

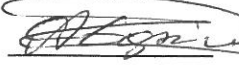
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно–комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА записка

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми аутентифікації корис-
тувачів комп'ютерної мережі організації на базі тех-
нології 802.1x та протоколу RADIUS»

Виконав студент 4–го курсу, групи КІ–3
спеціальності 123 «Комп'ютерна інженерія»

Керівник  Лісовський М.С.

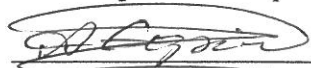
 Ефіменко А.А.

Рецензент  Россінський Ю.М.

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 123 «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Зав. кафедри комп'ютерної
інженерії та кібербезпеки

 Єфіменко А.А.

12 квітня 2021 р.

ЗАВДАННЯ

на випускн кваліфікаційну роботу

Студента Лісовського Миколи Сергійовича

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

Затверджена Наказом університету від «12» квітня 2021 р. № 133/С

Термін здачі студентом закінченої роботи 20 червня 2021 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження) процес проектування, розробки та налагодження підсистеми аутентифікації користувачів комп'ютерної мережі організації на базі технології 802.1x та протоколу RADIUS

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

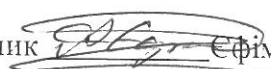
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1			
2			
3			

Керівник  Єфіменко А.А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка задачі. Пошук, огляд та аналіз аналогічних розробок. Формулювання технічного завдання. Опрацювання літературних джерел.	2 березня 2021 – 5 квітня 2021	
2	Проектування структурної схеми	6 квітня 2021 – 12 квітня 2021	
3	Налагодження обладнання мережі	13 квітня 2021 – 26 квітня 2021	
4	Тестування	27 квітня 2021 – 4 травня 2021	
5	Захист	22 червня 2021	

Студент  Лісовський М.С.

Керівник  Єфіменко А.А.

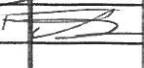
АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра містить проект підсистеми аутентифікації користувачів комп'ютерної мережі організації, пояснювальної записки та ілюстративного матеріалу до нього. Пояснювальна записка до випускної роботи містить 65 сторінок, 30 ілюстрацій та 8 таблиць.

Метою роботи є розробка та реалізація проекту підсистеми аутентифікації користувачів комп'ютерної мережі організації на базі технології 802.1x та протоколу RADIUS.

У роботі визначено основні завдання на розробку підсистеми аутентифікації в мережі, проаналізовано аналоги розробленої аутентифікації, розроблено структурну схему мережі, спроектовано підсистему аутентифікації користувачів. Також у роботі обгрунтовано вибір програмного забезпечення для реалізації проекту підсистеми і виконано тестування функціоналу мережі.

КЛЮЧОВІ СЛОВА: IPV4, RADIUS, AAA, VLAN, EAP, 802.1X.

					<i>KIK.KP.B-123-13-ПЗ</i>			
Зм.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Лісовський М.С.		18.06.21	Проект підсистеми аутентифікації користувачів комп'ютерної мережі організації на базі технології 802.1x та протоколу RADIUS	Літ.	Арк.	Аркушів
Керівник		Єфіменко А.А.		18.06.21			4	
Реценз.		Росітський Ю.М.		18.06.21		Житомирська політехніка, група КІ-3		
Н. контр.								
Зав.каф.		Єфіменко А.А.		18.06.21				

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. АНАЛІЗ ТЕХНОЛОГІЙ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНОЇ МЕРЕЖІ.....	10
1.1. Аналіз технології аутентифікації	10
1.2. Аналіз протоколів аутентифікації користувачів комп'ютерної мережі	13
1.3. Аналіз протоколів RADIUS, EAP та 802.1X	15
1.4. Постановка задачі	20
Висновки до розділу 2.....	21
РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ.....	22
2.1. Проектування фізичної мережної інфраструктури організації	22
2.2. Проектування логічних зв'язків мережі та розробка схеми адресації.....	25
2.3. Проектування підсистеми аутентифікації	31
Висновки до розділу 2.....	34
РОЗДІЛ 3 ВИБІР ОБЛАДНАННЯ, ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ	35
3.1. Вибір обладнання та програмного забезпечення	35
3.2. Налаштування роботи мережі та підсистеми аутентифікації.....	38
3.2. Перевірка працездатності мережі	48
Висновки до розділу 3.....	53
ВИСНОВКИ.....	54
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	56
ДОДАТКИ.....	59

ВСТУП

Комунікабельність являється важливою складовою нашого життя. Залишатись завжди на зв'язку з оточуючими нам дозволяють комунікаційні технології, а зокрема Інтернет. Розвиток глобальної мережі йде стрімкими темпами і в недалекому майбутньому саме вона стане основою, якщо не монополістом усіх комунікаційних мереж. У міру втілення в життя все нових і нових ідей та проектів, які здавалися раніше недосяжними, можливості об'єднаних мереж, що утворюють Інтернет, будуть грати все більш зростаючу роль в реалізації цих проектів.

Існує багато підприємств, які використовують комп'ютерні мережі. У комп'ютерних мережах усі важливі файли є частиною центральних файлових серверів. Ваші співробітники можуть отримувати доступ до цих файлів та змінювати їх, не відриваючись від свого робочого місця. Центральний сервер знижує кількість складних систем, необхідних для даних компаній.

Комп'ютерна мережа дозволяє спільне використання ресурсів різних пристроїв. Можливість ділитися технологічними активами між працівниками є однією з найбільших вигід від цього мережевого рішення. Мережі можуть складатись з комп'ютерних систем, серверів, баз даних, веб-сайтів та інших мережевих додатків. Для того щоб зловмисник не зміг отримати доступ до різних файлів мережі, створена аутентифікація.

Аутентифікація діє як перша лінія захисту, що дозволяє отримати доступ до цінних даних лише тим, кого схвалила організація

В 2019 році 29% порушень мережі пов'язані з викраденими даними, тому аутентифікація важлива, оскільки вона дозволяє організаціям захищати свої мережі, дозволяючи лише автентифікованим користувачам (або процесам) мати доступ до захищених ресурсів.

Тому важливо створити комп'ютерну мережу, яка буде гнучкою в користування та безпечною для користування.

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Метою випускної роботи є розробка проекту підсистеми аутентифікації користувачів комп'ютерної мережі організації на базі технології 802.1x та протоколу RADIUS.

Результатом випускної роботи є реалізована підсистема аутентифікації користувачів комп'ютерної мережі організації на базі технології 802.1x та протоколу RADIUS.

Мета роботи визначає такі завдання:

- Аналіз технології аутентифікації;
- Аналіз протоколів аутентифікації;
- Аналіз технолог протоколів Radius, 802.1X; EAP;
- Проектування фізичної мережної інфраструктури організації;
- Проектування логічних зв'язків мережі та розробка схеми адресації;
- Проектування підсистеми аутентифікації;
- Вибір обладнання та програмного забезпечення;
- Налаштування роботи мережі та підсистеми аутентифікації;
- Перевірка працездатності мережі.

Об'єктом дослідження є процеси аутентифікації користувачів комп'ютерної мережі організації.

Предметом дослідження аутентифікації аутентифікація на базі технології 802.1x та протоколу RADIUS.

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. АНАЛІЗ ТЕХНОЛОГІЙ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНОЇ МЕРЕЖІ

1.1. Аналіз технології аутентифікації

Аутентифікація використовується для підтвердження особи зареєстрованого користувача. Перевірка справжності – це процес перевірки облікових даних: ідентифікатора користувача (імені, адреси, електронної пошти, номера телефону) і пароля.

Типи аутентифікацій:

- однофакторна;
- двофакторна;
- єдиний вхід;
- багатофакторна.

Однофакторна аутентифікація є найпоширенішою формою автентифікації, також є й найменш безпечною, оскільки для отримання повного доступу до системи потрібен лише один фактор. Це може бути ім'я користувача та пароль, PIN-код або інший простий код. Однофакторна аутентифікація є зручною, але й водночас відносно легко проникнути шляхом фішингу, реєстрації ключів або взагалі звичайним вгадуванням паролю.

Двофакторна аутентифікація (2FA) – це аутентифікація яка по суті двічі перевіряє, чи користувач насправді є тим користувачем, яким він намагається увійти. За допомогою цього методу користувачі вводять свої основні облікові дані автентифікації, а потім повинні вводити другу частину ідентифікаційної інформації.

Єдиний вхід – цей метод є більш зручним для користувачів, оскільки він знімає обов'язок зберігати кілька наборів облікових даних і створює більш зручний доступ під час сесій. Організації можуть досягти цього, визначивши центральний домен (в ідеалі – систему IAM), а потім створивши безпечні зв'язки

SSO між ресурсами. Цей процес дозволяє перевіряти автентифікацію користувачів під контролем домену.

Багатофакторна автентифікація (MFA) є методом високого захисту даних, оскільки вона використовує більше системних факторів, що не мають значення для легітимації користувачів. Як і 2FA, MFA використовує такі фактори, як біометрія, підтвердження на основі пристрою, додаткові паролі і навіть інформацію про місцезнаходження чи поведінку для підтвердження ідентичності користувача. Однак різниця полягає в тому, що, хоча 2FA завжди використовує лише два фактори, MFA може використовувати два або три, з можливістю змінювати їх між сесіями, додаючи невловимий елемент для недійсних користувачів.

Способи аутентифікації:

- парольна;
- біометрична.

Парольна аутентифікація – здійснюється на основі володіння користувачем певною конфіденційною інформацією. Біометрична аутентифікація – заснована на унікальності певних антропометричних характеристик людини. Біометричний захист ефективніший ніж такі методи як, використання смарт-карток, паролів, PIN-кодів. Найчастіше використовується:

- відбитки пальців;
- риси обличчя;
- параметри голосу;
- особистий підпис;
- візерунок райдужної оболонки ока і карти сітківки ока.

За допомогою аутентифікації, ми отримуємо доступ до наших облікових записів в соціальних мережах, в лікарнях, в банках тощо. Перейдемо до розгляду аутентифікації у мережі.

AAA (Аутентифікація, авторизація та облік) – це система для відстеження діяльності користувачів у мережі на основі IP та контролю їх доступу до мережевих ресурсів. AAA часто реалізується як виділений сервер.

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

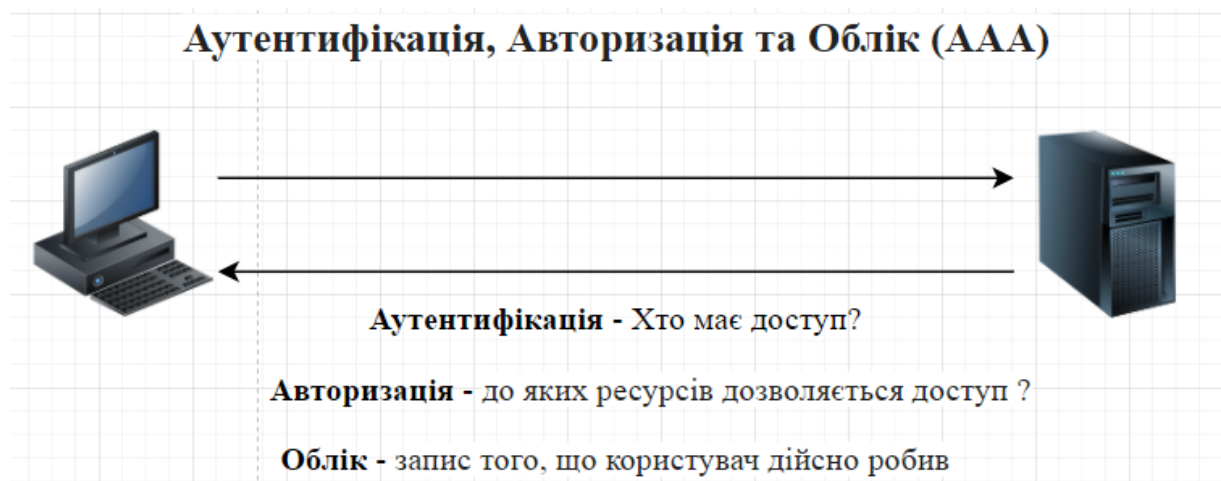


Рисунок 1.1 – Приклад AAA користувача на сервері

Аутентифікація відноситься до унікальної ідентифікаційної інформації від кожного користувача системи, як правило, у формі імені користувача та пароля. Системні адміністратори відстежують і додають або видаляють авторизованих користувачів із системи.

Авторизація відноситься до процесу додавання або заборони доступу окремого користувача до комп'ютерної мережі та її ресурсів. Користувачам можуть бути надані різні рівні авторизації, які обмежують їхній доступ до мережі та пов'язаних ресурсів. Визначення дозволу може базуватися на обмеженнях географічного розташування, обмеженнях дати або часу доби, частоті входів або декількох входах окремими фізичними або юридичними особами. Інші пов'язані типи послуг авторизації включають призначення маршрутів, фільтрацію IP-адрес, управління пропускнуою здатністю та шифрування.

Облік – паралельний з аутентифікацією і авторизацією етап, який записує в журнал успіх чи невдачу даних процесів, зміг людина проникнути в приміщення чи ні, чи отримав користувач доступ до мережних пристроїв і, якщо так, то які дії на ньому здійснював.

Є два основних типи AAA для мереж:

- AAA для адміністрування мережеских пристроїв;
- AAA для доступу до мережі.

AAA для адміністрування мережеских пристроїв здійснює управління тими, у кого є доступ для входу в консоль мережевого пристрою, Telnet-сесії,

Secure Shell (SSH–сесії) або іншим способом. AAA для доступу до мережі – ідентифікація користувача або пристрою до того, як йому буде надано доступ до мережі.

1.2. Аналіз протоколів аутентифікації користувачів комп'ютерної мережі

Для забезпечення безпеки мережі необхідно забезпечити контроль за доступом до різних елементів мережі з боку користувачів. Такими елементами можуть бути мережеві пристрої, сервери, комп'ютери, додатки або навіть сегменти самої мережі. Сценарії різні, а принцип один – аутентифікація, авторизація та облік (Authentication, Authorization, Accounting – AAA).

У сучасних мережах використовують два основних рішення для AAA: Remote Authentication Dial–In User Service (RADIUS) і Cisco's Terminal Access Controller Access–Control System Plus (TACACS +) протоколи. Існує ще й третій AAA–протокол, відомий як DIAMETER, але він зазвичай використовується тільки мобільними операторами. Розглянемо і порівняємо RADIUS і TACACS +, щоб допомогти вам визначити, який з них краще підходить для вашої мережі.

Розглянемо такі протоколи архітектури AAA:

- TACACS;
- XTACACS;
- TACACS;
- RADIUS;
- DIAMETR.

Найстарішими протоколами моделі AAA є протоколи TACACS, XTACACS і TACACS+, які забезпечують автентифікацію на основі IP без будь–якого шифрування (імена користувачів та паролі транспортувались як звичайний текст). Пізніша версія XTACACS (Розширений TACACS) додала авторизацію та облік. Обидва ці протоколи згодом були замінені на TACACS +. TACACS + відокремлює компоненти AAA, таким чином, їх можна розділити та обробляти

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

на окремих серверах (він може навіть використовувати інший протокол, наприклад, для авторизації). Він використовує TCP (Протокол управління передачею) для транспортування та шифрує весь пакет. TACACS+ є власністю Cisco.

RADIUS – є повноцінним протоколом, в якому повноваження в основному базуються на поєднанні ім'я користувача та пароля.

DIAMETR – еволюціонував від RADIUS і включає багато вдосконалень, таких як використання більш надійного протоколу TCP або SCTP та підвищення рівня безпеки завдяки TLS.

Протокол DIAMETR був розроблений щоб замінити протокол RADIUS, немає сумнівів, що він забезпечує чудову функціональність, але на жаль, старе обладнання не підтримує новий протокол, навіть якщо ми встановимо новий сервер з аутентифікацією DIAMETR, ми не знайдемо клієнтів, які зможуть підключитися за допомогою цього протоколу.

Таблиця 1.1 – Порівняння протоколів TACACS+ та RADIUS

Критерій	TACACS+	RADIUS
Протокол передачі	TCP:49	UDP:1812 та 1813 або UDP: 1645 та 1646
Аутентифікація та авторизація	Різні процеси для аутентифікації, авторизації та обліку	Об'єднує аутентифікацію і авторизацію
Підтримка мультипротоколів	Підтримується	Лише IP
Можливість перенаправлення запиту	немає	є
Доступ до команд CLI	Підтримує два методи контролю авторизації	Не підтримується
Шифрування	Пакетне навантаження	Тільки паролі

Переваги TACACS+ над RADIUS:

- оскільки TACACS+ використовує TCP протокол передачі, він є більш надійним ніж RADIUS;

- забезпечує більший контроль над авторизацією команд;
- всі пакети AAA зашифровані в TACACS+, тоді як в RADIUS зашифровані лише паролі.

Переваги RADIUS над TACACS+:

- RADIUS протокол є відкритим стандартом, TACACS+ є власністю Cisco, та його можна використовувати лише з пристроями Cisco;
- підтримує протокол передачі UDP, у якого вища продуктивність ніж у TCP.

Проаналізувавши різні протоколи AAA, можна сказати що найбільшим недоліком TACACS+ є те, що Cisco розробила протокол, який отримав широку підтримку лише на обладнанні Cisco. Основною перевагою RADIUS є те, що він безкоштовний. Однак він поставляється з обмеженими функціональними можливостями, такі як автентифікація та авторизація поєднуються, не надаючи гнучкості в тому, як їх можна налаштувати окремо.

1.3. Аналіз протоколів RADIUS, EAP та 802.1x

RADIUS (Remote Authentication Dial In User Service) – це мережевий протокол, який забезпечує централізоване управління автентифікацією, авторизацією та обліком (AAA) для користувачів, які підключаються та використовують мережеву послугу. RADIUS був розроблений компанією Livingston Enterprises у 1991 році як протокол автентифікації та обліку сервера доступу. Пізніше це було введено в стандарти IETF .

Основними поняттями протоколу RADIUS є: авторизація, радіус–клієнт, радіус–сервер, розглянемо детальніше ці процеси.

Авторизація – процес, протягом якого визначаються повноваження ідентифікованого користувача на доступ до певних мережевих ресурсів

Radius Client – це мережевий пристрій (маршрутизатор, комутатор), який використовується для аутентифікації користувачів.

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

RADIUS – сервер це фоновий процес, що виконується на сервері UNIX або Windows. Який дозволяє вести профілі користувачів у центральній базі даних. Отже, якщо у вас є сервер RADIUS, ви маєте контроль над тим, хто може з'єднуватися з вашою мережею.

Коли користувач намагається підключитись до вашої мережі, він надсилає запит на RADIUS-сервер, користувач може підключитися до клієнта RADIUS лише за умови, що сервер RADIUS аутентифікує та авторизує користувача.

Сервери RADIUS пропонують компаніям можливість зберігати конфіденційність та безпеку своєї системи та своїх користувачів, допомагаючи тим самим в управлінні безпекою та у створенні політики для адміністрування серверів.

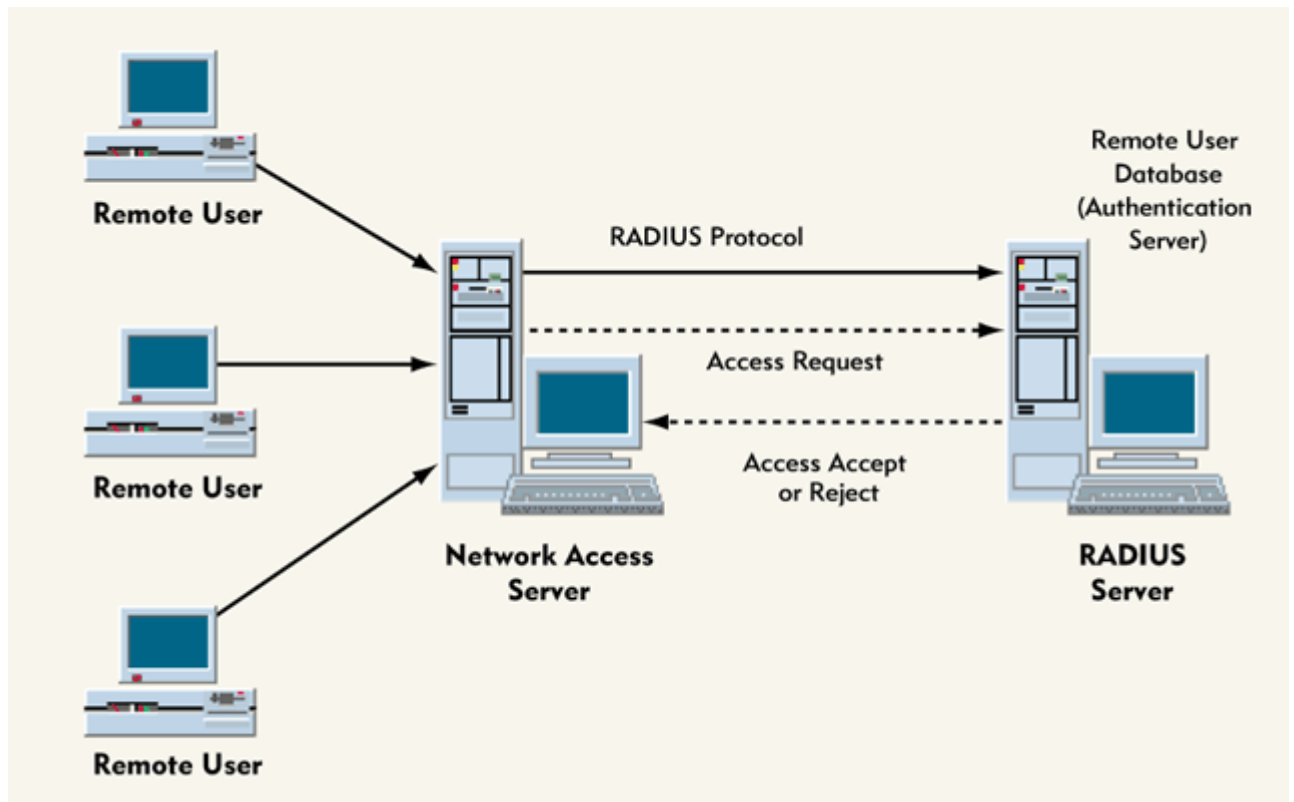


Рисунок 1.2– автентифікація користувача в мережі з RADIUS-сервером

Основний процес автентифікації та авторизації RADIUS включає наступні кроки:

Крок 1. Клієнт RADIUS намагається виконати автентифікацію на сервері RADIUS, використовуючи облікові дані користувача (ім'я користувача та пароль).

Крок 2. Клієнт надсилає повідомлення про запит доступу на сервер RADIUS. Паролі завжди шифруються в повідомленні.

Крок 3. Сервер RADIUS зчитує пароль і гарантує, що повідомлення про запит доступу надходить від уповноваженого клієнта. Якщо Запит на доступ не надходить від уповноваженого Клієнта, тоді повідомлення відкидається.

Крок 4. Якщо Клієнт авторизований, сервер RADIUS зчитує запрошений метод автентифікації.

Крок 5. Якщо застосовується метод автентифікації, сервер RADIUS зчитує облікові дані користувача з повідомлення. Він узгоджує облікові дані користувача з базою даних користувачів. Якщо є збіг, сервер RADIUS витягує додаткові дані про користувача з бази даних користувачів.

Крок 6. Тепер сервер перевіряє, чи існує політика доступу або профіль, який відповідає обліковим даним користувача.

Крок 7. Якщо політика відповідності відсутня, сервер надсилає повідомлення про відхилення доступу. Транзакція RADIUS закінчується, і користувачеві заборонено доступ до системи.

Крок 8. Якщо існує політика відповідності, сервер RADIUS надсилає на пристрій повідомлення Access–Асепт.

Крок 9. Повідомлення Access–Асепт складається із загальної таємниці та атрибута Filter ID. Якщо спільний секрет не збігається, клієнт RADIUS відхиляє повідомлення.

Крок 10. Якщо загальний секрет збігається, Клієнт зчитує значення атрибута Filter ID. Ідентифікатор фільтра – це рядок тексту. Клієнт RADIUS підключає користувача до певної групи RADIUS за допомогою цього ідентифікатора.

Крок 11. Користувач остаточно аутентифікований та авторизований, і він отримує доступ до RADIUS–клієнта.

Сервер RADIUS запобігає витоку приватної інформації вашої організації стороннім особам. Це також дозволяє окремим користувачам

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

призначати унікальні мережеві дозволи. Він може інтегруватися у вашу існуючу систему без істотних змін.

Розширюваний протокол автентифікації (EAP) – це протокол для бездротових мереж, який розширює методи автентифікації, що використовуються Протоколом від точки до точки (PPP), протоколом, який часто використовується при підключенні комп'ютера до Інтернету. EAP використовується в зашифрованих мережах для забезпечення безпечного способу надсилання ідентифікаційної інформації для забезпечення автентифікації мережі. Він підтримує різні методи автентифікації, включаючи маркери, смарт-картки, сертифікати, одноразові паролі та шифрування відкритим ключем .

Протокол EAP (Extensible Authentication Pro-ocol) (RFC 3748) дозволяє перевіряти справжність при підключеннях віддаленого доступу за допомогою різних механізмів перевірки автентичності. Точна схема перевірки справжності узгоджується клієнтом віддаленого доступу і сервером, який виконує перевірку автентичності (ним може бути сервер віддаленого доступу або RADIUS сервер). За умовчанням в маршрутизацію та віддалений доступ включена підтримка протоколів EAP–TLS і MD5–Challenge (MD5–задача). Підключення інших модулів EAP до сервера, який використовує маршрутизацію та віддалений доступ, забезпечує підтримку інших методів EAP.

Протокол EAP дозволяє вести вільний діалог між клієнтом віддаленого доступу і системою перевірки автентичності. Такий діалог складається із запитів системи перевірки справжності на необхідну їй інформацію і відповідей клієнта віддаленого доступу. Наприклад, коли протокол EAP використовується з генераторами кодів доступу, сервер, що виконує перевірку справжності, може окремо запитувати у клієнта віддаленого доступу ім'я користувача, ідентифікатор і код доступу. Після відповіді на кожен такий запит клієнт віддаленого доступу проходить певний рівень перевірки автентичності. Коли на всі запити будуть отримані задовільні відповіді, перевірка достовірності клієнта віддаленого доступу успішно завершується.

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

Схеми перевірки автентичності, що використовують протокол EAP, називаються типами EAP. Для успішної перевірки автентичності клієнт віддаленого доступу і сервер, що виконує перевірку автентичності, повинні підтримувати один і той же тип EAP.

802.1X – це мережевий протокол автентифікації, який відкриває порти для доступу до мережі, коли організація автентифікує особу користувача та авторизує його для доступу до мережі. Ідентифікація користувача визначається на основі його облікових даних або сертифіката, що підтверджується сервером RADIUS. Сервер RADIUS може це зробити, спілкуючись з каталогом організації, як правило, через протокол LDAP або SAML.

Для пристроїв, які намагаються підключитися до локальної мережі або мережі WLAN, потрібен механізм автентифікації. IEEE 802.1X, стандарт IEEE для портового контролю доступу до мережі (PNAC), забезпечує захищену автентифікацію для безпечного доступу до мережі.

Аутентифікація дротового мережевого з'єднання для 802.1X – це процес, подібний до бездротового. Користувач дротової мережі повинен підключитися до захищеної мережі зі свого пристрою та надати підписаний сертифікат або дійсні облікові дані для автентифікації своєї особи.

Основна відмінність полягає в тому, що замість встановлення безпечного з'єднання за допомогою бездротового комутатора ваш пристрій повинен бути підключений до Ethernet і аутентифікуватися на комутаторі, що підтримує 802.1X. Пристрій і сервер RADIUS встановлюють довіру до дротового з'єднання, і якщо користувач буде розпізнаний, вони будуть авторизовані для безпечного використання мережі.

У 802.1X є три основних компоненти – суплікант, аутентифікатор і сервер аутентифікації.

Супплікант – це ваш термінал і користувач з певним ПО (тут немає сенсу заглиблюватися в різні види супплікантов).

Аутентифікатор – це комутатор або точка доступу (перше мережеве пристрій рівня доступу, на який прийшов трафік з суппліканта).

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

І, нарешті, сервером аутентифікації є спеціальне програмне забезпечення або пристрій, що належить до класу NAC – Network Access Control , або засобам контролю мережевого доступу. Конкретний клас рішень для реалізації 802.1X називається RADIUS–сервером .

Отже, порядок підключення наступний: ви намагаєтеся отримати доступ в мережу і аутентифікатор каже – пред'явіть, будь ласка документи. Ваше пристрій (супплікант) надає потрібну інформацію – логін і пароль. Далі аутентифікатор відправляє отриману інформацію на сервер аутентифікації і чекає відповіді. В базовому варіанті, сервер аутентифікації відправить назад на аутентифікатор дозвіл і після цього аутентифікатор дозвіл суппліканту. До цього моменту майже ніякий трафік дозволений не буде.

802.1X потребує сервера RADIUS, оскільки для перевірки облікових даних повинен бути виділений сервер. Фасет автентифікації 802.1X фактично відбувається на сервері RADIUS. Сервер перевіряє каталог авторизованих користувачів, щоб підтвердити, чи має клієнт дозвіл на доступ до мережі, і передає цю інформацію назад контролеру / точці доступу. Без сервера RADIUS автентифікація мала б відбуватися в точці доступу (для цього потрібні досить потужні точки доступу), наприклад у випадку автентифікації PSK (попередньо спільний ключ).

1.4. Постановка задачі

Головною метою даної роботи є розробка та реалізація проекту підсистеми аутентифікації користувачів комп'ютерної мережі організації на базі технології 802.1x та протоколу RADIUS. Закріплення знань в процесі дослідження тематики аутентифікації відбувається шляхом створення комп'ютерної мережі організації, розподілу віртуальних мереж, налаштуванню адресації і в результаті – налаштування технології 802.1x та протоколу RADIUS.

В випускній роботі необхідно розробити структурну схему комп'ютерної мережі організації , якомога більше наблизити процес віртуальної мережі до

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

реальної, створити аутентифікацію користувачів до своїх віртуальних мереж.
Для реалізації поставленого завдання, основними етапами є:

1. Аналіз технологій аутентифікації користувачів комп'ютерної мережі.
 - 1.1. Аналіз технологій аутентифікації
 - 1.2. Аналіз протоколів аутентифікації користувачів комп'ютерної мережі
 - 1.3. Аналіз протоколу RADIUS, EAP та 802.1x
2. Проектування підсистеми аутентифікації користувачів комп'ютерної мережі на базі технології 802.1x та протоколу radius
 - 2.1. Проектування фізичної мережної інфраструктури організації
 - 2.2. Проектування логічних зв'язків мережі та розробка схеми адресації
 - 2.3. Проектування підсистеми аутентифікації
3. Вибір обладнання, програмного забезпечення, налаштування та тестування підсистеми аутентифікації користувачів комп'ютерної мережі на базі технології 802.1x та протоколу radius
 - 3.1. Вибір обладнання та програмного забезпечення
 - 3.2. Налаштування роботи мережі та підсистеми аутентифікації
 - 3.3. Тестування роботи мережі та підсистеми аутентифікації

Висновки до розділу 1

В даному розділі було проведено аналіз технологій аутентифікації та його протоколів для аутентифікації користувачів в комп'ютерній мережі.

Проведений аналіз дозволив обрати основні протоколи для аутентифікації користувачів в мережі, виявити їх переваги, недоліки та ознайомитись з їх роботою.

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

2.1. Проектування фізичної мережної інфраструктури організації

Комп'ютерна мережа – це два або більше комп'ютери, які з'єднані між собою з метою передачі даних в електронній формі. На додаток до фізичного з'єднання комп'ютера та комунікаційних пристроїв, мережева система виконує важливу функцію створення цілісної архітектури, яка дозволяє різним типам обладнання передавати інформацію майже безперешкодно.

Основні елементи комп'ютерної мережі:

- Сервер – завдяки серверу користувачи мають доступ до інформаційних ресурсів мережі;
- Робоча станція;
- Засоби комунікації – канали та засоби передачі інформаційних повідомлень.

У кожної комп'ютерної мережі є своя топологія.

Топологія мережі – це схематичний опис розташування фізичних та логічних елементів комунікаційної мережі. Існує багато різних способів з'єднання мережевих топологій, але виділяють основну топологію – зірка.

Макет мережі має прямий вплив на функціональність мережі. Вибір правильної топології може підвищити продуктивність та ефективність даних, оптимізувати розподіл ресурсів та зменшити експлуатаційні витрати. Ідеальна топологія мережі залежить від розміру, масштабу, цілей та бюджету кожного підприємства.

Розглянемо типову комп'ютерну мережу, на прикладі мережі для бібліотеки, що зображена на рисунку 2.1.

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

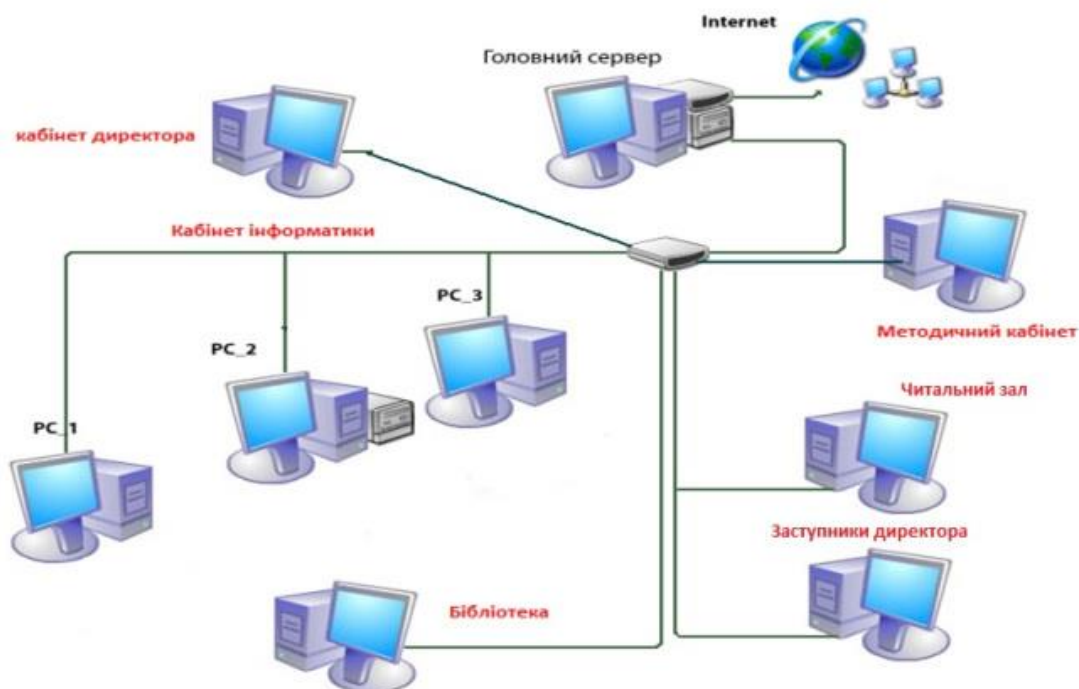


Рисунок 2.1 – Приклад комп'ютерної мережі

Мережа складається з вісьми комп'ютерів, комутатора та головного сервера. Завдяки тому, що всі комп'ютери підключені до одного комутатора, вони можуть передавати та отримувати дані один від одного, директор має можливість налаштовувати рівні доступу до сервера, бібліотекар може записувати в бази даних читачів, читальний зал може отримувати електронні книги щодо свого аккаунта з привілеями. Кожен комп'ютер під'єднаний до мережі за допомогою Ethernet кабеля, та має свій унікальний IP-адрес.

Задля того, щоб користувачі мали можливість спілкуватися в мережі один з одним, створимо для кожної групи людей свої віртуальні інтерфейси.

VLAN (англ. Virtual Local Area Network — віртуальна локальна комп'ютерна мережа) — це віртуальні мережі, які існують на другому рівні моделі OSI. Якщо дивитися на VLAN, абстрагуючись від поняття «віртуальні мережі», то можна сказати, що VLAN — це просто мітка в кадрі, який передається по мережі. Мітка містить номер віртуального інтерфейса на який відводиться 12 біт, тобто, VLAN може нумеруватися від 0 до 4095.

Поява VLAN забезпечила безпеку, простоту та гнучкість мережі. Це також призвело до зменшення адміністративних накладних витрат, необхідних

для управління середовищем із багатьма комутаторами. Уявіть, яка величезна складність характеризує сучасну локальну мережу – більше комутаторів, точок доступу, маршрутизаторів і, звичайно, більше кабелів. Це, очевидно, призводить до вищих загальних витрат на володіння кожною локальною мережею.

Можливості VLAN:

- Можливість побудови мережі, логічна структура якої не залежить від фізичної.
- Можливість розбиття одного широкомовного домену на кілька широкомовних доменів. При цьому зменшується навантаження на мережеві пристрої.
- Можливість убезпечити мережу від несанкціонованого доступу. Тобто, на каналному рівні кадри з інших VLAN будуть відсікатися портом комутатора незалежно від того, з якою вихідною IP –адресою пакет у даному кадрі
- Можливість застосовувати політики на групу пристроїв, які знаходяться в одному VLAN.
- Можливість використовувати віртуальні інтерфейси для маршрутизації.

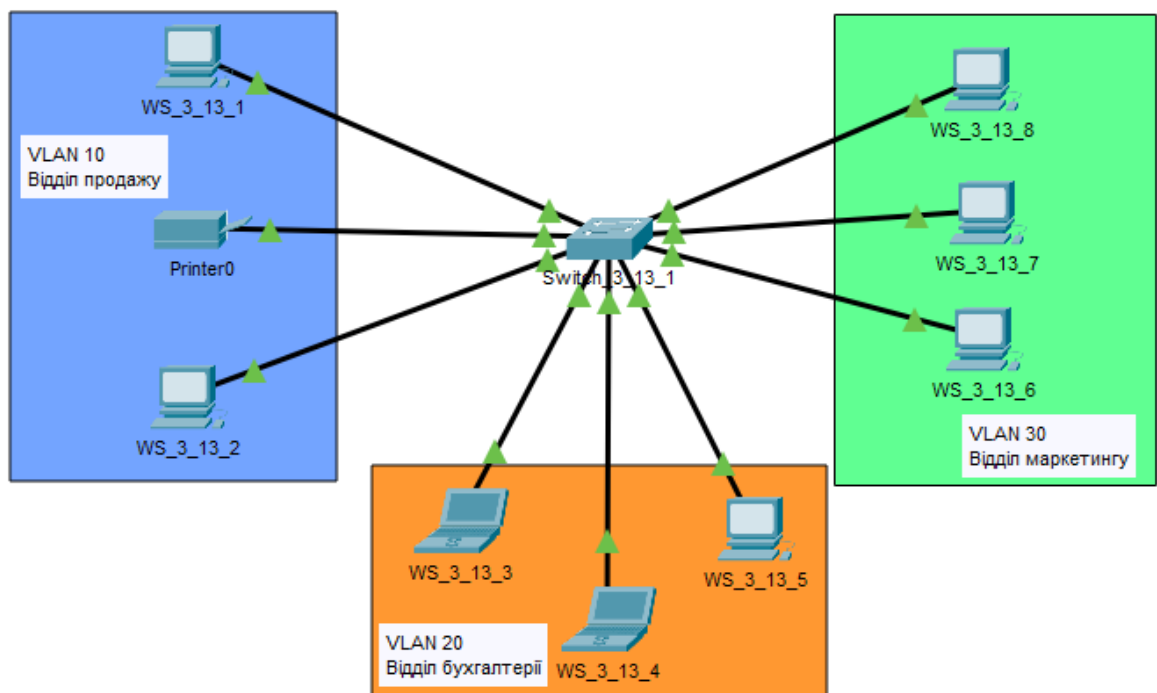


Рисунок 2.2 – Комп’ютерна мережа з VLAN

На рисунку 2.2 ми бачимо мережу, в якій були впроваджені VLAN. Інтерфейси комутації для пристроїв у відділі продажу були призначені VLAN 10, пристрої у відділі бухгалтерії підключені для комутації інтерфейсів у VLAN 20, а відділ маркетингу використовує VLAN 30. Завдяки розподілу віртуальних мереж, є можливість застосувати різну політику на групи пристроїв та убезпечити віртуальні мережі від несанкціонованого доступу. Також ми можемо надати доступ обмінюватись даним відділам між собою.

Оскільки порт може бути членом декількох віртуальних інтерфейсів, маршрутизація VLAN може бути включена для всіх VLAN на порту або для підмножини. Ви можете використовувати маршрутизацію VLAN, щоб дозволити більше ніж одному фізичному порту знаходитись в одній підмережі, охоплювати VLAN через кілька фізичних мереж або забезпечувати додаткову сегментацію або безпеку. Портом може бути порт VLAN або порт маршрутизатора, але не обидва.

2.2. Проектування логічних зв’язків мережі та розробка схеми адресації

При проектуванні мережі використана трирівнева ієрархічна модель мережі, в якій використовуються три рівні:

- Рівень ядра (Core layer);
- Рівень розподілу (Distribution layer);
- Рівень доступу (Access layer).

Загальна топологія спроектованої мережі представлена на рисунку 2.3

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

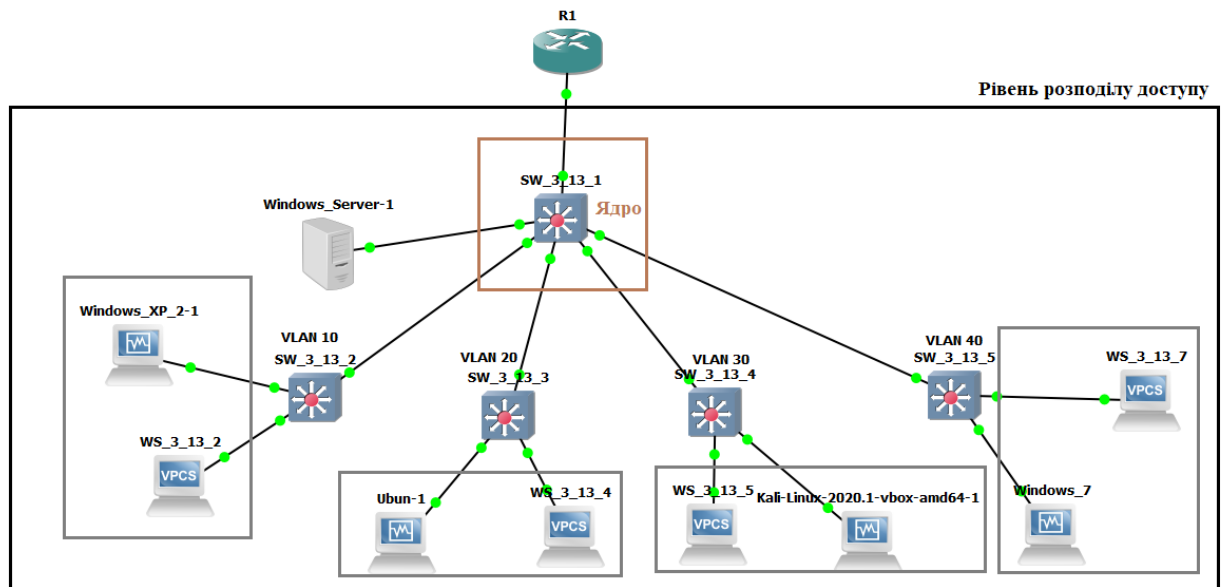


Рисунок 2.3 – Загальна топологія спроектованої мережі

Відповідно ядра в нашій моделі розміщено один комутатор. Відповідно рівню розподілу доступу, складається зі з'єднаних між собою за допомогою витої пари FastEthernet для забезпечення високої швидкості на даному рівні. Рівень доступу представлений RADIUS – сервером та комутаторами під'єднаними до них з кінцевими вузлами, які відносяться до різних віртуальних локальних мереж (VLAN), саме з'єднання комутаторів до ядра забезпечуються каналами з витих пар GigabitEthernet, а з'єднання до кінцевих вузлів вита пара FastEthernet. У загальному в мережі використано п'ять комутаторів, один маршрутизатор та RADIUS сервер. Мережа складається з чотирьох VLAN, які розподілені на різні комутатори.

Розглянемо детальніше спроектовану мережу.

Загальна структура мережі наведена у додатку А. Рівень доступу складається з п'яти комутаторів, до кожного з яких підключені різні VLAN. Комутатор SW_3_13_2 належить до віртуальної мережі VLAN10, який має два кінцевих вузла, але розрахований на 253 вузла.

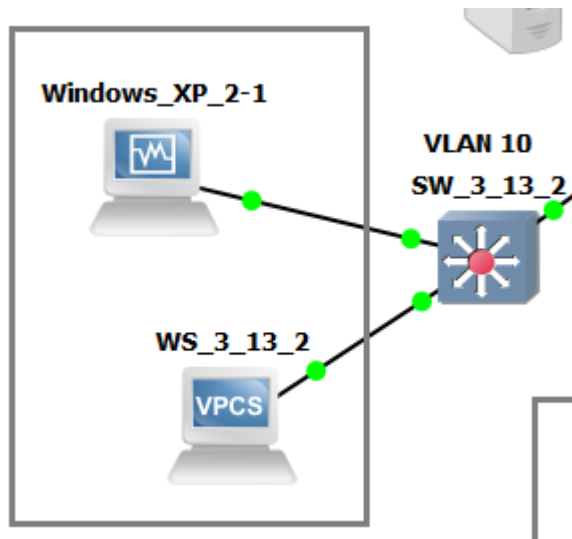


Рисунок 2.4 – До комутатора SW_3_13_2 підключені два кінцевих вузла

Комутатор SW_3_13_3 належить до віртуальної мережі VLAN20, який має два кінцевих вузла, але розрахований на 253 вузла.

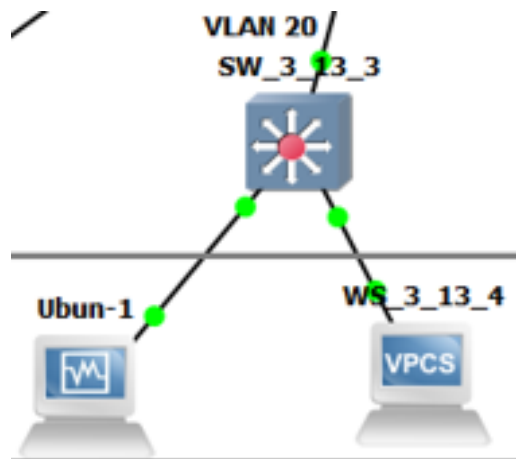


Рисунок 2.5 – До комутатора SW_3_13_3 підключені два кінцевих вузла

Комутатор SW_3_13_4 належить до віртуальної мережі VLAN30, який має два кінцевих вузла, але розрахований на 253 вузла.

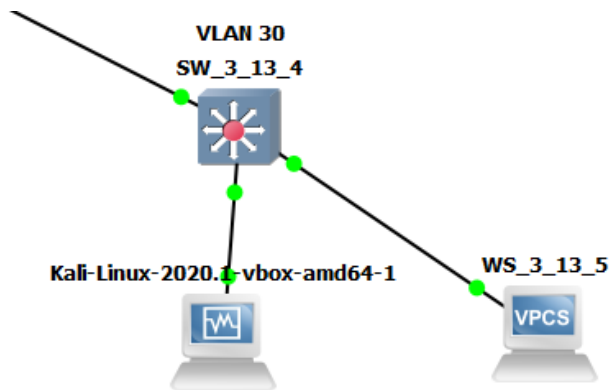


Рисунок 2.6 – До комутатора SW_3_13_4 підключені два кінцевих вузла

Комутатор SW_3_13_5 належить до віртуальної мережі VLAN40, який має два кінцевих вузла, але розрахований на 253 вузла.

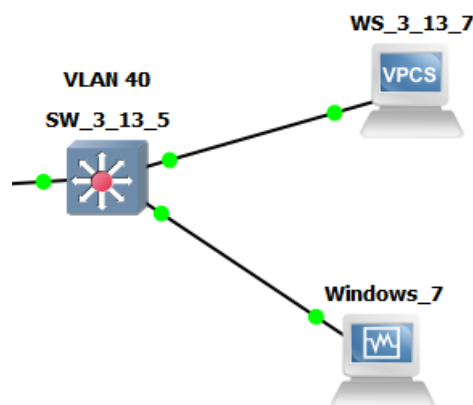


Рисунок 2.7 – До комутатора SW_3_13_5 підключені два кінцевих вузла

Загалом сумарна кількість кінцевих вузлів кожної VLAN наведено в табл. 2.1:

Таблиця 2.1 –Загальна кількість кінцевих вузлів кожної VLAN

Номер VLAN	Загальна кількість кінцевих вузлів	Доступна кількість кінцевих вузлів
VLAN10	2	253
VLAN20	2	253
VLAN30	2	253
VLAN40	2	253

Адресація пристроїв мережі наведена в таблиці 2.2

Таблиця 2.2 – Адресація пристроїв мережі на рівні розподілу

Пристрій мережі	Інтерфейс	IPv4–адреса	Маска мережі	Префікс мережі
Маршрутизатор R_3_13_1	FastE 0/0.1	203.3.13.1	255.255.255.0	/24
	FastE 0/0.10	204.3.13.1		
	FastE 0/0.20	205.3.13.1		
	FastE 0/0.30	206.3.13.1		
	FastE0/0.40	207.3.13.1		
Комутатор SW_3_13_2	Vlan 10	204.3.13.254		
Комутатор SW_3_13_3	Vlan 20	205.3.13.254		
Комутатор SW_3_13_4	Vlan 30	206.3.13.254		
Комутатор SW_3_13_5	Vlan 40	207.3.13.254		

Адресація всіх VLAN загальної мережі наведена в таблиці 2.3:

Таблиця 2.3 – Адресація всіх VLAN загальної мережі

VLAN	Призначення	IPv4–адреса
VLAN 10	Префікс	/24
	Маска префіксу	255.255.255.0
	Інверсна маска префіксу	0.0.0.255
	Мережа	204.3.13.0
	Шлюз по–замовчуванню	204.3.13.1
	Мінімальна адреса діапазону	204.3.13.1
	Максимальна адреса діапазону	204.3.13.255

VLAN	Призначення	IPv4-адреса
VLAN 20	Префікс	/24
	Маска префіксу	255.255.255.0
	Інверсна маска префіксу	0.0.0.255
	Мережа	205.3.13.0
	Шлюз по-замовчуванню	205.3.13.1
	Мінімальна адреса діапазону	205.3.13.1
	Максимальна адреса діапазону	205.3.13.255
VLAN 30	Префікс	/24
	Маска префіксу	255.255.255.0
	Інверсна маска префіксу	0.0.0.255
	Мережа	206.3.13.0
	Шлюз по-замовчуванню	206.3.13.1
	Мінімальна адреса діапазону	206.3.13.1
	Максимальна адреса діапазону	206.3.13.255
VLAN 40	Префікс	/24
	Маска префіксу	255.255.255.0
	Інверсна маска префіксу	0.0.0.255
	Мережа	207.3.13.0
	Шлюз по-замовчуванню	207.3.13.1
	Мінімальна адреса діапазону	207.3.13.1
	Максимальна адреса діапазону	207.3.13.255

2.3. Проектування підсистеми аутентифікації

Для того щоб спроектувати нашу підсистему аутентифікації, потрібно обрати RADIUS– сервер. Існують такі RADIUS – сервери:

- FreeRADIUS;
- WinRADIUS;
- TekRADIUS;
- Windows NPS.

FreeRADIUS – це безкоштовне програмне забезпечення з відкритим кодом є одним з найпопулярніших серверів RADIUS у світі. FreeRADIUS можна встановити на старій башті робочого столу для обслуговування до декількох сотень користувачів, або встановити на відповідні сервери для підтримки до мільйонів користувачів та запитів. FreeRADIUS призначений для роботи на Unix, Linux та інших Unix–подібних операційних системах. Ви можете знайти його у сховищах більшості дистрибутивів Linux, легко встановлених або складених вручну для більшості інших. За замовчуванням FreeRADIUS має інтерфейс командного рядка, і зміни налаштувань здійснюються за допомогою редагування файлів конфігурації, що найкраще підходить для IT–фахівців з досвідом роботи в Unix / Linux. Конфігурація є доступною для користувачів, і оскільки вона відкрита, ви навіть можете вносити зміни в програмне забезпечення.

WinRadius – це стандартний RADIUS–сервер для автентифікації мережі, обліку. Він простий у використанні і може використовуватися для телекомунікаційної платформи обліку, аутентифікації PPP, сервера обліку. Він підтримує PPP, PPPoE, PPTP, VPN, VoIP, ADSL, кабельний модем, CDMA, GSM, GPRS, WLAN (802.1x) тощо. Це ідеальне рішення для автентифікації, обліку для широкосмугових, VoIP, W–LAN тощо. .

TekRADIUS працює на Windows і пропонує графічний інтерфейс. Основні функції пропонуються безкоштовно; але існують і платні версії. Версія TekRADIUS Enterprise (\$ 149) додає підтримку EAP–TLS, динамічне створення самопідписаного сертифіката для сеансів PEAP, автентифікацію NTLM для

методів автентифікації MS–CHAP та відповідність атрибутів на основі регулярних виразів. Версія TekRADIUS SP (\$ 449) надає вам VoIP на додаток до функцій підприємства.

Сервер мережевої політики (NPS) – це реалізація корпорацією Microsoft сервера та проксі–сервера віддаленої автентифікації, що входить у службу користування (RADIUS). Як сервер RADIUS, NPS виконує централізовану автентифікацію та авторизацію для бездротових пристроїв, а також санкціонує комутацію, віддалений доступ і комутацію з віртуальною приватною мережею (VPN). Використовуючи NPS, ви можете централізовано налаштовувати та керувати автентифікацією доступу до мережі, надавати авторизацію для запитів на з'єднання та вести журнали інформації.

Таблиця 2.4 – Порівняння серверів FreeRADIUS, WinRADIUS, TekRADIUS, Windows NPS

	FreeRADIUS	WinRADIUS	TekRADIUS	Windows NPS
ОС	Unix/Linux	Windows	Windows	Windows Server
Простий у використанні	Складний	Легкий	Легкий	Середній
Ціна	Безкоштовно	Безкоштовно	Безкоштовно	Безкоштовно
Графічний інтерфейс	–	+	+	+
Методи аутентифікації	EAP–FAST, EAP–TLS, 802.1X,	PAP, CHAP, MS–CHAPv1, MS–CHAPv2, EAP–MD5, 802.1X	PAP, CHAP, EAP–MD5, EAP–TLS, LEAP, EAP–SIM	EAP–TLS, PEAP–MS–CHAP, 802.1X
Інше	Відкритий код		Обмеження кількості одночасних сеансів для користувачів	Доступний лише в Active Directory

Головним недоліком FreeRadius є той факт, що його потрібно встановити, налаштувати та керувати ним з терміналу, також FreeRadius доступний тільки на Unix та Linux. Подібні завдання забирають дорогоцінний час у IT-адміністратора і вимагають значних технічних знань.

Для нас ідеальним RADIUS – сервером є WinRadius, тому що він підтримує метод аутентифікації – 802,1X та є зручним у налаштуванні.

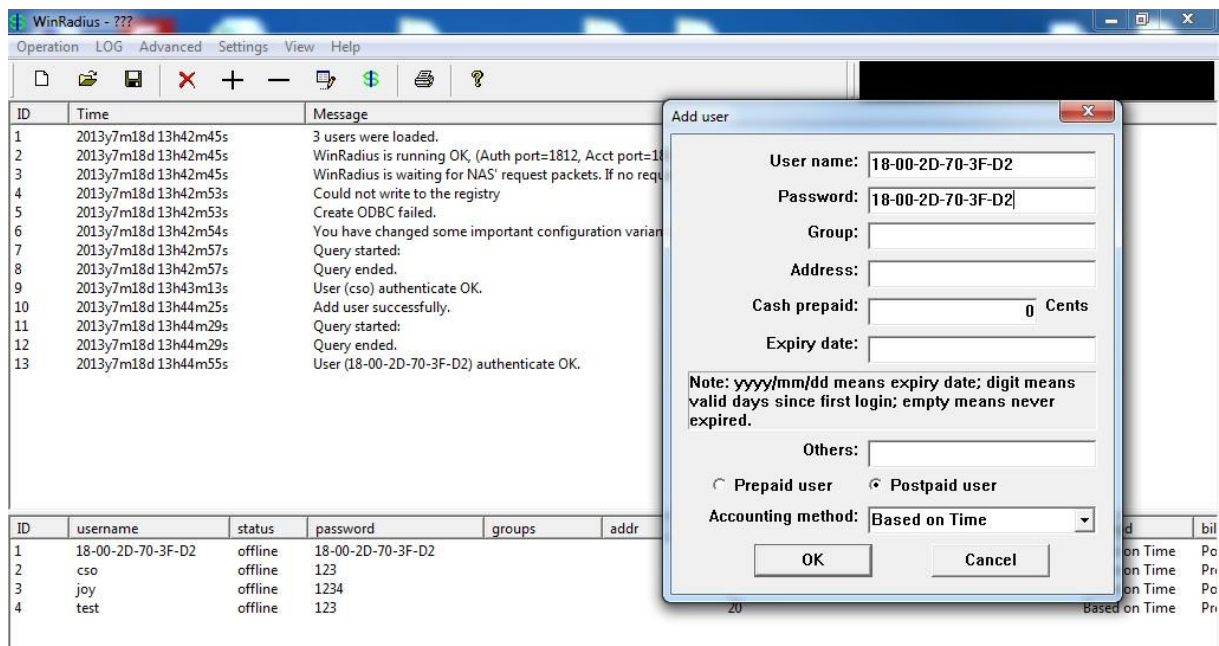


Рисунок 2.8. – Знімок екрану WinRadius

Функції WinRadius:

- WinRadius може обробляти в реальному часі всі види аутентифікації, облікових повідомлень, таких як PPP, PPPoE, PPTP, VPN, VoIP, ADSL, кабельний модем, CDMA, GSM, GPRS;
- може генерувати багато інформації журналу, і весь цей журнал можна переглядати або зберігати як на стороні сервера, так і на стороні клієнта;
- підтримка автентифікації, конфігурації портів обліку, проміжного оновлення;
- підтримка прив'язки вашого користувача до телефонного номера або MAC-адреси;
- підтримка всіх видів баз даних за допомогою ODBC для підключення бази даних, таких як Sql Server, MySql, Oracle тощо;

- підтримка всіх видів ОС Windows;
- може дуже швидко відповідати, використовуючи кеш–пам'ять та багатопотокову структуру мейнфрейма;
- автоматично створює резервне копіювання даних під час вимкнення бази даниї та відновлення;
- має стійку здатність до помилок;
- засіб перевірки ефективності є безкоштовним;
- може бути налаштований відповідно до вимог користувача;
- стандартна версія WinRadius безкоштовна.

Висновки до розділу 2

В даному розділі було наведено порядок проектування фізичної мережної інфраструктури організації та логічних зв'язків мережі зі схемою адресації.

Реалізована система віртуальних інтерфейсів, це призвело до зменшення адміністративних накладних витрат, необхідних для управління середовищем із багатьма комутаторами.

Також було проведено аналіз RADIUS–серверів, та обрано найкращий сервер для нашої мережі.

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 ВИБІР ОБЛАДНАННЯ, ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ

3.1 Вибір обладнання та програмного забезпечення

Для підсистеми аутентифікації користувачів комп'ютерної мережі організації на базі технології 802.1x та протоколу RADIUS потрібно таке обладнання:

- мережевий комутатор;
- маршрутизатор;
- RADIUS–сервер;
- супліканти.

Мережевий комутатор (англ. network switch) – пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента.

Маршрутизатор – електронний пристрій, що використовується для поєднання двох або більше мереж і керує процесом маршрутизації, тобто на підставі інформації про топологію мережі та певних правил приймає рішення про пересилання пакетів мережевого рівня (рівень 3 моделі OSI) між різними сегментами мережі.

Обрано комутатор Cisco SB SF250–48HP та маршрутизатор Cisco C1121–8p.

Cisco SB SF250–48HP — це якісний інтелектуальний комутатор, який поєднує в собі потужну продуктивність і надійність із повним набором функцій, необхідних для створення надійної бізнес–мережі.



Рисунок 3.1 – Комутатор Cisco SB SF250–48HP

Пристрій забезпечує функції безпеки й керування мережею, необхідні для запобігання несанкціонованому доступу користувачів до мережі та захисту ваших бізнес–даних. Виріб вмикають в інтегровану мережеву безпеку для зниження ризику порушень, безпеки портів IEEE 802.1x для контролю доступу до вашої мережі, запобігання атакам типу відмов в обслуговуванні (DoS) для збільшення часу безвідмовної роботи мережі під час атаки. Також комутатор підтримує списки контролю доступу (ACL) для захисту чутливих ділянок мережі від неавторизованих користувачів і захисту від мережевих атак. Комутатор підтримує технологію IEEE 802.1X та протокол RADIUS, що є ідеальним варіантом для нашої схеми.

Маршрутизатори інтегрованих служб Cisco серії 1000 (ISR) із програмним забезпеченням Cisco IOS® XE поєднують в собі доступ до Інтернету, всебічну безпеку та бездротові послуги (бездротова мережа LTE Advanced 3.0 і бездротова локальна мережа 802.11ac) в одному високопродуктивному пристрої.



Рисунок 3.2 – Маршрутизатор Cisco C1121–8p.

Маршрутизатори прості в розгортанні та управлінні, з окремими можливостями передачі даних. ISR серії Cisco 1000 добре підходять для розгортання обладнання для клієнтських приміщень (CPE) в корпоративних філіях. Маршрутизатор підтримує технологію IEEE 802.1X та протокол RADIUS.

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

Для відстежування мережевого трафіку в підсистемі аутентифікації користувачів комп'ютерної мережі було вирішено застосовувати програмне забезпечення Wireshark.

Wireshark (раніше звався Ethereal) — програма для аналізу мережевих пакетів Ethernet і інших мереж (сніфер) з вільним вихідним кодом. Має графічний інтерфейс користувача. У червні 2006 року проект був перейменований на Wireshark через проблеми з торговою маркою.

Wireshark перехоплює трафік і перетворює цей двійковий трафік у зручний для читання формат. Це дозволяє легко визначити, який трафік перетинає вашу мережу, скільки його, як часто, яка затримка між певними стрибками тощо.

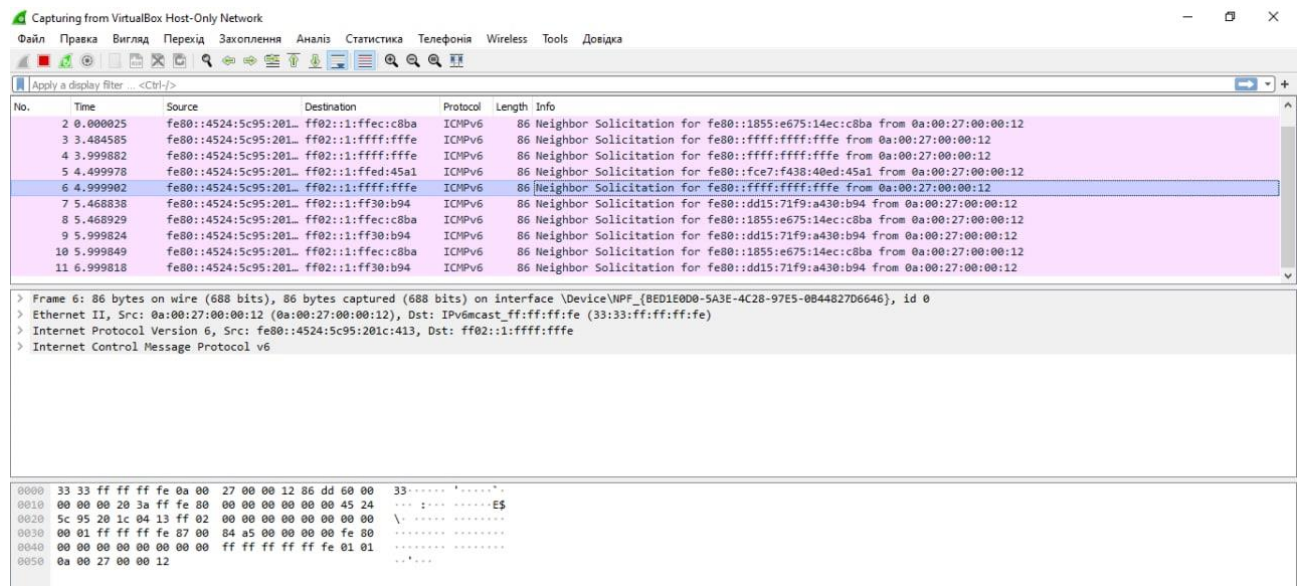


Рисунок 3.3 – Графічний інтерфейс програми Wireshark.

Існує так багато практичних застосувань Wireshark, що легко не помітити, яким ефективним інструментом навчання він може бути. Підняти капот автомобіля — найкращий спосіб зрозуміти, як працює двигун внутрішнього згоряння, а також підняти кришку від мережевого трафіку і спостерігати, як пролітають пакети — навіть до рівня байтів і вивчення заголовків TCP — це потужний спосіб навчитися та навчити інших, як працює Інтернет.

Програма розповсюджується під вільною ліцензією GNU GPL і використовує для формування графічного інтерфейсу кросплатформову

бібліотеку GTK+. Існують версії для більшості типів UNIX, зокрема GNU/Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X, а також для Microsoft Windows.

Восени 2013 розробники Wireshark, інтерфейс якого спочатку базувався на бібліотеці GTK+ і вже був адаптований для використання GTK+3, повідомили про перехід проекту на використання бібліотеки Qt.[5] Причиною міграції називається погіршення ситуації з ефективною підтримкою у GTK+ всіх платформ, для яких випускається Wireshark.

3.2. Налаштування роботи мережі та підсистеми аутентифікації

Для того, щоб спроектувати підсистему автентифікації користувачів комп'ютерної мережі організації в реальному житті, потрібно мати не малу кількість комп'ютерів, комутаторів, та маршрутизаторів, це немалі кошти, тому вирішено спроектувати нашу мережу віртуально, для цього потрібно програмне забезпечення, яке має можливість імітувати складні мережеві конструкції.

Існує цілий ряд мережевих емуляторів, які можна вибрати, щоб отримати доступ до моделювання віртуальної мережі преміум якості. Але коли справа доходить до вибору між найкращими інтерфейсами віртуального моделювання, тоді порівняння повинно бути між GNS3 та Eve-NG проти VIRL. Розглянемо їх переваги та недоліки і виберемо найкращий емулятор для нашої мережі.

GNS3— дозволяє імітувати складні мережеві конструкції, такі як маршрутизатор/комутатор Cisco, персональний комп'ютер. Ця програма має відкритий код та є безкоштовною. Програма дозволяє запускати реальні образи Cisco IOS за допомогою Dynamips в інфраструктурі GNS3, та за допомогою цього програмного забезпечення можна створювати складні мережеві конструкції на своєму комп'ютері.

Vir1 – це власний емулятор віртуальної мережі, винайдений компанією Cisco, який високо цінується людьми та навчальними закладами. Він є ефективним в емуляції мереж підприємств.

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

EVE-NG – це форма симулятора віртуальної мережі з багатьма постачальниками, яка була розроблена для приватних осіб та малого бізнесу. Він випускається як у безкоштовній версії, так і у професійній версії, плата за яку сплачується щороку.

Таблиця 3.1 – Порівняння GNS3, VIRL та EVE-NG

	GNS3	VIRL	EVE-NG
Походження	Безкоштовний інтерфейс сервера / клієнта з відкритим кодом, призначений для віртуалізації та емуляції мережі. Це платформа на основі Python	Компанія Cisco винайшла власний емулятор віртуальної мережі, який високо цінується людьми та навчальними закладами. Кращий вибір для корпоративної мережі.	Перший безклієнтський симулятор віртуальної мережі з багатьма постачальниками, розроблений для приватних осіб та малого бізнесу.
Простий у використанні	Легкий	Складний	Середній
Доступ до програмних зображень (IOU, IOS)	Доступно лише за договором про надання послуг або програмою, яку проводить коледж.	Можливість отримати доступ до них із щорічною підпискою.	Доступно лише за договором про надання послуг або програмою, яку проводить коледж.
Оптимізація ресурсів та підтримка	Використання ресурсів та підтримка інтерфейсу є кращими, ніж VIRL.	Обмежений базовий ресурс, оптимальне використання серверного пристрою та нестача підтримки послідовних інтерфейсів.	Використання ресурсів та підтримка інтерфейсу є кращими, ніж VIRL.
Вимога щодо застосування терміналу	Потрібен окремий термінальний додаток для функціонування та	Потрібен окремий термінальний додаток для функціонування та	Для побудови та модифікації топології мережі потрібен лише

	зміни топології мережі.	зміни топології мережі.	легкий термінальний додаток, такий як Putty. Може використовуватися як на настільних, так і на мобільних пристроях.
--	-------------------------	-------------------------	---

GNS3 та EVE-NG мають перевагу над VIRL, завдяки тому що VIRL має обмежений базовий ресурс та складний інтерфейс для новачка.

Після перегляду графічного інтерфейсу та інструкцій по даним емуляторам було прийнято використовувати GNS3.

Розглянемо детальніше переваги та недоліки цієї програми.

Переваги GNS3:

- безкоштовне програмне забезпечення;
- підтримує всі зображення IOS та IOU;
- підтримує різні гіпервізори (у тому числі і VirtualBox);
- кількість пристроїв мережі не обмежена;
- підтримує пристрої багатьох марок;
- не потрібно додаткове програмне забезпечення для віртуалізації.

Програма має як переваги, так і недоліки:

- Зображення IOS завантажується виключно користувачем.
- Програма працює на продуктивності вашого комп'ютера (тобто при віртуалізації комутаторів/маршрутизаторів/комп'ютерів використовується ваше обладнання: ЦП та оперативна пам'ять)

Отже, за допомогою GNS3 ми створюємо віртуальну мережу з вбудованими комутаторами та маршрутизаторами, також ми маємо встановити RADIUS-сервер та різні ОС, на яких зможемо перевірити аутентифікацію. Для цього ми використовуємо гіпервізор.

Гіпервізор також відомий як Virtual Machine Manager (VMM), і його єдиною метою є надання можливості декільком "машинам" спільно використовувати одну апаратну платформу. Операційні системи спроектовані

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

таким чином, що вони мають взаємозв'язок "один з одним" із апаратним забезпеченням, на якому працюють.

Гіпервізор відокремлює операційну систему(ОС) з обладнання, відповідаючи за те, щоб дозволити кожному часу роботи ОС з базовим обладнанням. Він виконує функцію коп-трафіку, що дає час використовувати процесор, пам'ять, GPU та інше обладнання. Кожна операційна система, керована гіпервізором, називається гостьовою ОС, а операційна система гіпервізора, якщо така є, називається хост-ОС. Оскільки він знаходиться між гостьовою ОС та обладнанням, у вас може бути стільки різних гостьових ОС, скільки ваша система може працювати; Ви навіть можете мати різні типи (наприклад, Windows, OS X, Linux).

Існує безліч гіпервізорів, але виділимо три найпопулярніші:

- VirtualBox;
- VMware;
- Hyper-V.

Таблиця 3.2 – Порівняння VirtualBox, VMware, Hyper-V

	VirtualBox	VMware	Hyper-V
Простий у використанні	Середній	Легкий	Складний
Інтеграція Windows	Так	Так	Ні
Шифрування	Так	Так (за допомогою гостьових додатків)	Так
Сумісні системи	Windows, Linux, macOS	Windows, Linux, macOS	Windows та Linux
Ціна	Безкоштовно/Платно	Безкоштовно	Безкоштовно
Інше	Відмінна безпека	Відкрите джерело	

Оскільки VirtualBox легкий у використанні, має усі необхідні сумісні системи для нашої схеми, та відмінно інтегрується в GNS3, ми використовуємо його.

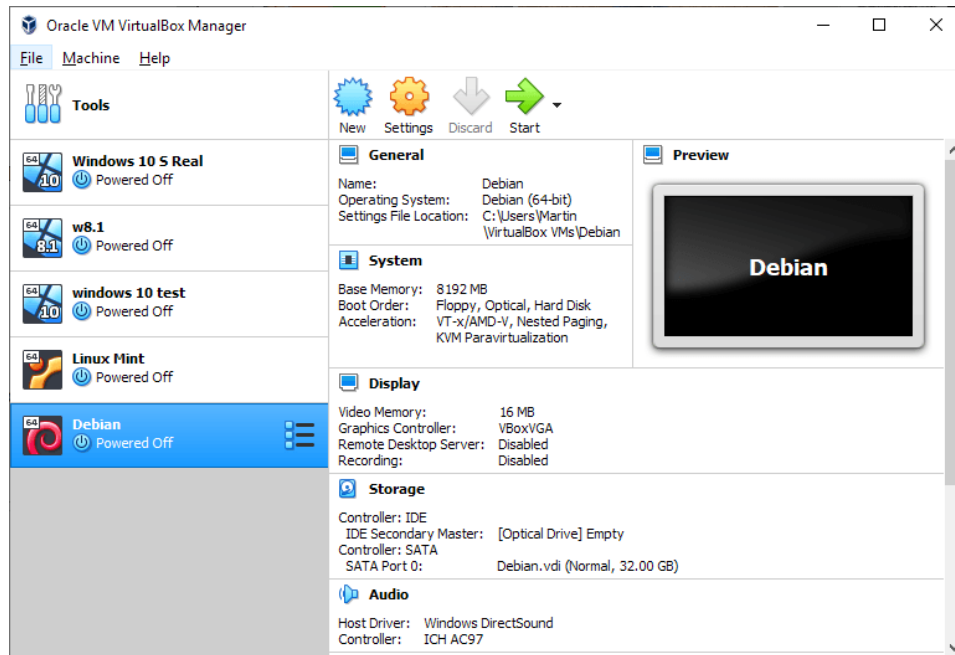


Рисунок 3.4 – Приклад створених ОС в VirtualBox

Розпочнемо налаштування нашої мережі.

Для налаштування взаємодії між декількома віртуальними мережами (Vlan), розташованими в одній мережі, потрібно мати маршрутизатор, підключений до комутатора через Trunk порт. При передачі трафіку з цього порту кожен пакет позначається номером Vlan, якому належить. Це дає їм змогу коректно перенаправляти пакети. На цьому інтерфейсі налаштовуються сабінтерфейси (subinterfaces) з відповідними ір адресами для кожної з мереж Vlan. Розглянемо сценарій налагодження:

```
...
R_3_13_1# configure termina
R_3_13_1(config)#int f0/0.1
R_3_13_1(config-subif)#encapsulation dot1q 1 native
R_3_13_1(config-subif)#ip add 203.3.13.1 255.255.255.0
R_3_13_1(config-subif)#no sh
R_3_13_1(config)#int f0/0.10
R_3_13_1(config-subif)#encapsulation dot1q 10
R_3_13_1(config-subif)#ip add 204.3.13.1 255.255.255.0
R_3_13_1(config-subif)#description LAN10
R_3_13_1(config-subif)#no sh
...
...
R_3_13_1(config)#int f0/0.40
R_3_13_1(config-subif)#encapsulation dot1q 40
R_3_13_1(config-subif)#ip add 207.3.13.1 255.255.255.0
R_3_13_1(config-subif)#no sh
```

```
R_3_13_1(config-subif)#description LAN40
R_3_13_1(config-subif)#ex
...
```

Наступний крок це налаштування транкових каналів, через які буде рухатись трафік різних VLAN.

```
...
SW_3_13_1(config)#int e0/0
SW_3_13_1(config-if)#switchport trunk allowed vlan 1,10-40
SW_3_13_1(config-if)#switchport trunk encapsulation dot1q
SW_3_13_1(config-if)#switchport mode trunk
SW_3_13_1(config-if)#no sh
SW_3_13_1(config-if)#ex
...
...
SW_3_13_1(config)#int e2/0
SW_3_13_1(config-if)#switchport trunk allowed vlan 1,10-40
SW_3_13_1(config-if)#switchport trunk encapsulation dot1q
SW_3_13_1(config-if)#switchport mode trunk
SW_3_13_1(config-if)#switchport mode trunk
SW_3_13_1(config-if)#no sh
SW_3_13_1(config-if)#ex
SW_3_13_1(config)#int vlan 1
SW_3_13_1(config-if)#ip add 203.3.13.4 255.255.255.0
SW_3_13_1(config-if)#no sh
SW_3_13_1(config-if)#ex
...
```

Налаштовуємо віртуальні мережі на коммутаторах SW_3_13_2–SW_3_13_3, та надаємо доступи до віртуальних мереж. Сценарій налагодження:

```
SW_3_13_1(config)#int vlan 1
SW_3_13_1(config-if)#ip add 203.3.13.3 255.255.255.0
SW_3_13_1(config-if)#no sh
SW_3_13_1(config)#int vlan 10
SW_3_13_1(config-if)#ip add 204.3.13.254 255.255.255.0
SW_3_13_1(config-if)#no sh
SW_3_13_1(config-if)#ex
SW_3_13_1(config)#int e0/0
SW_3_13_1(config-if)#switchport trunk allowed vlan 1,10-40
SW_3_13_1(config-if)#switchport trunk encapsulation dot1q
SW_3_13_1(config-if)#switchport mode trunk
SW_3_13_1(config-if)#no sh
SW_3_13_1(config)#int e0/1
SW_3_13_1(config-if)#switchport access vlan 10
SW_3_13_1(config-if)#switchport mode access
SW_3_13_1(config-if)#switchport access vlan 10
SW_3_13_1(config-if)#no sh
```

Після того як ми сформували всі VLAN – інтерфейси, переходимо до налаштування RADIUS – аутентифікації. Для початку потрібно увімкнути технологію AAA , глобально дозволити аутентифікацію на основі портів 802.1X та визначити сервер аутентифікації, зазначити порти та ключ доступу до WinRadius. Сценарій налагодження:

```
SW_3_13_2(config)#aaa new-model
SW_3_13_2(config)#dot1x system-auth-control
SW_3_13_2(config)#aaa group server radius packetfence
SW_3_13_2(config-sg-radius)#server 203.3.13.2 auth-port 1812 acct-port 1813
SW_3_13_2(config-sg-radius)#aaa authentication login default local
SW_3_13_2(config)#aaa authentication dot1x default group packetfence
SW_3_13_2(config)#aaa authorization network default group packetfence
SW_3_13_2(config)#$ radius-serverhost 203.3.13.2 auth-port 1812 acct-port 1813
timeout 2 key WinRadius
SW_3_13_2(config)#radius-server vsa send authentication
SW_3_13_3(config)#aaa new-model
SW_3_13_3(config)#dot1x system-auth-control
SW_3_13_3(config)#aaa group server radius packetfence
SW_3_13_3(config-sg-radius)#server 203.3.13.2 auth-port 1812 acct-port 1813
SW_3_13_3(config-sg-radius)#aaa authentication login default local
SW_3_13_3(config)#aaa authentication dot1x default group packetfence
SW_3_13_3(config)#aaa authorization network default group packetfence
SW_3_13_3(config)#$ radius-serverhost 203.3.13.2 auth-port 1812 acct-port 1813
timeout 2 key WinRadius
SW_3_13_3(config)#radius-server vsa send authentication
```

Також проводимо налагодження RADIUS-аутентифікації на інших комутаторах. Для того, щоб користувачі з'єднувались з мережой тільки за допомогою RADIUS-аутентифікації, ми повинні це указати на їх інтерфейсах, тому ініціюємо автентифікацію на основі порту та обміну повідомленнями, далі надаємо дозвіл на використання лише порту 802.1x, після того, як аутентифікація супліканта прийнята сервером аутентифікації, комутатор надає йому доступ. Обираємо пріоритет автентифікації за замовчуванням. Сценарій налагодження:

```
...
SW_3_13_2(config)#int e0/1
SW_3_13_2(config-if)#switchport mode access
SW_3_13_2(config-if)#authentication host-mode single-host
SW_3_13_2(config-if)#authentication order dot1x
SW_3_13_2(config-if)#authentication port-control auto
SW_3_13_2(config-if)#authentication priority dot1x
...
...
```

```

SW_3_13_2(config)#int e0/5
SW_3_13_2(config-if)#switchport mode access
SW_3_13_2(config-if)#authentication host-mode single-host
SW_3_13_2(config-if)#authentication order dot1x
SW_3_13_2(config-if)#authentication port-control auto
SW_3_13_2(config-if)#authentication priority dot1x
...

```

Проводимо налагодження інтерфейсів на інших коммутаторах з суплікантами. Надаємо дозвіл суплікантам на періодичну аутентифікацію, яка за замовченням вимкнена, та задаємо їй значення в 10800 секунд. Налагодження інтерфейса e0/1 на комутаторі SW_3_13_2:

```

SW_3_13_2(config)#int e0/1
SW_3_13_2(config-if)#authentication periodic
SW_3_13_2(config-if)#authentication timer restart 10800
SW_3_13_2(config-if)#authentication timer reauthentication 10800
SW_3_13_2(config-if)#authentication timer reauthenticate 10800
...
...
SW_3_13_2(config)#int e0/5
SW_3_13_2(config-if)#authentication periodic
SW_3_13_2(config-if)#authentication timer restart 10800
SW_3_13_2(config-if)#authentication timer reauthentication 10800
SW_3_13_2(config-if)#authentication timer reauthenticate 10800

```

Встановлюємо WinRadius на сервер для аутентифікації пристроїв мережі, встановлюємо пароль та порт для комутаторів.

Розглянемо налаштування на рис.3.5

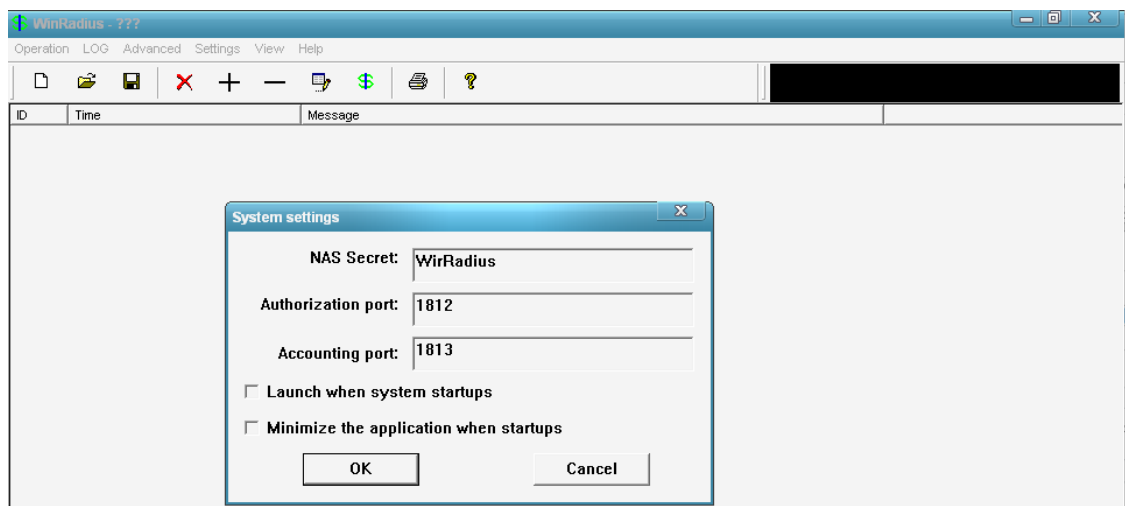


Рисунок 3.5. Налаштування WinRadius на сервері

Налаштовуємо 802.1x на Windows XP/7

Розглянемо налаштування 802.1x на рисунках 3.6 –3.7

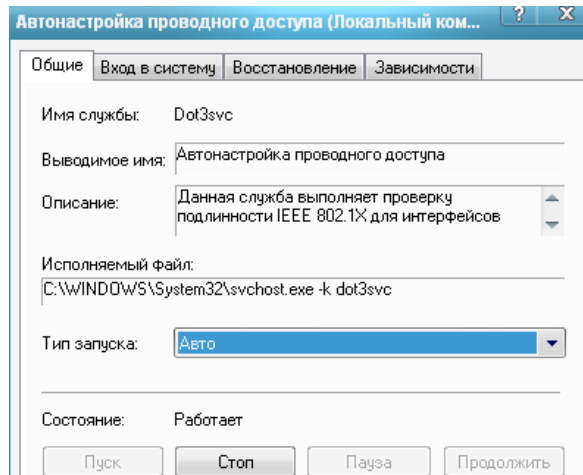


Рисунок 3.6. Вмикаємо службу автоматичного доступу (802.1x) на Windows

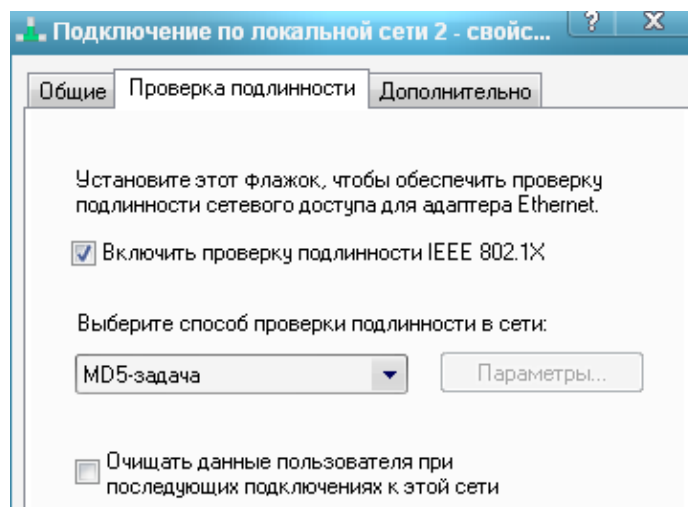


Рисунок 3.7. Обираємо спосіб перевірки аутентифікації на Windows

Налаштовуємо 802.1x на Ubuntu

Розглянемо налаштування 802.1x на рисунку 3.8

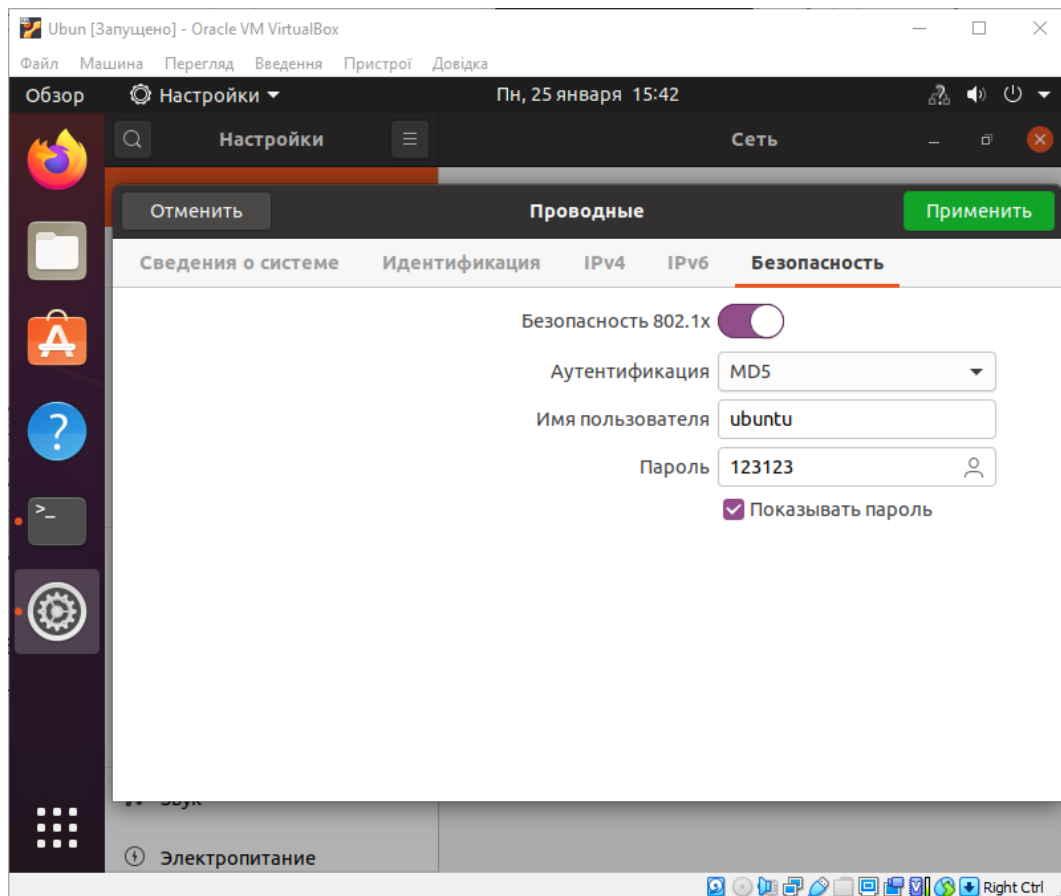


Рисунок 3.8. Вмикаємо службу автоматичного доступу (802.1x) на ОС Ubuntu
 Задаємо IPV4 адресу на Windows XP/7, Ubuntu, Kali Linux.
 Розглянемо налаштування на рисунках 3.9–3.11

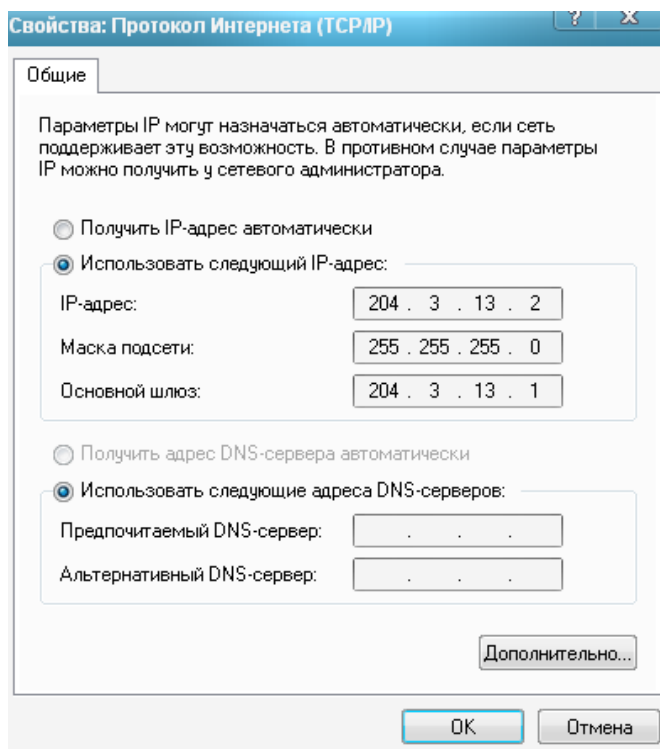


Рисунок 3.9. Задання IPv4-адреси на ОС Windows xp

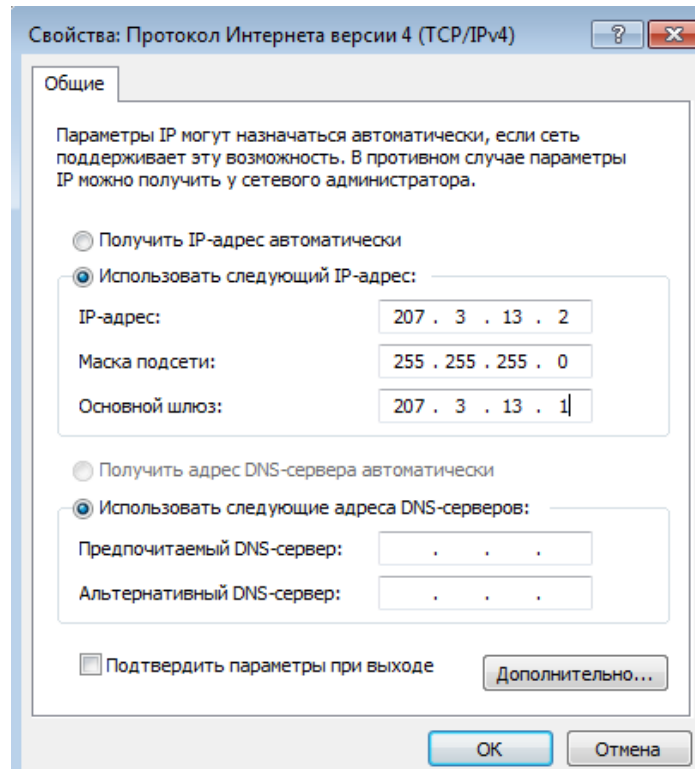


Рисунок 3.10. Задання IPv4-адреси на ОС Windows 7

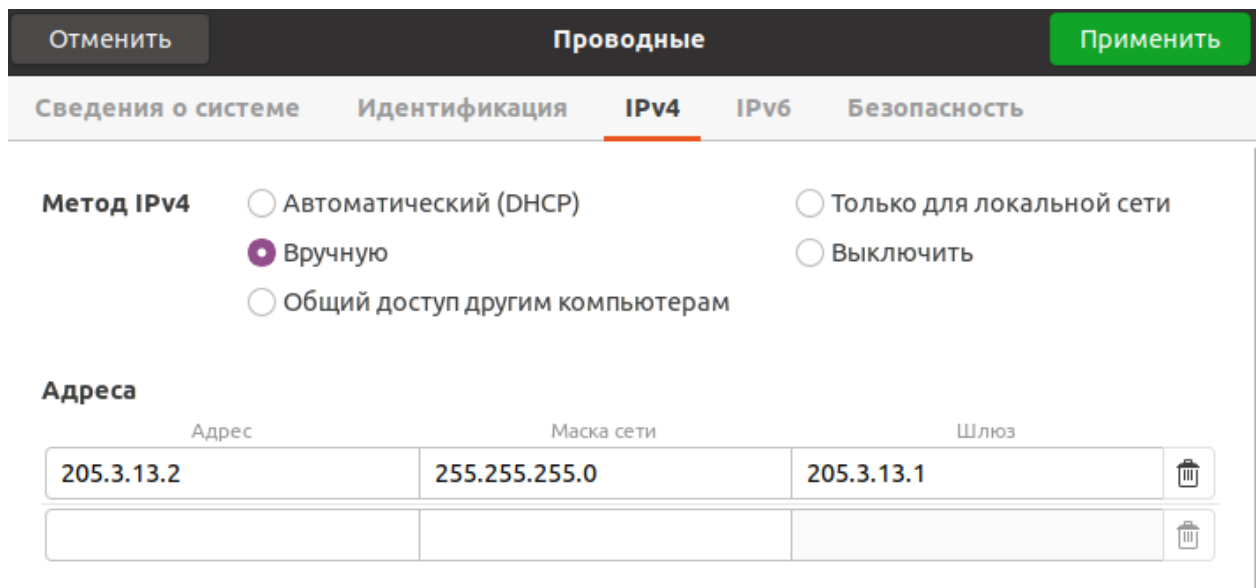


Рисунок 3.11. Задання IPv4-адреси на ОС Ubuntu

3.3. Перевірка працездатності мережі

Для перевірки працездатності мережі, потрібно провести такі дії:

1. Перевірити налаштування аутентифікації користувачів (IEEE 802.1x, EAP, RADIUS) на комутаторах з кінцевими вузлами за допомогою вбудованої команди **show dot1x int e0/1 detail**.

2. Створити користувачів на RADIUS – сервері для різних вланів, за допомогою вбудованого графічного інтерфейсу.
3. Провести спроби з'єднання з мережої, за допомогою створених користувачів на RADIUS – сервері.
4. Після вдалого підключення до підсистеми, перевірити зв'язок між суплікантами.
5. Перевірити логи авторизації на RADIUS – сервері.
6. Перевірити на комутаторах успішну авторизації суплікантів.

Перевіримо налаштування dot1x на інтерфейсі супліканта за допомогою команди **show dot1x int e0/1 detail**

```
SW_3_13_2#show dot1x int e0/1 detail
Dot1x Info for Ethernet0/1
-----
PAE                               = AUTHENTICATOR
QuietPeriod                       = 2
ServerTimeout                     = 0
SuppTimeout                       = 30
ReAuthMax                         = 2
MaxReq                            = 2
TxPeriod                          = 30
Dot1x Authenticator Client List Empty
```

Рисунок 3.12 – Перевірка dot1x на інтерфейсі супліканта

Створюємо користувачів на WinRadius–сервері для аутентифікації на комутаторах

Розглянемо налаштування на рисунках 3.13–3.15

Add user

User name:

Password:

Group:

Address:

Cash prepaid: Cents

Expiry date:

Note: yyyy/mm/dd means expiry date; digit means valid days since first login; empty means never expired.

Others:

☐ Prepaid user ☒ Postpaid user

Accounting method:

Рисунок 3.13. Створення користувача для ОС WindowsXP

Add user

User name:

Password:

Group:

Address:

Cash prepaid: Cents

Expiry date:

Note: yyyy/mm/dd means expiry date; digit means valid days since first login; empty means never expired.

Others:

☐ Prepaid user ☒ Postpaid user

Accounting method:

Рисунок 3.14. Створення користувача для ОС Ubuntu

Add user

User name:

Password:

Group:

Address:

Cash prepaid: Cents

Expiry date:

Note: yyyy/mm/dd means expiry date; digit means valid days since first login; empty means never expired.

Others:

☐ Prepaid user ☒ Postpaid user

Accounting method:

Рисунок 3.15. Створення користувача для ОС Windows7

Перевірка аутентифікації користувачів Windows та Ubuntu

Розглянемо на рисунках 3.16–3.21

Состояние Подключения: по локальной се...

Общие Поддержка

Ввод учетных данных

Пользователь:

Пароль:

Домен:

Рисунок 3.16. Аутентифікація користувача з Windows

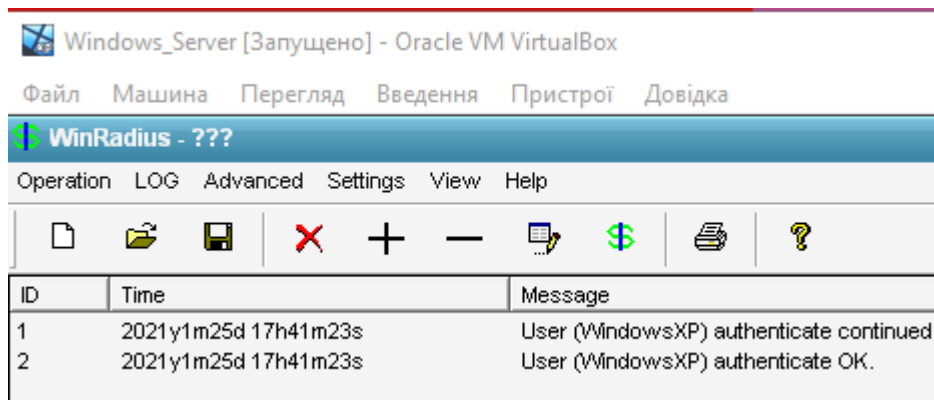


Рисунок 3.17. Успішна активація WindowsXP

Перевіримо чи авторизованих користувачів на комутаторі SW_3_13_2 за допомогою команди **show authentication sessions**

```
SW_3_13_2#sho authentication sessions
```

Interface	MAC Address	Method	Domain	Status	Fg	Session ID
Eth0/0	0800.27d0.d703	dot1x	DATA	Auth		CB030D030000000C00005836

Рисунок 3.18. Перевірка авторизованих користувачів на SW_3_13_2

Проводные Применить

Аутентификация IPv4 IPv6 **Безопасность**

Безопасность 802.1x ☒

Аутентификация MD5

Имя пользователя

Пароль

☒ Показывать пароль

Рисунок 3.19. Аутентифікація користувача з Ubuntu

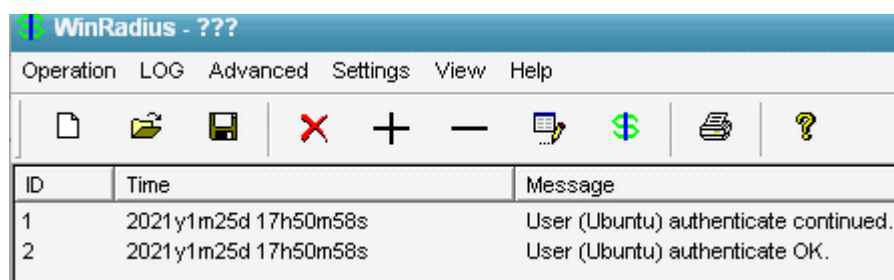


Рисунок 3.20. Успішна активація Ubuntu

```
SW_3_13_3#sho authentication sessions

Interface    MAC Address    Method  Domain  Status Fg Session ID
Et0/1        0800.27f0.5df1 dot1x    DATA   Auth    CD030DFE0000000C002A41CD

Session count = 1
```

Рисунок 3.21 Перевірка авторизованих користувачів на SW_3_13_3

Висновки до розділу 3

В даному розділі було наведено порядок вибору обладнання та програмного забезпечення для віртуалізації підсистеми аутентифікації користувачів в комп'ютерній мережі організації.

Реалізована віртуальна схема в GNS3, налаштована мережа та розподілена по віртуальним інтерфейсам, налаштована аутентифікація користувачів комп'ютерної мережі організації на базі технології 802.1x та протоколу RADIUS.

Також було проведено тестування комп'ютерної мережі, за допомогою аутентифікації на різних ОС через RADIUS – сервер. Знайдені помилки було виправлено, аутентифікація працює коректно та виконує поставлені задачі

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

Під час виконання випускної роботи бакалавра було спроектовано та реалізовано проект підсистеми аутентифікації користувачів комп'ютерної мережі організації на базі технології 802.1x та протоколу RADIUS,

Аутентифікація важлива, оскільки вона дозволяє організаціям захищати свої мережі, дозволяючи лише автентифікованим користувачам (або процесам) доступ до захищених ресурсів, які можуть включати комп'ютерні системи, мережі, бази даних, веб-сайти та інші мережеві додатки чи послуги.

Для проектування та реалізації проекту підсистеми аутентифікації користувачів комп'ютерної мережі організації на базі технології 802.1x та протоколу RADIUS було вирішено наступні завдання:

1. Задля чіткого розуміння поставленої задачі було детально описано постановку задачі, розглянуто особистості та методи аутентифікації користувачів комп'ютерної мережі.
2. Вивчаючи, як саме проходить аутентифікація, проведено аналіз між протоколами аутентифікації, огляд наявних аналогів та виявлення їх недоліків та переваг один між одним.
3. Для розподілу користувачів було прийнято використовувати віртуальні інтерфейси, це призвело до зменшення адміністративних накладних витрат, необхідних для управління середовищем із багатьма комутаторами.
4. Було розглянуто різні RADIUS – сервери, знайшли їх переваги та недоліки, вирішили який сервер потрібно використовувати в нашій підсистемі аутентифікації користувачів комп'ютерної мережі організації на базі технології 802.1x.
5. Було обрано обладнання для комп'ютерної мережі організації, основними вимоги до пристроїв була підтримка технології IEEE 802.1X та протоколу RADIUS.

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

6. У зв'язку з тим, що обладнання коштує немалих грошей, було прийнято рішення віртуалізувати підсистему, проаналізувавши різні емулятори, їх недоліки та переваги, обрали найкращу для нас систему.
7. Провели налаштування віртуальних інтерфейсів, RADIUS – протокола, визначили суплікантів, аутентифікаторів та сервера аутентифікації.
8. Під час розробки підсистеми проводилися постійні тестування роботи окремих частин, здійснювалися спроби аутентифікації.

В результаті було розроблено структуру ядра комп'ютерної мережі. Наведено загальну кількість необхідного обладнання. Для побудованої мережі розроблено схему її адресації, яка дозволяє легке управління адресами пристроїв та призначена до подальшого розширення комп'ютерної мережі організації на базі технології 802.1x та протоколу RADIUS.

Реалізована підсистема має весь необхідний функціонал для аутентифікації користувачів на сервері RADIUS за допомогою технології 802.1X та EAP, проте в подальшому планується робота над розширенням можливостей підсистеми, здійснення гостьових аутентифікацій та вивчення теми багатофакторної аутентифікації.

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Книги:

1. Дж.Бони. Руководство по CiscoIOS. – Издательство "Русская редакция", 2008. – 784 с
2. Jim Geier. Implementing 802.1X Security Solutions for Wired and Wireless Networks. – (1st Edition)
3. Гольдштейн Б. Протоколы AAA: RADIUS и Diameter / Борис Гольдштейн.. – (Книга 9 Телекоммуникационные протоколы).
4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3–е изд. – СПб.: Питер, 2005. – 958 с.
5. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. – СПб.: Питер, 2002. – 544 с.
6. Odom Wendell. CCNA 200–301 Official Cert Guide. Volume 1. / Wendell Odom. Cisco Press, 2020 – 1095 p.
7. Odom Wendell. CCNA 200–301 Official Cert Guide. Volume 2. / Wendell Odom. Cisco Press, 2020 – 1444 p.
8. Буров Є.В. Комп'ютерні мережі. Підручник. Том 1. / Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2019. – 334 с.
9. Буров Є.В. Комп'ютерні мережі. Підручник. Том 2. / Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2019. – 204 с.
10. Микитишин А.Г. Комп'ютерні мережі. Книга 2. Навчальний посібник. / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів, «Магнолія 2006», 2013. – 328 с.
11. Микитишин А.Г. Комп'ютерні мережі. Книга 1. Навчальний посібник / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник – Львів, «Магнолія 2006», 2013. – 256 с.

Електронні ресурси:

12. Топологія мереж [Електронний ресурс] – Режим доступу до ресурсу:
<https://www.omnisci.com/technical-glossary/network-topology>

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

13. Методи аутентифікації [Електронний ресурс] – Режим доступу до ресурсу: <https://www.sailpoint.com/identity-library/authentication-methods-used-for-network-security/>
14. Протокол Radius [Електронний ресурс] – Режим доступу до ресурсу: <https://uk.wikipedia.org/wiki/RADIUS>
15. Налаштування HSRP на Cisco. [Електронний ресурс]. Режим доступу: <http://snakeproject.ru/rubric/article.php?art=hsrp>
16. Принципи маршрутизації і комутації CCNA: Мережа VLAN. [Електронний ресурс]. Режим доступу: <https://static-course-assets.s3.amazonaws.com/RSE6/ru/index.html#6.0.1.1>
17. Протокол 802.1x [Електронний ресурс] – Режим доступу до ресурсу: <https://www.intel.com/content/www/us/en/support/articles/000006999/wireless/legacy-intel-wireless-products.html>
18. Протокол Ethernet [Електронний ресурс] – Режим доступу до ресурсу: <https://www.juniper.net/documentation/us/en/software/junos/interfaces-security-devices/topics/topic-map/security-interface-ipv4-ipv6-protocol.html>
19. Протокол RADIUS [Електронний ресурс] – Режим доступу до ресурсу: <https://en.wikipedia.org/wiki/RADIUS>
20. Порівняння емуляторів мереж [Електронний ресурс] – Режим доступу до ресурсу: <https://ipwithease.com/gns3-vs-eve-ng-vs-virl/>
21. Аутентифікація [Електронний ресурс] – Режим доступу до ресурсу: <https://www.securew2.com/blog/the-importance-of-authentication-security>.
22. WinRadius [Електронний ресурс] – Режим доступу до ресурсу: http://www.softsea.com/review/WinRadius.html#google_vignette
23. Налаштування IEEE 802.1X [Електронний ресурс] – Режим доступу до ресурсу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_8021x/configuration/xr-3se/3850/sec-user-8021x-xr-3se-3850-book/sec-ieee-8021x-vlan-assign.html

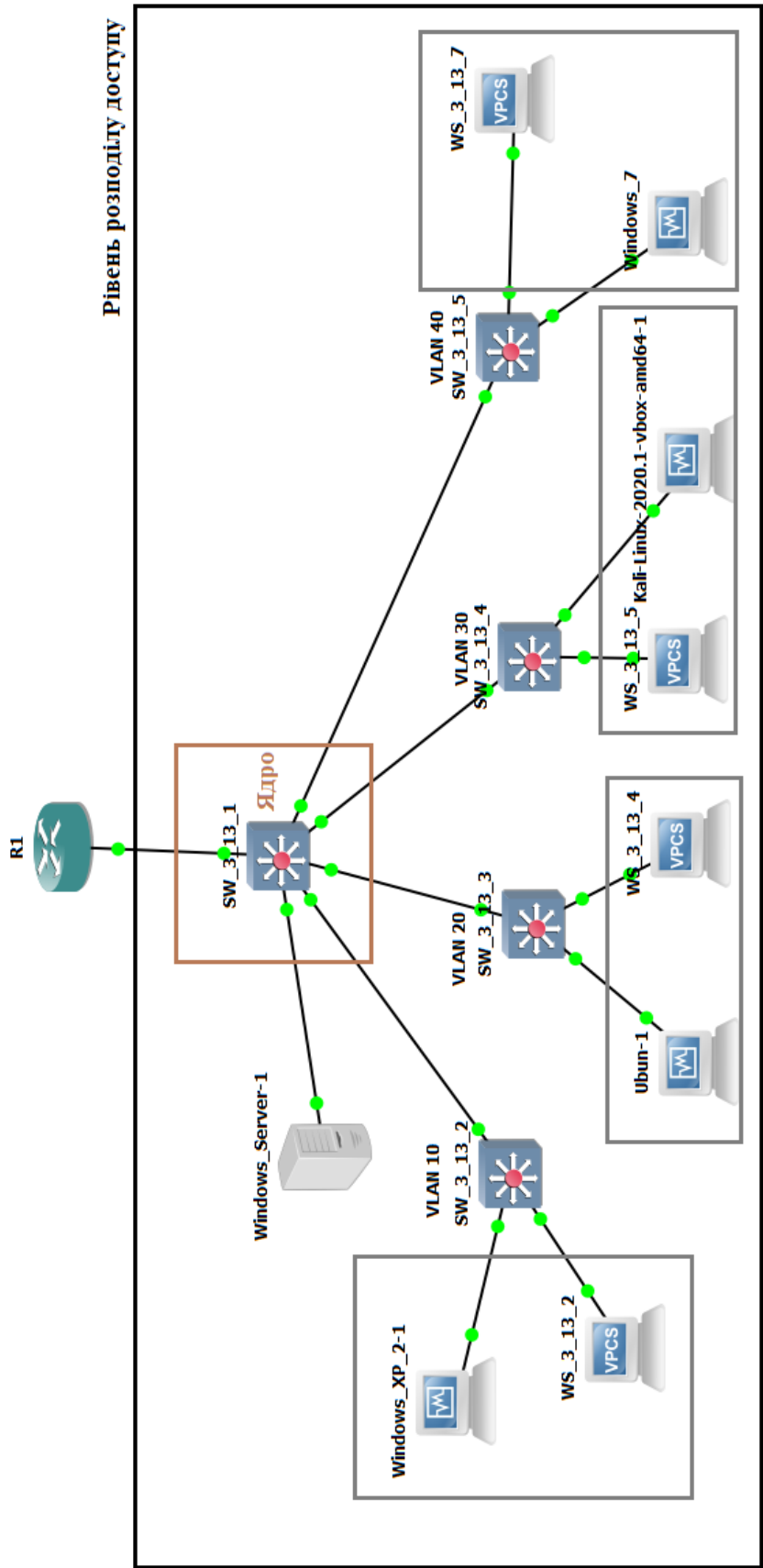
24. Технологія AAA [Електронний ресурс] – Режим доступу до ресурсу: [https://uk.wikiqube.net/wiki/Authentication_protocol#AAA_architecture_protocols_\(Authentication,_Authorization,_Accounting\)](https://uk.wikiqube.net/wiki/Authentication_protocol#AAA_architecture_protocols_(Authentication,_Authorization,_Accounting))
25. RADIUS та TACACS+ [Електронний ресурс] – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/difference-between-tacacs-and-radius/>
26. Гіпервізори [Електронний ресурс] – Режим доступу до ресурсу: <https://www.sim-networks.com/blog/hypervisors-vmware-kvm-xen-openvz>

		Лісовський М.С.			КІК.КР.Б-123-13-ПЗ	Арк.
		Єфіменко А.А.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Лісовський М.С.			ЖИТОМИРСЬКА ПОЛІТЕХНІКА 21.123.13.000	Арк.
		Єфіменко А.А.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

Схема комп'ютерної мережі організації



Файли конфігурацій мережних пристроїв

Файл конфігурації маршрутизатора R_3_13_1

hostname R_3_13_1 ! boot-start-marker boot-end-marker no aaa new-model ip source-route no ip icmp rate-limit unreachable ip cef !! no ip domain lookup no ipv6 cef ! multilink bundle-name authenticated ! redundancy !! ip tcp synwait-time 5 ! interface FastEthernet0/0 ip address 202.3.13.1 255.255.255.0 duplex half ! interface FastEthernet0/0.1 encapsulation dot1Q 1 native	ip address 203.3.13.1 255.255.255.0 interface FastEthernet0/0.10 encapsulation dot1Q 10 ip address 204.3.13.1 255.255.255.0 !interface FastEthernet0/0.20 encapsulation dot1Q 20 ip address 205.3.13.1 255.255.255.0 ! interface FastEthernet0/0.30 encapsulation dot1Q 30 ip address 206.3.13.1 255.255.255.0 ! interface FastEthernet0/0.40 encapsulation dot1Q 40 ip address 207.3.13.1 255.255.255.0 ! interface FastEthernet1/0 no ip address duplex half ! ! interface FastEthernet1/0.10
---	--

Файл конфігурації комутатора SW_3_13_1

Комутатор SW_3_13_1 hostname SW_3_13_1 ! boot-start-marker boot-end-marker !! logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL logging buffered 50000 logging console discriminator EXCESS ! no aaa new-model no ip icmp rate-limit unreachable	switchport trunk encapsulation dot1q switchport mode trunk interface Ethernet0/1 switchport trunk allowed vlan 1,10-40 switchport trunk encapsulation dot1q switchport mode trunk ! interface Ethernet0/2 switchport trunk allowed vlan 1,10-40 switchport trunk encapsulation dot1q switchport mode trunk ! interface Ethernet0/3 switchport trunk allowed vlan 1,10-40
--	---

		Лісовський М.С.			ЖИТОМИРСЬКА ПОЛІТЕХНІКА 21.123.13.000	Арк.
		Єфіменко А.А.				61
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
no ip domain-lookup
ip cef
no ipv6 cef
!!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy
ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
switchport trunk allowed vlan 1,10-40

```

```

switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/0
switchport trunk allowed vlan 1,10-40
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet1/1
switchport trunk allowed vlan 10-40
switchport trunk encapsulation dot1q
switchport mode access
!
interface Vlan1
ip address 203.3.13.4 255.255.255.0

```

Файл конфігурації комутатора SW_3_13_2 – SW_3_13_4

Комутатор SW_3_13_2

```

hostname SW_3_13_2
!
boot-start-marker
boot-end-marker
!!
logging discriminator EXCESS severity
drops 6 msg-body drops
EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5
$1$VBnb$4LruVikbpX5qSmCPVbytb.
!
username admin privilege 15 password
0 123123
aaa new-model
!
aaa group server radius packetfence
server 203.3.13.2 auth-port 1812 acct
port 1813
!
aaa authentication login default local
aaa authentication dot1x default group
packetfence

```

Комутатор SW_3_13_3

```

hostname SW_3_13_3
!
boot-start-marker
boot-end-marker
!!
logging discriminator EXCESS severity
drops 6 msg-body drops
EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5
$1$VBnb$4LruVikbpX5qSmCPVbytb.
!
username admin privilege 15 password
0 123123
aaa new-model
!
aaa group server radius packetfence
server 203.3.13.2 auth-port 1812 acct
port 1813
!
aaa authentication login default local
aaa authentication dot1x default group
packetfence

```

```

!!!!!!
aaa session-id common
!!!!!!
no ip icmp rate-limit unreachable
!!!
no ip domain-lookup
ip cef
no ipv6 cef
!!
dot1x system-auth-control
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy
ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
switchport trunk allowed vlan 1,10-40
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport access vlan 20
switchport mode access
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer reauthenticate
10800
authentication timer restart 10800
mab
no snmp trap link-status
dot1x pae authenticator
dot1x timeout quiet-period 2
dot1x timeout tx-period 3
!
interface Ethernet0/2
switchport access vlan 20
switchport mode access
!
interface Vlan1
ip address 203.3.13.252 255.255.255.0

```

```

!!!!!!
aaa session-id common
!!!!!!
no ip icmp rate-limit unreachable
!!!
no ip domain-lookup
ip cef
no ipv6 cef
!!
dot1x system-auth-control
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy
ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
switchport trunk allowed vlan 1,10-40
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
switchport access vlan 20
switchport mode access
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer reauthenticate
10800
authentication timer restart 10800
mab
no snmp trap link-status
dot1x pae authenticator
dot1x timeout quiet-period 2
dot1x timeout tx-period 3
!
interface Ethernet0/2
switchport access vlan 20
switchport mode access
!
interface Vlan1
ip address 203.3.13.252 255.255.255.0

```

```

!
interface Vlan10
ip address 204.3.13.254 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
snmp-server community public RO
snmp-server community private RW
!
radius-server host 203.3.13.2 auth-port
1812 acct-port 1813 timeout 2 key
WirRadius
!!
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

```

```

!
interface Vlan20
ip address 205.3.13.254 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
snmp-server community public RO
snmp-server community private RW
!
radius-server host 203.3.13.2 auth-port
1812 acct-port 1813 timeout 2 key
WirRadius
!!
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

```

```

Комутатор SW_3_13_4
hostname SW_3_13_4
!
boot-start-marker
boot-end-marker
!!
logging discriminator EXCESS severity
drops 6 msg-body drops
EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5
$1$hB2O$bS7RjZeY79X03dD/FYLDs.
!
username admin privilege 15 password

```

```

Комутатор SW_3_13_5
hostname SW_3_13_5
!
boot-start-marker
boot-end-marker
!!
logging discriminator EXCESS severity
drops 6 msg-body drops
EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5
$1$hB2O$bS7RjZeY79X03dD/FYLDs.
!
username admin privilege 15 password

```

```

0 123123
aaa new-model
*Jan 25 16:56:04.123: %SYS-5-
CONFIG_I: Configured from console
by console
!!
aaa group server radius packetfence
server 203.3.13.2 auth-port 1812 acct
port 1813
!
aaa authentication login default local
aaa authentication dot1x default group
packetfence
aaa authorization network default group
packetfence
aaa session-id common
no ip icmp rate-limit unreachable
!!!
no ip domain-lookup
ip cef
no ipv6 cef
!!
dot1x system-auth-control
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy
ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
switchport trunk allowed vlan 1,10-40
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
!
interface Ethernet0/2
switchport mode access
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic
authentication timer reauthenticate

```

```

0 123123
aaa new-model

Jan 25 16:57:10.543: %SYS-5-
CONFIG_I: Configured from console
by console
!!
aaa group server radius packetfence
server 203.3.13.2 auth-port 1812 acct
port 1813
!
aaa authentication login default local
aaa authentication dot1x default group
packetfence
aaa authorization network default group
packetfence
aaa session-id common
no ip icmp rate-limit unreachable
!!!
no ip domain-lookup
ip cef
no ipv6 cef
!!
dot1x system-auth-control
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy
ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
switchport trunk allowed vlan 1,10-40
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface Ethernet0/1
!
interface Ethernet0/2
switchport mode access
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication periodic

```

```

10800
authentication timer restart 10800
mab
no snmp trap link-status
dot1x pae authenticator
dot1x timeout quiet-period 2
dot1x timeout tx-period 3
interface Vlan1
no ip address
shutdown
!
interface Vlan30
ip address 206.3.13.254 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
snmp-server community public RW
radius-server host 203.3.13.2 auth-port
1812 acct-port 1813 timeout 2 key
WirRadius
!
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

```

```

authentication timer reauthenticate
10800
authentication timer restart 10800
mab
no snmp trap link-status
dot1x pae authenticator
dot1x timeout quiet-period 2
dot1x timeout tx-period 3
interface Vlan1
no ip address
shutdown
!
interface Vlan40
ip address 207.3.13.254 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
snmp-server community public RW
radius-server host 203.3.13.2 auth-port
1812 acct-port 1813 timeout 2 key
WirRadius
!
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

```

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 123 «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Зав. кафедри комп'ютерної
інженерії та кібербезпеки

 Єфіменко А.А.

12 квітня 2021 р.

ЗАВДАННЯ

на випускн кваліфікаційну роботу

Студента Лісовського Миколи Сергійовича

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

Затверджена Наказом університету від «12» квітня 2021 р. № 133/С

Термін здачі студентом закінченої роботи 20 червня 2021 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження) процес проектування, розробки та налагодження підсистеми аутентифікації користувачів комп'ютерної мережі організації на базі технології 802.1x та протоколу RADIUS

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1			
2			
3			

Керівник  Єфіменко А.А.