Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Білоуса Павла Романовича

на здобуття ступеня вищої освіти Бакалавра

Відмовостійка університетська комп'ютерна мережа

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ. 2102137.21.02.01 ПЗ

Виконав студент 4 курсу група КБ-21-2 Павло БІЛОУС
Керівник канд. техн. наук, доцент Юрій КЛЬОЦ
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

2 06 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
Юрій КЛЬОЦ
15 Лютого 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Білоуса Павла Романовича

1 Тема роботи Відмовостійка університетська комп'ютерна мережа

Керівник роботи канд. тех. наук, доц. кафедри КБ Юрій Павлович Кльоц

Затверджено наказом ректора університету від 07 лютого 2025 № 23

2 Строк подання студентом кваліфікаційної роботи на кафедру 06.06.2025

3 Вихідні дані до роботи спроєктувати методи покращення відмовостійкості університетської комп'ютерної мережі за рахунок технологій VRRP та віртуального маршрутизатора, провести дослідження вже існуючої університетської комп'ютерної мережі на основі вже доступних даних та налаштувань. Перевірка працездатності мережі під час виникнення критичних ситуацій.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Основні поняття комп'ютерної мережі. Огляд університетської мережі. Проєктування відмовостійкості університетської комп'ютерної мережі. Створення відмовостійкості університетської комп'ютерної мережі. Перевірка працездатності

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Генеральний план об'єкту інформаційної діяльності. Ситуаційний план об'єкту інформаційної діяльності.

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7 Дата видачі завдання 7 Лютого 2025 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень	
Ознайомлення з предметною областю	Січень	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Лютий	
Визначення загальних принципів рішення задачі	Березень	
Обґрунтування використаних методів у роботі	Березень	
Розробка політик мережі у мережі підприємства	Квітень	
Тестування налаштувань у мережі	Квітень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Травень	
Захист КР	Червень	

Студент Павло БІЛОУС

Керівник кваліфікаційної роботи Юрій КЛЬОЦ

АНОТАЦІЯ

Тема кваліфікаційної роботи: Відмовостійка університетська комп'ютерна мережа.

Автор роботи: Білоус Павло Романович.

Керівник роботи: Кльоц Юрій Павлович.

Пояснювальна записка: 70 с., 2 додатка, 29 рисунків, 8 таблиць, 43 джерела.

Графічна частина: 3 плакати, 10 презентаційних слайдів.

ПЕРЕЛІК КЛЮЧОВИХ СЛІВ: комп'ютерна мережа, VRRP, VLAN, відмовостійкість, безпека.

Кваліфікаційна робота бакалавра присвячена розробці відмовостійкої університетської комп'ютерної мережі для забезпечення

У роботі проаналізовано існуючу мережеву інфраструктуру університету, виявлено її потенційні слабкі місця та ризики відмови. Розглянуто принципи роботи технологій VLAN для сегментації мережі, VRRP для забезпечення резервування шлюзів і DHCP для автоматизованого керування IP-адресами. Результатом роботи стала розробка архітектури відмовостійкої мережі, що включає логічну та фізичну топологію, налаштування основних мережевих пристроїв, механізми балансування навантаження та резервування. Також було підготовлено супровідну документацію: технічне завдання, проєктну документацію, опис налаштувань мережевого обладнання та тестування роботи мережі в умовах різних відмов. Запропоноване рішення забезпечує стабільну та безперебійну роботу університетської комп'ютерної мережі, підвищує її безпеку та ефективність використання мережевих ресурсів.

29.05.2025 _____

ABSTRACT

Subject of qualification work: Fault-tolerant university computer network

Author: Bilous Pavlo Romanovich

Head of work: Klots Yuri Pavlovich

Explanatory note: 70 p., 2 appendices, 29 figures, 8 tables, 43 sources

Graphic part: 3 posters, 10 presentation slides.

KEYWORDS: computer network, VRRP, VLAN, fault-tolerant, security.

The bachelor's qualification work is devoted to the development of a fault-tolerant university computer network to provide

The work analyzed the existing network infrastructure of the university, identifies its potential weaknesses and risks of failure. The principles of VLAN technology for network segmentation, VRRP for gateway redundancy, and DHCP for automated IP address management are considered. The result of the work was the development of a fault-tolerant network architecture, including logical and physical topology, configuration of the main network devices, load balancing and redundancy mechanisms. Supporting documentation was also prepared: terms of reference, design documentation, a description of network equipment settings, and testing of network operation under various failures. The proposed solution ensures stable and uninterrupted operation of the university computer network, increases its security and efficiency of network resources.

29.05.2025 _____

ЗМІСТ

ВСТУП

Сучасні університетські комп'ютерні мережі є невід'ємною частиною освітнього процесу та науково-дослідницької діяльності. Вони забезпечують доступ до інформаційних ресурсів, електронних бібліотек, навчальних платформ, адміністративних систем. Висока залежність від цифрових технологій робить безперервність роботи мережі критично важливою, оскільки навіть короткочасний збій може призвести до серйозних проблем, таких як втрата доступу до важливих навчальних матеріалів, зрив дистанційних занять або неможливість комунікації між студентами та викладачами.

Університетська мережа повинна не лише забезпечувати високу швидкість і ефективний розподіл трафіку, а й бути відмовостійкою, тобто здатною автоматично адаптуватися до аварійних ситуацій та відновлювати роботу без втручання адміністратора. Одним із ключових методів підвищення надійності мережі є її правильна структура та впровадження резервних механізмів маршрутизації.

Одним з основних компонентів сучасної університетської мережі є віртуальні локальні мережі (VLAN). Використання VLAN дозволяє сегментувати мережевий трафік та забезпечити логічний поділ між різними групами користувачів, такими як студенти, викладачі, адміністрація та серверне обладнання. Це покращує безпеку, підвищує продуктивність і зменшує кількість широкомовного трафіку, що позитивно впливає на загальну стабільність мережі.

Ще одним важливим елементом є динамічне призначення IP-адрес за допомогою протоколу DHCP (Dynamic Host Configuration Protocol). DHCP дозволяє автоматично видавати пристроям у мережі унікальні IP-адреси, усуваючи необхідність ручного налаштування. Це значно спрощує адміністрування мережі, особливо в умовах великої кількості підключених пристроїв, які постійно змінюються.

Для ефективного управління маршрутизацією в університетській мережі часто використовуються пристрої компанії Mikrotik. Ці маршрутизатори підтримують широкий спектр мережевих функцій, включаючи VLAN, QoS

(керування якістю обслуговування), балансування навантаження та резервування каналів. Однією з найважливіших функцій для забезпечення відмовостійкості є Virtual Router Redundancy Protocol (VRRP).

VRRP дозволяє об'єднати два маршрутизатори в єдину групу, де один виконує роль основного, а інший резервного. У нормальному режимі основний маршрутизатор обробляє весь трафік, але якщо він виходить з ладу (наприклад, через відмову обладнання, збої у програмному забезпеченні або проблеми з живленням), VRRP автоматично передає контроль над мережею резервному маршрутизатору. Завдяки цьому користувачі навіть не помічають змін, і робота мережі продовжується безперервно.

Крім того, для забезпечення ще більшої відмовостійкості університетська мережа має два незалежні підключення до Інтернету від різних провайдерів. Це дозволяє запобігти повному відключенню університету від мережі у разі збоїв на стороні одного з провайдерів.

У разі критичної ситуації, такої як збій основного маршрутизатора або проблеми з одним із інтернет-провайдерів, VRRP активує резервний маршрутизатор, який автоматично перенаправляє весь трафік через іншого провайдера. Це дозволяє мінімізувати ризики простоїв, а університетська мережа залишається доступною без потреби в ручному втручанні з боку адміністратора.

Таким чином, побудова відмовостійкої університетської комп'ютерної мережі вимагає ретельного планування та впровадження низки технологій, включаючи VLAN, DHCP, VRRP. У цій роботі будуть детально розглянуті основні принципи побудови такої мережі, налаштування ключових компонентів на маршрутизаторах Mikrotik, а також реалізація механізму автоматичного перемикання трафіку у разі аварійної ситуації. Особливу увагу буде приділено практичним аспектам конфігурації VRRP, що дозволяє забезпечити безперебійну роботу університетської інфраструктури та мінімізувати вплив можливих збоїв на освітній процес.

1 ОСНОВНІ ПОНЯТТЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ. ОГЛЯД УНІВЕРСИТЕТСЬКОЇ МЕРЕЖІ

1.1 Аналіз термінів та їхній опис

Для початку потрібно розглянути поняття моделі OSI, VLAN, DHCP, VRRP, IP, TCP/IP та пристроїв Mikrotik.

Модель OSI (Open Systems Interconnection) – це концептуальна семирівнева модель, яка описує, як різні мережеві пристрої взаємодіють між собою для забезпечення передачі даних. Вона була розроблена ISO (International Organization for Standardization) у 1978 році. В 1980 році була опублікована специфікація 802. Для стандартизації мережевих протоколів та спрощення їхньої взаємодії у 1984 році було упроваджено модель OSI як міжнародний стандарт. [1, 3]

Модель OSI допомагає розділити складні мережеві процеси на окремі рівні, кожен із яких виконує свої унікальні функції. Рівні моделі OSI можна побачити на рисунку 1.1. [2]

Прикладний рівень (Application Layer) взаємодіє з користувачами та забезпечує доступ до мережевих сервісів та додатків за допомогою протоколів HTTP, HTTPS, FTP, SMTP, DNS, SNMP та інші. Використовується у браузерах, додатках, поштових серверах.

Рівень представлення (Presentation Layer) забезпечує шифрування, стиснення та форматування даних для передачі між пристроями за допомогою протоколів SSL/TLS, JPEG, GIF, MPEG, ASCII, Unicode. Використовується у медіа-конвертерах та шифрувальних модулях.

Сеансовий рівень встановлює, підтримує та завершує сеанси зв'язку між додатками за допомогою протоколів SSH, PPTP, RPC. Використовується на проксі-серверах та серверах додатків.

Транспортний рівень (Transport Layer) забезпечує надійну передачу даних між кінцевими пристроями та розділяє потоки даних для різних додатків за допомогою протоколів TCP та UDP. Використовується на серверах додатків та шлюзах (gateway).

Рисунок 1.1 – Рівні моделі OSI

Мережевий рівень (Network Layer) займається маршрутизацією пакетів між мережами та визначає найкращий маршрут для передачі даних за допомогою IP (IPv4, IPv6), ICMP, OSPF. Використовується на маршрутизаторах (router) та багатошарових комутаторах (Layer 3 switch).

Канальний рівень (Data Link Layer) забезпечує коректну передачу кадрів даних між двома пристроями, контролює помилки та доступ до середовища

передачі за допомогою протоколів Ethernet (MAC, LLC), Wi-Fi, PPP, HDLC. Використовується на комутаторах (switch), мостах (bridge) та мережевих картах (NIC).

Фізичний рівень (Physical Layer) забезпечує предачу бітів даних через фізичне середовище (мідний кабель, радіохвилі, оптоволокно та інші) за допомогою кабелів UDP, оптоволоконних кабелів, Wi-Fi, USB та Bluetooth. Використовується на концентраторах (hub), модемах, перетворювачах (repeater) та мережевих адаптерах.

Для кращого розуміння роботи моделі OSI уявімо ситуацію, що ви надсилаєте листа:

- фізичний рівень – поштовий кур'єр несе конверт (бітова передача);
- канальний рівень – пошта сортує листи за містами (адресація MAC);
- мережевий рівень – лист направляється в інше місто (маршрутизація);
- транспортний рівень – перевіряється, потрібно доставити швидко листа, незважаючи на певні втрати даних під час передачі, або потрібно бути впевненим, що лист прийде у тому вигляді, у якому його отримали (TCP/UDP);
- сеансовий рівень – відкривається конверт та розпочинається читання (сеанс);
- рівень представлення – переклад листа, якщо він написаний іншою мовою (шифрування, кодування);
- прикладний рівень – ви читаєте лист (взаємодія з користувачем).

Модель OSI, на даний момент, слугує, у більшості випадків, для кращого розуміння того, як працюють комп'ютерні мережі, та для того. Також вона являється стандартизованою, через що вона існує основною для розробки мережевого обладнання та програмного забезпечення. Саме на основі моделі OSI було створено модель TCP/IP, яка, на даний момент, використовується в реальних комп'ютерних мережах.

TCP/IP (Transmission Control Protocol/Internet Protocol) це набір мережевих протоколів, що використовуються для передачі даних у глобальній мережі Інтернет і локальних мережах. Він забезпечує взаємодію різних пристроїв у мережі незалежно від їхнього виробника чи операційної системи. [4, 5]

Основні характеристики TCP/IP:

- використовується в Інтернеті та корпоративних мережах;
- підтримує надійну та безпечну передачу даних;
- включає велику кількість протоколів для різних рівнів передачі даних;
- працює на основі унікальних IP-адрес для ідентифікації пристроїв;
- дозволяє маршрутизацію трафіку через складні мережеві топології.

Модель TCP/IP складається з чотирьох рівнів, які можна побачити на рисунку 1.2. [7]

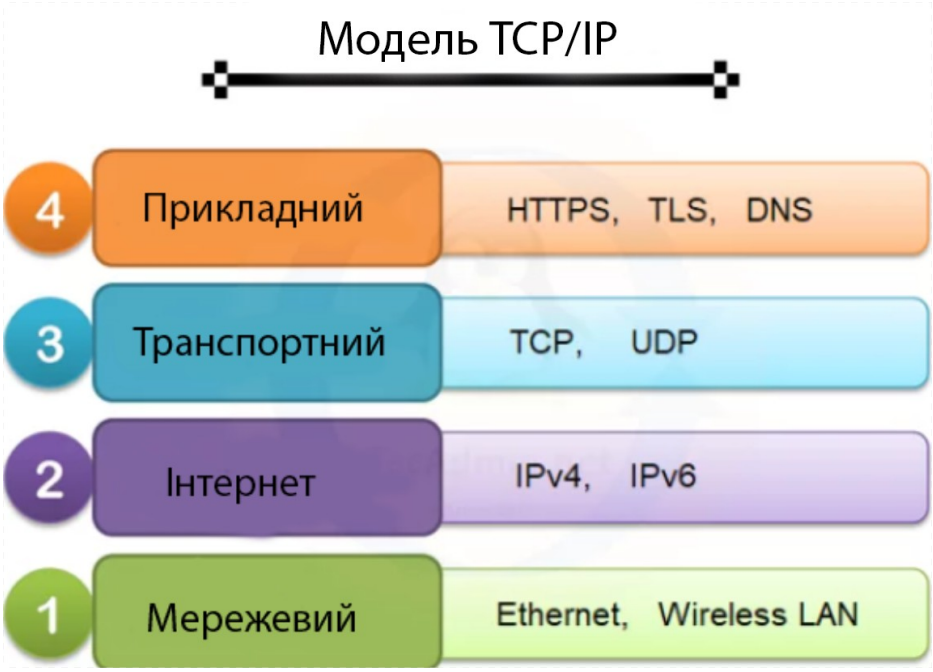


Рисунок 1.2 – Рівні моделі TCP/IP

Мережевий рівень (Network Access Layer) відповідає за передачу даних між пристроями в межах однієї фізичної мережі, використовуючи для цього Ethernet, Wi-Fi, DSL або оптоволоконні технології.

Інтернет-рівень (Internet Layer) визначає маршрутизацію пакетів між різними мережами, використовує унікальні IP-адреси для ідентифікації пристроїв, а також включає механізми фрагментації та збирання пакетів.

Транспортний рівень (Transport Layer) забезпечує надійну (TCP) або ненадійну (UDP) передачу даних між пристроями, а також використовує номери портів для ідентифікації конкретних додатків.

Прикладний рівень (Application Layer) Забезпечує взаємодію між додатками та користувачами через стандартизовані протоколи. Наприклад: HTTP, HTTPS, FTP, SFTP, DNS та інші.

Щоб краще зрозуміти транспортний рівень, слід розібрати що являють собою протоколи TCP та UDP

TCP (Transmission Control Protocol) і UDP (User Datagram Protocol) – це два основних транспортні протоколи в моделі TCP/IP, які забезпечують передачу даних у комп'ютерних мережах, включаючи Інтернет.

TCP працює наступним чином:

- встановлення з'єднання (3-way handshake);
- передача даних;
- закриття з'єднання (4-way handshake).

Протокол UDP працює без встановлення та закриття з’єднання, що забезпечує швидшу передачу даних, але він не гарантує доставку даних у тому самому вигляді, у якому вони були надіслані.

Для кращого розуміння різниці між протоколами TCP та UDP потрібно порівняти можливості кожного з них. Це можна побачити у таблиці 1.1. [8, 9, 10]

Таблиця 1.1 – Порівняння протоколів TCP та UDP

Характеристика	TCP	UDP
Надійність	Гарантована	Не гарантується
Контроль помилок	Так	Ні
Підтвердження отримання	Так	Ні
Швидкість	Нижча (через контроль та перевірки)	Вища
Приклади використання	Веб-сторінки, електронна пошта, передача даних	Прямі трансляції відео, онлайн-ігри

Як працює TCP/IP? Коли користувач відправляє дані через Інтернет або

локальну мережу, модель TCP/IP працює наступним чином:

- дані розбиваються на пакети на прикладному рівні;
- транспортний рівень додає заголовок TCP або UDP, що містить контрольні дані та номер порту;
- інтернет-рівень додає IP-адресу відправника і отримувача, після чого пакет передається в мережу;
- мережевий рівень визначає, як передати дані по фізичній мережі до наступного пристрою (маршрутизатора або кінцевого пристрою);
- на стороні отримувача весь процес повторюється у зворотному порядку, поки дані не досягнуть кінцевого додатка.

Для кращого та чіткішого розуміння різниці між моделями мережевих протоколів TPC/IP та OSI потрібно зробити порівняння цих двох моделей. Це порівняння з різницями у цих двох моделях можна чіткіше побачити у таблиці 1.2. [6, 11]

Таблиця 1.2 – Порівняння моделей OSI та TCP/IP

Рівні моделі OSI	Рівні моделі TCP/IP
7- Прикладний (Application)	4 – Прикладний (Application)
6 –Представлення (Presentation)	
5 – Сеансовий (Session)	
4- Транспортний (Transport)	3 – Транспортний (Transport)
3 – Мережевий (Network)	2 – Інтернет (Internet)
2 – Канальний (Data Link)	1 – Мережевий (Network)
1 – Фізичний (Physical)	

IP (Internet Protocol) це основний мережевий протокол, який використовується для ідентифікації та маршрутизації пристроїв у комп'ютерних мережах, включаючи Інтернет. IP-адресація дозволяє пристроям взаємодіяти між собою через унікальні числові ідентифікатори. IP буває IPv4 та IPv6. Їхня різниця заключається в тому, що IPv4 це 32-бітова адресація, представлена у вигляді

чотирьох чисел (від 0 до 255), розділених крапками (наприклад, 192.168.1.1), а IPv6 це 128-бітова адресація, представлена у вигляді восьми груп шістнадцяткових чисел (наприклад, 2001:0db8:85a3:0000:0000:8a2e:0370:7334). IPv6 був розроблений через обмежену кількість доступних IPv4-адрес. На момент написання цієї роботи, в Україні не підтримується IPv6. [12, 13, 14]

Функції IP:

- ідентифікація пристроїв. Кожен пристрій у мережі має унікальну IP-адресу;
- маршрутизація. IP визначає найкращий маршрут для передачі пакетів від відправника до отримувача;
- фрагментація та збирання пакетів. IP дозволяє розбивати великі повідомлення на менші частини (пакети) та збирати їх на стороні отримувача;
- визначення отримувача. IP-адреси використовуються для спрямування даних на правильний пристрій у локальній або глобальній мережі.

Для правильного розуміння IP-адрес потрібно також знати про маски, які використовуються при наданні IP-адрес.

Маска підмережі (англ. *subnet mask*) це спеціальний 32-бітний (для IPv4) шаблон, який допомагає визначити, до якої мережі належить IP-адреса, а яка частина адреси це адреса конкретного пристрою (вузла) в цій мережі.

IP-адреса складається з двох частин. З мережної частини, яка вказує до якої мережі належить IP-адреса, та хостова частина (вузол), яка вказує на конкретний пристрій у мережі. Маска підмережі визначає, де саме проходить межа між цими частинами.

Маска складається з чотирьох 8-бітних значень двійкового коду. Зазвичай ми бачимо це значення у десятковому вигляді. Наприклад, 255.255.255.0. Це значення було перетворене з двійкового в десяткове для кращого розуміння та освоєння людиною. Також можна побачити маску у вигляді кількості використаних бітів. Наприклад, /24. Це значення вказує кількість використаних бітів двійкового значення. Якщо порівняти ці варіанти, то /24 має ідентичне значення з 255.255.255.0. Якщо дивитись на значення двійкового коду, то воно виглядає послідовністю одиниць та нулів. Якщо взяти значення /24, то у

двійковому вигляді воно буде виглядати 11111111.11111111.11111111.00000000. Людському мозку краще дається запам’ятати значення у десятковому вигляді, або у вигляді /24. Якщо проводити аналогію між цими трьома виглядами маски, то можна дійти до висновків, які вказані у таблиці 1.3.

Таблиця 1.3 – Аналогія між різним відображенням маски

Маска у вигляді префіксу	Маска у десятковому вигляді	Маска у двійковому вигляді	Кількість можливих користувачів
/8	255.0.0.0	11111111 00000000 00000000 00000000	$2^{24}\approx$ 16 млн.
/16	255.255.0.0	11111111 11111111 00000000 00000000	$2^{16}\approx$ 65 тис.
/24	255.255.255.0	11111111 11111111 11111111 00000000	2^8=254 254-2=252 252
/25	255.255.255.128	11111111 11111111 11111111 10000000	2^7=128 128-2=126 126
/30	255.255.255.252	11111111 11111111 11111111 11111100	2^2=4 4-2=2 2

Для правильного вибору потрібної маски потрібно враховувати, що дві адреси буде зарезервовано. Одну зарезервовано для адреси мережі, а одну для Broadcast. Саме через цю причину у випадку маски /30 вільних користувачів всього 2, а не 4.

Отже, маска це інструмент для розділення IP-адрес на підмережі. Маски були створенні через те, що кількість пристроїв у глобальній мережі все зростало, а кількість IPv4 адрес було дуже обмежено. Саме для збільшення кількості можливих пристроїв було створено маски. Після того, як появилось розуміння, що навіть у такому випадку буде нестача IP-адрес для всіх користувачів, було створено IPv6, який має набагато більше можливих IP-адрес.

Broadcast -це широкомовна передача. Це тип повідомлення, яке надсилається всім пристроям в межах однієї мережі (або підмережі).

Broadcast використовується, коли один пристрій хоче знайти або повідомити всі інші пристрої в мережі. Наприклад, комп'ютер хоче дізнатись MAC-адресу іншого пристрою. Він надсилає ARP-запит на broadcast адресу. Також можна зазначити, що DHCP-запит при підключенні до мережі також являється запитом broadcast.

IP адреси бувають публічними (призначаються провайдерами), приватними (локальні адреси, до яких не можна отримати доступ з іншої приватної мережі). Якщо розглядати те, як пристрої отримують IP адреси, то це здійснюється за допомогою статичних адрес (Static IP), або за допомогою динамічних (Dynamic IP). Статичні адреси надаються в кожному пристрої вручну, та не змінюється з плином часу, а динамічні адреси змінюються з плином часу, та надаються автоматично за допомогою DHCP.

DHCP (Dynamic Host Configuration Protocol) це мережевий протокол, що автоматично призначає IP-адреси, шлюзи, DNS-сервери та інші мережеві параметри пристроям у мережі. [15, 18]

DHCP являє собою дуже важливий елемент мережі, бо завдяки йому більшість пристроїв отримує IP-адреси автоматично, також зникає дублювання адрес у мережі. Завдяки DHCP адміністратори можуть легко змінювати параметри без ручної конфігурації кожного пристрою. [16, 17]

У своїй роботі потрібно розібрати поняття VLAN, бо завдяки цій технології можна сегментувати мережу, що дозволить забезпечити відмовостійкість мережі.

VLAN (Virtual Local Area Network) це технологія в комп'ютерних мережах, яка дозволяє логічно сегментувати фізичну мережу на кілька ізольованих підмереж без потреби в додатковому фізичному обладнанні. [19, 20, 21, 22]

Для забезпечення відмовостійкості мережі потрібно розглянути що таке Firewall.

Firewall (брандмауер) це система захисту комп'ютерних мереж, яка контролює вхідний та вихідний мережевий трафік. Вона вирішує, які дані дозволено передавати, а які заблокувати, згідно з встановленими правилами безпеки.

Іншими словами, брандмауер це фільтр, що стоїть між твоїм комп'ютером (чи мережею) та інтернетом, і слідкує за тим, щоб небажаний трафік не потрапив всередину.

Він існує щоб захистити мережу від зовнішнього втручання зловмисників за допомогою блокування спроб злому. Також він запобігає витоку даних, бо не дозволяє програмам надсилати дані без дозволу. Можна зазначити, що він забезпечує контроль доступу тим, що обмежує доступ до певних сайтів або серверів. На додачу до всього зазначеного вище можна додати, що він захищає від шкідливого програмного забезпечення так як може зупиняти віруси чи трояни, які намагаються "спілкуватись" із зовнішнім світом. Візуально побачити що саме являє собою Firewall можна на рисунку 1.3. [23]

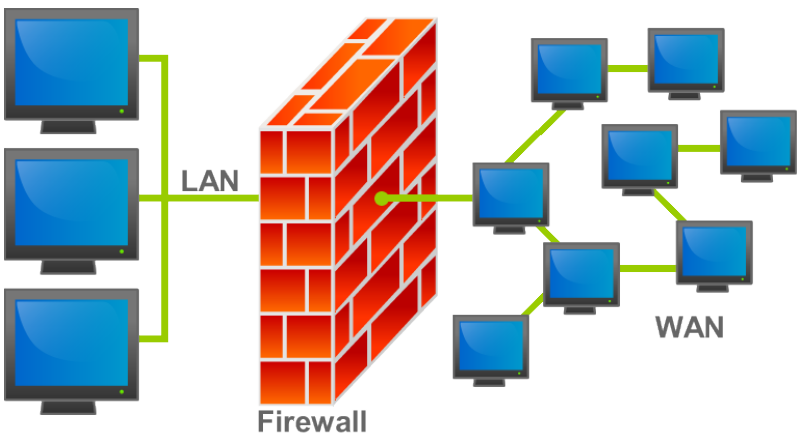


Рисунок 1.3 – Візуальний приклад Firewall

Брандмауер перевіряє кожний пакет трафіку, що надходить чи виходить, а також вирішує дозволяти його чи ні. Він працює за допомогою набору правил, які вказуються при налаштуванні. Також він забороняє або дозволяє трафік перевіряючи список правил зверху до низу. Якщо він “побачив” потрібне правило, то він дозволяє або забороняє трафік та не перевіряє подальші правила. У самому кінці списку має ставитись правило, яке забороняє всьому іншому трафіку, який не було зазначено до цього правила.

Всього існує декілька видів брандмауера:

- програмний Firewall;
- апаратний Firewall;
- мережевий Firewall;
- хмарний Firewall (Cloud Firewall).

Програмний Firewall встановлюється на комп’ютері або сервері та контролює трафік лише на пристрої, на якому він встановлений. Використовується він у кожному комп’ютері. Якщо комп’ютер має операційну систему Windows, то за допомогою Windows Firewall.

Апаратний Firewall являє собою окремий пристрій та захищає всю мережу. Його часто використовують у компаніях різних галузей тому, що він має високу продуктивність та, порівняно з апаратним Firewall, краще захищає всю мережу.

Мережевий Firewall захищає всю локальну мережу та впроваджується на маршрутизаторах або спеціальних пристроях у компанії.

Хмарний Firewall (Cloud Firewall) працює на віддалених серверах. Захищає він онлайн-сервіси, веб-сайти та хмарну інфраструктуру.

Firewall може фільтрувати трафік за допомогою IP-адрес, за допомогою різних портів (наприклад, порт 80 для HTTP, 443 для HTTPS та інші), за допомогою протоколів (наприклад, TCP або UDP), за вмістом трафіку за допомогою, так званого глибокого аналізу пакетів (Deep Packet Inspection) та за додатками, які надсилають трафік за допомогою визначення того, яка саме програма надсилала трафік та контролює даний трафік.

Для кращого розуміння кожного з видів Firewall потрібно їх порівняти та зрозуміти переваги та недоліки кожного. Це можна побачити у таблиці 1.4.

Таблиця 1.4 – Порівняння видів Firewall

Вид Firewall	Програмний	Апаратний	Мережевий	Хмарний
Місце розташування	На комп’ютері або сервері.	Між мережею підприємства та інтернетом.	На маршрутизаторі або шлюзі.	У хмарній інфраструктурі.
Призначення	Захист окремого пристрою.	Захист всієї мережі.	Фільтрація трафіку між мережами.	Захист хмарних сервісів та додатків.
Масштаб покриття	Один пристрій.	Вся локальна мережа.	Локальна мережа.	Хмарне середовище.
Приклади використання	Windows Firewall.	Cisco ASA.	MikroTik.	AWS, Azure Firewall.
Переваги	Легко встановити, контроль програм.	Висока продуктивність незалежно від операційної системи.	Захист всієї мережі, централізований контроль.	Легке управління та можливість масштабування.
Недоліки	Не захищає всю мережу, можливі конфлікти.	Дорожчий та складніший у налаштуванні.	Не фільтрує трафік всередині пристрою.	Залежить від з’єднання з інтернетом та щомісячна оплата.

Для кращого розуміння що таке Firewall можна провести аналогію. Можна уявити, що комп’ютер це будинок, а Firewall це охоронець біля дверей, який перевіряє кожного відвідувача та не робить винятків з правил. Якщо це знайомий (наприклад, браузер відкриває Google) то охоронець пропускає даного відвідувача. Якщо це незнайомець, або підозрілий незнайомець (вірус, троян або хакер) то охоронець не впускає його. Firewall потрібний саме для забезпечення безпеки у мережі.

1.2 Огляд топології університетської мережі

Для забезпечення якісного навчання та нормальних умов праці, університет повинен створити умови, які дозволять мати доступ до мережі інтернет якомога довше, та щоб впливи непередбачуваних критичних ситуацій не мали катастрофічний вплив на мережу всієї університетської комп'ютерної мережі.

Для того, щоб забезпечити дані умови, комп'ютерна мережа університету має такі компоненти:

- декілька незалежних інтернет-провайдерів;
- вхідні маршрутизатори;
- оптичні комутатори ;
- користувачі комп'ютерної мережі.

Інтернет-провайдери повинні бути незалежними, щоб у випадку збою роботи в одного провайдера, інший міг продовжувати надавати послуги, за допомогою яких університет має доступ до мережі інтернет.

Вхідні маршрутизатори використовуються як пристрої, які з'єднанні з інтернет-провайдерами та користувачами, що дозволяє користувачам використовувати мережу інтернет. Через вхідні маршрутизатори проходить весь трафік, а також вони роздають динамічні ip-адреси (DHCP).

Маршрутизатор (англ. Router) – це мережевий пристрій, який з'єднує різні мережі та керує передачею даних між ними. Він працює на третьому рівні моделі OSI (мережевий рівень) і використовує IP-адреси для визначення найкращого шляху передачі пакетів. [25, 27]

Маршрутизатор можна порівняти з транспортною розв'язкою, яка спрямовує автомобілі (дані) за правильними маршрутами до їхніх пунктів призначення.

Маршрутизатор направляє пакети між підмережами та Інтернетом за допомогою функції NAT, обирає оптимальний та найшвидший шлях для трафіку за допомогою таблиці маршрутизації, фільтрує дані та забезпечує безпеку за допомогою Firewall, NAT, VPN, дає змогу підключати багато пристроїв до однієї мережі, а також надає пріоритет важливим пакетам (відеоконференції і тп.).[26]

Також маршрутизатор може роздавати IP-адреси користувачам, іншими словами, він може виступати як DHCP-сервер.[24]

Оптичні комутатори існують для забезпечення швидкої та якісної комп'ютерної мережі для всіх користувачів цієї мережі. Є два оптичних комутатора, які підключені до вхідних маршрутизаторів. Для забезпечення обміну даними між двома вхідними маршрутизаторами та між собою, вони з'єднані оптоволоконним кабелем.

Комутатор (Switch) – це мережевий пристрій, який працює на канальному рівні (Layer 2) моделі OSI та забезпечує обмін даними між пристроями в локальній мережі (LAN). [28, 29, 32]

На відміну від маршрутизатора, який з'єднує різні мережі, та дозволяє підключатись до мережі Інтернет, комутатор з'єднує пристрої в одній мережі та розумно пересилає пакети лише потрібним адресатам, використовуючи MAC-адреси. [30]

Комутатор ефективно передає пакети між пристроями однієї мережі, у нього кожний порт працює окремо, та немає конфліктів пакетів, він дозволяє підключати в одній мережі, а також може розділяти трафік по підмережам (VLAN). [31, 33]

Комутатор, зазвичай, не має таблиці маршрутизації, та не може виступати як DHCP-сервер.

Для розуміння різниці між маршрутизатором та комутатором, потрібно їх зрівняти. Це порівняння можна побачити у таблиці 1.5. [34 - 38]

Таблиця 1.5 – Порівняння маршрутизатора та комутатора

Пристрій	Комутатор	Маршрутизатор
Рівень OSI	2 (Канальний)	3 (Мережевий)
Ключова функція	Передає пакети за MAC-адресами в одній мережі	З'єднує різні мережі та підмережі
Кому передає трафік	Тільки потрібному (конкретному) пристрою	Визначає шлях для передачі IP-пакетів

Топологію університетської комп’ютерної мережі можна побачити на рисунку 1.4

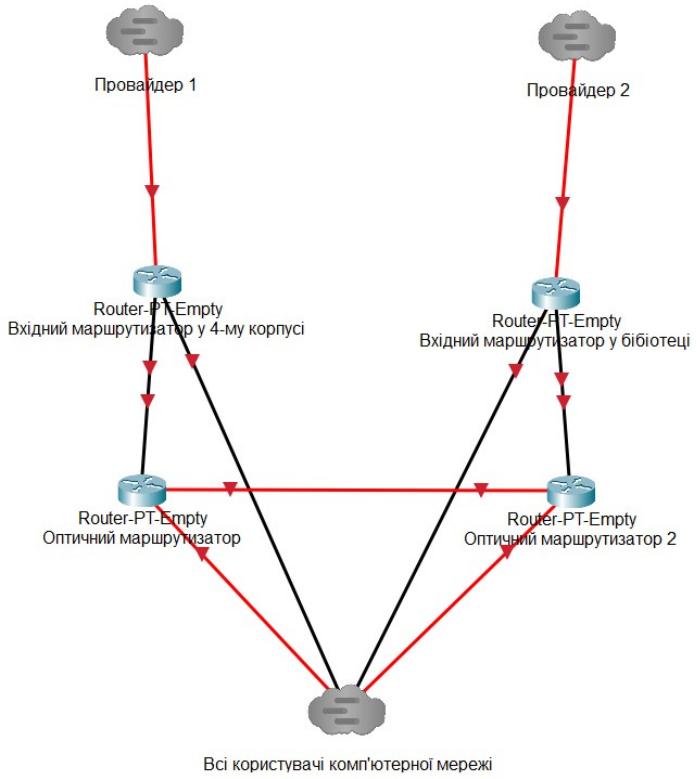


Рисунок 1.4 – Топологія університетської комп’ютерної мережі

На даний момент університетська комп’ютерна мережа використовує пристрої компанії MikroTik. Дані пристрої мають на вибір дві операційні системи, які дають змогу налаштовувати ці пристрої різними методами. Якщо використовувати SwitchOS, то налаштувати можна через веб-браузер, а якщо використовувати RouterOS, то за допомогою спеціальної програми WinBox. [41, 43]

MikroTik – це компанія, яка виробляє мережеве обладнання та програмне забезпечення для маршрутизації, управління мережею та бездротових з'єднань. Основна продукція включає маршрутизатори, комутатори, бездротові точки доступу та операційну систему RouterOS та SwitchOS. [39, 40] Як вже зазначалось вище, пристрої на опереційній системі SwitchOS налаштовуються за допомогою веб-браузера, а пристрої на операційній системі RouterOS налаштовуються за допомогою спеціального програмного забезпечення WinBox. В університетській

комп’ютерній мережі всі пристрої компанії MikroTik використовують операційну систему RouterOS.

Пристрої MikroTik широко використовуються в корпоративних мережах, провайдерами Інтернету (ISP) та у приватному секторі завдяки гнучкості, потужним можливостям налаштування та відносно низькій вартості. [42]

Університетська комп’ютерна мережа створена для забезпечення ефективного розподілу трафіку між двома інтернет-провайдерами. В ній використовуються пристрої компанії MikroTik моделей CCR (маршрутизатор) та CRS (комутатор). Це досягається за допомогою наявності двох інтернет-провайдерів у різних частинах університету, двох вхідних маршрутизаторів, за допомогою яких і проходить весь трафік, яким користуються всі користувачі. Розподіл трафіку відбувається за допомогою розділення комп’ютерної мережі на підмережі, залежно від місця розташування користувача, які вже розподілені на два вхідних маршрутизатора. Також у топології наявні два оптичні комутатори, які забезпечують високу швидкість трафіку у всіх частинах університету за допомогою оптоволоконних кабелів, бо, на відміну від мідних кабелів, оптоволоконні можуть підтримувати нормальну якість сигналу на довших дистанціях, а це необхідно, бо університет має доволі великі розміри.

1.3 Постановка задачі

Для створення відмовостійкої університетської комп’ютерної мережі спочатку потрібно розділити комп’ютерну мережу на підмережі, за допомогою VLAN, щоб підвищити безпеку та ефективність роботи мережі, а потім створити віртуальний маршрутизатор за допомогою VRRP для кожного VLAN, який наявний в мережі, щоб забезпечити безперебійну роботу під час більшості критичних ситуацій, які можуть виникнути у комп’ютерній мережі. Також для того, щоб все нормально працювало, потрібно спочатку визначити яким буде головний маршрутизатор для кожного VLAN, та для кожного DHCP. Після цього потрібно використати функцію VRRP, щоб все працювало в критичних ситуаціях

2 ПРОЄКТУВАННЯ ВІДМОВОСТІЙКОЇ УНІВЕРСИТЕТСЬКОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Політика безпеки

Політика безпеки у нашому випадку являє собою набір правил для забезпечення безпечної та стійкої комп'ютерної мережі.

Для забезпечення відмовостійкої комп'ютерної мережі потрібно спочатку визначити базову політику безпеки. Воно потрібна для розуміння того, як створена мережа та те, що можна робити та те, що не можна робити. Спочатку потрібно зазначити такі правила:

- на кожному пристрої, який можна налаштовувати, повинен бути логін та пароль, який відрізняється від стандартного;
- повинне бути розділення мережі на підмережі за допомогою технології VLAN;
- повинна бути підмережа для адміністраторів;
- повинен бути віртуальний маршрутизатор;
- повинен бути реалізований моніторинг пристроїв;
- робітники мають бути обізнаними що не можна робити.

Розберемо кожний пункт окремо.

Перший пункт потрібний для забезпечення безпеки, щоб була впевненість того, що ніхто, окрім адміністраторів, не зможе змінити налаштування пристроїв.

Другий пункт потрібний для забезпечення локалізації інцидентів, що також допомагає забезпечити відмовостійкість. Наприклад, хтось може принести з собою домашній роутер та підключити його не правильно, що призведе до збоїв в мережі у вигляді того, що користувачам університетської мережі буде роздаватись IP-адреса, яку видасть даний роутер за допомогою DHCP, а це призведе до того, що користувачі не матимуть доступ до інтернету. Завдяки тому, що підмережі створені для різних частин університету, це дозволяє швидше знайти де саме принесли даний роутер, а також це забезпечує стабільну роботу в інших підмережах, бо цей роутер не зможе впливати на пристрої в інших підмережах

Третій пункт випливає з другого тому, що якщо мережа розділиться на багато VLAN, то для того, щоб налаштувати якийсь пристрій, прийдеться бути в тому самому VLAN. Щоб позбутися даної проблеми, та можна було налаштовувати всі пристрої з будь-якої місця в межах університету, потрібно створити VLAN, через який можна буде налаштовувати всі пристрої. Цей влан буде існувати як додатковий на кожному пристрої, який можна налаштовувати.

Четвертий пункт, у цьому випадку, означає, що потрібно створити VRRP для кожного VLAN на вхідних маршрутизаторах. Це потрібно для того, щоб ,при виникненні критичної ситуації (наприклад, вимкнення сваітла), користувачі могли і надалі користуватись мережею. Як приклад критичної ситуації та дії під час її виникнення можна взяти вимкнення світла. За звичайних умов все працює в штатному режимі. Якісь пристрої мають доступ до інтернету через один маршрутизатор, у той самий час інші користувачі мають доступ до інтернету через інший маршрутизатор. На кожному маршрутизаторі є всі VLAN, які використовуються в університетській комп'ютерній мережі. Для кожного VLAN є своє VRRP, тобто, є основний та запасний маршрутизатор. Якщо відбудеться вимкнення світла на одному маршрутизаторі, то інший візьме роль головного, і ,у даному випадку, всі користувачі матимуть доступ до інтернету через один маршрутизатор.

П'ятий пункт, у цьому випадку, буде реалізований за допомогою функції "Log" на пристроях "Mikrotik". Дана функція дозволяє побачити проблеми, які виникають на пристрої, вжити заходів, які дозволять позбавитись від даної проблеми, та запобігти її виникнення в майбутньому.

Шостий пункт, у даному випадку, буде реалізований у вигляді того, що робітники повинні бути обізнаними, що не можна приносити свої мережеві пристрої в університет, і при виникненні проблеми, яка зв'язана з мережею, звертатись до відповідного відділу.

2.2 Визначення кількості VLAN та їх розміщення

Для забезпечення відмовостійкості університетської комп’ютерної мережі потрібно розібратись, скільки VLAN нам потрібно у даній мережі, де вони будуть знаходитись та адреси, які будуть притаманні для певних VLAN.

Спочатку потрібно розібратись з тим, скільки потрібно VLAN та де вони будуть знаходитись.

Для університетської комп’ютерної мережі потрібно окремі VLAN для кожного корпусу, а також окремі VLAN для охорони (камер), та для адміністраторів. Це потрібно щоб можна було локалізувати певні інциденти в певній частині мережі, а не шукати потім по всій мережі. У даному випадку буде розглянуто варіант з 7 VLAN.

Приклад розміщення VLAN можна побачити на рисунку 2.1

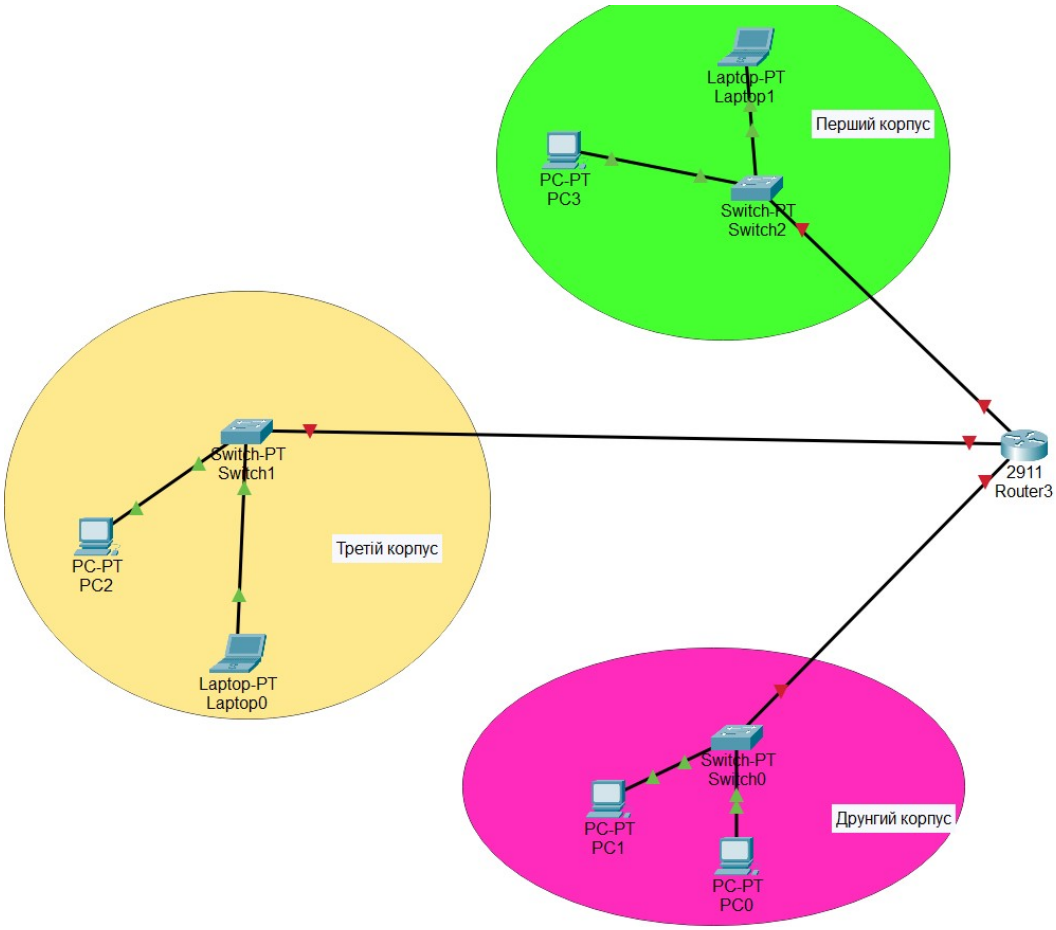


Рисунок 2.1 – Приклад розміщення VLAN в університетській комп’ютерній мережі

Ось перелік VLAN для даної роботи:

- VLAN для першого корпусу;
- VLAN для другого корпусу;
- VLAN для третього корпусу;
- VLAN для четвертого корпусу;
- VLAN для відеоспостереження;
- VLAN для адміністраторів;
- VLAN для всіх інших користувачів.

Тепер потрібно розібрати причини створення всіх цих VLAN, та їхні IP-адреси.

VLAN для кожного корпусу потрібний щоб локалізувати випадки інцидентів в одному корпусі, і щоб цей інцидент не мав впливу на інші частини мережі. VLAN для відеоспостереження потрібний для того, щоб до всіх камер відеоспостереження був доступ лише певним особам, які мають таке право. Також він надає змогу безперебійно спостерігати та, у випадку потреби, протидіяти інцидентам, спричиненими фізично на території університету. VLAN для адміністраторів потрібний щоб полегшити роботу та збільшити продуктивність робітникам, які працюють з мережею. VLAN для всіх інших користувачів потрібний для всіх інших користувачів, які користуються мережею, та, у деяких випадках, для певних аудиторій.

Для VLAN першого корпусу буде використано IP-адреси 172.16.12.0/22 (172.16.12.1 – 172.16.15.254).

Для VLAN другого корпусу буде використано IP-адреси 172.16.24.0/22 (172.16.24.1 – 172.16.27.254.

Для VLAN третього корпусу буде використано IP-адреси 172.16.34.0/23 (172.16.34.1 – 172.16.35.254).

Для VLAN четвертого корпусу буде використано IP-адреси 172.16.36.0/22 (172.16.36.1 – 172.16.39.254).

VLAN для адміністраторів має свій список IP-адрес, які на жаль вказати не можливо, бо це буде порушувати конфіденційність інформації, яка стосується університетської комп’ютерної мережі.

VLAN для відеоспостереження також має свій список IP-адрес, який також не можливо вказати, через те що це порушить конфіденційність інформації.

Для VLAN всіх інших користувачів буде використано IP-адреси 172.20.0.0/16 (172.20.0.1 – 172.20.255.254).

2.3 WinBox та Bridge (міст)

Для забезпечення стабільної роботи комп'ютерної мережі потрібно спочатку розібратись з програмним забезпеченням, яке буде використовуватись для виконання даного завдання, а також розібрати що таке Bridge (міст), та що він робить у мережевих пристроях. Для початку потрібно розібрати WinBox.

WinBox це програмне забезпечення, яке було створено спеціально для того, щоб налаштовувати пристрої компанії Mikrotik.

Інтерфейс даного програмного забезпечення можна побачити на рисунку 2.2.

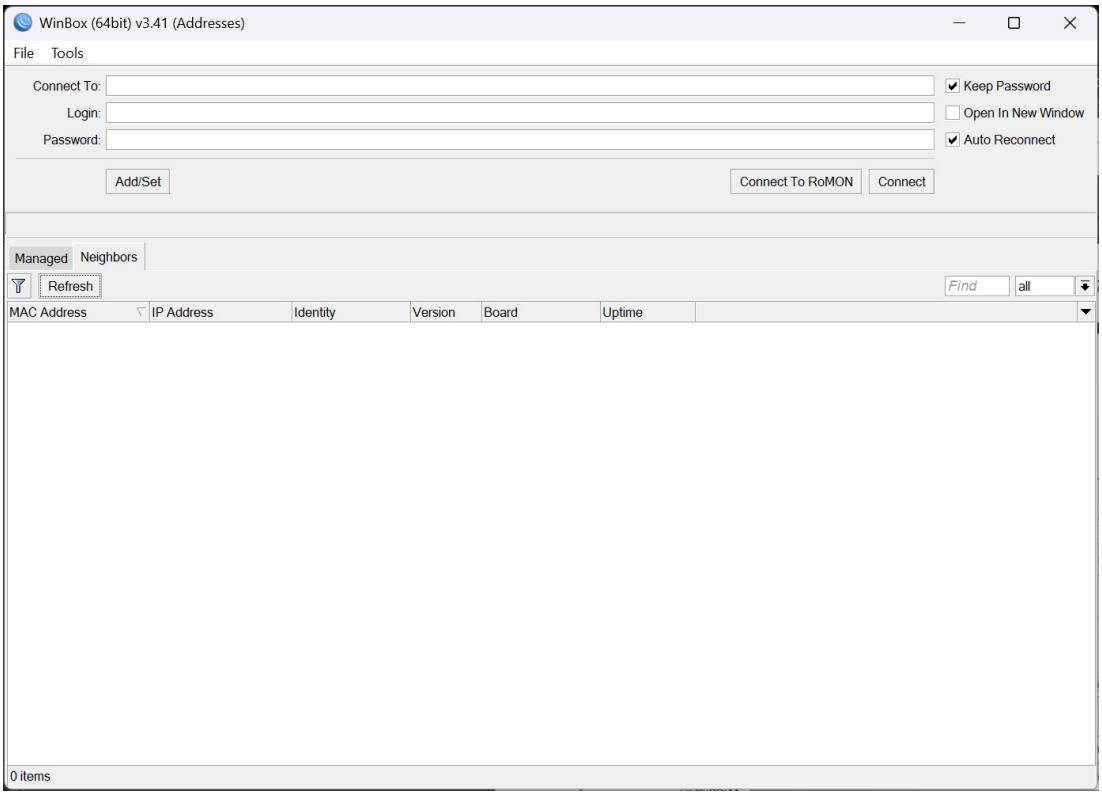


Рисунок 2.2 – Зовнішній вигляд програмного забезпечення WinBox

Розберемось у тому, що означає кожний елемент даної програми.

Поле “Connect To” вказує на те, до якого пристрою буде підключатись. У дане поле можна ввести IP-адресу, MAC-адресу, або натиснути ЛКМ на параметри, через які ми хочемо під’єднатись до пристрою, зі списку у нижній частині програми.

Поле “Login” вказує на те, за допомогою якого користувача ми будемо підключатись до нашого пристрою. Сюди потрібно вписати потрібного нам користувача.

Поле “Password” потрібне для того, щоб ввести пароль конкретного користувача.

Трохи нижче є вкладки “Managed” та “Neighbours”. За допомогою цих вкладок у нас є вибір того, як саме ми будемо підключатись до пристроїв. У вкладці “Managed” відображаються збережені адреси, за допомогою якиї можна підключитись до певних пристроїв. Ці адреси потрібно зберегти самому. У вкладці “Neighbours” ми бачемо всі пристрої, які “WinBox” може «побачити» у нашій мережі. Якщо робота відбувається безпосередньо на підприємстві, то вкладка “Neighbours” буде потрібна набагато частіше. Якщо ж ми працюємо віддалено, то вкладка “Managed” стане в нагоді, бо вкладка “Neighbours” нічого не покаже.

Наступним кроком у процесі побудови університетської комп’ютерної мережі є розуміння того, що таке Bridge (міст), а також визначення його ролі у виконанні даного завдання. Це важливий елемент логічної структури мережі, який дозволяє більш гнучко організовувати взаємодію між різними інтерфейсами та підмережами.

Bridge це програмний мережевий комутатор, який працює на другому рівні моделі OSI (канальний рівень) і дозволяє об’єднати кілька фізичних або віртуальних інтерфейсів в одну логічну мережу. Простими словами, він дає змогу налаштувати декілька портів маршрутизатора або комутатора так, щоб вони поводилися як один як ніби це один загальний порт.

У контексті побудови мережі на базі пристроїв MikroTik, використання bridge є особливо актуальним. MikroTik дозволяє гнучко керувати bridge

конфігураціями через RouterOS, що дозволяє налаштовувати мережу відповідно до конкретних потреб проєкту.

До основних причин використання Bridge у даній роботі можна віднести:

- об'єднання кількох інтерфейсів у одну локальну мережу (LAN), що дозволяє всім пристроям, підключеним до цих інтерфейсів, працювати у спільному мережевому середовищі, ніби вони фізично з’єднані з одним і тим же свічем, а це доволі корисно, наприклад, для об’єднання різних корпусів, які мають свої окремі порти підключення, але входять до одного VLAN;
- забезпечення роботи MikroTik як повноцінного комутатора у випадках, коли маршрутизатор MikroTik використовується не лише для маршрутизації, але й для перемикання (switching) трафіку між пристроями всередині підмережі, функція bridge дозволяє йому працювати як класичний свіч;
- об’єднання фізичних і віртуальних інтерфейсів, наприклад, коли потрібно поєднати реальний порт Ethernet з певним віртуальним VLAN інтерфейсом, то це часто застосовується у випадках, коли фізична структура мережі не співпадає з логічною, і потрібно правильно організувати передавання трафіку VLAN через один порт;
- створення прозорих мостів у більш складних сценаріях, наприклад, при побудові L2 VPN або підключенні до віддалених мереж так, щоб трафік проходив без змін на рівні Ethernet-кадрів, а це дозволяє створювати мережі, де комп’ютери можуть бачити один одного, як ніби вони знаходяться у тій самій локальній мережі, навіть якщо фізично розміщені у різних будівлях чи навіть містах.

2.4 Вибір пристроїв

Для створення відмовостійкої університетської комп’ютерної мережі необхідно на першому етапі чітко визначити, які мережеві пристрої будуть використовуватись під час проєктування та реалізації інфраструктури. Це дозволить не лише побудувати ефективну та стабільну мережу, а й забезпечити її гнучкість, масштабованість та захищеність у випадку аварійних ситуацій.

У даному випадку для побудови мережі було прийнято рішення використовувати обладнання компанії MikroTik, яка зарекомендувала себе як надійний виробник мережевих рішень для різних масштабів проєктів від невеликих офісів до великих корпоративних мереж. MikroTik пропонує функціональні пристрої за доступною ціною, що робить їх популярними у навчальних закладах, зокрема університетах.

У структурі майбутньої мережі будуть застосовуватись:

- маршрутизатор MikroTik CCR2116-12G-4S+, який буде виконувати роль одного з головних пристроїв, який забезпечує керування трафіком, маршрутизацію між VLAN та обробку ключових мережевих процесів;

- комутатор MikroTik CRS326-24G-2S+, який застосовуватиметься для організації дротових підключень користувачів, серверів та точок доступу в окремих корпусах університету;

- оптичний комутатор MikroTik CRS317-1G-16S+, який призначений для високошвидкісного з'єднання між корпусами через оптоволоконні лінії, що дозволяє забезпечити швидкий обмін даними між основними вузлами мережі.

На початковому етапі впровадження важливо ознайомитися з тим, як виглядає маршрутизатор MikroTik CCR2116-12G-4S+, оскільки саме він відіграватиме ключову роль у побудові загального логічного центру мережі. Розуміння його зовнішнього вигляду, габаритів, роз’ємів та розташування елементів керування допоможе правильно його встановити, підключити та інтегрувати у загальну інфраструктуру. Його зовнішній вигляд можна побачити на рисунку 2.3.

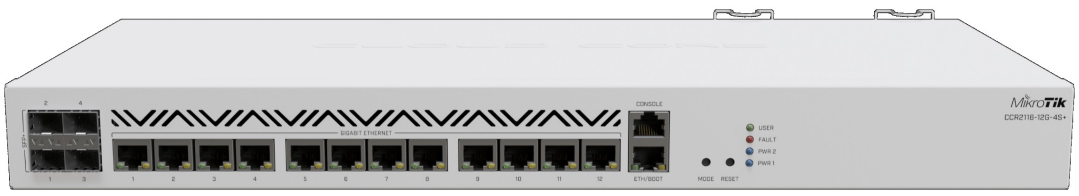


Рисунок 2.3 – Зовнішній вигляд приладу MikroTik CCR2116-12G-4S+

Далі потрібно розібратись як виглядає MikroTik CRS326-24G-2S+. Його

зовнішній вигляд можна побачити на рисунку 2.4.

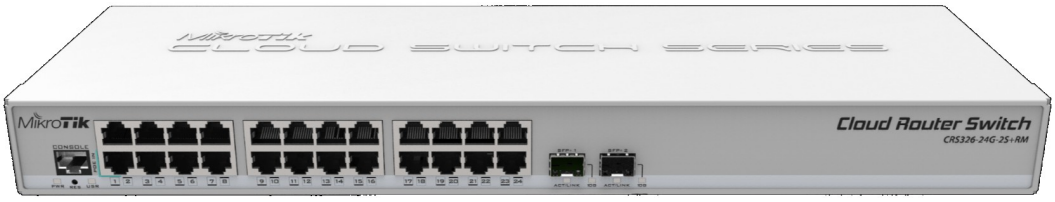


Рисунок 2.4 – Зовнішній вигляд приладу MikroTik CRS326-24G-2S+

Далі потрібно розібратись як виглядає MikroTik CRS317-1G-16S+. Його зовнішній вигляд можна побачити на рисунку 2.5.

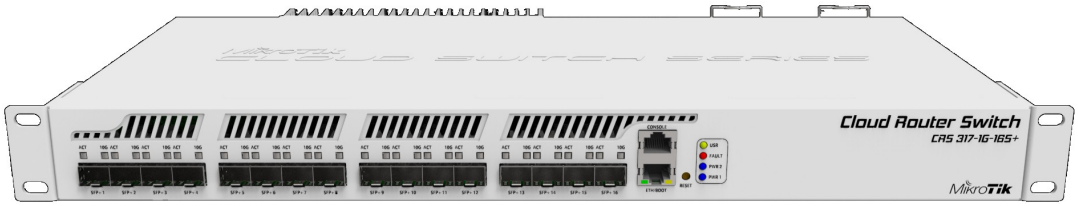


Рисунок 2.5 – Зовнішній вигляд приладу MikroTik CRS317-1G-16S+

Наступним кроком потрібно детально розібратися з тим, які характеристики має кожен з наявних мережевих пристроїв, щоб повною мірою зрозуміти їх можливості, функціональність, а також визначити їхнє доцільне використання в межах університетської комп’ютерної мережі. Такий аналіз дозволить раціонально розподілити ресурси, уникнути перевантаження окремих сегментів мережі та забезпечити стабільну й ефективну її роботу.

Перш за все, варто звернути увагу на маршрутизатори. Це ключові пристрої, що забезпечують маршрутизацію трафіку між різними мережами та VLAN. Університетські маршрутизатори повинні мати достатню обчислювальну потужність, високу пропускну здатність, підтримку сучасних протоколів (наприклад, OSPF, BGP), а також функції безпеки, зокрема фільтрацію трафіку, захист від DDoS-атак, VPN-тунелі тощо. Важливою характеристикою є також кількість портів та їх тип (Gigabit Ethernet, SFP+), що впливає на швидкість та масштабованість мережі.

Далі потрібно розглянути керовані комутатори (switches). Вони

відповідають за розподіл трафіку всередині однієї мережі або VLAN і можуть підтримувати функції віртуалізації, пріоритезації трафіку (QoS), моніторингу (наприклад, SNMP), агрегації каналів та виявлення петлей (STP). Деякі моделі також мають вбудовані функції маршрутизації на рівні 3, що дозволяє реалізовувати складніші мережеві схеми. Комутатори використовуються для підключення кінцевих пристроїв, наприклад комп'ютерів, принтерів, камер відеоспостереження, Wi-Fi точок доступу тощо.

MikroTik CCR2116-12G-4S+ це високопродуктивний маршрутизатор корпоративного класу, який ідеально підходить для обробки великих обсягів трафіку в середніх і великих мережах. Пристрій належить до потужної серії Cloud Core Router (CCR) і спроєктований для сценаріїв, де необхідна максимальна швидкодія, масштабованість і надійність.

Основу CCR2116 становить сучасна 64-бітна ARM-архітектура, яка забезпечує не лише високу енергоефективність, але й виняткову продуктивність. Пристрій оснащений 8-ядерним процесором Amazon Annapurna Labs AL73400, що працює на частоті 2.0 ГГц, і підтримує 16 потоків одночасної обробки даних, що робить його здатним до роботи з надзвичайно інтенсивним трафіком без втрати швидкості.

До ключових переваг даного пристрою можна віднести:

- апаратне прискорення маршрутизації L3, яке суттєво знижує навантаження на процесор і забезпечує стабільну обробку великої кількості маршрутів та пакетів;

- 12 гігабітних Ethernet портів (12x 1G RJ45), що забезпечують підключення різноманітних мережевих пристроїв і сегментів;

- 4 високошвидкісні оптичні порти SFP+, кожен з яких підтримує швидкість 10G, дозволяючи використовувати CCR2116 як ядро мережі або гігабітний шлюз у дата-центрах;

- висока надійність завдяки підтримці резервного живлення (Dual power supply support), яка являється критично важливою функцією для підприємств, де безперервна робота обладнання має ключове значення;

- розширені можливості маршрутизації, фільтрації трафіку, VPN, QoS та

інші функції корпоративного рівня.

CCR2116-12G-4S+ це не просто маршрутизатор, а центральний елемент для побудови масштабованої, безпечної та стабільної мережевої інфраструктури. Він ідеально підходить для використання у великих офісах, дата-центрах, телекомунікаційних компаніях та інтернет-провайдерах, які потребують швидкого, надійного та багатофункціонального рішення.

Характеристики пристрою MikroTik CCR2116-12G-4S+ можна побачити у таблиці 2.1.

Таблиця 2.1 – Характеристики пристрою MikroTik CCR2116-12G-4S+

CPU (процесор)	AL73400 2 ГГц
Ethernet порти (DownLink)	13 Ethernet 10/100/1000 Гбіт/с
Ethernet порти (Uplink)	4 SFP+
ROM/RAM	RAM 16 Гб
Живлення	100-240В AC
Монітор температури на платі	Підтримує
Операційна система	RouterOS
Порт живлення	2 AC
Потужність споживання	72 Вт
Розміри	443 x 199 x 44 мм
Робоча температура	-40°C - +60°C

MikroTik CRS326-24G-2S+ це потужний керований гігабітний комутатор з функціями маршрутизації, розроблений для використання в корпоративних, офісних та операторських мережах, де важливими є гнучкість налаштування, висока надійність і ефективність роботи.

Цей пристрій належить до серії Cloud Router Switch (CRS), яка поєднує функціональність повноцінного Layer 2-комутатора з можливостями маршрутизації на базі RouterOS. CRS326-24G-2S+ дозволяє ефективно вирішувати завдання побудови як локальних мереж (LAN), так і більш складних

мережевих топологій із використанням оптичних ліній зв’язку.

До ключових переваг пристрою можна віднести:

- 24 гігабітні порти Ethernet (10/100/1000 Мбіт/с), які дозволяють зручно організувати доступ користувачів до мережі або з’єднання між різними мережевими сегментами;
- 2 високошвидкісні порти SFP+, що підтримують до 10 Гбіт/с кожен ідеально підходять для агрегації трафіку або для з'єднання з іншими комутаторами чи мережевими ядрами на високих швидкостях;
- можливість вибору між операційними системами SwOS та RouterOS;
- низьке енергоспоживання, що робить його ідеальним варіантом для енергоефективної інфраструктури;
- компактний форм-фактор (металевий корпус, 1U) дозволяє легко розміщувати пристрій у серверних шафах або настінних рішеннях;
- інтуїтивно зрозуміле веб-інтерфейсне управління через Winbox.

Цей комутатор ідеальне рішення для компаній малого та середнього бізнесу, офісів, філій підприємств, шкіл, готелів та навіть невеликих дата-центрів, де необхідна стабільна гігабітна мережа з можливістю масштабування.

MikroTik CRS326-24G-2S+ забезпечує оптимальне поєднання ціни, продуктивності та функціональності, що робить його одним із найпопулярніших комутаторів у своєму класі. Характеристики пристрою MikroTik CRS326-24G-2S+ можна побачити у таблиці 2.2.

Таблиця 2.2 – Характеристики пристрою MikroTik CRS326-24G-2S+

1	2
CPU (процесор)	98DX3236A1-BTD4C000 800 MHz, 1 ядро
RAM	512 MB
Flash	16 MB
Операційна система	RouterOS або SwitchOS
Електроживлення	24 V, 1.5 A, PoE in: 10-30V on Ether1

Кінець таблиці 2.2

1	2
Споживання	≤24
Порти	24 × 10/100/1000 Mbit/s Ethernet with Auto-MDI/X 2 × SFP+ cage Gigabit Ethernet (Mini-GBIC; SFP модуль не поставляється, підтримуються модулі 1.25 Gb SFP та 10 Gb SFP+) 1 × serial port RJ45
Розміри	440 x 144 x 44 мм
Робоча температура	-40°C - +60°C
Споживання	≤24

MikroTik CRS317-1G-16S+ це високопродуктивний керований комутатор рівня L2/L3, спеціально розроблений для роботи у вимогливих мережевих середовищах. Завдяки своїм технічним характеристикам, цей пристрій ідеально підходить для використання в ядрах мереж (core), серверних фермах, дата-центрах, а також у провайдерських інфраструктурах, де критично важливими є висока пропускна здатність, надійність та стабільність з'єднання.

CRS317-1G-16S+ обладнаний 16 оптичними портами SFP+, кожен з яких підтримує швидкість передачі даних як у 1G, так і у 10G, що дає змогу гнучко масштабувати мережу залежно від потреб. Така кількість високошвидкісних портів дозволяє ефективно об'єднувати велику кількість серверів або мережевих сегментів у єдину інфраструктуру з мінімальними затримками.

Комутатор також оснащений одним гігабітним Ethernet-портом (1G RJ45) для управління або резервного підключення. Однією з важливих переваг є подвійна система живлення (dual power supply), яка забезпечує додаткову надійність та безперервну роботу навіть у випадку відмови одного з джерел живлення.

Ще однією особливістю пристрою є можливість вибору між двома операційними системами RouterOS та SwitchOS.

Пристрій забезпечує апаратне прискорення обробки L2/L3-трафіку, що дозволяє зменшити навантаження на процесор і підвищити загальну продуктивність мережі. Завдяки високій щільності портів у компактному 1U корпусі, CRS317-1G-16S+ дозволяє зекономити місце в серверній шафі без компромісів по функціональності.

Цей комутатор є чудовим вибором для тих, хто шукає потужне, надійне та гнучке рішення з підтримкою 10G-мережі, що легко інтегрується в існуючу інфраструктуру та забезпечує стабільну роботу на довгі роки.

Характеристики пристрою MikroTik CRS317-1G-16S+ можна побачити у таблиці 2.3.

Таблиця 2.3 – Характеристики пристрою MikroTik CRS317-1G-16S+

CPU (процесор)	98DX8216 800 МГц ARM 32bit
Ethernet порти (DownLink)	16 (підтримує модулі SFP 1,25 Гбіт/с та SFP+ 10 Гбіт/с; модулів немає в комплекті), підтримка DDMI
ROM/RAM	16Мб/1Гб
Живлення	100-240 В
Монітор температури на платі	Підтримує
Операційна система	RouterOS / SwitchOS
Потужність споживання	44 Вт
Розміри	443 x 224 x 44 мм
Робоча температура	-20°C - 60°C

У даному випадку університетська комп’ютерна мережа складається саме з даних пристроїв, що дозволяє без перешкод використовувати різні функції для забезпечення відмовостійкості мережі. Також можна зазначити, що пристрої даної компанії мають чудову якість, відносно не дорогу ціну та можливість

підтримувати різні функції, які потрібні для забезпечення безперебійної комп'ютерної мережі. Саме завдяки даним позитивним моментам можна зазначити, що університетська комп'ютерна мережа може мати доволі гарну продуктивність, чудову контрольованість завдяки наявним функціям моніторингу та можливість зробити мережу відмовостійкою.

2.5 Trunk порти

Trunk порт це спеціальний тип порту мережевого пристрою (зазвичай комутатора або маршрутизатора), який призначений для передавання трафіку з кількох VLAN (віртуальних локальних мереж) через один фізичний інтерфейс. У звичайних умовах кожна VLAN передавалася б окремим кабелем, але завдяки Trunk-портам можна об'єднати цей трафік і передавати його по одному каналу зв'язку, що значно спрощує інфраструктуру та зменшує витрати на обладнання та кабелі.

Щоб розрізняти пакети, що належать до різних VLAN, у trunk-трафік додається спеціальна мітка (тег). Найпоширенішим стандартом для тегування VLAN-пакетів є IEEE 802.1Q, який додає 4-байтовий тег до Ethernet-кадру. Цей тег містить ідентифікатор VLAN (VLAN ID), завдяки чому кінцевий пристрій або наступний комутатор може правильно обробити трафік відповідно до належної VLAN.

Trunk порти використовуються переважно між комутаторами або між комутатором і маршрутизатором, а також у випадках, коли один пристрій повинен взаємодіяти з кількома VLAN. Наприклад, якщо є офіс із кількома відділами, кожен з яких знаходиться у власній VLAN, то замість прокладки окремого кабелю до кожного відділу, можна використати одне trunk з'єднання, що передаватиме трафік усіх VLAN.

До переваг trunk портів можна віднести:

- зменшення кількості кабелів та портів, бо один фізичний порт може передавати трафік кількох VLAN, що зменшує потребу в зайвому обладнанні;

- гнучкість, бо легко додавати нові VLAN без фізичного втручання;
- масштабованість, бо мережу можна легко розширювати, підключаючи нові пристрої та сегменти;
- оптимізація топології, бо дозволяє ефективніше організувати мережеву інфраструктуру, особливо у великих або розподілених мережах.

Trunk порти є невід'ємною частиною побудови складних VLAN-мереж, особливо у корпоративних, дата-центрових або навчальних інфраструктурах. Вони дозволяють створити чітку логічну структуру в межах єдиної фізичної мережі.

У випадку з MikroTik, підтримка trunk-функціональності реалізована через механізм Bridge VLAN Filtering, який дозволяє визначати, які порти комутатора належать до яких VLAN, які з них є access, а які trunk. MikroTik також підтримує IEEE 802.1Q, що дозволяє легко інтегрувати ці пристрої з обладнанням інших виробників.

2.6 Визначення головних пристроїв для реалізації VRRP

Для даного завдання також потрібно ретельно розібратися з тим, який пристрій буде виступати у ролі головного для кожного VLAN. Це рішення має базуватись не лише на технічних характеристиках мережевого обладнання, а й на ряді додаткових чинників. У першу чергу, важливо враховувати фізичне розташування корпусів університету, а також місця розташування головних маршрутизаторів. Від цього залежить як ефективність маршрутизації, так і мінімізація затримок у мережі.

Окрім того, слід проаналізувати, наскільки часто у відповідних корпусах трапляються перебої з електропостачанням. Якщо маршрутизатор знаходиться у корпусі, де часто вимикається світло, то є ризик втрати зв'язку для всього VLAN, якщо не передбачено резервного живлення. Водночас, у деяких частинах університету встановлено системи безперебійного живлення (UPS або генератори), які дозволяють продовжувати роботу навіть під час аварійного

вимкнення електроенергії. Така інфраструктура значно підвищує надійність мережі, тому у цих корпусах доцільно розміщувати головні пристрої для критично важливих сегментів VLAN.

Також потрібно враховувати схему підключення кінцевих користувачів – студентських аудиторій, комп'ютерних класів, адміністративних приміщень тощо. Якщо більшість користувачів VLAN фізично підключені ближче до одного з маршрутизаторів, то це також аргумент на користь призначення цього маршрутизатора як головного.

Спочатку потрібно чітко визначити, де саме розташовані головні маршрутизатори. В університеті наявно два основні маршрутизатори, які забезпечують функціонування всієї університетської мережі. Перший з них встановлений у четвертому корпусі, а другий – у бібліотеці. Обидва ці об'єкти відіграють стратегічну роль у мережевій інфраструктурі, проте мають певні відмінності.

Такий розподіл дозволить оптимізувати мережеве навантаження, забезпечити стабільність з'єднання та зробити мережу університету більш стійкою до аварій та збоїв. У подальшому також слід розглянути можливість створення механізмів автоматичного перемикання між маршрутизаторами у разі відмови одного з них, що забезпечить додатковий рівень відмовостійкості.

Якщо порівняти ці дані з тим, як розташовані корпуси, у яких потрібно буде проведено той чи інший VLAN, то можна сказати, що буде раціонально використати перший та другий маршрутизатори у ролі головного у такому форматі:

Маршрутизатор, який знаходиться у четвертому корпусі виступає головним для таких VLAN:

- VLAN для третього корпусу;
- VLAN для четвертого корпусу;
- VLAN для адміністраторів;
- VLAN для відеоспостереження;
- VLAN для всіх інших користувачів.

Маршрутизатор, який знаходиться у бібліотеці виступає головним для таких

VLAN:

- VLAN для першого корпусу;
- VLAN для другого корпусу.

Далі потрібно розібрати варіант використання цих двох маршрутизаторів у ролі головного для різних VLAN за допомогою знань того, де, коли та наскільки часто відбувається вимкнення світла у різних будівлях, та те, які будівлі мають резервне живлення, яке забезпечує безперебійну роботу навіть у випадку, коли інші будівлі залишились без світла. Проаналізувавши дану інформацію можна сказати, що буде раціонально використати перший та другий маршрутизатори у ролі головного для певних VLAN у такому вигляді:

Маршрутизатор, який знаходиться у четвертому корпусі виступає головним для таких VLAN:

- VLAN для четвертого корпусу;
- VLAN для всіх інших користувачів.

Маршрутизатор, який знаходиться у бібліотеці виступає головним для таких VLAN:

- VLAN для першого корпусу;
- VLAN для другого корпусу;
- VLAN для третього корпусу;
- VLAN для відеоспостереження;
- VLAN для адміністраторів.

Для реалізації схеми, яка буде забезпечувати максимальну відмовостійкість університетської комп’ютерної мережі потрібно використати саме другий варіант тому, що мета створення даної комп’ютерної мережі полягає у тому, щоб забезпечити відмовостійкість комп’ютерної мережі.

3 СТВОРЕННЯ ВІДМОВОСТІЙКОЇ УНІВЕРСИТЕТСЬКОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ. ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ

3.1 Базові налаштування

Для початку потрібно зробити стандартні налаштування для вхідних маршрутизаторів. Налаштувати пристрої можна за допомогою програмного забезпечення "WinBox".

Наступним кроком потрібно підключитись до маршрутизатора та налаштовую його. Для цього вибираємо пристрій, до якого потрібно підключитись, та вводимо логін та пароль. Далі потрібно зробити стандартні налаштування, щоб в подальшому можна було перейти до налаштувань різних VLAN, створювати DHCP та налаштовувати VRRP.

Для початку потрібно створити користувача, який буде відрізнятись логіном та паролем від стандартного, а далі потрібно видалити (або вимкнути) стандартного користувача. Також при створені нового користувача та налатування паролю для нього потрібно врахувати те, хто цей співробітник, які цілі прислідуються при наданні доступу. Також потрібн врахувати те, що користувачі повинні створити пароль, який буде відповідати політиці безпеки даного підприємства.

Для створення нового користувача потрібно зайти у вкладку System/User, далі натиснути на кнопку "+". Ця кнопка знаходиться у лівому верхньому куті. Потім потрібно вказати які права доступу будуть надані даному користувачу. Всього наявно три рівні доступу: Read, Write, Full.

Якщо надати рівень доступу Read, то даний користувач зможе лише переглядати конфігурацію пристрою, а налаштовувати його він не зможе.

Рівень доступу Write дозоляє переглядатит конфігурацію пристрою, та змінювати частину конфігурації. Користувач з даним рівнем доступу не може створювати користувачів та змінювати права доступу користувачам. Також заборонено доступ до певних системних служб, такий як резервне копіювання/відновлення та оновлення прошивки.

Якщо користувачу буде надано рівень доступу Full, то даний користувач

зможе робити будь-які дії на даному пристрої.

У даному випадку потрібно створити користувача з рівнем доступу Full. Також потрібно не забути вимкнути стандартного користувача. Створення користувача, який буде відрізнятись від стандартного та надання йому рівня доступу Full можна побачити на рисунку 3.1.

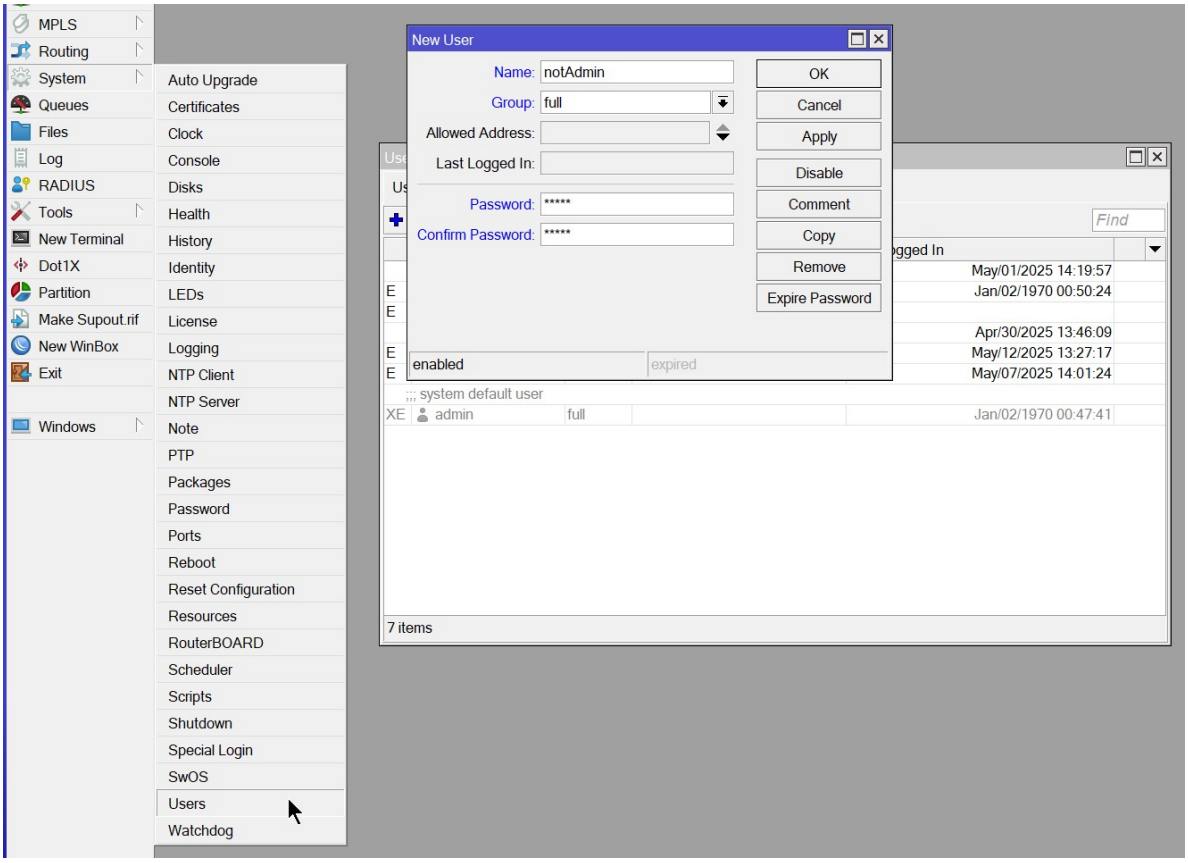


Рисунок 3.1 – Створення користувача та надання відповідних прав доступу

Наступним кроком потрібно створити Bridge та додати в нього майже всі порти. Майже всі тому, що у маршрутизаторі наявні порти, які потрібно зарезервувати для провайдера. Якщо дані порти будуть у Bridge, то справи будуть поганими. Також є інший варіант. Можна додати всі порти у Bridge, а для провайдера створити свій окремий VLAN, який буде створений саме для них, і саме завдяки цьому буде забезпеченно нормальне функціонування мережі.

Створити міст можна у вкладці “Bridge”. Щоб створити самий міст потрібно натиснути кнопку “+”, яка знаходиться у лівому верхньому куті вікна, яке відкрилось.

В налаштуваннях моста потрібно вказати назву моста, а також потрібно перейти у вкладку “Vlan Filtering” та ввімкнутит дану функцію. Ця функція буде потрібна пізніше, бо за допомогою неї можна буде налаштовувати всі VLAN для даної мережі. Створення Bridge можна побачити на рисунку 3.2.

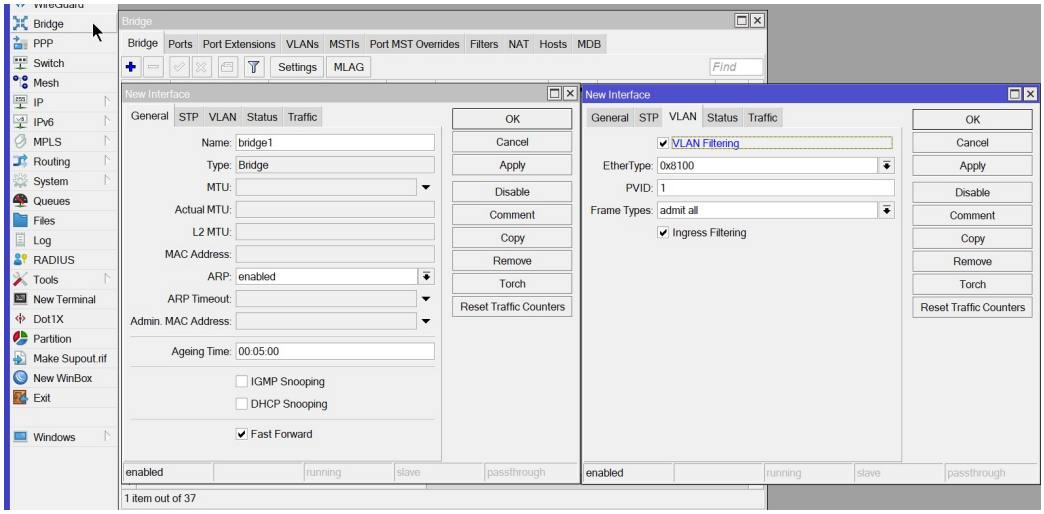


Рисунок 3.2 – Створення Bridge

Після того як створено Bridge (тобто логічне об’єднання портів), наступним кроком є додавання до нього більшості наявних портів пристрою. Це потрібно для того, щоб всі ці порти працювали разом як одна єдина частина мережі, і пристрої, підключені до них, могли спокійно обмінюватися даними між собою.

Щоб це зробити, потрібно перейти у вкладку “Ports” в меню налаштувань. У цій вкладці буде відображено список усіх портів, які можна додати до моста. Для початку додавання потрібно натиснути кнопку “+” у лівому верхньому куті вікна. Після натискання з’явиться вікно з налаштуваннями. У ньому потрібно вказати у який міст буде відбуватись додавання та порт, який буде додано.

Поки що на цьому етапі нічого більше змінювати не потрібно. Достатньо просто додати порти до моста один за одним.

Цей процес є дуже важливим, адже після додавання портів до моста, вони почнуть працювати разом, як єдина частина локальної мережі, що значно спрощує керування мережею та покращує взаємодію між пристроями.Додавання портів у Bridge можна побачиити на рисунку 3.3.

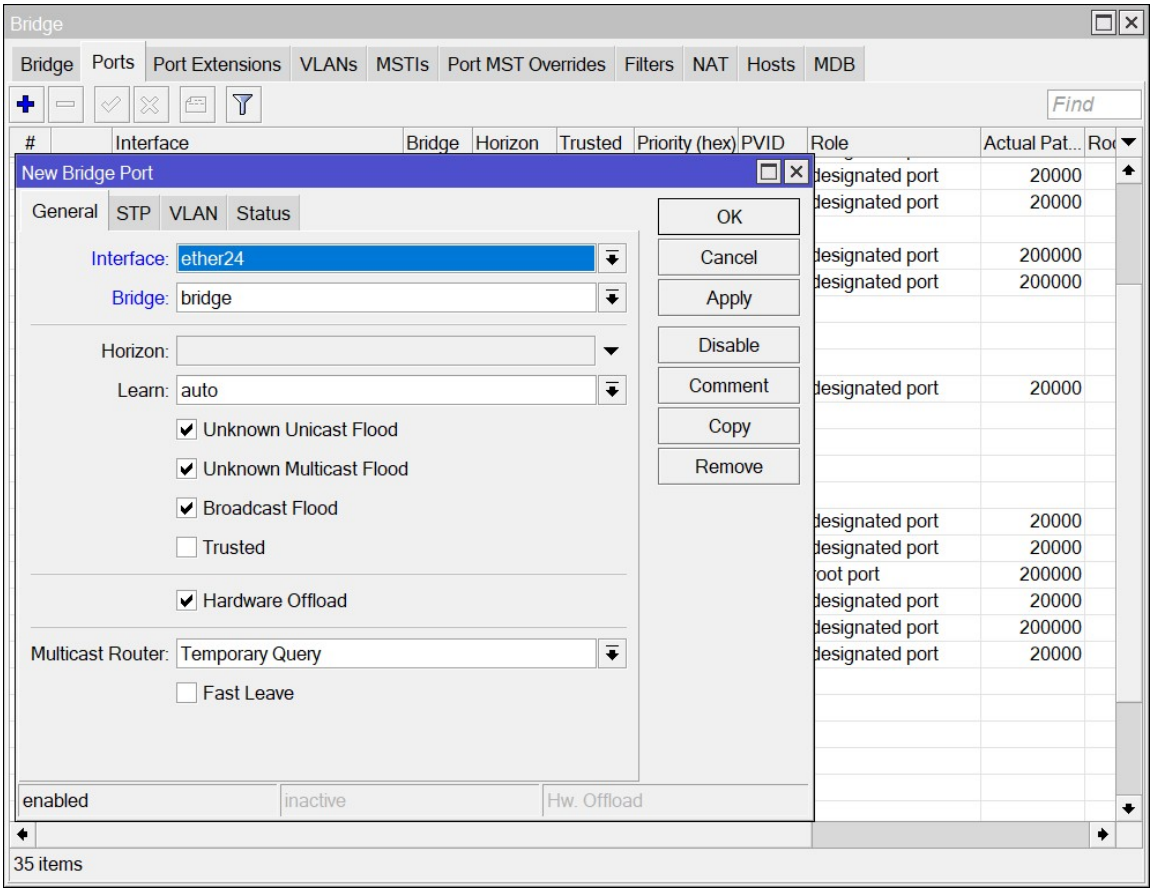


Рисунок 3.3 – Додавання портів у Bridge

3.2 Створення та налаштування VLAN

Після того як ми об’єднали потрібні порти в один міст, наступним кроком є створення VLAN, окремих частин мережі для різних груп користувачів або пристроїв. Це допоможе впорядкувати мережу, зробити її більш безпечною та керованою.

Щоб створити VLAN, потрібно відкрити вкладку “Interfaces” у меню налаштувань. У цій вкладці ми працюємо з усіма мережевими підключеннями пристрою. У верхньому лівому куті знаходиться кнопка з плюсом “+”. Далі натискаємо на неї, щоб додати новий елемент.

Після натискання з’явиться список, де потрібно вибрати пункт “VLAN”. Це відкриє вікно створення нового VLAN.

У цьому вікні потрібно вказати до якого порту буде прив’язаний VLAN. У даному випадку ним являється раніше створений міст, адже через нього буде

проходити весь трафік усередині локальної мережі.

Також потрібно вказати VLAN ID. Це просто унікальний номер, який дозволяє відрізняти один VLAN від іншого. Для кожного VLAN потрібно вказувати свої індивідуалні значення. На одинакових VLAN у тразних пристроях буде використовуватись одинакове значення.

А ще потрібно вказати назву VLAN. Потрібно вказувати назву, яка буде зробуміла до якого сегменту мережі належить даний VLAN. Це значно полегшує розуміння та подальшу роботу з мережею.

Після заповнення цих полів можна зберегти налаштування. Створення декількох VLAN таким чином дозволяє чітко розмежувати різні частини університетської мережі, розподілити навантаження та краще контролювати доступ між ними. Створення VLAN можна побачити на рисунку 3.4.

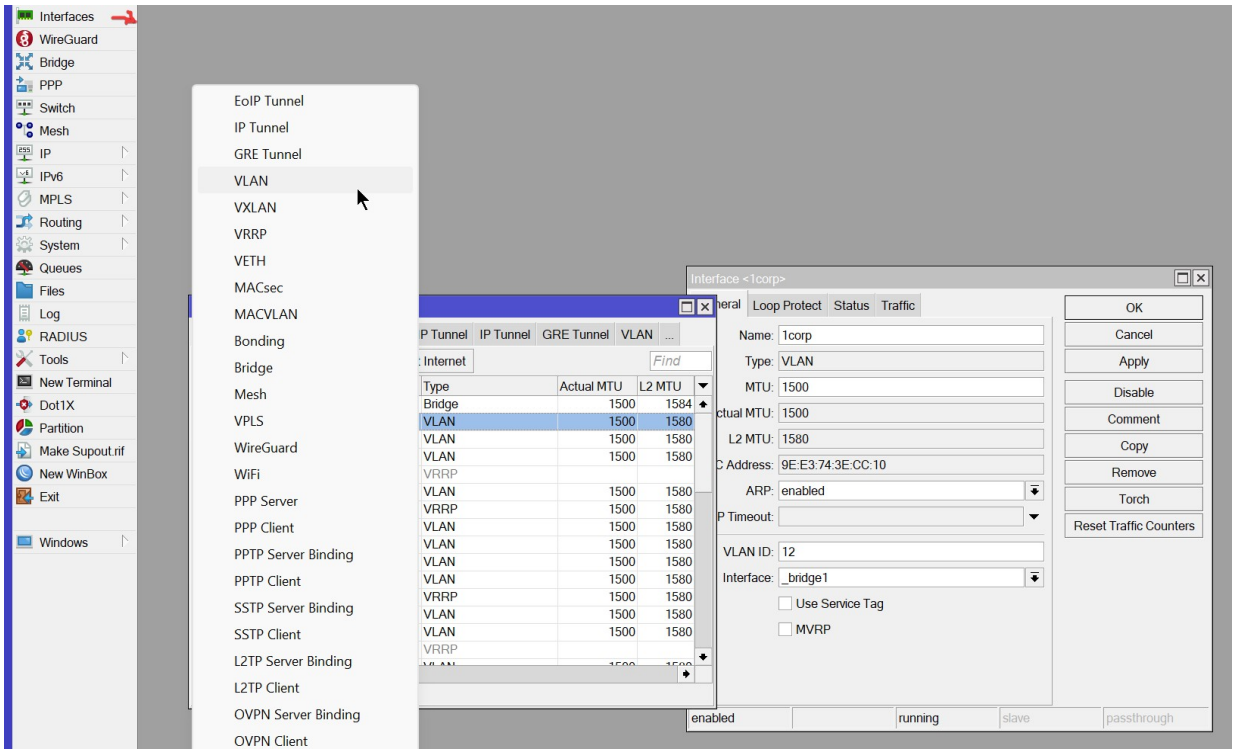


Рисунок 3.4 – Створення VLAN

Наступним важливим кроком є додавання всіх створених VLAN до нашого раніше налаштованого моста. Це необхідно для того, щоб усі частини мережі, які ми розділили за допомогою VLAN, могли правильно працювати разом через один спільний центр з’єднання.

Щоб це зробити, потрібно знову повторити дії, подібні до тих, які вже виконувались раніше на рисунку 3.3. Знову переходимо до вкладки, де додаються порти до моста, і для кожного VLAN створюємо окремий запис.

Однак цього разу є ще один важливий момент. Після того як вказали міст і обрали порт (у даному випадку потрібний VLAN), необхідно перейти до вкладки “PVID”. У цій вкладці потрібно вказати той самий номер, який було використано раніше під час створення відповідного VLAN. Це потрібно для того, щоб пристрій знав, до якої частини мережі належить цей порт і як правильно спрямовувати трафік, який через нього проходить.

Повторюючи ці дії для кожного VLAN, буде забезпечено правильну прив’язку кожної частини мережі до свого сегменту, що дозволить всій системі працювати злагоджено та ефективно. Завдяки цьому користувачі, підключені до різних VLAN, будуть взаємодіяти лише у межах своєї мережі, що підвищує рівень безпеки та впорядковує загальну структуру.

Додаткові налаштування при додаванні VLAN у Bridge можна побачити на рисунку 3.5.

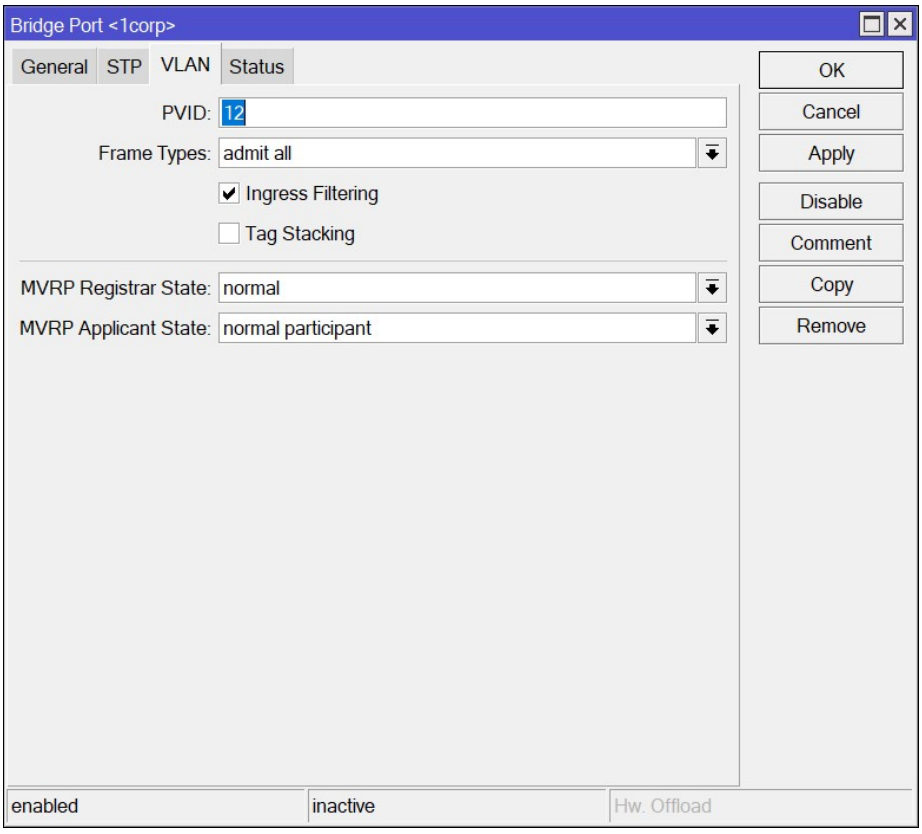


Рисунок 3.5 – Додаткові налаштування при додаванні VLAN у Bridge

Наступним кроком потрібно створити Trunk порти. Для цього раніше було ввімкненно функцію Vlan Filtering при створенні Bridge. Щоб налаштувати певні порти як Trunk порти потрібно зайти у вкладку “Bridge”, а потім зайти у вкладку “VLANs”. Саме у цій вкладці налаштовуються всі Trunk порти. Також у даній вкладці можна побачити вже створенні Trunk порти.

Щоб створити Trunk порт потрібно натиснути на кнопку “+”, яка знаходиться у лівому верхньому куті вікна. При створенні потрібно вказати PVID, на який Bridge буде створено даний Trunk порт, а також вказати Tagged та Untagged порти. Tagged порти це саме Trunk порти. Також потрібно створювати окремі записи для кожного VLAN, бо якщо налаштовувати це іншим методом, то мережа не буде працювати належним чином.

Для нормального функціонування у колонці Tagged потрібно вказати Bridge, вхідний порт (якщо це головний маршрутизатор, то вхідного порта не буде, бо він і являється пристроєм, який буде надавати IP-адреси за допомогою DHCP), та порти, які будуть фізично вмикатись у пристрої, на яких також буде налаштовано різні VLAN, та на яких пристрій буде керувати мережею за допомогою різних VLAN.

Далі потрібно вказати Untagged. Зазвичай вказується лише конкретний VLAN, для якого і створюється trunk порт. При потребі можна вказати пристрої, які будуть виступати кінцевими пристроями, або пристрої, які не будуть займатись регулюванням трафіку за допомогою VLAN. Зазвичай, у колонці Untagged вказується лише конкретний VLAN, а визначення, який порт буде належати конкретному VLAN, відбуваєтсья за допомогою зміни PVID у вкладці “Bridge/Ports”.

Після надання порту PVID потрібного нам VLAN, пристрій компанії MikroTik автоматично буде відносити даний порт як Untagged. Це дозволяє зручніше та ефективніше налаштовувати мережу, бо адміністаторам не потрібно буде кожного разу заходити у налаштування Trunk портів, щоб прибрати один порт з налаштувань Untagged певного Trunk порта та додати даний порт у налаштування до іншого Untagged Trunk порта. Потрібно лише змінити PVID конкретного порта. Створення Trunk портів можна побачити на рисунку 3.6.

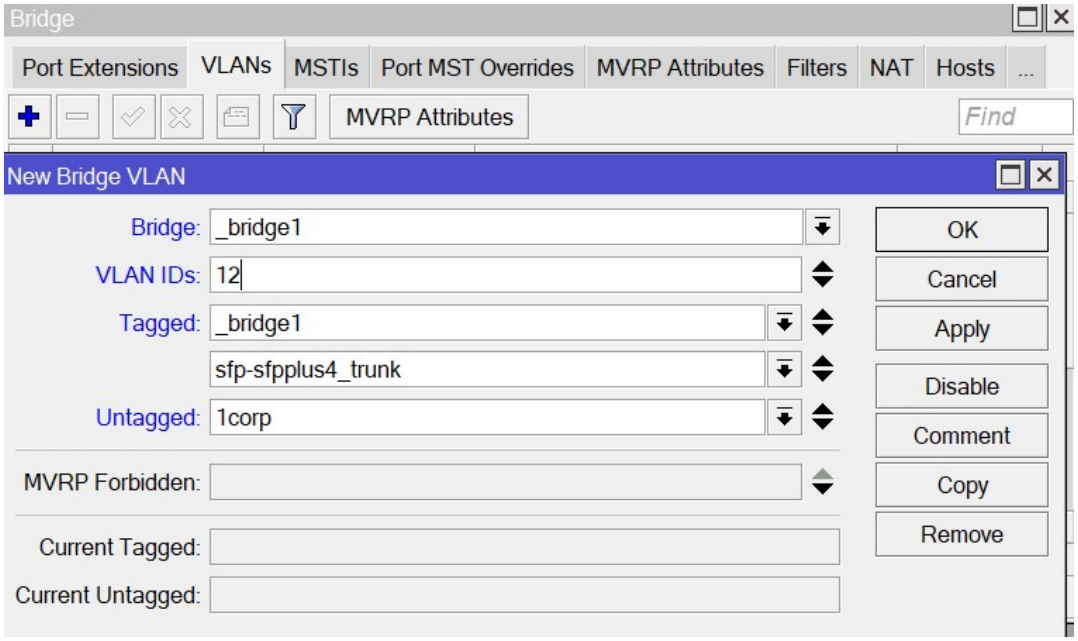


Рисунок 3.6 – Створення Trunk портів

Як вже згадувалося раніше, іноді потрібно зробити так, щоб певний порт був повністю закріплений за конкретною частиною мережі, тобто щоб він “розумів”, до якого саме VLAN належить. Це дозволяє пристроям, підключеним до цього порту, автоматично потрапляти в потрібний сегмент мережі без додаткових налаштувань.

Щоб це зробити, потрібно зайти у меню “Bridge/Ports”, де відображаються всі порти, які вже були додані до моста. Далі потрібно двічі натиснути на той порт, для якого потрібно зробити зміни.

Після цього відкриється вікно з налаштуваннями порту. У цьому вікні потрібно перейти на вкладку “PVID”. Тут і знаходиться найважливіше, бо потрібно просто вказати той номер, який відповідає VLAN, до якого потрібно приєднати цей порт. Наприклад, якщо порт має належати до VLAN з номером 12, то у полі потрібно ввести саме 12.

Це дуже зручний спосіб автоматично “прив’язати” конкретний порт до певної частини мережі. Завдяки цьому підключений до нього комп’ютер або інший пристрій одразу опиниться у потрібному середовищі, без зайвих дій з боку користувача.

Зміна PVID для порта можна побачити на рисунку 3.7.

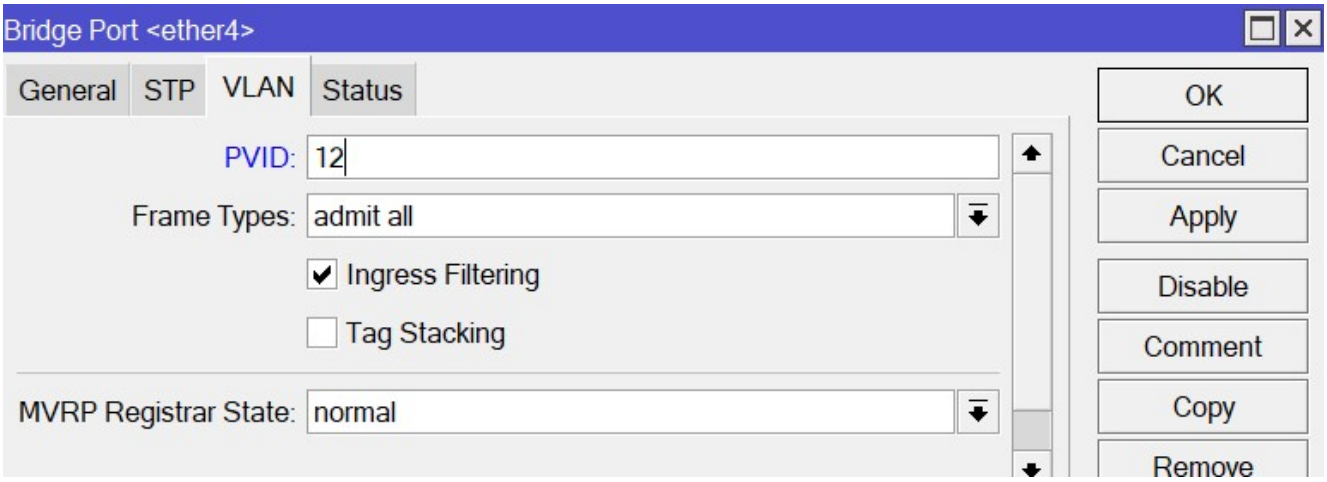


Рисунок 3.7 – Зміна PVID для порта

3.3 Створення та налаштування DHCP

Щоб кожен пристрій у мережі міг автоматично отримувати свою унікальну IP-адресу, потрібно створити DHCP-сервер. Але перед цим слід визначити, які саме діапазони IP-адрес будуть використовуватись для кожної частини мережі. Інакше кажучи, потрібно вирішити, які адреси можна буде "роздавати" пристроям, які підключатимуться до певного сегменту мережі.

Перший крок це створення так званого пулу IP-адрес (тобто списку адрес, які DHCP-сервер зможе видавати). Для цього потрібно відкрити вкладку “IP”, а потім підрозділ “Pool”. Тут зібрані всі набори адрес, які використовуються для автоматичної роздачі.

У верхньому лівому куті потрібно натиснути кнопку**“+”**, щоб додати новий пул. У вікні, що відкриється, потрібно вказати назву пулу, щоб було зрозуміло для якого DHCP він буде використаний.

Далі потрібно вказати початкуву та кінцеві IP адрреси, які будуть використовуватись при роздачі. Потрібно вказувати через тире.

За потреби можна вказати наступний пул. Якщо всі адреси з основного будуть використані, то DHCP почне роздавати IP адреси з наступного.

Це дає гнучкість у налаштуванні мережі й дозволяє уникнути ситуацій, коли новим пристроям не вистачає адрес. Завдяки цьому кожна частина мережі матиме

власний набір адрес, і всі користувачі зможуть без проблем підключатися до мережі та користуватись інтернетом чи внутрішніми ресурсами. Створення Pool можна побачити на рисунку 3.8.

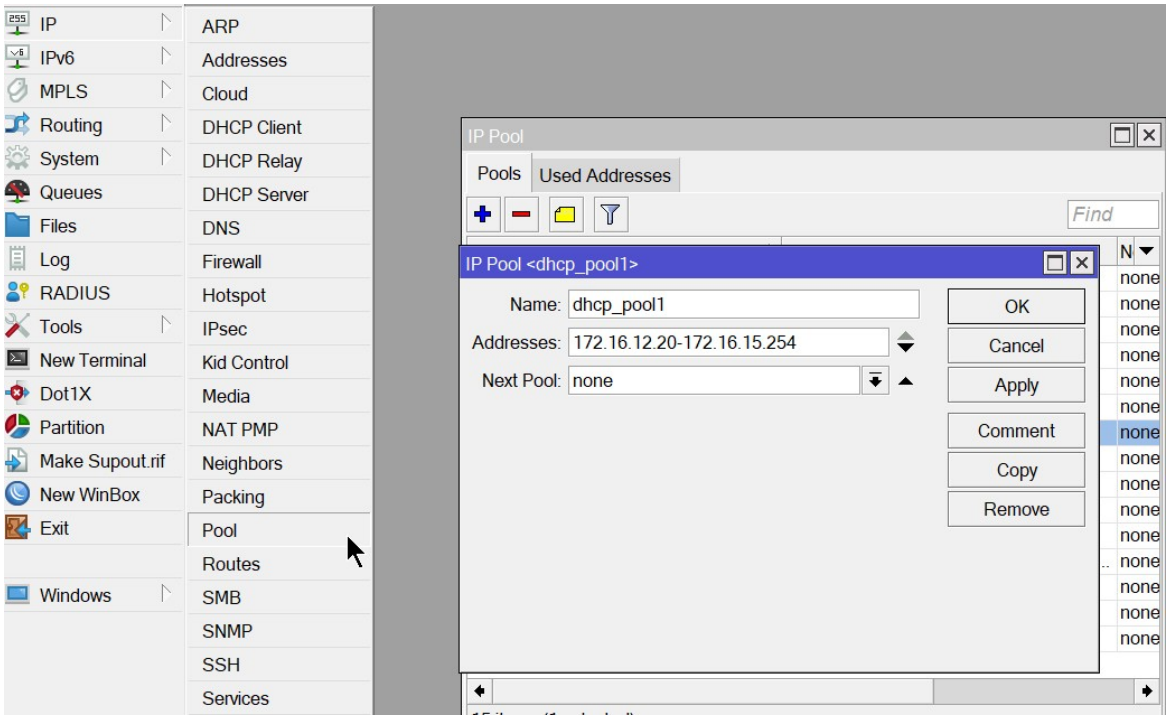


Рисунок 3.8 – Створення Pool

Після того як було створено набір IP-адрес (Pool), які будуть використовуватись для автоматичної роздачі, наступним кроком є створення самого DHCP-сервера, тобто механізму, який буде видавати ці адреси підключеним пристроям.

Для цього потрібно перейти у меню “IP”, а далі обрати розділ “DHCP Server”. У цьому розділі зібрані всі DHCP-сервери, які вже створено або будуть створені для різних частин мережі.

У верхньому лівому куті вікна потрібно натиснути на кнопку “+” для додавання нового DHCP-сервера. Відкриється вікно з налаштуваннями, де потрібно вказати назву DHCP-сервера. Потрібно вказувати зрозумілу назву, яка буде відповідати тому, до якої частини мережі буде застосований даний DHCP. Наприклад, можна написати “DHCP_(назва VLAN)”. Далі потрібно вибрати раніше створений Pool (список IP адрес, завдяки якому DHCP буде знати діапазон

IP адрес, які він може роздавати). Також потрібно вказати порт, для якого створюється даний DHCP. У даному випадку портом буде виступати потрібний VLAN. Потрібно не забути вказати також час видачі адреси. Це означає, наскільки довго IP адреса буде закріплена за кожним пристроєм. Якщо даний час сплине, то або користувач знову отримає дану IP адресу (якщо він активний у даній мережі), або новий користувач отримає дану IP адресу (якщо попередній не активний у період, коли час сплине).

Після заповнення всіх полів можна зберегти налаштування. У результаті кожен користувач або пристрій, що підключається до певного VLAN, буде автоматично отримувати потрібну IP-адресу без необхідності щось додатково налаштовувати вручну.

Створення DHCP-сервера можна побачити на рисунку 3.9.

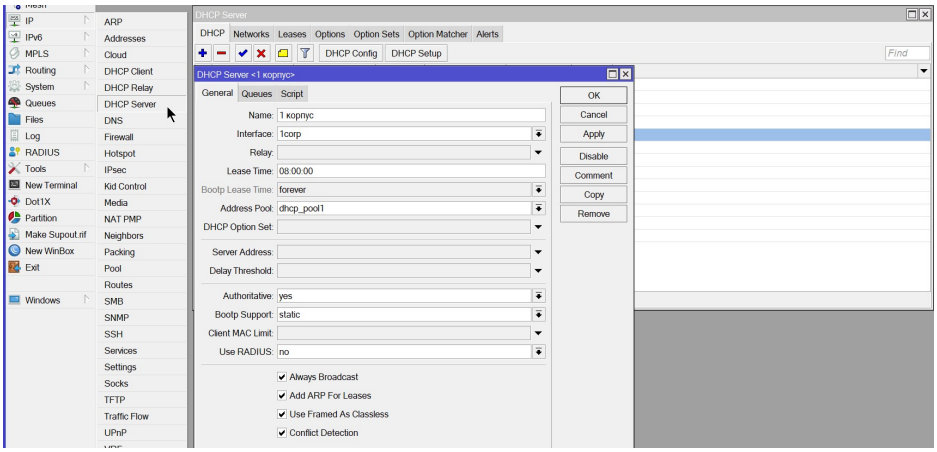


Рисунок 3.9 – Створення DHCP-сервера

Щоб DHCP-сервер правильно працював і міг забезпечити повноцінне підключення до мережі, потрібно вказати основні налаштування для користувачів, які будуть підключатися до певної частини мережі. Зокрема, потрібно вказати, через який “вихід” у мережу буде йти трафік (це називається шлюзом або Default Gateway), а також який сервер буде відповідати за імена сайтів (DNS Server).

Для цього потрібно зайти у меню “IP”, потім обрати розділ “DHCP Server”, і далі перейти у вкладку “Networks”. У цьому розділі можна задати налаштування, які автоматично будуть отримувати всі користувачі тієї чи іншої підмережі.

У верхньому лівому куті потрібно натиснути на кнопку “+”, щоб додати новий запис. У вікні, що відкриється, потрібно вказати підмережу, до якої буде застосовано дані налаштування. Також потрібно вказати шлюз (Default Gateway). Це адреса пристрою, через який користувачі зможуть “виходити” у інші частини мережі. Потрібно не забути також вказати IP адресу DNS-сервера. Це адреса, яка допоможе користувачам перетворювати IP адреси у зрозумілий для людей вигляд. Наприклад, google.com.

У більшості випадків шлюз (Gateway) і DNS Server мають однакові значення, тому що і ту, і ту функцію виконує головний маршрутизатор, який керує всією мережею.

Після збереження налаштувань, кожен пристрій, який підключиться до відповідної частини мережі, отримає ці параметри автоматично. Це забезпечить стабільну роботу мережі, доступ до інтернету та внутрішніх ресурсів без необхідності вручну щось налаштовувати. Дані налаштування можна побачити на рисунку 3.10.

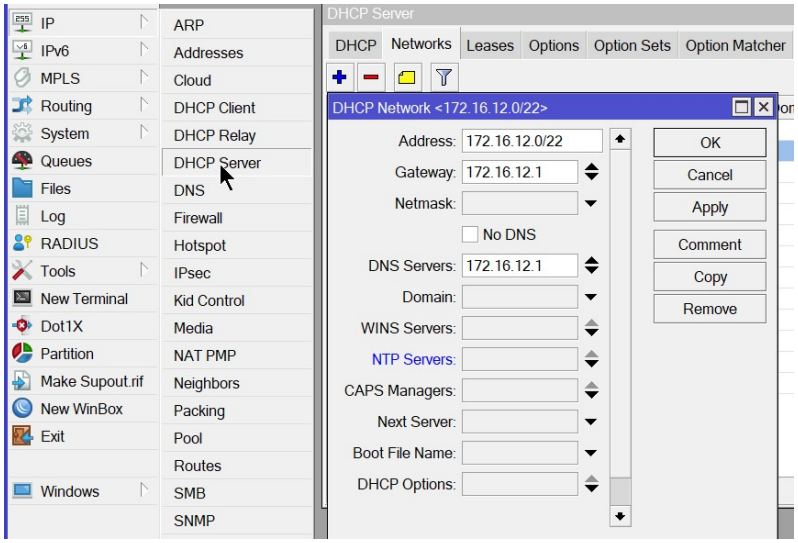


Рисунок 3.10 – Додавання шлюзу за замовчуванням та DNS серверу

Коли налаштування мережі й DHCP-сервера завершено, потрібно присвоїти кожному VLAN свою постійну IP-адресу, через яку до нього звертатимуться всі пристрої в цій частині мережі. Іншими словами, це буде "основна адреса", на яку орієнтуватимуться комп’ютери, щоб знати, куди надсилати запити або з ким

обмінюватись даними.

Ця IP-адреса зазвичай збігається з тією адресою, яку було вказано як Default Gateway. Тобто для кожного VLAN вона буде “центральною” точкою зв’язку.

Для того, щоб надати IP адресу кодному VLAN потрібно зайти у вкладку “IP”, а далі вибрати пункт “Addresses”. Наступним кроком у верхньому лівому куті потрібно натиснути на кнопку “+”, щоб надати IP адресу порту.

Щоб додати дану адресу потрібно вказати IP адресу, яку потрібно закріпити за певним портом. Також потрібно вказати маску підмережі, щоб пристрій міг та знав до якої підмережі належить дана IP адреса. Потрібно не забути також вказати порт, за яким буде закріплена дана IP адреса. У даному випадку потрібно вказати VLAN, для якого створювався DCHP.

Після збереження цих налаштувань конкретний VLAN отримає свою офіційну адресу, через яку до нього зможуть звертатися всі пристрої, які працюють у цій частині мережі. іЦе дуже важливо для правильної роботи всіх з’єднань та сервісів, які використовуються в університетській мережі. Надання IP-адреси інтерфейсам можна побачити на рисунку 3.11.

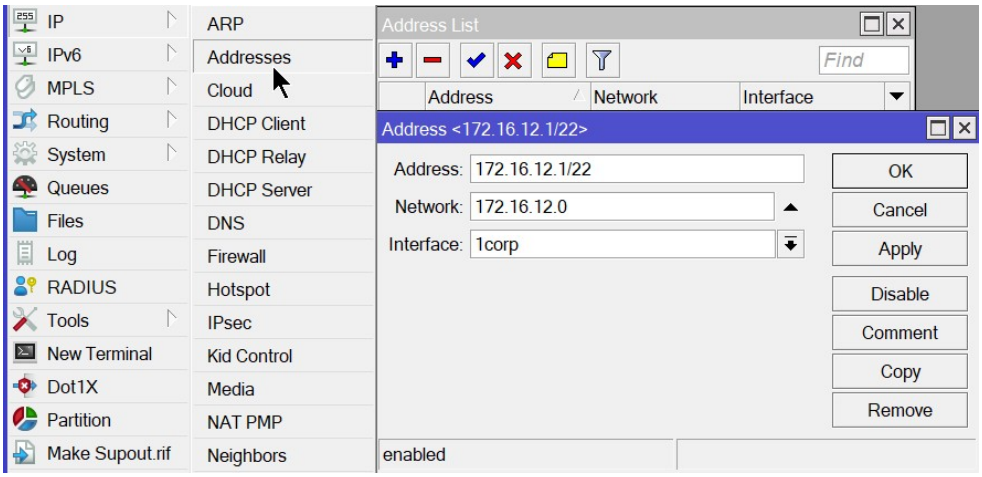


Рисунок 3.11 – Надання IP-адреси інтерфейсам

Якщо не надати IP-адреси інтерфейсу, для якого було створено DHCP, то DHCP працювати не буде тому, що користувачі не будуть знати що саме на даному пристрої було розгорнуто DHCP, через що вони просто не матимуть згоди до нього звернутись, і в результаті не зможуть отримати свою IP-адресу.

3.4 Створення NAT та маскараду

Після того, як було налаштовано внутрішню мережу і всі пристрої можуть між собою обмінюватися інформацією, з’являється наступне завдання, а саме надати доступ до Інтернету для всіх користувачів у мережі. Зараз внутрішня мережа працює добре, але вихід у зовнішню мережу, тобто в Інтернет, ще не налаштований.

Щоб це реалізувати, потрібно зробити спеціальне налаштування, яке дозволяє пристроям з внутрішньої мережі виходити в Інтернет через одну загальну зовнішню адресу. Це досягається за допомогою двох важливих механізмів NAT і маскарад.

NAT (мережева адресація) це спосіб, за допомогою якого маршрутизатор змінює адреси пакетів, коли ті проходять з внутрішньої мережі назовні. Завдяки цьому багато пристроїв можуть користуватись Інтернетом, маючи лише одну зовнішню (публічну) адресу.

Маскарад це один із видів NAT, який автоматично підставляє правильну зовнішню адресу маршрутизатора, через яку відбувається вихід у мережу. Він зручний тим, що не потрібно вручну вказувати конкретну адресу, бо все працює динамічно.

Інакше кажучи, маскарад “ховає” внутрішні адреси за однією зовнішньою, що дозволяє кожному пристрою в мережі користуватись Інтернетом, як ніби він підключений напряму.

Щоб налаштувати NAT і маскарад, потрібно перейти до розділу “IP/Firewall” та відкрити вкладку “NAT”. Потім у верхньому лівому куті натиснути на кнопку “+”, і в налаштуваннях обрати правильні параметри, зокрема вказати, що буде використовуватись дія masquerade. Так маршрутизатор знатиме, що потрібно автоматично підмінювати адреси всім пристроям, які виходять у зовнішню мережу.

Після цього всі користувачі університетської мережі зможуть без проблем користуватись Інтернетом, навіть якщо вони працюють у різних VLAN або знаходяться в різних корпусах. Усі з’єднання будуть проходити через один

основний маршрутизатор, який “перекладає” внутрішні запити в зовнішні й навпаки. Створення NAT та маскараду можна побачити на рисунку 3.12.

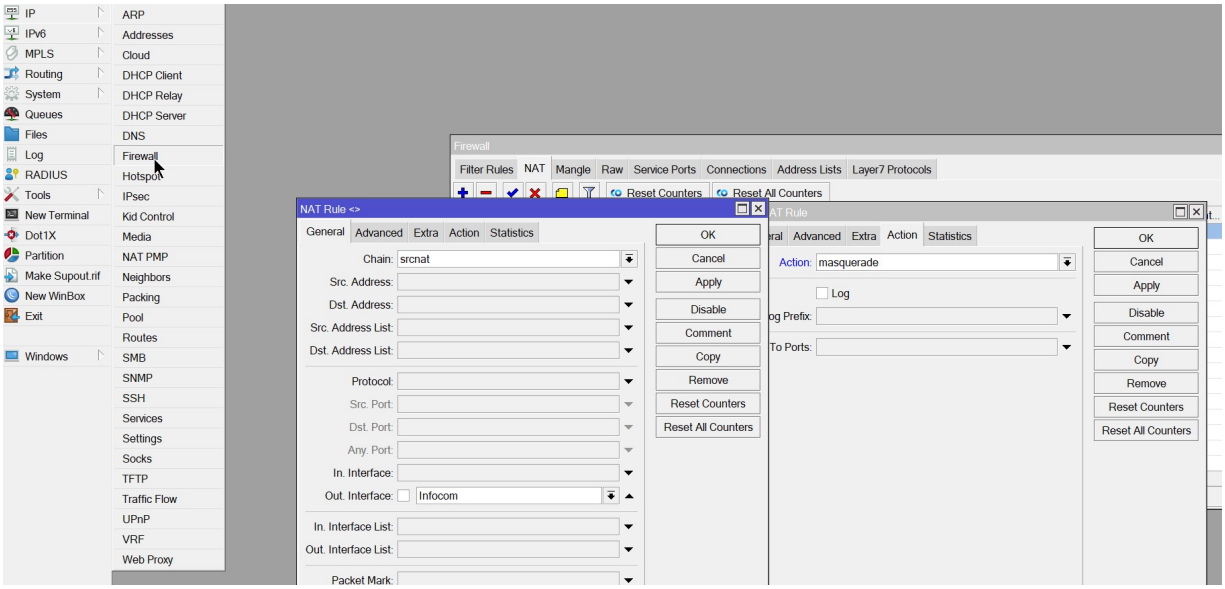


Рисунок 3.12 – Створення NAT та маскараду

Отже, NAT та маскарад відіграють надзвичайно важливу роль у комп’ютерній мережі. Саме завдяки цим налаштуванням усі користувачі всередині локальної мережі можуть мати доступ до Інтернету, навіть якщо в них немає окремої зовнішньої (публічної) IP адреси.

Ця функція стала особливо актуальною через те, що в мережі Інтернет не вистачає “білих” IPv4-адрес, тобто унікальних адрес, які можна було б виділити кожному пристрою. Замість того, щоб виділяти кожному комп’ютеру власну зовнішню адресу, використовується одна спільна для всіх, а маршрутизатор “переводить” дані між внутрішньою мережею і зовнішнім світом.

Іншими словами, завдяки NAT і маскараду мережа працює ефективно навіть у ситуації, коли ресурсів не вистачає, і всі пристрої всередині можуть безперешкодно відкривати сайти, працювати з хмарними сервісами, спілкуватися в месенджерах тощо.

Без цієї функції кожному комп’ютеру потрібна була б окрема унікальна адреса для виходу в Інтернет, а це не лише дорого, а й технічно складно, враховуючи загальну обмеженість IPv4-адрес у світі.

Завдяки NAT та маскараду, університетська мережа може об'єднати велику кількість пристроїв, надати їм доступ до зовнішнього світу, при цьому використовуючи лише одну або декілька зовнішніх адрес.

3.5 Створення та налаштування VRRP

Після того, як мережа була правильно налаштована і все працює як потрібно, важливо зробити її надійнішою, тобто забезпечити відмовостійкість. Це означає, що навіть якщо один із головних пристроїв вийде з ладу або зникне живлення, мережа не припинить свою роботу. Усе продовжить працювати автоматично, бо на себе обов’язки візьме інший пристрій.

Щоб реалізувати цю можливість, використовується спеціальний механізм під назвою VRRP. Це така функція, яка дозволяє двом пристроям "домовитися" між собою: один з них основний, а інший резервний, який автоматично підключається у разі проблем з основним.

Щоб налаштувати VRRP, потрібно перейти у вкладку “Interfaces”. У лівому верхньому куті натиснути кнопку “+”, а далі вибрати “VRRP” зі списку. У вікні, яке з’явиться, потрібно вказати для якого інтерфейсу буде застосований даний VRRP. Також потрібно вказати зрозумілу назву, щоб можна було легше орієнтуватись для якої частини мережі застосовується даний VRPP. Наступним потрібно вказати унікальний ідентифікатор, так званий VRID. Його можна вказати таким самим, як і VLAN ID для якого створюється даний VRRP. Потрібно не забути вказати пріоритетність. Це число, яке буде вказувати на те, який маршрутизатор буде виступати у ролі головного.

Для кожного VLAN потрібно створити окремий VRRP, щоб уся мережа могла автоматично перемикатись у разі неполадок.

Щодо пріоритету, то чим більше число, тим вищий рівень важливості. Наприклад, якщо один маршрутизатор має пріоритет 125, а інший 100, то перший буде головним. Якщо щось станеться з головним, другий автоматично замінить його, і мережа продовжить працювати без зупинки.

Ці значення можна підбирати індивідуально, залежно від можливостей пристрою. Деякі пристрої підтримують числа більші за 100, інші обмежуються саме сотнею. Головне щоб головний пристрій мав більше значення, ніж резервний. У даній роботу будуть використовуватись різні варіанти, а саме ті, коли головний маршрутизатор матиме значення більше 100, та коли головний маршрутизатор матиме значення не більше 100.

Таке налаштування дозволяє створити надійну мережу, яка автоматично відреагує на збій і продовжить працювати, не створюючи проблем для користувачів. Створення VRRP можна побачити на рисунку 3.13.

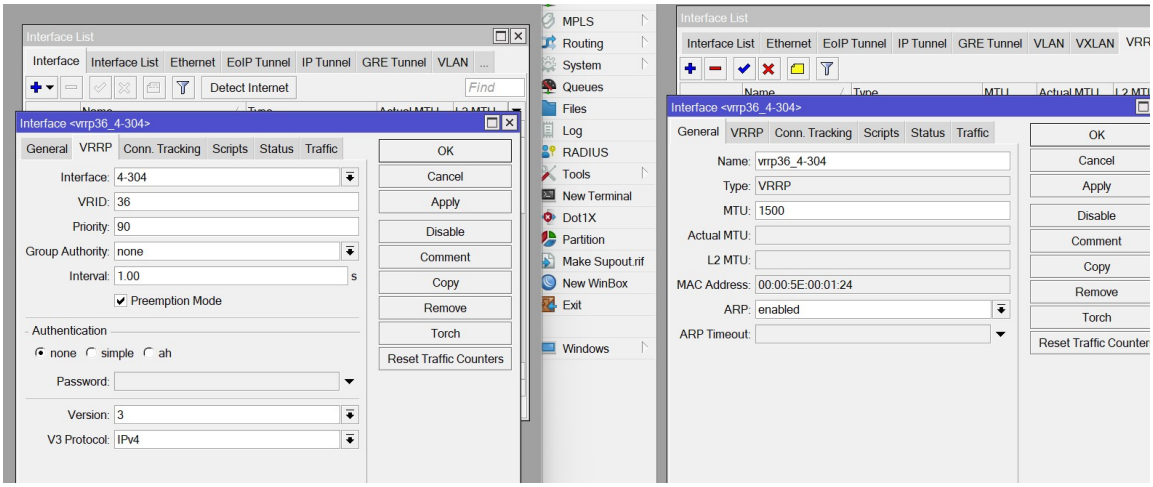


Рисунок 3.13 – Створення VRRP

Після того як був створений VRRP, наступним кроком є призначення йому IP адреси, яка буде використовуватись усіма користувачами певної частини мережі. Це потрібно для того, щоб, незалежно від того, який із маршрутизаторів (головний чи резервний) працює в даний момент, користувачі завжди звертались до однієї і тієї ж адреси, і все працювало стабільно.

Головне, що потрібно пам’ятати в цьому процесі, це IP адреса, яка призначається VRRP, має бути однакова і на головному маршрутизаторі, і на резервному. Тобто обидва пристрої "розуміють", що ця адреса належить до спільного віртуального інтерфейсу, який буде працювати або на одному пристрої, або на іншому залежно від ситуації.

Для кожного створеного VRRP потрібно призначити свою унікальну IP

адресу, яка буде відноситись до відповідного VLAN. Це дозволяє зробити так, щоб кожна частина мережі працювала незалежно та стабільно.

Щоб призначити IP адресу, потрібно виконати ті ж самі дії, що й при звичайному налаштуванні адрес, що було вказано на рисунку 3.10. Єдина відмінність це порт, до якого прив'язується ця адреса. У цьому випадку потрібно вибрати не звичайний порт або VLAN, а саме VRRP інтерфейс, який був створений раніше.

У результаті, після цього налаштування, мережа зможе автоматично переключатись між головним і резервним пристроєм, при цьому користувачі навіть не помітять змін, бо все буде працювати як і раніше, через одну й ту ж адресу.

Наступним важливим кроком є налаштування автоматичного перемикання між головним і резервним маршрутизатором. Для цього потрібно відкрити вкладку "Tools/Netwatch". Саме тут налаштовується система, яка буде стежити за тим, чи працює головний маршрутизатор.

Ідея дуже проста: резервний маршрутизатор періодично перевірятиме, чи є зв'язок із головним. Це схоже на те, як людина час від часу телефонує другові, щоб переконатись, що з ним усе добре. Якщо резервний маршрутизатор не отримає відповіді, тобто, якщо головний маршрутизатор стане недоступним, тоді резервний "візьме на себе" всі обов'язки і почне самостійно обслуговувати користувачів.

Для цього резервний маршрутизатор увімкне роздачу DHCP та візьме на себе роль головного маршрутизатора. Але як тільки зв'язок із головним маршрутизатором знову з'явиться, резервний "віддасть повноваження", тобто, вимкне DHCP та перестане виступати у ролі головного маршрутизатор.

Таким чином, вся система буде працювати максимально надійно та без збоїв, навіть якщо в мережі щось трапиться. Користувачі цього майже не помітять, бо інтернет і локальні сервіси будуть доступні завжди.

Потрібно відкрити вкладку "Tools/Netwatch" на резервному маршрутизаторі. Далі натиснути у лівому верхньому куті кнопку "+", щоб відкрилось вікно для створення потрібної функції.

При створенні функції потрібно вказати ім’я, щоб можна було відрізняти один від іншого. Також потрібно вказати IP адресу головного маршрутизатора (потрібно вказувати адресу, яка призначена на потрібний нам VLAN). Після цього потрібно не забути вказати, що буде виконуватись запит icmp. Наступним кроком потрібно вказати період часу, через який буде працювати дана функція. У даному випадку час буде 5 секунд, бо це оптимальний час, щоб користувачі не помітили змін під час критичної ситуації. Також потрібно не забути написати скрипти, які будуть спрацьовувати у разі вимкнення головного маршрутизатора та у разі ввімкнення головного маршрутизатора. Це можна зробити у вкладках “Up” та “Down”. У вкладці “Up” потрібно написати скрипт, який буде вимикати DHCP на резервному маршрутизаторі, а у вкладці “Down” потрібно написати скрипт, який буде вмикати DHCP на резервному маршрутизаторі Створення перевірки роботи головного маршрутизатора зі всіма нюансами можна побачити на рисунку 3.14.

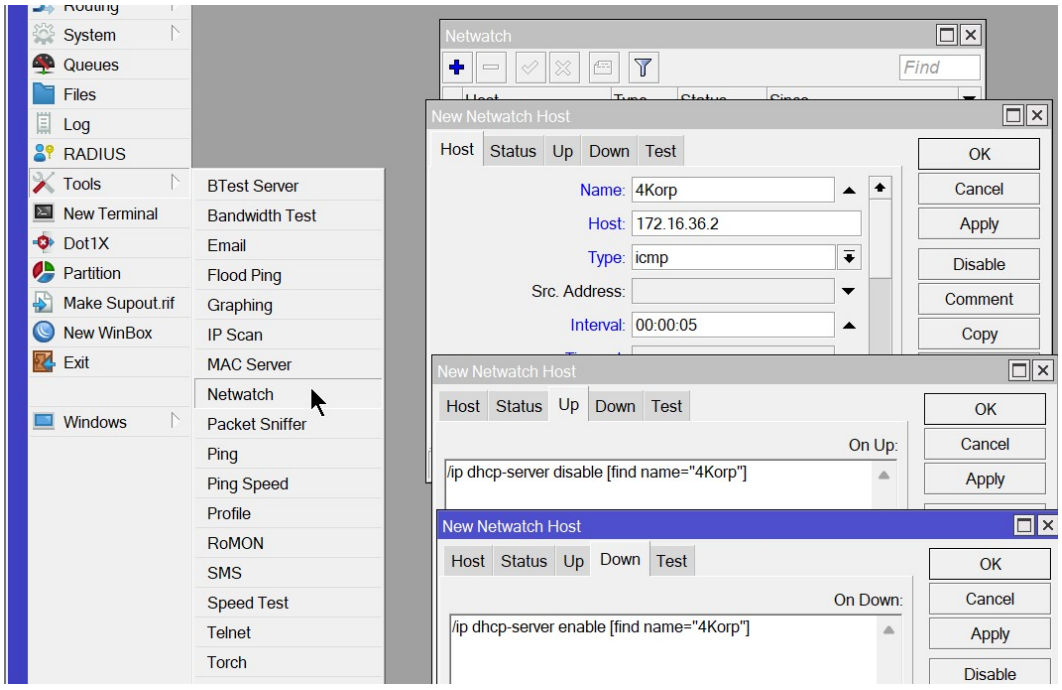


Рисунок 3.14 – Створення перевірки роботи головного маршрутизатора

Ця функція дуже потрібна для функціонування відмовостійкої університетської комп’ютерної мережі, бо саме завдяки їх резервний маршрутизатор зможе працювати як головний у разі настання надзвичайної ситуації, яка може зашкодити роботі мережі.

3.6 Перевірка виконаного завдання

Після завершення створення та налаштування комп’ютерної мережі дуже важливо перевірити, чи вона дійсно працює правильно. Адже навіть при правильному налаштуванні все одно можуть бути непомітні на перший погляд помилки. Щоб упевнитись у стабільності мережі, потрібно провести тестування в умовах, які імітують реальні критичні ситуації.

Спочатку потрібно підключитися до мережі як звичайний користувач. Тобто, під'єднатися до одного з VLAN. Уданому випадку до VLAN, що розташований у 4-му корпусі. Після підключення можна перейти до перевірки.

Для цього використовується команда “tracert” у командному рядку. Вона дозволяє побачити, яким шляхом проходить трафік через мережу від комп’ютера користувача до певного пункту (наприклад, іншого пристрою чи зовнішнього ресурсу в інтернеті). Таким чином, можна побачити, через які пристрої та вузли проходить трафік і переконатися, що все працює так, як заплановано.

Щоб впевнитися, що в обох частинах мережі все працює стабільно, і кожна частина правильно обробляє дані та підключення, потрібно двічі зробити перевірку для даного VLAN. Перший раз щоб перевірити, що все чудово працює на головному маршрутизаторі. Потім потрібно імітувати критичну ситуацію. Другий раз потрібно перевірити чи все чудово працює на резервному маршрутизаторі. Перевірку на головному маршрутизаторі можна побачити на рисунку 3.15.

```
C:\Users\admin>tracert google.com

Tracing route to google.com [172.217.16.46]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.16.36.1
  2     4 ms     4 ms     4 ms  31.128.80.1.ipv4.datagroup.ua [31.128.80.1]
```

Рисунок 3.15 – Перевірка доступу через головний маршрутизатор

Наступним кроком потрібно створити імітацію інциденту, який вимкне головний маршрутизатор. Це можна побачити на рисунку 3.16.

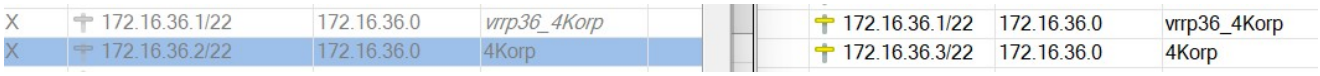


Рисунок 3.16 – Імітація вимкнення головного маршрутизатора

Фінальним етапом потрібно перевірити перевірити чи все чудово працює на резервному маршрутизаторі. Дану перевірку можна побачити на рисунку 3.17.

```
C:\Users\admin>tracert google.com

Tracing route to google.com [142.250.203.142]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.16.36.1
  2     1 ms    <1 ms    <1 ms  ge1-11.br01-lilu.ic.km.ua [78.152.161.61]
^C
```

Рисунок 3.17 – Перевірка доступу через резервний маршрутизатор

Для правдивої перевірки виконання завдання також потрібно перевірити, як буде проходити трафік через мережу, використовуючи інший VLAN. Для цього буде використано VLAN для 2-го корпусу. Потрібно повторити всі дії, які було проведено з VLAN 4-го корпусу. У даному випадку головним маршрутизатором повинен виступати маршрутизатор, який розсташований у бібліотеці. Саме через цей нюанс було вирішено використати VLAN 2-го корпусу для повної перевірки працездатності мережі. Перевірку на головному маршрутизаторі можна побачити на рисунку 3.18.

```
C:\Users\фівц>tracert google.com

Tracing route to google.com [142.250.203.142]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.16.24.1
  2    <1 ms    <1 ms    <1 ms  ge1-11.br01-lilu.ic.km.ua [78.152.161.61]
```

Рисунок 3.18 - Перевірка доступу через головний маршрутизатор

Наступним етапом потрібно імітувати настання інциденту, який буде направлений на головний маршрутизатор. Це можна побачити на рисунку 3.19

Рисунок 3.19 - Імітація вимкнення головного маршрутизатора

Останнім етапом потрібно ще раз провести аналіх трафіку, щоб впевнетись, що резервний маршрутизатор бере на себе роль головного та те, що все працює у тому вигляді, як і було задумано. Дану перевірку можна побачити на рисунку 3.20.

```
C:\Users\фівц>tracert google.com

Tracing route to google.com [142.250.203.142]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.16.24.1
  2     3 ms     3 ms     3 ms  31.128.80.1.ipv4.datagroup.ua [31.128.80.1]
```

Рисунок 3.20 - Перевірка доступу через резервний маршрутизатор

Інші VLAN налаштовані таким самим методом. Саме через це потреба показувати кожний VLAN, як така, не велика, бо все налаштовано подібним методом.

Наскільки видно на рисунках, які відображають послідовність перевірки працездатності мережі, можна побачити, що все працює належним чином. Це означає, що користувачі університетської комп’ютерної мережі не відчують сильних незручностей під час критичної ситуації, яка може статись у будь-який момент. Також це означає, що якщо виникне потреба замінити або перезагрузити один з головних маршрутизаторів, то резервний візьме на себе роль головного та користувачі мережі не відчують різниці. Також це забезпечує ефективний розподіл трафіку по двої маршрутизаторах та по двої провайдерах, що зменшить навантаження на маршрутизатори та дозволить їм працювати ефективніше та швидше. Отже, можна сказати, що було вибрано правильні методи, які було використано для створення безперебійної університетської комп’ютерної мережі. Саме завдяки правильному вибору методів та правильної реалізації було створено безперебійну університетську комп’ютерну мережу.

ВИСНОВКИ

У ході виконання роботи було спроєктовано та реалізовано відмовостійку комп'ютерну мережу для університетського середовища з використанням обладнання MikroTik та низки сучасних мережевих технологій. Основна мета була у забезпечені надійності, гнучкості та безперервного доступу до мережевих ресурсів у разі відмови окремих вузлів або каналів зв'язку, та була досягнута завдяки впровадженню наступних рішень:

- сегментація мережі за допомогою VLAN (Virtual LAN) підвищила рівень безпеки та ефективності передачі даних, дозволивши логічно розділити мережу на ізольовані підмережі, кожна з яких відповідає окремим структурним підрозділам університету;

- використання моста (Bridge) надало можливість об'єднати кілька фізичних інтерфейсів в один логічний, що дозволило оптимізувати трафік та спростити керування топологією мережі;

- протокол DHCP (Dynamic Host Configuration Protocol) забезпечив автоматичне призначення IP-адрес, що значно спростило адміністрування мережі та зменшило ризик помилок при ручному конфігуруванні;

- використання протоколу VRRP (Virtual Router Redundancy Protocol) дозволило реалізувати механізм автоматичного перемикання маршрутизаторів, забезпечуючи безперервність доступу до шлюзу у випадку виходу з ладу основного маршрутизатора.

У результаті було отримано надійну, масштабовану та відмовостійку мережу, здатну забезпечити стабільну роботу в умовах інтенсивного навантаження та потенційних збоїв. Запропоноване рішення є ефективним як з технічної, так і з економічної точки зору, що робить його доцільним для впровадження в реальній інфраструктурі університету.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Все про модель OSI за 7 хвилин. IT Education Center Blog. URL: https://itedu.center/ua/blog/articles/everything-about-the-osi-model-in-7-minutes/?srsltid=AfmBOoq0s5ZOzfOZzj4lbYbEYUhDQQUyeCSvofZqtV2aVnLwpI5FsulF (дата звернення: 20.02.2025).

2. Мережева модель OSI. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Мережева_модель_OSI (дата звернення: 20.02.2025).

3. Мережева модель OSI для чайників. KR. Laboratories. URL: https://kr-labs.com.ua/blog/model-osi/ (дата звернення: 21.02.2025).

4. TCP/IP. Вікіпедія. URL: https://uk.wikipedia.org/wiki/TCP/IP (дата звернення: 25.02.2025).

5. Протокол TCP/IP або як працює Інтернет (для початківців). QALight. URL: https://qalight.ua/baza-znaniy/protokol-tcp-ip-abo-yak-praczyuє-internet-dlya-pochatkivcziv/ (дата звернення: 25.02.2025).

6. TCP IP: історія розвитку протоколів і основні принципи роботи. FoxmindEd. URL: https://foxminded.ua/tcp-ip/ (дата звернення: 28.02.2025).

7. Основи та застосування протоколів TCP/IP, повний путівник. HackYourMom. URL: https://hackyourmom.com/kibervijna/osnovy-ta-zastosuvannya-protokoliv-tcp-ip-povnyj-putivnyk/ (дата звернення: 28.02.2025).

8. Протоколи TCP та UDP - пояснення простою мовою. DevZone. URL: https://devzone.org.ua/post/protokoly-tcp-ta-udp-poiasnennia-prostoiu-movoiu (дата звернення: 1.03.2025).

9. UDP та TCP VPN. Що це таке і як вибрати правильний варіант. VPN Unlimited - Fast & Secure VPN service. URL: https://www.vpnunlimited.com/ua/help/more-about-vpn/udp-vs-tcp?srsltid=AfmBOoptJsi64pSvfkXSZygCoQ5mTPUAxfpryYM1zEDii4ZiSFyKANuU (дата звернення: 1.03.2025).

10. Список номерів портів TCP та UDP. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Список_номерів_портів_TCP_та_UDP (дата звернення: 5.03.2025).

11. 11.TCP/IP проти моделі OSI – різниця між ними. Guru99. URL: https://www.guru99.com/uk/difference-tcp-ip-vs-osi-model.html?gpp&gpp_sid (дата звернення: 5.03.2025).

12. IP-адреса. Вікіпедія. URL: https://uk.wikipedia.org/wiki/IP-адреса (дата звернення: 5.03.2025).

13. Що таке IP-адреса і для чого вона потрібна. Trium. URL: https://trium.com.ua/43-shcho-take-ip-adresa-i-dlia-choho-vona-potribna (дата звернення: 5.03.2025).

14. Що таке IP-адреса. Mozilla. URL: https://www.mozilla.org/uk/products/vpn/more/what-is-an-ip-address/ (дата звернення: 9.03.2025).

15. DHCP. Вікіпедія. URL: https://uk.wikipedia.org/wiki/DHCP (дата звернення: 9.03.2025).

16. Що таке DHCP? Простий посібник із розуміння призначення IP-адрес. Fiberroad Technology. URL: https://fiberroad.com/uk/resources/glossary/what-is-dhcp/ (дата звернення: 9.03.2025).

17. Що значить DHCP. Технології мереж. URL: https://nettech.ua/news/dhcp-dynamic-host-configuration-protocol (дата звернення: 10.03.2025).

18. Що таке протокол Dynamic Host Configuration Protocol (DHCP). RubyDevelopers URL: https://rubydevelopers.org/t/dynamic-host-configuration-protocol-dhcp/188 (дата звернення: 10.03.2025).

19. VLAN. Вікіпедія. URL: https://uk.wikipedia.org/wiki/VLAN (дата звернення: 10.03.2025).

20. Пояснення VLAN: що таке VLAN, як це працює. Fiberroad Technology. URL: https://fiberroad.com/uk/resources/glossary/vlan-explained-what-is-vlan-how-does-it-work/ (дата звернення: 12.03.2025).

21. Що таке VLAN: логіка, технологія і налаштування. Реалізація VLAN в пристроях CISCO. EServer. URL: https://e-server.com.ua/uk/poradi/shho-take-vlan-logika-tehnologija-i-nalashtuvannja-realizacija-vlan-v-pristrojah-cisco?srsltid=AfmBOop0ir1eI13z4iXEWEYTAPkvSFEsWkcRBWeGOf2vRjBZjqWiR50H (дата звернення: 12.03.2025).

22. [Бездротовий маршрутизатор] Що таке VLAN і як її налаштувати? ASUS. URL: https://www.asus.com/ua-ua/support/faq/1049415/ (дата звернення: 14.03.2025).

23. Мережевий екран. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Мережевий_екран (дата звернення: 14.03.2025).

24. Маршрутизатор. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Маршрутизатор (дата звернення: 14.03.2025).

25. Що таке маршрутизатор. Network Tools. URL: https://ntools.com.ua/uk/information/faq/chto-takoe-marshrutizator-router (дата звернення: 14.03.2025).

26. Маршрутизатори: основні функції та принципи роботи. PRAVDA.IF.UA. URL: https://pravda.if.ua/marshrutyzatory-osnovni-funkcziyi-ta-prynczypy-roboty/ (дата звернення: 15.03.2025).

27. Маршрутизатори локальної мережі. InfoTel. URL: https://infotel.ua/aktivne-merezheve-obladnannya/marshrutizatori-lokalnoi-merezhi (дата звернення: 15.03.2025).

28. Мережевий комутатор. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Мережевий_комутатор (дата звернення: 15.03.2025).

29. Що таке світ (свіч, switch) або мережевий комутатор – це пристрій, який дозволяє з'єднувати ділянки комп'ютерної мережі Технології мереж. URL: https://nettech.ua/news/svitch-switch-setevoy-kommutator (дата звернення: 16.03.2025).

30. Мережевий комутатор (світч): що це таке та як обрати. GAZIK. URL: https://gazik.ua/blog/porady-pokuptsyam/merezhevyy-komutator-svitch-shcho-tse-take-ta-yak-obraty/?srsltid=AfmBOor3pDPMOPK_92bn_VC5IClIKhJLFHK32b3hKEMf3-TsuBfzlwnl (дата звернення: 16.03.2025).

31. Комутатор, що це таке. Network Tools. URL: https://ntools.com.ua/uk/information/faq/chto-takoe-kommutator-switch (дата звернення: 16.03.2025).

32. Що таке комутатор: види, функції та принцип роботи. ITBIZ. URL: https://itbiz.ua/statti-ta-obzori/sho-take-komutator-vidi-funkciyi-ta-princip-roboti/ (дата

звернення: 17.03.2025).

33. Що таке інтернет комутатор. EServer. URL: https://e-server.com.ua/uk/poradi/shcho-take-internet-komutator?srsltid=AfmBOor88JFz5M7qPUxTi2P7NJEJd3rU0EuNWP7wyuNcQb6FtfjdZmit (дата звернення: 17.03.2025).

34. Різниця між комутатором і маршрутизатором. ITBIZ. URL: https://itbiz.ua/statti-ta-obzori/riznicya-mizh-komutatorom-i-marshrutizatorom/ (дата звернення: 17.03.2025).

35. Чим відрізняється комутатор від маршрутизатора. Stack Systems. URL: https://stack-systems.com.ua/blogs/chym-vidrizniajetsia-komutator-vid-marshrutyzatora?srsltid=AfmBOorz1w1LsFaCzOpn9XBJA5JX8r5vxoUJZ52mx__VpkyJm6fvUtBX (дата звернення: 17.03.2025).

36. Розуміння відмінностей між комутаторами рівня 3 і маршрутизаторами. Fiberroad Technology. URL: https://fiberroad.com/uk/resources/tech-notes/understanding-the-differences-between-layer-3-switches-and-routers/ (дата звернення: 17.03.2025).

37. Маршрутизатор проти комутатора – різниця між ними. Guru99. URL: https://www.guru99.com/uk/router-vs-switch-difference.html (дата звернення: 19.03.2025).

38. Комутатор та маршрутизатор: у чому різниця і що вибрати. Goodok.ua. URL: https://goodok.com.ua/ua/v-cem-raznica-mezdu-kommutatorom-i-marsrutizatorom?srsltid=AfmBOoqfs3t035SI8i2hN-kGHwry21kXCD7NZrdqGUo0Gq9YTWh4jD2T (дата звернення: 19.03.2025).

39. MikroTik. Вікіпедія. URL: https://uk.wikipedia.org/wiki/MikroTik (дата звернення: 19.03.2025).

40. Налаштування Mikrotik. Nixj. URL: https://nixj.ua/services/nalashtuvannya-mikrotik (дата звернення: 21.03.2025).

41. RouterOS. Mstream. URL: https://mstream.com.ua/uk/routerboard/routeros-mikrotik/ (дата звернення: 21.03.2025).

42. Що таке MikroTik RouterBOARD. LanTorg. URL: https://lantorg.com/article/chto-takoe-mikrotik-

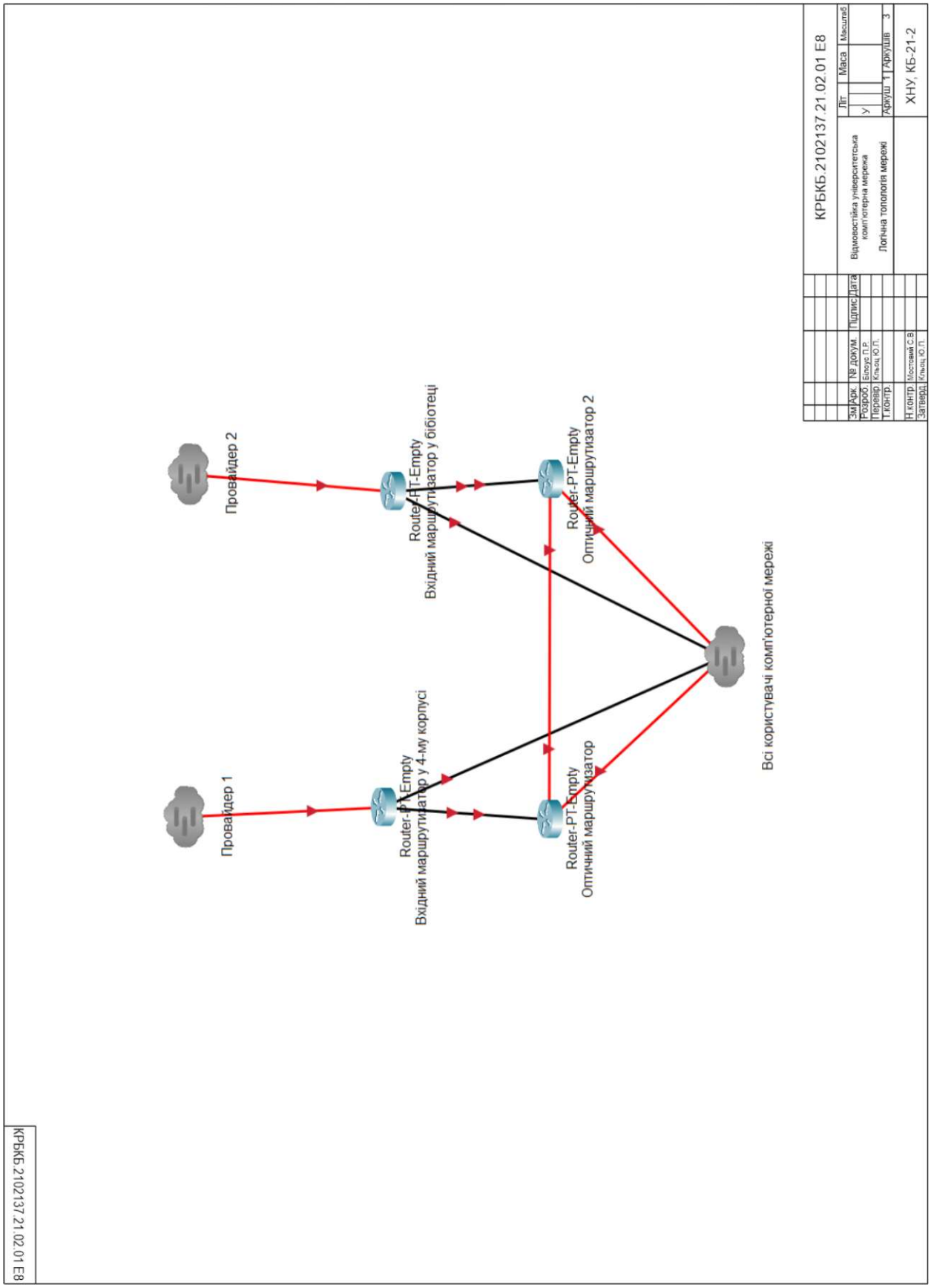
routerboard/?srsltid=AfmBOorhO1YGt58TUVgkdEGWm8VB30Y3eRcglWb3nexMsc-9gepxp5nH (дата звернення: 21.03.2025).

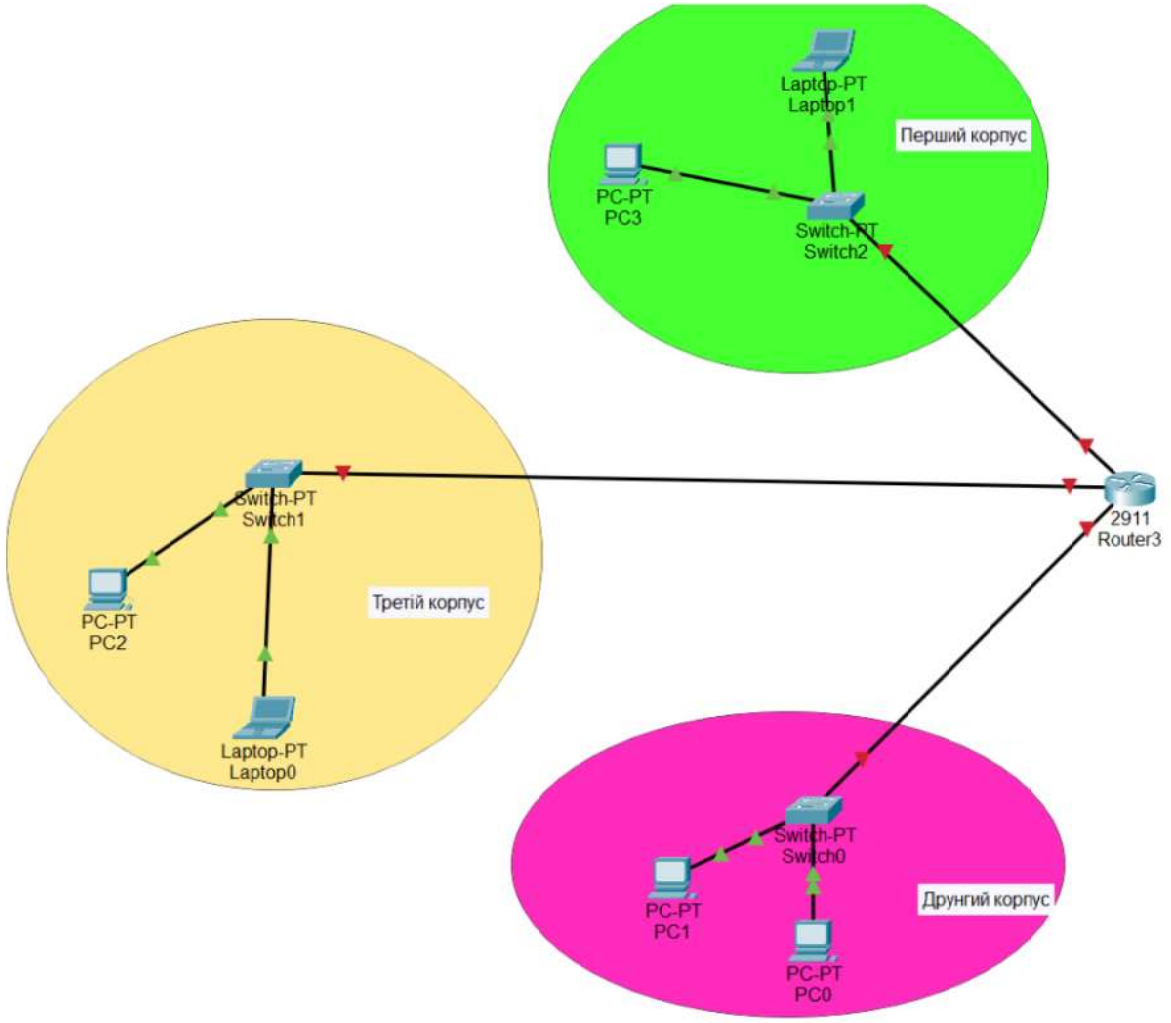
43. SwOS. MikroTik Routers and Wireless - Support. URL: https://help.mikrotik.com/docs/spaces/SWOS/pages/328415/SwOS (дата звернення: 21.03.2025).

ДОДАТОК А

(обов’язковий)

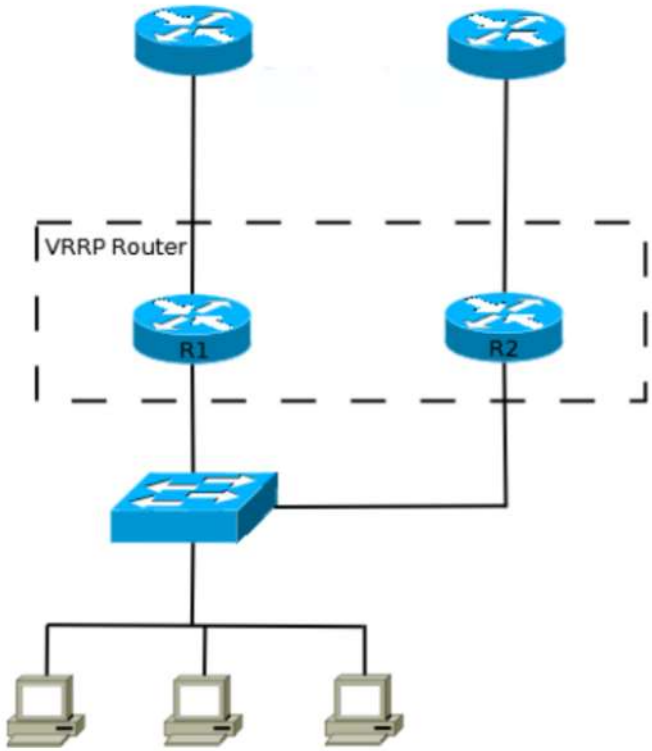
Копія графічної частини

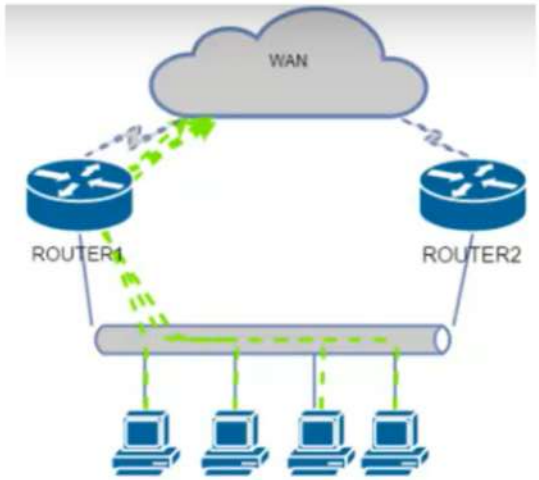


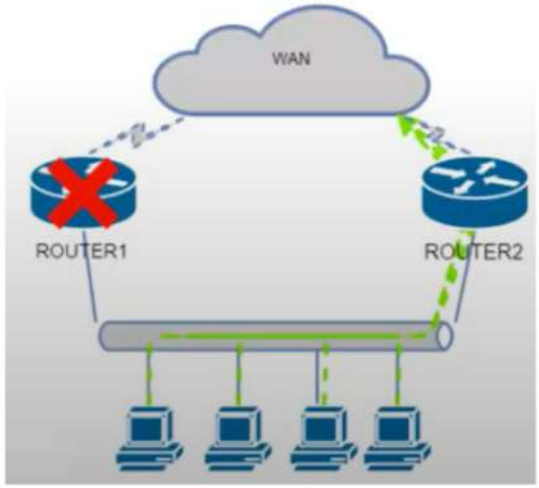


						КРБКБ.2102137.21.02.01 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Білоус П.Р.			Відмовостійка університетська комп'ютерна мережа	Літ.	Маса / Масштаб
Перевір.		Кльоц Ю.П.				У	
Т.контр.					Приклад розміщення VLAN	Аркуш 2	Аркушів 3
Н.контр.		Мостовий С.В.				ХНУ, КБ-21-2	
Затверд.		Кльоц Ю.П.					

КРБКБ.2102137.21.02.01 Е8







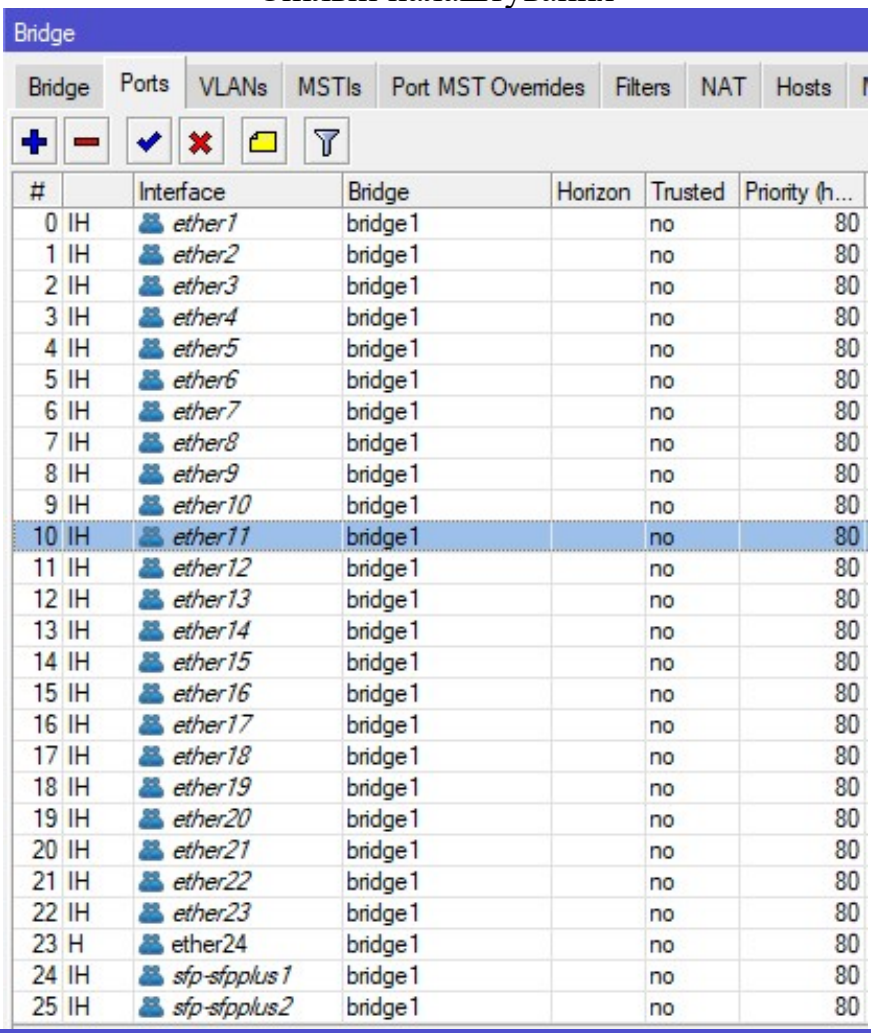
					КРБКБ.2102137.21.02.01 Е8		
Зм.	Арк.	№ докум.	Підпис	Дата	Відмовостійка університетська комп'ютерна мережа	Літ	Маса / Масштаб
Розроб.		Білоус П.Р.				У	
Перевір.		Кльоц Ю.П.			Приклад роботи VRRP	Аркуш 3	Аркушів 3
Т.контр.							
Н.контр.		Мостовий С.В.				ХНУ, КБ-21-2	
Затверд.		Кльоц Ю.П.					

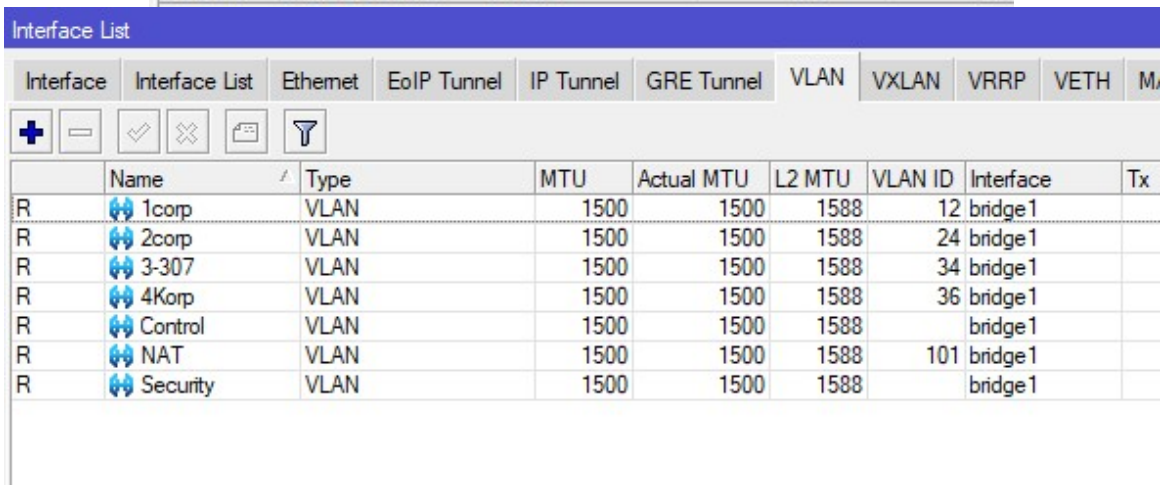
ДОДАТОК Б

(обов’язковий)

Налаштування маршрутизаторів

Спільні налаштування





Bridge

Bridge | Ports | VLANs | MSTIs | Port MST Overrides | Filters | NAT | Hosts | M

MVRP Attributes

	Bridge	VLAN IDs	Current Tagged
	;;; added by pvid		
D	bridge1	1	
	bridge1		bridge1
	bridge1	12	bridge1
	bridge1	24	bridge1
	bridge1	34	bridge1
	bridge1	36	bridge1
	bridge1		bridge1
	bridge1	101	bridge1

DHCP Server

DHCP | Networks | Leases | Options | Option Sets | Option Matcher | Alerts

DHCP Config | DHCP Setup

	Name	Interface	Address Pool	Relay	Lease Time	Add AR...
	dhcp_1corp	1corp	pool_1corp		00:30:00	no
	dhcp_2corp	2corp	pool_2corp		00:30:00	no
	dhcp_3-307	3-307	pool_3-307		00:30:00	no
X	dhcp_4Korp	4Korp	pool_4Korp		00:30:00	no
	dhcp_Control	Control	pool_Control		00:30:00	no
X	dhcp_NAT	NAT	pool_NAT		00:30:00	no
	dhcp_Security	Security	pool_Security		00:30:00	no

DHCP Server

DHCP | Networks | Leases | Options | Option Sets | Option Matcher | Alert

Address	Gateway	DNS Servers	Domain
172.16 .0/24	172.16 1	172.16 1	
172.16.12.0/22	172.16.12.1	172.16.12.1	
172.16.24.0/22	172.16.24.1	172.16.24.1	
172.16.34.0/23	172.16.34.1	172.16.34.1	
172.16.36.0/22	172.16.36.1	172.16.36.1	
172.16. .0/24	172.16 1	172.16. 1	
172.20.0.0/16	172.20.0.1	172.20.0.1	

Маршрутизатор у бібліотеці

Interface List

Interface | Interface List | Ethernet | EoIP Tunnel | IP Tunnel | GRE Tunnel | VLAN | VXLAN | VRRP | VETH | MACsec | MACVLAN | Bonding

	Name	Type	MTU	Actual MTU	L2 MTU	Interface	VRID	Priority	Group Authority
RM	vrrp12_1corp	VRRP	1500	1500	1588	1corp	12	100	none
RM	vrrp24_2corp	VRRP	1500	1500	1588	2corp	24	100	none
RM	vrrp34_3-307	VRRP	1500	1500	1588	3-307	34	100	none
RM	vrrp36_4Korp	VRRP	1500	1500	1588	4Korp	36	100	none
RM	vrrp101_NAT	VRRP	1500	1500	1588	NAT	101	90	none
RM	vrrp_Control	VRRP	1500	1500	1588	Security		100	none
RM	vrrp_Security	VRRP	1500	1500	1588	Security		100	none

Address List

Find

Address	Network	Interface
172.16. 1/24	172.16 0	vrrp_Control
172.16 2/24	172.16 0	Control
172.16.12.1/22	172.16.12.0	vrrp12_1corp
172.16.12.2/22	172.16.12.0	1corp
172.16.24.1/22	172.16.24.0	vrrp24_2corp
172.16.24.2/22	172.16.24.0	2corp
172.16.34.1/23	172.16.34.0	vrrp34_3-307
172.16.34.2/23	172.16.34.0	3-307
172.16.36.1/22	172.16.36.0	vrrp36_4Korp
172.16.36.3/22	172.16.36.0	4Korp
172.16. 1/24	172.16 0	vrrp_Security
172.16. 2/24	172.16. 0	Security
172.20.0.1/16	172.20.0.0	vrrp101_NAT
172.20.0.3/16	172.20.0.0	NAT

14 items

Netwatch

Name	Host	Type	Status	Since
4Korp	172.16.36.2	icmp	down	Mar/26/2025 12:57:21
NAT	172.20.0.2	icmp	down	Mar/26/2025 12:57:14

Маршрутизатор у 4-му корпусі

Interface List

Interface | Interface List | Ethernet | EoIP Tunnel | IP Tunnel | GRE Tunnel | VLAN | VXLAN | VRRP | VETH | MACsec | MACVLAN | Bondir

	Name	Type	MTU	Actual MTU	L2 MTU	Interface	VRID	Priority	Group Authority
RM	vrrp12_1corp	VRRP	1500	1500	1588	1corp	12	90	none
RM	vrrp24_2corp	VRRP	1500	1500	1588	2corp	24	90	none
RM	vrrp34_3-307	VRRP	1500	1500	1588	3-307	34	90	none
RM	vrrp36_4Korp	VRRP	1500	1500	1588	4Korp	36	120	none
RM	vrrp101_NAT	VRRP	1500	1500	1588	NAT	101	100	none
RM	vrrp_Control	VRRP	1500	1500	1588	Security		90	none
RM	vrrp_Security	VRRP	1500	1500	1588	Security		90	none

Address List

Find

Address	Network	Interface
172.16 1/24	172.16.9.0	vrrp_Control
172.16 3/24	172.16.9.0	Control
172.16.12.1/22	172.16.12.0	vrrp12_1corp
172.16.12.3/22	172.16.12.0	1corp
172.16.24.1/22	172.16.24.0	vrrp24_2corp
172.16.24.3/22	172.16.24.0	2corp
172.16.34.1/23	172.16.34.0	vrrp34_3-307
172.16.34.3/23	172.16.34.0	3-307
172.16.36.1/22	172.16.36.0	vrrp36_4Korp
172.16.36.2/22	172.16.36.0	4Korp
172.16 1/24	172.16.100.0	vrrp_Security
172.16 3/24	172.16.100.0	Security
172.20.0.1/16	172.20.0.0	vrrp101_NAT
172.20.0.2/16	172.20.0.0	NAT

14 items (1 selected)

Netwatch

Find

Name	Host	Type	Status	Since
1corp	172.16.12.2	icmp	down	Mar/26/2025 13:04:06
2corp	172.16.24.2	icmp	down	Mar/26/2025 13:04:08
3-307	172.16.34.2	icmp	down	Mar/26/2025 13:04:17
Control	172.16 2	icmp	down	Mar/26/2025 13:03:59
Security	172.16 2	icmp	down	Mar/26/2025 13:04:30

5 items

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Білоуса Павла Романовича
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-21-2

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (StrikePlagiarism та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

28.05.2025
дата

підпис

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 1.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 14%**

	Document		Sum coincidence on the DB	
ID: 242689 Title: Відмовостійка університетська комп'ютерна мережа Added in a DB: 2025-05-30 Authors: Білоус Павло Романович Heads: Кльоц Ю.П, Consultants: Opponents:	Symbols	Lexemes	Symbols	Lexemes
	82498	701	804 (1%)	9 (1%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Білоус Павло Романович

Співавтор:

Назва: Відмовостійка університетська комп'ютерна мережа

Науковий керівник:

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:2.8%

Коефіцієнт подібності 2:0.3%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-05-30 23:42:51.0

Після аналізу Звіту подібності констатую наступне:

☑ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

02.06.2025р.

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Метод оцінки впливу маршрутизації на надійність корпоративної мережі

Автор: Білоус Павло Романович
Спеціальність: 125 – Кібербезпека
Освітня програма: освітньо-професійна
Науковий керівник: Кльоц Юрій Павлович, канд. техн. наук, доцент
Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 97,2%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100 %, визнається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ Ю.П. Кльоц

Гарант ОП _____ В.М. Чешун

Завідувач кафедри кібербезпеки _____ Ю.П. Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Білоус Павло Романович

Тема Відмовостійка університетська комп'ютерна мережа

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 3; кількість сторінок записки 70.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі була розроблена відмовостійка університетська комп'ютерна мережа. Система базується на створенні та налаштуванні віртуального маршрутизатора. Складається з двох компонентів: за допомогою віртуального маршрутизатора визначає та перенаправляє трафік між двома головними маршрутизаторами, а також ввімкнення та вимкнення DHCP у разі інциденту на головному маршрутизаторі. Для розробки системи було проведено детальний аналіз протоколів мереж та можливі варіанти реалізації завдання.

2. Висновок про відповідність кваліфікаційної роботи завданню У кваліфікаційній роботі було виконано поставлене завдання як у теоретичній, так і в практичній частині.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі роботи описано класифікацію мереж та функції, за допомогою яких можна реалізувати дане завдання. Другий розділ присвячено розробці методів, які було використано при розробці відмовостійкої університетської комп'ютерної мережі. В третьому розділі проведено налаштування пристроїв, які потрібно для нормальної та безперебійної роботи мережі, а також була зроблена перевірка працездатності даної системи.

4. Позитивні сторони роботи Кваліфікаційна робота має практичну цінність. Вона полягає у відмовостійкості мережі під час інцидентів різного роду.

5. Негативні сторони роботи В разі компрометації облікового запису адміністратора чи недотримання адміністратором політики безпеки у вигляді стандартних логіна та пароля, можливі компрометація даних, а також можливі проблеми у вигляді поганого функціонування мережі.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. В цілому, графічне оформлення є якісним, а пояснювальна записка відповідає нормам оформлення.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи. Графічний матеріал допомагає наочно продемонструвати доцільність та ефективність прийнятих рішень для досягнення мети.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінки «відмінно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Підченко Сергій Констянтинович, завідувач кафедри телекомунікацій, медійних та інтелектуальних технологій, доктор технічних наук, професор ХНУ.

« 2 » 06 2025 _____ (підпис)