

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми аутентифікації клієнтських вузлів локальної комп'ютерної мережі на базі технології 802.1x та протоколу RADIUS»

Термін здачі студентом закінченої роботи 28 червня 2022 р.

Вихідні дані роботи (вказується предмет і об'єкт дослідження): Локальна комп'ютерна мережа

Обладнання та програмне забезпечення:

1. Windows OS
2. GNS3

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

Консультанти з випускної кваліфікаційної роботи та її захисту стосуються

Керівник, старший викладач кафедри КІ та КБ

Розділ	Консультант	Відомості про виконання роботи
1	Байлюк Є. М.	Рецензент, старший викладач кафедри КІ та КБ
2	Байлюк Є. М.	22.04.2022
3	Байлюк Є. М.	27.06.2022

Студент Лещенко А. П.

Керівник Байлюк Є. М.

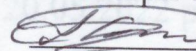
Житомир – 2022

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

1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Лещенко Андрій Павлович

Тема роботи: «Проект підсистеми аутентифікації клієнтських вузлів локальної комп'ютерної мережі на базі технології 802.1x та протоколу RADIUS»

затверджена Наказом університету від 1 березня 2022 р. № 128/с

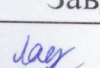
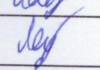
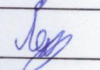
Термін здачі студентом закінченої роботи 28 червня 2022 р.

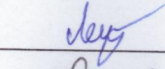
Вихідні дані роботи (зазначається предмет і об'єкт дослідження): Локальна комп'ютерна мережа

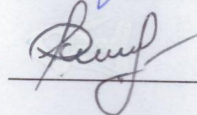
Обладнання та програмне забезпечення:

1. Windows OS
2. GNS3

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Байлюк Є. М.	 06.03.2022	 06.03.2022
2	Байлюк Є. М.	 22.04.2022	 22.04.2022
3	Байлюк Є. М.	 27.06.2022	 27.06.2022

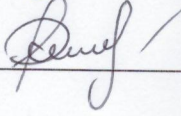
Студент  Лещенко А. П.

Керівник  Байлюк Є. М.

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз отриманого завдання та уточнення поставлених завдань	06.03.2022 р.	
2	Аналіз літературних джерел	11.05.2022 р.	
3	Аналіз об'єкта дослідження	16.05.2022 р.	
4	Постановка задачі дослідження	20.05.2022 р.	
5	Розробка структурної моделі	10.06.2022 р.	
6	Розрахунок параметрів адресації	15.06.2022 р.	
7	Налаштування мережі	25.06.2022 р.	
8	Перевірка працездатності	26.06.2022 р.	
9	Оформлення пояснювальної записки	27.06.2022 р.	
	Захист	Згідно розкладу	

Студент  Лещенко А. П.

Керівник  Байлюк Є. М.

КМ КР.Б - 125 - 10 - ПЗ

№	№ докум.	Підпис	Дата	Гит.	Арк.	Архивна
1	Лещенко А. П.		27.06.2022	Г	4	52
2	Байлюк Є. М.		27.06.2022	Г	4	52
3	Посетко О. А.		27.06.2022	Г	4	52
4	Байлюк Є. М.		27.06.2022	Г	4	52
5	Степаненко І. С.		27.06.2022	Г	4	52

Простий підпис та/або підпис з ініціалами

підпис та/або підпис з ініціалами

підпис та/або підпис з ініціалами

підпис та/або підпис з ініціалами

Гит.

Арк.

Архивна

ФІКТ, Гр. КБ-2

АНОТАЦІЯ

Кваліфікаційна робота складається з проєкту підсистеми аутентифікації клієнтських вузлів локальної комп'ютерної мережі на базі технології 802.1x та протоколу RADIUS та пояснювальної записки до нього. Пояснювальна записка містить у собі 50 сторінок і 45 зображень.

Метою роботи є розробка підсистеми аутентифікації клієнтських вузлів локальної комп'ютерної мережі.

В роботі визначено основні завдання на розробку підсистеми, яка забезпечить автентифікацію. Також в роботі проаналізовані та описані можливі варіанти для отримання несанкціонованого доступу. Обґрунтована актуальність даної тематики та описана сфера її використання. Розроблено та налаштовано загальний проєкт локальної мережі. Проведено тестування мережі.

Ключові слова: 802.1X, RADIUS, AAA, АУТЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ, АУДИТ

					КІК.КР.Б – 125 – 10 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми аутентифікації клієнтських вузлів локальної комп'ю- терної мережі на базі технології 802.1x та протоколу RADIUS	Літ.	Арк.	Аркушів
Розроб.		Леценко А.П.		10.06				
Керівник		Байлюк Є.М.		20.06			4	52
Реценз.		Покотило О.А.		20.06				
Висновок		Байлюк Є.М.		20.06				
Затверд.		Єфіменко А.А.		10.06		ФІКТ, Гр. КБ-2		

ANNOTATION

The qualification work consists of the project of the subsystem for authentication of client nodes of the local computer network based on 802.1x technology and the RADIUS protocol and an explanatory note to it. The explanatory note contains 50 pages and 45 images.

The purpose of the work is to develop a subsystem for authentication of client nodes of the local computer network.

The paper identifies the main tasks for the development of a subsystem that will provide authentication. The paper also analyzes and describes possible options for obtaining unauthorized access. The relevance of this topic is substantiated and the scope of its use is described. The general project of a local area network is developed and adjusted. Network testing was performed.

Keywords: 802.1X, RADIUS, AAA, AUTHENTICATION, AUTHORIZATION ACCOUNTING

		Леценко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ РОБОТИ	9
1.1 Огляд протоколу 802.1х	9
1.2 Протокол AAA	12
1.3 Огляд протоколу RADIUS	13
1.4 Процеси автентифікації та авторизації в протоколі RADIUS	18
1.5 Механізм аудиту протоколу RADIUS	20
1.6 Аналіз вразливостей протоколу RADIUS	21
1.7 Обхід 802.1х в LAN	27
1.8 Постановка технічного завдання	31
РОЗДІЛ 2 ПРОЄКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА	
РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ	32
2.1 Розробка топології комп'ютерної мережі	32
2.2 Налаштування мережевих клієнтів	33
2.3 Налаштування RADIUS сервера	34
2.4 Налаштування протоколу 802.1х	35
РОЗДІЛ 3 ТЕСТУВАННЯ МЕРЕЖІ	37
3.1 Перевірка роботи мережі	37
ВИСНОВКИ	47
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	48
ДОДАТКИ	50

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

PAE – Access Entity Port

EAP – Extensible Authentication Protocol (Розширюваний Протокол Автентифікації)

EAPOL – EAP over LAN (Протокол розширеної перевірки автентичності через локальну мережу)

MAB – MAC Authentication Bypass

		Леценко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. В даний час кількість інтернет сервісів швидко зростає, що призводить до необхідності постійного вдосконалення маршрутизаторів та серверів доступу до мережі з метою задоволення нових вимог. Але постачальники послуг розмежування доступу до ресурсів повинні не тільки пропонувати вільний порт для кожного з'єднання. Вони також повинні забезпечити захист від викрадення даних користувачів, перевірку рівня доступу користувача до ресурсів. Також можуть знадобитися дані про час підключення користувача до мережі для виставлення рахунків та подальшого планування ресурсів. Усі ці послуги вимагають координації між різними системами. Рішення цієї проблеми базується на використанні протоколу автентифікації, авторизації та аудиту (AAA), який, по суті, є фреймворком, який вирішує всі ці окремі завдання разом за допомогою різних мережевих технологій та платформ, включаючи протокол RADIUS.

Метою кваліфікаційної роботи є набуття навичок та знань в сфері технологій протоколу 802.1x та протоколу RADIUS

Визначена мета обумовлює наступні завдання:

- Пошук вразливостей у технологіях
- Тестування роботи мережі
- Збір інформації про протоколи

Об'єктом дослідження є група стандартів IEEE для локальних комп'ютерних мереж та мереж мегаполісів.

Предметом дослідження є особливості автентифікації на базі технології 802.1x та протоколу RADIUS.

У процесі виконання кваліфікаційної роботи було розроблено проєкт в додатку GNS3 для демонстрації роботи.

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ РОБОТИ

1.1 Огляд протоколу 802.1x

IEEE 802.1X — протокол контролю доступу клієнт-сервер, що дозволяє встановлювати автентичність та забороняє підключатись до локальної мережі через загальнодоступні порти комутатора. До того, як клієнта буде автентифіковано, згідно протоколу 802.1X дозволяється пересилка лише трафіку протоколу розширеної перевірки автентичності через локальну мережу (EAPOL) через порт, до якого підключений клієнт. Після успішної автентифікації звичайний трафік може проходити через порт. Автентифікація 802.1X передбачає три сторони: заявник (supplicant), автентифікатор (authenticator) та сервер автентифікації (authentication server).

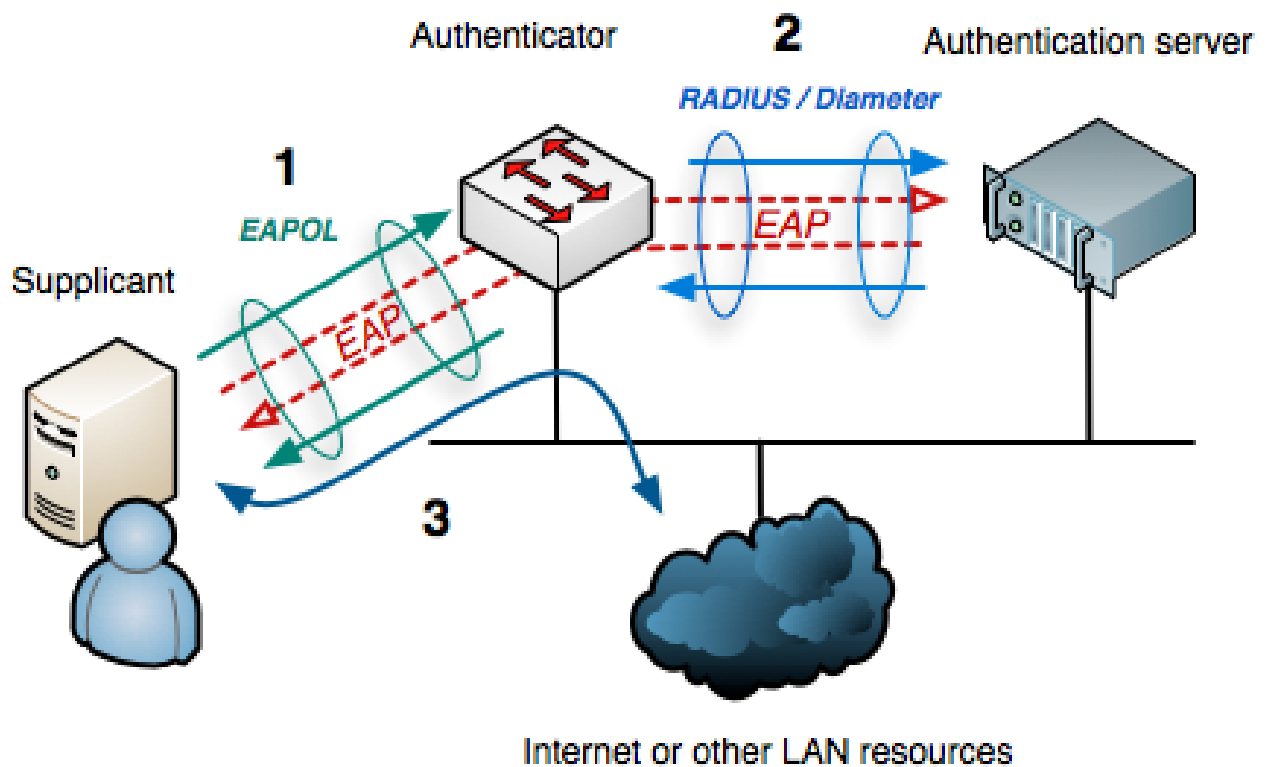


Рисунок 1.1 – Сторони автентифікації

Заявник — це клієнтський пристрій (наприклад, ноутбук), який під'єднується до локальної мережі або бездротової локальної мережі. Термін «supplicant» також може позначати програмне забезпечення, яке працює на клієнтському пристрої та

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

надає облікові дані автентифікатору. Автентифікатор — це мережевий пристрій, такий як комутатор Ethernet або бездротова точка доступу. Сервер автентифікації, зазвичай, хост, який підтримує протоколи RADIUS і EAP. У деяких випадках програмне забезпечення сервера автентифікації може працювати на апаратному засобі автентифікатора.

Аутентифікатор діє як охоронець захищеної мережі. Заявнику (тобто клієнтському пристрою) не дозволяється доступ через аутентифікатор до захищеної сторони мережі, доки не буде підтверджено та авторизовано особу запитувача. При аутентифікації на основі порту 802.1X запитувач спочатку повинен надати аутентифікатору необхідні облікові дані - вони будуть заздалегідь вказані адміністратором мережі і можуть включати ім'я користувача/пароль або дозволений цифровий сертифікат. Аутентифікатор пересилає ці облікові дані на сервер аутентифікації, щоб вирішити, чи потрібно надавати доступ. Якщо сервер аутентифікації визначає, що облікові дані дійсні, він повідомляє про це аутентифікатор, який, у свою чергу, дозволяє запитувачу (клієнтському пристрою) отримати доступ до ресурсів, розташованих на захищеній стороні мережі.

802.1X-2001 визначає два логічних стани для порту автентифікатора — «контрольований порт» і «неконтрольований порт». Контрольований порт керується 802.1X RAE, щоб дозволити (у авторизованому стані) або заборонити (у несанкціонованому стані) мережевий трафік, який передається або приймається через цей порт. Неконтрольований порт використовується 802.1X RAE для передачі та прийому кадрів EAPOL.

802.1X-2004 визначає еквівалентні об'єкти порту для запитувача; тому запитувач, який реалізує 802.1X-2004, може запобігти використанню протоколів вищого рівня, якщо його вміст не завершився успішно. Це особливо корисно, коли використовується метод EAP, що забезпечує взаємну аутентифікацію, оскільки запитувач може запобігти витоку даних при підключенні до неавторизованої мережі.

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

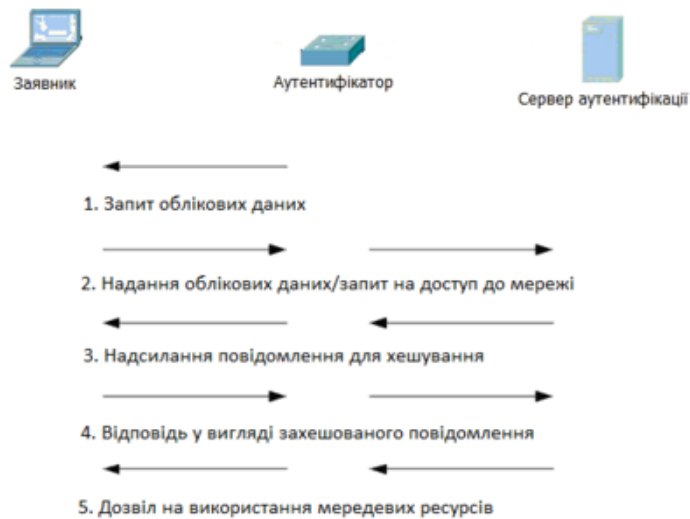


Рисунок 1.2 – Процес перевірки автентичності

Процес перевірки автентичності

1. Ініціалізація: при виявленні нового запитувача порт на комутаторі (аутентифікаторі) активується і встановлюється в стан «неавторизований». У цьому стані дозволений лише трафік 802.1X; інший трафік, наприклад Інтернет-протокол (і разом з цим TCP і UDP), припиняється.

2. Ініціація: для початку аутентифікації аутентифікатор буде періодично передавати кадри ідентифікації EAP-запиту на спеціальну адресу рівня 2 (01:80:C2:00:00:03) у сегменті локальної мережі. Запитувач прослуховує цю адресу, і після отримання кадру ідентифікації EAP-Request Identity, він відповідає кадром EAP-Response Identity, який містить ідентифікатор запитувача, такий як User ID. Потім аутентифікатор інкапсулює цю відповідь Identity в пакет RADIUS Access-Request і пересилає її на сервер аутентифікації. Заявник може також ініціювати або перезапустити аутентифікацію, надсилаючи кадр EAPOL-Start аутентифікатору, який потім відповідає кадром ідентифікації EAP-Request.

3. Узгодження: сервер аутентифікації надсилає відповідь (інкапсульований у пакет RADIUS Access-Challenge) до аутентифікатора, що містить запит EAP із зазначенням методу EAP. Аутентифікатор інкапсулює запит EAP у кадр EAPOL і передає його запитувачу. На цьому етапі заявник може почати використовувати

		Леценко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

запитуваний метод EAP або зробити NAK («Негативне підтвердження») і відповісти методами EAP, які він готовий виконати.

4. Аутентифікація: Якщо сервер аутентифікації та запитувач погоджуються щодо методу EAP, запити та відповіді EAP надсилаються між запитувачем та сервером аутентифікації (перекладаються аутентифікатором), доки сервер аутентифікації не відповість повідомленням EAP-Success, або повідомлення EAP-Failure. Якщо аутентифікація пройшла успішно, аутентифікатор встановлює порт у стан «авторизований», і звичайний трафік дозволено, якщо він не успішний, порт залишається в «неавторизованому» стані. Коли запитувач виходить із системи, він надсилає аутентифікатору повідомлення про вихід із системи EAPOL, потім аутентифікатор встановлює порт у «неавторизований» стан, знову блокуючи весь трафік, що не є EAP.

1.2 Протокол AAA

Протокол AAA (Authentication, Authorization, Accounting — Автентифікація, Авторизація, Аудит) — використовується для опису процесу надання доступу до комп'ютерної мережі та контролю за ним. Протокол AAA дозволяє сильно обмежити можливості порушників, залишаючи законним користувачам мережі право мати доступ до мережевих ресурсів. Розглянемо кожен частину більш детально.

Аутентифікація — це процес ідентифікації користувача, який намагається отримати доступ до ресурсу чи об'єкта. Цей процес визначає, чи має кінцевий користувач унікальну інформацію, тобто комбінацію «ім'я користувача та пароль», секретний ключ або біометричні дані (наприклад, відбитки пальців), які служать унікальними даними. Сервер AAA порівнює надані користувачем облікові дані з даними користувача, що зберігаються в базі даних сервера. Якщо облікові дані збігаються, користувачеві надається доступ до мережі. В іншому випадку сталася помилка автентифікації, і користувачеві було відмовлено у доступі до мережі. Відповідно до RFC2989 авторизація — це визначення, чи може певне право чи послуга бути надана пред'явнику ідентифікаційних даних. Таким правом/послугою можуть бути доступ до мережі, надання IP-адреси, виклик фільтра для визначення,

		Леценко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

які програми чи протоколи підтримуються. У деяких випадках процеси авторизації та автентифікації поєднані.

Авторизація – надання певній особі або групі осіб прав на виконання певних дій, а також процес перевірки (підтвердження) даних прав при спробі виконання цих дій. Часто можна почути вираз, що якийсь чоловік «авторизований» для виконання даної операції - це значить, що він має на неї прав. Авторизація виконує контроль доступу легальних користувачів до ресурсів системи після успішного проходження ними автентифікації. Найчастіше процедури автентифікації і авторизації поєднуються. В інформаційних технологіях за допомогою авторизації встановлюються права доступу до інформаційних ресурсів і систем обробки даних.

Аудит – паралельний з автентифікацією і авторизацією етап, який записує в журнал успіх чи невдачу даних процесів, змогла людина проникнути в приміщення чи ні, чи отримав користувач доступ до мережних пристроїв і, якщо так, то які дії на ньому здійснював. Цей процес важливий з точки зору безпеки та контролю доступу, так як дозволяє визначати потенційні загрози і шукати «діри» в системі. Сучасні системи використовують такі протоколи для автентифікації, авторизації та аудиту: Служба віддаленої автентифікації (Dial-In User Service) (RADIUS), Cisco Terminal Access Controller Access-Control System Plus (TACACS +) і DIAMETER.

В даній роботі серед перелічених вище буде розглядатися лише протокол RADIUS.

1.3 Огляд протоколу RADIUS

Управління розсіяними послідовними лініями та пулами модемів для великої кількості користувачів може створити потребу в значній адміністративній підтримці.

Оскільки пули модемів за визначенням є зв'язком із зовнішнім світом, вони вимагають пильної уваги до безпеки, авторизації та обліку. Найкраще цього можна досягти, керуючи єдиною «базою даних» користувачів, яка дозволяє здійснювати автентифікацію (перевірка імені користувача та пароля), а також інформацію про

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

конфігурацію, де детально описує тип послуги, яка надається користувачеві (наприклад, SLIP, PPP, telnet, rlogin).

Забезпечити дану роботу можна за допомогою протоколу RADIUS.

RADIUS (remote authentication dial-in user service) - це мережевий протокол, який забезпечує клієнт-серверну аутентифікацію, авторизацію і аудит віддалених користувачів. Для підключення віддалених користувачів, в мережі повинні бути встановлені сервери доступу та засоби для віддаленого підключення. Сервер доступу запитує у користувача облікові дані для входу і передає їх на сервер RADIUS, на якому зберігаються імена користувачів і паролі. При цьому віддалений користувач є клієнтом сервера доступу, а сервер доступу є клієнтом RADIUS-сервера.

Незважаючи на те, що цей протокол був розроблений у 1991 році, він все ще широко використовується, як правило, у білінгових системах, або для доступу адміністратора до локальної мережі підприємства.

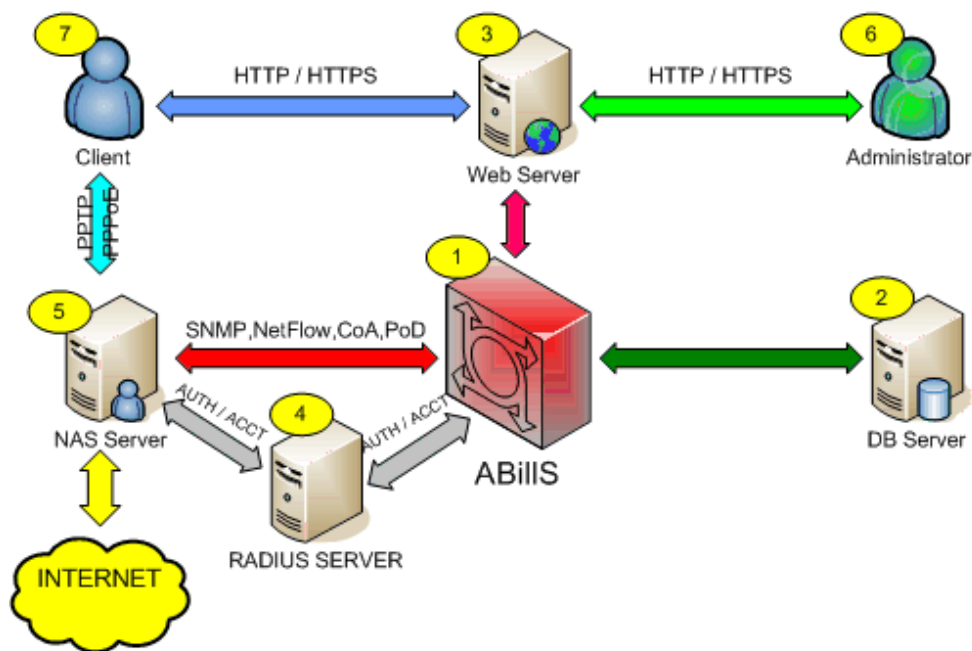


Рисунок 1.3 – Приклад білінгової системи із використанням протоколу RADIUS

RADIUS також використовується в корпоративних середовищах, щоб забезпечити доступ до корпоративної мережі співробітникам під час відряджень або з дому. RADIUS дозволяє компаніям зберігати профілі користувачів в централізо-

ваній базі даних. Після успішної аутентифікації, зовнішньому користувачу при-
своюється попередньо налаштований профіль, який визначає до яких ресурсів він
може отримати доступ, а до яких - ні. Ця технологія дозволяє компанії мати єдину
керовану точку входу, що забезпечує стандартизацію з точки зору безпеки та надає
простий спосіб контролю використання віддаленого доступу і збору мережевий
статистики.

RADIUS був розроблений Карлом Рігні (англ. Carl Rigney) у фірмі Livingston
Enterprises для серії серверів доступу компанії, але потім у 1997 був опублікований
у вигляді стандартів RFC 2058 та RFC 2059 (та пізніше оновлений до стандартів
RFC 2865 та RFC 2866). Це відкритий протокол, який може використовувати будь-
який виробник в своїх продуктах. Конфігурації і облікові дані користувачів можуть
зберігатися на серверах LDAP, в різних базах даних або текстових файлах.

Повідомлення у цьому протоколі передаються у формі пакетів протоколу пе-
редачі даних без встановлення з'єднання UDP. Крім того, усі проблеми пов'язані з
доступністю сервера, повторною передачею даних та часу очікування обробля-
ються пристроями з підтримкою RADIUS, а не самим протоколом передачі. У па-
кеті UDP завжди є лише одне повідомлення RADIUS. Поточна реалізація прото-
колу використовує порт 1812 для автентифікації та порт 1813 для аудиту. Деякі
сервери можуть використовувати порт 1645 для автентифікації та порт 1646 для
аудиту. Протокол реалізує архітектуру клієнт-сервер, де клієнтом є сервер мереже-
вого доступу (NAS), а сервер - це процес, що працює на машині UNIX або Windows
NT. NAS діє як шлюз між користувачем і сервером, відповідає за передачу інфор-
мації про користувача на сервери RADIUS, а потім діє залежно від відповіді, отри-
маної від сервера. RADIUS сервера отримують запити на надання з'єднання кори-
стувачеві, автентифікують користувача, а потім повертають інформацію про
конфігурацію, необхідну клієнту для надання послуг, які запитав користувач.

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

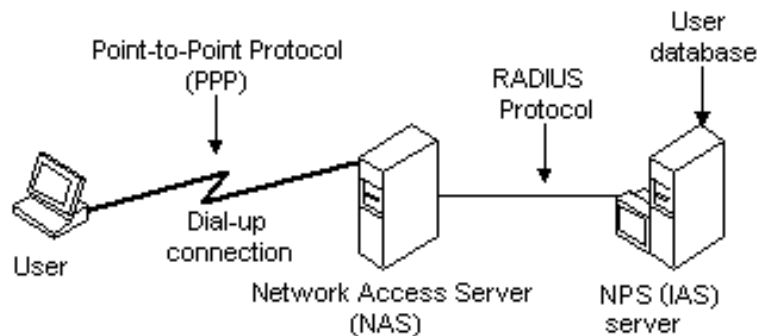


Рисунок 1.4 – Схема взаємодії протоколу RADIUS

Розглянемо процеси аутентифікації та авторизації RADIUS більш детально.

Аутентифікація та авторизація RADIUS описані в RFC 2865. Як правило, вхід користувача складається із запиту від NAS до сервера RADIUS (запит на доступ) та відповіді сервера (доступ приймається або забороняється). RFC 2865 та 2866 підтримують такі типи повідомлень:

1. Access-Request. Відправляється клієнтом RADIUS для запиту автентифікації та спроб авторизації при підключенні до мережі.

2. Access-Accept. Надіслане сервером у відповідь на повідомлення із запитом на доступ. Це повідомлення інформує клієнта про прийняття спроби автентифікації та авторизації.

3. Access-Reject. Надіслане сервером у відповідь на повідомлення із запитом на доступ. Це повідомлення інформує клієнта про те, що його спроба автентифікації та авторизації була відхилена. Сервер надсилає це повідомлення, якщо інформація про користувача неправильна або спроба підключення заборонена.

4. Access-Challenge. Він містить додаткову інформацію від користувача, таку як другий пароль, PIN-код або маркер. Він також використовується в більш складних випадках автентифікації, коли між хостом і сервером користувача встановлюється захищений тунель, щоб клієнт не міг отримати доступ до даних користувача.

5. Accounting-Request. Надіслане клієнтом для ініціювання процесу аудиту прийнятого з'єднання.

6. Accounting-Response. Надіслане сервером у відповідь на AccountingRequest. Підтверджує успішне отримання запиту на аудит.

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

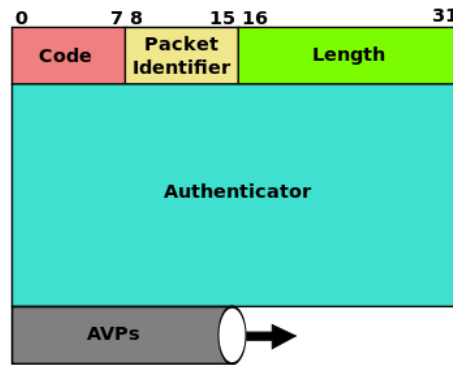


Рисунок 1.5 – Загальна схема пакету RADIUS

Кожен пакет складається з наступних полів:

1. Код. Поле Код становить один октет і визначає тип пакета RADIUS: Access-Request (1), Access-Accept (2), Access-Reject (3), Access-Challenge (11), Accounting-Request (4) або Accounting-Response (5). Коли отримано пакет з недійсним полем коду, він відкидається.

2. Ідентифікатор. Поле Ідентифікатор складається з одного октета і допомагає узгоджувати запити та відповіді. Сервер RADIUS може виявити повторюваний запит протягом короткого проміжку часу, якщо він має однакову IP-адресу джерела клієнта та вихідний порт UDP та ідентифікатор.

3. Довжина. Поле довжини складається з двох октетів. Служить простим механізмом перевірки помилок. Сервер відкидає пакет, якщо його довжина менше значення, вказаного в цьому полі. Якщо довжина пакета перевищує це поле, додаткові октети ігноруються сервером. Мінімальна довжина — 20, максимальна— 4096.

4. Автентифікатор. Поле автентифікатора складається з чотирьох октетів. Містить значення або запиту, або автентифікатора відповіді. Автентифікатор запиту включений до пакету Access-Request. Це значення непередбачуване і унікальне. Він використовується для шифрування пароля користувача при його передачі від клієнта на сервер.

5. Атрибути. Залежить від типу пакету, до складу якого він входить. Кількість пар атрибут/значення, що містяться в цьому полі, є змінною, включаючи обов'язкову або необов'язкову для типу послуги, що вимагається.

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Кінцевий користувач знаходиться у довірчих відносинах із сервером RADIUS через логін та пароль. NAS і сервер мають довірчі відносини на основі спільного пароля. Коли користувач намагається отримати доступ до мережі, NAS передає облікові дані між користувачем та сервером RADIUS. Цей процес називається «RADIUS conversation». Усі RADIUS conversations ініціюються NAS від імені користувача.

1.4 Процеси автентифікації та авторизації в протоколі RADIUS

Транзакції між клієнтом та сервером RADIUS здійснюються із використанням спільного пароля, який відомий і клієнту, і серверу, не надсилається по мережі та вказується системним адміністратором як текстовий рядок. Єдиним технічним обмеженням спільного секрету є те, що його довжина повинна бути більше 0, але RFC рекомендує, щоб довжина секрету становила щонайменше 16 байт. Ця вимога пов'язана з тим, що таємницю такої довжини практично неможливо зламати атакою грубої сили.

Клієнт створює пакет Access-Request, що містить принаймні ім'я користувача та пароль. Ідентифікатор пакету Access-Request генерується клієнтом. Зазвичай це звичайний лічильник, який виставляється за рахунок кожного нового запиту. Пакет Access-Request містить аутентифікатор запиту, який є випадково вибраним 16-байтовим рядком. Запит на доступ повністю захищений, за винятком атрибута User-Password, який захищений наступним механізмом. Клієнт і сервер діляться секретом. Результат конкатенації спільного пароля та автентифікатора запиту хешується за допомогою MD5 для отримання значення 16 байт, до якого додається за модулем пароль користувача. Якщо пароль користувача перевищує 16 байт, додаткові обчислення MD5 виконуються за допомогою зашифрованого блоку пароля користувача замість автентифікатора запиту.

Сервер отримує пакет запитів на доступ і перевіряє, чи має сервер спільний пароль для вказаного клієнта. Це робиться шляхом доступу сервера до бази даних (текстові файли, сервери LDAP тощо. Вони можуть служити альтернативною базою даних). Якщо відповідний клієнт не отримує таку розподілену таємницю, запит

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

просто відхиляється. Якщо поле RequestAuthenticator відсутнє або його неможливо перевірити в повідомленні клієнта, сервер також відхиляє запит.

Наступним кроком сервер використовує свою базу даних автентифікації для перевірки імені користувача та пароля. База даних RADIUS зберігає інформацію про користувача (ім'я, пароль) та дані сеансу (загальний час сеансу та статистику трафіку, що входять до / з користувача). Якщо пароль правильний або ім'я користувача відсутнє в базі даних сервера, сервер створює пакет Access-Accept, який слід відправити назад клієнту. Якщо пароль неправильний, сервер створює пакет Access-Reject для надсилання назад клієнту. Це повідомлення може супроводжуватися текстовим повідомленням, що обґрунтовує відмову. Пакети Access-Accept та Access-Reject використовують однаковий ідентифікатор пакета Access-Request, надісланого клієнтом. Сервер також розміщує Response Authenticator у полі Authenticator. Аутентифікатор відповіді - це результат хеш-функції MD5, вхідним сигналом якої є пакет відповідей сервера із відповідним аутентифікатором запиту та загальним секретом:

$$\text{Response Authenticator} = \text{MD5}(\text{Code} + \text{ID} + \text{Length} + \text{RequestAuthenticator} + \text{Attributes} + \text{Secret}), (1.1)$$
 де RequestAuthenticator – автентифікатор запросу;

Secret – спільний секрет клієнта та сервера.

Коли клієнт отримує пакет відповідей від сервера, він намагається зіставити його із своїм запитом за допомогою поля ID. Якщо клієнт не надіслав запит, але отримав відповідь, така відповідь відхиляється. В іншому випадку клієнт перевіряє автентифікатор відповіді, використовуючи ті самі розрахунки, що і у формулі (1.1), а потім порівнює результат із полем Authenticator із відповіді сервера. Якщо вони не збігаються, пакет відповідей із сервера відкидається. Якщо клієнт отримує пакет Access-Accept, ім'я користувача та пароль є дійсними, а користувача аутентифіковано. Якщо клієнт отримує підтверджене повідомлення про відмову в доступі, ім'я користувача та пароль вважаються недійсними, а користувач не аутентифікований.

		Леценко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

У RADIUS процеси авторизації та аутентифікації пов'язані, тому, як тільки аутентифікація буде виконана, користувач автоматично отримує авторизацію в системі.

1.5 Механізм аудиту протоколу RADIUS

Процес аудиту в протоколі RADIUS виконується незалежно від аутентифікації та авторизації. Аудит протоколу описаний у RFC2866. Аудит дозволяє передавати дані на початку та в кінці сесії із зазначенням кількості ресурсів, використаних під час сесії. Такими ресурсами можуть бути час, пакети, байти тощо.

Основною метою процесу аудиту є облік користувача щодо використовуваного доступу до мережі для цілей статичного та загального моніторингу мережі.

Коли NAS надає користувачеві доступ до мережі, він надсилає запис Accounting Start на сервер, щоб повідомити серверу про те, що користувач почав використовувати мережеві ресурси. Accounting Start - це пакет запитів на проводку, який має значення атрибуту Acct-Status-Type у значенні "start". Цей пакет зазвичай містить інформацію про ідентифікацію користувача, його мережеву адресу, точку доступу та унікальний ідентифікатор сеансу.

Періодично під час сеансу NAS може надсилати проміжні записи оновлення на сервер для оновлення стану поточного сеансу. В тілі таких пакунків атрибуту Acct-Status-Type встановлено значення "проміжне оновлення". Проміжні пакети зазвичай надсилають інформацію про тривалість поточного сеансу та використання даних.

Нарешті, коли сеанс припиняється і доступ користувача до мережі припиняється, NAS надсилає на сервер запис зупинки обліку, що містить інформацію про час сеансу, переданий пакет, передані дані, причину відключення та іншу інформацію, пов'язану з доступом користувача до мережі. Атрибут Acct-Status-Type у цьому записі встановлено на "зупинка". Зазвичай клієнт продовжує надсилати пакети Accounting-Request, поки не отримає пакет Accounting-Response від сервера.

Обчислення вмісту пакету Access-Request відрізняється від обчислення пакета Accounting-Request. На відміну від Request Authenticator у пакеті

		Леценко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

AccessRequest, значення Request Authenticator у пакеті Authenticator-Request не є випадковим і обчислюється згідно з RFC 2866 згідно з формулою (1.2).

$$\text{Response Authenticator} = \text{MD5}(\text{Code} + \text{ID} + \text{Length} + 16 \text{ нульових байтів} + \text{Attributes} + \text{Secret}),$$
 (1.2) де Secret – спільний секрет сервера та клієнта.

Таким чином, сервер може перевірити запит на розрахунки та відкинути пакет, якщо при перетворенні того самого значення на стороні сервера результат не збігається з отриманим від клієнта. У більшості випадків це пов'язано з неправильним спільним паролем.

1.6 Аналіз вразливостей протоколу RADIUS

Сервер RADIUS підтримує кілька протоколів автентифікації. Найчастіше використовуються PAP (Password Authentication Protocol), протокол автентифікації CHAP (Challenge Handshake Authentication Protocol) та перша або друга версія протоколу MS-CHAP (MS-CHAPv2), доступ до сервера клієнт-сервер 802.1X (EAP, EAP-TLS, PEAP, EAP-TTLS, EAP-MD5, EAP-GTC, LEAP), аутентифікація HTTP. Крім того, можна використовувати RADIUS з протоколом Point-to-Point. Коли сервер RADIUS надається спільно з усіма вищезазначеними протоколами, результати автентифікації користувача та сервера доступу надсилаються на сервер RADIUS, який приймає рішення про автентифікацію користувача.

Безпека цього алгоритму базується на хеші MD5. MD5 - це 128-розрядний алгоритм хешування, розроблений у 1991 році. На момент розробки протоколу хеш MD5 вважався безпечним, але на наш час, згідно з RFC 6151, алгоритм вважався ненадійним. В даний час існує кілька типів злому хеш-алгоритму MD5:

1. Метод грубої сили. Це підхід, який передбачає перегляд усіх можливих входних значень, поки не отримається потрібний хеш.
2. Використання райдужних таблиць. Райдужна таблиця – це попередньо обчислена таблиця для інвертування хеш-функцій, як правило, для пошуку хешей паролей.

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

3. Колізія хеш-функції. Під колізією розуміють отримання одного і того ж результату обчислення хеш-функції з різними вхідними даними.

Крім того, RADIUS має вразливі місця безпеки, що виникають як через сам протокол, так і через погану реалізацію клієнта.

Однією з основних проблем протоколу, що призводить до можливості багаторазових атак на конкретний протокол, є відсутність перевірки на стороні сервера джерела вхідних повідомлень про доступ-запит. Сервер перевіряє запит на доступ з IP-адреси для налаштованого клієнта RADIUS, але IP-адреси можна легко підробити.

Рішенням цієї проблеми є використання атрибута Message-Authenticator у пакетах Access-Request. Цей атрибут визначений у RFC 3579. Він використовується для перевірки пакета Access-Request на стороні сервера та містить код автентифікації повідомлень на основі хешу (HMAC), який служить механізмом перевірки цілісності інформації для забезпечення того, що дані, надіслані від клієнта на сервер, не були змінені третіми сторонами, тобто запобігання нападу, який опосередковується людиною.

Перед відправкою пакету Access-Request клієнт обчислює MD5 HMAC з даних пакета, який він має намір надіслати на сервер, і додає отримане хешзначення як атрибут Message-Authenticator. Зі свого боку, сервер перевіряє поле Message-Authenticator, виконуючи ті самі дії. Якщо пакет не був протестований на стороні сервера, сервер повинен скинути пакет. Формула для обчислення атрибута Message-Authenticator така:

Message-Authenticator = HMAC-MD5 (Type, Identifier, Length, Request Authenticator, Attributes) (1.3)

Цей атрибут повинен використовуватися для будь-якого пакету, що містить повідомлення розширеного протоколу автентифікації. Атрибут необов'язковий для інших протоколів.

Звернемо увагу, що перший пакет у сеансі 802.1x RADIUS ніколи не містить повідомлення EAP. У цьому випадку поле Message-Authenticator не генерується, і

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

неможливо перевірити клієнтський пакет на стороні сервера. Але клієнт все ще може перевірити відповідь сервера за допомогою поля Request Authenticator.

Відомі наступні атаки на конкретний протокол:

1. Атака, отримана розподіленим секретом за допомогою атрибута логін-пароль.

Зловмисник може отримати спільну секретну інформацію про пароль, якщо зможе контролювати мережевий трафік. Це полягає в наступному: зловмисник намагається здійснити автентифікацію, надіславши клієнту будь-який пароль. Потім зловмисник перехоплює пакет запитів на доступ, який клієнт надсилає на сервер для перевірки облікових даних користувача, та виконує операцію XOR, операндами якої є пароль, за допомогою якого він намагався автентифікуватися, та атрибуту зашифрованого пароля входу з захопленого пакету запиту на доступ. Таким чином, він отримує значення MD5 (загальний секрет + аутентифікатор запиту) та аутентифікатор запиту, і може обчислити значення спільного секрету.

2. Атака на отримання пароля за допомогою пари атрибутів логін-пароль.

Спочатку зловмисник намагається пройти автентифікацію, використовуючи валідне ім'я користувача та будь-який пароль. Наступним кроком атакуючий перехоплює пакет Access-Request, що надходить від клієнта до сервера, та визначає результат MD5(спільний секрет + автентифікатор запиту), як в попередній атаці. Далі зловмисник може відсилати на сервер від імені клієнта пакети Access-Request, використовуючи автентифікатор запиту та MD5(спільний секрет + автентифікатор запиту) та перебирати паролі, при цьому змінюючи значення атрибуту логін-пароль, до тих пір, поки не буде отриманий пакет Access-Accept від сервера, тобто знайдений відповідний логіну пароль. Ця атака можлива за умови відсутності обмежень на кількість запитів на стороні сервера від клієнта. Також для цього виду атаки необхідно, щоб довжина паролю становила менше, ніж 16 символів, оскільки механізм потокового шифру пари логін-пароль використовує зашифровані на минулому етапі дані, якщо ті перевищують 16 байтів виводу. Будь-яка потужна автентифікація, наприклад двухфакторна автентифікація, унеможлиблює цю атаку.

		Леценко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

Рівень безпеки RADIUS залежить від генерації модуля Request Authenticator. Аутентифікатор запитів повинен бути унікальним та непередбачуваним. Багато реалізацій протоколів використовують ненадійні генератори псевдовипадкових чисел для отримання автентифікатора запитів. Для проведення наступних двох атак зловмисникові потрібно, щоб клієнт згенерував певне значення автентифікатора запитів. Зазвичай це не є серйозною проблемою, оскільки це поле не було розроблено як функція захисту. Протокол не описує процес генерації автентифікатора запитів, але найпоширенішим способом його створення є збільшення одного байта для кожного нового запиту та використання цього лічильника як значення цього поля. Таким чином, зловмисник може надсилати додаткові запити, змушуючи лічильник збільшувати значення набагато частіше, ніж у звичайному режимі.

3. Пасивна компрометація пари атрибутів логін-пароль завдяки повторюваному значенню Request Authenticator. Якщо зловмисник міг контролювати трафік між клієнтом та сервером RADIUS, він міг створити словник, де кожне значення автентифікатора запиту асоціюється із захищеною парою атрибутів логін-пароль. Якщо зловмисник помітить повторну автентифікацію запиту для двох запитів, загальне секретне значення не матиме значення, оскільки XOR двох відомих пар логін-пароль може призвести до перших 16 байт незахищених паролів, для яких використовується операція XOR:

Успішність цієї атаки залежить від вимог до вибору користувачів паролів. Якщо всі користувачі обрали випадкові паролі однакової довжини, зловмисник не зможе нічого отримати з вилучених даних. Це досі малоімовірне явище. На практиці зазвичай зустрічаються випадки, коли користувачі вибирають паролі різної довжини (як правило, менше 16 символів) та різного ступеня випадковості.

Найпростішим випадком отримання паролів зі знайденого результату операції XOR є випадок, коли паролі значно відрізняються за довжиною. У цьому випадку один з паролів має більше символів, тому символи цього пароля, які виходять за рамки довжини іншого пароля, будуть незмінні (тобто ці символи будуть результатом операції XOR з 0). Це призводить до того, що символи, що не перекриваються довшим паролем, піддаються дії зловмисника без аналізу.

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Більш складним є випадок, коли зломисник припускає, що користувачі обрали паролі з низькою ентропією. У цій ситуації можна здійснити атаку за словником, керуючись статистичним аналізом тих біт, що перекриваються у двох паролів.

Навіть паролі довші за 16 символів підпадають під цю атаку, оскільки зломисник все одно отримує інформацію про перші 16 символів пароля.

4. Активна компрометація пари атрибутів логін-пароль завдяки повторюваному значенню Request Authenticator.

Ця атака зводиться до того, що зломисник пробує багато разів пройти автентифікацію, використовуючи різні значення паролів, кожного разу перехоплюючи згенерований клієнтом пакет Access-Request, отримуючи автентифікатор запиту та відповідну йому захищену пару логін-пароль. Наступним кроком атакуючий отримує значення MD5(спільний секрет + автентифікатор запиту), здійснюючи операцію XOR над паролем, який використовувався при спробах автентифікації та захищеним атрибутом логін-пароль. Зломисник генерує словник значень, де кожному автентифікатору запиту ставиться у відповідність значення MD5(спільний секрет + автентифікатор запиту).

Коли зломисник перехоплює валідний пакет Access-Request, який містить значення автентифікатора запиту, що присутнє у його словнику, він може здійснити операцію XOR над захищеною парою логін-пароль та значенням MD5(спільний секрет + автентифікатор запиту), що знаходиться у його словнику, таким чином отримуючи значення паролю.

5. Атака на повторення відповідей від сервера за допомогою повторюваного Request Authenticator.

Зломисник може скласти словник, де кожному Request Authenticator та ідентифікатору ставиться у відповідність пакет з відповіддю від сервера. Коли зломисник бачить запит, у якому знаходиться Request Authenticator та пов'язаний з ним ідентифікатор, який присутній у словнику, він може маскуватися як сервер та відсилати відповідь клієнту, яку він спостерігав раніше при складанні словника.

		Леценко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

Більш того, якщо серед відповідей сервера у словнику міститься хоч один пакет Access-Accept, зломисник може здійснити спробу проходження автентифікації, змусивши клієнта створити пакет Access-Request з тим самим Request Authenticator та ідентифікатором, що у словнику відповідають пакету Access-Accept, а потім підмінити відповідь від сервера на ту, що знаходиться у словнику, таким чином успішно підтвердити автентифікацію клієнта, насправді не знаючи пароля.

6. DOS атака, що можлива завдяки передбачуваному значенню Request Authenticator.

Завдяки тому, що зломисник може передбачати майбутні значення Request Authenticator, він може діяти як клієнт та створити словник майбутніх значень Request Authenticator та пов'язаних з ними відповідей сервера. Наступним кроком зломисник від імені сервера на кожен клієнтський запит Access-Reject, створюючи таким чином відмову в обслуговуванні.

7. Атака переговорів (Negotiation attack).

У ході цієї атаки NAS, RADIUS проксі-сервер або RADIUS сервер атакуючого намагаються змусити хост, який забезпечує процес автентифікації вибрати менш безпечний метод автентифікації. Наприклад, сеанс автентифікації, що використовує EAP, замість цього буде використовувати CHAP або PAP; з'єднання, яке було встановлено за допомогою EAP-TLS, під час цієї атаки може бути здійснено за допомогою MD5-Challenge і т.д. Захист від переговорних атак вимагає усунення низхідних переговорів. RADIUS може бути додатково захищений за допомогою IPsec. В якості альтернативи, якщо IPsec не використовується, уразливість можна зменшити за допомогою реалізації політики на з'єднання з боку аутентифікуючого однорангового користувача та політики для однорангового користувача з боку RADIUS серверу. Для автентифікаційного однорангового пристрою політику автентифікації слід встановити на основі кожного з'єднання. Політика щодо підключення дозволяє одноранговому партнеру, що аутентифікується, узгоджувати потужний метод EAP при підключенні до однієї служби, у той час як узгоджувати більш слабкий метод EAP для іншої служби.

		Леценко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

Крім того, однією із слабких сторін стандарту протоколу є те, що він дозволяє спільно використовувати один і той же пароль із кількома клієнтами, щоб один вразливий клієнт міг взяти під контроль кілька комп'ютерів. Усі клієнти RADIUS з однаковим загальним секретом можуть розглядатися як один клієнт RADIUS для всіх вищезазначених атак, оскільки жоден механізм захисту протоколу не використовує адресу клієнта або іншу унікальну інформацію у своїй роботі.

Обмеження, що існують у структурі спільних секретів, також можуть вплинути на позицію безпеки. Більшість реалізацій клієнта та сервера дозволяють вводити лише загальні секрети у вигляді рядків ASCII. Є лише 94 різних символів ASCII, які можна ввести зі стандартної американської клавіатури (з 256 можливих). Багато реалізацій протоколів також обмежують загальну довжину спільного секрету до 16 символів або менше. Обидва ці обмеження штучно зменшують розмір значень, які зломисник повинен шукати, щоб отримати загальний секрет.

1.7 Обхід 802.1x в LAN

1. Обхід MAB

Найпростіший метод обходу. MAB (MAC Authentication Bypass) взагалі начебто був придуманий спеціально для пентестерів. Навіть у назві є слово «Bypass».

Загалом, знаходимо старенький принтер (камеру, телефон ...), дізнаємося його MAC-адресу та відключаємо від комутатора. Змінюємо свій MAC на MAC пристрою та підключаємося замість нього. Останнім часом метод дещо втратив актуальність за рахунок використання профілювання

2. Класична атака (Bridged-based)

У 2005 році Стів Райлі, дослідник з Microsoft, виявив вразливість у протоколі 802.1x, яка призводила до можливості атак "Людина посередині". Суть уразливості полягала в тому, що автентифікація за протоколом 802.1x відбувається лише за умови встановлення нового з'єднання. Коли клієнт, що підключився до порту комутатора, проходить автентифікацію, порт переходить у стан «controlled» і всі подальші з'єднання від цього клієнта не потребують автентифікації. Зломисник, що

		Леценко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

розмістив хаб між клієнтом, що аутентифікувався, і портом комутатора, може підключити свій пристрій до хаба і відправляти пакети в мережу, підмінивши вихідні MAC- і IP-адреси на адреси легітимного клієнта.

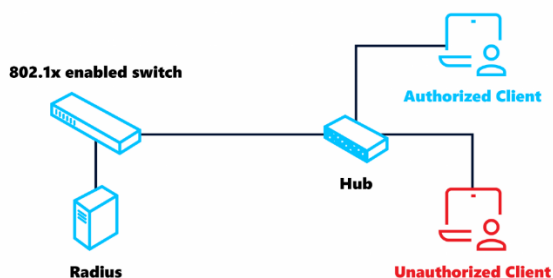


Рисунок 1.6 – Bridged-based attack

Очевидно, що така атака мала проблеми, пов'язані зі станом гонки. Якщо легітимний клієнт відповідав швидше, то нелегітимний втрачав з'єднання:

1. Хост зломисника відправляє SYN-пакет у мережу.
2. У відповідь приходить SYN/ACK, який попадає на обидва пристрої: і хост зломисника, і хост клієнта.
3. Клієнт відправляє RST/ACK.
4. Хост зломисника відправляє ACK.
5. Якщо клієнт встиг надіслати RST/ACK раніше, з'єднання розривається.

Тому в класичному варіанті атаки можна було надсилати лише UDP-трафік.

Логічним розвитком MITM-атаки стало використання мосту.

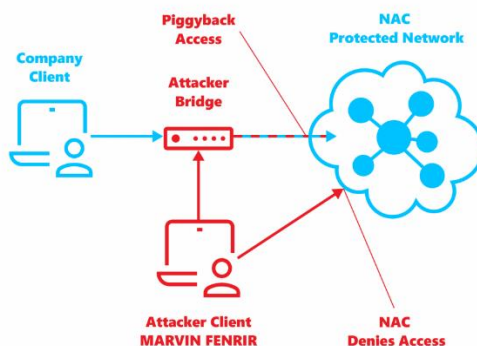


Рисунок 1.7 – Атака з використанням мосту

Алгоритм атаки

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

1. Нам знадобиться ноутбук з двома інтерфейсами і якийсь співробітник компанії (а точніше, його девайс).
2. Одним інтерфейсом підключаємось до девайсу, а іншим – до порту комутатора. Наступний план дій такий:
3. Дозволяємо форвардинг
4. Перекладаємо інтерфейси в Promisc-режим
5. Піднімаємо між ними міст і теж переводимо в Promisc-режим
6. MAC девайса міняємо на MAC комутатора
7. Налаштовуємо SNAT для пакетів, які відправляємо самі – вони мають виглядати так, ніби їх надіслав девайс.
8. Додається маршрут до мережі за комутатором через міст

3. Атака Rogue Gateway

Можна сказати, що це Evil Twin, тільки в LAN. Працює у випадку, якщо клієнт налаштований так, що з'єднання може бути встановлене навіть у разі невалідного сертифіката сервера. Наприклад, у налаштуваннях не варто галочка "Перевіряти сертифікат сервера".

Піднімаємо міст і починаємо слухати трафік. В результаті з'ясуємо параметри клієнта та автентифікатора: MAC- та IP-адреси, Маршрут за замовчуванням, Маска підмережі

Далі починається сама атака.

1. Піднімаємо підроблений RADIUS-сервер та вимикаємо інтерфейс, підключений до автентифікатора.
2. Потім надсилаємо на підроблений RADIUS-сервер кадр EAPOL-Start з MAC-адресою клієнта. В результаті, сервер відповідає клієнту запитом EAP-Request-Identity.
3. Якщо клієнт прийме сертифікат, він автентифікується у підробленого сервера.
4. Атакуючий прослуховує MS-CHAPv2-challenge та response, згенерований на основі NTLM-хешу пароля. У разі використання словникового пароля його можна отримати перебором за словником.

		Леценко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

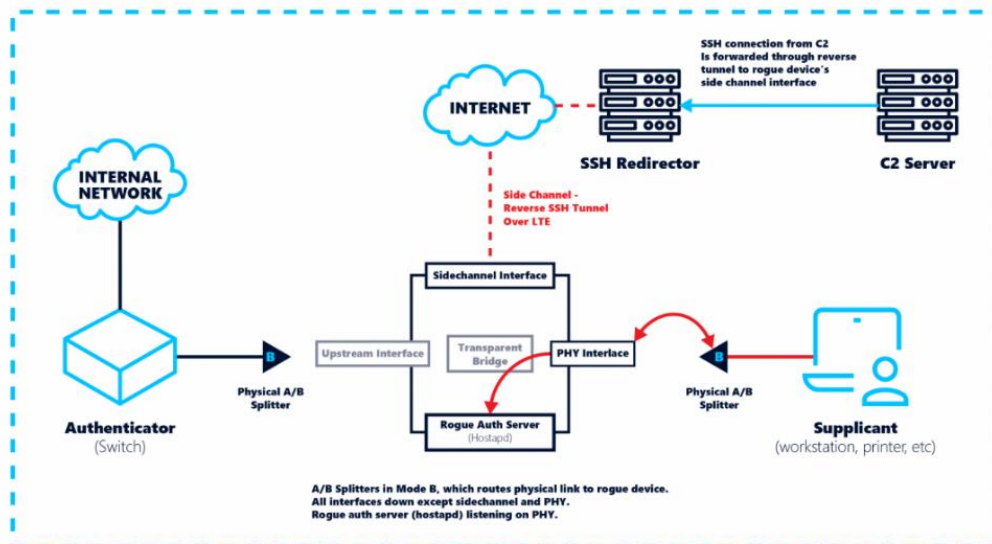


Рисунок 1.8 – Атака Rogue Gateway

Якщо атака пройшла успішно, можна відключити клієнта від мережі та авторизуватись з його даними.

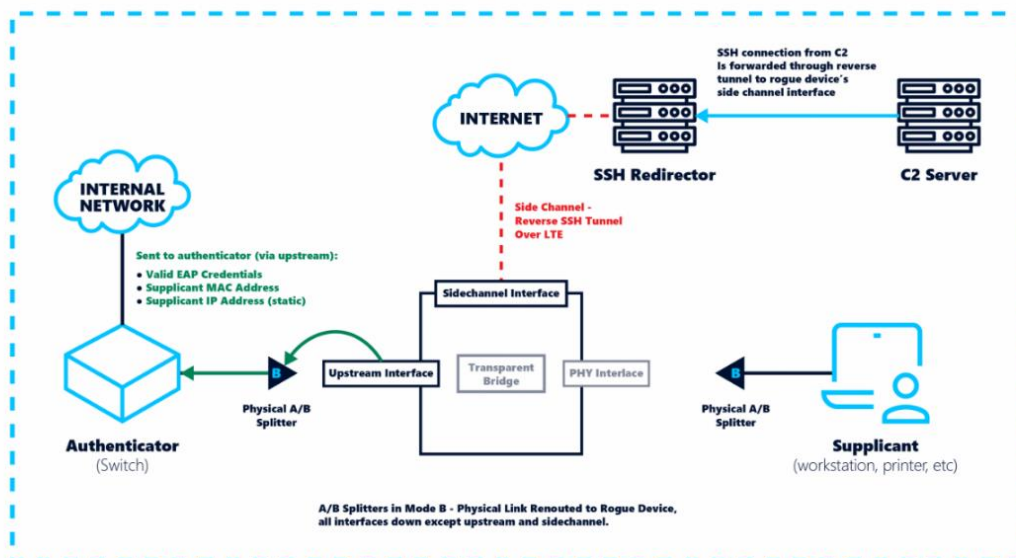


Рисунок 1.9 – Відключення клієнта

Як захиститись?

Для захисту від дурня обходу МАВ вигадали профілювання. Наприклад, у Cisco ISE є профілі для Windows, різних моделей принтерів і т.д. Якщо налаштована політика дозволяти доступ МАВ тільки принтерам, заміна MAC хакеру вже не

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

допоможе. Добре налаштоване профіль обійти досить складно, оскільки зловмисник не знає ні параметрів профілювання (які метрики збираються для ідентифікації пристрою), ні параметрів пристрою (точні значення цих метрик).

Що стосується захисту від атак на EAP, варто відмовитись від EAP-MD5 або використовувати досить сильні паролі. У випадку з EAP-TTLS/EAP-PEAP/EAP-TLS/EAP-TTLS необхідно примусово заборонити встановлення з'єднання, якщо сертифікат сервера є невалідним.

Для захисту від MITM-атак можуть допомогти різні види детекту аномалій у мережі. Якщо хакер, підключившись до порту, запустить брут або скан, неадекватну поведінку хоста можна буде легко виявити та заблокувати порт. Однак, чим тихіше поведеться хакер, тим складніше його виявити. Детект аномалій — річ хороша, але 100% захисту не дає. Для 100%-ного захисту від MITM-атак немає нічого кращого, ніж сейф шифрування. Наприклад, IPsec. А ще є 802.1xAE, також відомий як 802.1x-2010, що передбачає шифрування. Щоправда, вже після автентифікації.

1.8 Постановка технічного завдання

Призначенням данної дипломної роботи є налаштування та аналіз роботи мережі та автентифікації з використанням технологій протоколів 802.1x та RADIUS.

Висновки до розділу 1

В цьому розділі було розглянуто та досліджено інформацію про протоколи 802.1X, AAA та RADIUS. Знайдені та проаналізовані вразливості і проблеми реалізації протоколів RADIUS та 802.1x.

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ПРОЄКТУВАННЯ ТОПОЛОГІЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ

2.1 Розробка топології комп'ютерної мережі

Для демонстрації роботи аутентифікації, було обрано створити проєкт в емуляторі GNS3.

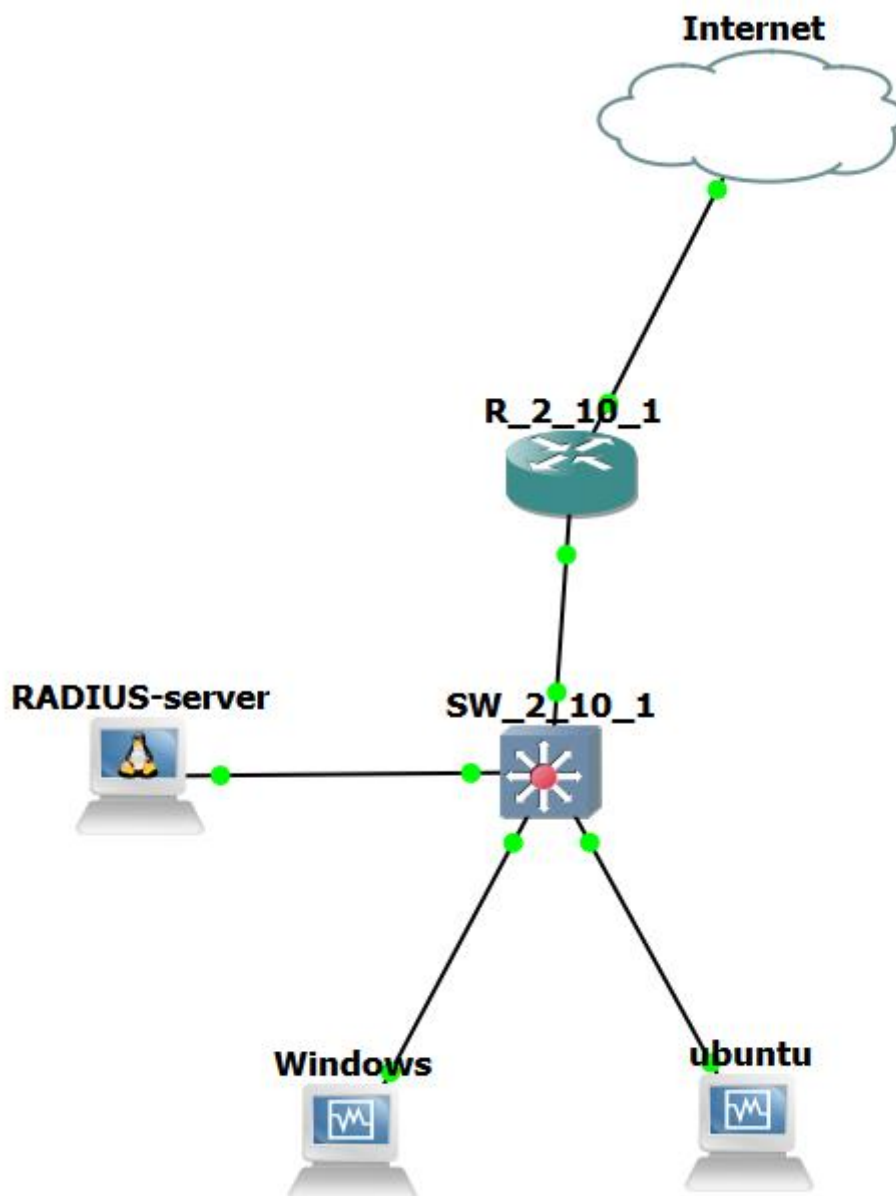


Рисунок 2.1 – Проєкт мережі

На рисунку 2.1 можемо побачити схему мережі з протоколом RADIUS та 802.1x. Для повноцінної роботи мережі, потрібно налаштувати RADIUS сервер, та клієнтів.

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

2.2 Налаштування мережевих клієнтів

```
R_2_10_1(config)#aaa new-model
R_2_10_1(config)#username andrew privilege 15 password cisco
R_2_10_1(config)#enable password cisco
R_2_10_1(config)#
```

Рисунок 2.2 – Налаштування маршрутизатора

Для початку було створенно користувача, який не входить до списку RADIUS, для того щоб мати змогу увійти, якщо виникнуть проблеми із сервером. Та вмикання протоколу AAA.

```
R_2_10_1(config)#radius-server host 192.168.1.254 auth-port 1812 acc
R_2_10_1(config)#$er host 192.168.1.254 auth-port 1812 acct-port 1813 k
R_2_10_1(config)#$2.168.1.254 auth-port 1812 acct-port 1813 key gns3
```

Рисунок 2.3 – Налаштування маршрутизатора

Далі було додано IP-адресу серверу для підключення до RADIUS сервера та вказані нові порти для підключення(1812 та 1813), оскільки за замовчуванням встановленні 1645 для автентифікації, та 1646 для аудиту, але FreeRadius працює за новою специфікацією. А також вказуємо спільний секретний ключ.

```
R_2_10_1(config)#aaa group server radius radiusgroup
R_2_10_1(config-sg-radius)#serv
R_2_10_1(config-sg-radius)#server192.168.1.254 auth-port 1812 acct-port 1813
^
% Invalid input detected at '^' marker.

R_2_10_1(config-sg-radius)#server 192.168.1.254 auth-port 1812 acct-port 1813
R_2_10_1(config-sg-radius)#exit
```

Рисунок 2.4 – Створення групи

Створюємо групу для визначення серверів AAA та об'єднання членів групи під один тип, тобто RADIUS. Також пов'язуємо цю групу із нашим сервером за ip-адресою uid номером порту.

```
R_2_10_1(config)#aaa authentication login default group radiusgroup local
R_2_10_1(config)#aaa authentication enable default enable
```

Рисунок 2.5 – Налаштування маршрутизатора

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

Налаштування що дає змогу перемкнутися на вхід під локальних користувачів, якщо не буде доступу до серверу.

2.3 Налаштування RADIUS сервера

Для роботи було обрано RADIUS сервер – FreeRadius. Цей програмний продукт, є альтернативою комерційним Radius-серверам. Має високу гнучкість та функціонал, модульність, підтримує усі сучасні EAP-автентифікаційні типи, має підтримку LDAP, MySQL, PostgreSQL, Oracle та багато інших баз даних. При цьому є програмою з відкритим кодом та вільним користуванням.

```
ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.254 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 fe80::c49b:9eff:fe50:4569 prefixlen 64 scopeid 0x20<lin
    ether c6:9b:9e:50:45:69 txqueuelen 1000 (Ethernet)
    RX packets 1197 bytes 89687 (89.6 KB)
    RX errors 0 dropped 7 overruns 0 frame 0
    TX packets 14 bytes 1076 (1.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Рисунок 2.6 – Налаштування IP-адреси

Першим ділом налаштовуємо IP-адресу для того, щоб можна було підключитися до сервера. Другим кроком буде створення облікових записів користувачів якими можна буде підключатися.

```
root@RADIUS-server:~# nano /etc/freeradius/3.0/ users
root@RADIUS-server:~# cat /etc/freeradius/3.0/users
alice    Cleartext-Password := "gns3"
        Reply-Message = "Hello, %{User-Name}"

bob      Cleartext-Password := "gns3"
        Reply-Message = "Hello, %{User-Name}"
```

Рисунок 2.7 – Створення користувачів

Останім кроком буде налаштування IP-адрес від яких можуть надходити запити для зіставлення інформації про облікові записи. Та встановлення секретного ключа.

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

```
client 0.0.0.0/0 {
    secret = gns3
    shortname = all_ipv4_clients
}
```

Рисунок 2.8 – Встановлення ір-адрес та секретного ключа

2.4 Налаштування протоколу 802.1x

```
SW_2_10_1(config)#aaa new-model
SW_2_10_1(config)#aaa authentication dot1x default group radius
SW_2_10_1(config)#int range e0/0-3
```

Рисунок 2.9 – Вмикання AAA

Перш ніж зануритися в реальні налаштування 802.1X, нам потрібно увімкнути автентифікацію, авторизацію та аудит (AAA) для комутатора. Оскільки здійснюється змінюється метод автентифікації після увімкнення AAA, який використовується лініями VTY (telnet), відповідно до моделі AAA. Необхідно також створити користувача для того, щоб мати змогу увійти, якщо щось піде не так.

```
SW_2_10_1(config)#username andrew secret cisco
```

Рисунок 2.10 – Створення користувача

Далі вмикаємо глобальну автентифікацію 802.1x на комутаторі. Та налаштуємо комутатор на використання авторизації RADIUS для всіх запитів, пов'язаних із мережею, наприклад ACL для кожного користувача або призначення VLAN.

```
SW_2_10_1(config)#dot1x system-auth-control
SW_2_10_1(config)#aaa authorization network default group radius
```

Рисунок 2.11 – Налаштування 802.1x

```
SW_2_10_1(config)#radius server radius
SW_2_10_1(config-radius-server)#add
SW_2_10_1(config-radius-server)#address ipv4 192.168.1.254 aut
SW_2_10_1(config-radius-server)#address ipv4 192.168.1.254 auth-port 1812 acc
SW_2_10_1(config-radius-server)#$1.254 auth-port 1812 acct-port 1813
SW_2_10_1(config-radius-server)#key gns3
SW_2_10_1(config-radius-server)#exit
SW_2_10_1(config)#ip radius source-interface e0/1
```

Рисунок 2.12 – Підключення до RADIUS сервера

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

І на останок вмикаємо 802.1x на інтерфейсах переводячи їх у режим доступу та вмикаючи автоматичний режим для роботи 802.1x. Також встановлюємо інтерфейси Port Access Entity, щоб вони діяли лише як аутентифікатори та ігнорували повідомлення, призначені для запитувача.

```
SW_2_10_1(config)#int range e0/0-3
SW_2_10_1(config-if-range)#swi
SW_2_10_1(config-if-range)#switchport m
SW_2_10_1(config-if-range)#switchport mode a
SW_2_10_1(config-if-range)#switchport mode access
SW_2_10_1(config-if-range)#authentication port-control auto
SW_2_10_1(config-if-range)#dot1x pae authenticator
SW_2_10_1(config-if-range)#exit
```

Рисунок 2.13 – Налаштування інтерфейсів

Таблиця 2.1 Параметри IP-адресації мережі

Мережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска	Пре фікс
Маршрутизатор R_2_10_1	Інтерфейс F0/1	192.168.1.1	255.255.255.0	/24
	Інтерфейс F0/0	DHCP		
Комутатор SW_2_10_1	Мережний адаптер	192.168.1.2	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.1	—	—
Робоча станція Ub- untu	Мережний адаптер	DHCP		
	Шлюз за замовчуванням			
Робоча станція Win- dows	Мережний адаптер			
	Шлюз за замовчуванням			
Сервер RADIUS- server	Мережний адаптер	192.168.1.254	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.1	—	—

Висновки до розділу 2

В другому розділі була досягнута мета розробки підсистеми локальної мережі. Було встановлено та налаштовано RADIUS сервер, та налагоджена робота протоколу 802.1x для авторизації на інтерфейсах.

РОЗДІЛ 3 ТЕСТУВАННЯ МЕРЕЖІ

3.1 Перевірка роботи мережі

Для початку необхідно перевірити роботу налаштованих протоколів 802.1x та RADIUS.

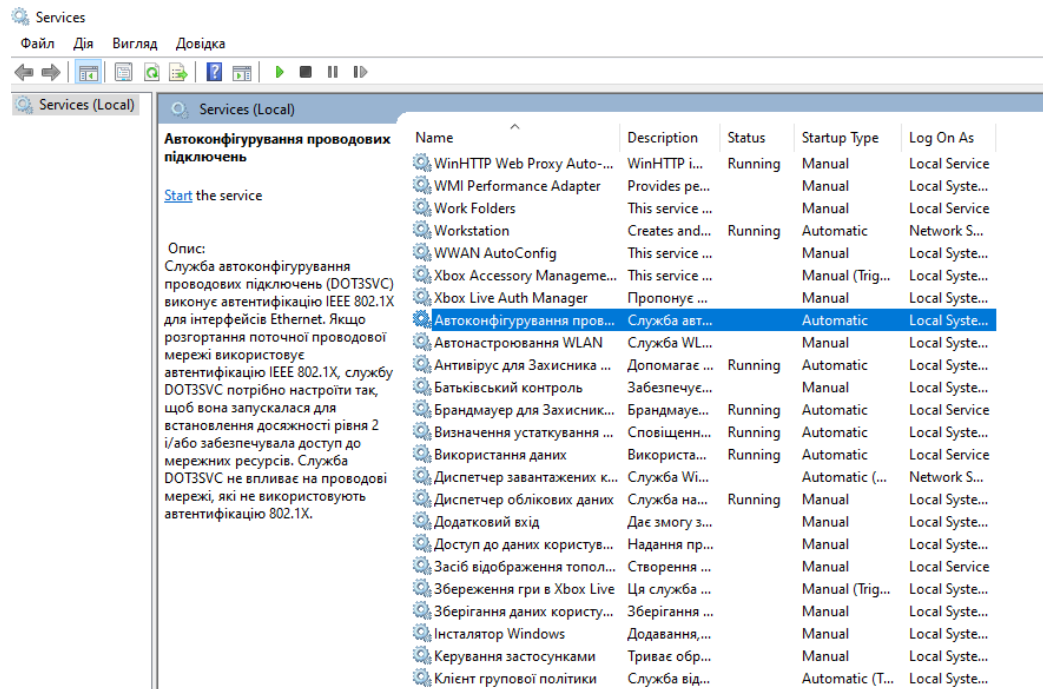


Рисунок 3.1 – Увімкнення служби

За замовчуванням в операційній системі Windows прихована інформація пов'язана із 802.1x, для початку роботи необхідно увімкнути службу «Автоконфігурування проводів інтерфейсів»

Ставимо режим на подальше автоматичне включення, та запускаємо службу.

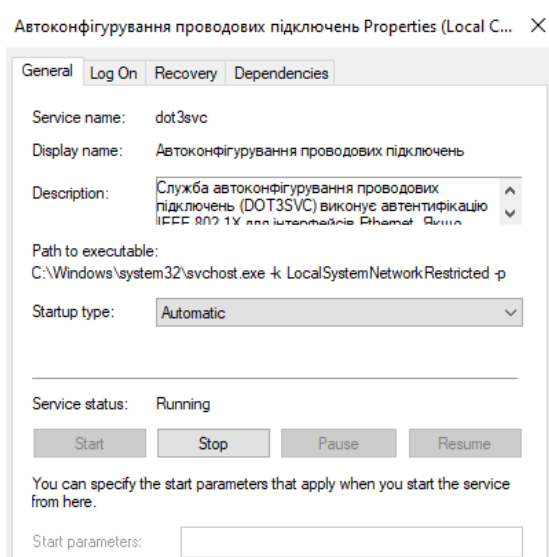


Рисунок 3.2 – Увімкнення служби

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Після запуску служби переходимо до налаштування мережного адаптера.

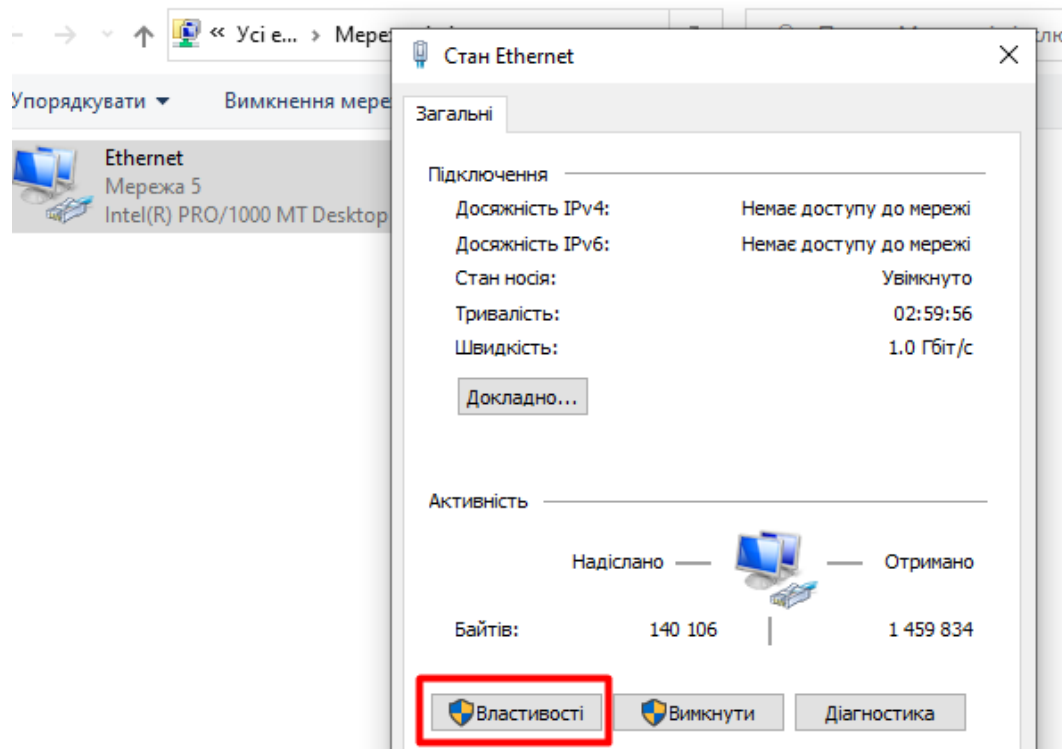


Рисунок 3.3 – Мережевий адаптер

Можемо побачити, що після того як увімкнули службу «Автоконфігурування проводових інтерфейсів», у властивостях мережевого адаптера з'явилася нова вкладка «Автентифікація».

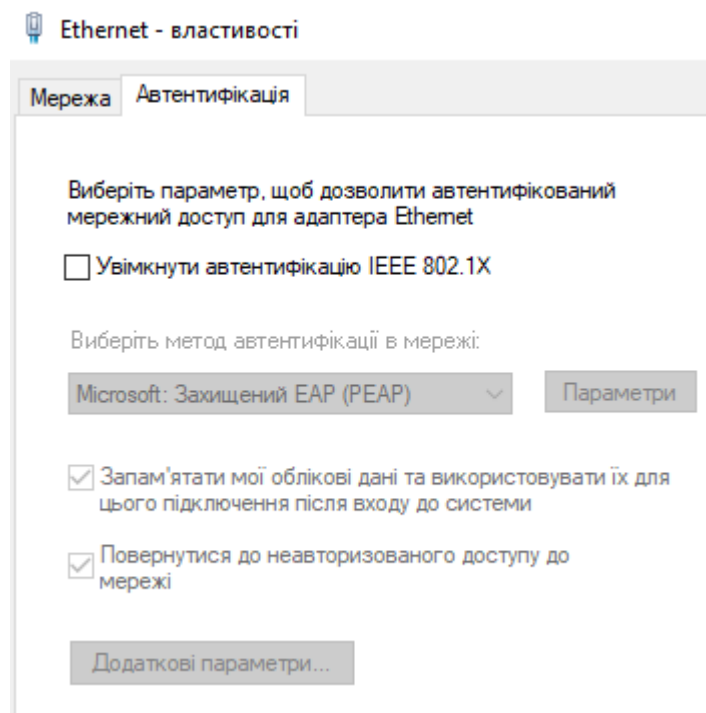


Рисунок 3.4 – Властивості мережевого адаптера

Вмикаємо автентифікацію IEEE 802.1x, вибираємо метод автентифікації та переходимо до параметрів методу.

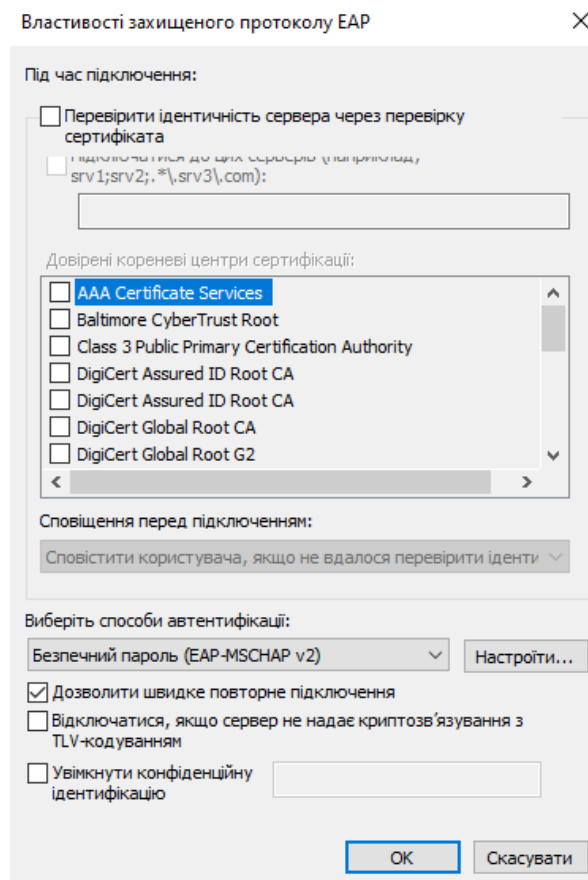


Рисунок 3.5 – Властивості захищеного протоколу EAP

Обираємо спосіб автентифікації, заходимо у налаштування та знімаємо прапорець про автоматичне використання імені входу та паролю Windows.

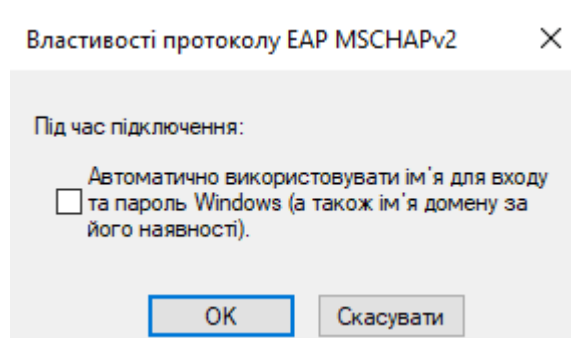


Рисунок 3.6 – Властивості протоколу EAP MSCHAPv2

Наступним кроком переходимо до додаткових параметрів автентифікації.

		Лещенко А.П.			KIK.KP.B – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

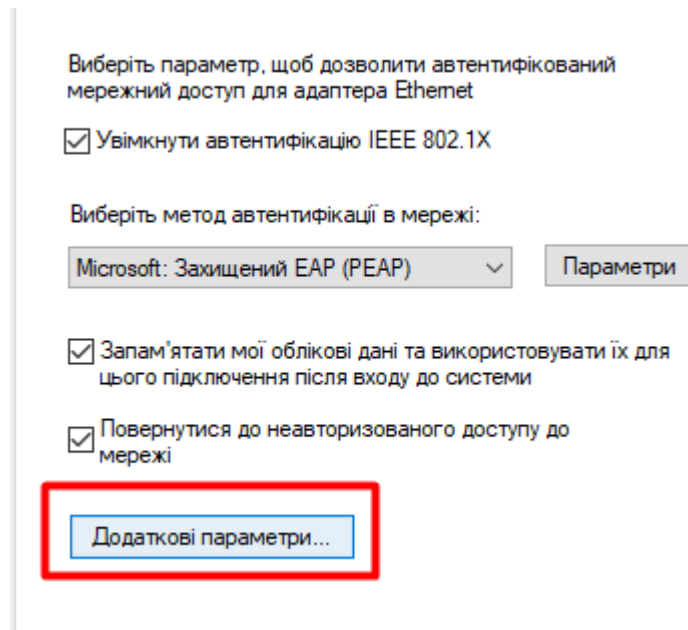


Рисунок 3.7 – Властивості мережевого адаптера

В меню додаткових параметрів ми ставимо прапорець про указання режиму автентифікації, змінюємо сам режим автентифікації на «Автентифікація користувача».

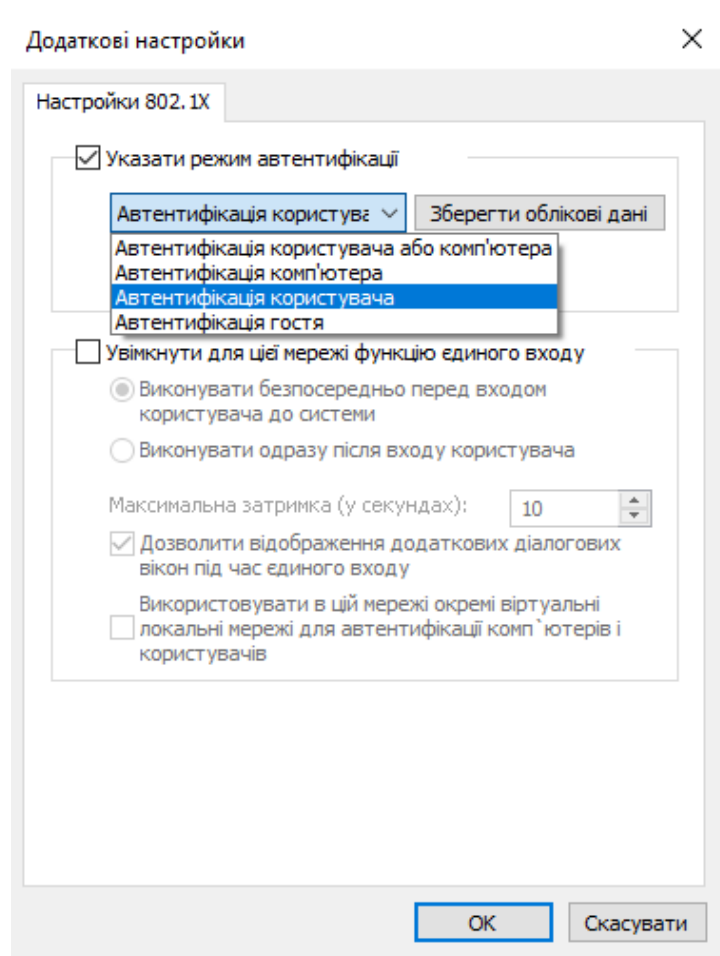


Рисунок 3.8 – Додаткові налаштування

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

Нажимаємо кнопку «Зберегти облікові дані», та вводимо їх після того як з'явиться відповідне віконце.

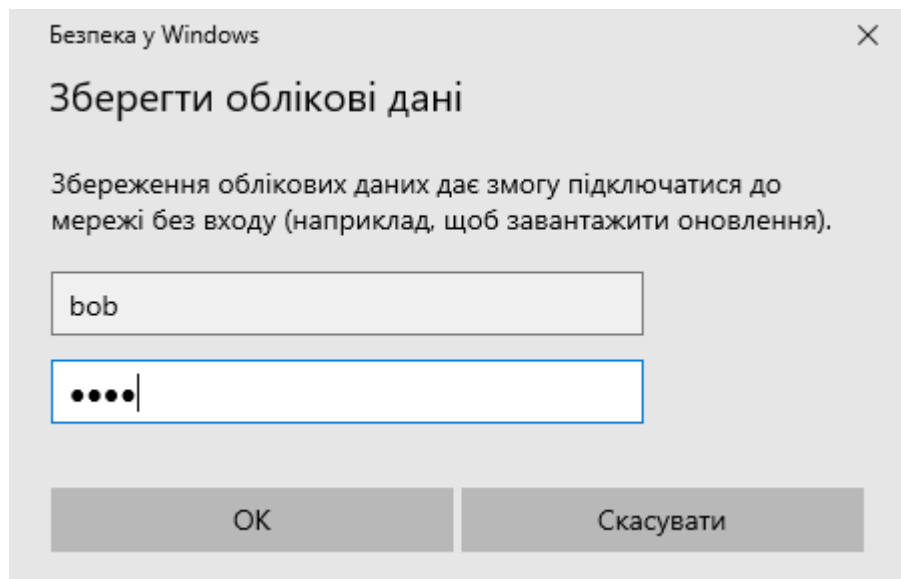


Рисунок 3.9 – Збереження облікових даних

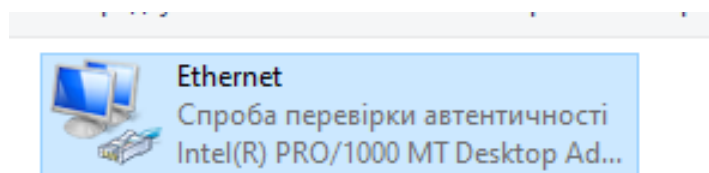


Рисунок 3.10 – Стан мережі

Після введення даних облікового запису можемо побачити, що пішов процес перевірки автентичності. Та на RADIUS сервер прийшов запит від клієнта про спробу авторизуватися.

```
2022-06-28 18:27:40.278797 (1) Access-Request Id 14 eth0:192.168.1.2:1645 -> 192.168.1.254:1812 +0.000
  User-Name = "bob"
  NAS-IP-Address = 192.168.1.2
  NAS-Port = 50003
  Service-Type = Framed-User
  Framed-IP-Address = 192.168.1.3
  Framed-MTU = 1500
  Called-Station-Id = "AA-BB-CC-00-01-30"
  Calling-Station-Id = "08-00-27-EF-F2-E9"
  NAS-Port-Type = Ethernet
  EAP-Message = 0x020b000801626f62
  Message-Authenticator = 0x8169671e9a39fa9bc5abcbfc2e1c955a
  NAS-Port-Id = "Ethernet0/3"
  Cisco-AVPair = "service-type=Framed"
  Cisco-AVPair = "audit-session-id=C0A80102000000B0000EBC5"
  Cisco-AVPair = "method=dot1x"
  Authenticator-Field = 0x8fcecfd90dc34604d545d745b0de2c7
```

Рисунок 3.11 – Запит клієнта

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

```

2022-06-28 18:27:40.278922 (2) Access-Challenge Id 14 eth0:192.168.1.2:1645 <- 192.168.1.254:1812 +0.000 +0.000
State = 0xf289ca50f285ce3eeb772eb3565a3ab8
EAP-Message = 0x010c0016041043b0341d3ac01281a70d6919d8644441
Message-Authenticator = 0x53fe3106aa913a024c5f66e487e88ee8
Authenticator-Field = 0x18a9c75edda93862b6ea8b61b4ca5faa
2022-06-28 18:27:40.281285 (2) Access-Request Id 15 eth0:192.168.1.2:1645 >- 192.168.1.254:1812 +0.000 +0.000

```

Рисунок 3.12 – Повідомлення із додатковою інформацією

```

2022-06-28 18:27:41.896912 (20) Access-Accept Id 23 eth0:192.168.1.2:1645 <- 192.168.1.254:1812 +1.618 +0.000
User-Name = "bob"
EAP-Message = 0x03140004
Message-Authenticator = 0xbca04282fb5796780f574db38cc0cf49
Attr-26.311.17 = 0x97ebc0d50bbce447f62ee2d6f1fcf587ad0bd08ddd2deda70964215149e93947ce91a6dbe15b3f72098442f36e3aef9b3ab3
Attr-26.311.16 = 0x9cee1620709192fdbbbd5d28c9dda1bacd4666a4bf3bd1754e1b26472a8422acf551c8a63c15d2563305d5215c64d7ebab7f
Authenticator-Field = 0xebff3df90524da51922f6fb5a4b75276

```

Рисунок 3.13 – Повідомлення про прийняття спроби авторизації

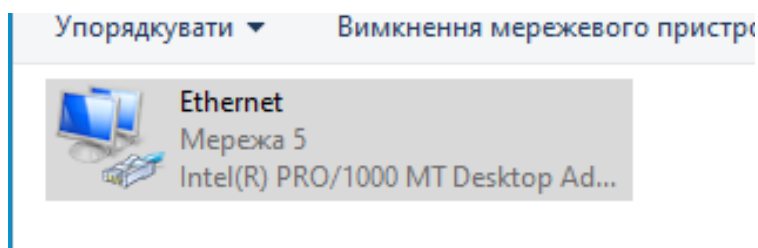


Рисунок 3.14 – Стан мережі

При введенні невірних даних, стан мережі зміниться на «Не вдалося виконати автентифікацію». Сервер відправить повідомлення про відмову в автентифікації.

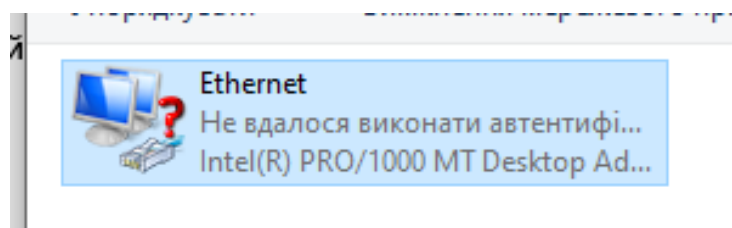


Рисунок 3.15 – Стан мережі

```

2022-06-28 18:35:02.756300 (18) Access-Reject Id 41 eth0:192.168.1.2:1645 <- 192.168.1.254:1812 +1.194 +1.001
EAP-Message = 0x04090004
Message-Authenticator = 0x5d24097c63e86e370f4c576d346601d9
Authenticator-Field = 0x482d476f09ddb94ac3627e621fa2f564

```

Рисунок 3.16 – Повідомлення про відмову

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

```

040 is being marked alive.
SW_2_10_1(config-if)#
*Jun 28 00:36:20.261: %DOT1X-5-FAIL: Authentication failed for client (0800.27ef
.f2e9) on Interface Et0/3 AuditSessionID C0A80102000000C00E2A689
SW_2_10_1(config-if)#

```

Рисунок 3.17 – Повідомлення про помилку

Та на комутаторі з'явиться повідомлення про невдачу спробу автентифікації, з вказанням часу, порту, MAC-адреси, та ID сесії.

Після вдалого підключення можна також перевірити наявність зв'язу між мережними пристроями.

```

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=4ms TTL=255
Reply from 192.168.1.1: bytes=32 time=8ms TTL=255
Reply from 192.168.1.1: bytes=32 time=16ms TTL=255
Reply from 192.168.1.1: bytes=32 time=18ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 18ms, Average = 11ms

C:\Users\Student>ping 192.168.1.254

Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time=6ms TTL=64
Reply from 192.168.1.254: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.1.254:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 6ms, Average = 4ms
Control-C
^C
C:\Users\Student>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time=3ms TTL=255
Reply from 192.168.1.2:

```

Рисунок 3.18 – Перевірка зв'язку

Більшість дистрибутивів Linux підтримують 802.1X через wpa_supplicant та інтеграцію з робочим столом, як-от NetworkManager. Тому з підключення машини зі встановленою операційною системою Linux, швидше та легше.

Першим ділом заходимо у налаштування та переходимо до пункту мережі.

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

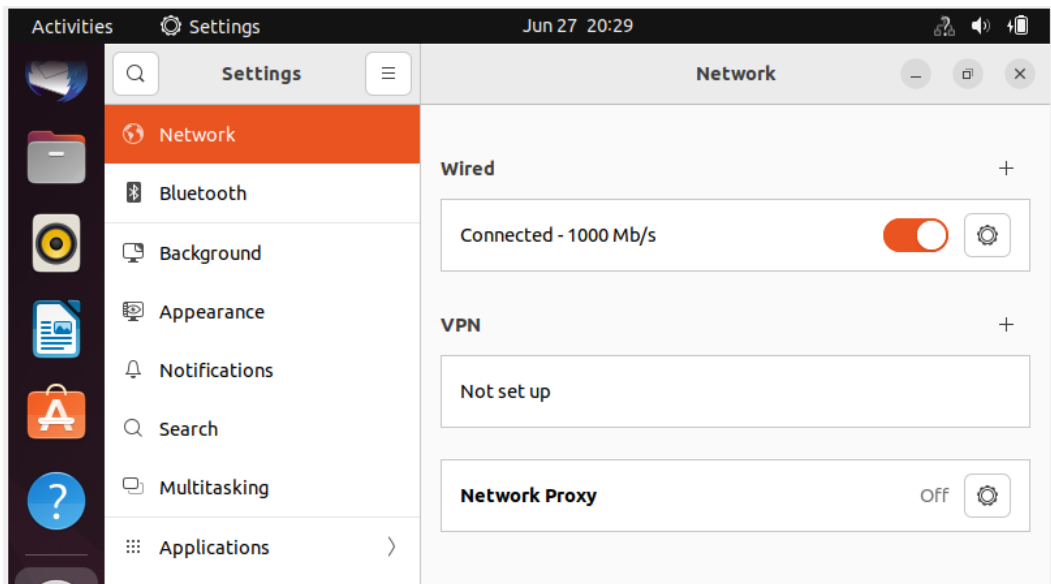


Рисунок 3.19 – Меню налаштувань

Наступне, що потрібно зробити це перейти до налаштувань, свого з'єднання і там перейти на вкладку безпеки.

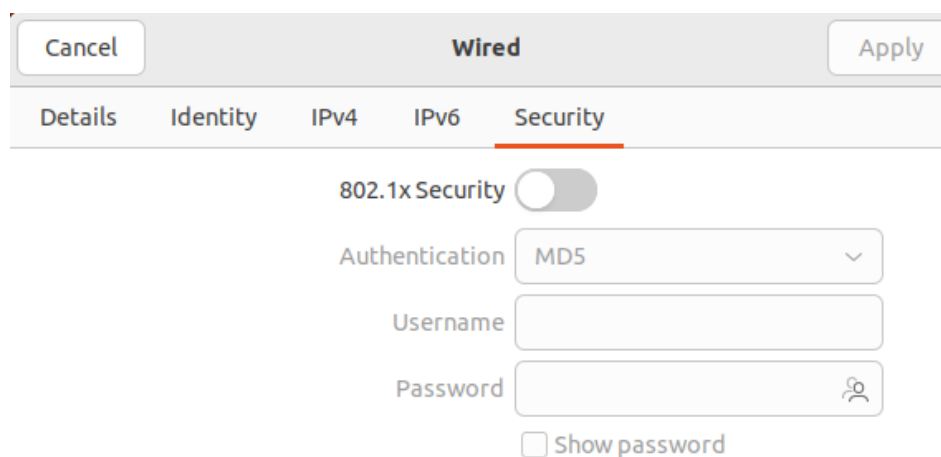


Рисунок 3.20 –Налаштування безпеки

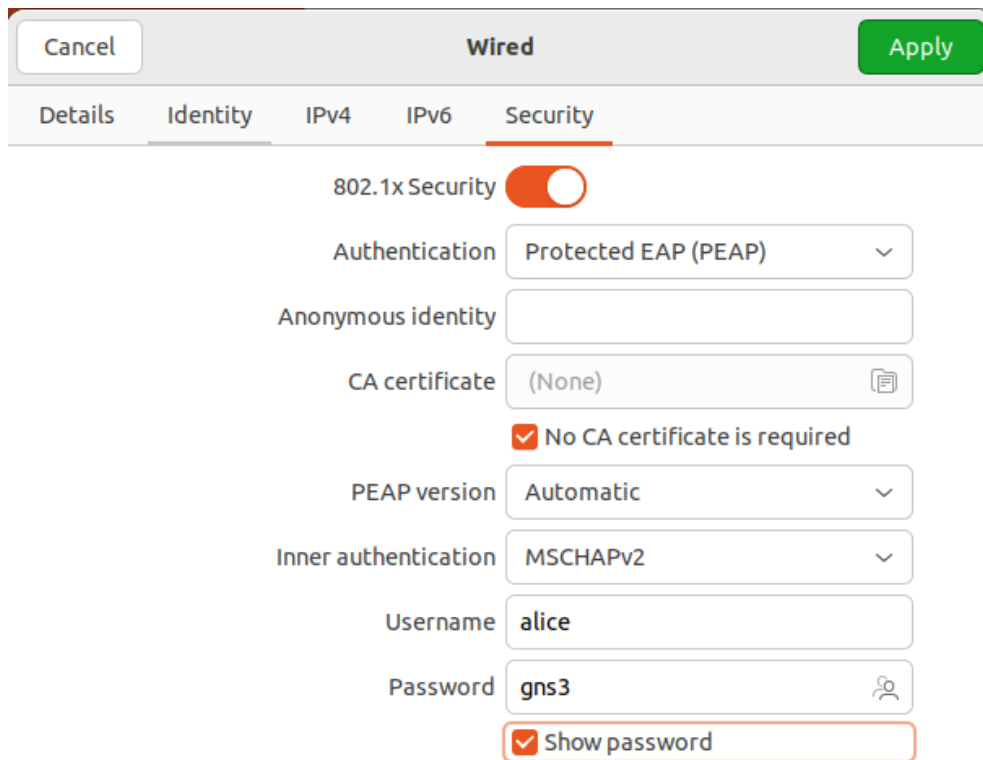


Рисунок 3.21 – Налаштування автентифікації

Також як і раніше в Windows, спочатку вмикаємо можливість автентифікації через 802.1x, обираємо метод та спосіб автентифікації, вводимо дані облікового запису користувача та нажимаємо прийняти.

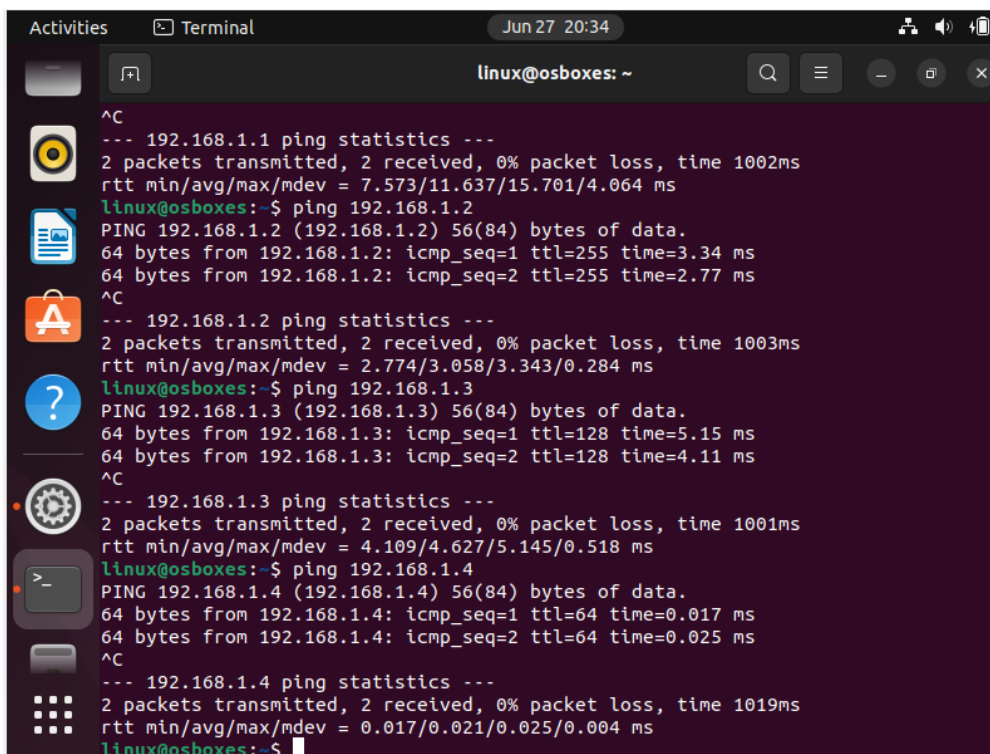


Рисунок 3.22 –Перевірка зв'язку

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

Після вдалої перевірки зв'язку також можна перевірити можливість використання RADIUS сервера для підключення до мережних пристроїв із використанням віддаленого доступу.

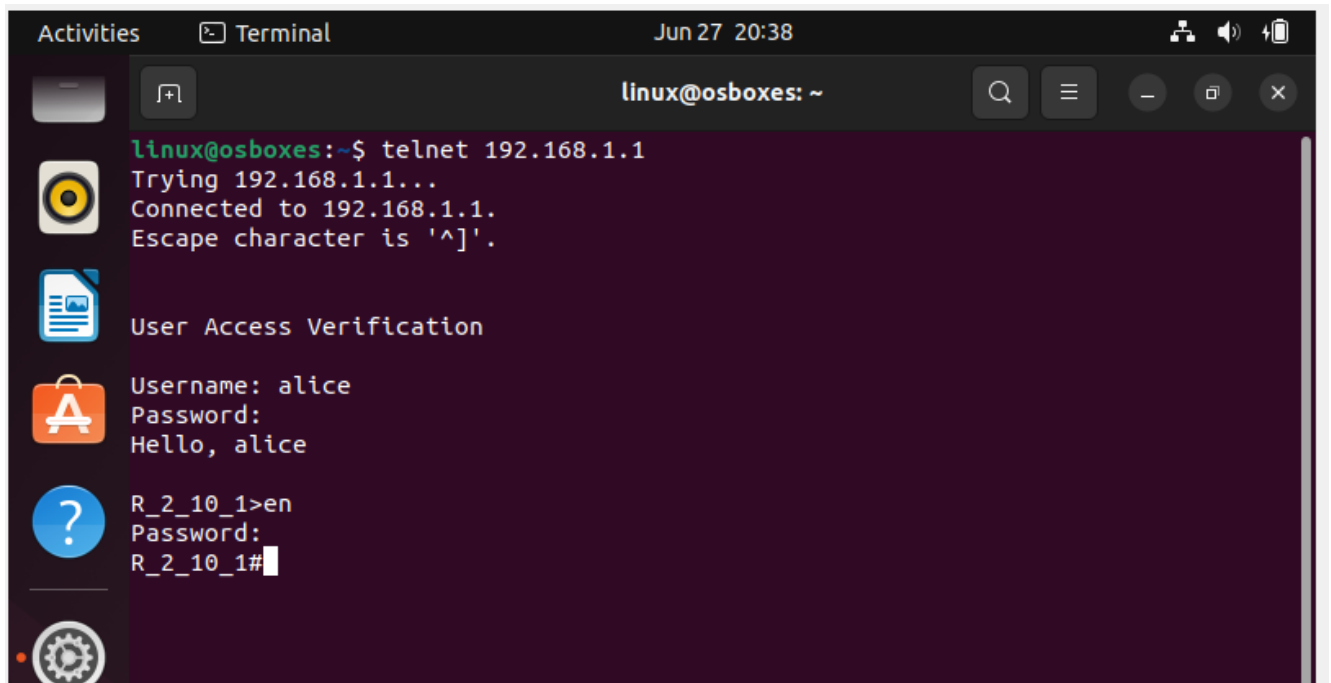


Рисунок 3.23 – Перевірка можливості підключення за допомогою віддаленого доступу

Висновки до розділу 3

В цьому розділі було протестовано мережу на коректність налаштувань, перевірка працездатності та розглянуто особливості роботи протоколів RADIUS та 802.1x.

		Лещенко А.П.			KIK.KP.B – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

В першому розділі було розглянуто та досліджено інформацію про протоколи 802.1X, AAA та RADIUS. Знайдені та проаналізовані вразливості та проблеми реалізації протоколів RADIUS та 802.1x. Було сформоване уявлення про поставлене завдання.

В другому розділі була досягнута мета розробки підсистеми локальної мережі. Було встановлено та налаштовано RADIUS сервер за допомогою програмного забезпечення FreeRadius, та налагоджена робота протоколу 802.1x для авторизації на інтерфейсах.

В третьому розділі було протестовано мережу на коректність налаштувань, перевірка працездатності та розглянуто особливості роботи протоколів RADIUS та 802.1x.

В результаті було отримано навички роботи та розробки мережі із використанням технології протоколів 802.1x та RADIUS.

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. – 6-е изд. / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2020.
2. RFC 6151. Updated Security Considerations for the MD5 MessageDigest and the HMAC-MD5 Algorithms. [Електронний ресурс] – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc6151>
3. RFC 2865. Remote Authentication Dial In User Service (RADIUS). [Електронний ресурс] – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc2865>
4. RFC 2866. RADIUS Accounting. [Електронний ресурс] – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc2866>
5. RFC 3579. RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP). [Електронний ресурс] – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc3579>
6. RFC 3748. Extensible Authentication Protocol (EAP). [Електронний ресурс] – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc3748>
7. RFC 5931. Extensible Authentication Protocol (EAP) Authentication Using Only a Password. [Електронний ресурс] – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc5931>
8. RFC 2989. Criteria for Evaluating AAA Protocols for Network Access. [Електронний ресурс] – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc2989>
9. RFC 2903. Generic AAA Architecture. [Електронний ресурс] – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc2903>
10. RFC 4764. RADIUS Accounting. [Електронний ресурс] – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc2866>
11. RFC 4962. Guidance for Authentication, Authorization, and Accounting (AAA) Key Management. [Електронний ресурс] – Режим доступу до ресурсу: <https://datatracker.ietf.org/doc/html/rfc4962>

		Леценко А.П.			<i>KIK.KP.B – 125 – 10 – ПЗ</i>	Арк.
		Байлюк Є.М.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

- 12.IEEE 802.1X [Електронний ресурс] – Режим доступу до ресурсу:
https://en.wikipedia.org/wiki/IEEE_802.1X
- 13.An Analysis of the RADIUS Authentication Protocol [Електронний ресурс] –
Режим доступу до ресурсу: <https://www.untruth.org/~josh/security/radius/radius-auth.html>
- 14.GNS3 Talks: AAA Docker Appliance: Easy TACACS & RADIUS GNS3 servers! [Електронний ресурс] – Режим доступу до ресурсу: <https://davidbom-bal.com/gns3-talks-aaa-docker-appliance-easy-tacacs-radius-gns3-servers-part-3/>
- 15.802.1X Authentication. [Електронний ресурс] – Режим доступу до ресурсу:
<https://www.juniper.net/documentation/us/en/software/junos/user-access/topics/topic-map/802-1x-authentication-switching-devices.html>
- 16.Configuring IEEE 802.1x Port-Based Authentication. [Електронний ресурс] –
Режим доступу до ресурсу:
https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_0111000.html
- 17.AAA Authentication. [Електронний ресурс] – Режим доступу до ресурсу:
<https://contenthub.netacad.com/cyberops/>
- 18.Ольков Е. Практическая безопасность сетей [Електронний ресурс] – Ре-
жим доступу до ресурсу:
https://learn.ztu.edu.ua/pluginfile.php/125241/mod_resource/content/1/PraktichesBezopasSetej.pdf
- 19.Налаштування Radius-серверів [Електронний ресурс]. – 2018. – Режим до-
ступу до ресурсу: <https://docs.microsoft.com/ru-ru/windowsserver/networking/technologies/nps/nps-radius-clients-configure>
- 20.Розгортання бездротового доступу з автентифікацією на основі паролів
802.1X [Електронний ресурс] – Режим доступу до ресурсу:
<https://docs.microsoft.com/ru-ru/windows-server/networking/core-network-guide/cncg/wireless/a-deploy-8021x-wireless-access>

		Лещенко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Леценко А.П.			КІК.КР.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

Лістинги конфігурацій

R_2_10_1

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R_2_10_1
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
aaa new-model
!
aaa group server radius radiusgroup
server 192.168.1.254 auth-port 1812 acct-port 1813
!
aaa authentication login default group radiusgroup local
aaa authentication enable default enable
!
aaa session-id common
memory-size iomem 5
no ip icmp rate-limit unreachable
!
ip cef
ip domain name domain.com
ip name-server 8.8.8.8
ip name-server 8.8.4.4
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.2
ip dhcp excluded-address 192.168.1.254
!
ip dhcp pool LAN
network 192.168.1.0 255.255.255.0
dns-server 192.168.1.1
domain-name domain.com
default-router 192.168.1.1
!
username andrew privilege 15 password 0 cisco
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
ip address dhcp
ip nat outside
ip virtual-reassembly

```

```

duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
!
no ip http server
no ip http secure-server
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.122.1
!
ip nat inside source list 1 interface FastEthernet0/0 overload
ip dns server
!
access-list 1 permit 192.168.1.0 0.0.0.255
no cdp log mismatch duplex
!
radius-server host 192.168.1.254 auth-port 1812 acct-port 1813 key gns3
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
transport input telnet
!
end

```

SW_2_10_1

```

! Last configuration change at 20:37:31 UTC
Mon Jun 27 2022
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

```

		Леценко А.П.			KIK.KP.B – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

```

service compress-config
!
hostname SW_2_10_1
!
boot-start-marker
boot-end-marker
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
username andrew secret 5
$1$IBle$2.1jkozckksmfFOEN3BGq1
aaa new-model
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
!
aaa session-id common
!
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip domain-name domain.com
ip name-server 192.168.1.1
ip cef
no ipv6 cef
!
dot1x system-auth-control
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
switchport mode access
!
interface Ethernet0/1
switchport mode access
!
interface Ethernet0/2
switchport mode access
authentication port-control auto
dot1x pae authenticator
!
interface Ethernet0/3
switchport mode access

authentication port-control auto
dot1x pae authenticator
!
interface Ethernet1/0
!
interface Ethernet1/1
!
interface Ethernet1/2
!
interface Ethernet1/3
!
interface Ethernet2/0
!
interface Ethernet2/1
!
interface Ethernet2/2
!
interface Ethernet2/3
!
interface Vlan1
ip address 192.168.1.2 255.255.255.0
!
ip default-gateway 192.168.1.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip radius source-interface Ethernet0/1
!
radius-server host 192.168.1.254
!
radius server radius
address ipv4 192.168.1.254 auth-port 1812
acct-port 1813
key gns3
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
!
!
end

```

		Леценко А.П.			KIK.KP.Б – 125 – 10 – ПЗ	Арк.
		Байлюк Є.М.				5
Змн.	Арк.	№ докум.	Підпис	Дата		