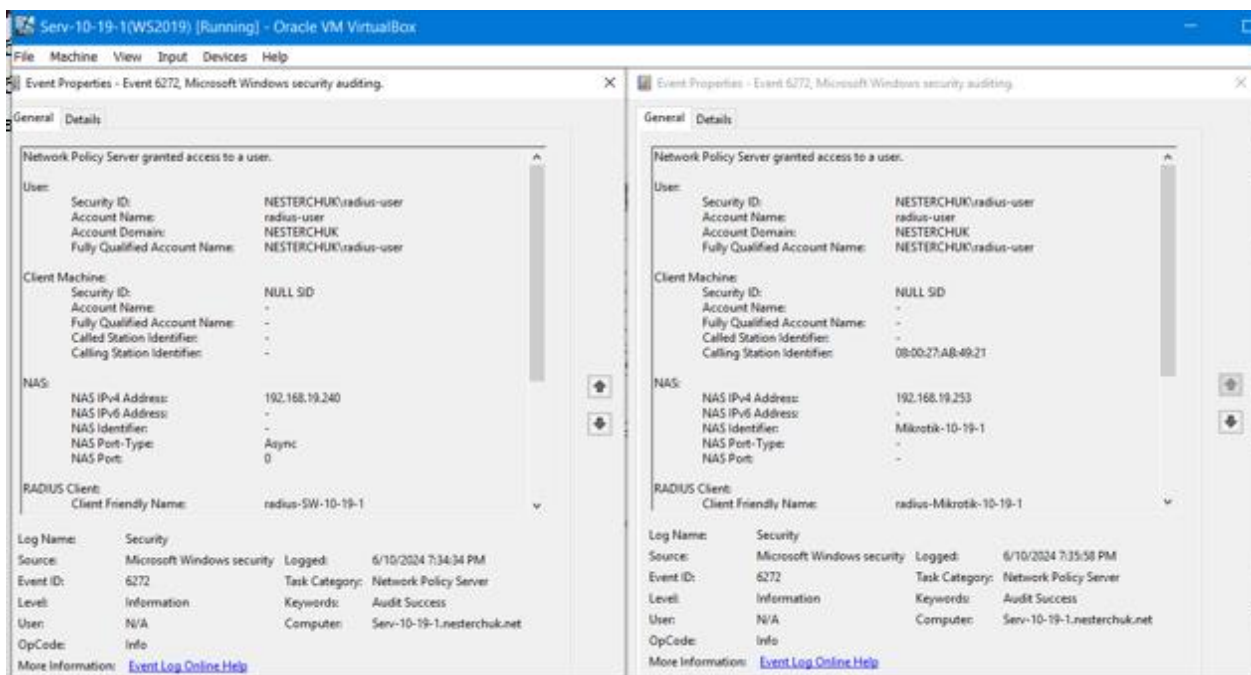


Рисунок 3.46 – Перевірка подій Radius-сервера

SSH дозволяє безпечно підключатися до комутатора для адміністрування. Потрібно налаштувати SSH-сервер на комутаторі та створити ключі для автентифікації.

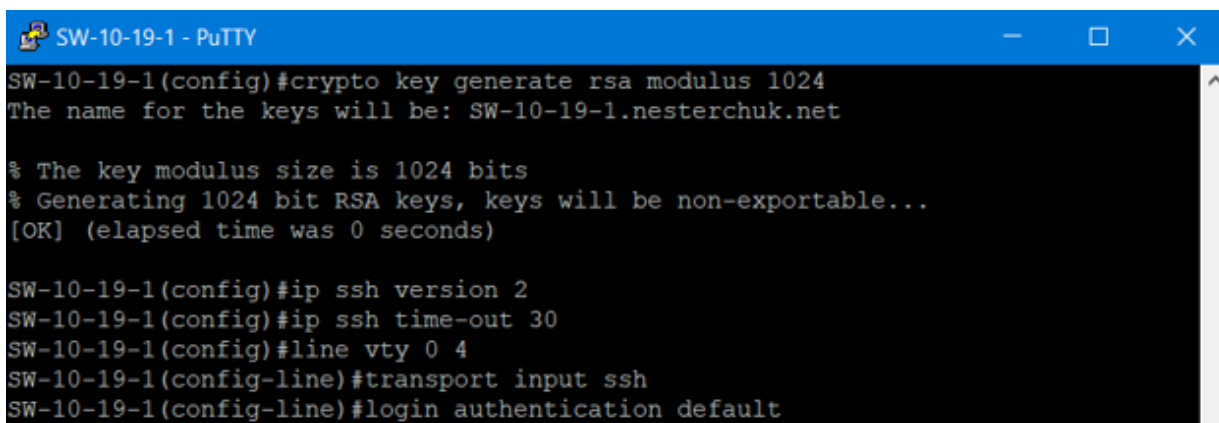


Рисунок 3.47 – Налаштування SSH на комутаторі

Після налаштування, перевірте підключення до комутатора через SSH, використовуючи відповідні клієнтські програми. Це забезпечує безпечний доступ до конфігураційних налаштувань пристрою.

```

Serv-10-19-1(WS2019) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

OpenSSH SSH client

PS C:\Users\Administrator> ssh radius-user@SW-10-19-1
The authenticity of host 'sw-10-19-1 (192.168.19.240)' can't be established.
RSA key fingerprint is SHA256:4UBIIFR67xb58QXvhaa/18Z9U+gYvIMy9CoFCj5FZ0Y.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'sw-10-19-1,192.168.19.240' (RSA) to the list of known hosts.
Password:

SW-10-19-1>enable
Password:
SW-10-19-1#show run
SW-10-19-1#show running-config
Building configuration...

Current configuration : 2392 bytes
!
! Last configuration change at 22:42:48 EEST Thu Jun 13 2024 by radius-user
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-10-19-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5 $1$bTcC$LBCFFydKF9Tdefc0bje6T0
!
username radius privilege 15 secret 5 $1$04bX$eZ/1/M/aJfwjpD44j05if/
aaa new-model
!
!
aaa authentication login default group radius local
aaa authorization console
aaa authorization exec default group radius local if-authenticated
!
!

```

Рисунок 3.48 – Підключення через SSH до комутатора

Port Security дозволяє обмежити кількість пристроїв, що можуть підключатися до певного порту комутатора, та запобігає несанкціонованим підключенням.

```

SW-10-19-3 - PuTTY

SW-10-19-3(config)#int range eth0/0-3
SW-10-19-3(config-if-range)#switchport mode access
SW-10-19-3(config-if-range)#switchport port-security
SW-10-19-3(config-if-range)#switchport port-security maximum 1
SW-10-19-3(config-if-range)#switchport port-security mac-address sticky
SW-10-19-3(config-if-range)#switchport port-security violation shutdown
SW-10-19-3(config-if-range)#exit
SW-10-19-3(config)#int range eth3/1-3
SW-10-19-3(config-if-range)#switchport mode access
SW-10-19-3(config-if-range)#switchport port-security
SW-10-19-3(config-if-range)#switchport port-security maximum 10
SW-10-19-3(config-if-range)#switchport port-security violation shutdown

```

Рисунок 3.49 – Налаштування параметрів Port Security

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

```

SW-10-19-3#show port-security int eth0/0
Port Security                : Enabled
Port Status                  : Secure-up
Violation Mode               : Shutdown
Aging Time                   : 0 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 1
Total MAC Addresses          : 0
Configured MAC Addresses     : 0
Sticky MAC Addresses         : 0
Last Source Address:Vlan     : 0000.0000.0000:0
Security Violation Count     : 0

```

Рисунок 3.50 – Перевірка налаштувань Port Security на інтерфейсі

DHCP Snooping допомагає запобігти атакам типу "DHCP Spoofing" шляхом перевірки DHCP-повідомлень. Потрібно налаштувати цю функцію на комутаторі для додаткової безпеки.

```

SW-10-19-3(config)#ip dhcp snooping
SW-10-19-3(config)#ip dhcp snooping vlan 1
SW-10-19-3(config)#int range eth3/1-3
SW-10-19-3(config-if-range)#ip dhcp snooping trust
SW-10-19-3(config-if-range)#exit
SW-10-19-3(config)#int range eth0/0-3, eth1/0-3, eth2/0-3
SW-10-19-3(config-if-range)#ip dhcp snooping limit rate 15

```

Рисунок 3.51 – Налаштування DHCP Snooping на комутаторі

Після налаштування, перевірте правильність роботи DHCP Snooping, відслідковуючи DHCP-трафік та перевіряючи лог-файли.

```

SW-10-19-3#show ip dhcp snooping
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:

DHCP snooping is operational on following VLANs:

DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: aabb.cc00.0200 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface          Trusted    Allow option    Rate limit (pps)
-----
Ethernet0/0        no        no              15
  Custom circuit-ids:
Ethernet0/1        no        no              15
  Custom circuit-ids:
Ethernet0/2        no        no              15
Interface          Trusted    Allow option    Rate limit (pps)
-----
  Custom circuit-ids:
Ethernet0/3        no        no              15
  Custom circuit-ids:
Ethernet1/0        no        no              15
  Custom circuit-ids:
Ethernet1/1        no        no              15
  Custom circuit-ids:
Ethernet1/2        no        no              15
  Custom circuit-ids:
Ethernet1/3        no        no              15
  Custom circuit-ids:
Ethernet2/0        no        no              15
  Custom circuit-ids:
Ethernet2/1        no        no              15
  Custom circuit-ids:
Ethernet2/2        no        no              15
  Custom circuit-ids:
Ethernet2/3        no        no              15
  Custom circuit-ids:
Ethernet3/1        yes        yes             unlimited
  Custom circuit-ids:

```

Рисунок 3.52 – Перевірка параметрів DHCP Snooping

Port Fast, BPDU Guard та BPDU Filtering допомагають забезпечити швидке підключення кінцевих пристроїв та запобігають можливим петлям у мережі. Налаштуйте ці функції на відповідних портах комутатора.

```

SW-10-19-3 - PuTTY
SW-10-19-3(config)#int range eth0/0-2
SW-10-19-3(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast will be configured in 3 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
SW-10-19-3(config-if-range)#exit
SW-10-19-3(config)#spanning-tree portfast bpduguard default
SW-10-19-3(config)#spanning-tree portfast bpduguard default

```

Рисунок 3.53 – Налаштування Port Fast, BPDU Guard та BPDU Filtering

Перегляньте конфігурацію STP та впевніться, що всі функції безпеки налаштовані правильно. Це допомагає забезпечити стабільну роботу мережі.

```

SW-10-19-3 - PuTTY
SW-10-19-3#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default              is disabled
Portfast Edge BPDU Guard Default is enabled
Portfast Edge BPDU Filter Default is enabled
Loopguard Default             is disabled
PVST Simulation Default       is enabled but inactive in pvst mode
Bridge Assurance               is enabled but inactive in pvst mode
EtherChannel misconfig guard  is enabled
Configured Pathcost method used is short
UplinkFast                    is disabled
BackboneFast                   is disabled

Name                           Blocking Listening Learning Forwarding STP Active
-----
VLAN0001                       0           0           0           16           16
1 vlan                          0           0           0           16           16

```

Рисунок 3.54 – Перегляд загальної інформації про STP та налаштовані функції безпеки

Syslog дозволяє централізовано зберігати логи подій з різних пристроїв. Налаштували комутатор для відправки логів на Syslog-сервер.

```

SW-10-19-1 - PuTTY
SW-10-19-1(config)#service timestamps log datetime
SW-10-19-1(config)#logging Serv-10-19-1
SW-10-19-1(config)#logging trap notifications

```

Рисунок 3.55 – Налаштування Syslog на комутаторі

Також налаштували маршрутизатор Mikrotik для відправки логів на той самий Syslog-сервер. Це допоможе централізовано моніторити події в мережі.

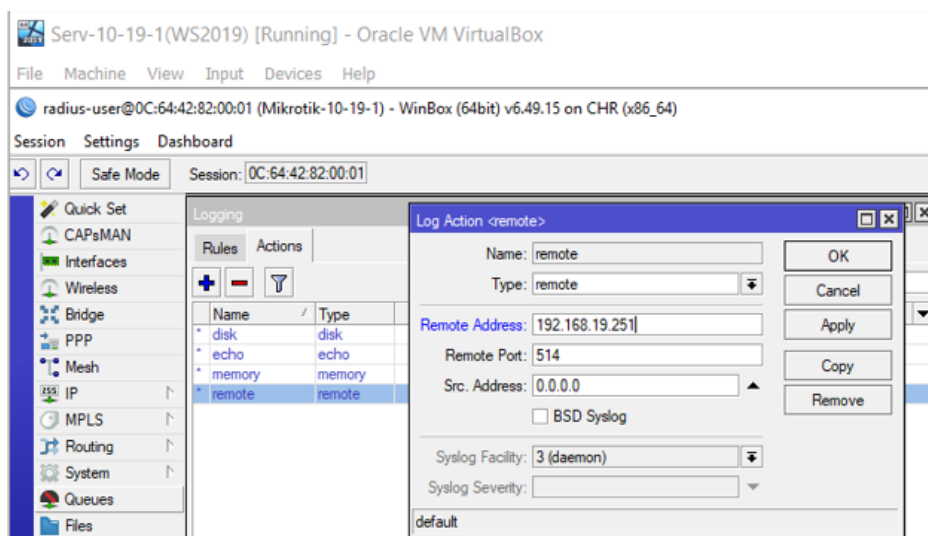


Рисунок 3.56 – Налаштування Syslog на Mikrotik

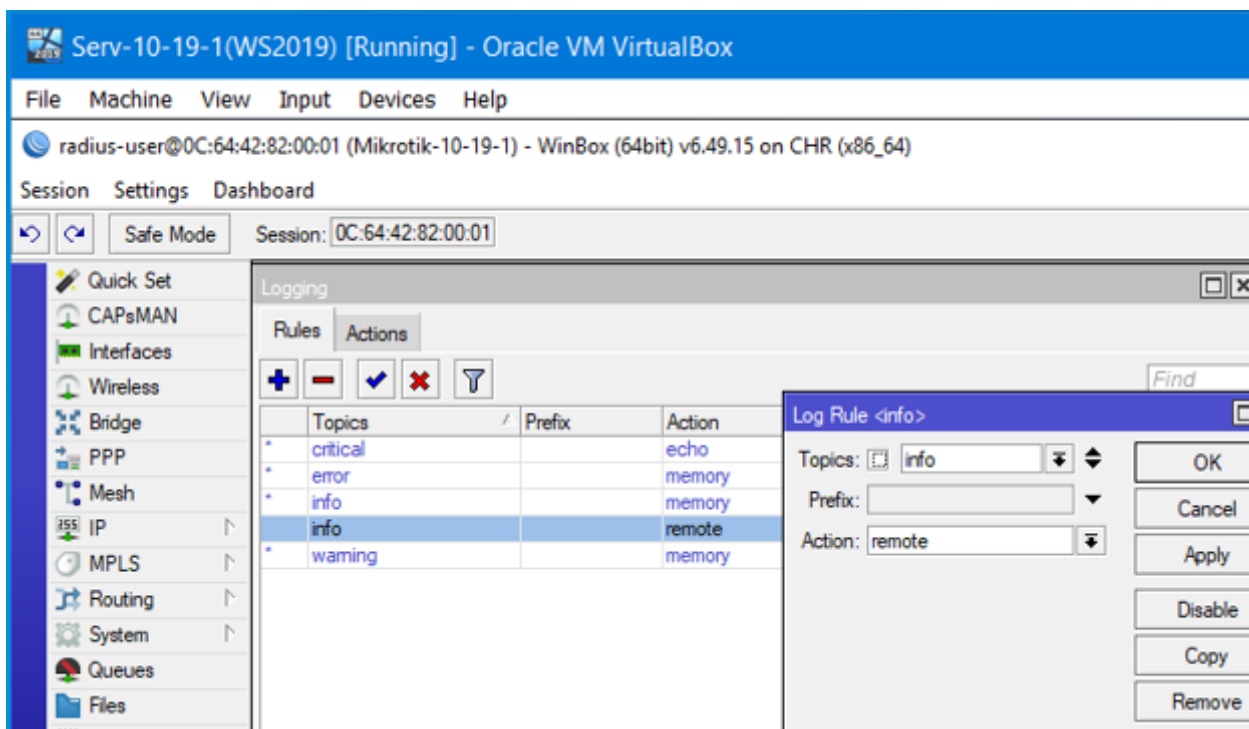


Рисунок 3.57 – Налаштування Syslog на Mikrotik

Перевірили, чи правильно надходять логи з комутатора та Mikrotik на Syslog-сервер. Це дозволить своєчасно виявляти та реагувати на мережеві події та можливі проблеми.

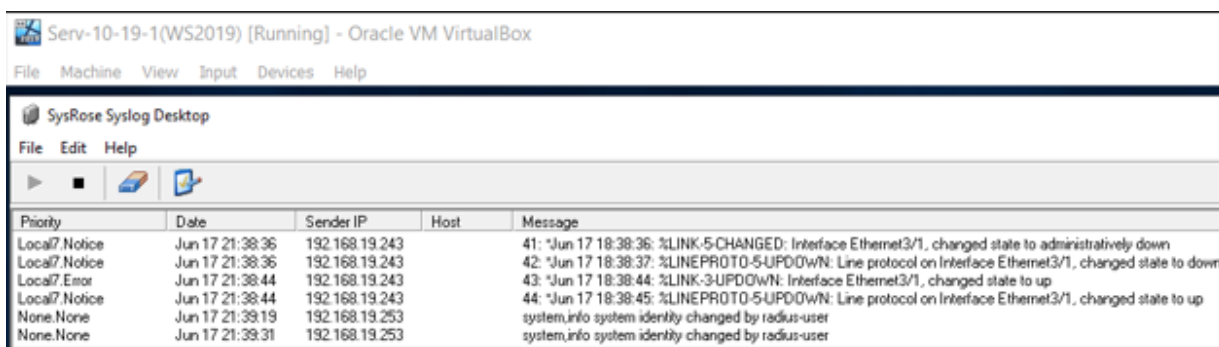


Рисунок 3.58 – Отримані сповіщення на Syslog сервері

Фаєрвол на Mikrotik допомагає захистити мережу від несанкціонованих доступів. Налаштуйте стандартні правила фаєрволу для базового захисту.

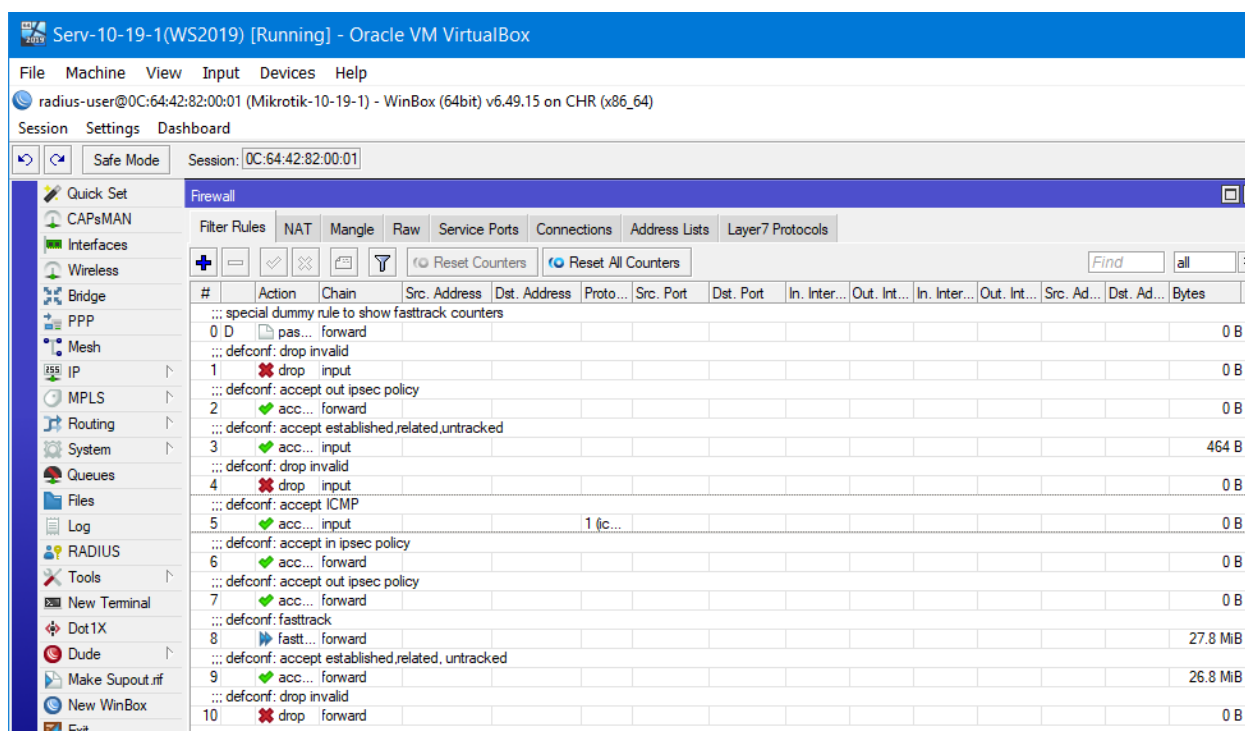


Рисунок 3.59 – Стандартні правила фаєрвол на Мікротік

Для обмеження доступу до певних веб-сайтів (наприклад, YouTube, Reddit, Netflix, Facebook), додали відповідні правила в фаєрвол на Mikrotik.

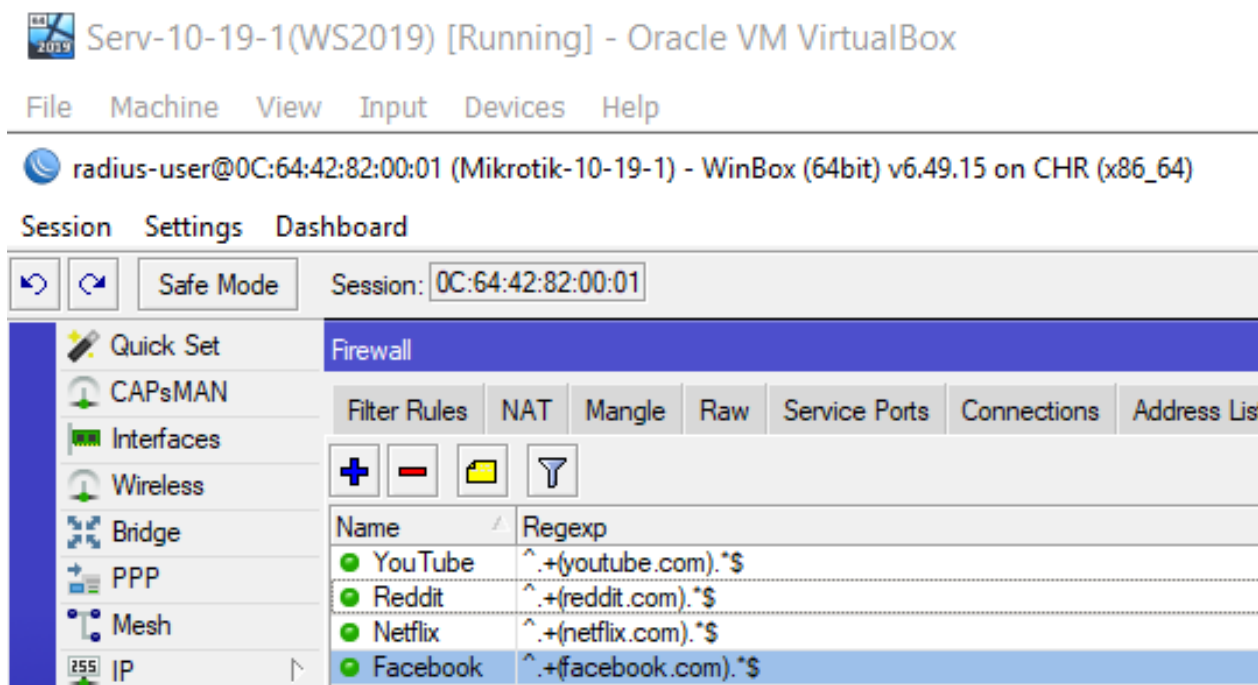


Рисунок 3.60 – Вказання сайтів які будуть заблоковані для доступу

Створили та налаштували правила фаєрволу на Mikrotik для блокування доступу до вказаних веб-сайтів. Це може бути зроблено через Winbox.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

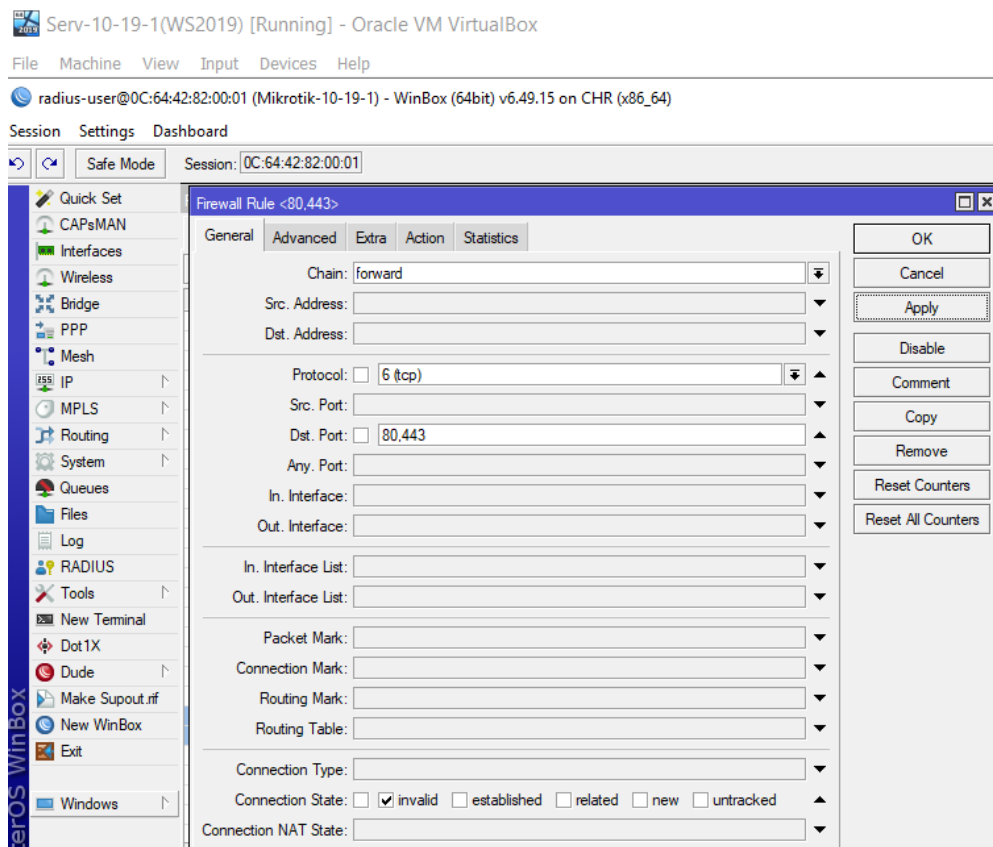


Рисунок 3.61 – Налаштування правила фаєрвол для блокування

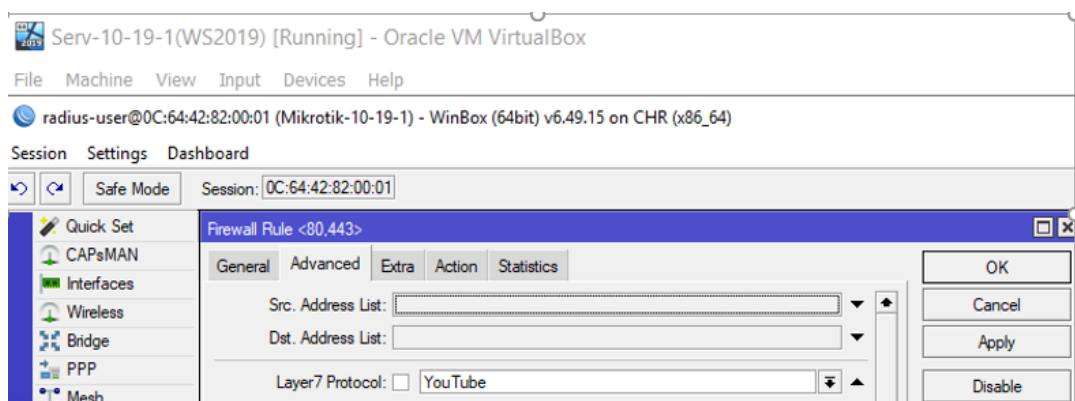


Рисунок 3.62 – Налаштування правила фаєрвол для блокування

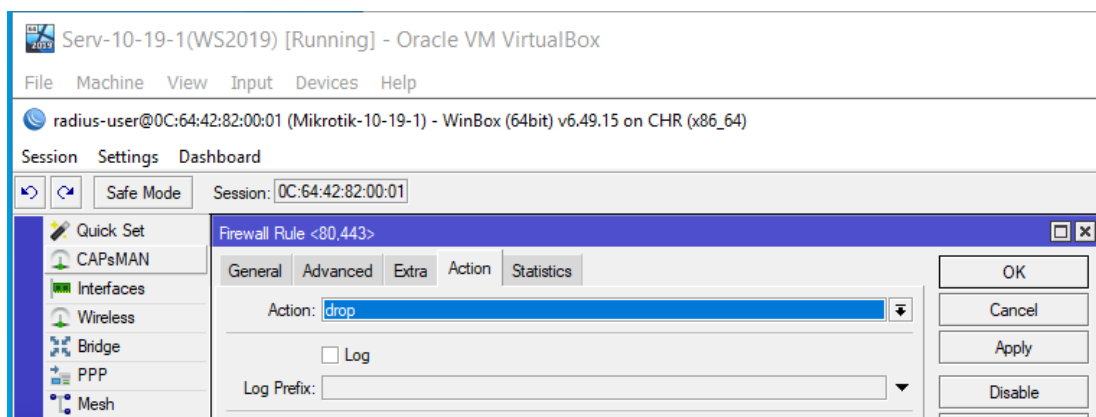


Рисунок 3.63 – Налаштування правила фаєрвол для блокування

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

3.4 Тестування роботи підсистеми захисту мережі

Розпочнемо перевірку з роботи аутентифікації протоколу VRRP. За допомогою мережевого аналізатора Wireshark виконаємо перехоплення трафіку між Mikrotik-1 та SW-1 і відфільтруємо пакети за протоколом VRRP. В полі «Auth Type» є значення «IP Authentication Header» (IP заголовок аутентифікації). Даний метод аутентифікації дозволяє ідентифікувати відправника даних і забезпечити цілісність даних. Завдяки цьому зломиснику буде значно важче виконати підробку трфіку VRRP.

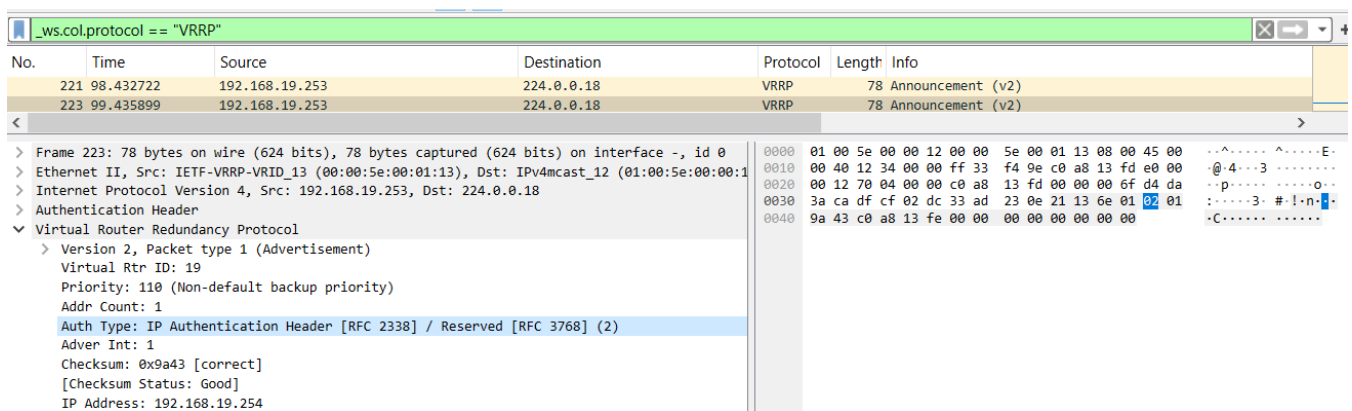


Рисунок 3.64 – Перехоплені пакети VRRP

Переходимо до перевірки Port Security. Відключимо легальну станцію WS-10-19-4 та замість неї підключимо комп'ютер зломисника (Hacker)

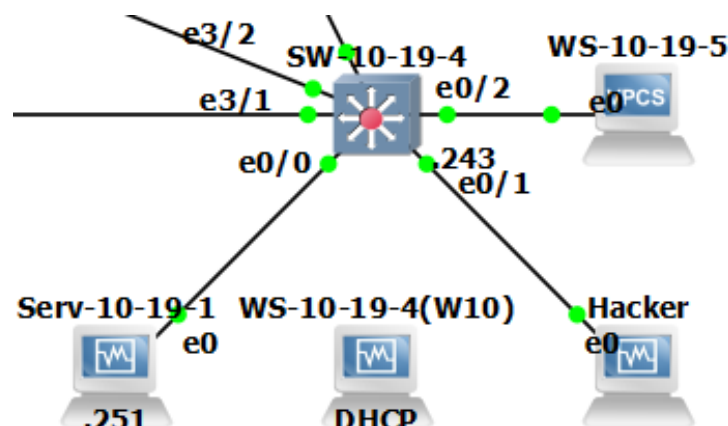


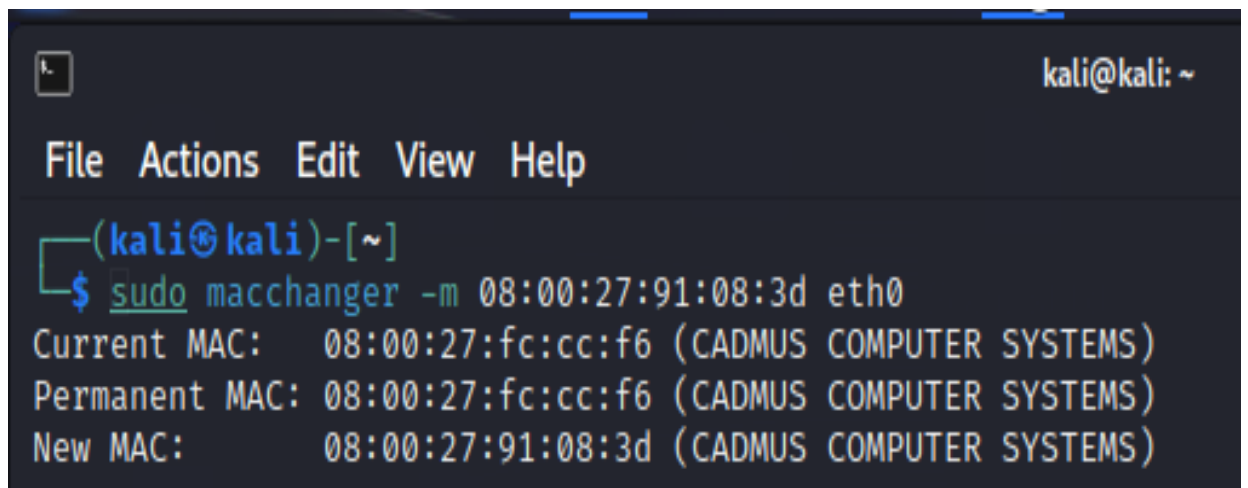
Рисунок 3.65 – Підключення станції зломисника Hacker замість легальної станції WS-10-19-4

На комутатор надійшло сповіщення про спрацювання функції Port Security на інтерфейсі eth0/1 (до якого і підключений Hacker). Відповідно до налаштованої реакції Port Security даний інтерфейс переходить в стан err-disable і вимикається.

```
SW-10-19-4#
*Jun 18 11:14:39: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/1,
putting Et0/1 in err-disable state
SW-10-19-4#
*Jun 18 11:14:39: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address 0800.27fc.ccf6 on port Ethernet0/1.
*Jun 18 11:14:40: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1,
changed state to down
SW-10-19-4#
*Jun 18 11:14:41: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to down
SW-10-19-4#
```

Рисунок 3.66 – Повідомлення на комутаторі

Припустим, що зловмисник дізнався MAC-адресу легальної станції і підмінив свою адресу на допустиму. Тим самим обійшовши функцію Port Security.



```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ sudo macchanger -m 08:00:27:91:08:3d eth0
Current MAC: 08:00:27:fc:cc:f6 (CADMUS COMPUTER SYSTEMS)
Permanent MAC: 08:00:27:fc:cc:f6 (CADMUS COMPUTER SYSTEMS)
New MAC: 08:00:27:91:08:3d (CADMUS COMPUTER SYSTEMS)
```

Рисунок 3.67 – Підміна MAC-адреси станції зловмисника на легальну

Тепер зловмисник спробує провести STP DOS атаки з використанням інструменту Yersinia.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				83
Змн.	Арк.	№ докум.	Підпис	Дата		

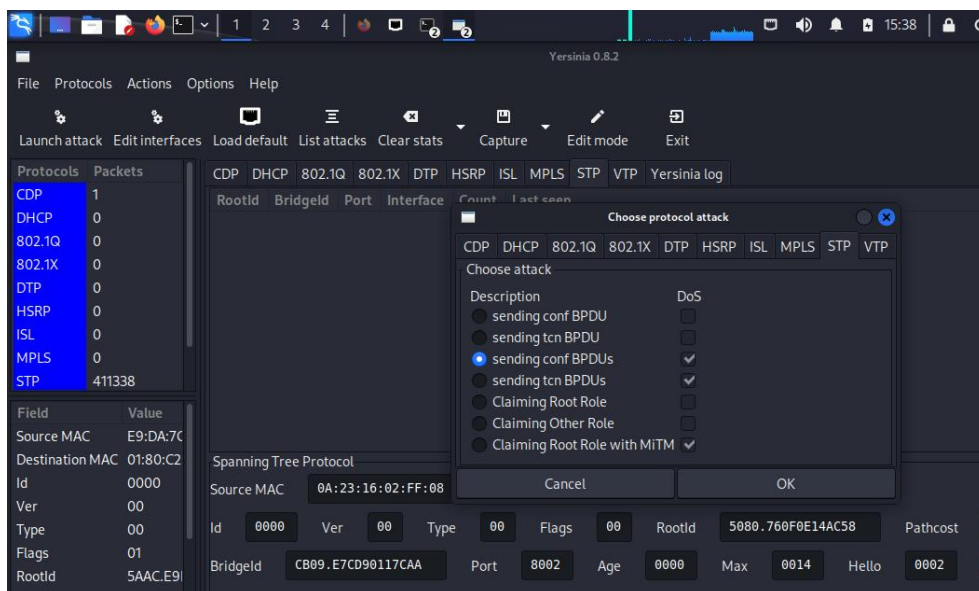


Рисунок 3.68 – Проведення атаки STP DOS

Однак знову тут спрацює функція Port Security і даний порт вимкнеться.

```
SW-10-19-4#
*Jun 18 12:40:41: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/1,
putting Et0/1 in err-disable state
SW-10-19-4#
*Jun 18 12:40:41: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurre
d, caused by MAC address 06c4.5773.bf9a on port Ethernet0/1.
*Jun 18 12:40:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, c
hanged state to down
SW-10-19-4#
*Jun 18 12:40:48: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to down
SW-10-19-4#
```

Рисунок 3.69 – Повідомлення на комутаторі

Тепер зломисник спробує провести атаку типу DHCP Starvation/DHCP Exhaustion з використанням все тієї ж утиліти Yersinia.

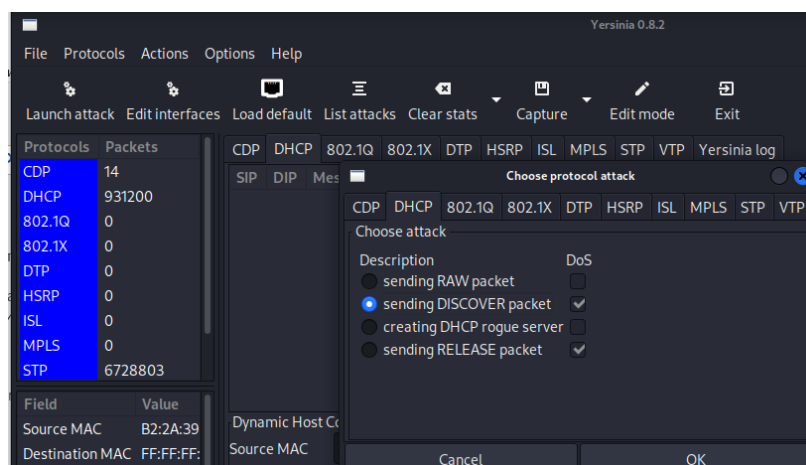


Рисунок 3.70 – Проведення атаки DHCP Starvation/DHCP Exhaustion

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		84

Однак і цього разу атака вийшла невдалою, бо на комутаторі одночасно спрацювали функцію Port Security і DHCP Snooping і інтерфейс знову вимкнувся.

```
SW-10-19-4#
*Jun 18 12:45:04: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/1,
putting Et0/1 in err-disable state
*Jun 18 12:45:04: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
caused by MAC address a696.194e.c1be on port Ethernet0/1.
SW-10-19-4#
*Jun 18 12:45:04: %DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE_WARNING: DHCP Snooping
received 15 DHCP packets on interface Et0/1
*Jun 18 12:45:04: %DHCP_SNOOPING-4-DHCP_SNOOPING_RATE_LIMIT_EXCEEDED: The interface
Et0/1 is receiving more than the threshold set
*Jun 18 12:45:05: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1,
changed state to down
SW-10-19-4#
*Jun 18 12:45:06: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to down
```

Рисунок 3.71 – Повідомлення на комутаторі

Перейдемо до серверу Serv-1 та переглянемо отримані повідомлення на Syslog сервері. Як видно тут зібрані всі повідомлення від комутатора SW-10-19-4 (192.168.19.243) що були отримані протягом всіх спроб проведення невдалих атак. Подібні інформація може бути використано адміністраторами мережі для проведення подальших розслідувань з виявлення та нейтралізації загрози.

Serv-10-19-1(W52019) [Running] - Oracle VM VirtualBox					
File Machine View Input Devices Help					
SysRose Syslog Desktop					
File Edit Help					
Priority	Date	Sender IP	Host	Message	
Local7/Notice	Jun 18 14:14:01	192.168.19.243		56: *Jun 18 11:14:03: %SYS-5-CONFIG_I: Configured from console by radius-user on console	
Local7/Warning	Jun 18 14:14:37	192.168.19.243		57: *Jun 18 11:14:39: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/1, putting Et0/1 in err-disable state	
Local7/Critical	Jun 18 14:14:38	192.168.19.243		58: *Jun 18 11:14:39: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0800.27fc.ccf6 on port Ethernet0/1.	
Local7/Notice	Jun 18 14:14:39	192.168.19.243		59: *Jun 18 11:14:40: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down	
Local7/Error	Jun 18 14:14:40	192.168.19.243		60: *Jun 18 11:14:41: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to down	
Local7/Notice	Jun 18 14:19:49	192.168.19.243		61: *Jun 18 11:19:52: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up	
Local7/Notice	Jun 18 14:19:51	192.168.19.243		62: *Jun 18 11:19:52: %SYS-5-CONFIG_I: Configured from console by radius-user on console	
Local7/Warning	Jun 18 15:40:38	192.168.19.243		63: *Jun 18 12:40:41: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up	
Local7/Critical	Jun 18 15:40:46	192.168.19.243		64: *Jun 18 12:40:41: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/1, putting Et0/1 in err-disable state	
Local7/Warning	Jun 18 15:40:46	192.168.19.243		65: *Jun 18 12:40:41: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 06c4.5773.bf3a on port Ethernet0/1.	
Local7/Notice	Jun 18 15:40:53	192.168.19.243		66: *Jun 18 12:40:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down	
Local7/Notice	Jun 18 15:43:04	192.168.19.243		67: *Jun 18 12:40:48: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to down	
Local7/Notice	Jun 18 15:43:05	192.168.19.243		68: *Jun 18 12:43:06: %SYS-5-CONFIG_I: Configured from console by radius-user on console	
Local7/Warning	Jun 18 15:43:05	192.168.19.243		69: *Jun 18 12:43:07: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up	
Local7/Warning	Jun 18 15:45:01	192.168.19.243		70: *Jun 18 12:43:08: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up	
Local7/Critical	Jun 18 15:45:01	192.168.19.243		71: *Jun 18 12:45:04: %PM-4-ERR_DISABLE: psecure-violation error detected on Et0/1, putting Et0/1 in err-disable state	
Local7/Warning	Jun 18 15:45:03	192.168.19.243		72: *Jun 18 12:45:04: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address a696.194e.c1be on port Ethernet0/1.	
Local7/Warning	Jun 18 15:45:03	192.168.19.243		73: *Jun 18 12:45:04: %DHCP_SNOOPING-4-DHCP_SNOOPING_ERRDISABLE_WARNING: DHCP Snooping received 15 DHCP packets on interface Et0/1	
Local7/Notice	Jun 18 15:45:03	192.168.19.243		74: *Jun 18 12:45:05: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to down	
Local7/Notice	Jun 18 15:45:10	192.168.19.243		75: *Jun 18 12:45:06: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to down	

Рисунок 3.72 – Зібрані повідомлення на Syslog сервері

Тепер перейдемо до кінцевих станцій. Спробуємо перейти на сайт «youtube.com», однак сторінка не прогружається. Пов'язано це з налаштованими правилами фаєрвол на маршрутизаторах Mikrotik, які забороняють доступ до зазначених соціальних сторінок і розважальних сайтів серед яких Youtube, Reddit, Netflix та Facebook. Однак не заборонені сайти успішно відображаються.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				85
Змн.	Арк.	№ докум.	Підпис	Дата		

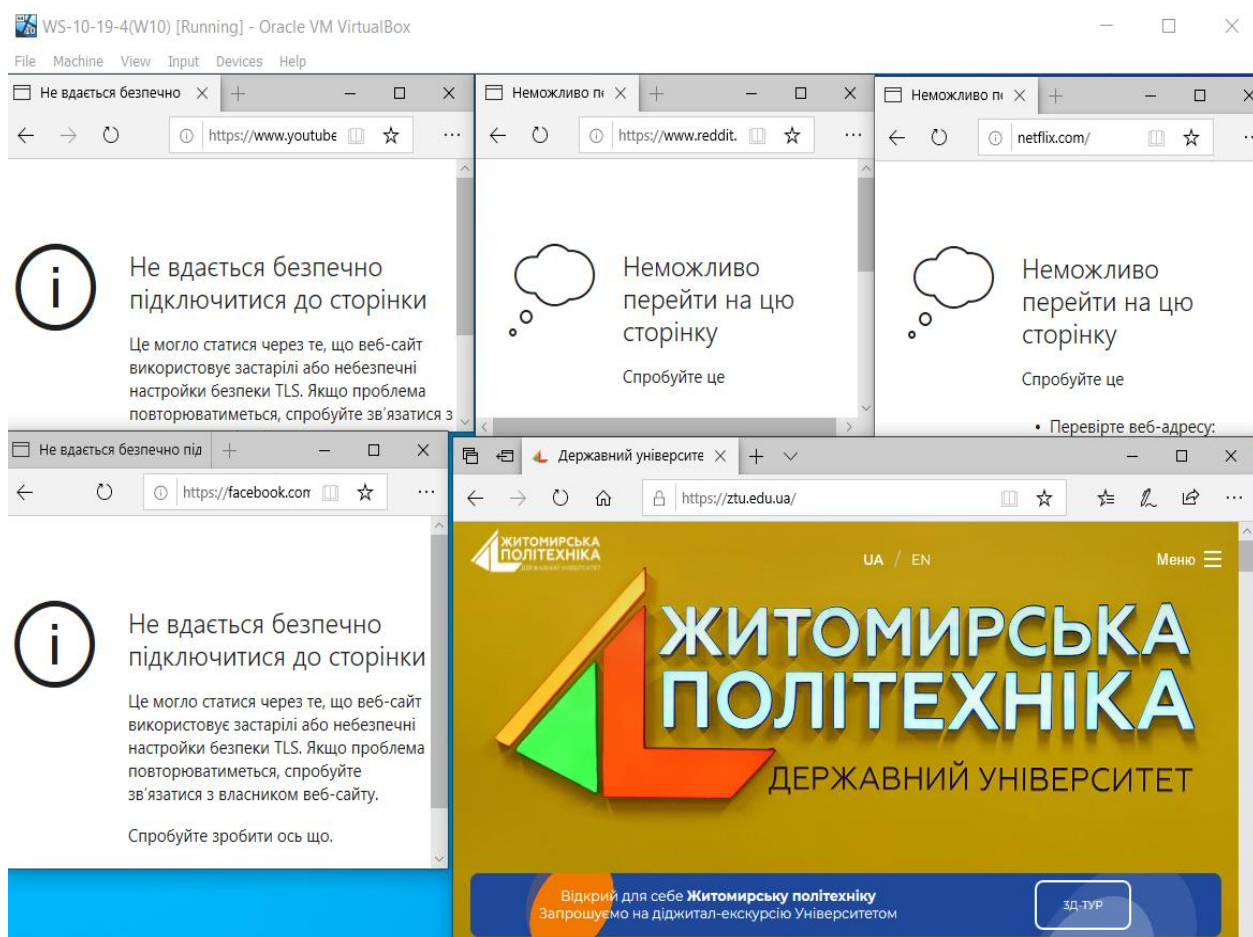


Рисунок 3.73 – Доступ до заблокованих сайтів заборонений

Якщо на Mikrotik перейти в пункт налаштування фаєрвола, то помітимо налаштовані правила блокування веб-ресурсів із зазначенням кількості байтів та пакетів, які були відкинуті.

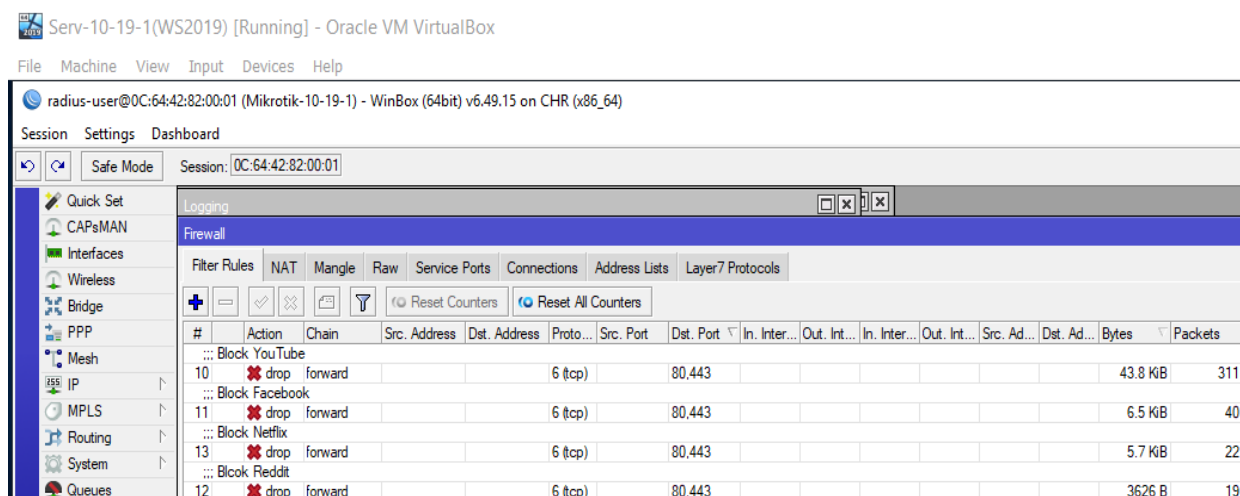


Рисунок 3.74 – Перегляд роботи правил фаєрвол

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

Висновки до третього розділу:

В розділі 3 було проведено комплексне налаштування мережевої інфраструктури, яке включало базове налагодження пристроїв мережі, конфігурацію Active Directory і робочих станцій, налаштування підсистеми захисту та тестування її ефективності. Спочатку було здійснено налаштування основних мережевих пристроїв, що забезпечило стабільну та ефективну роботу мережі. Наступним кроком стало створення домену nesterchuk.net, налаштування служб DNS та DHCP, що дозволило централізовано керувати користувачами та ресурсами мережі. Було підключено клієнтські станції з різними операційними системами до домену, забезпечивши їх автоматичне отримання IP-адрес. Далі була налаштована підсистема захисту, включаючи RADIUS-сервер, політики безпеки для мережевих пристроїв, а також функції Port Security, DHCP Snooping, STP та Syslog. Завершальним етапом стало тестування роботи підсистеми захисту, яке підтвердило її ефективність та надійність. Проведені заходи забезпечили високий рівень безпеки та стабільну роботу мережі, що дозволяє організації ефективно функціонувати в сучасному мережевому середовищі.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		87

ВИСНОВКИ

У даному дипломному проекті було виконано комплексне дослідження та налагодження гетерогенної мережі з метою забезпечення її надійної та безпечної роботи.

У першому розділі було розглянуто теоретичні аспекти побудови та функціонування гетерогенних мереж. Зокрема, було досліджено протоколи і функції захисту канального рівня, протокол резервування шлюзу VRRP, стандарт відправки і реєстрації подій Syslog, протокол аутентифікації та авторизації Radius, а також принципи роботи міжмережевих екранів. Це дослідження забезпечило глибоке розуміння ключових технологій і протоколів, необхідних для ефективного управління та захисту мереж.

У другому розділі була розроблена топологія комп'ютерної мережі, обрано відповідне обладнання та створено систему адресації. Також було розроблено підсистему захисту гетерогенної мережі організації. Це включало в себе вибір і налаштування маршрутизаторів, комутаторів, серверів і клієнтських станцій, забезпечуючи інтеграцію різних операційних систем і пристроїв у єдину мережу з централізованим управлінням.

Третій розділ був присвячений налагодженню та тестуванню підсистеми захисту мережі. Було проведено базове налагодження пристроїв мережі, налаштовано Active Directory і робочі станції, впроваджено підсистему захисту, яка включає налаштування RADIUS-сервера, політик безпеки для мережеских пристроїв, функцій Port Security, DHCP Snooping, STP та Syslog. Проведене тестування підтвердило ефективність і надійність налаштувань, забезпечуючи стабільну роботу мережі та високий рівень безпеки.

Загалом, виконана робота продемонструвала високу ефективність розробленої підсистеми захисту для гетерогенної мережі, забезпечуючи відповідність сучасним стандартам інформаційної безпеки та захист від кіберзагроз. Реалізація даного проекту сприяла підвищенню рівня безпеки даних, стабільності роботи мережі та довіри клієнтів і партнерів до організації.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		88

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

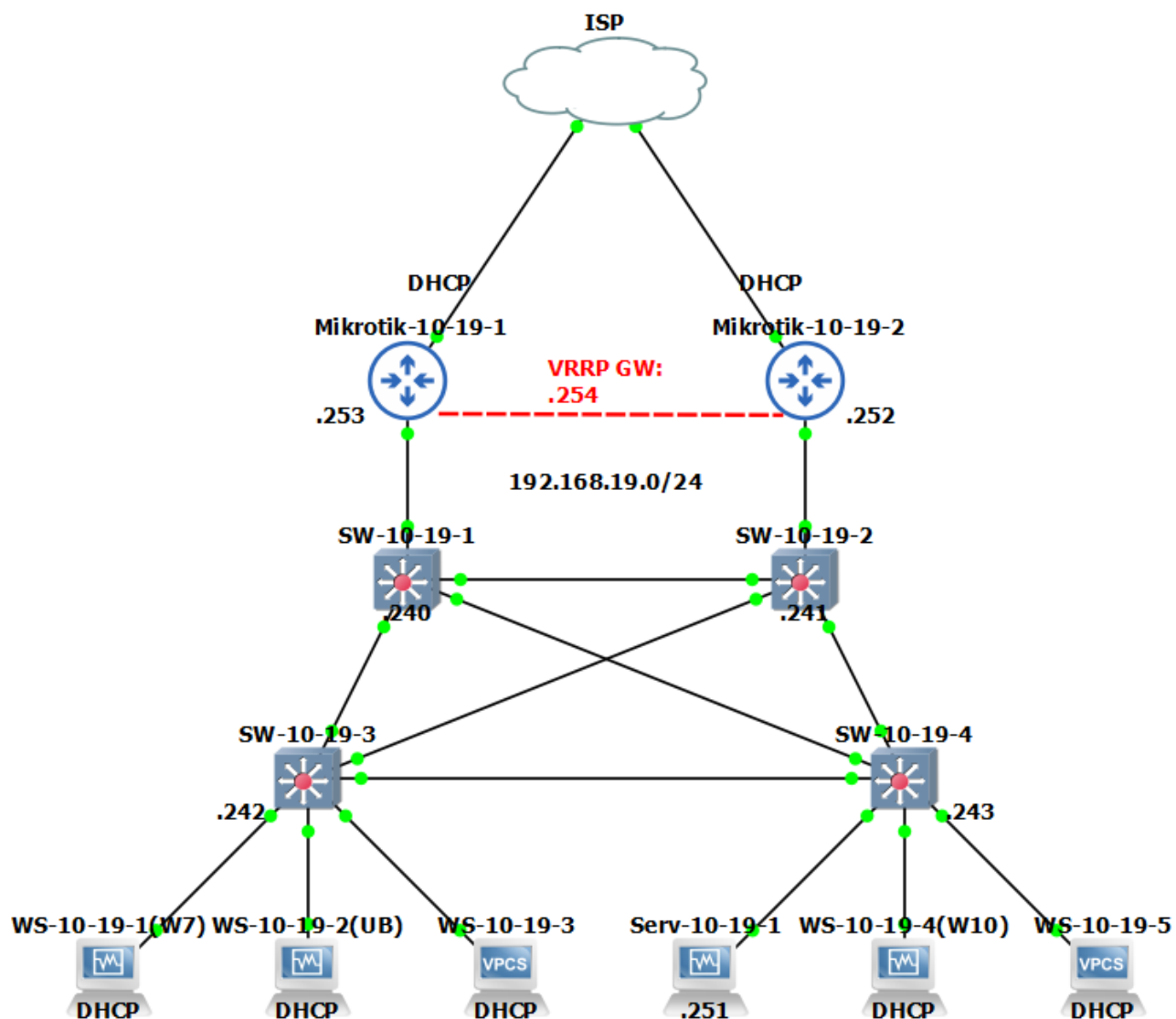
1. Що Таке Міжмережєвий Екран І Навіщо Він Потрібен? [Електронний ресурс] – Режим доступу до ресурсу: <https://stack-systems.com.ua/blogs/shtcho-take-mizmerezevyj-ekran-i-navishtcho-vin-potriben>
2. MikroTik RB3011UiAS-RM [Електронний ресурс] – Режим доступу до ресурсу: https://www.technotrade.com.ua/Products/MikroTik_RB3011UiAS-RM.php
3. Cisco Systems, Cisco Networking Academy Program [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com>
4. Гетерогенна комп'ютерна мережа [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Гетерогенні_комп'ютерні_мережі
5. Мережева модель ОСІ [Електронний ресурс] – Режим доступу до ресурсу: <https://kr-labs.com.ua/blog/model-osi/>
6. Port security [Електронний ресурс] – Режим доступу до ресурсу: <https://linkmeup.gitbook.io/sdsm/4.-stp/06-port-security>
7. DHCP Snooping [Електронний ресурс] – Режим доступу до ресурсу: <https://fiberroad.com/uk/resources/glossary/what-is-dhcp-snooping-and-why-should-you-use-it/>
8. BPDU GUARD [Електронний ресурс] – Режим доступу до ресурсу: <https://sealan.net.ua/ua/a463801-ataka-zaschita-protokola.html>
9. VRRP Protocol [Електронний ресурс] – Режим доступу до ресурсу: <https://info.support.huawei.com/info-finder/encyclopedia/en/VRRP.html>
10. Захист мережевих інфраструктур [Електронний ресурс] – Режим доступу до ресурсу: <https://www.securityinfrastructure.com>
11. syslog [Електронний ресурс] – Режим доступу до ресурсу: <https://wiki.dieg.info/syslog>
12. Radius [Електронний ресурс] – Режим доступу до ресурсу: <https://info.support.huawei.com/info-finder/encyclopedia/en/RADIUS.html>
13. Chap [Електронний ресурс] – Режим доступу до ресурсу: <https://ru.wikipedia.org/wiki/CHAP>
14. Оліфер В. Комп'ютерні мережі. Принципи, технології, протоколи. – СПб.: Пітер, 2020. – 944 с.
15. Скалий І. Безпека мереж. – К.: Видавничий дім «Києво-Могилянська академія», 2020. – 276 с.

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				89
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

Детальна схема побудованої мережі



		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

```
!
!
ip dhcp snooping vlan 1
ip dhcp snooping
ip domain-name nesterchuk.net
ip name-server 192.168.19.251
ip cef
no ipv6 cef
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
    switchport mode access
    ip dhcp snooping trust
!
interface Ethernet0/1
    switchport mode access
    ip dhcp snooping trust
!
interface Ethernet0/2
    switchport mode access
    ip dhcp snooping trust
!
interface Ethernet0/3
    description UNUSED-PORT-VLAN1001
    switchport access vlan 1001
    switchport mode access
    shutdown
    ip dhcp snooping limit rate 15
!
interface Ethernet1/0
    description UNUSED-PORT-VLAN1001
    switchport access vlan 1001
```

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				92
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet1/1
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet1/2
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet1/3
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet2/0
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet2/1
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet2/2
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet2/3
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet3/0
description UNUSED-PORT-VLAN1001

```

```

switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet3/1
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet3/2
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet3/3
switchport mode access
ip dhcp snooping limit rate 15
!
interface Vlan1
ip address 192.168.19.240
255.255.255.0
!
ip default-gateway 192.168.19.254
ip forward-protocol nd
!
ip http server
!
ip ssh time-out 30
ip ssh version 2
ip ssh server algorithm encryption
aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption
aes128-ctr aes192-ctr aes256-ctr
!
!
no logging trap
logging host 192.168.1.2
logging host 192.168.19.251
!
!
!
radius server Serv-10-19-1
address ipv4 192.168.19.251 auth-
port 1812 acct-port 1813
key WinRadius
!
!
control-plane
!

```

		Нестерчук А.В.			KIK.KP.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```
!
line con 0
    exec-timeout 0 0
    privilege level 15
    logging synchronous
line aux 0
line vty 0 4

SW-10-19-2:

!
! Last configuration change at
15:59:28 EEST Tue Jun 18 2024 by
radius-user
!
version 15.2
service timestamps debug datetime
msec
service timestamps log datetime
no service password-encryption
service compress-config
!
hostname SW-10-19-2
!
boot-start-marker
boot-end-marker
!
logging discriminator EXCESS
severity drops 6 msg-body drops
EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5
$1$9y44$Aaw9yp6fEnvmmmcmBxAYj/
!
username radius privilege 15 secret
5 $1$u9fB$tWjm/3Kc9/nFw8IcS5NEQ/
aaa new-model
!
!
aaa authentication login default
group radius local
aaa authorization exec default group
radius local if-authenticated
!
!
!
!
!
aaa session-id common
clock timezone EEST 3 0
!
!
```

```
transport input ssh
!
ntp server Serv-10-19-1 prefer
!
!
end

!
!
!
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping vlan 1
ip dhcp snooping
ip domain-name nesterchuk.net
ip name-server 192.168.19.251
ip cef
no ipv6 cef
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
    switchport mode access
    ip dhcp snooping trust
!
interface Ethernet0/1
    switchport mode access
    ip dhcp snooping trust
!
interface Ethernet0/2
    switchport mode access
    ip dhcp snooping trust
!
interface Ethernet0/3
```

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

```

description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet1/0
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet1/1
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet1/2
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet1/3
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet2/0
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet2/1
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet2/2
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!

```

```

interface Ethernet2/3
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet3/0
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet3/1
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet3/2
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet3/3
switchport mode access
switchport port-security maximum 20
ip dhcp snooping limit rate 15
!
interface Vlan1
ip address 192.168.19.241
255.255.255.0
!
ip default-gateway 192.168.19.254
ip forward-protocol nd
!
ip tcp synwait-time 5
ip http server
!
ip ssh time-out 30
ip ssh version 2
ip ssh server algorithm encryption
aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption
aes128-ctr aes192-ctr aes256-ctr
!
!
logging trap notifications
logging host 192.168.1.2
logging host 192.168.19.251
!

```

		Нестерчук А.В.			KIK.KP.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

```

!
!
!
radius server Serv-10-19-1
  address ipv4 192.168.19.251 auth-
port 1812 acct-port 1813
  key WinRadius
!
!
control-plane
!
!
line con 0
  exec-timeout 0 0

```

```

privilege level 15
logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  transport input ssh
!
ntp server Serv-10-19-1 prefer
!
!
end

```

SW-10-19-3:

```

!
! Last configuration change at
15:58:16 EEST Tue Jun 18 2024 by
radius-user
!
version 15.2
service timestamps debug datetime
msec
service timestamps log datetime
no service password-encryption
service compress-config
!
hostname SW-10-19-3
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS
severity drops 6 msg-body drops
EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5
$1$yJkd$GNxE07d5uJZExEyXgRUEh1
!
username radius privilege 15 secret
5 $1$ArWE$yDBnrrwVeaD9DjrMIduL0
aaa new-model
!
!
aaa authentication login default
group radius local
aaa authorization exec default group
radius local if-authenticated
!
!
!

```

```

!
!
!
aaa session-id common
clock timezone EEST 3 0
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping vlan 1
no ip dhcp snooping information
option
ip dhcp snooping
ip domain-name nesterchuk.net
ip name-server 192.168.19.251
ip cef
no ipv6 cef
!
!
!
spanning-tree mode pvst
spanning-tree portfast edge
bpduguard default
spanning-tree portfast edge
bpdufilter default
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!

```

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – КБ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

```

!
!
!
!
!
!
!
interface Ethernet0/0
    switchport mode access
    spanning-tree portfast edge
    ip dhcp snooping limit rate 15
!
interface Ethernet0/1
    switchport mode access
    spanning-tree portfast edge
    ip dhcp snooping limit rate 15
!
interface Ethernet0/2
    switchport mode access
    spanning-tree portfast edge
    ip dhcp snooping limit rate 15
!
interface Ethernet0/3
    description UNUSED-PORT-VLAN1001
    switchport access vlan 1001
    switchport mode access
    switchport port-security mac-
address sticky
    switchport port-security
    shutdown
    ip dhcp snooping limit rate 15
!
interface Ethernet1/0
    description UNUSED-PORT-VLAN1001
    switchport access vlan 1001
    switchport mode access
    shutdown
    ip dhcp snooping limit rate 15
!
interface Ethernet1/1
    description UNUSED-PORT-VLAN1001
    switchport access vlan 1001
    switchport mode access
    shutdown
    ip dhcp snooping limit rate 15
!
interface Ethernet1/2
    description UNUSED-PORT-VLAN1001
    switchport access vlan 1001
    switchport mode access
    shutdown
    ip dhcp snooping limit rate 15
!
interface Ethernet1/3
    description UNUSED-PORT-VLAN1001
    switchport access vlan 1001
    switchport mode access
    shutdown
    ip dhcp snooping limit rate 15
!
interface Ethernet2/0
    description UNUSED-PORT-VLAN1001
    switchport access vlan 1001
    switchport mode access
    shutdown
    duplex full
    ip dhcp snooping limit rate 15
!
interface Ethernet2/1
    description UNUSED-PORT-VLAN1001
    switchport access vlan 1001
    switchport mode access
    shutdown
    ip dhcp snooping limit rate 15
!
interface Ethernet2/2
    description UNUSED-PORT-VLAN1001
    switchport access vlan 1001
    switchport mode access
    shutdown
    ip dhcp snooping limit rate 15
!
interface Ethernet2/3
    description UNUSED-PORT-VLAN1001
    switchport access vlan 1001
    switchport mode access
    shutdown
    ip dhcp snooping limit rate 15
!
interface Ethernet3/0
    description UNUSED-PORT-VLAN1001
    switchport access vlan 1001
    switchport mode access
    shutdown
!
interface Ethernet3/1
    switchport mode access
    switchport port-security maximum 10
    switchport port-security
    ip dhcp snooping trust
!
interface Ethernet3/2
    switchport mode access
    switchport port-security maximum 10
    switchport port-security
    ip dhcp snooping trust
!
interface Ethernet3/3
    switchport mode access
    ip dhcp snooping trust

```

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – ПЗ	Арк.
		Трокоз Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Vlan1
  ip address 192.168.19.242
  255.255.255.0
!
ip default-gateway 192.168.19.254
ip forward-protocol nd
!
ip tcp synwait-time 5
ip http server
!
ip ssh time-out 30
ip ssh version 2
ip ssh server algorithm encryption
aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption
aes128-ctr aes192-ctr aes256-ctr
!
!
logging trap notifications
logging host 192.168.1.2
logging host 192.168.19.251
!
!
!

```

SW-10-19-4:

```

!
! Last configuration change at
15:58:36 EEST Tue Jun 18 2024 by
radius-user
!
version 15.2
service timestamps debug datetime
msec
service timestamps log datetime
no service password-encryption
service compress-config
!
hostname SW-10-19-4
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS
severity drops 6 msg-body drops
EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5
$1$qeOR$zIKAkqTwNtu0YsTeKfndt0
!

```

```

!
radius server Serv-10-19-1
  address ipv4 192.168.19.251 auth-
port 1812 acct-port 1813
  key WinRadius
!
!
control-plane
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  transport input ssh
!
ntp server Serv-10-19-1 prefer
!
!
!
end

```

```

username radius privilege 15 secret
5 $1$HNU8$HTt5u3IxcQBAkBWNiE3710
aaa new-model
!
!
aaa authentication login default
group radius local
aaa authorization exec default group
radius local if-authenticated
!
!
!
!
!
aaa session-id common
clock timezone EEST 3 0
!
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
ip dhcp snooping vlan 1
ip dhcp snooping

```

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – ПЗ	Арк.
		Трокоз Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

```
ip domain-name nesterchuk.net
ip name-server 192.168.19.251
ip cef
no ipv6 cef
!
!
!
spanning-tree mode pvst
spanning-tree portfast edge
bpduguard default
spanning-tree portfast edge
bpdufilter default
spanning-tree extend system-id
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Ethernet0/0
    switchport mode access
    switchport port-security mac-
address sticky
    switchport port-security mac-
address sticky 0800.27ab.4921
    switchport port-security
    spanning-tree portfast edge
    ip dhcp snooping limit rate 15
    ip dhcp snooping trust
!
interface Ethernet0/1
    switchport mode access
    switchport port-security mac-
address sticky
    switchport port-security mac-
address sticky 0800.2791.083d
    switchport port-security
    spanning-tree portfast edge
    ip dhcp snooping limit rate 15
!
interface Ethernet0/2
    switchport mode access
    switchport port-security mac-
address sticky
    switchport port-security mac-
address sticky 0050.7966.6803
```

```

switchport port-security
spanning-tree portfast edge
ip dhcp snooping limit rate 15
!
interface Ethernet0/3
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
switchport port-security mac-
address sticky
switchport port-security
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet1/0
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet1/1
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet1/2
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet1/3
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet2/0
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15
!
interface Ethernet2/1
description UNUSED-PORT-VLAN1001
switchport access vlan 1001
switchport mode access
shutdown
ip dhcp snooping limit rate 15

```

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – ПЗ	Арк.
		Трокоз Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Ethernet2/2
  description UNUSED-PORT-VLAN1001
  switchport access vlan 1001
  switchport mode access
  shutdown
  ip dhcp snooping limit rate 15
!
interface Ethernet2/3
  description UNUSED-PORT-VLAN1001
  switchport access vlan 1001
  switchport mode access
  shutdown
  ip dhcp snooping limit rate 15
!
interface Ethernet3/0
  description UNUSED-PORT-VLAN1001
  switchport access vlan 1001
  switchport mode access
  shutdown
!
interface Ethernet3/1
  switchport mode access
  switchport port-security maximum 10
  switchport port-security
  ip dhcp snooping trust
!
interface Ethernet3/2
  switchport mode access
  switchport port-security maximum 10
  switchport port-security
  ip dhcp snooping trust
!
interface Ethernet3/3
  switchport mode access
  switchport port-security maximum 10
  switchport port-security
  ip dhcp snooping trust
!
interface Vlan1
  ip address 192.168.19.243
  255.255.255.0
!
ip default-gateway 192.168.19.254

```

```

ip forward-protocol nd
!
ip tcp synwait-time 5
ip http server
!
ip ssh time-out 30
ip ssh version 2
ip ssh server algorithm encryption
aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption
aes128-ctr aes192-ctr aes256-ctr
!
!
logging trap notifications
logging host 192.168.1.2
logging host 192.168.19.251
!
!
!
!
radius server Serv-10-19-1
  address ipv4 192.168.19.251 auth-
  port 1812 acct-port 1813
  key WinRadius
!
!
control-plane
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  transport input ssh
!
ntp server Serv-10-19-1 prefer
!
!
end

```

		Нестерчук А.В.			КІК.КР.Б – 125 – 19 – ПЗ	Арк.
		Трокоз Є.М.				6
Змн.	Арк.	№ докум.	Підпис	Дата		