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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра

на тему: «Проєкт захищеної комп'ютерної мережі організації, побудованої на базі обладнання Cisco»

Виконала студентка 4-го курсу групи КБ-20-1
спеціальності 125 «Кібербезпека»
_____ Маргарита ГОЛИШЕВСЬКА
Керівник старший викладач кафедри КІ та КБ
_____ Єлизавета ТРОКОЗ
Рецензент старший викладач кафедри КІ та КБ
_____ Олександра ПОКОТИЛО

Житомир – 2024

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

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
Андрій Єфіменко
5 березня 2024 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу бакалавра

Студентка: Голишевська Маргарита Юріївна
Тема роботи: «Проєкт захищеної комп'ютерної мережі організації, побудованої на базі обладнання Cisco»
затверджена Наказом університету від 5 березня 2024 р. № 98
Термін здачі студентом закінченої роботи 9 червня 2024 р.

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

– комп'ютерна мережа організації;
– методи захисту від загроз та атак;
– застосування різних технологій та протоколів для реалізації захисту мережі організації;

Обладнання та програмне забезпечення:

1. Емулятор GNS3
2. Образ маршрутизатора Cisco 7200 Series VRX
3. Образ комутатора Cisco Catalyst WS-C2960-24TT-L
4. ОС Windows 10 та Linux Ubuntu 22

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Трокоз Є. М.	11.03.2024	11.03.2024
2	Трокоз Є. М.	03.04.2024	03.04.2024
3	Трокоз Є. М.	16.05.2024	16.05.2024

Студент _____ Голишевська М. Ю.
Керівник _____ Трокоз Є. М.

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	17.03.2024	Виконано
2	Аналіз літературних джерел	24.03.2024	Виконано
3	Розробка структурної моделі	02.04.2024	Виконано
4	Розрахунок параметрів адресації	04.04.2024	Виконано
5	Вибір технологій для реалізації	06.04.2024	Виконано
6	Проєктування КМ	21.04.2024	Виконано
7	Підготовка компонентів для мережі	04.05.2024	Виконано
8	Налаштування мережі	13.05.2024	Виконано
9	Налагодження захисту мережі	18.05.2024	Виконано
10	Тестування роботи КМ	26.05.2024	Виконано
11	Оформлення пояснювальної записки	29.05.2024	Виконано
12	Оформлення презентації	09.06.2024	Виконано
13	Захист		Виконано

Студент _____ Голишевська М. Ю.

Керівник _____ Трокоз Є. М.

АНОТАЦІЯ

Кваліфікаційна робота на тему «Проєкт захищеної комп'ютерної мережі організації, побудованої на базі обладнання Cisco» складається з переліку умовних скорочень, вступу, трьох розділів, висновків, списку використаної літератури та додатків.

Пояснювальна записка містить 72 рисунки та займає 73 сторінки. Список використаних джерел містить 16 найменувань і розташований на 2 сторінках.

Метою даної роботи є розробка проєкту захищеної комп'ютерної мережі організації на базі обладнання Cisco.

В роботі було описано загрози мережі і обрано відповідні заходи для забезпечення її захисту. Також описано мережеве обладнання, за допомогою якого створено та налаштовано проєкт. Проведено тестування роботи мережі та сформовано висновки по проведеній роботі.

У додатку представлена схема спроєктованої мережі, таблиця адресації та конфігурація пристроїв.

Ключові слова: КОМП'ЮТЕРНА МЕРЕЖА, CISCO, ЗАХИСТ, БЕЗПЕКА, VLAN, АВТЕНТИФІКАЦІЯ, ACL, VPN.

					ККІК.КР.Б – 125 – 3 – ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Голишевська М.Ю.		17.06	Проєкт захищеної комп'ютерної мережі організації, побудованої на базі обладнання Cisco.	Літ.	Арк. 4 / Аркушів 87
Керівник		Трокоз С.М.		17.06			
Реценз.		Покотило О. А.		17.06		ФІКТ, Гр. КБ-20-1	
Н. контр.		Колощук М. С.		17.06			
Затверд.		Сфіменко А.А		17.06			

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра

на тему: «Проєкт захищеної комп'ютерної мережі організації, побудованої на базі обладнання Cisco»

Виконала студентка 4-го курсу групи КБ-20-1
спеціальності 125 «Кібербезпека»
_____ Маргарита ГОЛИШЕВСЬКА
Керівник старший викладач кафедри КІ та КБ
_____ Єлизавета ТРОКОЗ
Рецензент старший викладач кафедри КІ та КБ
_____ Олександра ПОКОТИЛО

Житомир – 2024

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

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
Андрій Єфіменко
5 березня 2024 р.

ЗАВДАННЯ
на випускну кваліфікаційну роботу бакалавра

Студентка: Голишевська Маргарита Юріївна
Тема роботи: «Проєкт захищеної комп'ютерної мережі організації, побудованої на базі обладнання Cisco»
затверджена Наказом університету від 5 березня 2024 р. № 98
Термін здачі студентом закінченої роботи 9 червня 2024 р.

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

– комп'ютерна мережа організації;
– методи захисту від загроз та атак;
– застосування різних технологій та протоколів для реалізації захисту мережі організації;

Обладнання та програмне забезпечення:

1. Емулятор GNS3
2. Образ маршрутизатора Cisco 7200 Series VRX
3. Образ комутатора Cisco Catalyst WS-C2960-24TT-L
4. ОС Windows 10 та Linux Ubuntu 22

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Трокоз Є. М.	11.03.2024	11.03.2024
2	Трокоз Є. М.	03.04.2024	03.04.2024
3	Трокоз Є. М.	16.05.2024	16.05.2024

Студент _____ Голишевська М. Ю.
Керівник _____ Трокоз Є. М.

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	17.03.2024	Виконано
2	Аналіз літературних джерел	24.03.2024	Виконано
3	Розробка структурної моделі	02.04.2024	Виконано
4	Розрахунок параметрів адресації	04.04.2024	Виконано
5	Вибір технологій для реалізації	06.04.2024	Виконано
6	Проєктування КМ	21.04.2024	Виконано
7	Підготовка компонентів для мережі	04.05.2024	Виконано
8	Налаштування мережі	13.05.2024	Виконано
9	Налагодження захисту мережі	18.05.2024	Виконано
10	Тестування роботи КМ	26.05.2024	Виконано
11	Оформлення пояснювальної записки	29.05.2024	Виконано
12	Оформлення презентації	09.06.2024	Виконано
13	Захист		Виконано

Студент _____ Голишевська М. Ю.

Керівник _____ Трокоз Є. М.

АНОТАЦІЯ

Кваліфікаційна робота на тему «Проєкт захищеної комп'ютерної мережі організації, побудованої на базі обладнання Cisco» складається з переліку умовних скорочень, вступу, трьох розділів, висновків, списку використаної літератури та додатків.

Пояснювальна записка містить 72 рисунки та займає 73 сторінки. Список використаних джерел містить 16 найменувань і розташований на 2 сторінках.

Метою даної роботи є розробка проєкту захищеної комп'ютерної мережі організації на базі обладнання Cisco.

В роботі було описано загрози мережі і обрано відповідні заходи для забезпечення її захисту. Також описано мережеве обладнання, за допомогою якого створено та налаштовано проєкт. Проведено тестування роботи мережі та сформовано висновки по проведеній роботі.

У додатку представлена схема спроєктованої мережі, таблиця адресації та конфігурація пристроїв.

Ключові слова: КОМП'ЮТЕРНА МЕРЕЖА, CISCO, ЗАХИСТ, БЕЗПЕКА, VLAN, АВТЕНТИФІКАЦІЯ, ACL, VPN.

					ККІК.КР.Б – 125 – 3 – ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Голишевська М.Ю.		17.06	Проєкт захищеної комп'ютерної мережі організації, побудованої на базі обладнання Cisco.	Літ.	Арк. 4 / Аркушів 87
Керівник		Трокоз С.М.		17.06			
Реценз.		Покотило О. А.		17.06		ФІКТ, Гр. КБ-20-1	
Н. контр.		Колощук М. С.		17.06			
Затверд.		Сфіменко А.А		17.06			

ANNOTATION

The qualification work “Project of a secure computer network of an organization based on Cisco devices” consists of a list of abbreviations, introduction, three chapters, conclusions, a list of used sources and attachments.

The explanatory note contains 72 illustrations and takes up 73 pages. The list of used sources consists of 16 titles and is located on 2 pages.

The purpose of this work is to create a project of a secure computer network of an organization based on Cisco equipment.

The document describes the threats to the network and selects appropriate measures to ensure its protection. The network equipment used to create and configure the project is also described. The network has been tested and conclusions about its functioning have been summarized.

The attachment contains a scheme of the designed network, addressing table, and device configuration.

Keywords: COMPUTER NETWORK, CISCO, PROTECTION, SECURITY, VLAN, AUTHENTICATION, ACL, VPN.

ЗМІСТ

ВСТУП 8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ (ПРИНЦИПИ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ) ТЕХНОЛОГІЙ ТА ПРОТОКОЛІВ ДЛЯ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ 9
1.1 Огляд загроз та порівняння сучасних методів захисту від них 9
1.2 Вибір оптимальних мережевих протоколів та сервісів для безпеки мережі організації 16
1.3 Методи автентифікації, авторизації та обліку на основі моделі AAA та протоколу TACACS+ 22
1.4 Принципи фільтрації трафіку з використанням списків контролю доступу 24
РОЗДІЛ 2 ПРОЄКТУВАННЯ ТА РОЗРОБКА ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ НА БАЗІ ОБЛАДНАННЯ CISCO 27
2.1 Вибір обладнання та ОС для організації роботи мережі 27
2.2 Проєктування топології мережі на базі обладнання Cisco 31
2.3 Розробка проєкту захищеної комп'ютерної мережі організації 33
2.4 Розробка схеми адресації мережі 37
РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ СПРОЄКТОВАНОЇ КМ ОРГАНІЗАЦІЇ НА БАЗІ ОБЛАДНАННЯ CISCO 39
3.1 Підготовка до створення захищеної комп'ютерної мережі 39
3.2 Налагодження спроєктованої мережі та її захисту 43
3.3 Тестування роботи побудованої мережі організації на базі обладнання Cisco 55
ВИСНОВКИ 70
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 71
ДОДАТКИ 73

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КМ – комп’ютерна мережа

ОС – операційна система

ПК – персональний комп’ютер

IP – Internet Protocol

VLAN – Virtual Local Area Network

HSRP – Hot Standby Router Protocol

AAA – Authentication, Authorization and Accounting

ACL – Access Control List

VPN – Virtual Private Network

TACACS+ – Terminal Access Controller Access-Control System Plus

SSH – Secure Shell

SYSLOG – System Log

OSPF – Open Shortest Path First

ВСТУП

Актуальність теми. У наш час цифрові технології стали невід'ємною частиною практично будь-якого бізнесу, безпека комп'ютерних мереж стала пріоритетним завданням для організацій. Швидкість і обсяг передачі даних, зростаючі загрози кібербезпеки і необхідність захисту конфіденційної інформації вимагають вживання відповідних заходів. У цьому контексті проєкт зі створення захищеної комп'ютерної мережі на базі обладнання Cisco – важлива і доцільна ініціатива, покликана забезпечити надійний захист інформації та стійкість мережевої інфраструктури до сучасних кіберзагроз.

Метою кваліфікаційної роботи є розробка захищеної комп'ютерної мережі організації на базі обладнання Cisco.

Визначена мета обумовлює наступні завдання:

- проаналізувати теоретичні аспекти які є підґрунтям для створення захисту комп’ютерних мереж;
- розробити проєкт надійно захищеної комп’ютерної мережі організації;
- налагодити та протестувати роботу готової мережі.

Об’єктом дослідження є процес розробки комп'ютерної мережі організації з використанням обладнання Cisco.

Предметом дослідження є технології та протоколи, які забезпечують захист комп'ютерної мережі організації, побудованої на базі обладнання Cisco.

У процесі виконання кваліфікаційної роботи було розроблено проєкт захищеної комп'ютерної мережі організації, що включає аналіз сучасних загроз, проєктування мережевої інфраструктури та впровадження засобів захисту з використанням обладнання Cisco.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ (ПРИНЦИПИ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ) ТЕХНОЛОГІЙ ТА ПРОТОКОЛІВ ДЛЯ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Огляд загроз та порівняння сучасних методів захисту від них

У цифровому середовищі, що постійно змінюється та розвивається, важливість захисту мережевої інфраструктури стає вирішальною для забезпечення конфіденційності, цілісності та доступності даних. Сучасні загрози стають дедалі складнішими та різноманітнішими, що вимагає постійного вдосконалення методів захисту. Щоб забезпечити ефективний захист, важливо знати про загрози, які можуть завдати шкоди мережі [1], а також про відповідні атаки, які використовують ці небезпеки. Нижче наведено таблицю з описом найпоширеніших типів атак:

Таблиця 1.1 – Типи атак та їх вплив на мережу

Тип атаки	Опис	Загрози для мережі
DoS/DDoS	Атаки на відмову в обслуговуванні (DoS) та розподілену відмову в обслуговуванні (DDoS) спрямовані на те, щоб зробити мережу або послугу недоступною шляхом затоплення її потоком трафіку. DDoS-атаки запускаються з декількох скомпрометованих систем.	Перевантаження мережевих ресурсів, відмова в обслуговуванні користувачів, зниження продуктивності.
Фішинг	Фішингові атаки полягають у надсиланні шахрайської інформації, яка виглядає як така, що надійшла з надійного джерела, зазвичай через електронну пошту. Метою є викрадення конфіденційних даних, таких як облікові дані для входу в систему або фінансова інформація.	Крадіжка облікових даних, фінансових даних та доступу до конфіденційної інформації.
Шкідливе ПЗ	Шкідливе програмне забезпечення включає віруси, хробаки, трояни, програми-вимагачі та шпигунські програми. Це шкідливе програмне забезпечення може порушити роботу, викрасти інформацію або зашифрувати дані з метою отримання викупу.	Пошкодження або знищення даних, крадіжка конфіденційної інформації та порушення роботи систем.

Продовження табл. 1.1 – Типи атак та їх вплив на мережу

Тип атаки	Опис	Загрози для мережі
«Людина посередені» (MitM)	MitM-атаки відбуваються, коли зловмисник перехоплює і змінює комунікацію між двома сторонами без їхнього відома.	Перехоплення конфіденційних даних, модифікація або знищення даних, порушення цілісності комунікацій.
SQL-ін'єкції	Атаки SQL-ін'єкцій передбачають вставку шкідливих SQL-запитів у поля введення для маніпулювання базою даних. Це може призвести до несанкціонованого доступу до даних або їх модифікації.	Крадіжка даних або маніпуляції з ними, порушення цілісності баз даних та злом веб-додатків.
Мережеві перехоплення	Мережеве перехоплення відбувається, якщо зловмисник отримує доступ до мережевого трафіку між двома пристроями і перехоплює його, щоб проаналізувати або змінити без відома користувачів. Зловмисник може отримати конфіденційну інформацію, таку як паролі або конфіденційні дані, або навіть внести зміни в дані, що надсилаються.	Перехоплення конфіденційних даних, розголошення конфіденційної інформації та порушення приватності користувачів.

Згідно з зазначеними вище небезпеками для мережі необхідно усвідомлювати потенційні загрози та застосовувати відповідні заходи безпеки. Щоб досягти цього, необхідно гарантувати відповідний рівень безпеки для всіх її компонентів, їх взаємодії всередині мережі, а також для підключення до Інтернету. Для безпечного підключення до Інтернету необхідно встановити міжмережевий екран або бандмауер, щоб фільтрувати вхідний і вихідний трафік на комп’ютері користувача. Дії, наведені нижче, можуть підвищити безпеку мережі та периферійного обладнання:

– фільтрація за MAC-адресами;

– використання механізму довірених/недовірених інтерфейсів і підтримка єдиної бази MAC-IP;

– використання захищених протоколів;

– використання складних паролів та їх періодична зміна;

– захист від несанкціонованого доступу до пристрою;

– налаштування системи автентифікації, авторизації та обліку;

– відключення сервісів, які не використовуються;

– підключення мережевих пристроїв до джерела безперебійного живлення;

– регулярне та своєчасне оновлення програмного забезпечення та антивірусних програм;

– використання засобів шифрування та резервне копіювання дуже важливої інформації.

Фільтрація MAC-адрес може відповідати таким протоколам, як Port Security або MAC Address Filtering. Під час порівняння MAC Address Filtering і Port Security слід мати на увазі основні відмінності між ними.

MAC Address Filtering:

1. Простота налаштування: легко встановлюється і підходить для невеликих мереж або сценаріїв з обмеженою кількістю пристроїв.

2. Гнучкість: надає можливість дозволити або заблокувати певні MAC-адреси на кожному порту.

3. Вразливість до злому: можна легко обійти, якщо зловмисники дізнаються реальні MAC-адреси та імітують їх.

Port Security:

1. Складність: забезпечує вищий рівень безпеки, оскільки відстежує не лише MAC-адреси, а й кількість підключених пристроїв.

2. Універсальність: дозволяє обмежувати не тільки конкретні MAC-адреси, а й кількість пристроїв, які можна підключити до порту.

3. Керування: складніший у налаштуванні, але надає більше можливостей керування, особливо у великих мережах.

Вибираючи один із цих двох методів, слід враховувати розмір мережі та вимоги до безпеки. Port Security забезпечить більшу функціональність і безпеку в більших і складніших умовах, тоді як MAC Address Filtering може бути ефективнішим і швидшим інструментом для невеликих мереж.

Для фільтрації трафіку також часто використовується технологія VLAN. VLAN – це спосіб розділити мережу на віртуальні сегменти, які можуть використовувати однакові ресурси та фізично розташовані в різних частинах мережі. Це дозволяє контролювати трафік між різними групами користувачів, що підвищує стійкість і продуктивність мережі.

Списки контролю доступу можуть бути використані для запобігання несанкціонованому доступу до пристроїв мережі. ACL – це набір правил, які дозволяють або забороняють трафік у мережі на основі параметрів, таких як протоколи, порти та IP-адреси. Вони дозволяють модифікувати контроль доступу до мережі та реагувати на різноманітні загрози безпеці. На всіх рівнях моделі OSI можуть бути реалізовані списки доступу.

У порівнянні цих двох технологій варто зазначити, що VLAN і ACL мають різні можливості. В той час як віртуальні локальні мережі забезпечують логічне розділення мережі, списки ACL регулюють доступ до ресурсів, розташованих у цій мережі. Обидві технології можна використовувати для створення комплексних систем управління мережею та безпеки.

Використання захищених протоколів є наступним аспектом, на який слід звернути увагу. Він є важливим компонентом безпеки мережі. Telnet і SSH є двома основними протоколами, які можна використовувати для виконання цієї операції.

Telnet і SSH є універсальними програмами для клієнт-серверів, які дозволяють користувачам взаємодіяти з віддаленими системами.

Незважаючи на те, що Telnet і SSH схожі, існує багато відмінностей між ними. Найважливішим з них є те, що SSH має більшу безпеку, ніж Telnet, тому він майже повністю замінює Telnet у повсякденному використанні. За замовчуванням Telnet і SSH використовують різні порти. SSH може шифрувати трафік у двох напрямках, а Telnet може передавати дані лише у вигляді звичайного тексту [2].

Таблиця 1.2 – Порівняння Telnet та SSH

Функція	**Telnet**	**SSH**
Операція	Використовує порт TCP 23 і найкраще працює у локальних мережах	За замовчуванням використовується порт TCP 22. Легко змінити номер порту
Безпека	Менш безпечний, ніж SSH, має багато вразливостей. Важко зашифрувати дані	Високий рівень безпеки
Автентифікація	Немає механізму автентифікації	Використовується шифрування з відкритим ключем
Формати даних	Дані передаються у вигляді простого тексту	Дані передаються в зашифрованому форматі через захищений канал
Операційні системи	Linux і Windows	Всі популярні операційні системи
Використання пропускної здатності	Низька	Висока

Для підвищення безпеки також використовується модель AAA. Це важливий компонент безпеки комп'ютерних мереж, який забезпечує аутентифікацію, авторизацію та облік користувачів, які намагаються отримати доступ до мережевих ресурсів. Існує кілька стандартів, покликаних забезпечити уніфікований підхід до контролю доступу до мережі.

Мережеве обладнання Cisco підтримує три протоколи серверів безпеки – TACACS+, RADIUS і Kerberos. TACACS+ і RADIUS є основними протоколами серверів безпеки, які використовуються для виконання завдань AAA з маршрутизаторами, міжмережевими екранами та серверами мережевого доступу. Сервер безпеки та мережеве обладнання обмінюються даними про контроль доступу через ці протоколи.

Ключова різниця між RADIUS і TACACS+ полягає в тому, що TACACS+ розділяє функції авторизації, в той час як RADIUS поєднує в собі і автентифікацію, і авторизацію. RADIUS призначений для абонентів AAA, а TACACS+ – для її адміністраторів. RADIUS все ще можна використовувати для адміністраторів невеликих мереж, але тільки якщо авторизація не потребується або якщо це стосується

однорідної мережі (все від одного постачальника). Однак для гетерогенного середовища або для мережевих пристроїв, які потребують політики авторизації, TACACS+ є найкращим вибором.

Підключення мережевих пристроїв до джерела безперебійного живлення є не менш важливим аспектом у забезпеченні надійності та захищеності мережевої інфраструктури. Для цього можна використовувати не лише фізичні засоби, такі як джерела безперебійного живлення (ДБЖ) та резервні джерела живлення, але й мережеві протоколи.

Наприклад, протокол HSRP дозволяє створити віртуальний маршрутизатор з двох або більше фізичних маршрутизаторів, де один виступає в ролі активного маршрутизатора, а інший – резервного, автоматично перемикаючись у разі збою. Схожий протокол, VRRP, також забезпечує автоматичне перемикання між маршрутизаторами, але він є відкритим стандартом, на відміну від HSRP, який є власністю компанії Cisco. Обидва протоколи підтримують конфігурацію пріоритетності та забезпечують високу доступність каналів, проте HSRP має кращу підтримку стану інтерфейсу, що може бути дуже корисним для мережевої безпеки в майбутньому.

Одним з ключових компонентів мережевої безпеки є використання технології VPN. Це передовий метод безпеки, який дозволяє захистити і зберегти конфіденційність трафіку між вузлами мережі за допомогою шифрування та автентифікації. Використовується для підвищення безпеки при передачі даних через незахищені мережі шляхом створення захищеного тунелю для передачі інформації. Найпоширенішими видами цієї технології є:

1. IPsec VPN – це протокол віртуальної приватної мережі, який захищає локальне підключення шляхом шифрування та автентифікації даних на рівні мережевих пакетів.

2. SSL VPN – це технологія VPN, яка використовує протокол SSL (Secure Sockets Layer) для встановлення безпечного з'єднання між користувачем і сервером через веб-браузер.

3. L2TP/IPsec – це комбінована технологія VPN, яка використовує L2TP для створення тунелю і IPsec для шифрування трафіку. Ця технологія часто використовується для створення VPN на рівні маршрутизатора.

4. PPTP – це протокол VPN, який забезпечує шифрування трафіку та автентифікацію даних на рівні пакетів. Хоча він менш безпечний, його зазвичай легко налаштувати і використовувати.

Порівняємо ці технології за наступними критеріями:

1. Рівень безпеки:

– IPsec VPN: забезпечує високий рівень безпеки завдяки шифруванню та автентифікації даних на рівні мережевих пакетів.

– SSL VPN: також забезпечує високий рівень безпеки завдяки шифруванню та автентифікації, але на транспортному рівні (SSL/TLS).

– L2TP/IPsec: забезпечує рівень безпеки, подібний до IPsec, але з використанням комбінованого підходу L2TP та IPsec.

– PPTP: має нижчий рівень безпеки, ніж інші технології, оскільки використовує менш безпечний метод шифрування.

2. Сумісність та розгортання:

– IPsec VPN: Підтримується більшістю мережевих пристроїв і операційних систем, але вимагає додаткового налаштування для роботи через брандмауери і NAT.

– SSL VPN: Простий у використанні, оскільки може використовуватися через стандартні веб-браузери і не вимагає встановлення спеціального клієнта. Може не підтримуватися деякими маршрутизаторами та мережевими пристроями.

– L2TP/IPsec: Підтримується багатьма пристроями та операційними системами, але може бути менш простим у розгортанні через необхідність налаштування L2TP та IPsec.

– PPTP: Простий у розгортанні, оскільки підтримується більшістю операційних систем. Однак він менш безпечний і не рекомендується для критично важливих середовищ.

3. Продуктивність:

– IPsec VPN, SSL VPN і L2TP/IPsec зазвичай мають приблизно однакову продуктивність, оскільки використовують схожі методи шифрування.

– PPTP може працювати трохи краще завдяки менш складному шифруванню.

Як правило, вибір конкретної технології VPN залежить від потреб і вимог мережі, а також від балансу між безпекою, простотою використання і продуктивністю.

1.2 Вибір оптимальних мережевих протоколів та сервісів для безпеки мережі організації

Щоб захистити організацію, потрібен структурований підхід для забезпечення необхідного рівня захищеності. Для вирішення цього питання організації використовують різноманітні технології та протоколи. Серед них можна виділити найважливіші, які допомагають підвищити рівень безпеки даних у мережі.

1. *VLAN* (віртуальна локальна мережа) – це група вузлів зі спільним набором вимог, які взаємодіють так, ніби вони належать до одного домену, незалежно від їх фізичного розташування. VLAN має ті ж властивості, що і фізична локальна мережа, але дозволяє об'єднувати кінцеві точки в групи, навіть якщо вони не під'єднані до одного мережевого комутатора. Налаштування мережі можна змінювати за допомогою програмного забезпечення, а не фізичного переміщення пристроїв.

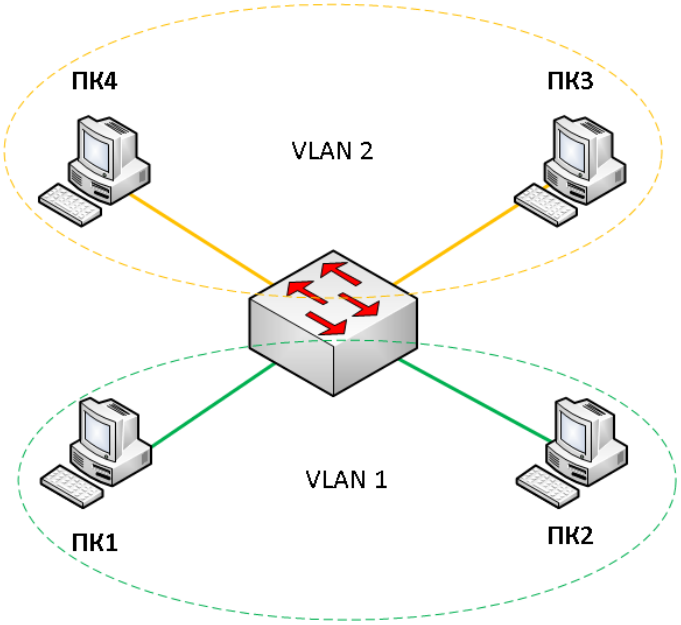


Рис. 1.1 – Принцип роботи технології VLAN

Використання VLAN для захисту комп'ютерних мереж може мати наступні переваги [3]:

– логічна сегментація мережі: віртуальні локальні мережі дозволяють розділити мережу на окремі сегменти, допомагаючи керувати трафіком і обмежувати доступ до ресурсів. Це знижує ризик несанкціонованого доступу та поширення загроз по мережі.

– покращена безпека: віртуальні локальні мережі дозволяють впроваджувати політики безпеки на рівні VLAN. Адміністратори можуть встановлювати правила доступу, контролювати зв'язок між VLAN і відстежувати активність користувачів в кожній VLAN.

– мінімізація обсягу трафіку: розділивши мережу на VLAN, можна зменшити обсяг трафіку, який надходить до кожного пристрою. Це покращує продуктивність мережі та зручність роботи користувачів.

– легка масштабованість: віртуальні локальні мережі дозволяють легко розширювати мережу, додаючи нові VLAN або змінюючи конфігурацію існуючих. Це забезпечує гнучкість і простоту керування мережею.

Мережа VLAN – це широкомовний домен, тож комп'ютери в інших віртуальних локальних мережах не можуть взаємодіяти без використання пристроїв маршрутизації. Для виконання базових функцій маршрутизації можна використовувати будь-який пристрій, що підтримуватиме маршрутизацію 3-го рівня, наприклад, маршрутизатор або багаторівневий комутатор.

2. *HSRP* (протокол гарячого резервування маршрутизатора) – це фірмовий протокол, створений компанією Cisco Systems, який забезпечує більшу надійність роботи шлюзу завдяки використанню кількох, як правило, фізично розділених, пристроїв 3-го рівня.

HSRP дозволяє сформувати одну або декілька пар фізичних або віртуальних інтерфейсів 3-го рівня, що належать до різних пристроїв (комутаторів або маршрутизаторів 3-го рівня), і призначити спільну MAC-адресу та IP-адресу для кожної з груп інтерфейсів (які можна вважати віртуальними). Водночас лише один інтерфейс 3-го рівня в групі перебуває в активному стані і лише один інтерфейс – у стані

очікування. IP-пакети маршрутизуються тільки через інтерфейс 3-го рівня, який знаходиться в активному стані. Активний інтерфейс, після отримання ARP-запиту, що містить віртуальну IP-адресу відповідної HSRP-групи, надсилає ARP-відповідь, що містить віртуальну MAC-адресу HSRP-групи, що призводить до надсилання наступного Ethernet-кадру на активний інтерфейс. Відмова поточного активного інтерфейсу призводить до переходу на резервний інтерфейс, який виконує функцію маршрутизації IP-пакетів.

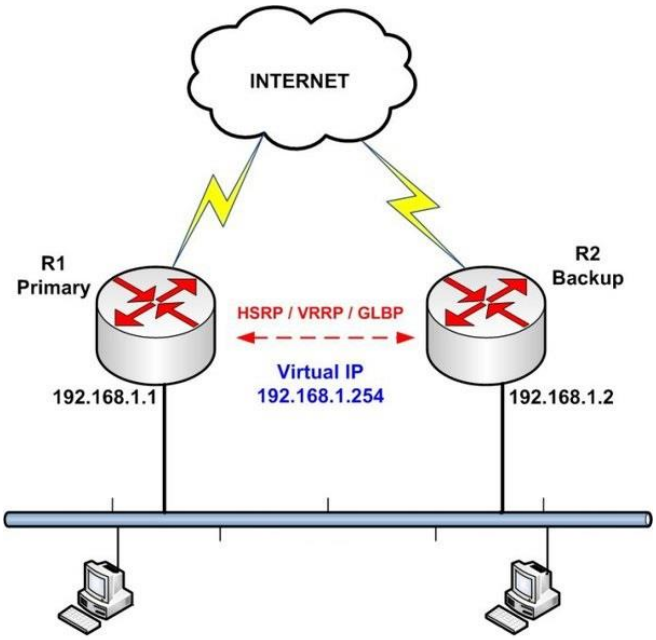


Рис. 1.2 – Принцип роботи протокола HSRP

Використання HSRP для захисту мережі має кілька важливих переваг:

– висока доступність: HSRP забезпечує швидке виявлення та автоматичний перехід на резервний маршрутизатор у разі виходу з ладу основного роутера. Це гарантує безперебійну роботу мережі та дозволяє уникнути втрати зв'язку.

– надійність: система резервування HSRP мінімізує ризик відмови мережі та забезпечує стабільну роботу в умовах високих навантажень або технічних проблем.

– простота налаштування: HSRP має простий у використанні синтаксис конфігурації, що дозволяє адміністраторам швидко та ефективно налаштовувати резервування шлюзів безпеки.

– забезпечує безперервність роботи: автоматичне перемикання на резервний маршрутизатор забезпечує безперервну роботу мережі без значних збоїв навіть у разі відмови апаратного забезпечення.

3. *IPSec Site-to-Site VPN* (віртуальна приватна мережа) – це технологія шифрування та захисту з'єднань між двома віддаленими мережами [4]. Вона використовується для утворення захищеного тунелю між двома мережевими вузлами, який дозволяє передавати дані через незахищений канал, наприклад, Інтернет. Одним з найпоширеніших варіантів реалізації IPSec VPN є використання обладнання Cisco. Обладнання Cisco має можливість підтримки IPSec VPN і забезпечує широкий діапазон можливостей для налаштування та управління VPN-з'єднаннями.

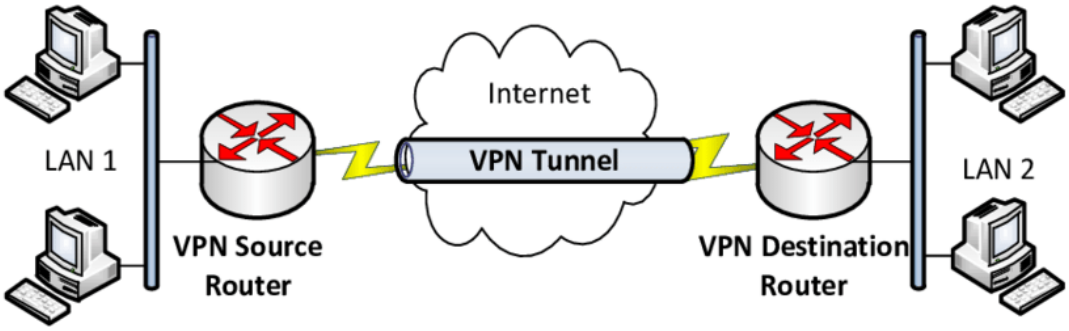


Рис. 1.3 – Принцип роботи IPSec Site-to-Site VPN

Основні характеристики та відомості про використання IPSec Site-to-Site VPN в мережі на основі Cisco включають в себе наступне:

– автентифікація: IPSec Site-to-Site VPN надає можливість автентифікації між віддаленими мережами для перевірки їх дійсності перед встановленням VPN-з'єднання. Пристрої Cisco підтримують різні способи автентифікації, такі як приватні ключі, встановлені паролі або цифрові сертифікати.

– шифрування даних: IPSec VPN між мережами використовує механізм шифрування для захисту конфіденційності даних під час їхнього передавання між віддаленими мережами. Обладнання Cisco підтримує різні алгоритми шифрування, такі як AES (Advanced Encryption Standard), 3DES (Triple Data Encryption Standard) та інші.

– керування ключами: IPSec VPN використовує протоколи обміну ключами для забезпечення захищеного з'єднання. Обладнання Cisco підтримує такі протоколи обміну ключами, як IKEv1 (Internet Key Exchange version 1) і IKEv2 (Internet

Key Exchange version 2), які дозволяють безпечно встановлювати VPN-з'єднання і обмінюватися ключами шифрування між віддаленими мережами.

– маршрутизація: пристрої Cisco мають потужні функції маршрутизації, які дозволяють налаштовувати трафік, що проходить через мережу IPSec VPN. Це дозволяє ефективно спрямовувати дані між віддаленими мережами через безпечний тунель.

– моніторинг та управління: обладнання Cisco надає інструменти для моніторингу та управління мережами IIPSec Site-to-Site VPN. Вони включають можливість налаштування політик безпеки, перевірки стану VPN-з'єднань, реєстрації та аудиту подій, а також налаштування резервних з'єднань для забезпечення безперервності роботи мережі.

IPSec Site-to-Site VPN на базі обладнання Cisco забезпечує високий рівень захисту і конфіденційності даних завдяки шифруванню, дозволяє розширювати мережу за рахунок безпечного підключення віддалених офісів, а також легко налаштовується за допомогою CLI і графічного інтерфейсу. Висока продуктивність і механізми резервування забезпечують ефективну передачу великих обсягів даних і безперервну роботу мережі.

4. *SSH* – це криптографічний мережевий протокол, призначений для віддаленого підключення до ОС і безпечного віддаленого керування через незахищену мережу (наприклад, Інтернет).

SSH забезпечує захищений канал зв'язку між клієнтом і сервером, через який можна передавати дані (пошту, відео, файли), працювати в командному рядку і запускати віддалені програми, в тому числі графічні. SSH-сервер має бути встановлено на віддаленій операційній системі. SSH-клієнт має працювати на комп'ютері, до якого буде здійснюватися віддалене підключення.

Безпека SSH-з'єднання досягається за рахунок:

– шифрування даних за допомогою одного з існуючих алгоритмів;

– автентифікації сервера і клієнта одним з багатьох доступних методів;

– наявністю додаткових функцій протоколу, призначених для запобігання різним хакерським атакам.

Серверна автентифікація забезпечує захист від:

– підміни IP-адреси, коли віддалений хост відправляє пакети від імені іншого віддаленого хоста;

– підміни DNS-записів, коли підробляється запис DNS-сервера, в результаті чого замість бажаного з'єднання встановлюється з'єднання з хостом, зазначеним у фальшивому записі;

– перехоплення відкритих паролів та інших даних, які явно передаються через статичне з'єднання.

На сьогодні існує дві версії протоколу SSH (SSH-1 і SSH-2), при цьому друга версія була вдосконалена і розширена в порівнянні з першою. Наприклад, друга версія стійка до атак типу «людина посередині». Існує також дві версії цього протоколу: з відкритим вихідним кодом (безкоштовна) і комерційна (платна).

5. *Syslog* (системний журнал) – це стандартний сервіс для надсилання та реєстрації повідомлень про події в системі подій (тобто створення журналів), що використовується в комп'ютерних мережах. Він працює за протоколом IP.

Сучасні системи журналювання подій зазвичай є централізованими мережевими системами, які використовують бази даних (у тому числі розподілені) для зберігання інформації. Централізований підхід до організації логів надає адміністратору наступні переваги:

– швидкий пошук записів про події, оскільки вся інформація міститься в єдиному системному журналі;

– спрощення процесу поточного управління пристроями та користувачами мережі, тому що останні дані системного журналу можуть використовуватися для моніторингу стану всіх пристроїв та користувачів мережі;

– полегшення аналізу даних системного журналу, адже великий об'єм інформації дозволяє більш точно відслідковувати та прогнозувати поведінку окремих пристроїв та користувачів мережі, а також їх поведінку в цілому;

– зменшення ризику втрати даних, тому що в більшості сучасних серверів використовується резервне сховище даних;

– підвищення рівня безпеки мережі, оскільки миттєве виявлення аномальних подій, пов'язаних з втручанням зловмисника в роботу мережі, дозволяє запобігти діям зловмисника і не допустити втрати інформації.

1.3 Методи автентифікації, авторизації та обліку на основі моделі AAA та протоколу TACACS+

У сфері мережевої безпеки термін AAA розшифровується як автентифікація, авторизація та облік. Це модель або система, яка використовується для захисту корпоративних мереж шляхом ідентифікації та контролю доступу, гарантії дотримання політик безпеки та відстеження активності користувачів. Вона є комплексним підходом до управління автентифікацією користувачів, привілеями доступу та записом інформації про користувачів для звітності та аудиту. У службах AAA найчастіше використовуються два протоколи: TACACS+ і RADIUS.

Розглянемо детальніше три компоненти системи AAA [5]:

1. Автентифікація: процес перевірки особи або пристрою, який намагається отримати доступ до мережі. Це важливий етап системи AAA, який гарантує, що доступ до мережі можуть отримати лише особи, які отримали дозвіл. Паролі, сертифікати, біометричні фактори (наприклад, відбитки пальців, розпізнавання обличчя) або автентифікація на основі ключів є прикладами методів автентифікації.

2. Авторизація: наступний етап AAA, який визначає ступінь доступу та дозволів, наданих автентифікованому суб’єкту. Щоб переконатися, що користувачі мають належні привілеї відповідно до своїх ролей та обов’язків в організації, необхідно впровадити детальну політику контролю доступу.

3. Облік: цей крок фіксує важливі дані, такі як час входу/виходу з системи, тривалість сеансу, передані дані та конкретні дії, що допомагає в аудиті безпеки та виявленні шахрайства. Механізми обліку, централізовані в системі AAA, полегшують моніторінг і аналіз.

Протокол TACACS+ був розроблений Cisco, і він є продовженням попередніх версій TACACS і XTACACS. Незважаючи на те, що назви схожі, TACACS+ був значно змінений і не сумісний з TACACS, який зараз майже не використовується.

Хоча TACACS+ зазвичай використовується для адміністрування мережевих пристроїв, він також може використовуватися для деяких типів AAA під час доступу до мережі. TACACS+ використовує протокол управління передачею (TCP) порт 49, а не порт UDP, оскільки він більш надійний і дозволяє отримувати інформацію про потенційні помилки заздалегідь за допомогою пакету TCP-RST. Хоча протокол TCP є менш швидким, він має інші переваги, такі як можливість розділити автентифікацію, авторизацію та облік як окремі та автономні процеси, багаторазові авторизації після однієї автентифікації та шифрування всього вмісту пакету.

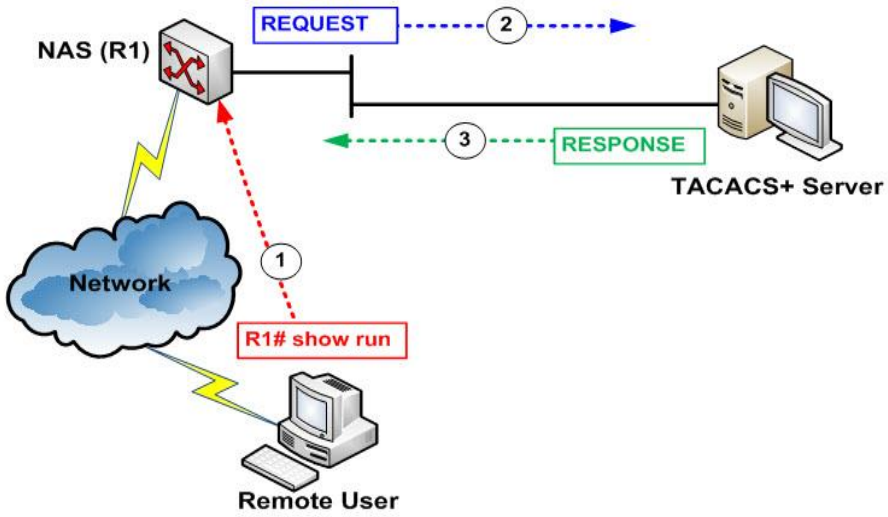


Рис. 1.4 – Принцип роботи протоколу TACACS+

TACACS+ використовує клієнтський підхід. Клієнт запитує сервер, а сервер перевіряє, чи є користувач автентифікованим чи ні. Важливо пам'ятати, що клієнт – це не користувач або його комп'ютер, а пристрій, який намагається визначити, чи має користувач дозвіл на доступ до мережі. Зазвичай таким пристроєм є маршрутизатор або брандмауер.

Щоб побудувати безпечну мережу, інженери отримують додатковий рівень захисту, використовуючи TACACS+ для забезпечення автентифікації, авторизації та обліку. Це дозволяє їм більш детально контролювати доступ до мережевих сервісів. За допомогою спеціальної бази даних і налаштованих політик можна віддалено відстежувати користувачів мережі. Ці політики регулюють доступ користувача до різних пристроїв і сервісів, доступних на цьому пристрої. Їх можна відклю-

чити, якщо обліковий запис користувача зламано. Облікові записи можна використовувати для відстеження доступу користувача до сервісів. Оскільки все більше співробітників починають працювати віддалено, TACACS+, безумовно, може підвищити ефективність і безпеку управління обліковими записами користувачів і мережевими службами.

1.4 Принципи фільтрації трафіку з використанням списків контролю доступу

Фільтрація трафіку (Traffic filtering) – це процес обробки повідомлення, отриманого пристроєм зв'язку, з метою відкинути повідомлення або переслати його на інший пристрій чи вузол. Термін "фільтрація" використовується для опису стандартних і додаткових правил, які використовуються при цьому процесі. Алгоритм пристрою визначає стандартні правила фільтрації, тоді як системний адміністратор встановлює індивідуальні правила для користувачів.

Загалом, список контролю доступу (ACL) – це набір правил, які дозволяють або забороняють трафіку проходити через пристрій. ACL можуть бути представлені на всіх рівнях моделі Open Systems Interconnection (OSI). Зазвичай ACL працюють тільки на мережевому або транспортному рівнях моделі OSI. ACL L3 і ACL L3/L4 відображаються на цих рівнях відповідно. Сьогодні стек TCP/IP є основним стеком, на якому базуються сучасні мережі, тому переважна більшість комунікаційних пристроїв використовують списки доступу до протоколів цього стека.

Застосування списків ACL на маршрутизаторах досить різноманітне. Вони використовуються для виконання таких завдань:

- фільтрація пакетів на інтерфейсах пристроїв;
- обмеження доступу при встановленні віддалених Telnet/SSH-з'єднань;
- налаштування пріоритету обробки QoS-трафіку;
- налаштування функцій шифрування трафіку для VPN-мереж;
- надання широкомовних адрес у технології NAT, тощо.

Списки контролю доступу можуть мати відмінності в застосуванні, призначенні, зовнішньому вигляді, часі використання тощо. На маршрутизаторах Cisco існує два типи списків управління доступом:

– стандартні списки контролю доступу (Standard ACL);

– розширені списки контролю доступу (Extended ACL).

Стандартні ACL можуть перевіряти тільки адреси джерел пакетів [6], розширені ACL можуть перевіряти як адреси джерел, так і адреси отримувачів. Розширені ACL для протоколу IP можуть виконувати перевірку протоколу вищого рівня та номери портів TCP/UDP.

Списки контролю доступу поділяються на два види:

– нумеровані (Numbered ACLs);

– іменовані (Named ACLs).

Нумерований список доступу позначається номером. Номери таких списків можуть відноситися до основного та розширеного діапазонів. Як правило, певний діапазон зарезервований для певного мережевого протоколу.

Іменований список доступу позначається символом (текстовим ім'ям). Назва іменованого списку доступу є чутливою до регістру. Як нумеровані, так і іменовані ACL поділяються на стандартні та розширені списки.

Приклад роботи стандартних списків контролю доступу полягає в наступному:

1. Визначення правил: адміністратор визначає правила, які вказують, які пакети дозволити або заборонити. Ці правила походять від джерела IP-адреси, яка може бути конкретною IP-адресою або її діапазоном.

2. Визначення пріоритетів: у стандартному списку контролю доступу кожне правило має пріоритет, який визначає порядок його застосування. Правила з меншими цифрами мають вищий пріоритет і будуть перевірятися першими.

3. Застосування списку до інтерфейсу: стандартний список контролю доступу повинен бути прикріплений до вхідного або вихідного інтерфейсу маршрутизатора. Після проходження пакета через цей інтерфейс він перевіряється на відповідність правилам, зазначеним у списку.

4. Дія з пакетом: якщо пакет відповідає правилам списку, встановленим адміністратором, йому може бути дозволено або заборонено пройти через маршрутизатор. Це залежить від того, як налаштовані правила в списку.

5. Моніторинг і налагодження: після впровадження списку контролю доступу адміністратор має можливість відстежувати трафік і коригувати правила, якщо це необхідно.

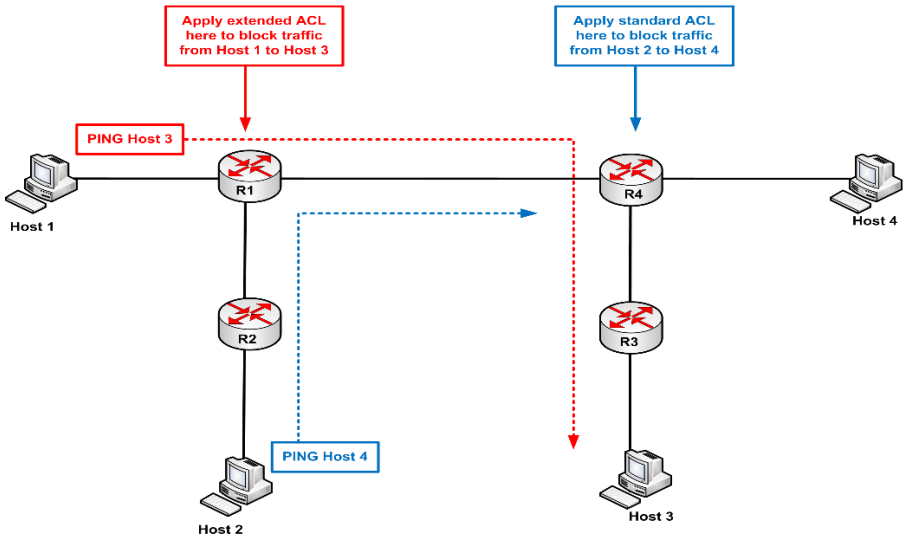


Рис. 1.5 – Принцип фільтрації трафіку за допомогою стандартних списків доступу

Отже, використання списків контролю доступу дозволяє мережевим адміністраторам фільтрувати трафік і регулювати доступ до ресурсів. Це підвищує безпеку мережі та запобігає несанкціонованому доступу до конфіденційних даних.

Висновки до першого розділу:

У цьому розділі було розглянуто основні аспекти захисту для підвищення безпеки мережі. Визначено оптимальні технології та протоколи для створення високого рівня безпеки та контролю доступу. Розглянуто використання сегментації мережі за допомогою VLAN, контроль трафіку за допомогою ACL, використання протоколів HSRP та IPSec VPN для забезпечення доступності та захисту даних. Проаналізовано реалізацію автентифікації на основі протоколів TACACS+ та SSH, а також моніторинг мережевих подій за допомогою протоколу SYSLOG.

РОЗДІЛ 2 ПРОЄКТУВАННЯ ТА РОЗРОБКА ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ НА БАЗІ ОБЛАДНАННЯ CISCO

2.1 Вибір обладнання та ОС для організації роботи мережі

Особлива увага приділялася вибору обладнання, яке відповідало б вимогам організації щодо продуктивності, надійності та безпеки мережі під час створення захищеної комп'ютерної мережі організації на базі обладнання Cisco. Вибір Cisco для мережевого проєкту ґрунтувався на кількох ключових факторах [7]:

– надійність та якість: компанія Cisco вже багато років є провідним виробником мережевого обладнання. Їх продукція відповідає високим стандартам надійності та відмовостійкості і забезпечує безперебійну роботу мережі.

– широкий асортимент продукції: Cisco пропонує широкий асортимент мережевих пристроїв, таких як комутатори, брандмауери, маршрутизатори та інші мережеві компоненти. Це дозволяє обрати найкраще обладнання для проєкту та забезпечити інтеграцію і сумісність.

– інновації та технологічний прогрес: Cisco постійно впроваджує інноваційні рішення в мережеву індустрію. Використання обладнання Cisco забезпечує масштабованість і готовність до майбутніх викликів, а також дозволяє йти в ногу з останніми тенденціями.

– підтримка стандартів безпеки: Cisco пропонує широкий спектр інструментів для захисту мережевих з'єднань і активно працює над вирішенням проблем безпеки. Вибір обладнання Cisco допомагає захистити і контролювати доступ до мережевих ресурсів.

Маршрутизатор Cisco 7200 Series VXR – один з ключових компонентів, який було обрано. Маршрутизатор Cisco 7200 Series VRX – це потужний мережевий маршрутизатор, який забезпечує розширені функції, високу надійність і високу швидкість передачі даних для побудови складних мережевих інфраструктур. Цей маршрутизатор був обраний для проєкту комп'ютерної мережі з кількох причин. Потужна обчислювальна платформа та оптимізований апаратний прискорювач маршрутизатора Cisco 7200 Series VRX забезпечують високу продуктивність. Це дозволяє

маршрутизатору ефективно обробляти великі обсяги трафіку та ресурсоємні додатки, що є важливою вимогою для проєкту.



Рис. 2.1 – Маршрутизатор Cisco 7200 Series VRX

Масштабованість маршрутизатора Cisco 7200 Series VRX є однією з його ключових переваг [8]. Це забезпечує гнучкість і дозволяє розширювати мережу відповідно до зростаючих потреб. Маршрутизатор підтримує широкий спектр різних інтерфейсів на різних швидкостях, забезпечуючи різноманітність підключень і високу пропускну здатність. Крім того, маршрутизатор Cisco 7200 Series VRX підтримує кілька протоколів маршрутизації, таких як OSPF, EIGRP і BGP. Це дозволяє створювати складні мережі з кількома маршрутизаторами та забезпечує найкращий можливий шлях передачі даних у мережі.

Також маршрутизатор Cisco 7200 Series VRX має вбудовані механізми мережевої безпеки, такі як брандмауер, фільтрація пакетів і VPN, щоб задовольнити вимоги щодо безпеки. Це забезпечує захист даних і обмежує несанкціонований доступ до мережі.

Для комутації мережевого трафіку у КМ було обрано комутатор Cisco Catalyst WS-C2960-24TT-L [9]. Цей комутатор підтримує кілька мережевих протоколів і функцій безпеки, а також забезпечує швидку та надійну комутацію. Він є хорошим способом у побудуві надійної та високопродуктивної мережі.



Рис. 2.2 – Комутатор Cisco Catalyst WS-C2960-24TT-L

У Catalyst WS-C2960-24TT-L є 24 порти Fast Ethernet, що дозволяє підключати його до 24 робочих станцій або інших мережевих пристроїв. Крім того, комутатор підтримує технологію Power over Ethernet (PoE), яка дозволяє мережевим кабелям живити підключені пристрої, такі як IP-телефони та бездротові точки доступу. Це робить розгортання простішим і забезпечує живлення багатьох пристроїв у мережі. Крім того, комутатор Cisco Catalyst WS-C2960-24TT-L пропонує додаткові функції безпеки та управління. Він підтримує кілька протоколів управління, таких як SNMP, SSH і Telnet, що дозволяє віддалено керувати комутатором. Крім того, комутатор підтримує звичайні функції безпеки, такі як списки доступу, ізоляція VLAN і безпечний доступ до управління. Це дозволяє контролювати трафік мережі та запобігати несанкціонованому доступу. Комутатор Cisco Catalyst WS-C2960-24TT-L також надійний і ефективний, адже він використовує оптимізовану апаратну платформу, яка зменшує втрату пакетів і забезпечує швидку обробку мережевого трафіку. Крім того, комутатор забезпечує резервні джерела живлення, щоб мережа могла працювати безперервно в разі відключення електроенергії.

Крім обладнання Cisco, були враховані також вимоги до продуктивності робочих станцій. Операційні системи Windows 10 і Linux Ubuntu 22 були обрані для цього. Ці операційні системи забезпечують зручне та надійне середовище для роботи з мережевими додатками, а також забезпечують сумісність з обладнанням Cisco та іншими компонентами мережі.

Windows 10 – одна з найпопулярніших операційних систем, розроблених компанією Microsoft. Вона має широкі можливості та надійну роботу, що дозволяє використовувати її на різних типах комп'ютерів і пристроїв. Використання

Windows 10 дозволяє ефективно контролювати та аналізувати події, що відбуваються на мережевих пристроях.



Рис. 2.3 – Обрана ОС для SYSLOG-сервера (Windows 10)

Linux Ubuntu 22 є одним із найбільш поширених дистрибутивів операційної системи Linux. Це безкоштовне програмне забезпечення з відкритим вихідним кодом, яке надає користувачам більше свободи та контролю над операційною системою: багато додатків, інструментів для розробки та простий у використанні графічний інтерфейс. Використання Linux Ubuntu 22 в якості клієнта TACACS+ гарантує безпеку та аудит доступу до мережевих ресурсів, дозволяючи керувати доступом до мережевих пристроїв.



Рис. 2.4 – Обрана ОС для TACACS+ клієнта (Linux Ubuntu 22)

2.2 Проєктування топології мережі на базі обладнання Cisco

Більшість мережевих атак спрямовані на такі цілі, як мережеві служби та додатки, маршрутизатори, комутатори, сервери та дані, що передаються. Напади можуть статися на різних рівнях моделі OSI, включаючи фізичний, канальний, мережевий, транспортний, сеансовий, рівень представлення та рівень прикладних програм.

Тому при проєктуванні мережі була використана трирівнева структура. Вона є логічною та надійною через надмірність апаратного забезпечення. Таким чином, мережа поділяється на три рівні [10]:

– рівень ядра (Core Layer);

– рівень розподілу (Distribution Layer);

– рівень доступу (Access Layer).

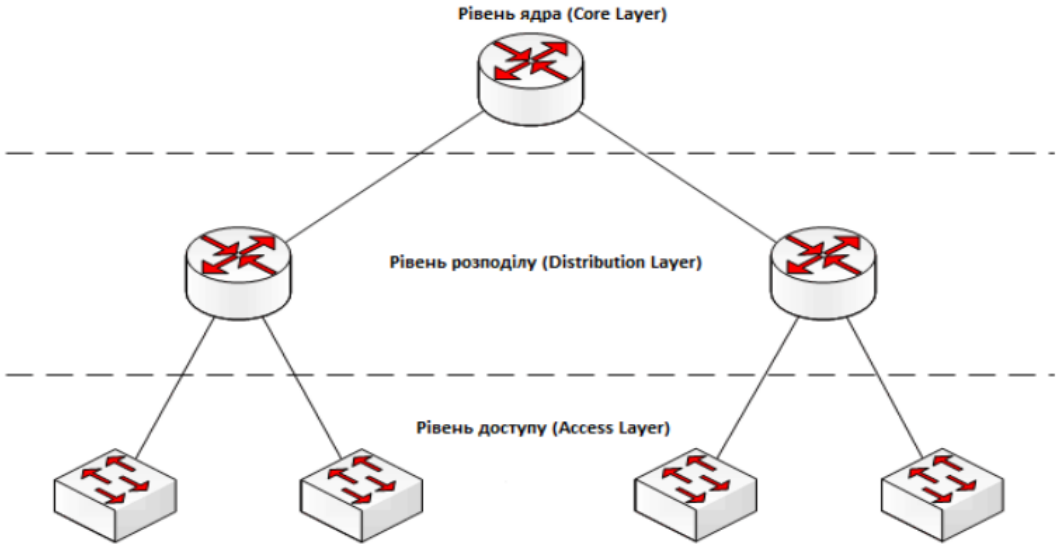


Рис. 2.5 – Приклад трирівневої структури мережі

1. Базовий рівень, або рівень ядра, є основою мережі. Цей рівень, який знаходиться на верхньому рівні ієрархії, відповідає за швидку та надійну передачу великих обсягів трафіку, а також за з'єднання мережі з мережами інших провайдерів.

Якщо щось піде не так на базовому рівні, це вплине на кожного користувача. Отже, забезпечити високу надійність на базовому рівні має вирішальне значення. На цьому рівні обробляються значні кількості трафіку, тому важливо враховувати затримки та швидкість.

2. Рівень робочих груп або рівень розподілу розташований між рівнем доступу та основним рівнем.

Рівень розподілу відповідає за визначення найшвидшого методу обробки запитів до сервісів. Після визначення найкращого шляху доступу на рівні розподілу запит можна передати на рівень ядра, де його можна передати до необхідного сервісу з високою швидкістю.

3. Рівень доступу використовується для контролю того, як користувачі та робочі групи можуть отримати доступ до об'єднаних мережевих ресурсів. Кожен користувач підключається прямо до рівня доступу.

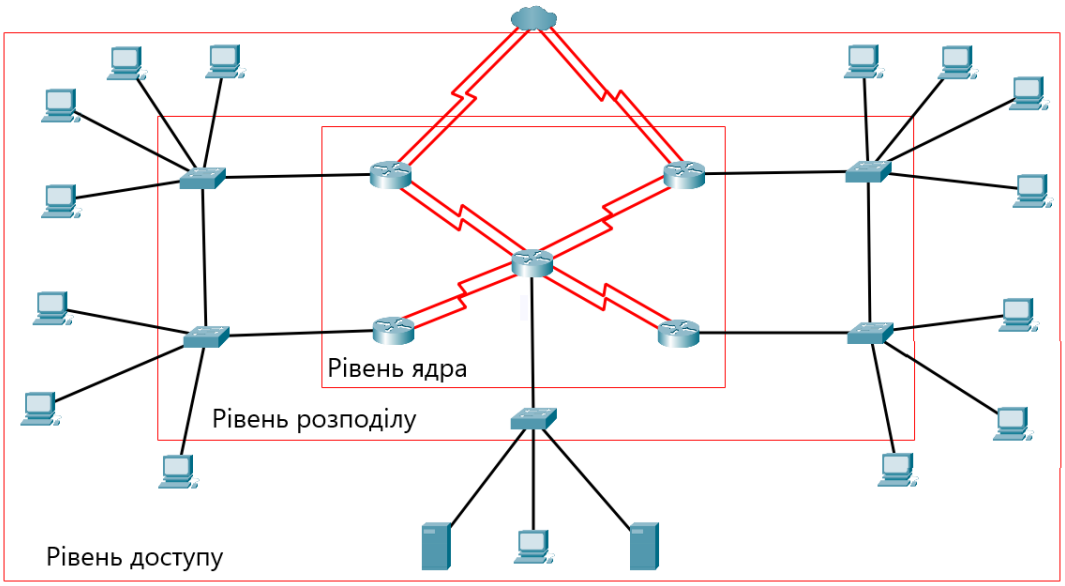


Рис. 2.6 – Топологія розробленої мережі

Основою мережі є архітектура з п'ятьма маршрутизаторами, щоб забезпечити високий рівень доступності та продуктивності. Забезпечуючи надійний канал передачі даних у мережі, ці маршрутизатори з'єднані послідовним з'єднанням (Serial). П'ять маршрутизаторів дозволяють створювати резервні шляхи та маршрути, щоб гарантувати безперервність роботи мережі навіть у разі виходу з ладу одного з них. Така конфігурація дозволяє підтримувати високу надійність і пропускну здатність ядра, що є критично важливим для оптимальної роботи мережі в цілому.

Розподільчий рівень мережі складається з п’яти комутаторів, які забезпечують маршрутизацію та перемикання між різними рівнями мережі. На розподільчому рівні ці комутатори є життєво важливими для забезпечення надійності та ефективності мережі. Вони з’єднані з основним мережевим рівнем за допомогою Ethernet-з’єднань, що дозволяє комутаторам і маршрутизаторам обмінюватися даними.

Мережа обслуговує загалом 15 робочих станцій, які користувачі використовують для виконання своїх завдань та доступу до мережевих ресурсів. Крім того, на рівні доступу розміщено два сервери, які виконують різні функції, включаючи зберігання даних і автентифікацію користувачів мережі.

2.3 Розробка проєкту захищеної комп’ютерної мережі організації

У процесі розробки захисту комп’ютерної мережі було прийнято багато стратегічних рішень для підвищення ефективності, безпеки та надійності мережі.

Насамперед мережа була розділена на сім віртуальних локальних мереж (VLAN) з номерами 10, 20, 30, 40, 50, 60 і 70. Це дозволить розмістити пристрої відповідно до їх функціональних потреб і логічно сегментувати мережу. VLAN 70 буде призначений для мережевих серверів, що забезпечить їм окреме управління та безпеку. З п’яти комутаторів, чотири можуть підтримувати два VLAN. Це означає, що кожна з цих підмереж фізично відокремлена від іншої. В результаті пристрої, які входять до однієї VLAN, не зможуть безпосередньо взаємодіяти з пристроями, які входять до іншої VLAN. Такий поділ VLAN дозволяє забезпечувати захист мережі та контролювати трафік, зменшуючи ймовірність несанкціонованого доступу до ресурсів. Кожна VLAN матиме унікальне ім'я, яке починається з літери, які використовуються в назвах робочих станцій. Це полегшує виявлення та управління групами пристроїв у мережі. Комутатори, які використовують VLAN, можуть сегментувати мережу, забезпечувати логічну ізоляцію груп пристроїв і контролювати доступ до ресурсів. Це підвищує безпеку мережі та забезпечує гнучкість у настройці та управлінні комп’ютерною мережею.

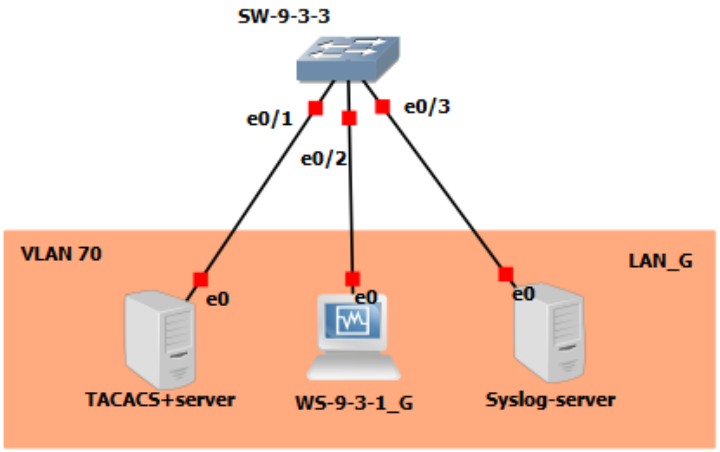


Рис. 2.7 – Представлення серверної підмережі VLAN 70

Як зазначалося вище, пристрої в одній VLAN не можуть зв'язуватися з іншими VLAN. Таким чином, протокол маршрутизації OSPF був обраний для забезпечення зв'язку між комп'ютерами адміністраторів мережі. OSPF буде поєднано з п'ятьма маршрутизаторами, які забезпечують маршрутизацію в мережі. Налаштування протоколу OSPF на маршрутизаторах дозволяє віртуальним локальним мережам взаємодіяти та обмінюватися інформацією про маршрутизацію в мережі. OSPF визначає найкоротші шляхи між VLAN на основі вартості маршруту та пропускної здатності. OSPF пропонує найкращий шлях для пакетів між VLAN, оскільки він автоматично адаптується до змін у топології мережі. Такий розподіл мережевого трафіку покращує загальну продуктивність і безпеку мережі.

Щоб підвищити відмовостійкість, кожен маршрутизатор повинен мати багатоканальне з'єднання, окрім використання протоколу маршрутизації OSPF та створення VLAN. Це досягається шляхом об'єднання двох послідовних кабелів в одне логічне з'єднання. Багатоканальне з'єднання дозволяє маршрутизаторам об'єднувати свої фізичні інтерфейси з віртуальними, що збільшує пропускну здатність і надійність. Коли доступні два кабелі для з'єднання маршрутизаторів, це дуже корисно. Багатоканальне з'єднання між маршрутизаторами дозволяє створювати з'єднання з високою пропускною здатністю та підвищувати надійність мережі. Це дозволить маршрутизаторам передавати дані швидко та стабільно, підвищуючи загальну ефективність і продуктивність комп'ютерної мережі.

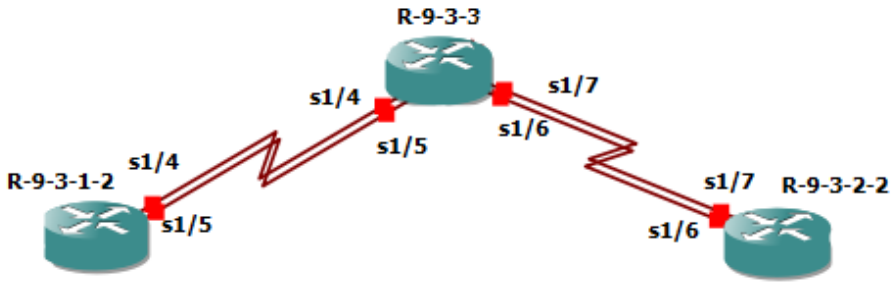


Рис. 2.8 – Вигляд з'єднання типу Multilink між маршрутизаторами мережі

Крім того, передбачається впровадження протоколу HSRP, щоб забезпечити надійність мережі та її стійкість. З використанням цього протоколу можна створити віртуальну IP-адресу та мережевий інтерфейс, який служить віртуальним шлюзом для всіх пристроїв у мережі. Забезпечуючи постійну доступність до мережі, резервний маршрутизатор автоматично стає активним у випадку, якщо активний маршрутизатор виходить з ладу. Протокол HSRP буде налаштований між маршрутизаторами 1-1 і 1-2 та 2-1 і 2-2. Перший маршрутизатор у кожній групі буде налаштований як активний, а другий – як резервний. Це означає, що весь трафік мережі буде передаватися активним маршрутизатором. У той же час резервний маршрутизатор буде працювати в режимі очікування, щоб виконувати функції активного маршрутизатора в разі його виходу з ладу. Такий метод забезпечить доступність і відмовостійкість мережі, мінімізує час простою мережі та надасть користувачам безперервний доступ до мережевих ресурсів.

Налаштування безпеки портів для кожного комутатора також було б вигідним. Протокол Port Security контролює доступ до порту комутатора та обмежує кількість пристроїв, підключених до порту. Використовуючи його, можна налаштувати обмеження на основі MAC-адреси, кількості підключених пристроїв або типу пристрою. Це запобігає несанкціонованому доступу та захищає мережу від несанкціонованих підключень пристроїв. Налаштування протоколу Port Security на кожному комутаторі дозволить нам керувати підключеними пристроями.

Налагоджені в майбутньому протоколи SSHv2 і TACACS+ підвищать безпеку мережі. TACACS+ забезпечує контроль доступу до мережевих пристроїв і автентифікацію користувачів, а SSHv2 шифрує трафік і захищає від перехоплення та злому. Це дозволяє централізовано контролювати привілеї та обмежує доступ до

мережевих ресурсів тільки авторизованим користу-вачам. Налаштування SSHv2 і TACACS+ покращують управління мережею, зменшують небезпеку несанкціонованого доступу та захищають і керують доступом до мережевих пристроїв.

Щоб захистити комп'ютерну мережу, було введено списки контролю доступу в кожну підмережу. ACL будуть налаштовані на кожному маршрутизаторі, який забезпечує зв'язок між підмережами. Кожен ACL міститиме набір правил, які визначають, який трафік дозволений або заборонений відповідно до джерела, призначення, порту та інших факторів. Крім того, передбачається використання списків для віддаленого підключення до мережевих пристроїв з комп'ютера адміністратора. Стандартні списки доступу дозволяють ізолювати та захистити важливі ресурси, детально контролювати трафік між підмережами та знизити ризик несанкціонованого доступу до мережевих ресурсів.

Реалізація IPsec Site-to-Site VPN забезпечує додатковий рівень захисту даних у КМ між маршрутизаторами 1-1 та 2-1. IPsec дозволяє створювати віртуальну приватну мережу (VPN), яка шифрує та захищає зв'язок між вузлами мережі. Це означає, що всі повідомлення, які передаються між цими маршрутизаторами, будуть захищені від несанкціонованого доступу. За допомогою IPsec Site-to-Site VPN можна створити безпечне тунельне з'єднання між цими маршрутизаторами, що гарантує конфіденційність і цілісність передачі даних. Це рішення дозволяє віддаленим частинам мережі мати надійний зв'язок і запобігає потенційним загрозам безпеки, таким як перехоплення або зміна даних під час передачі.

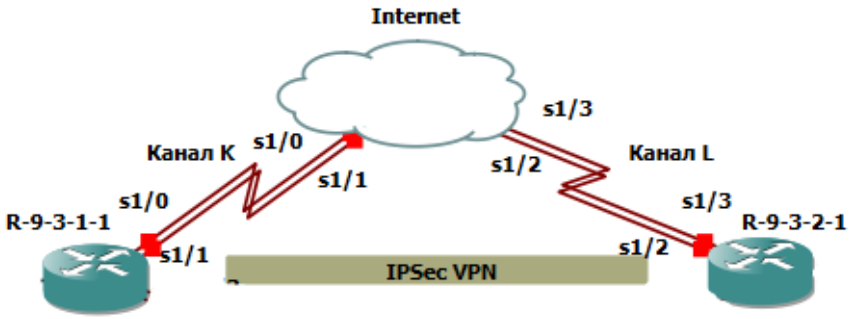


Рис. 2.9 – Представлення тунелювання IPsec Site-to-Site VPN між маршрутизаторами мережі

Всі ці дії спрямовані на те, щоб підвищити надійність, безпеку та ефективність мережі, зменшити загрози та ризики для організації, а також забезпечити високий рівень сервісу для користувачів.

2.4 Розробка схеми адресації мережі

Кожній підмережі виділено відповідний діапазон IP-адрес, щоб оптимізувати використання ресурсів і задовольнити потреби підключених вузлів. Це полегшує управління мережею та запобігає потенційним конфліктам IP-адрес. Хороше планування IP-адрес дозволяє використовувати механізми фільтрації трафіку та контролю доступу, щоб запобігти несанкціонованому доступу та зловживанням.

Представимо схему адресації у вигляді таблиці, щоб наочно відобразити IP-адреси, призначені кожному рівню, оскільки мережа містить багато каналів, інтерфейсів і віртуальних мереж з різними IP-адресами. В цьому розділі представлено скорочену версію таблиці адресації. Повний перелік інтерфейсів та їхніх адрес буде наведено в додатку Б.

Таблиця 2.1 – Параметри IP-адресації мережі

Мережа/ Пристрій	**Інтерфейс/Мережний адаптер/Шлюз**	**IP-адреса**	**Маска**	**Префікс**
Підмережа A (VLAN 10)	-	191.9.3.0	255.255.255.0	/24
Підмережа B (VLAN 20)	-	192.9.3.0	255.255.255.0	/24
Підмережа C (VLAN 30)	-	193.9.3.0	255.255.255.0	/24
Підмережа D (VLAN 40)	-	194.9.3.0	255.255.255.0	/24
Підмережа E (VLAN 50)	-	195.9.3.0	255.255.255.0	/24
Підмережа F (VLAN 60)	-	196.9.3.0	255.255.255.0	/24

Продовження табл. 2.1 – Параметри IP-адресації мережі

Мережа/ Пристрій	**Інтерфейс/Мережний адаптер/Шлюз**	**IP-адреса**	**Маска**	**Префікс**
Підмережа G (VLAN 70)	-	197.9.3.0	255.255.255.0	/24
Підмережа K (Канал K)	-	198.9.3.0	255.255.255.0	/24
Підмережа L (Канал L)	-	199.9.3.0	255.255.255.0	/24
Підмережа M (Канал M)	-	200.9.3.0	255.255.255.0	/24
Підмережа N (Канал N)	-	201.9.3.0	255.255.255.0	/24
Підмережа O (Канал O)	-	202.9.3.0	255.255.255.0	/24
Підмережа P (Канал P)	-	203.9.3.0	255.255.255.0	/24

Висновки до другого розділу:

У другому розділі було описано моделі маршрутизатора та комутатора, а також операційні системи, які будуть використовуватися у спроєктованій мережі. Зокрема, було розглянуто ключові аспекти проєктування захисту мережі, розробку комп'ютерної мережі з урахуванням заходів безпеки та розробку схеми адресації для ефективного функціонування мережі. Ці кроки сприяли створенню надійної та захищеної мережевої інфраструктури, яка відповідає потребам організації.

РОЗДІЛ 3 НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ СПРОЄКТОВАНОЇ КМ ОРГАНІЗАЦІЇ НА БАЗІ ОБЛАДНАННЯ CISCO

3.1 Підготовка до створення захищеної комп'ютерної мережі

Вибір методу журналювання подій у мережі є першим кроком у підготовці до проєкту. Для цього можна використовувати різні інструменти в середовищі GNS3, наприклад, програмне забезпечення Kiwi Syslog Server або SolarWinds Kiwi Syslog Server. Ці програми дозволяють створювати мережеву систему моніторингу та журналювання подій, яка розташована в одному місці. Таким чином, першим кроком у підготовці до роботи буде отримання доступу до Syslog-сервера на станції, а також встановлення його на операційну систему Windows 10.

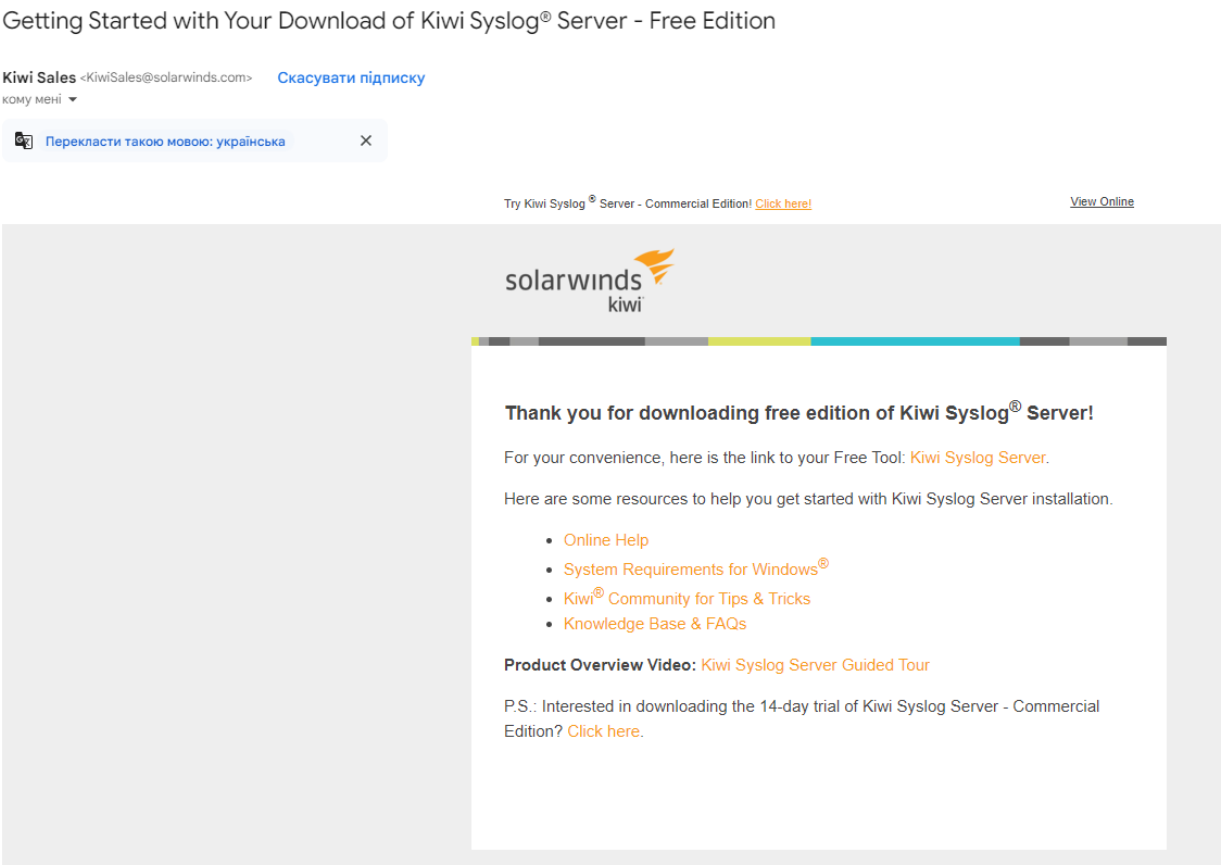


Рис. 3.1 – Лист з отриманням доступу для завантаження Kiwi Syslog Server

Перед підключенням станції до мережі потрібно розпакувати архівний файл і встановити програмне забезпечення, вибравши встановлення сервера замість додатку [11].

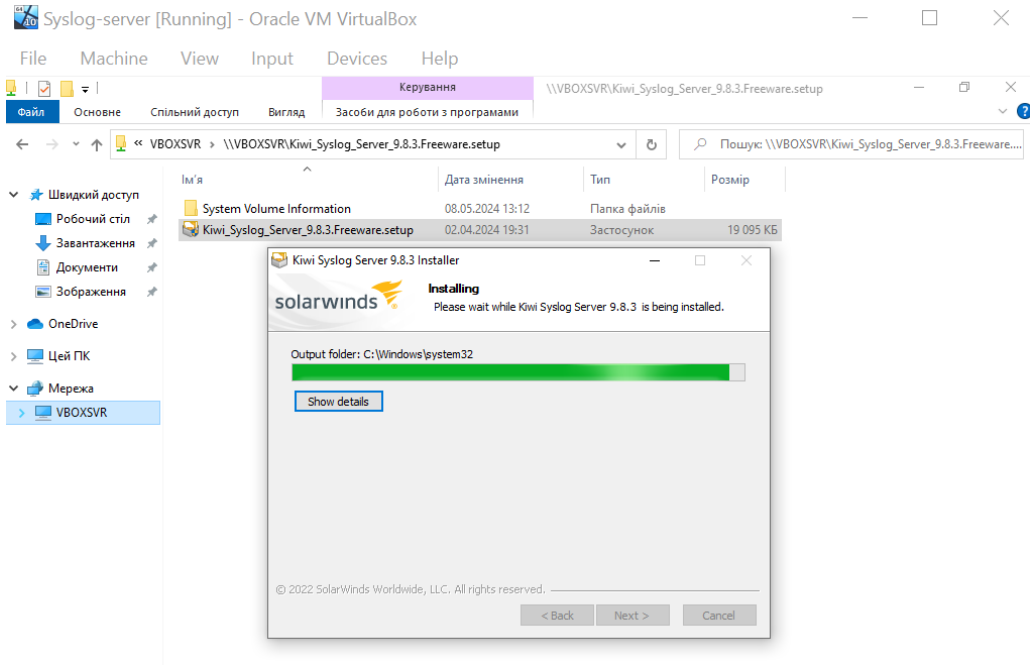


Рис. 3.2 – Встановлення Kiwi Syslog Server на станцію

Оскільки безкоштовна версія має обмеження на користування продуктом, програма повідомляє, що ми можемо налаштовувати журналювання подій лише для п'яти ресурсів.

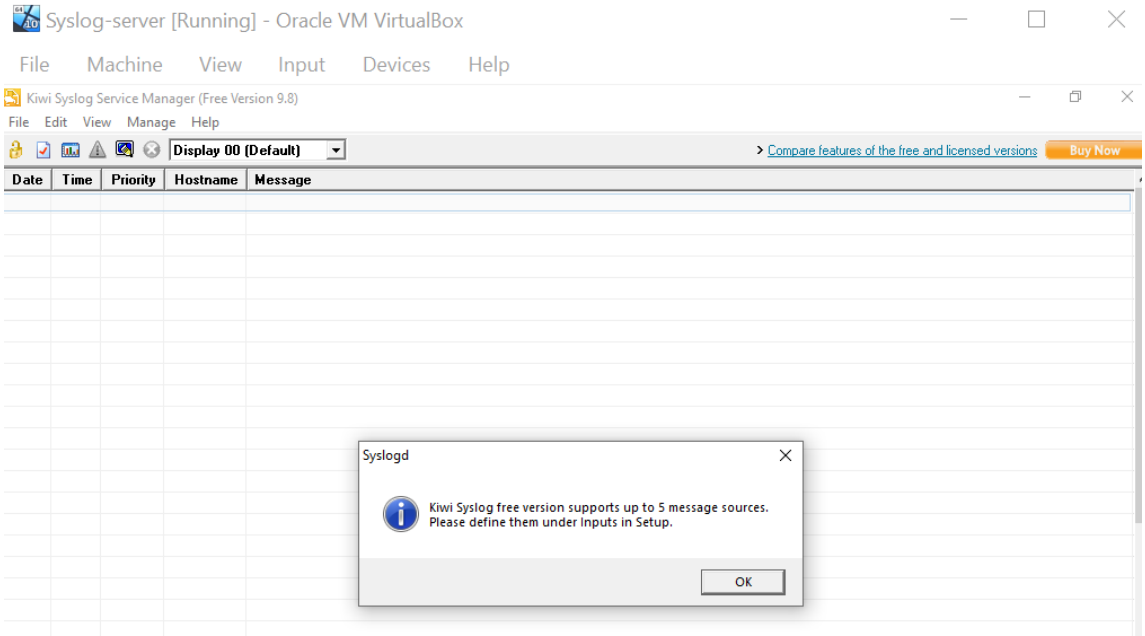


Рис. 3.3 – Успішне вастановлення та повідомлення про обмежені можливості безкоштовної версії

Після успішного встановлення сервера Syslog ми можемо перейти до зміни мережевих налаштувань як на серверах, так і на робочій станції-клієнті.

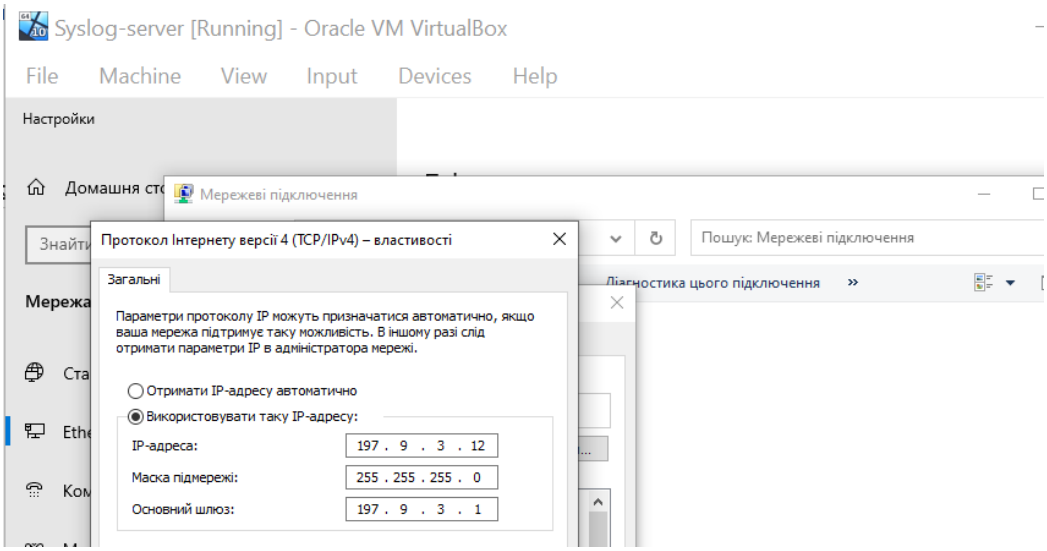


Рис. 3.4 – Зміна адреси на Syslog-сервері

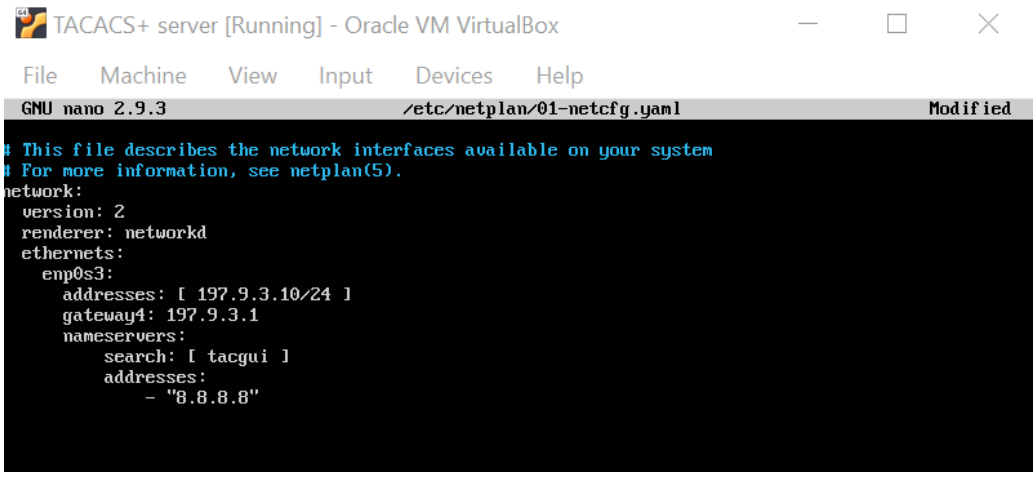


Рис. 3.5 – Зміна адреси на TACACS+ сервері

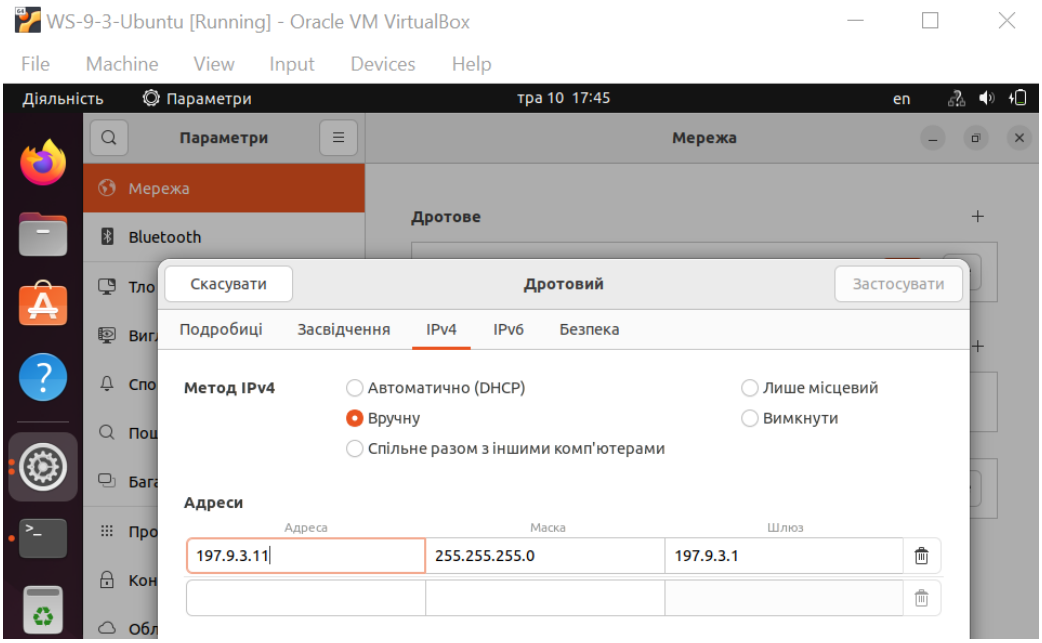


Рис. 3.6 – Зміна адреси на станції-клієнті Ubuntu

Для підключення до сервера TACACS+ було обрано варіант зміненого порту. Цей варіант використовує нестандартний порт для підключення до сервера TACACS+. Зазвичай сервер TACACS+ працює на порту 49. Однак для підвищення безпеки та запобігання потенційним атакам можна використовувати порт, відмінний від порту за замовчуванням. Підключаючись до сервера TACACS+ через інший порт, необхідно вказати номер порту у вигляді адреси сервера. Наприклад, на нашому сервері TACACS+, що працює на порту 8008, адреса сервера матиме вигляд адреса_сервера:8008. Після успішного з'єднання вікно повинно мати такий вигляд:

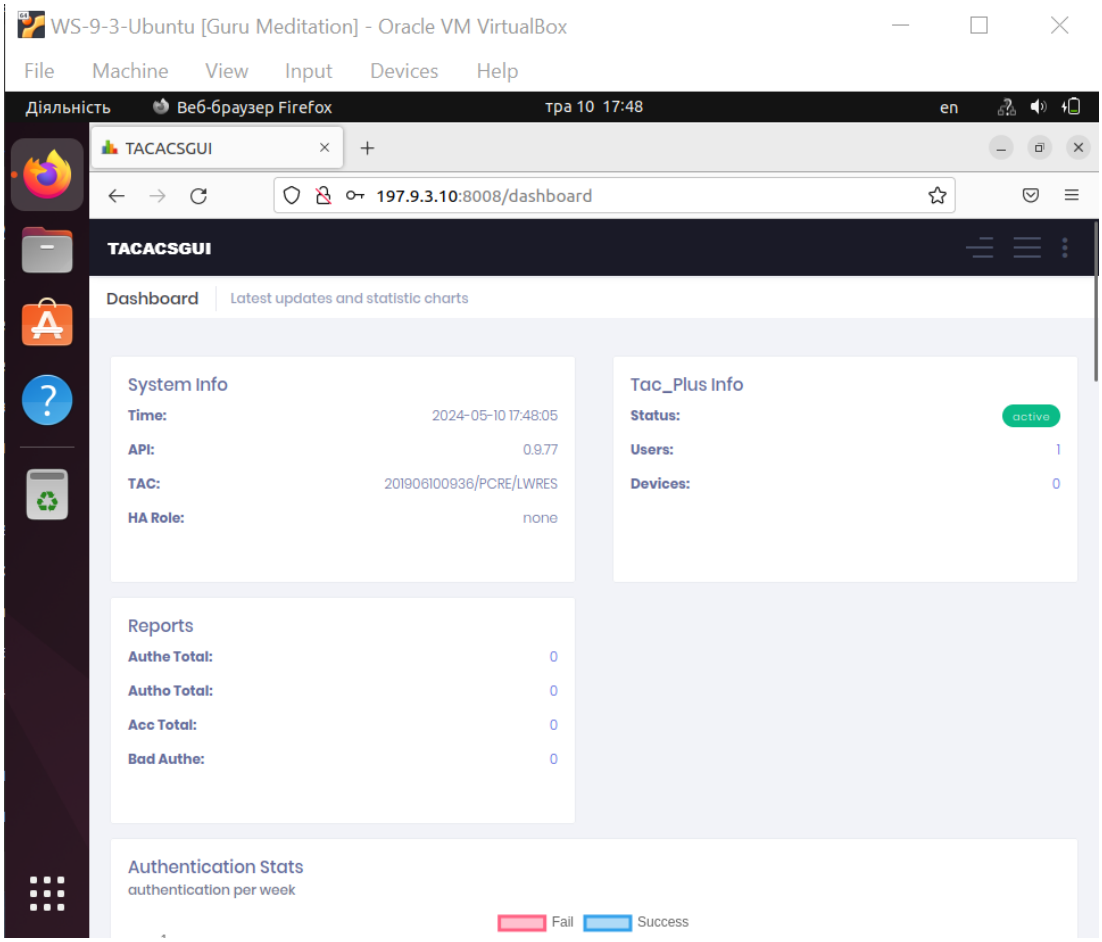


Рис. 3.7 – Вдалий вхід на сервер у TACACSGUI

Останнім кроком у підготовці мережі до конфігурації є додавання всіх необхідних інтерфейсів на мережевих пристроях. Оскільки маршрутизатори в середовищі GNS3 за замовчуванням мають лише один порт FastEthernet, нам потрібно додати до конфігурації пристрою ще один слот з послідовним з'єднанням:

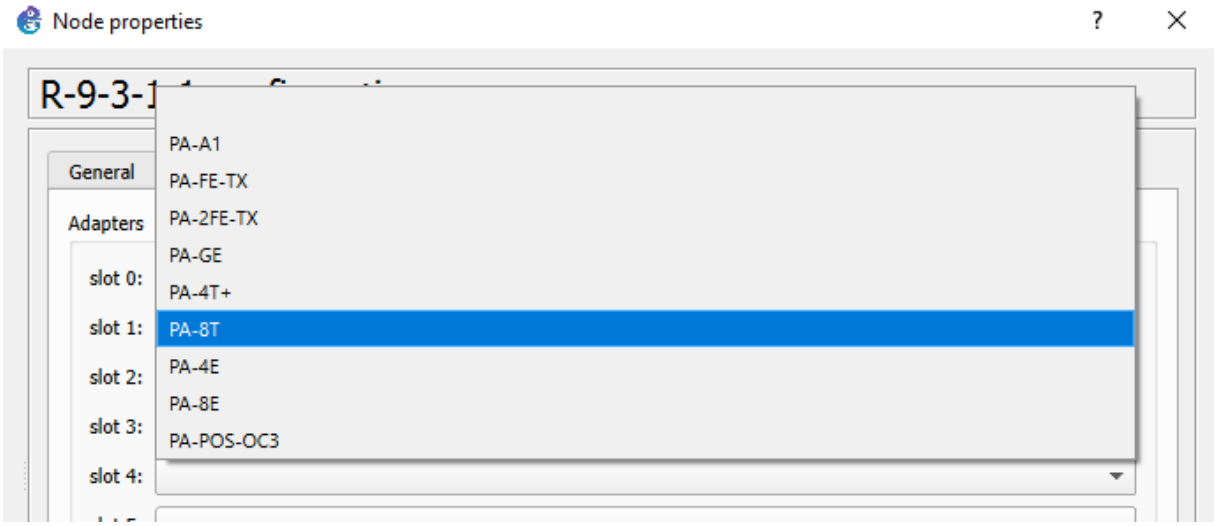
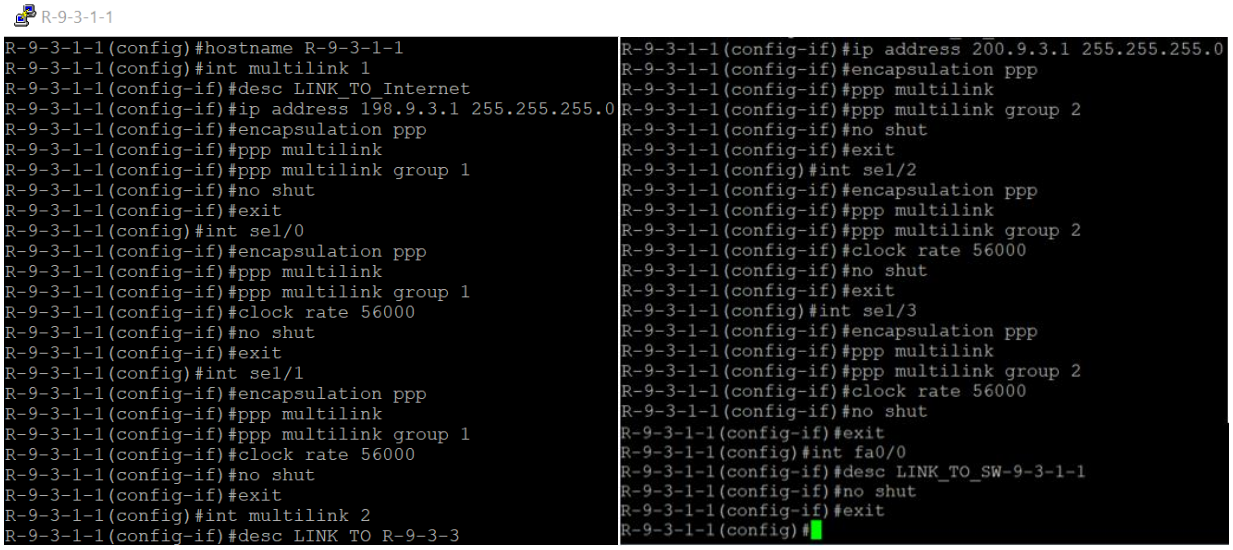


Рис. 3.8 – Додавання Serial портів на машрутизаторі мережі

Після завершення підготовки можемо переходити до безпосереднього налаштування мережі та впровадження системи безпеки.

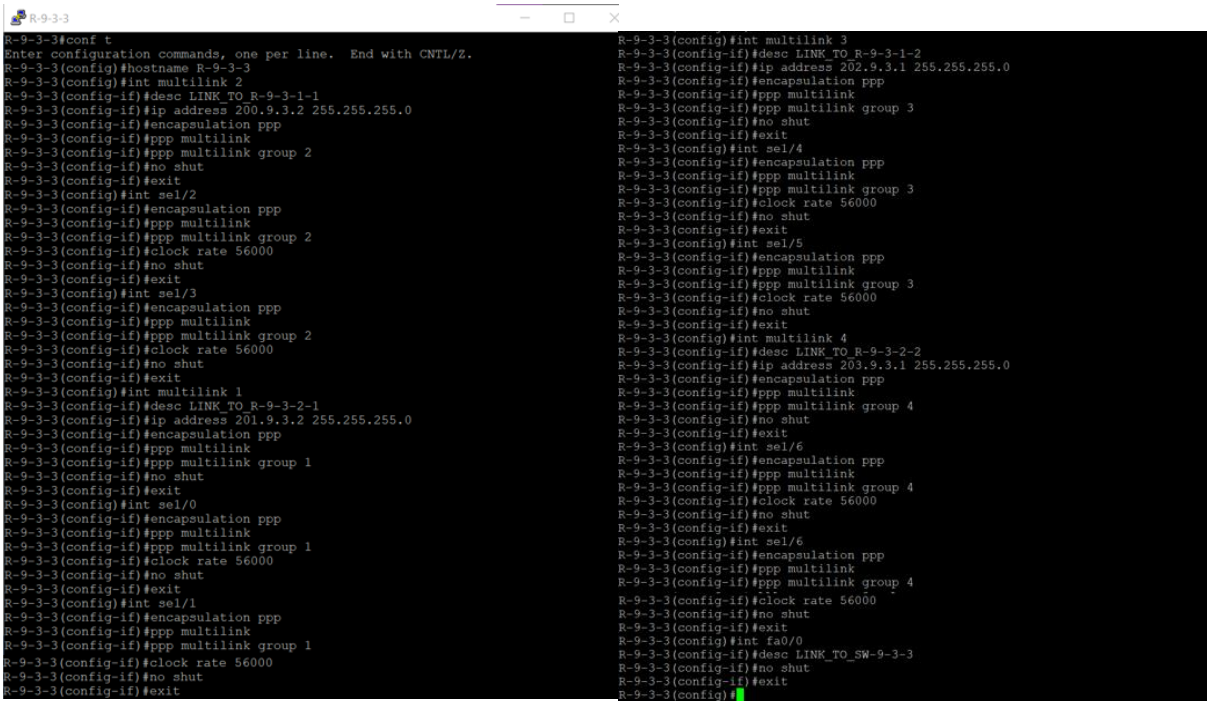
3.2 Налагодження спроєктованої мережі та її захисту

Перед початком налаштування захисту мережі потрібно здійснити базові налагодження. Тому першим кроком проводимо налаштування адресації каналів зв'язку маршрутизаторів типу Multilink [12]. Демонстрація проводиться на прикладі двох маршуртизаторів: R-9-3-1-1(схожий з іншими пристроями, які підключенні до локальних мереж і мають підтримувати декілька VLAN) та центральним маршрутизатором R-9-3-3 (підключений до серверної VLAN).



а) б)

Рис 3.9 – Приклад базового налагодження маршрутизатора R-9-3-1-1



а) б)

Рис 3.10 – Приклад базового налагодження маршрутизатора R-9-3-3

Після базового налагодження маршрутизаторів можна приступати до налагодженя адресації на кожній робочій станції. Приклад показано на декількох комп'ютерах мережі:

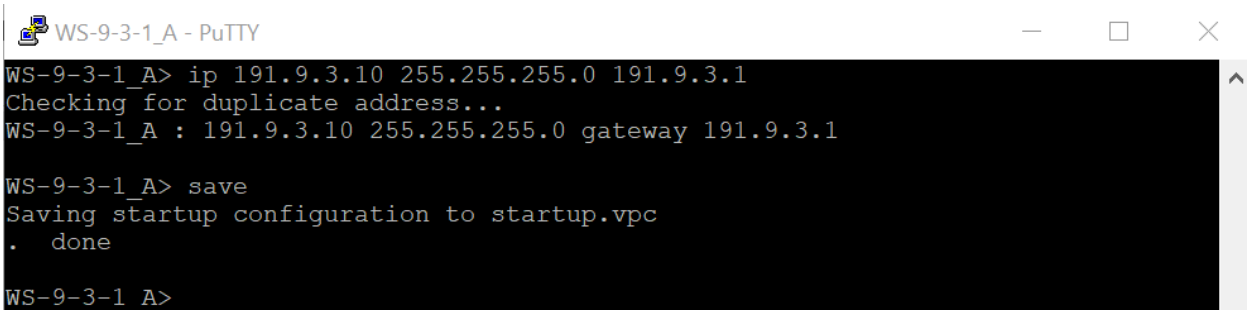


Рис. 3.11 – Приклад налагодження адресації на звичайній робочій станції WS-9-3-1_A



Рис. 3.12 – Приклад налагодження адресації на звичайній робочій станції WS-9-3-2_B

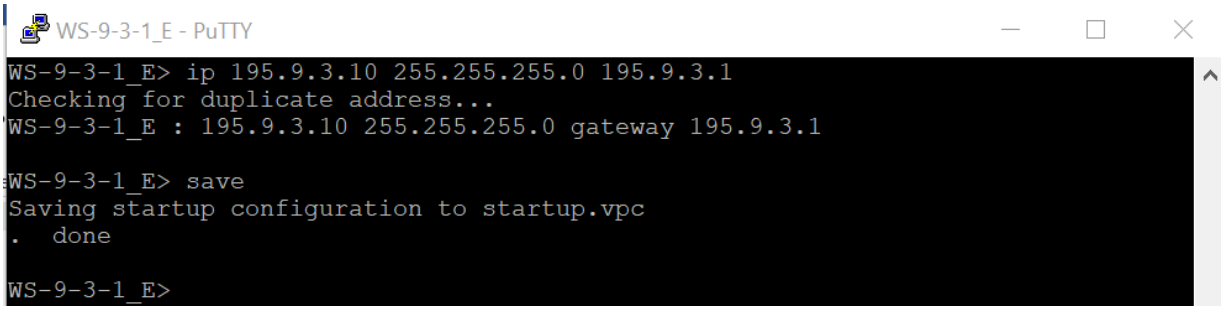


Рис. 3.13 – Приклад налагодження адресації на звичайній робочій станції WS-9-3-1_E

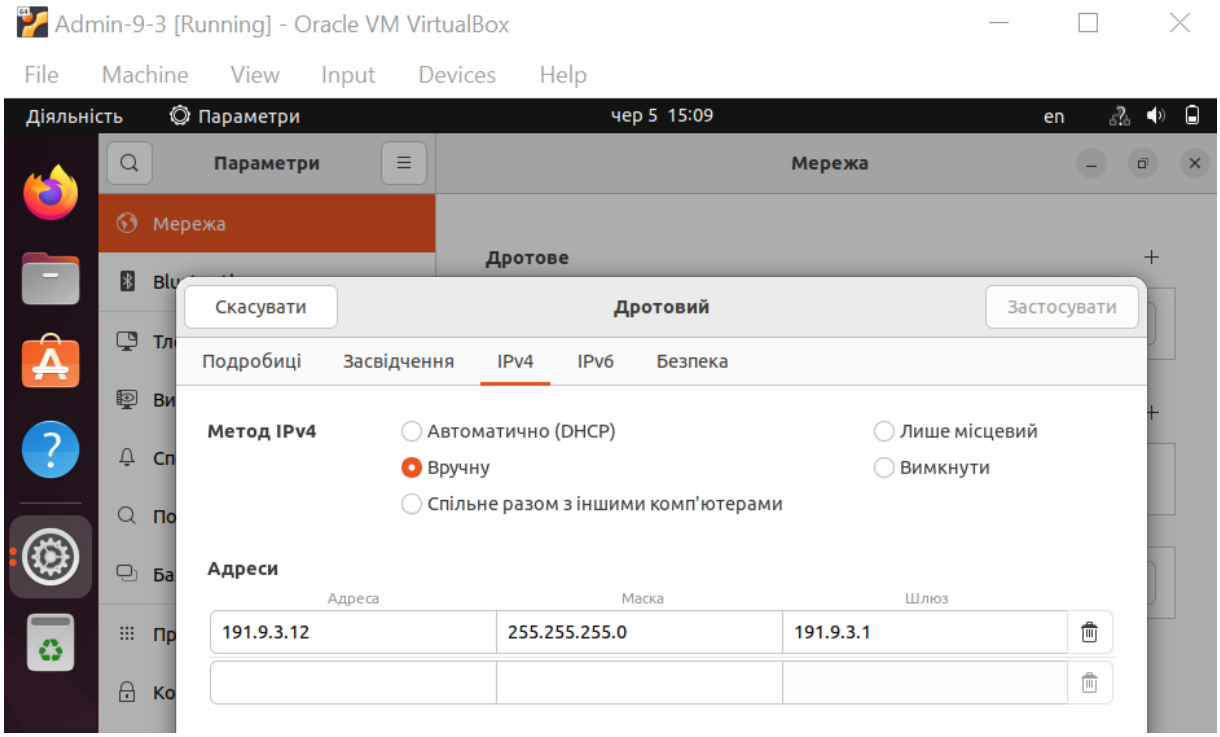


Рис. 3.14 – Приклад налагодження адресації на робочій станції адміністратора Admin-9-3-1

Після того, як всі станції отримали свої статичні адреси, можна приступити до налагодження VLAN на комутаторах мережі. Також разом з VLAN було налагоджено Port Security [13] для усіх інтерфейсів комутатора. Приклад налагодження показано на комутаторах SW-9-3-1-1 та SW-9-3-3:

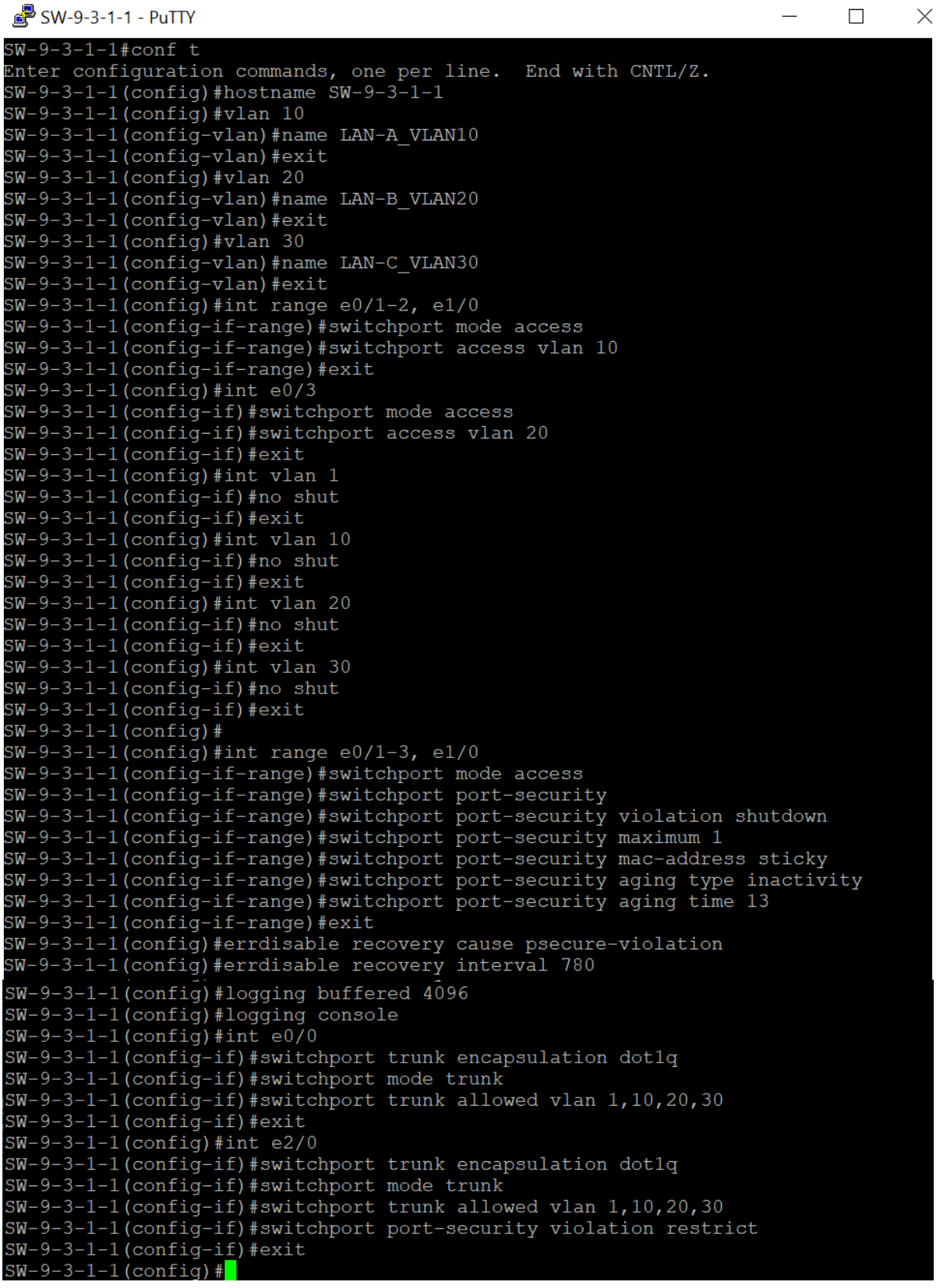


Рис. 3.15 – Приклад налагодження декількох VLAN і Port Security на комутаторі SW-9-3-1-1

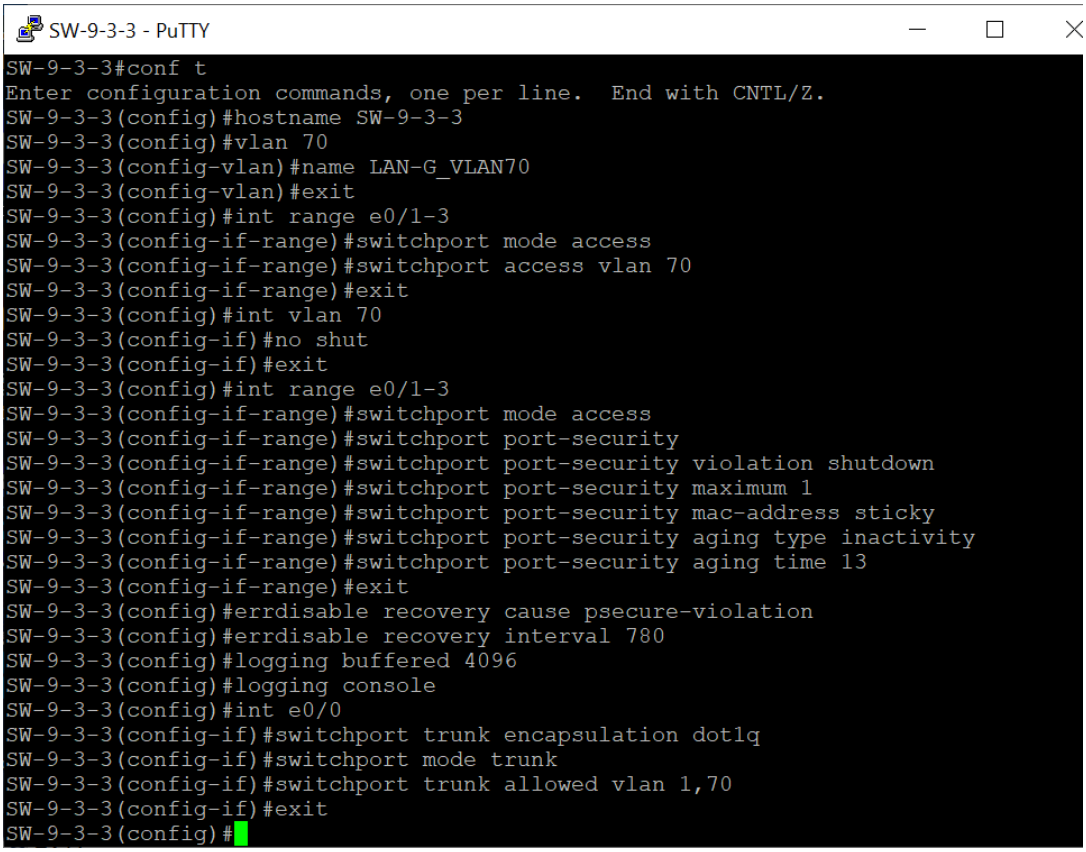


Рис. 3.16 – Приклад налагодження однієї VLAN і Port Security на комутаторі SW-9-3-3

Для того, щоб наші VLAN запрацювали коректно і станції адміністраторів могли мати зв’язок, потрібно налагодити саб-інтерфейси на маршрутизаторах [14]. Налагодження маршрутизаторів R-9-3-1-1 і R-9-3-3 відповідно комутаторам наведено нижче:

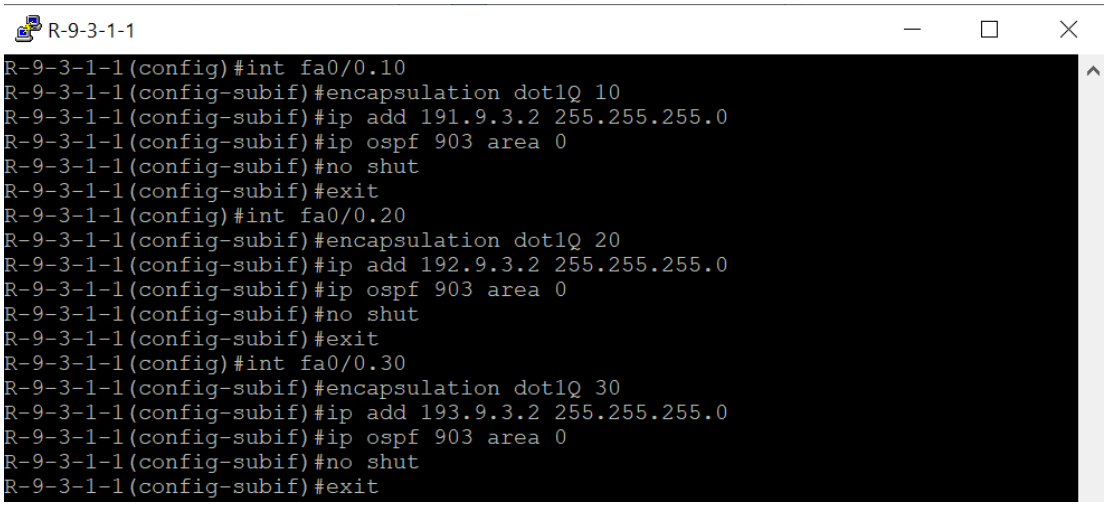


Рис. 3.17 – Приклад налагодження саб-інтерфейсів на маршрутизаторі R-9-3-1-1

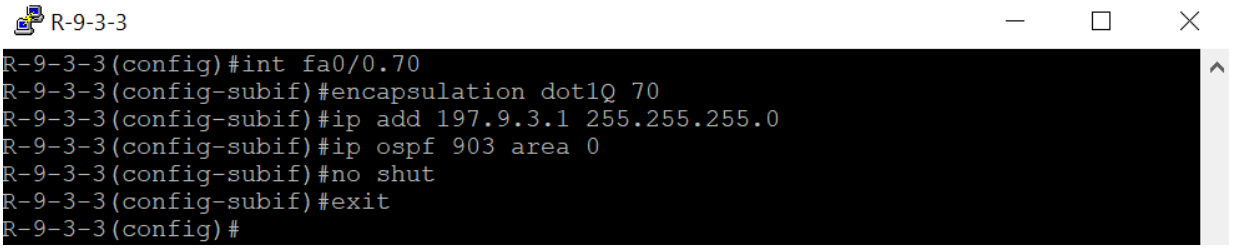


Рис. 3.18 – Приклад налагодження саб-інтерфейсу на маршрутизаторі R-9-3-3

Після проведених налаштувань можна перейти до призначення віртуальних адрес за допомогою протокола резервування шлюзу HSRP. Оскільки цей протокол налагоджений на чотирьох маршрутизаторах, прикладом слугуватиме друга пара, яка знаходиться в правій частині мережі – R-9-3-2-1 і R-9-3-2-2.

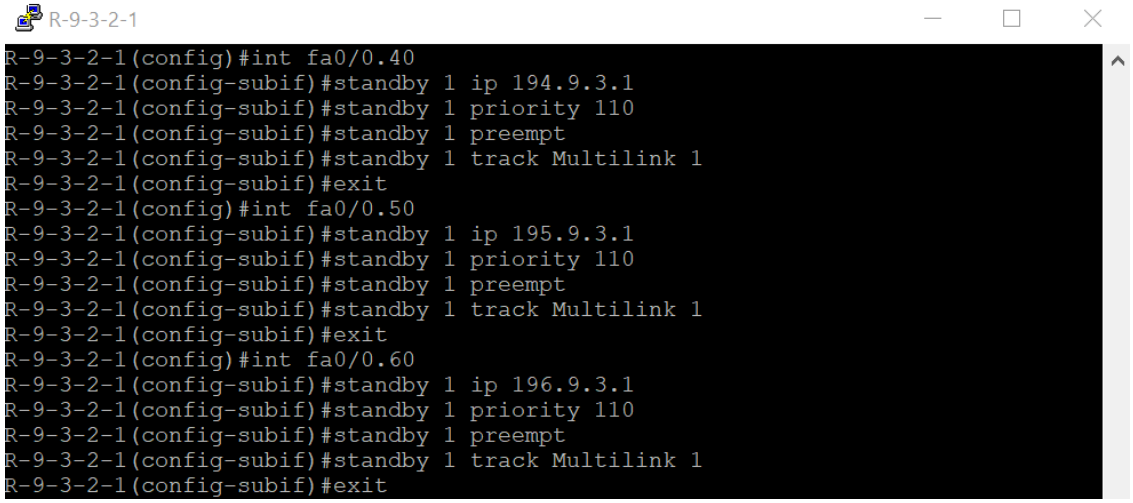


Рис. 3.19 – Приклад налагодження активного маршрутизатора R-9-3-2-1

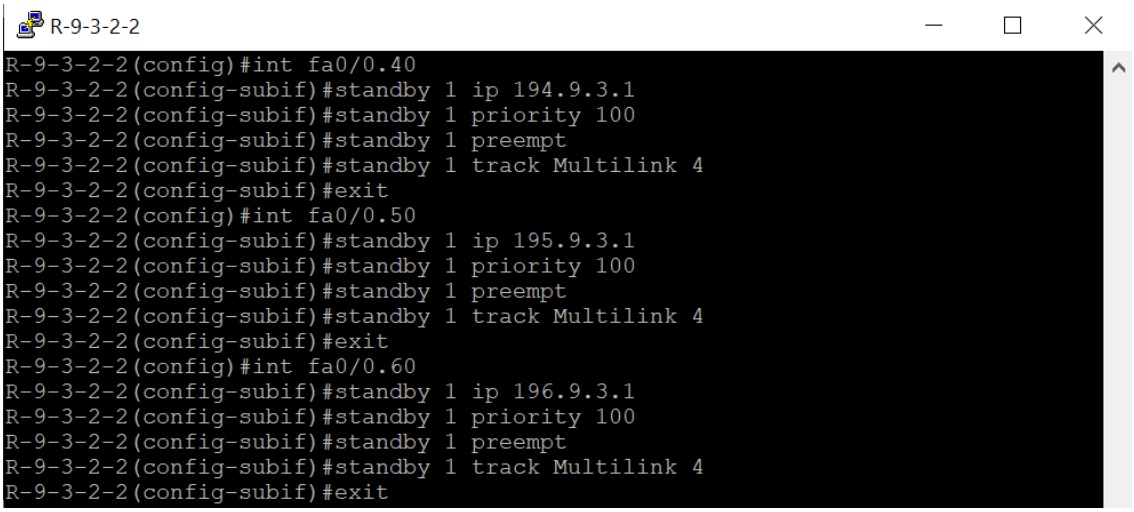


Рис. 3.20 – Приклад налагодження резервного маршрутизатора R-9-3-2-2

Наступним кроком у налагодженні мережі є забезпечення зв'язку між адміністраторами мережі та серверами з усіма робочими станціями. Це здійснено за допомогою протоколу маршрутизації OSPF. Налаштування проводиться на всіх маршрутизаторах мережі, але прикладом слугують R-9-3-1-2 та R-9-3-3:

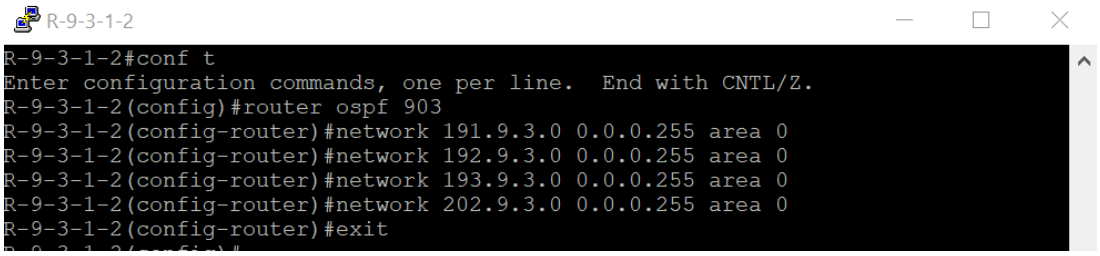


Рис. 3.21 – Приклад налагодження протоколу OSPF на маршрутизаторі R-9-3-1-2

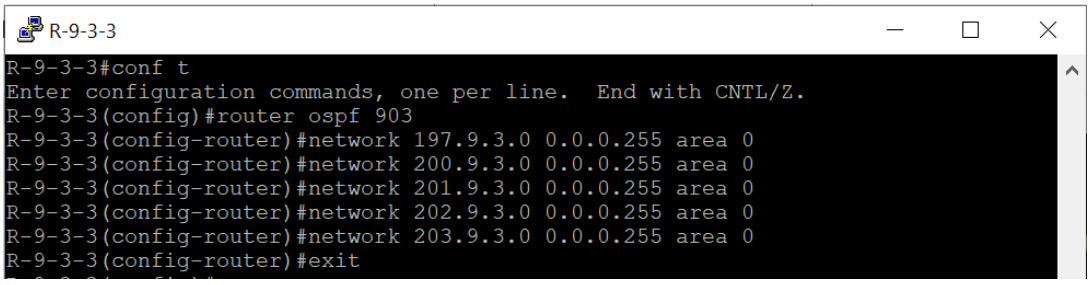


Рис. 3.22 – Приклад налагодження протоколу OSPF на маршрутизаторі R-9-3-3

Після створення усіх VLAN та забезпечення маршрутизації, можемо приступити до налагодження моделі AAA у нашій мережі. Першим кроком потрібно створити користувачів і додати усі пристрої мережі до серверу TACACS+ та налаштувати SSHv2 на кожному маршрутизаторі [15].

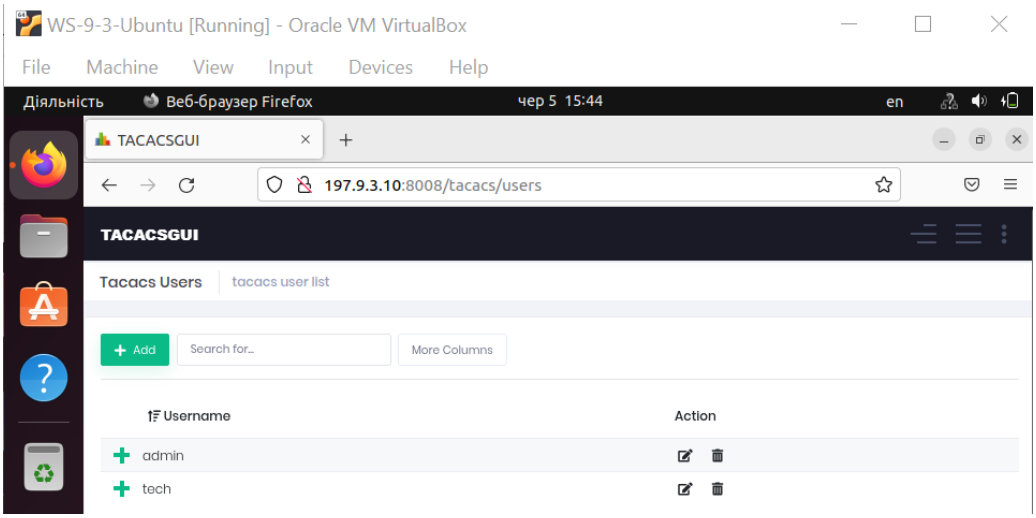


Рис. 3.23 – Усі створені користувачі TACACS+

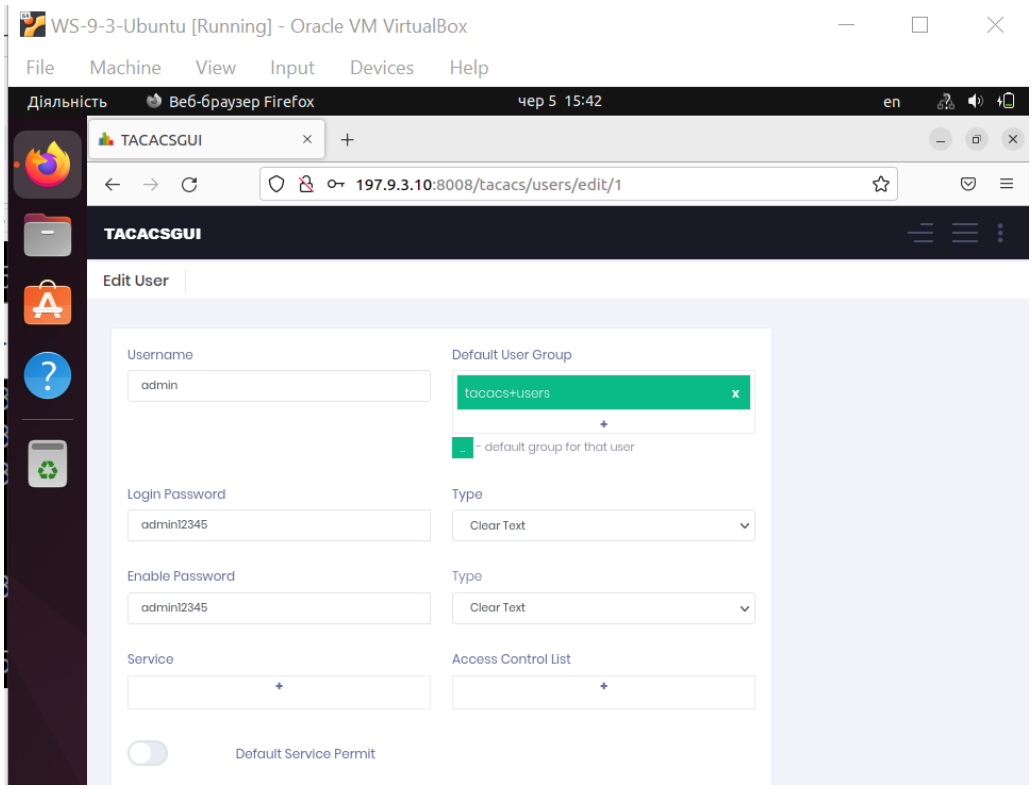


Рис. 3.24 – Приклад створення користувача в TACACSGUI

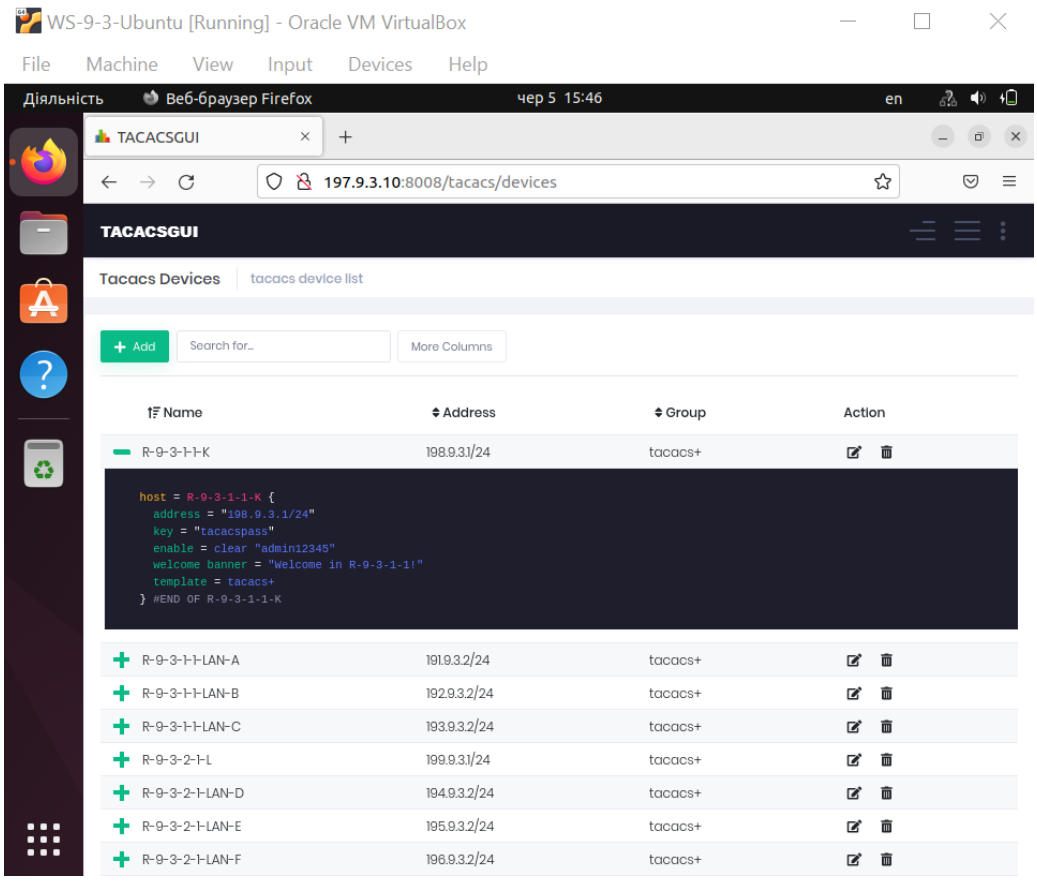


Рис. 3.25 – Усі додані маршрутизатори мережі в TACACSGUI

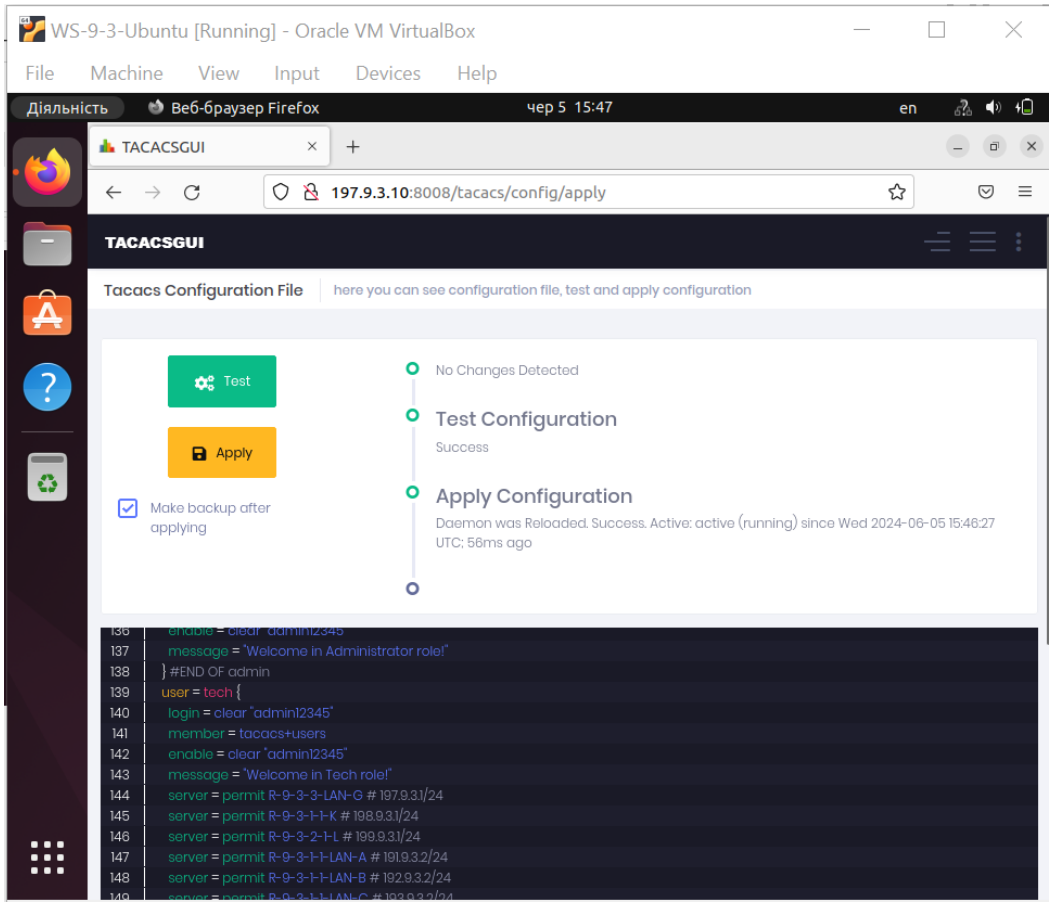


Рис. 3.26 – Тестування та застосування усіх налаштувань TACACS+

Далі проводимо налаштування усіх маршрутизаторів мережі для захисту та змоги підключатися за допомогою віддаленого доступу.

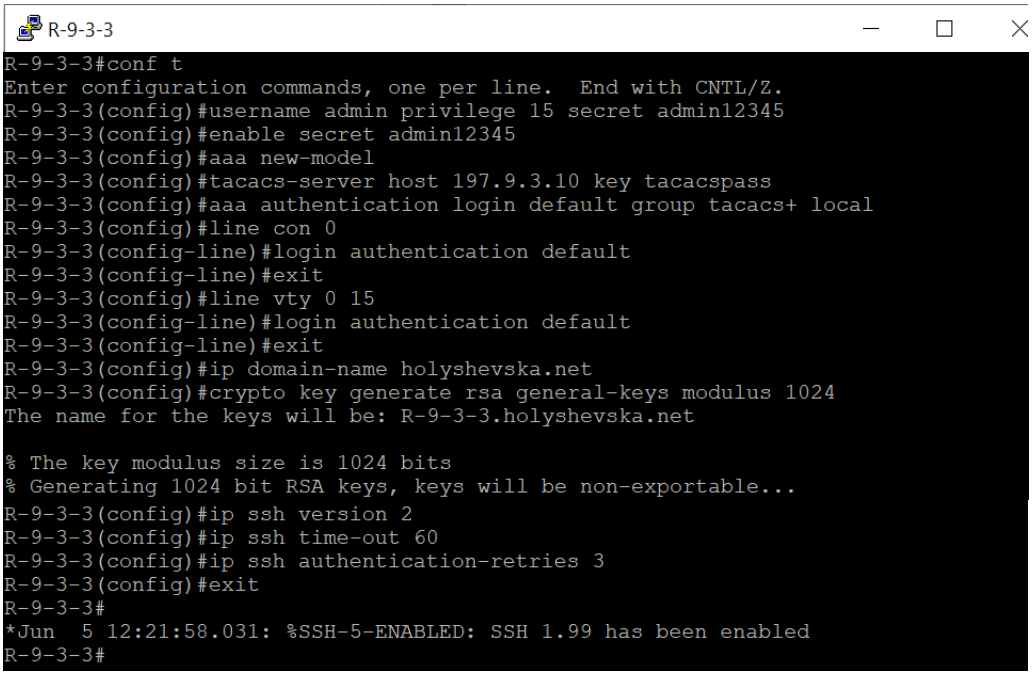


Рис. 3.27 – Приклад налагодження TACACS+ та SSH на маршрутизаторі R-9-3-3

Також проводимо налаштування авторизації та аудиту (здійснюється за допомогою віддаленого підключення під акаунтом адміністратора):

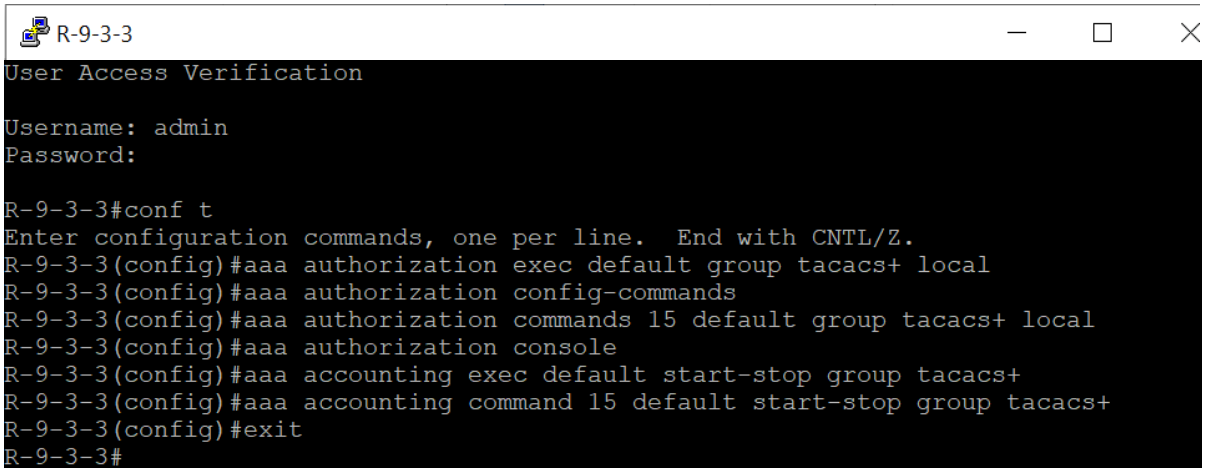


Рис. 3.28 – Налаштування авторизації та аудиту на маршрутизаторі R-9-3-3

Наступним кроком у забезпеченні захисту мережі організації є запровадження списків контролю доступу. На всіх маршрутизаторах мережі було налагоджено фільтрацію трафіку так, щоб тільки адміністративні VLAN мали зв’язок між собою. Тим самим ACL мають забороняти надходження будь-якого трафіку у локальні мережі. Також було налаштовано списки доступу для віддаленого підключення [16]. Це означає, що маршрутизатори будуть забороняти усі підключення зі станцій, які не вказані як дозволені в правилах фільтрації.

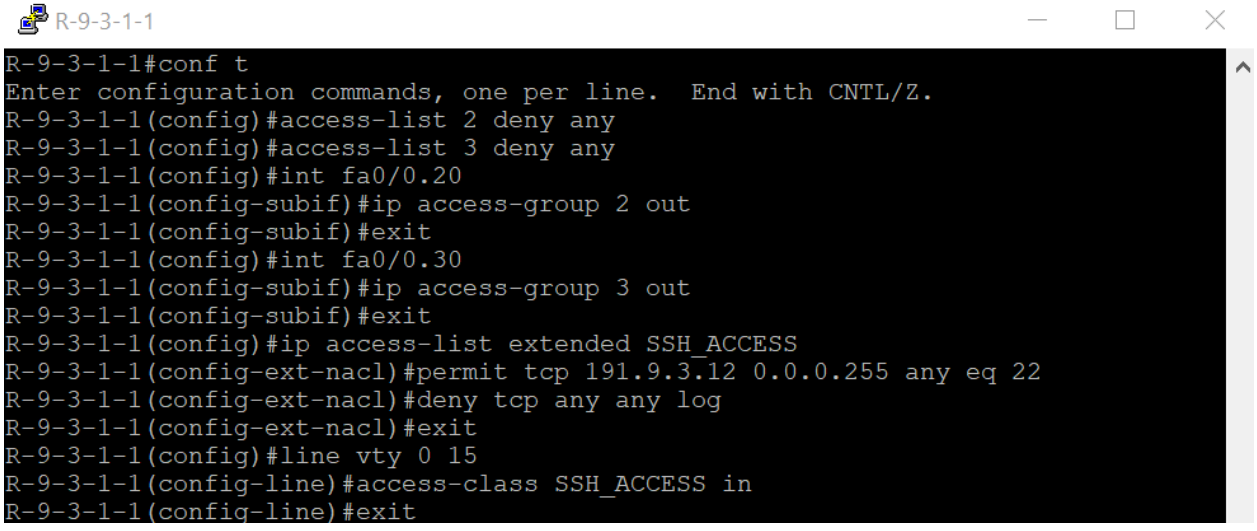


Рис. 3.29 – Приклад налаштування ACL на маршрутизаторі R-9-3-1-1

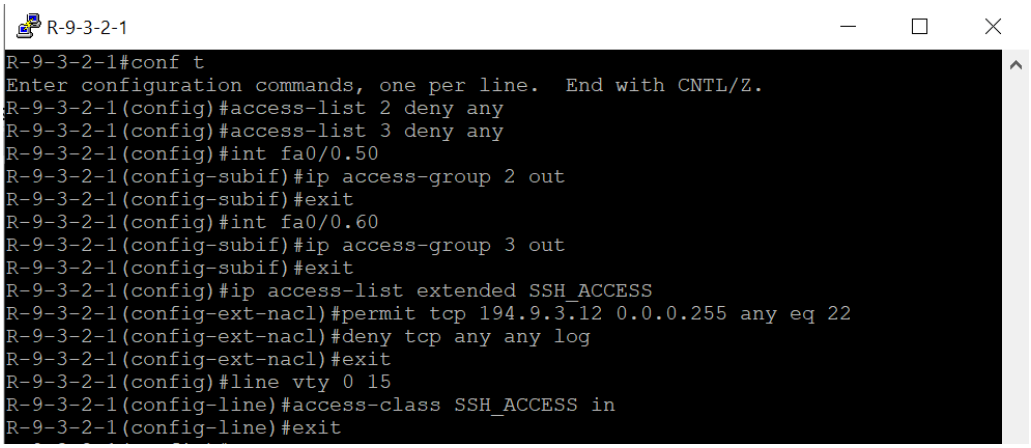


Рис. 3.30 – Приклад налаштування ACL на маршрутизаторі R-9-3-2-1

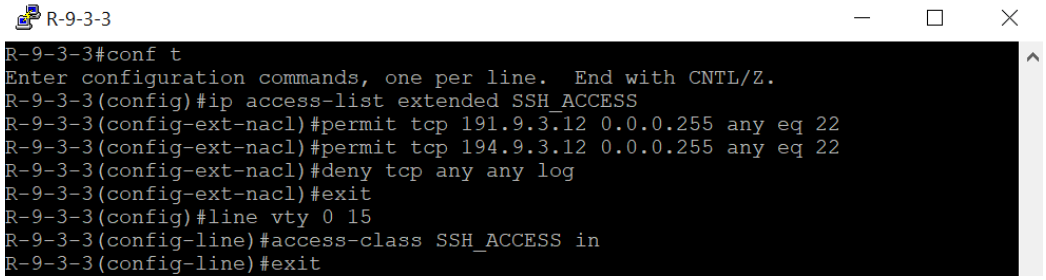


Рис. 3.31 – Приклад налаштування ACL на маршрутизаторі R-9-3-3

Останнім етапом у забезпеченні надійної мережі є налагодження IPsec Site-to-Site VPN. Налагодження тунелю VPN здійснено на парі пристроїв R-9-3-1-1 та R-9-3-2-1. Налагодження маршрутизатора R-9-3-1-1:

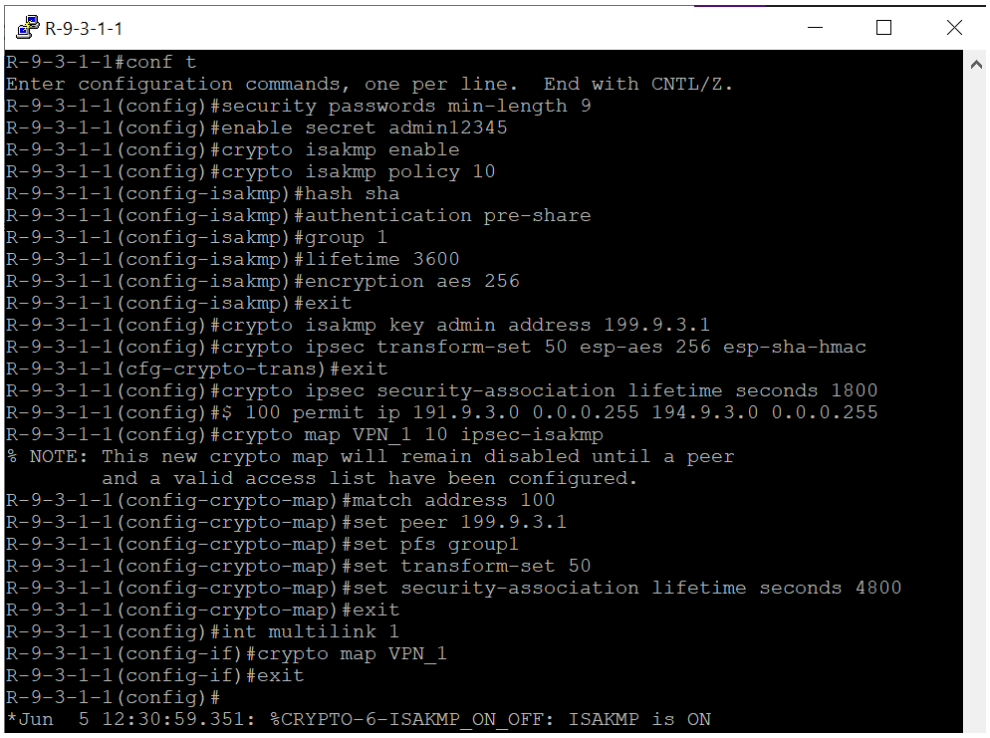


Рис. 3.32 – Налагодження IPsec Site-to-Site VPN на маршрутизаторі R-9-3-1-

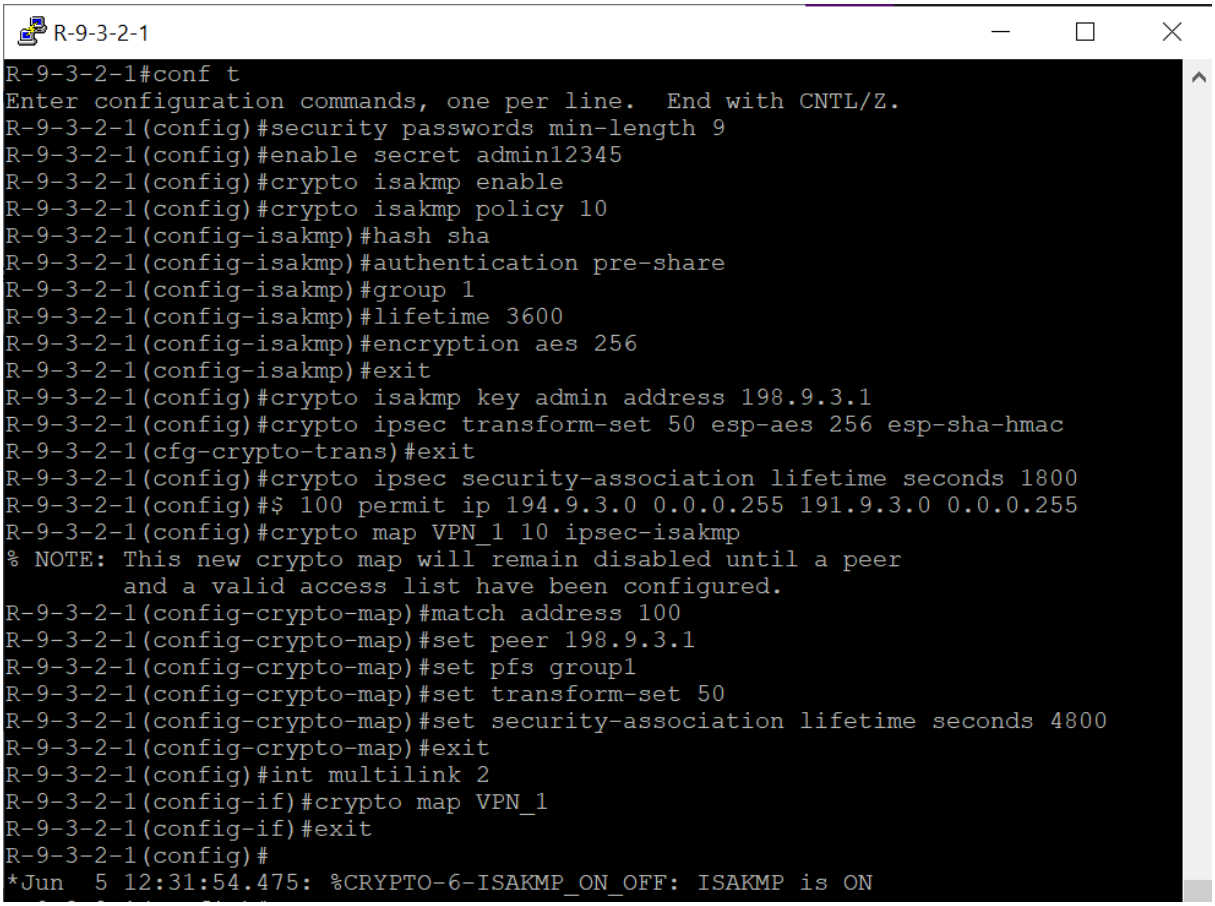


Рис. 3.33 – Налагодження IPsec Site-to-Site VPN на маршрутизаторі R-9-3-2-1

Налагодження Syslog-сервера для відображення журналювання подій у мережі:

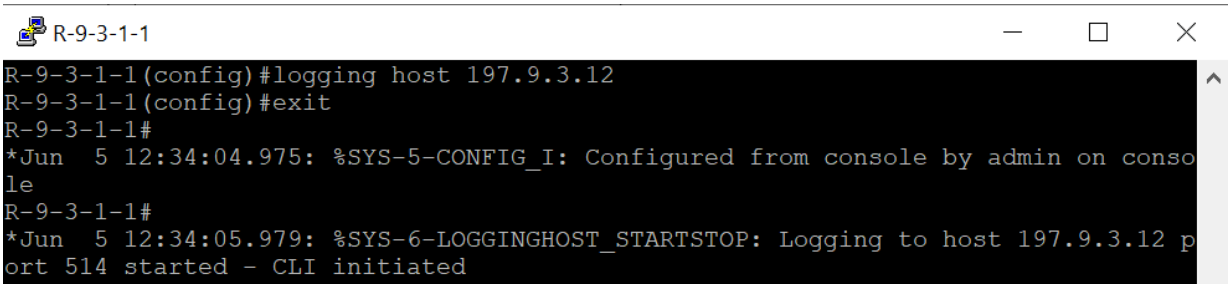


Рис. 3.34 – Налагодження Syslog-сервера на маршрутизаторі R-9-3-1-1

Усі інші пристрої маршрутизації в мережі були налагоджені аналогічно маршрутизатору R-9-3-1-1 (рис. 3.34).

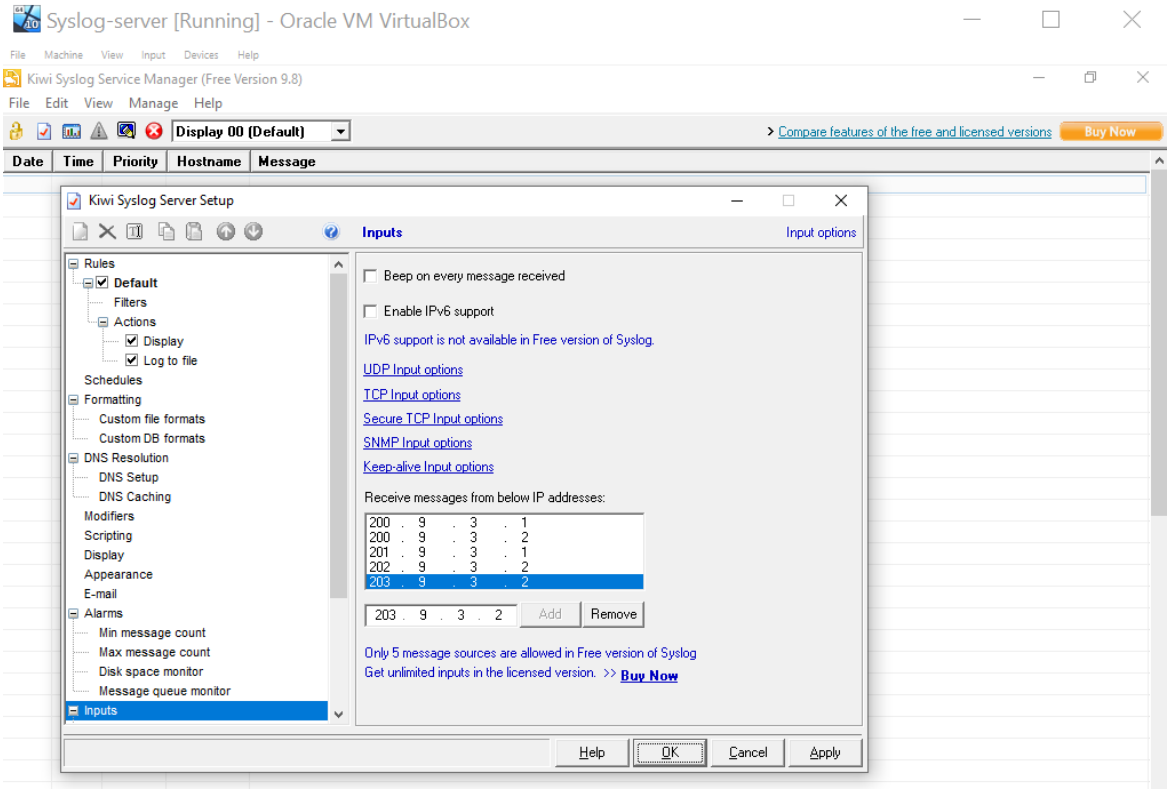


Рис. 3.35 – Додавання адрес маршрутизаторів до Syslog-сервера

3.3 Тестування роботи побудованої мережі організації на базі обладнання Cisco

Після усіх налагоджень мережі потрібно перевірити її працездатність та надійність. Першим кроком перевіряємо наявність зв'язку між робочими станціями мережі:

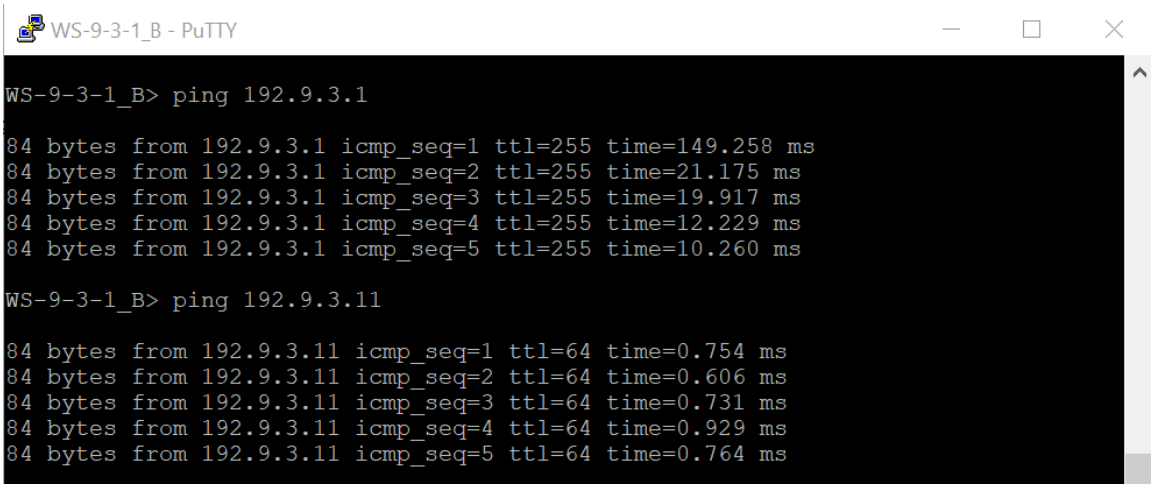


Рис. 3.36 – Успішна перевірка зв'язку між робочими станціями у VLAN 20 за допомогою команди ping

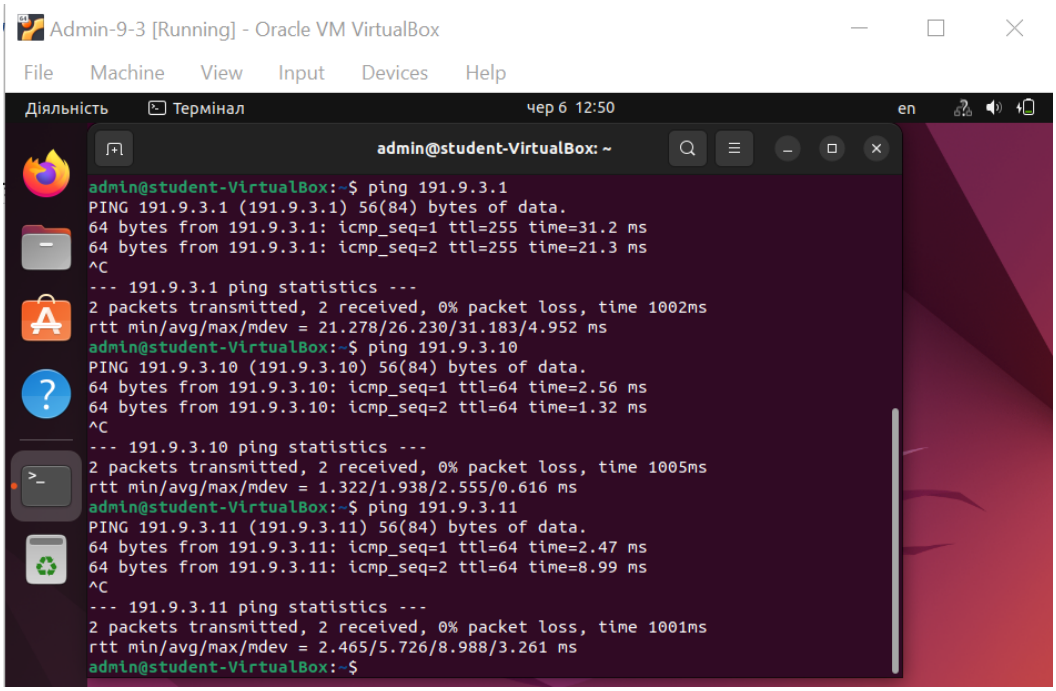


Рис. 3.37 – Успішна перевірка зв’язку між робочими станціями у VLAN 10 за допомогою команди ping

Бачимо, що все успішно працює. А тепер спробуємо перевірити правильність налагодження списків доступу. Зв’язок має бути наявний тільки між підмережами A та D. Інші станції мають пінгуватися тільки в межах своєї VLAN.

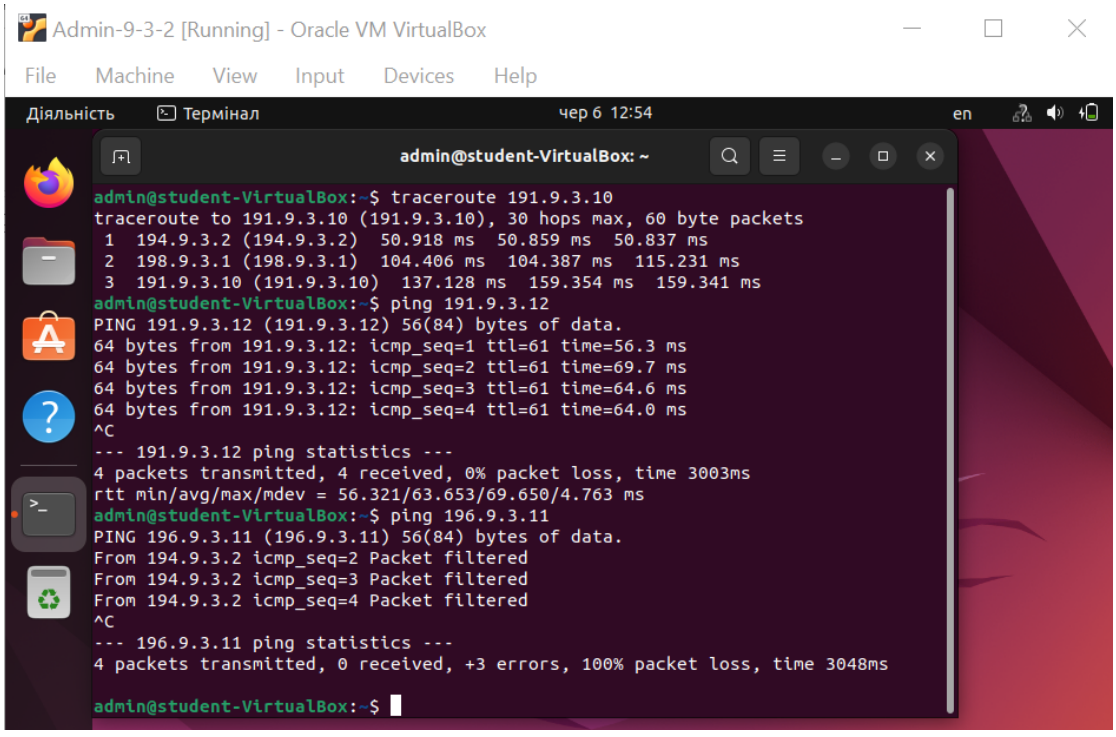


Рис. 3.38 – Успішна перевірка роботи стандартних списків доступу

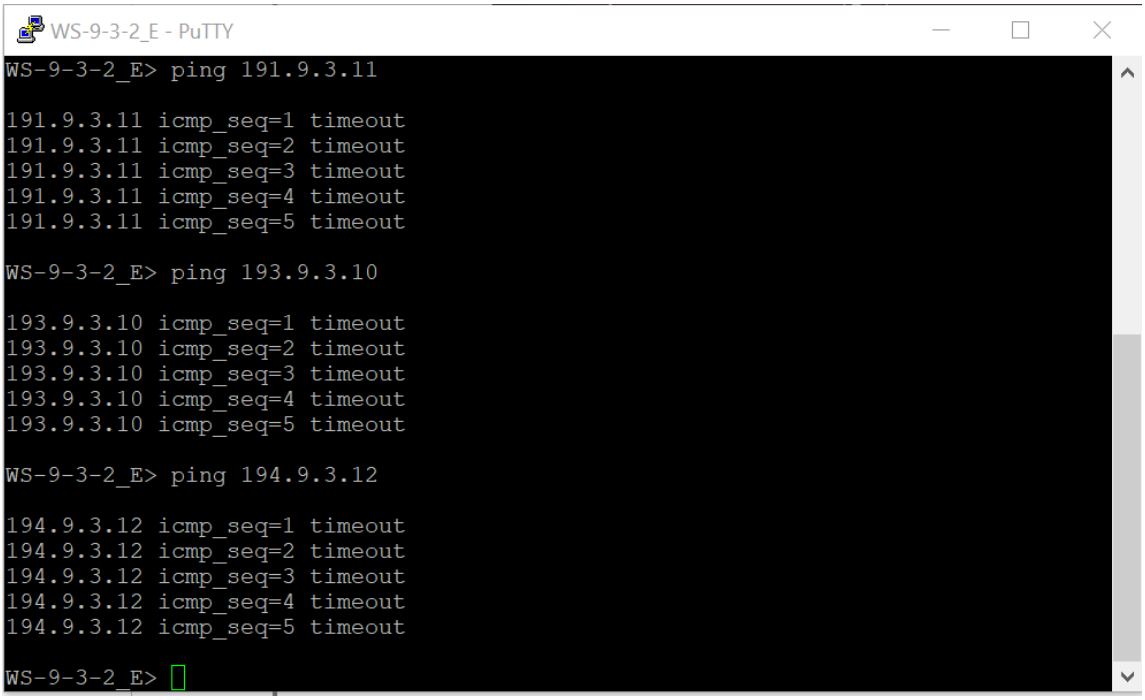


Рис. 3.39 – Успішна перевірка роботи стандартних списків доступу

Після перевірки зв'язку та ACL можемо побачити, що мережа повністю функціонує. Також спробуємо перевірити роботу TACACS+ сервера та протоколу SSH:

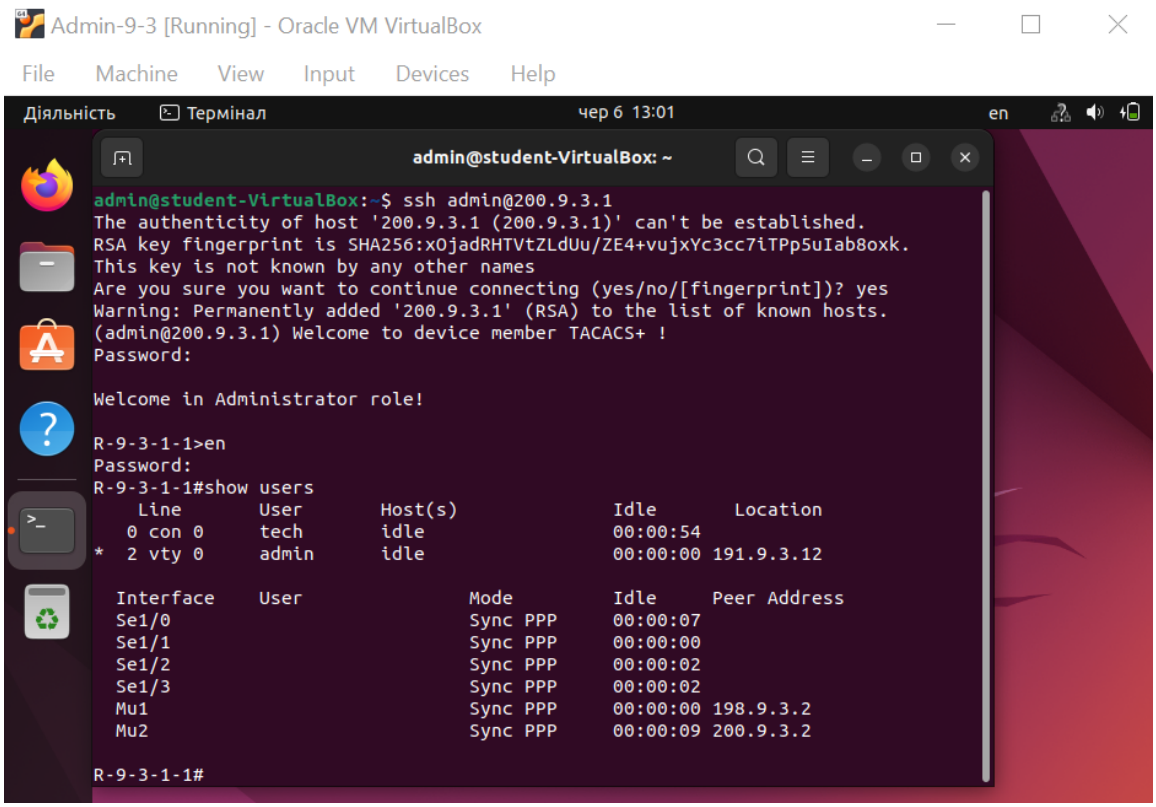


Рис. 3.40 – Успішне віддалене підключення до маршрутизатора R-9-3-1-1 за допомогою створеного користувача Admin на TACACS+ сервері

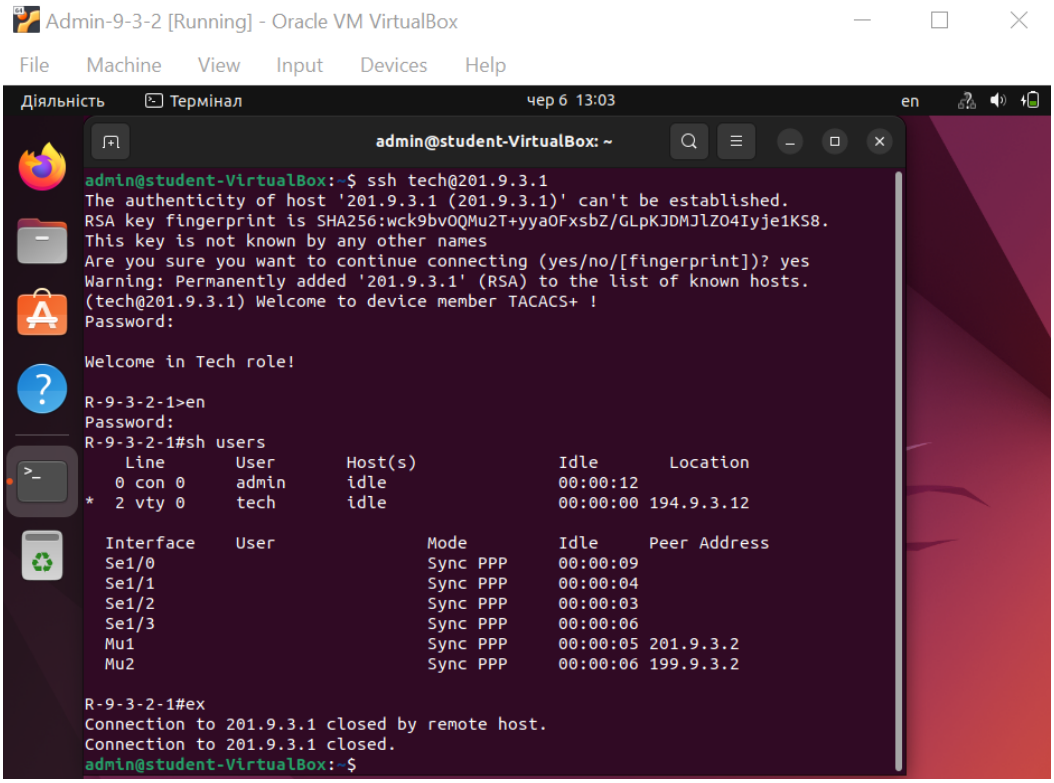


Рис. 3.41 – Успішне віддалене підключення до маршрутизатора R-9-3-2-1 за допомогою створеного користувача Tech на TACACS+ сервері

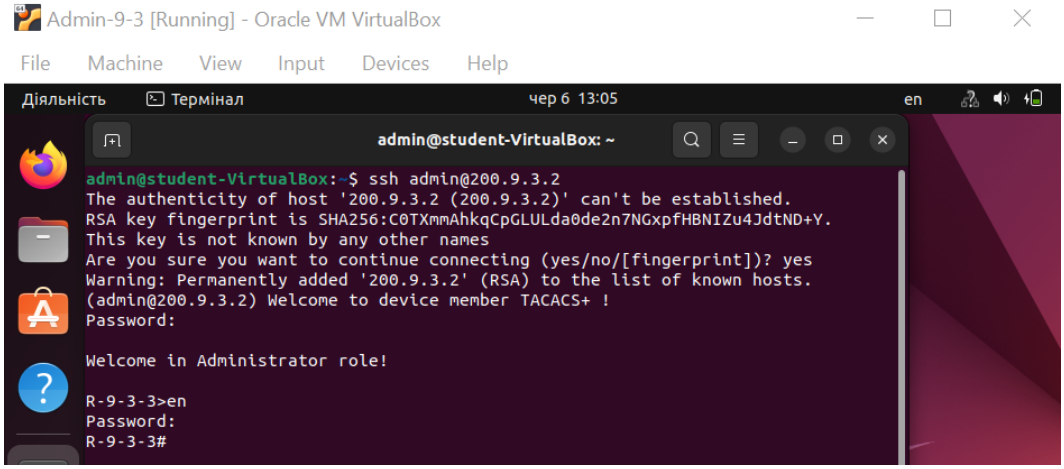


Рис. 3.42 – Успішне віддалене підключення до маршрутизатора R-9-3-3 за допомогою створеного користувача Admin на TACACS+ сервері

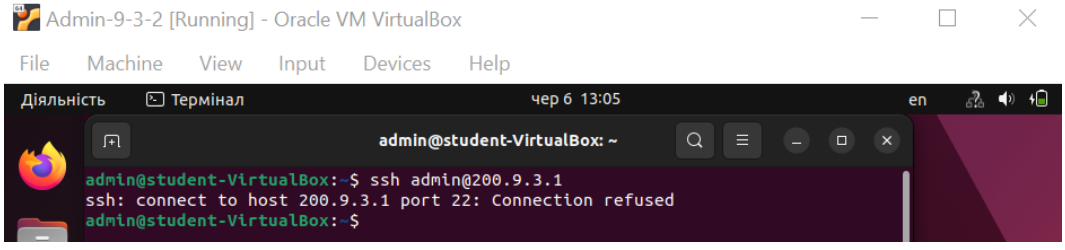


Рис. 3.43 – Перевірка віддаленого підключення до маршрутизатора R-9-3-1-1 при використанні списків контролю доступу

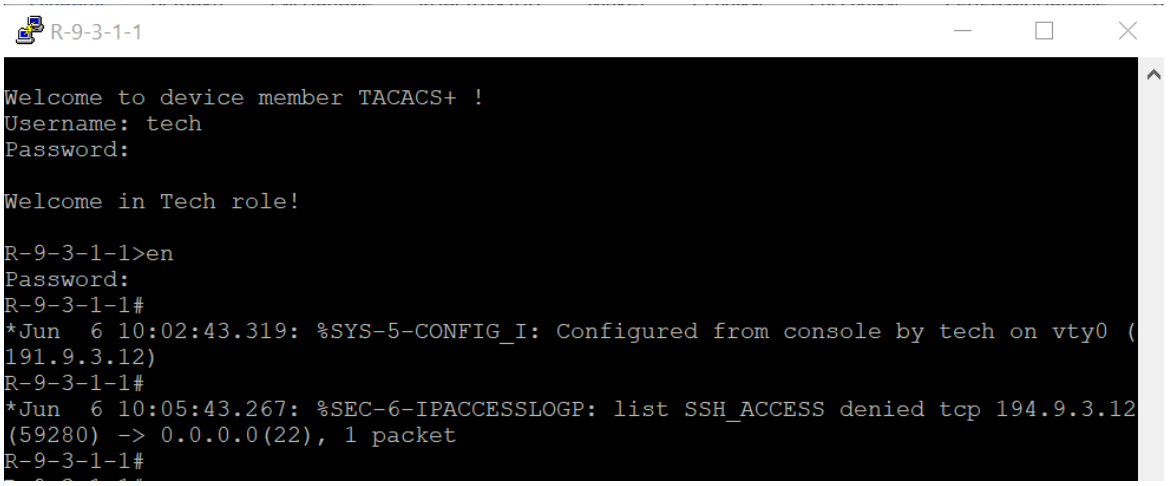


Рис. 3.44 – Інформаційне повідомлення на маршрутизаторі R-9-3-1-1 при підключенні забороненого хоста

Після усіх спроб віддаленого підключення до маршрутизаторів мережі, можемо перейти в TACACSGUI та переглянути всю необхідну інформацію.

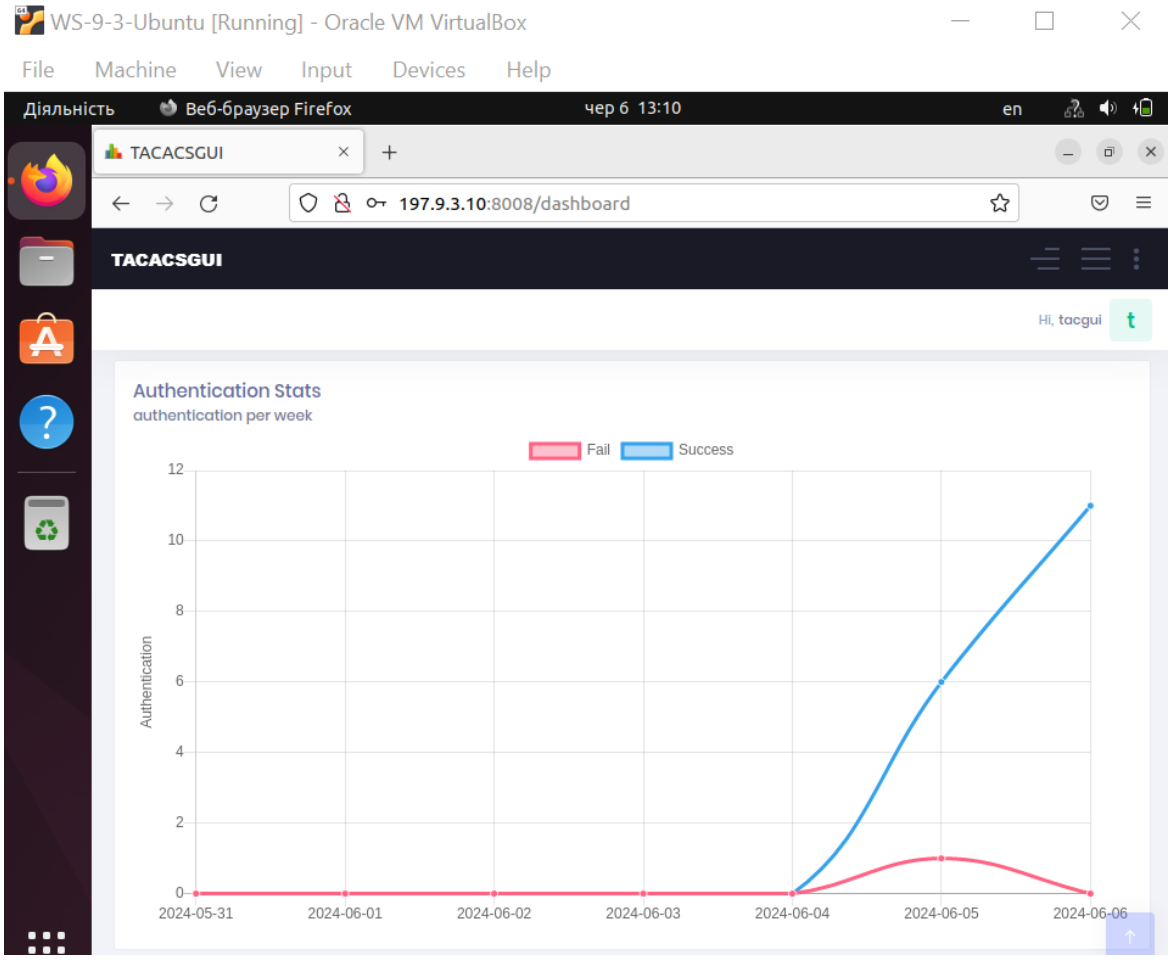


Рис. 3.45 – Перегляд статистики автентифікації у TACACSGUI

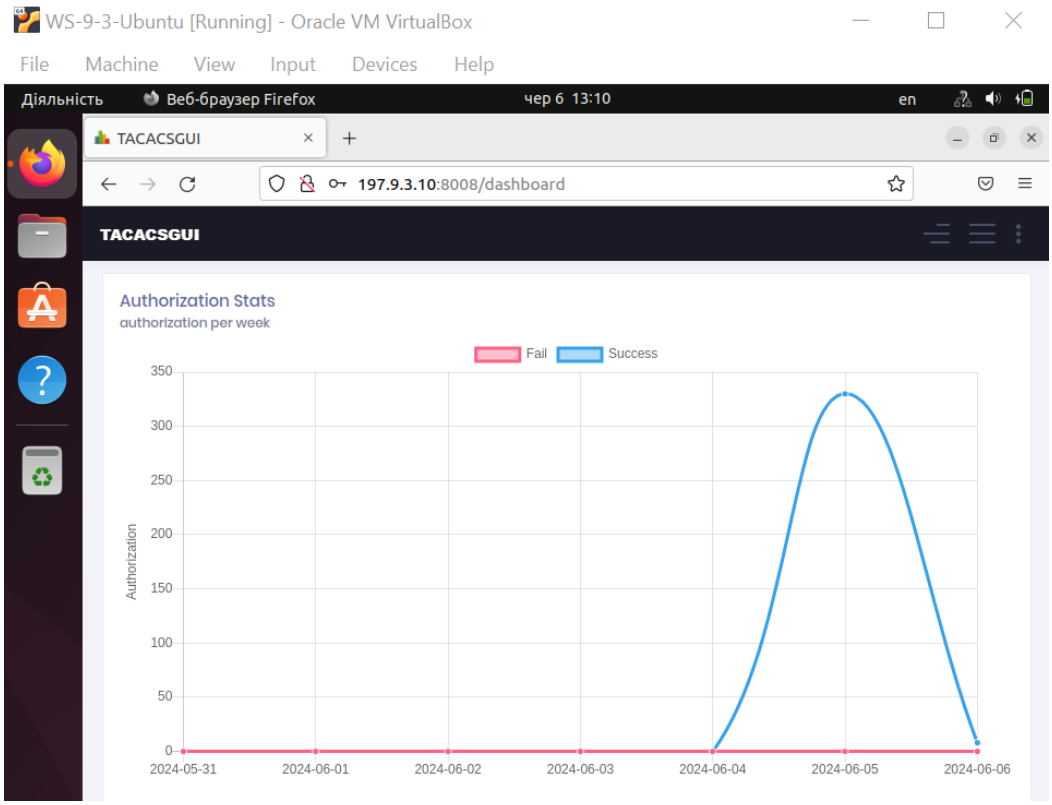


Рис. 3.46 – Перегляд статистики авторизації у TACACSGUI

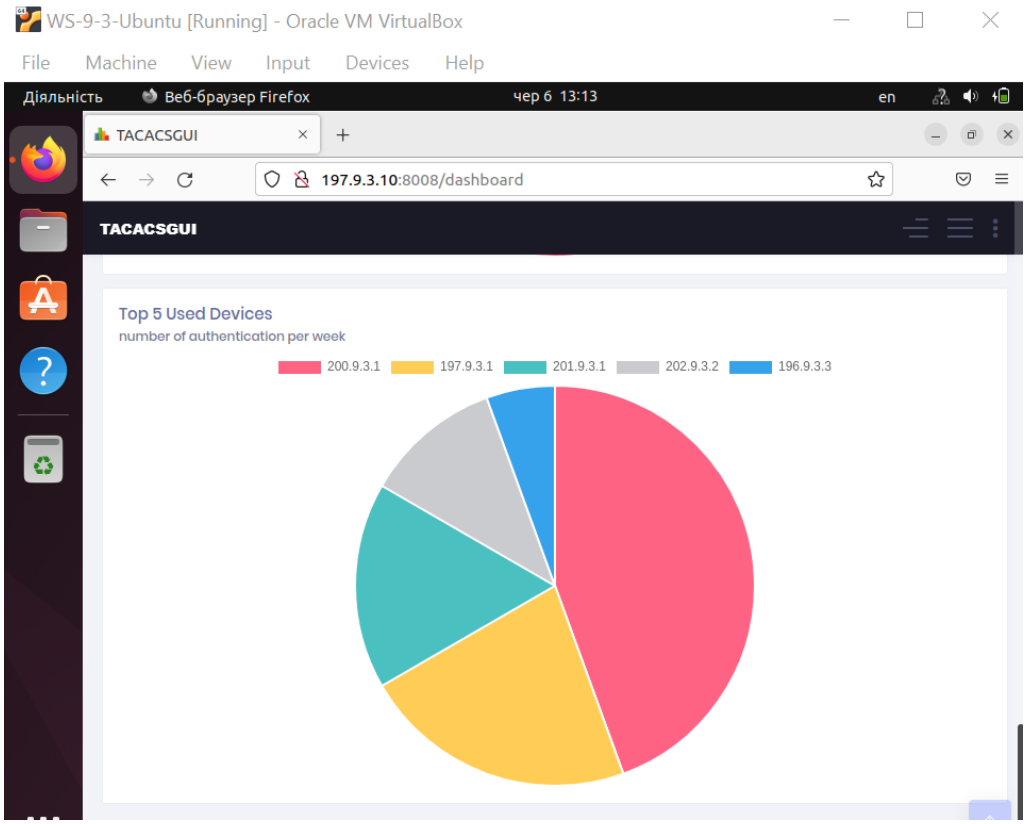


Рис. 3.47 – Діаграма пристроїв, з яких частіше проводиться вхід під створеними користувачами

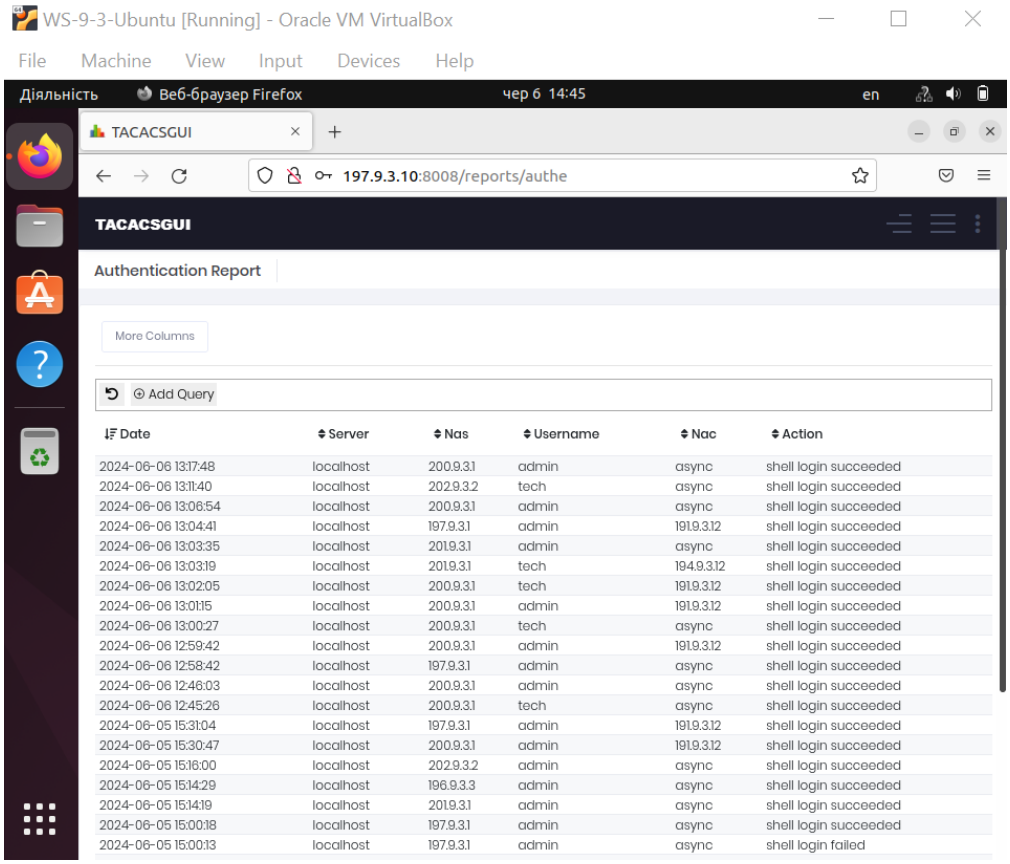


Рис. 3.48 – Перегляд звіту автентифікації у TACACSGUI

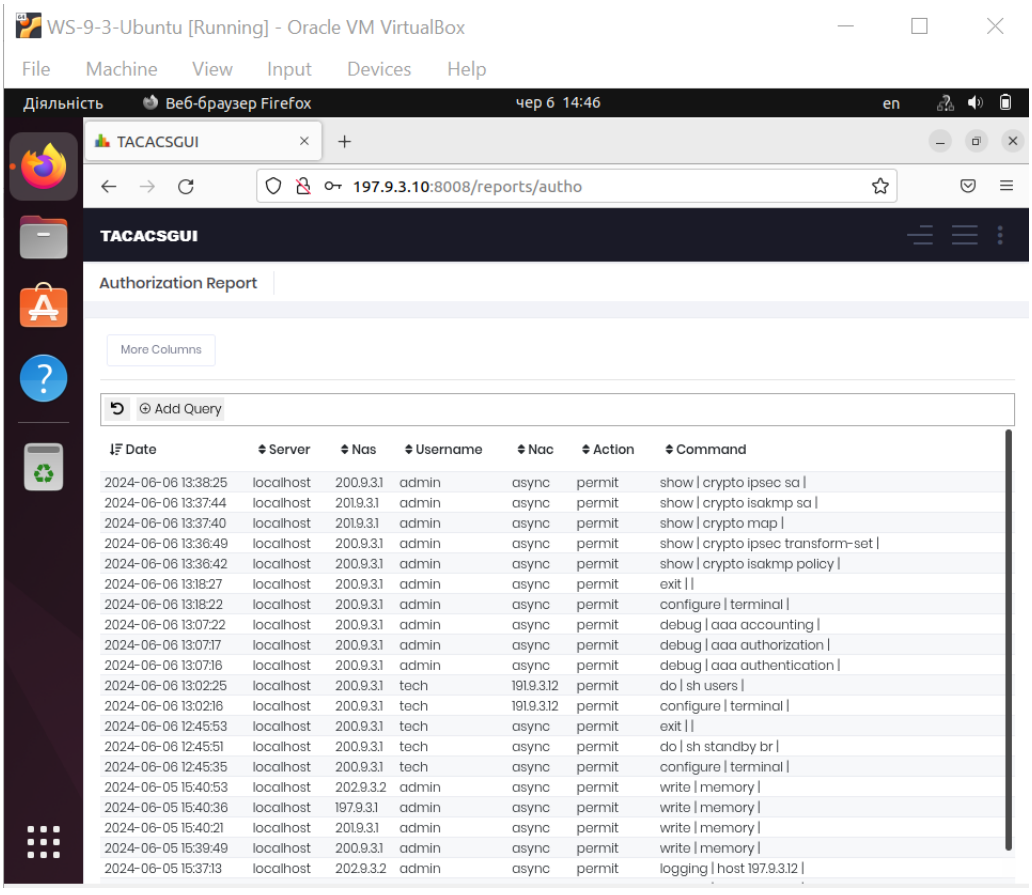


Рис. 3.49 – Перегляд звіту авторизації у TACACSGUI

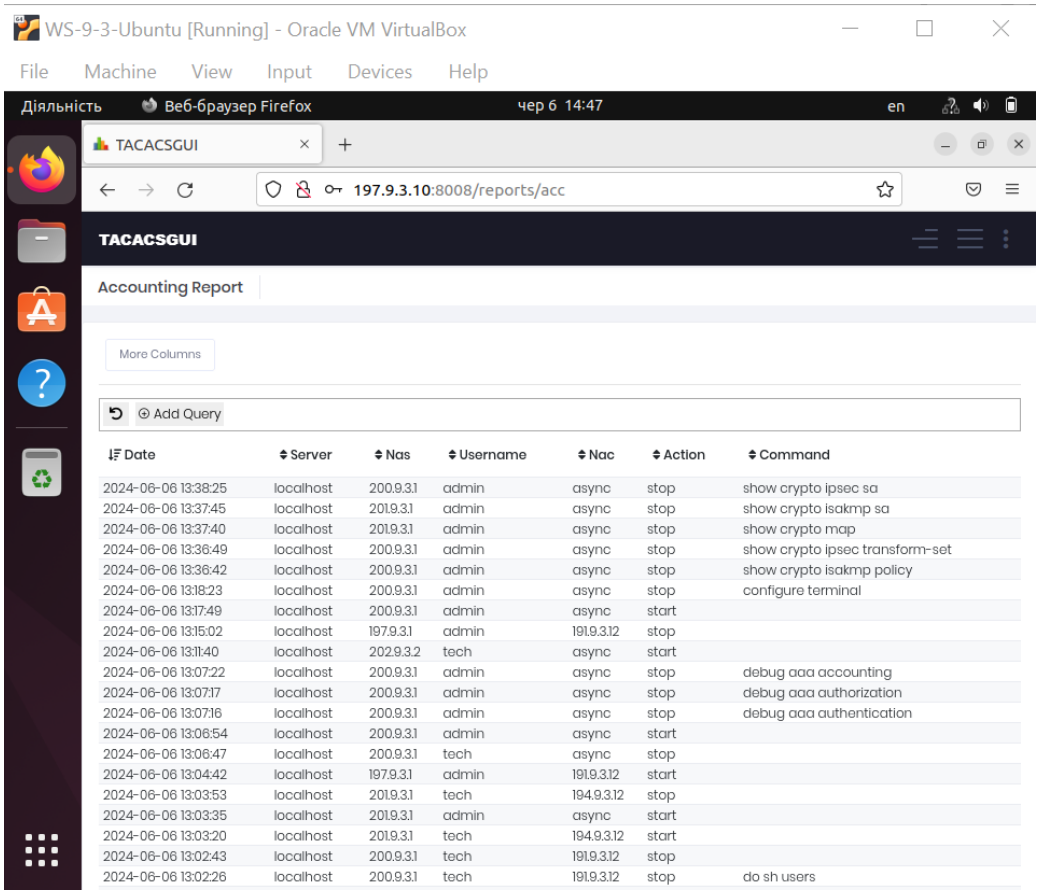


Рис. 3.50 – Перегляд звіту обліку у TACACSGUI

На рисунках 3.45 – 3.50 можемо побачити, що вся інформація щодо віддалених підключень передається і зберігається у TACACSGUI. Це означає, що модель AAA разом із протоколами TACACS+ та SSH були налагоджені вірно.

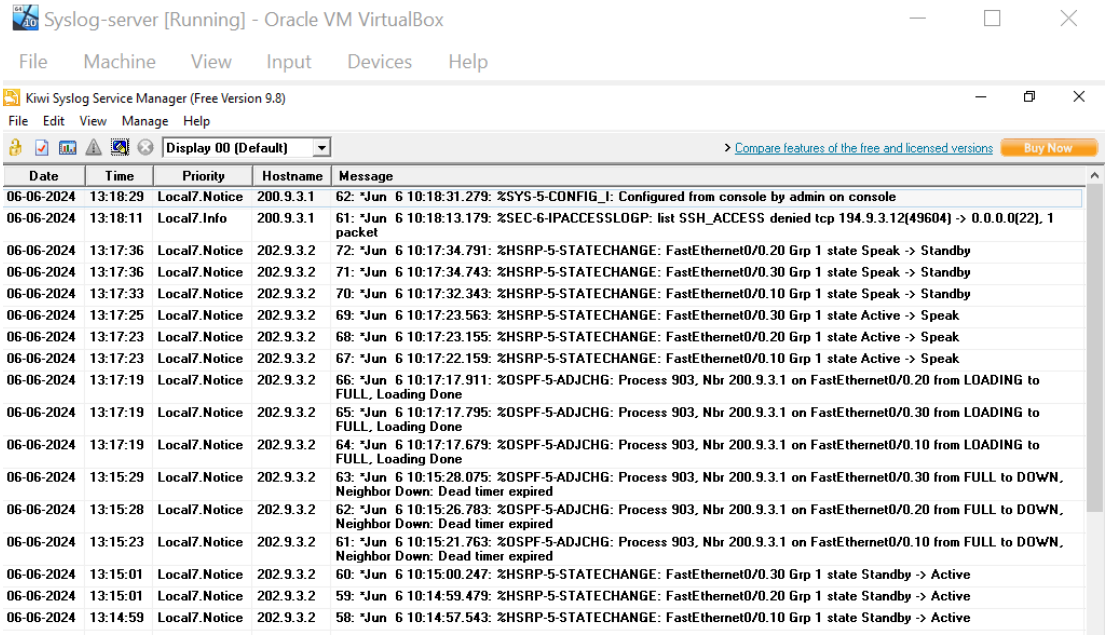


Рис. 3.51 – Успішна перевірка роботи Syslog-сервер

На рисунку 3.51 бачимо, що Syslog-сервер отримує всі повідомлення від маршрутизаторів та зберігає їх у журналі системних подій.

Також потрібно протестувати протокол HSRP на маршрутизаторах. Для цього виведемо з ладу (в нашому випадку просто вимкнемо) активний маршутизатор R-9-3-1-1 та переглянемо інформаційні повідомлення на резервному маршрутизаторі R-9-3-1-2:

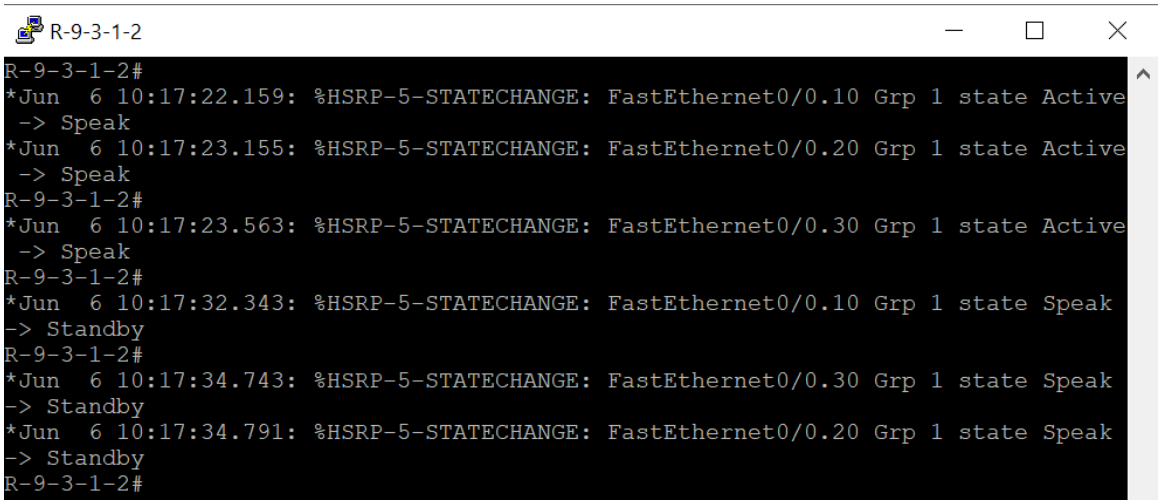


Рис. 3.52 – Повідомлення на резервному маршрутизаторі R-9-3-1-2 при відмові та після відновлення роботи основного маршрутизатора R-9-3-1-1

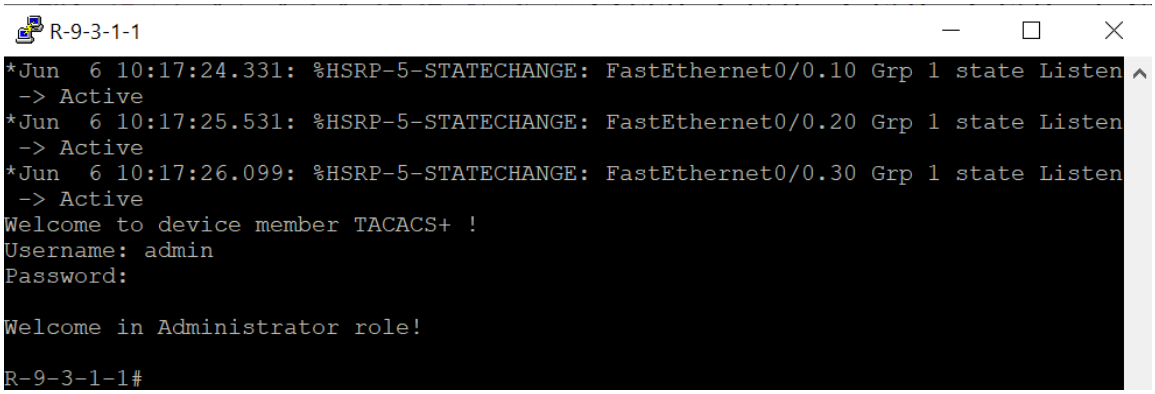


Рис. 3.53 – Повідомлення про активний стан на основному маршрутизаторі R-9-3-1-1 після відновлення його роботи

Оскільки на всіх комутаторах було налагоджено протокол Port Security, його також потрібно перевірити в дії. Для цього в мережу був доданий комп’ютер під назвою Hacker та налаштований як один із комп’ютерів мережі. Йому було присвоєно IP-адресу із діапазону адрес VLAN 50 та підключено до одного з портів комутатора SW-9-3-2-2 замість робочої станції мережі.

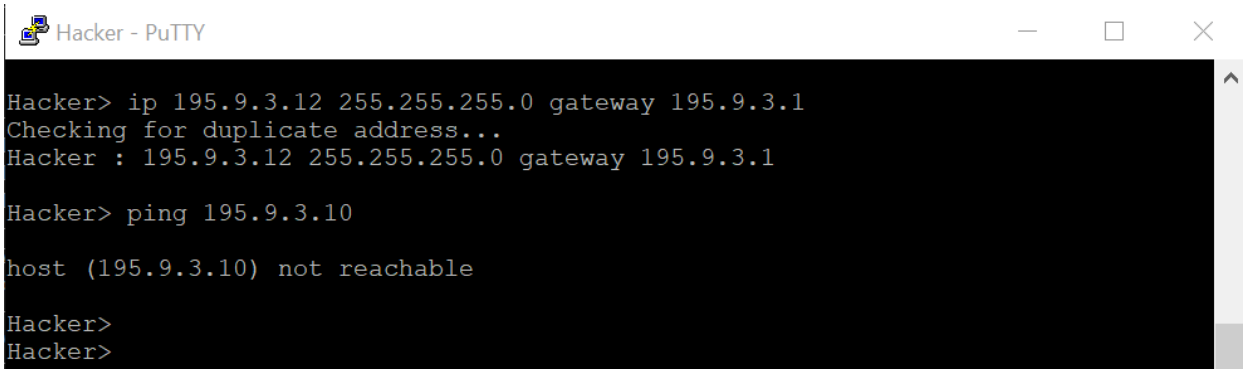


Рис. 3.54 – Спроба перевірки зв'язку зі станцією підмережі VLAN 50 з комп'ютера Hacker

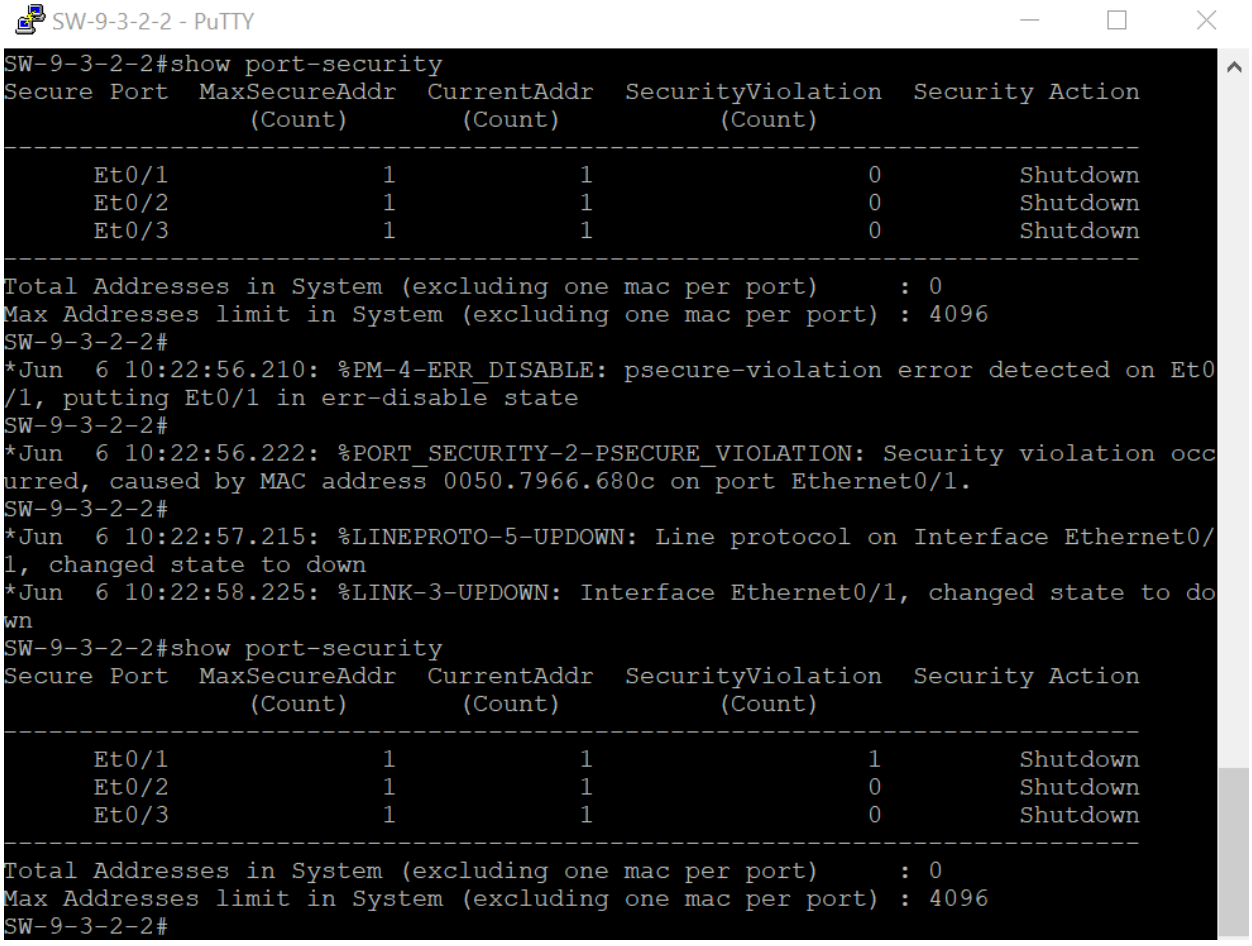


Рис. 3.55 – Результат захисту комутатора та вивід команди show port-security до підключення стороннього комп'ютера та після

Після перевірки роботи всіх налаштувань, можемо переглянути вивід довідкових команд стосовно безпеки та стану мережі:

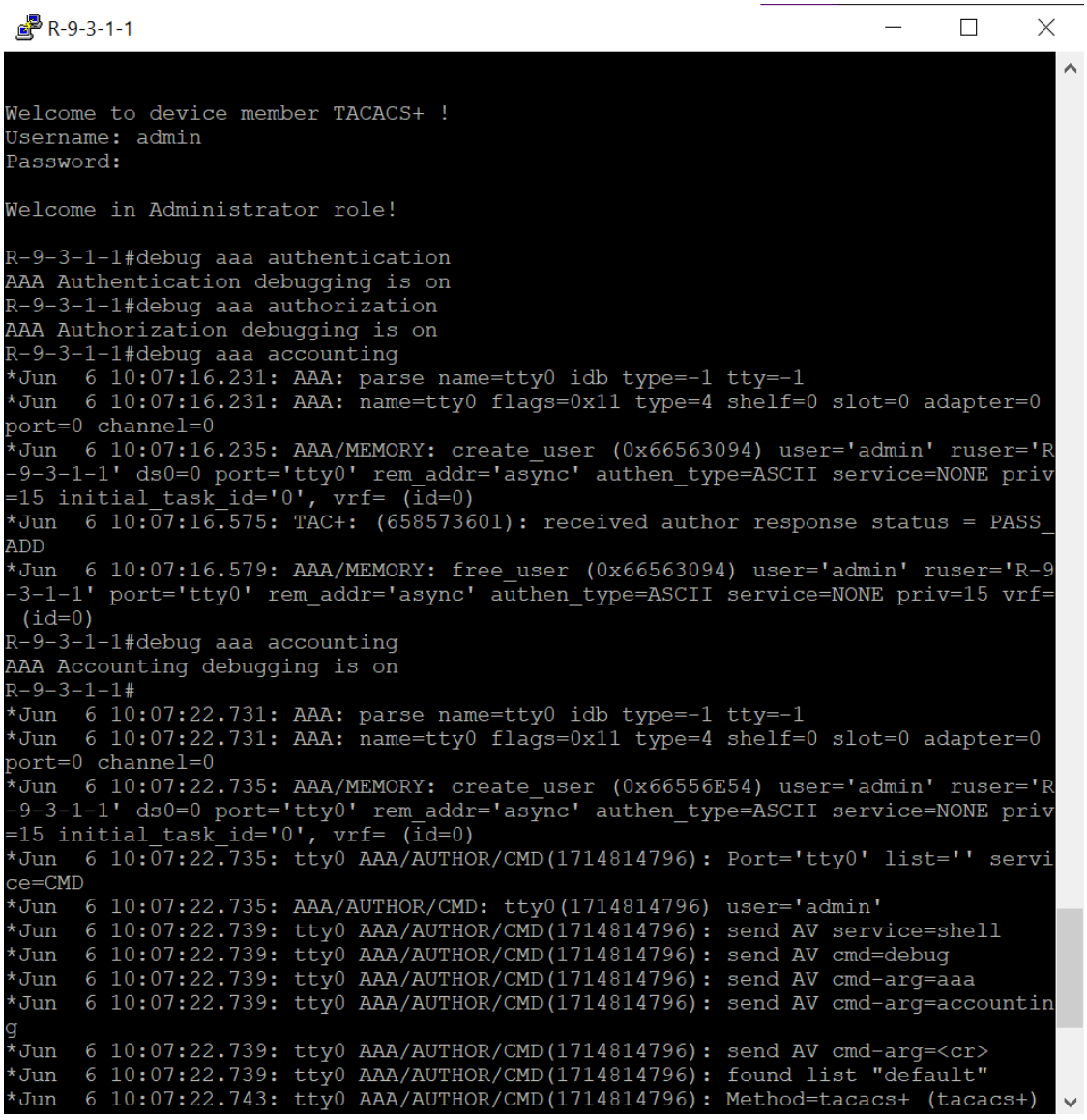


Рис. 3.56 – Виконання діагностичних команд моделі AAA на маршрутизаторі R-9-3-1-1

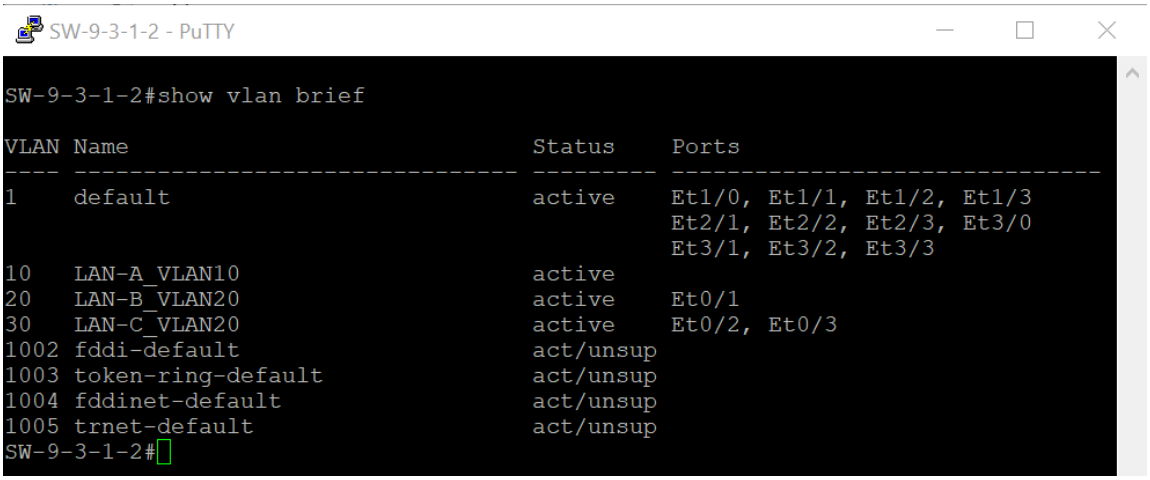


Рис. 3.57 – Виконання команди show vlan brief на комутаторі SW-9-3-1-2

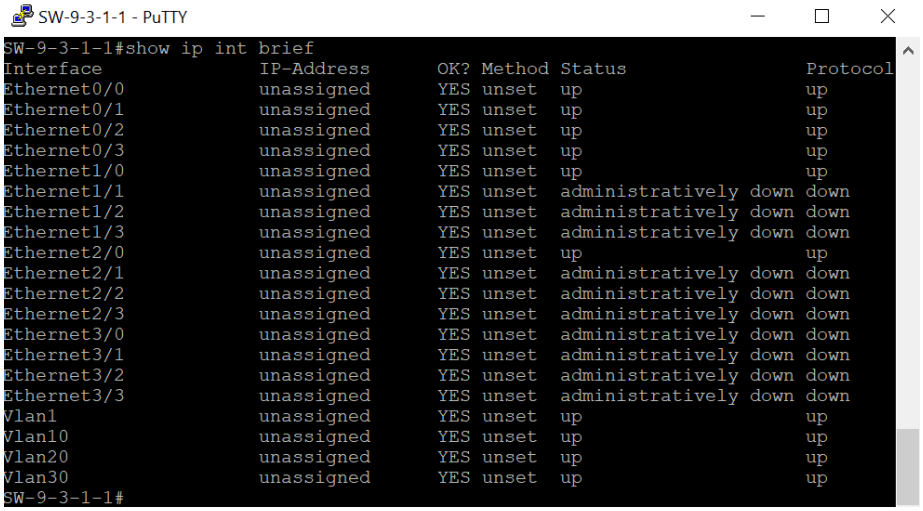


Рис. 3.58 – Виконання команди show ip int brief на комутаторі SW-9-3-1-1

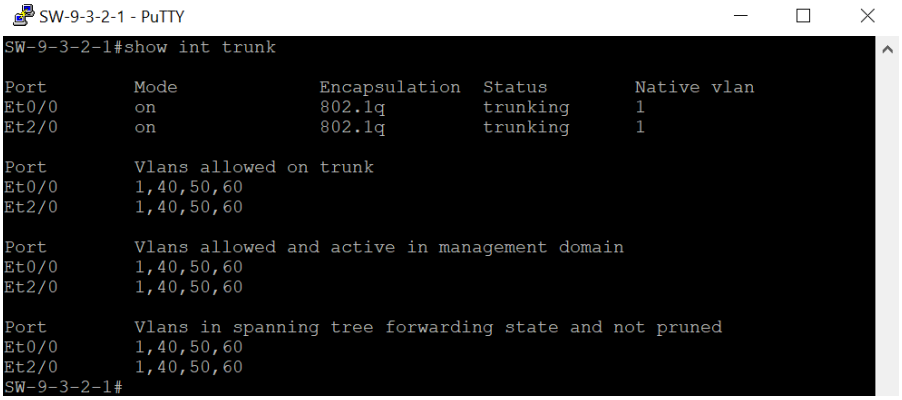


Рис. 3.59 – Виконання команди show int trunk на комутаторі SW-9-3-2-1

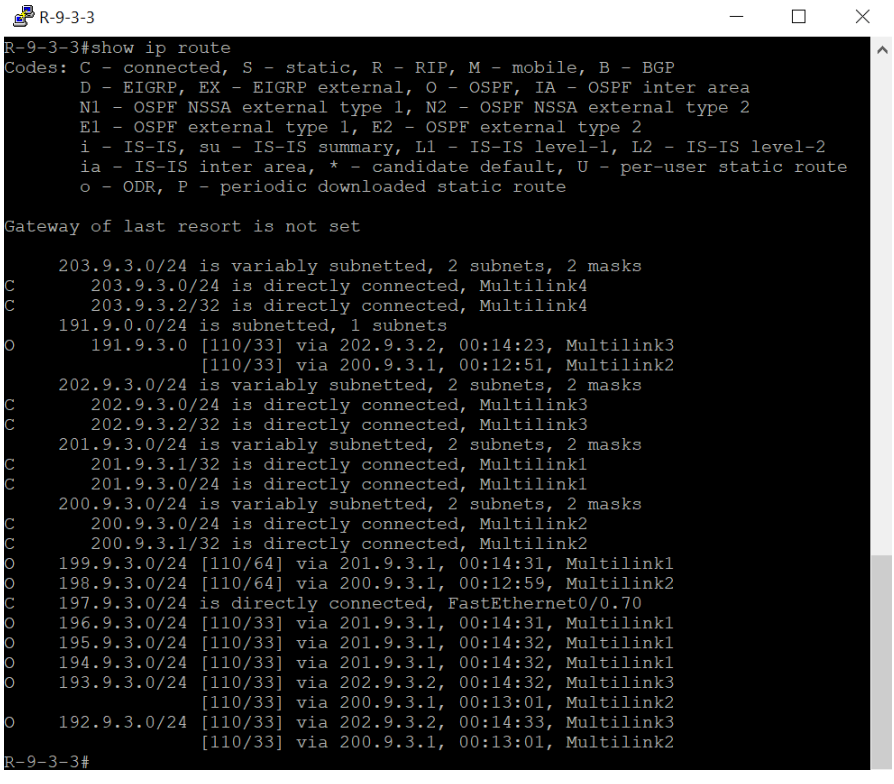


Рис. 3.60 – Виконання команди show ip route на маршрутизаторі R-9-3-3

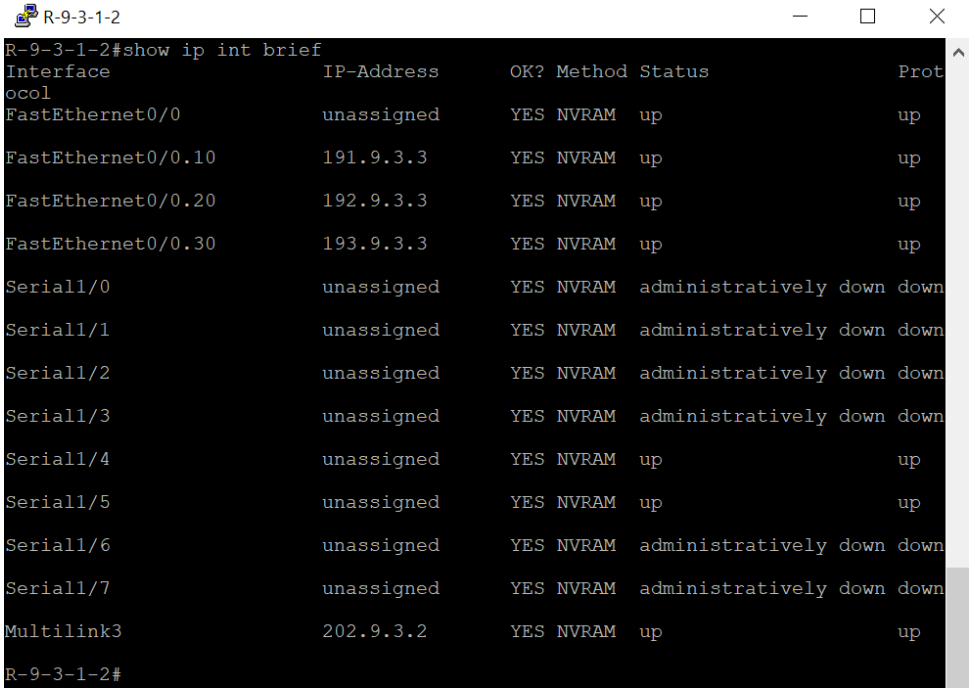


Рис. 3.61 – Виконання команди show ip int brief на маршрутизаторі R-9-3-1-2

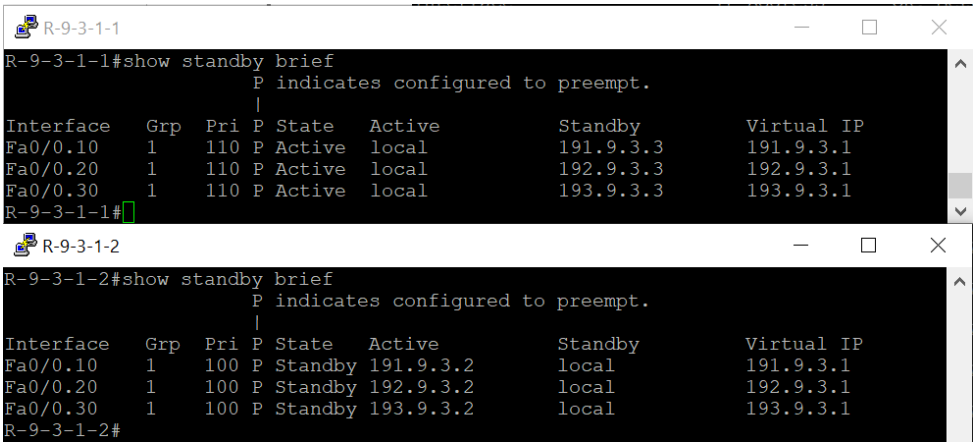


Рис. 3.62 – Виконання команди show standby brief на першій парі маршрутизаторів R-9-3-1-1 та R-9-3-1-2

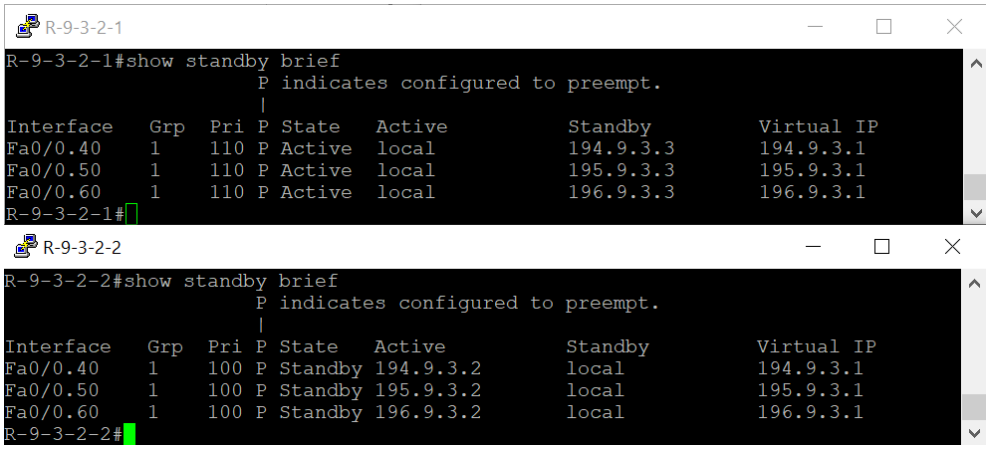


Рис. 3.63 – Виконання команди show standby brief на другій парі маршрутизаторів R-9-3-2-1 та R-9-3-2-2

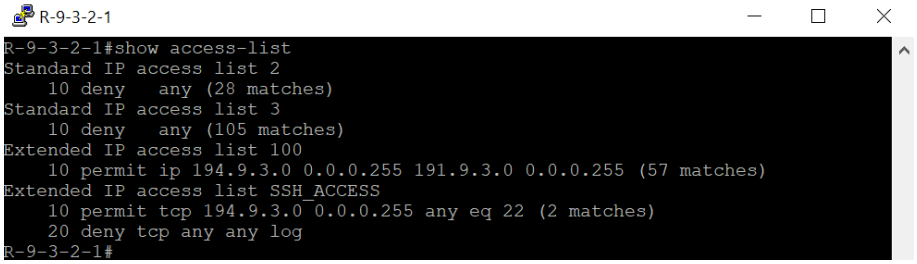


Рис. 3.64 – Виконання команди show access-list на маршрутизаторі R-9-3-2-1

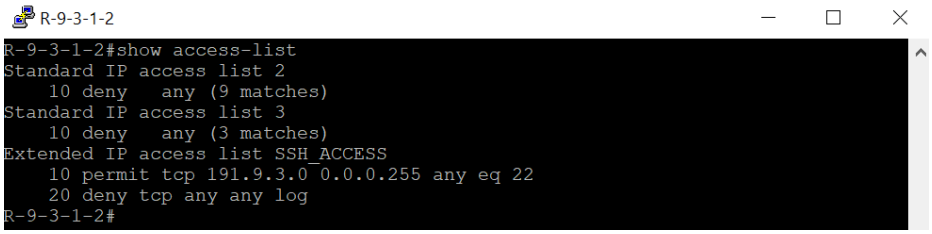


Рис. 3.65 – Виконання команди show access-list на маршрутизаторі R-9-3-1-2

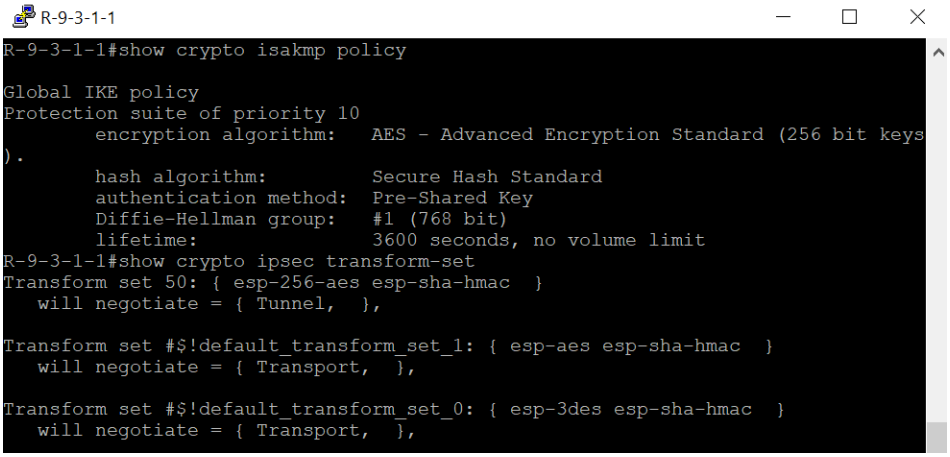


Рис. 3.66 – Виконання команд show crypto isakmp policy та show crypto ipsec transform-set на маршрутизаторі R-9-3-1-1

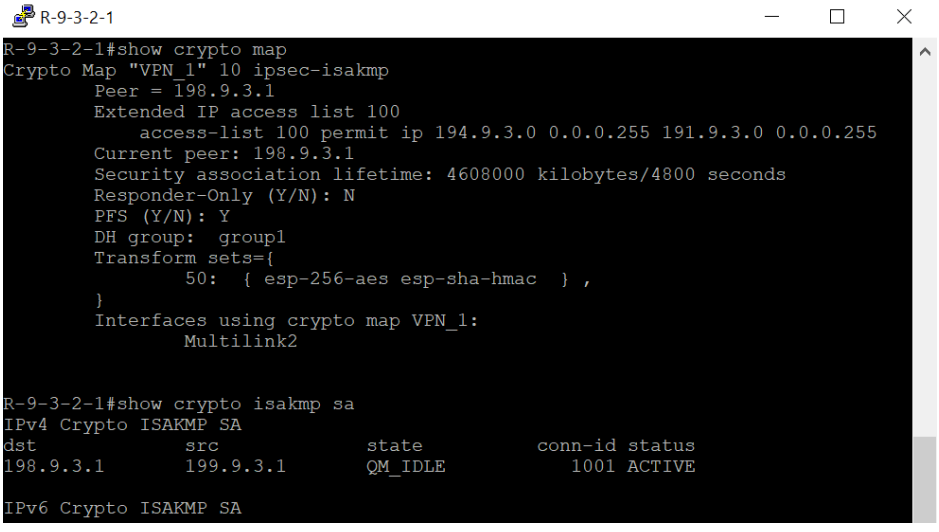


Рис. 3.67 – Виконання команд show crypto map та show crypto isakmp sa на маршрутизаторі R-9-3-2-1

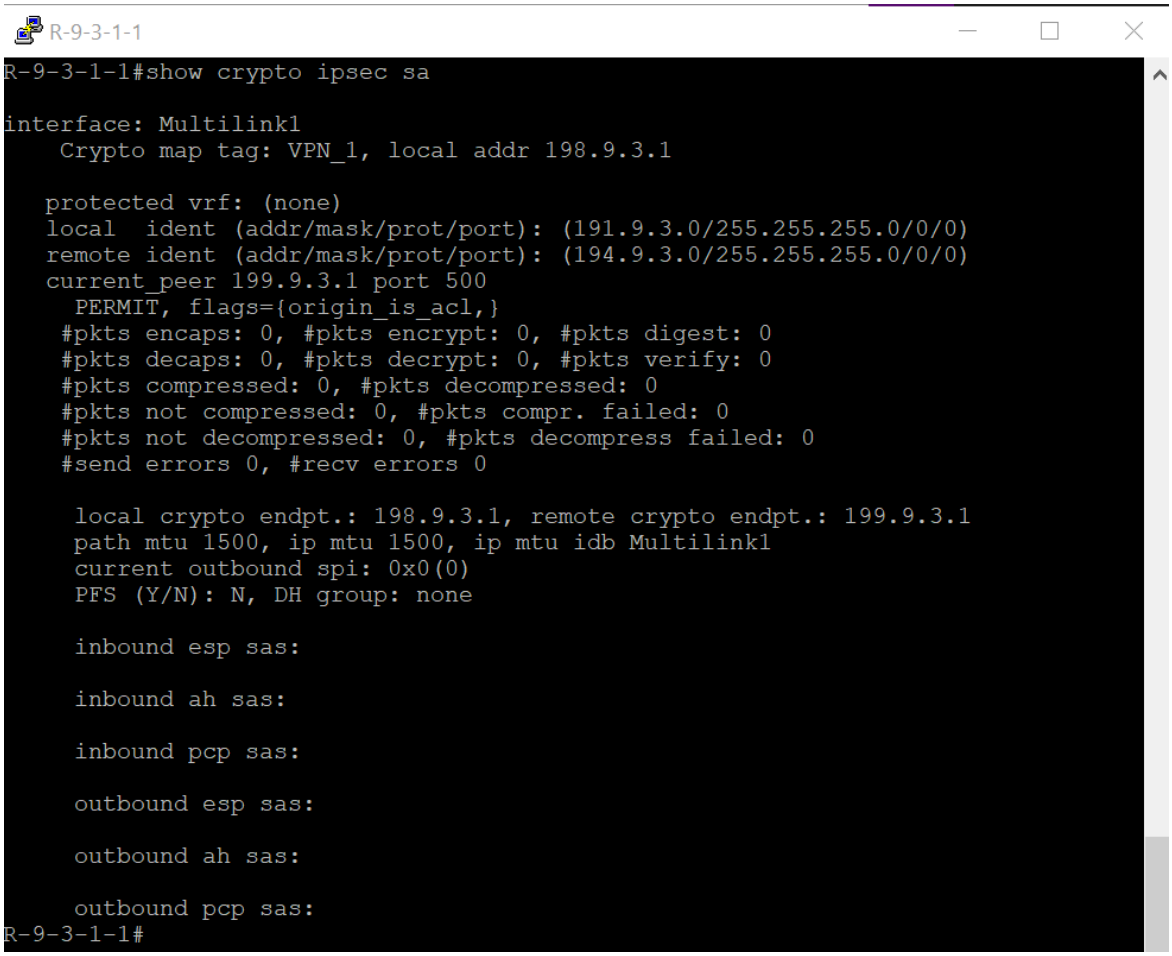


Рис. 3.68 – Виконання команди show crypto ipsec sa на маршрутизаторі R-9-3-1-1

Висновки до третього розділу:

У цьому розділі проведено підготовку до налаштування мережі, що включала встановлення необхідних програм та розширення функціональності мережних пристроїв. Також детально описано кроки налагодження самої мережі та її захисту . У останньому пункті розділу було показано успішний результат налагодження усіх протоколів, технологій, сервісів та служб. Перевірено зв’язок між станціями, роботу захисту мережі та показано вивід довідникових команд.

ВИСНОВКИ

У даній кваліфікаційній роботі було спроєктовано та налаштовано систему захисту комп’ютерної мережі організації, побудованої на базі обладнання Cisco.

У першому розділі було розглянуто можливі загрози для мережі та відповідно їм визначено оптимальні технології та протоколи для підвищення безпеки. Проаналізовано використання VLAN для сегментації мережі, ACL для контролю трафіку, протоколів HSRP та IPsec VPN для забезпечення доступності та захисту даних, а також реалізацію автентифікації за допомогою TACACS+ та SSH і моніторинг мережевих подій через SYSLOG.

У другому розділі описано моделі пристроїв, а також операційні системи для спроєктованої мережі. Розглянуто ключові аспекти захисту мережі, розроблено проєкт комп'ютерної мережі з урахуванням заходів безпеки та створено схему адресації для ефективного функціонування мережі.

У третьому розділі проведено підготовку до налаштування мережі, включаючи встановлення програм і розширення функціональності пристроїв. Детально описано налаштування мережі та її захисту. Успішно налаштовано протоколи, технології, сервіси та служби, перевірено зв’язок між станціями та роботу захисту мережі.

В результаті виконання кваліфікаційної роботи були виконані всі поставлені завдання. Розглянуто теоретичні аспекти безпеки комп'ютерних мереж, розроблено проєкт захищеної комп'ютерної мережі на базі обладнання Cisco, налаштовано та протестовано систему. Всі ці заходи сприяли створенню надійної та безпечної мережевої інфраструктури, яка надає високий рівень захисту інформації та відповідає сучасним вимогам кібербезпеки.

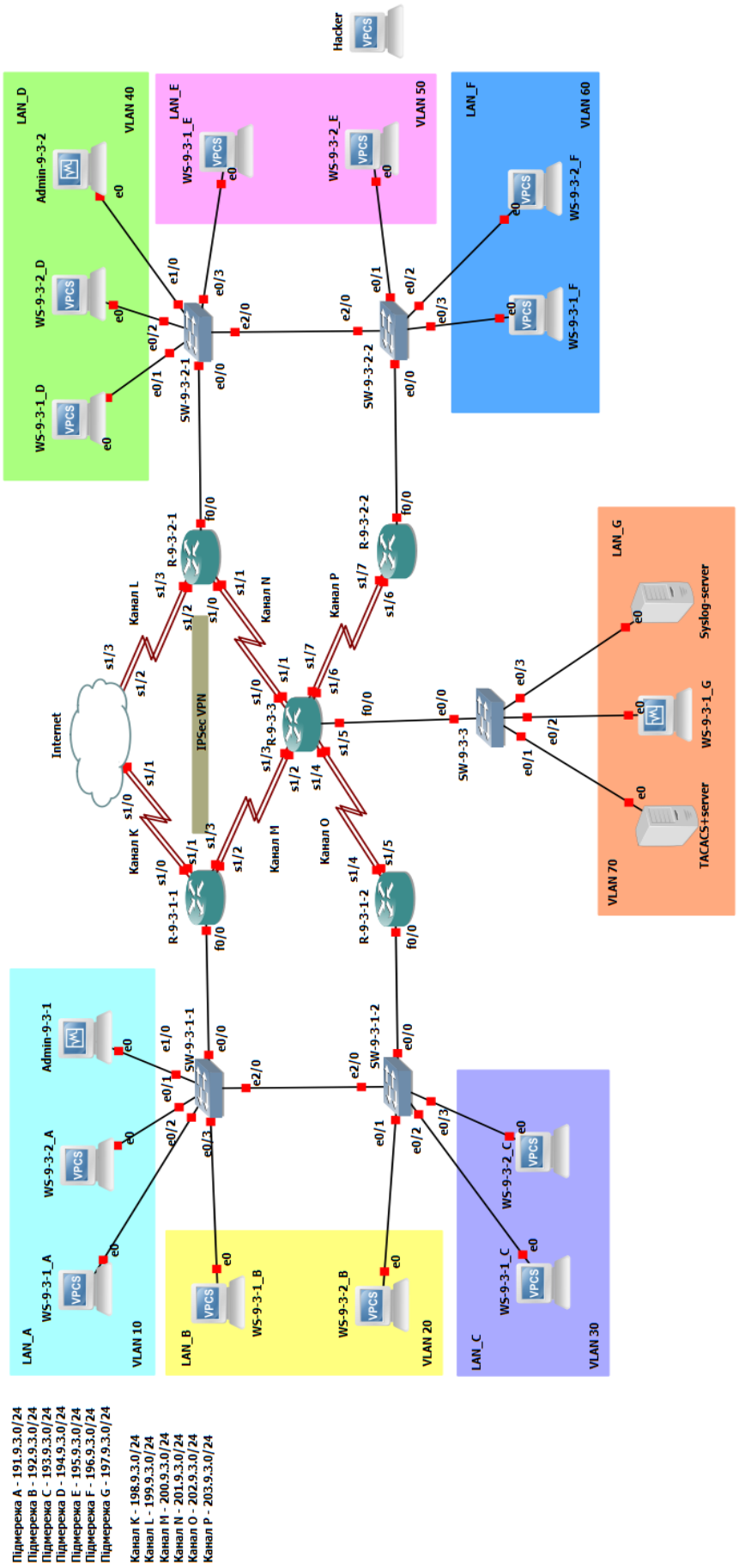
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Top 10 Common Network Security Threats Explained. [Електронний ресурс] : Режим доступу: https://securitytrails.com/blog/top-10-common-network-security-threats-explained
2. Telnet vs. SSH: how is SSH different from telnet? [Електронний ресурс] : Режим доступу: https://phoenixnap.com/kb/telnet-vs-ssh
3. VLANs: effective network segmentation for security. [Електронний ресурс] : Режим доступу: https://www.esecurityplanet.com/networks/what-is-a-vlan/
4. What Is a Site-to-Site VPN? [Електронний ресурс] : Режим доступу: https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn
5. Implement AAA with TACACS server: for enterprise networks. [Електронний ресурс] : Режим доступу: https://www.miniorange.com/blog/aaa-tacacs-authentication/
6. Що таке списки контролю доступу (ACL) і як вони підвищують безпеку мережі, контролюючи потік трафіку на основі визначених правил? [Електронний ресурс] : Режим доступу: http://surl.li/uitut
7. Why Users Should Choose CISCO Devices For Networking. [Електронний ресурс] : Режим доступу: https://www.multisoftvirtualacademy.com/blog/why-users-should-choose-cisco-devices-for-networking/
8. Маршрутизатор Cisco 7200 (7206VXR/NPE-G1). [Електронний ресурс] : Режим доступу: https://stack-systems.com.ua/marshrutizator-Cisco-7206vxr-npe-g1
9. Комутатор cisco catalyst 2960 (WS-C2960-24TT-L). Електронний ресурс] : Режим доступу: https://stack-systems.com.ua/kommutator-cisco-ws-c2960-24tt-l
10. Ієрархічна модель мережі. [Електронний ресурс] : Режим доступу: https://rci-c.com/technology/yerarkhycheskaia-model-sety/
11. Lab : syslog server for Cisco router in GNS3. [Електронний ресурс] : Режим доступу: https://yaser-rahmati.gitbook.io/Cisco-ccnp-r-s-300-115-switch/lab-syslog-server-for-Cisco-router-in-gns3

12. PPP MultiLink. [Електронний ресурс] : Режим доступу: https://networkles-sons.com/Cisco/ccna-routing-switching-icnd2-200-105/ppp-multilink
13. How to configure port security on Cisco Catalyst switches that run Cisco IOS system software. [Електронний ресурс] : Режим доступу: https://commu-nity.cisco.com/t5/networking-knowledge-base/how-to-configure-port-secu-rity-on-cisco-catalyst-switches-that/ta-p/3132907
14. What is router on a stick | best explained – 2023. [Електронний ресурс] : Ре-жим доступу: https://www.nwkings.com/what-is-router-on-a-stick
15. VaelTech. Setup and Configure TacacsGui Appliance in GNS3 to Authenti-cate Devices using Cisco TACACS+ security, 2023. [Електронний ресурс] : Режим доступу: https://www.youtube.com/watch?v=ZLeIdUA8SFY
16. Network Engineer Pro. Configuring an ACL on VTY lines (telnet/ssh), 2021. [Електронний ресурс] : Режим доступу: https://www.youtube.com/watch?v=yo4zSiOzh-E

ДОДАТКИ

Додаток А. Схема побудованої мережі



		Голишевська М.Ю.			ККІКБ.КР.Б – 125 – 3 – ПЗ	Арк.
		Трокоз Є.М.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток Б. Таблиця адресації пристроїв

Таблиця Б.1 – Адресація пристроїв

Мережа/ Пристрій	**Інтерфейс/Мереж-ний адаптер/Шлюз**	**IP-адреса**	**Маска**	**Пре-фікс**
Підмережа A	-	191.9.3.0	255.255.255.0	/24
Підмережа B	-	192.9.3.0	255.255.255.0	/24
Підмережа C	-	193.9.3.0	255.255.255.0	/24
Підмережа D	-	194.9.3.0	255.255.255.0	/24
Підмережа E	-	195.9.3.0	255.255.255.0	/24
Підмережа F	-	196.9.3.0	255.255.255.0	/24
Підмережа G	-	197.9.3.0	255.255.255.0	/24
Підмережа K	-	198.9.3.0	255.255.255.0	/24
Підмережа L	-	199.9.3.0	255.255.255.0	/24
Підмережа M	-	200.9.3.0	255.255.255.0	/24
Підмережа N	-	201.9.3.0	255.255.255.0	/24
Підмережа O	-	202.9.3.0	255.255.255.0	/24
Підмережа P	-	203.9.3.0	255.255.255.0	/24
Internet	Інтерфейс Multilink 1 (Se1/0, Se1/1)	198.9.3.2	255.255.255.0	/24
	Інтерфейс Multilink 2 (Se1/2, Se1/3)	199.9.3.2	255.255.255.0	/24
Маршрутиза-тор R-9-3-1-1	Інтерфейс Multilink 1 (Se1/0, Se1/1)	198.9.3.1	255.255.255.0	/24
	Інтерфейс Multilink 2 (Se1/2, Se1/3)	200.9.3.1	255.255.255.0	/24
Маршрутиза-тор R-9-3-1-1	Інтерфейс Fa0/0.10	191.9.3.2	255.255.255.0	/24
	Інтерфейс Fa0/0.20	192.9.3.2	255.255.255.0	/24
	Інтерфейс Fa0/0.30	193.9.3.2	255.255.255.0	/24
Маршрутиза-тор R-9-3-2-1	Інтерфейс Multilink 2 (Se1/2, Se1/3)	199.9.3.1	255.255.255.0	/24
Маршрутиза-тор R-9-3-2-1	Інтерфейс Multilink 1 (Se1/0, Se1/1)	201.9.3.1	255.255.255.0	/24
	Інтерфейс Fa0/0.40	194.9.3.2	255.255.255.0	/24

Продовження табл. Б.1 – Адресація пристроїв

Маршрутизатор R-9-3-2-1	Інтерфейс Fa0/0.50	195.9.3.2	255.255.255.0	/24
	Інтерфейс Fa0/0.60	196.9.3.2	255.255.255.0	/24
Маршрутизатор R-9-3-3	Інтерфейс Multilink 2 (Se1/2, Se1/3)	200.9.3.2	255.255.255.0	/24
	Інтерфейс Multilink 1 (Se1/0, Se1/1)	201.9.3.2	255.255.255.0	/24
	Інтерфейс Multilink 3 (Se1/4, Se1/5)	202.9.3.1	255.255.255.0	/24
Маршрутизатор R-9-3-3	Інтерфейс Multilink 4 (Se1/6, Se1/7)	203.9.3.1	255.255.255.0	/24
	Інтерфейс Fa0/0.70	197.9.3.1	255.255.255.0	/24
Маршрутизатор R-9-3-1-2	Інтерфейс Multilink 3 (Se1/4, Se1/5)	202.9.3.2	255.255.255.0	/24
Маршрутизатор R-9-3-1-2	Інтерфейс Fa0/0.10	191.9.3.3	255.255.255.0	/24
	Інтерфейс Fa0/0.20	192.9.3.3	255.255.255.0	/24
	Інтерфейс Fa0/0.30	193.9.3.3	255.255.255.0	/24
Маршрутизатор R-9-3-2-2	Інтерфейс Multilink 4 (Se1/6, Se1/7)	203.9.3.2	255.255.255.0	/24
	Інтерфейс Fa0/0.40	194.9.3.3	255.255.255.0	/24
	Інтерфейс Fa0/0.50	195.9.3.3	255.255.255.0	/24
	Інтерфейс Fa0/0.60	196.9.3.3	255.255.255.0	/24
Робоча станція WS-9-4-1_A	Мережний адаптор	191.9.3.10	255.255.255.0	/24
	Шлюз за замовчуванням	191.9.3.1	255.255.255.0	/24
Робоча станція WS-9-4-2_A	Мережний адаптор	191.9.3.11	255.255.255.0	/24
	Шлюз за замовчуванням	191.9.3.1	255.255.255.0	/24
Робоча станція Admin-9-3-1	Мережний адаптор	191.9.3.12	255.255.255.0	/24
	Шлюз за замовчуванням	191.9.3.1	255.255.255.0	/24
Робоча станція WS-9-4-1_B	Мережний адаптор	192.9.3.10	255.255.255.0	/24
	Шлюз за замовчуванням	192.9.3.1	255.255.255.0	/24

Продовження табл. Б.1 – Адресація пристроїв

Робоча станція WS-9-4-2_B	Мережний адаптор	192.9.3.11	255.255.255.0	/24
	Шлюз за замовчуванням	192.9.3.1	255.255.255.0	/24
Робоча станція WS-9-4-1_C	Мережний адаптор	193.9.3.10	255.255.255.0	/24
	Шлюз за замовчуванням	193.9.3.1	255.255.255.0	/24
Робоча станція WS-9-4-2_C	Мережний адаптор	193.9.3.11	255.255.255.0	/24
	Шлюз за замовчуванням	193.9.3.1	255.255.255.0	/24
Робоча станція WS-9-4-1_D	Мережний адаптор	194.9.3.10	255.255.255.0	/24
	Шлюз за замовчуванням	194.9.3.1	255.255.255.0	/24
Робоча станція WS-9-4-2_D	Мережний адаптор	194.9.3.11	255.255.255.0	/24
	Шлюз за замовчуванням	194.9.3.1	255.255.255.0	/24
Робоча станція Admin-9-3-2	Мережний адаптор	194.9.3.12	255.255.255.0	/24
	Шлюз за замовчуванням	194.9.3.1	255.255.255.0	/24
Робоча станція WS-9-4-1_E	Мережний адаптор	195.9.3.10	255.255.255.0	/24
	Шлюз за замовчуванням	195.9.3.1	255.255.255.0	/24
Робоча станція WS-9-4-2_E	Мережний адаптор	195.9.3.11	255.255.255.0	/24
	Шлюз за замовчуванням	195.9.3.1	255.255.255.0	/24
Робоча станція WS-9-4-1_F	Мережний адаптор	196.9.3.10	255.255.255.0	/24
	Шлюз за замовчуванням	196.9.3.1	255.255.255.0	/24
Робоча станція WS-9-4-2_F	Мережний адаптор	196.9.3.11	255.255.255.0	/24
	Шлюз за замовчуванням	196.9.3.1	255.255.255.0	/24
Сервер TACACS+	Мережний адаптор	197.9.3.10	255.255.255.0	/24
	Шлюз за замовчуванням	197.9.3.1	255.255.255.0	/24

Продовження табл. Б.1 – Адресація пристроїв

Робоча станція WS-9-4-1_G	Мережний адаптор	197.9.3.11	255.255.255.0	/24
	Шлюз за замовчуванням	197.9.3.1	255.255.255.0	/24
Сервер SYSLOG	Мережний адаптор	197.9.3.12	255.255.255.0	/24
	Шлюз за замовчуванням	197.9.3.1	255.255.255.0	/24

Маршрутизатори:

```
R-9-3-1-1#show run
hostname R-9-3-1-1
security passwords min-length 9
logging message-counter syslog
enable secret 5 $1$Adk8$LdfEJcxVGIlghu2oBzgOK/
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ lo-
cal
aaa accounting exec default
 action-type start-stop
 group tacacs+
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip domain name holyshevska.net
no ipv6 cef
multilink bundle-name authenticated
username admin privilege 15 secret 5 $1$DHXs$AV-
aLQxoRK6KNhGjbvpsyg0
archive
 log config
  hidekeys
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 lifetime 3600
crypto isakmp key admin address 199.9.3.1
crypto ipsec security-association lifetime seconds 1800
crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
crypto map VPN_1 10 ipsec-isakmp
 set peer 199.9.3.1
 set security-association lifetime seconds 4800
 set transform-set 50
 set pfs group1
 match address 100
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
interface Multilink1
 description LINK_TO_Internet
 ip address 198.9.3.1 255.255.255.0
 ppp multilink
 ppp multilink group 1
 crypto map VPN_1
interface Multilink2
 description LINK_TO_R-9-3-3
 ip address 200.9.3.1 255.255.255.0
 ppp multilink
 ppp multilink group 2
interface FastEthernet0/0
 description LINK_TO_SW-9-3-1-1
 no ip address
 duplex half
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 191.9.3.2 255.255.255.0
 ip ospf 903 area 0
 standby 1 ip 191.9.3.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 track Multilink2
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.9.3.2 255.255.255.0
 ip access-group 2 out
 ip ospf 903 area 0
 standby 1 ip 192.9.3.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 track Multilink2
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 193.9.3.2 255.255.255.0
 ip access-group 3 out
 ip ospf 903 area 0
 standby 1 ip 193.9.3.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 track Multilink2
interface Serial1/0
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 1
interface Serial1/1
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 1
interface Serial1/2
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 2
interface Serial1/3
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 2
interface Serial1/4
 no ip address
```

```
 shutdown
 serial restart-delay 0
interface Serial1/5
 no ip address
 shutdown
 serial restart-delay 0
interface Serial1/6
 no ip address
 shutdown
 serial restart-delay 0
interface Serial1/7
 no ip address
 shutdown
 serial restart-delay 0
router ospf 903
 log-adjacency-changes
 network 191.9.3.0 0.0.0.255 area 0
 network 192.9.3.0 0.0.0.255 area 0
 network 193.9.3.0 0.0.0.255 area 0
 network 198.9.3.0 0.0.0.255 area 0
 network 200.9.3.0 0.0.0.255 area 0
ip access-list extended SSH_ACCESS
 permit tcp 191.9.3.0 0.0.0.255 any eq 22
 deny   tcp any any log
logging 197.9.3.12
access-list 2 deny   any
access-list 3 deny   any
access-list 100 permit ip 191.9.3.0 0.0.0.255 194.9.3.0
0.0.0.255
tacacs-server host 197.9.3.10 key tacacspass
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 access-class SSH_ACCESS in
line vty 5 15
 access-class SSH_ACCESS in
!
end


R-9-3-2-1#show run
hostname R-9-3-2-1
security passwords min-length 9
logging message-counter syslog
enable secret 5 $1$0uAE$pO8glmm5JkLyvSpSfgbws/
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ lo-
cal
aaa accounting exec default
 action-type start-stop
 group tacacs+
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
aaa session-id common
ip source-route
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip domain name holyshevska.net
no ipv6 cef
multilink bundle-name authenticated
username admin privilege 15 secret 5
$1$4BdB$LNn4HfkxfoshL9QxA1zkY.
archive
 log config
  hidekeys
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 lifetime 3600
crypto isakmp key admin address 198.9.3.1
crypto ipsec security-association lifetime seconds 1800
crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
crypto map VPN_1 10 ipsec-isakmp
 set peer 198.9.3.1
 set security-association lifetime seconds 4800
 set transform-set 50
 set pfs group1
 match address 100
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
interface Multilink1
 description LINK_TO_R-9-3-3
 ip address 201.9.3.1 255.255.255.0
 ppp multilink
 ppp multilink group 1
interface Multilink2
 description LINK_TO_Internet
 ip address 199.9.3.1 255.255.255.0
 ppp multilink
 ppp multilink group 2
 crypto map VPN_1
interface FastEthernet0/0
 description LINK_TO_SW-9-3-2-1
 no ip address
 duplex half
interface FastEthernet0/0.40
 encapsulation dot1Q 40
 ip address 194.9.3.2 255.255.255.0
 ip ospf 903 area 0
 standby 1 ip 194.9.3.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 track Multilink1
interface FastEthernet0/0.50
 encapsulation dot1Q 50
 ip address 195.9.3.2 255.255.255.0
 ip access-group 2 out
 ip ospf 903 area 0
 standby 1 ip 195.9.3.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 track Multilink1
```

```
interface FastEthernet0/0.60
 encapsulation dot1Q 60
 ip address 196.9.3.2 255.255.255.0
 ip access-group 3 out
 ip ospf 903 area 0
 standby 1 ip 196.9.3.1
 standby 1 priority 110
 standby 1 preempt
 standby 1 track Multilink1
interface Serial1/0
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 1
interface Serial1/1
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 1
interface Serial1/2
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 2
interface Serial1/3
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 2
interface Serial1/4
 no ip address
 shutdown
 serial restart-delay 0
interface Serial1/5
 no ip address
 shutdown
 serial restart-delay 0
interface Serial1/6
 no ip address
 shutdown
 serial restart-delay 0
interface Serial1/7
 no ip address
 shutdown
 serial restart-delay 0
router ospf 903
 log-adjacency-changes
 network 194.9.3.0 0.0.0.255 area 0
 network 195.9.3.0 0.0.0.255 area 0
 network 196.9.3.0 0.0.0.255 area 0
 network 199.9.3.0 0.0.0.255 area 0
 network 201.9.3.0 0.0.0.255 area 0
ip access-list extended SSH_ACCESS
 permit tcp 194.9.3.0 0.0.0.255 any eq 22
 deny   tcp any any log
logging 197.9.3.12
access-list 2 deny   any
access-list 3 deny   any
access-list 100 permit ip 194.9.3.0 0.0.0.255 191.9.3.0
0.0.0.255
no cdp log mismatch duplex
tacacs-server host 197.9.3.10 key tacacspass
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 access-class SSH_ACCESS in
line vty 5 15
 access-class SSH_ACCESS in
!
end


R-9-3-3#show run
hostname R-9-3-3
logging message-counter syslog
enable secret 5 $1$jOS3$uYxtFmU4nDEmjiI.Z7ut30
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ lo-
cal
aaa accounting exec default
 action-type start-stop
 group tacacs+
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
aaa session-id common
ip source-route
no ip domain lookup
ip domain name holyshevska.net
username admin privilege 15 secret 5
$1$eo0c$6u1p01QlPrXsNu4FQFAgS0
archive
 log config
  hidekeys
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
interface Multilink1
 description LINK_TO_R-9-3-2-1
 ip address 201.9.3.2 255.255.255.0
 ppp multilink
 ppp multilink group 1
interface Multilink2
 description LINK_TO_R-9-3-1-1
 ip address 200.9.3.2 255.255.255.0
 ppp multilink
```

```
 ppp multilink group 2
interface Multilink3
 description LINK_TO_R-9-3-1-2
 ip address 202.9.3.1 255.255.255.0
 ppp multilink
 ppp multilink group 3
interface Multilink4
 description LINK_TO_R-9-3-2-2
 ip address 203.9.3.1 255.255.255.0
 ppp multilink
 ppp multilink group 4
interface FastEthernet0/0
 description LINK_TO_SW-9-3-3
 no ip address
 duplex half
interface FastEthernet0/0.70
 encapsulation dot1Q 70
 ip address 197.9.3.1 255.255.255.0
 ip ospf 903 area 0
interface Serial1/0
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 1
interface Serial1/1
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 1
interface Serial1/2
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 2
interface Serial1/3
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 2
interface Serial1/4
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 3
interface Serial1/5
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 3
interface Serial1/6
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 4
interface Serial1/7
 no ip address
 shutdown
 serial restart-delay 0
router ospf 903
 log-adjacency-changes
 network 197.9.3.0 0.0.0.255 area 0
 network 200.9.3.0 0.0.0.255 area 0
 network 201.9.3.0 0.0.0.255 area 0
 network 202.9.3.0 0.0.0.255 area 0
 network 203.9.3.0 0.0.0.255 area 0
ip access-list extended SSH_ACCESS
 permit tcp 191.9.3.0 0.0.0.255 any eq 22
 permit tcp 194.9.3.0 0.0.0.255 any eq 22
 deny   tcp any any log
logging 197.9.3.12
tacacs-server host 197.9.3.10 key tacacspass
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 access-class SSH_ACCESS in
line vty 5 15
 access-class SSH_ACCESS in
!
end


R-9-3-1-2#show run
hostname R-9-3-1-2
logging message-counter syslog
enable secret 5 $1$J6JK$sfsbgreeb5.r2iwRdfCqK0
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ lo-
cal
aaa accounting exec default
 action-type start-stop
 group tacacs+
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
aaa session-id common
username admin privilege 15 secret 5
$1$fIVO$2bNjwfhL.T2agfIl64ZNr.
archive
 log config
  hidekeys
```

```
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
interface Multilink3
 description LINK_TO_R-9-3-3
 ip address 202.9.3.2 255.255.255.0
 ppp multilink
 ppp multilink group 3
interface FastEthernet0/0
 description LINK_TO_SW-9-3-1-2
 no ip address
 duplex half
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 191.9.3.3 255.255.255.0
 ip ospf 903 area 0
 standby 1 ip 191.9.3.1
 standby 1 preempt
 standby 1 track Multilink3
interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.9.3.3 255.255.255.0
 ip access-group 2 out
 ip ospf 903 area 0
 standby 1 ip 192.9.3.1
 standby 1 preempt
 standby 1 track Multilink3
interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 193.9.3.3 255.255.255.0
 ip access-group 3 out
 ip ospf 903 area 0
 standby 1 ip 193.9.3.1
 standby 1 preempt
 standby 1 track Multilink3
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
interface Serial1/4
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 3
interface Serial1/5
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 3
router ospf 903
 log-adjacency-changes
 network 191.9.3.0 0.0.0.255 area 0
 network 192.9.3.0 0.0.0.255 area 0
 network 193.9.3.0 0.0.0.255 area 0
 network 202.9.3.0 0.0.0.255 area 0
ip access-list extended SSH_ACCESS
 permit tcp 191.9.3.0 0.0.0.255 any eq 22
 deny   tcp any any log
logging 197.9.3.12
access-list 2 deny   any
access-list 3 deny   any
no cdp log mismatch duplex
tacacs-server host 197.9.3.10 key tacacspass
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 access-class SSH_ACCESS in
line vty 5 15
 access-class SSH_ACCESS in
!
end


R-9-3-2-2#show run
hostname R-9-3-2-2
logging message-counter syslog
enable secret 5 $1$Ohfj$nKncTRqc0fjF5rxsvNTCe1
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ lo-
cal
aaa accounting exec default
 action-type start-stop
 group tacacs+
aaa accounting commands 15 default
 action-type start-stop
 group tacacs+
aaa session-id common
ip source-route
username admin privilege 15 secret 5
$1$q7uX$fy1ZJoTkwh8K2Pf7xy1YH1
archive
 log config
  hidekeys
ip tcp synwait-time 5
ip ssh time-out 60
ip ssh version 2
interface Multilink4
 description LINK_TO_R-9-3-3
 ip address 203.9.3.2 255.255.255.0
 ppp multilink
 ppp multilink group 4
interface FastEthernet0/0
 description LINK_TO_SW-9-3-2-2
 no ip address
 duplex half
interface FastEthernet0/0.40
```

```
 encapsulation dot1Q 40
 ip address 194.9.3.3 255.255.255.0
 ip ospf 903 area 0
 standby 1 ip 194.9.3.1
 standby 1 preempt
 standby 1 track Multilink4
interface FastEthernet0/0.50
 encapsulation dot1Q 50
 ip address 195.9.3.3 255.255.255.0
 ip access-group 2 out
 ip ospf 903 area 0
 standby 1 ip 195.9.3.1
 standby 1 preempt
 standby 1 track Multilink4
interface FastEthernet0/0.60
 encapsulation dot1Q 60
 ip address 196.9.3.3 255.255.255.0
 ip access-group 3 out
 ip ospf 903 area 0
 standby 1 ip 196.9.3.1
 standby 1 preempt
 standby 1 track Multilink4
interface Serial1/6
 no ip address
 encapsulation ppp
 serial restart-delay 0
 clock rate 56000
 ppp multilink
 ppp multilink group 4
interface Serial1/7
 no ip address
 shutdown
 serial restart-delay 0
router ospf 903
 log-adjacency-changes
 network 194.9.3.0 0.0.0.255 area 0
 network 195.9.3.0 0.0.0.255 area 0
 network 196.9.3.0 0.0.0.255 area 0
 network 203.9.3.0 0.0.0.255 area 0
ip access-list extended SSH_ACCESS
 permit tcp 194.9.3.0 0.0.0.255 any eq 22
 deny   tcp any any log
logging 197.9.3.12
access-list 2 deny   any
access-list 3 deny   any
tacacs-server host 197.9.3.10 key tacacspass
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 access-class SSH_ACCESS in
line vty 5 15
 access-class SSH_ACCESS in
!
end
```

Комутатори:

```
SW-9-3-1-1#show run
hostname SW-9-3-1-1
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
errdisable recovery cause psecure-violation
errdisable recovery interval 780
spanning-tree mode rapid-pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Ethernet0/0
 switchport trunk allowed vlan 1,10,20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Ethernet0/1
 switchport access vlan 10
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet0/2
 switchport access vlan 10
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
0050.7966.6801
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet0/3
 switchport access vlan 20
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
0050.7966.6802
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet1/0
 switchport access vlan 10
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
0800.2773.c425
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet2/0
 switchport trunk allowed vlan 1,10,20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport port-security violation restrict
interface Vlan1
 no ip address
interface Vlan10
 no ip address
interface Vlan20
```

```
 no ip address
interface Vlan30
 no ip address
ip forward-protocol nd
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end
```

```
SW-9-3-2-1#show run
hostname SW-9-3-2-1
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
errdisable recovery cause psecure-violation
errdisable recovery interval 780
spanning-tree mode rapid-pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Ethernet0/0
 switchport trunk allowed vlan 1,40,50,60
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Ethernet0/1
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
0050.7966.6806
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet0/2
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet0/3
 switchport access vlan 50
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
0050.7966.6808
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet1/0
 switchport access vlan 40
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet2/0
 switchport trunk allowed vlan 1,40,50,60
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport port-security violation restrict
interface Vlan1
 no ip address
interface Vlan40
 no ip address
interface Vlan50
 no ip address
interface Vlan60
 no ip address
ip forward-protocol nd
no ip http server
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end
```

```
SW-9-3-3#show run
hostname SW-9-3-3
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
errdisable recovery cause psecure-violation
errdisable recovery interval 780
spanning-tree mode rapid-pvst
spanning-tree extend system-id
vlan internal allocation policy ascending
ip tcp synwait-time 5
interface Ethernet0/0
 switchport trunk allowed vlan 1,70
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Ethernet0/1
 switchport access vlan 70
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
0800.2718.edb7
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet0/2
 switchport access vlan 70
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
0800.2773.c425
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet0/3
```

```
 switchport access vlan 70
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
0800.277c.8b17
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Vlan1
 no ip address
 shutdown
interface Vlan70
 no ip address
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end
```

```
SW-9-3-1-2#show run
hostname SW-9-3-1-2
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
errdisable recovery cause psecure-violation
errdisable recovery interval 780
interface Ethernet0/0
 switchport trunk allowed vlan 1,10,20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Ethernet0/1
 switchport access vlan 20
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky
0050.7966.6803
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet0/2
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet0/3
 switchport access vlan 30
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet2/0
 switchport trunk allowed vlan 1,10,20,30
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport port-security violation restrict
interface Vlan1
 no ip address
interface Vlan10
 no ip address
interface Vlan20
 no ip address
interface Vlan30
 no ip address
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end
```

```
SW-9-3-2-2#show run
hostname SW-9-3-2-2
logging discriminator EXCESS severity drops 6 msg-
body drops EXCESSCOLL
errdisable recovery cause psecure-violation
errdisable recovery interval 780
interface Ethernet0/0
 switchport trunk allowed vlan 1,40,50,60
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface Ethernet0/1
 switchport access vlan 50
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet0/2
 switchport access vlan 60
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet0/3
 switchport access vlan 60
 switchport mode access
 switchport port-security mac-address sticky
 switchport port-security aging time 13
 switchport port-security aging type inactivity
 switchport port-security
interface Ethernet2/0
 switchport trunk allowed vlan 1,40,50,60
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport port-security violation restrict
interface Vlan1
 no ip address
interface Vlan40
```

```
 no ip address
interface Vlan50
 no ip address
interface Vlan60
 no ip address
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
end
```