

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 магістра
на тему:

«Проект підсистеми аутентифікації користувачів та
кінцевих пристроїв кампусної мережі організації»

Виконав студент II-го курсу, групи КБм-21-1
спеціальності 125 «Кібербезпека»

 Боговик Д.В.

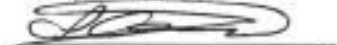
Керівник

Професор кафедри комп'ютерної інженерії та
кібербезпеки, доктор технічних наук, доцент

 Воротніков В. В.

Рецензент,

Завідувач кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук, доцент

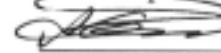
 Сфіменко А.А.

Житомир 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки

 Сфіменко А. А.

«01» 03 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента Боговика Дмитра Васильовича

Тема роботи: Проект підсистеми аутентифікації користувачів та кінцевих пристроїв кампусної мережі організації

затверджена Наказом по університету від «1» березня 2023 р. № 96/с

Термін здачі студентом закінченої роботи – «20» квітня 2023_р.

Вихідні дані для роботи:

- 1.Розроблені технічні вимоги до проекту
2. Розроблена модель проекту
3. Досліджено топологію проекту
4. Налаштовано систему аутентифікації

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

Керівник



Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання.	02.03.2023	Виконано
2	Пошук, огляд та аналіз літературних джерел.	05.03.2023	Виконано
3	Дослідження технологій аутентифікації.	15.03.2023	Виконано
4	Налаштування системи	20.03.2023	Виконано
5	Аналіз результатів	30.04.2023	Виконано
6	Перевірка працездатності	03.04.2023	Виконано
7	Написання пояснювальної записки	10.04.2023	Виконано
8	Підготовка презентації та виступу	15.04.2023	Виконано
9	Отримання відгуку керівника та рецензії на кваліфікаційну роботу	25.04.2023	Виконано
10	Захист		

Студент  Боговик Д.В.

Керівник  Воротніков В. В.

РЕФЕРАТ

Кваліфікаційна робота складається з проекту підсистеми аутентифікації користувачів та кінцевих пристроїв кампусної мережі організації та пояснювальної записки до нього. Пояснювальна записка до роботи містить 56 сторінок, 37 ілюстрацій та 2 таблиці.

Метою побудови такої підсистеми мережі є дослідження процесу налаштування ситеми аутентифікації, аналіз типів аутентифікації. Об'єктом дослідження є процес побудови підсистеми кампусної мережі з використанням моделі AAA. Предметом дослідження є використання протоколу аутентифікації RADIUS в великих кампусних мережах.

В роботі визначено основні завдання проекту, проаналізовано теоретичні аспекти аутентифікації в кампусних мережах. Наведено порівняльний аналіз протоколів аутентифікації які використовують в сучасних мережах організацій. Проаналізовано топологію та досліджено типові схеми аутентифікації пристроїв та ролей користувачів підсистеми. Повністю налаштовано мережу за допомогою додатку GNS3. Також наводяться результати тестування та налагодження системи.

КЛЮЧОВІ СЛОВА: AAA, RADIUS, АУТЕНТИФІКАЦІЯ, КАМПУСНА МЕРЕЖА, GNS3, 802.1X.

Зм.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми аутентифікації користувачів та кінцевих пристроїв кампусної мережі організації		
Розроб.		Боговик Д.В.					
Керівник		Воротніков В.В.					
Рецензент.		Єфіменко А. А.					
Зав. каф.		Єфіменко А. А.					
					Літ.	Арк.	Аркушів
						4	
					Житомирська політехніка, група КБм-21-1		

ABSTRACT

The qualification work consists of a project of the user authentication subsystem and end devices of the organization's campus network and an explanatory note to it. The explanatory note to the work contains 56 pages, 41 illustrations and 2 tables.

The purpose of building such a network subsystem is to study the process of setting up authentication systems, to analyze authentication types. The object of research is the process of building a campus network subsystem using the AAA model. The subject of the study is the use of the RADIUS authentication protocol in large campus networks.

The work defines the main tasks of the project, analyzes the theoretical aspects of authentication in campus networks. A comparative analysis of authentication protocols used in modern networks of organizations is presented. The topology was analyzed and typical authentication schemes of devices and user roles of the subsystem were investigated. Fully configured network using GNS3 application. The results of system testing and debugging are also given.

KEY WORDS: AAA, RADIUS, AUTHENTICATION, CAMPUS NETWORK, GNS3, 802.1X.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

РЕФЕРАТ.....	4
ABSTRACT.....	5
ВСТУП.....	7
РОЗДІЛ 1. АНАЛІЗ ТЕОРЕТИЧНИХ АСПЕКТІВ АУТЕНТИФІКАЦІЇ В КАМПУСНИХ МЕРЕЖАХ	9
1.1 Базові поняття та визначення аутентифікації.....	9
1.2 Порівняльний аналіз поширених протоколів аутентифікації. Аналіз функціональних можливостей протоколу RADIUS.....	21
1.3 Технологія 802.1X та її застосування в поєднанні з RADIUS.....	27
РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ	302
2.1 Аналіз топології мережі та розробка загальної структури системи.....	32
2.2 Розробка типових схем аутентифікації пристроїв та ролей користувачів....	33
2.3 Розробка схеми журналювання подій системи аутентифікації.....	37
РОЗДІЛ 3. ВИБІР ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ, ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ТЕСТУВАННЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ...	371
3.1 Вибір обладнання та програмного забезпечення.....	41
3.2 Налаштування підсистеми аутентифікації.....	43
3.3 Тестування роботи підсистеми аутентифікації.....	47
ВИСНОВКИ	51
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ.....	53
ДОДАТКИ.....	58

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Інформаційно-комунікаційні системи та мережі – невід’ємна частина сучасного світу, бізнесу, політики, державних і регіональних органів. Головним завданням є забезпечення безпеки інформації, розмежування доступу, авторизація користувача і даних. Збільшення кількості користувачів, розширення спектру послуг, збільшення потоку передачі даних вимагає складної і точно побудованої системи управління мережею. Кожний користувач сучасних інформаційно-комунікаційних систем декілька разів на день стикається з процедурами ідентифікації та аутентифікації. Ці процедури виконуються кожний раз, коли користувач вводить пароль для доступу до інформаційної системи, мережі, бази даних або при запуску прикладної програми. В результаті їх виконання оператор або отримує доступ до певних ресурсів інформаційної системи, або ні. Процедура аутентифікації користувача є обов’язковим етапом функціонування будь-якої сучасної інформаційнокомунікаційної системи та отримує особливу актуальність.

Актуальність даного проєкту полягає в тому, що без аутентифікації користувачів та пристроїв не може обійтись жодна велика організація, в особливості кампусна мережа організації.

Кампусна мережа – це велика багатосегментна локальна мережа на території до декількох кілометрів в діаметрі, яка об’єднує локальні мережі близько розташованих будівель. Кампусні види мереж набули широкого поширення в США. Вони переважно розвинені в коледжах і університетах. Найчастіше об’єднують різноманітні будівлі, в тому числі адміністративні будівлі, навчальні корпуси, бібліотеки, гуртожитки, гімназії та інші споруди.

Об’єктом дослідження є процес побудови підсистеми кампусної мережі з використанням моделі AAA.

Предметом дослідження є використання протоколу аутентифікації RADIUS в великих кампусних мережах.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

Метою кваліфікаційної роботи є побудова такої підсистеми мережі, яка б забезпечувала кампусну мережу системою аутентифікації пристроїв та користувачів в межах організації використовуючи протокол RADIUS.

Встановлена мета створює наступні завдання:

- Ознайомлення поняттям та визначенням аутентифікації;
- Огляд моделі AAA та її складових;
- Порівнянн протоколів аутентифікації;
- Аналіз протоколу аутентифікації пристроїв 802.1X;
- Налаштування пристроїв, створення користувачів,
- Перевірка працездатності мережі.

Наукова новизна дослідження полягає в використанні можливостей емулятору програмного забезпечення GNS3 для розробки підсистеми аутентифікації з використанням сучасних пристроїв.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. АНАЛІЗ ТЕОРЕТИЧНИХ АСПЕКТІВ АУТЕНТИФІКАЦІЇ В КАМПУСНИХ МЕРЕЖАХ

1.1 Базові поняття та визначення аутентифікації

Процес реєстрації користувача в будь-якій системі складається з трьох взаємопов'язаних процедур, що послідовно виконуються: ідентифікації, автентифікації та авторизації.

Ідентифікація - процедура розпізнавання суб'єкта за його ідентифікатором. У процесі реєстрації суб'єкт пред'являє свій ідентифікатор системі, яка перевіряє його у своїй базі даних. Суб'єкти з відомими системами ідентифікаторами вважаються легальними (законними), решта відносяться до нелегальних.

Аутентифікація — процедура перевірки справжності суб'єкта, яка дозволяє достовірно переконатися, що суб'єкт, який пред'явив свій ідентифікатор, насправді є саме тим суб'єктом, ідентифікатор якого він використовує. Для цього він повинен підтвердити факт володіння деякою інформацією, яка може бути доступна лише йому одному (пароль, ключ тощо).

Авторизація - процедура схвалення суб'єкту певних прав доступу до ресурсів системи після проходження ним проієлури аутентифікації. Для кожного суб'єкта у системі визначається набір прав, які може використовувати при зверненні до її ресурсам.

Для того щоб забезпечити управління та контроль над даними процедурами, додатково використовуються процеси адміністрування та аудиту. Адміністрування - процес управління доступом суб'єктів до ресурсів системи.

Цей процес включає:

- створення ідентифікатора суб'єкта (облікового запису користувача) у системі;
- керування даними суб'єкта, що використовуються для його аутентифікації (зміна пароля, видання сертифіката тощо);
- управління правами доступу суб'єкта ресурсів системи.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

Аудит - процес контролю (моніторингу) доступу суб'єктів до ресурсів системи, що включає протоколювання дій суб'єктів при їх доступі до ресурсів системи з метою виявлення несанкціонованих дій.

Таким чином, у загальному випадку йдеться про п'ять основних процедур надання доступу до інформації. При цьому можливий різний підхід до встановлення пріоритетів при виконанні цих процедур.

Незалежно від типу системи автентифікації в ній всі присутні п'ять елементів.

Перший елемент — конкретна людина або процес, який має проходити автентифікацію, — суб'єкт доступу.

Другий елемент — розпізнавальний знак, ідентифікатор, який виділяє цю людину або цей процес серед інших.

Третій елемент — відмінна характеристика (автентифікатор), що підтверджує приналежність ідентифікатора суб'єкту доступу.

Четвертий елемент — власник системи (адміністратор), який несе відповідальність за використання системи, і в розмежуванні авторизованих і не авторизованих користувачів полягається на механізм аутентифікації.

П'ятий елемент — механізм аутентифікації, який дозволяє перевірити присутність відмітної характеристики.

При успішному проходженні аутентифікації суб'єкту доступу повинні бути видані деякі права (привілеї).

Для цього служить механізм керування доступом. За допомогою цього ж механізму суб'єкт доступу втрачає права (привілеї), коли автентифікація була невдалою.

Прикладом аутентифікації є вхід фізичної особи до системи за паролем. Фізична особа — це людина, якій можна користуватися комп'ютером. Зазвичай у системі фізичній особі призначається символічне ім'я або ідентифікаційний код користувача, який ми називатимемо ім'ям користувача. Наприклад, якщо користувач є авторизованим користувачем системи, адміністратор присвоює йому ім'я користувача «Користувач». Відмінною характеристикою користувача

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

буде його секретний пароль, наприклад, «qwerty». Ця процедура знайома, оскільки у процесі реєстрації комп'ютер видає запит на введення імені користувача та пароля.

Процес включає процедуру аутентифікації, тобто порівняння пароля, введеного, з клавіатури, з паролем, встановленим або самим користувачем, або адміністратором системи. Процедура завершується успішно, якщо обидва паролі збігаються. У цьому випадку механізм управління доступом дозволяє користувачеві продовжувати роботу на комп'ютері, і система використовує ім'я користувача щоразу, коли їй потрібне рішення служби управління доступом до захищеного ресурсу.

Розглядаючи проблеми захисту комп'ютерів, слід завжди проводити різницю між тим, що ми хочемо зробити, і тим, що ми насправді робимо.

Перше питання «чого ми хочемо» зазвичай озвучують у вигляді цілей захисту. Наприклад, метою зграї сорока розбійників був захист видобутку від злодійства. У цьому вони покладалися на механізм захисту – двері печери. У обчислювальній системі метою власника системи є надання доступу лише авторизованим (законним) користувачам.

На практиці ж завжди існує щілина між тим, що ми хочемо, і що відбувається насправді. Так, замок дозволяє увійти кожному, у кого є екземпляр потрібного ключа, проте сторонні зможуть увійти також, якщо ми не запобігаємо отриманню ними ключа.

Це може виявитися складною справою, особливо якщо ті, кого ми прагнемо не впустити за допомогою замку, справді хочуть потрапити всередину. Більше того, ми не завжди можемо дозволити собі поставити замки на все у світі. Часто є один великий замок на входних дверях, і нам доводиться довіряти тим, кого ми впустили всередину.

У комп'ютерних системах автентифікація та управління доступом зазвичай реалізуються як дві різні функції. Хоча іноді має сенс проводити різницю між засувкою, що утримує двері зачиненими, і замком, який керує засувкою, засувка і замок часто вбудовані в один механізм. У комп'ютерних системах

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

процес аутентифікації підтверджує справжність імені користувача, а керування доступом здійснюється шляхом порівняння імені користувача з правилами доступу, пов'язаними з конкретним файлом або іншим ресурсом. Якщо правила дозволяють доступ користувачеві з цим ім'ям, він отримує можливість використовувати ресурс.

Сорок розбійників прагнули до того, щоб у печеру мали доступ тільки члени зграї, але їх механізм не міг запобігти використанню пароля іншими людьми.

Ця проблема властива як процесу автентифікації, і механізму управління доступом.

Механізми автентифікації недосконалі. Неавторизовані люди можуть замаскуватись під легального користувача.

Така сама проблема виникає і при управлінні доступом: необхідно авторизувати на користування системою лише певних людей і для цього встановлюється система управління доступом. В ідеальному світі техніки із засобами захисту доступ видається за принципом «найменшого привілею», відповідно до якого люди мають рівно стільки дозволів та привілеїв, скільки їм потрібно: не більше і не менше. Але в реальному світі система управління доступом не може дати людям рівно стільки привілеїв, скільки їм потрібно: ми змушені або надавати їм надто багато привілеїв, або забирати деякі з тих, які дійсно потрібні. На практиці міра довіри авторизованим користувачам зазвичай розширюється, так що у них є інструментарій для виконання своєї роботи, навіть якщо технічно це дозволяє їм робити такі речі, які вони не повинні робити.

Управління доступом може бути дуже складним навіть без спроби домогтися виконання принципу найменших привілеїв. Сучасні обчислювальні системи забезпечують широкий діапазон підходів та механізмів керування доступом. Механізми керування доступом навіть у таких відносно простих системах, як Unix або Windows, дозволяють користувачам та адміністраторам встановлювати дуже складні набори правил отримання та позбавлення прав на

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

використання різних ресурсів комп'ютера. Однак багато організацій дотримуються щодо простого підходу, пов'язуючи управління доступом і аутентифікацію, так що користувачі, що пройшли аутентифікацію, мають лише невелику кількість обмежень доступу.

Хоча проблема аутентифікації користувачів є серйозною проблемою для комп'ютерних систем, користувачі не є єдиними суб'єктами, які підлягають аутентифікації.

На відміну від процесу аутентифікації користувача, тут немає реальної людини, яка стоїть поруч із сервером, щоб виконати аутентифікацію. Ми ж хочемо мати гарантію, що взаємодіємо з потрібним обладнанням, яке перебуває під керуванням потрібних людей чи підприємства. Ніхто не захоче замовляти туфлі через комп'ютер, що оголошує себе «Shoes», якщо зрештою він ці туфлі не отримає. Коли ми виконуємо аутентифікацію суб'єкта, що представляється сервером компанії Shoes, ми повинні бути впевнені, що саме він управляється і контролюється підприємством, що належить компанії Shoes. Зазвичай браузер попереджує користувача, якщо він не може аутентифікувати сервер і залишає рішення щодо керування доступом за користувачем (Чи повинен я оформляти замовлення на туфлі, з урахуванням того, що цей сервер, схоже, не є сервером компанії Shoes? Вважаю, ні). У певному сенсі такий процес перевертає функцію автоматичної аутентифікації з ніг на голову.

Чинники аутентифікації

Для підтвердження своєї справжності суб'єкт повинен надати деяку секретну інформацію, яка має бути доступна лише йому одному. Він може пред'являти системі різні види інформації.

Фактор автентифікації - певний вид інформації, що надається суб'єктом системі за його автентифікації.

Опис факторів автентифікації

Виділяють три фактори аутентифікації, що використовуються в різних комбінаціях: на основі знання чогось, володіння чимось, на основі біометричних характеристик (Таблиця 1.1).

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 1.1

Чинник автентифікації	Класифікація типів факторів автентифікації NCSC-TG- 017 ¹	Приклади факторів автентифікації
На основі знання чого-небудь	Type 1: Authentication by Knowledge	• Пароль або парольна фраза • PIN-код
На основі здобуття чого-небудь	Type 2: Authentication by Ownership	• Фізичний ключ • Карта з магнітною полосою • OTP-токен, що генерує одноразовий пароль
На основі біометричних характеристик	Type 3: Authentication by Characteristic	• Відбиток пальця • Малюнок сітки ока • Голос

NCSC-TG-017¹ — документ «A Guide to Understanding Identification and Authentication in Trusted Systems», опублікований U.S. National Computer Security Center. Керівництво містить комплект рекомендованих інструкцій з процедурами автентифікації та аутентифікації.

У деяких компаніях організується «суворий контроль» доступу до приміщення, тобто у певні приміщення доступ надається лише обмеженій кількості осіб. Наприклад, у серверну кімнату може увійти тільки адміністратор або до кімнати фінансового відділу компанії можуть мати доступ лише його співробітники. Якщо при цьому встановити для комп'ютерів, що знаходяться в цих приміщеннях, суворо визначені IP-адреси, то з'являється можливість якісніше виконувати аутентифікацію при доступі співробітників до ресурсів комп'ютерної мережі. Їм надається доступ до певних дій або даних лише в тому випадку, якщо вони це роблять у суворо певному приміщенні та відповідно з

					Арк.
Змн.	Арк.	№ докум.	Підпис	Дата	

певних комп'ютерів, що мають певні IP-адреси. У цьому випадку іноді говорять про використання «четвертого» типу аутентифікаційного фактора — на основі місця проведення процедури. Цей фактор не вважається додатковим, оскільки його не можна використовувати окремо від інших факторів для автентифікації суб'єкта. Наприклад, не можна забезпечити, щоб тільки певний співробітник працював на певному робочому місці (комп'ютері).

Останнім часом намітилися тенденції інтеграції логічних засобів аутентифікації та засобів контролю та управління доступом (ЗКУД). Смарт-картки, які використовуються для аутентифікації користувача при доступі до ресурсів комп'ютерної системи, інтегруються з RFID (радіочастотною ідентифікацією). У цьому випадку з'являється можливість додатково використовувати їх для автентифікації людини при її доступі до різних приміщень. Як і раніше, у цьому випадку йтиметься про використання аутентифікації «на основі володіння чимось». Це розширює можливості використання смарт-карти, дає додаткові зручності для користувача, але не підвищує якість автентифікації.

Багатофакторна автентифікація

Аутентифікація може бути реалізована за допомогою одного з трьох факторів аутентифікації. Наприклад, у процесі аутентифікації користувача може бути запрошений пароль, або потрібно представити відбиток пальця.

Аутентифікація, у процесі якої використовується лише один фактор аутентифікації, називається однофакторною.

Аутентифікація, у пронесенні якої використовується кілька факторів аутентифікації, називається багатофакторною.

Наприклад, у процесі автентифікації користувач повинен використовувати смарт-картку та додатково пароль (або PIN-код). Також використовуються поняття двофакторної та трифакторної аутентифікації при використанні комбінації двох та трьох факторів аутентифікації відповідно.

В документі MCSC-TG-017 вводяться терміни для різних видів багатофакторної аутентифікації: типу 12, типу 23 і типу 123. Аутентифікація

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

типу 12 (вимовляється як «аутентифікація типу один два»), наприклад використовує два фактори аутентифікації: перший (на основі чогось) і другий (на основі володіння чимось).

Трьохфакторна аутентифікація використовує комбінацію трьох факторів аутентифікації («на основі знання чого-небудь», «на основі володіння чим-небудь» і «на основі біометрії»). Цю аутентифікацію називають аутентифікація типу 123.

Якщо для аутентифікації використовується лише один фактор аутентифікації, вона виявляється уразливою. При багатофакторній аутентифікації використовується декілька (два і більше) факторів аутентифікації, що забезпечує надійність безпеки.

Найбільш поширене використання комбінації двох факторів при аутентифікації користувача в банкоматі. Потрібно одночасно використати карту з манітною полозою та PIN-код.

Модель AAA

AAA (Authentication, Authorization and Accounting) або автентифікація, авторизація та обліковий запис – це термін, який використовується для опису трьох функцій в ІТ.

В основному AAA використовується для керування доступом до різних ІТ-ресурсів, таких як мережа, служби, сервери і т.д.

AAA складається з трьох протоколів, кожен з яких виконує свою функцію для забезпечення ідеальної безпеки.

Tacacs або Tacacs+ – це протокол AAA, створений Cisco для використання мережних продуктів.

Tacacs – це перше покоління протоколу, а Tacacs+ – це протокол AAA наступного покоління із розширеними функціями.

Radius – це один протокол AAA, який надає функції та служби, дуже схожі на Tacacs.

Radius – це відкритий стандарт і широко використовується протокол, який визначається RFC.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

LDAP – ще один популярний протокол, що забезпечує аутентифікацію та авторизацію, пов'язану з AAA.

Популярний протокол LDAP забезпечує автентифікацію та авторизацію відкритим способом, який підтримується безліччю різних пристроїв, систем та програмного забезпечення.

LDAP зберігає інформацію про користувача, таку як ім'я користувача, ідентифікатор, пароль, домашній каталог, сертифікат тощо, та перевіряє автентифікацію з наданими обліковими даними та повертає результат. А також він надає користувачам інформацію про авторизацію.

AAA визначає архітектуру, яка автентифікує та надає авторизацію користувачам і обліковим записам для їхньої діяльності. Коли AAA не використовується, архітектура мережі є «відкритою», де будь-хто може отримати доступ і робити що завгодно без відстеження. Відкрита мережева архітектура зазвичай використовується на малих підприємствах, де доступ до офісу можна фізично контролювати.

Без AAA мережевий адміністратор мав би статично налаштовувати мережу. Навіть у перші дні комутованого доступу мережеві адміністратори вважали статичну модель невідповідною. AAA забезпечує гнучкість мережевих політик. AAA також дає мережевим адміністраторам можливість переміщувати системи; без AAA їм довелося б чітко визначати варіанти підключення.

Сьогодні широке поширення мобільних пристроїв, різноманітні споживачі мережі та різноманітні методи доступу до мережі разом створюють середовище, яке висуває більші вимоги до AAA. AAA відіграє роль майже в усіх способах доступу до мережі: бездротові точки доступу використовують AAA для безпеки; розділені мережі потребують AAA для забезпечення доступу; усі форми віддаленого доступу використовують AAA для авторизації віддалених користувачів.

Протокол взаємної аутентифікації Kerberos

Головною особливістю Kerberos є те, що первинні ключі за системою не передаються взагалі. Ця система була розроблена в Массачусетському

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

технологічному інституті в рамках проекту Афіна. Головним призначенням системи є забезпечення захищеного обміну даними у мережі загального користування. Обмін даними побудовано за принципом клієнт/сервер. Усі ПК користувачів оснащуються клієнтською частиною Kerberos. Сервер може бути встановлений на окремому комп'ютері або навіть рознесений багатьом. При чому в протоколі враховано той факт, що початковий обмін інформацією між клієнтом і сервером відбувається в незахищеному середовищі, а пакети, що передаються, можуть бути перехоплені і модифіковані.

Протокол Kerberos використовує технології аутентифікації, що спираються на загальний секрет. Основна концепція досить проста: якщо є секрет, відомий лише двом, будь-який з його зберігачів може легко переконатися, що має справу саме зі своїм партнером. Для цього достатньо якимось способом перевірити, чи знає співрозмовник їхній спільний секрет. Замість того, щоб повідомляти один одному пароль, учасники сеансу обмінюються криптографічним ключем, знання якого підтверджує особу співрозмовника. Один із учасників використовує такий ключ для шифрування блоку інформації, а інший за його допомогою витягує цю інформацію.

Після підтвердження Kerberos забезпечує обидва комп'ютери ключами шифрування щодо захищеного сеансу зв'язку. Аутентифікація за допомогою Kerberos є тристороннім процесом, у якому роль посередника виконує окремий сервіс (KDC), що підтверджує особистість комп'ютера за запитом іншого комп'ютера і ключі, що поставляє для встановлення між ними захищеного з'єднання. Кожен з комп'ютерів, що беруть участь у сеансі зв'язку, «ділить секрет» з ІХС, який складається з двох компонентів: сервера автентифікації та сервера видачі квитків (шифрованих повідомлень).

Якщо KDC отримує запит про невідомий йому сервер призначення, він перенаправляє аутентифікаційну транзакцію на інший KDC, що має потрібні відомості. Обмінюючись із клієнтом серією шифрованих повідомлень - квитків, KDC генерує нові ключі шифрування кожного етапу процесу аутентифікації. Він може успішно підтвердити особистість одного комп'ютера на запит іншого,

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

не видаючи секретних ключів жодної зі сторін і не вимагаючи від жодного з них постійного зберігання ключів доступу до всіх комп'ютерів, з якими вони коли-небудь встановлять з'єднання. Квиток дійсний протягом заданого періоду часу і може використовуватися лише одним певним комп'ютером для підключення до іншого комп'ютера. Після видачі квитка клієнт може використовувати його для отримання доступу до цільового сервера необмежену кількість разів, але тільки в період дії квитка.

Ні клієнт, ні хтось інший не можуть рахувати або модифікувати квиток, не зробивши його недійсним. KDC є службою, що працює на фізично захищеному сервері. Вона веде БД з інформацією про облікові записи всіх головних абонентів безпеки (security principal) своєї області. Разом з інформацією про кожного абонента безпеки в базі даних KDC зберігається криптографічний ключ, відомий лише цьому абоненту та службі KDC.

1.2 Порівняльний аналіз поширених протоколів аутентифікації. Аналіз функціональних можливостей протоколу RADIUS

Порівняння протоколів TACACS+ та RADIUS

Протокол RADIUS є стандартом IETF для AAA. Використовується з початку 1990-х років і спочатку застосовувався для модемних комутованих з'єднань. Спочатку використовувався для розширення Layer 2 протоколу точка-точка (PPP) між кінцевим користувачем та сервером доступу до мережі (NAS), передаючи трафік автентифікації з NAS на сервер AAA. Відомості від автентифікації та авторизації доставляють одним типом пакетів, а облік обробляється окремим процесом. RADIUS має широке поширення та підтримується більшістю виробників пристроїв та розробників програмних продуктів.

Сучасна реалізація RADIUS використовує порти 1812 (аутентифікація) та 1813 (облік) протоколу UDP (також можливе використання портів 1645 та 1646). UDP має високу швидкість, але має ряд недоліків, які необхідно враховувати при його застосуванні. Коли розробляли RADIUS, питання безпеки не були настільки актуальними, як зараз, тому він підтримує досить малу

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

кількість типів аутентифікації (Clear text і CHAP), шифрує лише поле з паролем і загалом має середній рівень безпеки.

TACACS+, цей протокол розроблений компанією Cisco та є розвитком минулих версій TACACS та XTACACS. Незважаючи на схожість назв, TACACS+ був сильно видозмінений і не має зворотної сумісності з TACACS, який зараз практично ніде не застосовується. Основна сфера використання TACACS+ – це адміністрування мережних пристроїв, проте він може застосовуватися для деяких типів AAA при доступі до мережі. TACACS+ використовує Transmission Control Protocol (TCP) порт 49, а не UDP, оскільки він має більшу надійність і дозволяє заздалегідь отримувати інформацію про потенційні помилки завдяки пакету TCP-RST. TCP більш повільний протокол, але має додаткові переваги: можливість поділу аутентифікації, авторизації та обліку в якості окремих і незалежних функцій, множинна авторизація після однієї аутентифікації, шифрування всього вмісту пакета.

Протокол RADIUS (Remote Authentication Dial In User Service), на відміну від TACACS+, був розроблений незалежною групою розробників (на даний момент протокол не модифікується) і тому набув широкого поширення у сторонніх розробників.

Як правило, всі виробники програмних та апаратних клієнтів підтримують цей протокол. RADIUS (Remote Authentication in Dial-In User Service) - відкритий протокол AAA.

Розглянемо ключові характеристики даного протоколу:

1) Як транспортний протокол використовується UDP. Для аутентифікації порт 1812 (раніше 1645), а обліку - 1813 (раніше 1646).

2) При взаємодії між AAA-сервером та AAA-клієнтом протокол шифрує тільки пароль. Решта даних передається у відкритому вигляді.

3) Аутентифікація та авторизація є єдиним процесом. Як тільки користувач проходить автентифікацію, він відразу автоматично проходить авторизацію і отримує відповідний йому рівень привілеїв (можливість виконувати ту чи іншу

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

команду). Після цього користувач може робити все, що йому дозволено в рамках своїх привілеїв.

4) Має дуже докладний процес обліку (accounting).

5) Відкритий протокол (open source).

Яскравим представником цього протоколу є FreeRADIUS – AAA-сервер з відкритим вихідним кодом.

TACACS+ (Terminal Access Controller Access Control System). Вимовляється як ТА-КАКС плюс.

Основні відмінності:

1) Як транспортний протокол використовується TCP (порт 49)

2) Протокол шифрує всі дані між AAA-сервером та AAA-клієнтом.

3) Процеси автентифікації та авторизації абсолютно незалежні. Це дозволяє авторизувати кожну команду, яку вводить користувач. Таким чином, ми отримуємо більш гнучкий контроль усіх дій.

4) Пропрієтарний протокол (тобто закритий).

Таблиця 1.2

	RADIUS	TACACS+
Використовувані протоколи та порти	UDP: 1812 & 1813 або UDP: 1645 & 1646	TCP:49
Сервіси	Об'єднує аутентифікацію та авторизацію	Різні процеси для аутентифікації, авторизації та обліку
Типи автентифікації, що підтримуються	Clear text (ASCII, PAP), CHAP	Clear text (ASCII, PAP), CHAP, ARAP
Можливість перенаправлення запиту	Є (до іншого AAA-сервера)	Ні
Основне призначення	Доступ до мережі	Адміністрування пристроїв

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

Безпека	Шифрується пароль	Шифрується все тіло пакету
---------	-------------------	----------------------------

Найвідоміший TACACS+ сервер – Cisco Secure Access Control Server (ACS). Це також пропрієтарна розробка компанії Cisco. Продукт є платним, але є demo період (можливість безкоштовного тестування).

Протокол TACACS+ використовує протокол TCP, тобто. він потенційно повільніший за протокол RADIUS, але TACACS+ здатний в кожний момент часу обслуговувати кілька користувачів.

RADIUS сервер зустрічається в мережі будь-якого Інтернет-провайдера, де потрібно аутентифікувати сотні та тисячі користувачів. TACACS+ найчастіше застосовується для аутентифікації та авторизації адміністраторів на мережевих пристроях. Знову ж таки, вибір для кожного обумовлений більш гнучкою авторизацією, коли можна перевіряти буквально кожну команду.

RADIUS підтримується практично будь-яким мережевим обладнанням, чого не скажеш про TACACS.

Отже, основні відмінності зводяться до того, що TACACS+ шифрує весь вміст пакета, залишаючи лише простий заголовок. Такий спосіб захищає від зломисників, які прослуховують повідомлення, що надсилаються між пристроями. Також TACACS+ реалізує функції AAA окремо, що дозволяє винести кожну їх на окремий сервер і навіть використовувати інший протокол (не TACACS+).

TACACS+ також пропонує тіснішу інтеграцію з пристроями Cisco і дозволяє здійснювати детальне управління маршрутизаторами (процес авторизації). З сервером TACACS + можна передати управління командами із застосуванням рівнів доступу (які далі налаштовуються на самих пристроях). RADIUS також дозволяє частково реалізувати цю можливість, але не так добре та гнучко, як TACACS+.

При використанні протоколу TACACS+ між клієнтом та сервером не може бути брандмауера, оскільки сервер повинен отримати запит від клієнта з його

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

IP-адресою, а не з адресою брендмауера. RADIUS IP-адреса клієнта міститься ще й у самому пакеті, що дозволяє AAA-серверу отримати його звідти.

А ось найбільший недолік TACACS+ полягає в тому, що Cisco розробила цей протокол для власних потреб і тому найширшу підтримку отримали саме мережеві пристрої цієї компанії. Однак поступово ситуація змінюється, і решта виробників стали також підтримувати TACACS+.

У версії 6.0 СКАТ DPI стала доступна авторизація IPoE-сесій на RADIUS, що розширило можливості оператора зв'язку щодо здійснення контролю доступу абонентів до мережі Інтернет та застосування політик тарифних планів та додаткових тарифних опцій:

- призначення та зміна політик (тарифних планів та опцій);
- перенаправлення користувачів у Captive Portal (блокування);
- робота на рівні L3;
- ідентифікація користувачів за IP або за міткою Q-in-Q.

Який протокол використовувати для AAA-сервера, необхідно вибирати в залежності від завдання. Якщо це адміністрування пристроїв, то TACACS+ стане найкращим варіантом, а якщо доступ до мережі, то універсальніший і швидший – RADIUS.

Структура RADIUS складається з трьох основних компонентів:

- Клієнт: Це той же NAS. Мережевий пристрій, який використовується для автентифікації користувачів.

- Сервер: це фоновий процес, який виконується на сервері UNIX або Windows.

- База даних

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

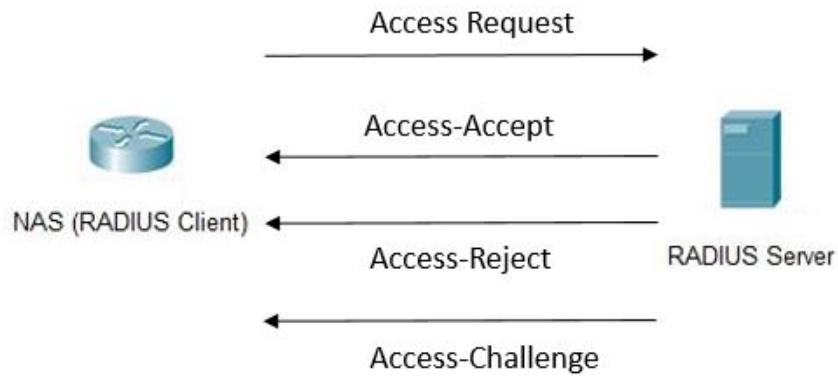


Рисунок 1.1 Механізм роботи серверу RADIUS

Цей механізм від початку до кінця включає наступні етапи:

1. Користувач або машина надсилає запит до NAS для отримання доступу до певного мережевого ресурсу за допомогою облікових даних (зазвичай це ім'я користувача та пароль або сертифікат безпеки, наданий користувачем). Як облікові дані передаються до NAS? Ця інформація передається на пристрій NAS через протокол канального рівня (наприклад, безпечна веб-форма PPP або HTTPS).
2. Коли NAS отримує облікові дані, надсилає повідомлення запиту доступу RADIUS на сервер RADIUS. Цей запит містить облікові дані доступу.
3. На цьому кроці сервер RADIUS перевіряє правильність інформації. Для цього він використовує схеми автентифікації (наприклад, PAP, CHAP або EAP). Якщо запит на доступ не від авторизованого клієнта, повідомлення відхиляється. Крім того, RADIUS-сервер перевіряє, чи існує політика доступу або профіль, який відповідає обліковим даним користувача.
4. Однак на цьому кроці стає зрозуміло, чи дозволено зазначеному вище користувачеві доступ до запитаних ресурсів чи ні. (Проведено автентифікацію та авторизацію).
5. Тепер сервер RADIUS повертає NAS одну з трьох відповідей:
 - Відмова в доступі: користувачеві відмовлено в доступі до всіх запитуваних ресурсів мережі.
 - Проблема доступу: запитує додаткову інформацію від користувача, наприклад додатковий пароль, PIN-код, маркер або картку.

Змн.	Арк.	№ докум.	Підпис	Дата		Арк.

- Прийняти доступ: користувачеві надано доступ. Звичайно, Radius Server оголошує атрибути авторизації для NAS, обумовлюючи умови надання доступу. Наприклад: конкретна IP-адреса, яку буде призначено користувачеві, пул адрес, з якого слід вибрати IP-адресу користувача, максимальний час, протягом якого користувач може залишатися на зв'язку, список доступу або параметри L2TP.

6. Тепер доступ до мережі надається користувачеві NAS, NAS надсилає серверу обліковий запис (пакет RADIUS Accounting Request, що містить атрибут Acct-Status-Type зі значенням «start»), щоб повідомити про початок доступ користувача до мережі.

7. Нарешті, коли доступ користувача до мережі (сеанс користувача) закрито, NAS видає остаточний обліковий запис на сервер, надаючи інформацію про використання в термінах часу, переданих пакетів, переданих даних, причину відключення та іншу пов'язану інформацію. на доступ користувача до мережі.

1. 3 Технологія 802.1X та її застосування в поєднанні з RADIUS

Протокол IEEE 802.1X визначає основні компоненти та алгоритми, що використовуються в мережах Ethernet/IEEE 802.3 для обмеження несанкціонованого підключення абонента до мережних пристроїв із застосуванням процедури аутентифікації.

Протокол IEEE 802.1X був спочатку розроблений для використання у звичайних і бездротових мережах з множинним доступом до середовища передачі даних. Далі перераховані основні переваги використання протоколу IEEE 802.1X для обмеження несанкціонованого доступу в мережах Ethernet/IEEE 802.3:

- Протокол IEEE 802.1X є стандартним рішенням, яке підтримується всіма виробниками комунікаційного обладнання;

- В якості вузла обмеження доступу IEEE 802.1X використовується комутатор Ethernet;

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

- При негативному результаті аутентифікації або відмові від неї абонента автоматично відбувається його відключення від мережевого пристрою IEEE 802.1X.

Основні компоненти IEEE 802.1X

У протоколі IEEE 802.1X для організації встановлення справжності абонента використовується модель клієнт-сервер. Основними компонентами IEEE 802.1X є:

- Сервер аутентифікації (Authentication Server);
- Клієнт-здобувач, що проходить процедуру аутентифікації (Supplicant);
- Вузол обмежування доступу (Access Point).

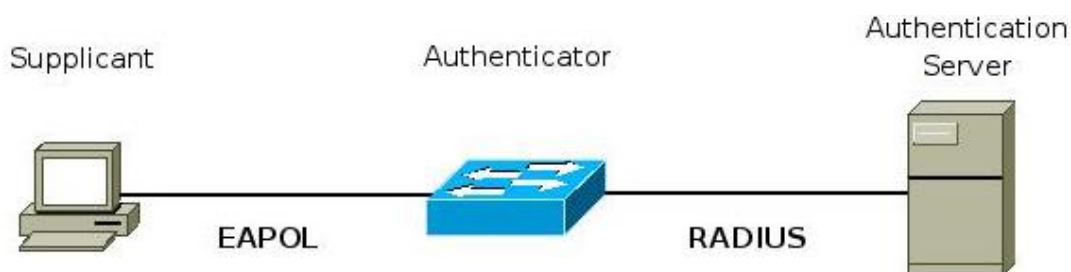


Рисунок 1.2 Основні компоненти IEEE 802.1X

Як сервер аутентифікації може бути використана одна або кілька робочих станцій, що знаходяться в захищеній зоні, на яких виконується додаток RADIUS-server. Функції, які виконує сервер аутентифікації IEEE 802.1X, нічим не відрізняються від функцій, що виконуються аналогічними серверами під час використання протоколів PPPoE, PPTP і L2TP. Абонентом IEEE 802.1X є клієнтська робоча станція, де встановлено програмне забезпечення для аутентифікації за цим протоколом.

Вузол обмеження доступу призначений для підключення або відключення абонента від мережі залежно від результатів його аутентифікації на сервері. Порти вузла доступу IEEE 802.1X можуть бути в одному з двох можливих станів, що відповідають статусу авторизації підключених до них абонентів:

- Абонента авторизовано (Authorized) — нормальний стан після успішної аутентифікації абонента. Порт приймає від абонента всі кадри;

					Арк.
Змн.	Арк.	№ докум.	Підпис	Дата	

- Абонента не авторизовано (Unauthorized) — нормальний стан перед початком автентифікації абонента. Порт приймає від абонента тільки кадри з повідомленнями розширюваного протоколу аутентифікації EAPOL (Extensible Authentication Protocol Over LAN).

Власне, вузол доступу IEEE 802.1X грає роль ключа, керованого сервером аутентифікації.

Особливості застосування протоколу IEEE 802.1X

Той факт, що протокол IEEE 802.1X є стандартним рішенням, істотно полегшує його впровадження в мультисервісних мережах. Але, слід враховувати, що реалізації цього протоколу можуть виявитися несумісними з фірмовими рішеннями різних виробників комунікаційного устаткування. Наприклад, на комутаторах Cisco Systems протокол IEEE 802.1X не може бути застосований на тих портах, де використовується Port Security і навпаки. Не допускається на комутаторах Cisco Systems також використання протоколу IEEE 802.1X на портах магістрального, агрегованого та деяких інших типів. Тому перед впровадженням протоколу IEEE 802.1X в мультисервісну ЛОМ адміністратор повинен уважно ознайомитися з документацією виробника про особливості застосування цього протоколу на даному устаткуванні.

Налаштування протоколу IEEE 802.1X на комутаторі зазвичай виконується за стандартною схемою і включає налаштування портів для управління підключенням абонентів і визначення параметрів взаємодії вузла доступу з сервером аутентифікації. Деякі виробники комунікаційного обладнання дозволяють використовувати додаткові функції, що полегшують адміністрування мережі та керування абонентами IEEE 802.1X. До таких функцій можна віднести, наприклад, аутентифікацію абонента з ініціативи адміністратора (команда *dot1x re-authenticate* Cisco Systems) або додатковий контроль параметрів абонента, що підключається (команда *dot1x port method* ZCOM).

У останній час для протоколу були розроблені нові механізми автентифікації з загальною назвою EAP (Extensible Authentication Protocol).

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

Протокол EAP був створений з метою упередження приватних механізмів аутентифікації та розповсюдження стандартизованих підходів — схеми типу «запит—відповідь» (challenge-response) та інфраструктури, заснованої на публічних сертифікаціях. Стандартизація механізмів EAP дозволила зробити аутентифікацію прозорою для серверів доступу різних виробників. Наприклад, при підключенні користувачів до сервера віддаленого доступу й використанню механізму EAP протокола PPP для аутентифікації сам сервер доступу не повинен знати або підтримувати конкретні механізми аутентифікації, його призначення в цьому випадку — передати пакети EAP-повідомлень RADIUS-серверу, на якому фактично проводиться аутентифікація. У цьому випадку сервер доступу виконує роль посередника між клієнтом і RADIUS-сервером, в задачі якого входить передача EAP-повідомлень між ними.

Стандарт 802.1x описує процедуру передачі EAP-повідомлень сервером доступу (наприклад, комутатором або бездротовою точкою доступу) у дротових або бездротових Ethernet-мережах. При цьому стандарт 802.1x напряду упаковує EAP-повідомлення в Ethernet-кадри, не використовуючи для їх передачі протокол PPP. Це викликано тим, що використовувати протокол PPP у багатьох випадках не обов'язково, наприклад, при підключенні Ethernet-робочої станції, що не підтримує протоку TCP/IP, або в тому випадку, коли використання протоколу PPP є надлишковим.

Ключовим показником є те, що мережеві пристрої — аутентифікатори — можуть бути досить прості, оскільки для реалізації функцій 802.1x в них потрібні мінімальні апаратні затрати, в той час як весь інтелект концентрується на RADIUS-сервері. Така схема має додаткові переваги і дозволяє організувати тісну інтеграцію керування мережевим обладнанням та мережевим ПЗ, що значно полегшує управління інформаційною системою великого підприємства.

Висновки до першого розділу

В даному розділі було розглянуто поняття автентифікації, та які елементи вона включає до себе. Ми з'ясували, що аутентифікація — це підтвердження

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

того, ким є користувач на вході. Далі ми розглянули модель AAA (Authentication, Authorization and Accounting) та три протоколи, з яких вона складається, таких як RADIUS, TACACS+ та LDAP. В основному AAA використовується для керування доступом до різних ІТ-ресурсів, таких як мережа, служби, сервери і т.д. В кінці першого пункту ми дізнались про особливості і принцип роботи протоколу взаємної аутентифікації Kerberos.

В другому пункті ми розглянули протоколи RADIUS та TACACS+. А саме, їх порівняння і з'ясували, що RADIUS підтримується практично будь-яким мережевим обладнанням, чого не скажеш про TACACS, а який протокол використовувати для AAA-сервера, необхідно вибирати в залежності від завдання. Якщо це адміністрування пристроїв, то TACACS+ стане найкращим варіантом, а якщо доступ до мережі, то універсальніший і швидший – RADIUS.

В останньому пункті було розглянено технологію 802.1X, основні її компоненти та особливості застосування. А також механізм автентифікації з загальною назвою EAP (Extensible Authentication Protocol), який дозволив зробити аутентифікацію прозорою для серверів доступу різних виробників.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ

2.1. Аналіз топології мережі та розробка загальної структури системи

Для проектування мережі було використано данну модель мережі, та додано сервер AAA, для реалізації підсистеми аутентифікації.

Проект даної мережі представлено на рисунку 2.1.

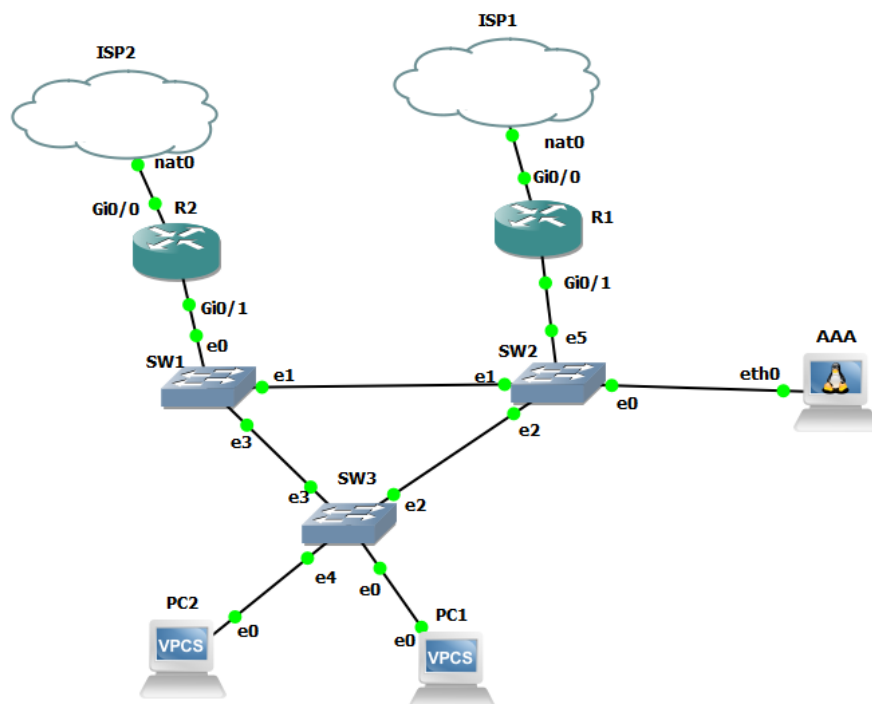


Рисунок 2.1 Загальна топологія мережі

В топології використано дві кінцеві точки доступу, два маршрутизатори, три комутатори, сервер та дві мережі ISP. З'єднання між комутаторами, сервером та кінцевими пристроями виконано за допомогою технології витой пари Ethernet, а від маршрутизаторів йдуть потужні GigabitEthernet з'єднання.

2.2. Розробка типових схем аутентифікації пристроїв та ролей користувачів

Типові моделі аутентифікації

Відомо 4 типові моделі аутентифікації: локальна, пряма, непряма та автономна. При цьому по-різному організовано адміністрування автентифікації, зосереджене на вирішенні двох завдань: додавання записів для нових користувачів та видалення застарілих записів:

					Арк.
Змн.	Арк.	№ докум.	Підпис	Дата	

- з однією точкою обслуговування - всі служби, необхідні для адміністрування, знаходяться на одному хості;

- з кількома точками обслуговування – є служби, що виконуються на різних комп'ютерах; автентифікація має працювати надійно та прозоро;

- екстранет-варіант - схоже на попередній випадок, але є лише кілька власників ресурсів.

Розглянемо докладніше названі типові моделі автентифікації. Відразу зазначимо, що ідеальної для всіх випадків моделі не існує. На її свідомий вибір впливає опірність атак, легкість адміністрування та потенційні втрати у разі збоїв автентифікації.

Локальна автентифікація

Ця типова модель відноситься до ситуацій, коли користувачі працюють із системою безпосередньо, а не віддалено. Як систему можна розглядати портативні та кишенькові пристрої, а також автономні робочі станції. Суть підходу полягає в тому, що механізми автентифікації та керування доступом розміщуються усередині периметра безпеки. Користувачі отримують доступ до комп'ютера або іншої захищеної системи через інтерфейс на периметрі безпеки. Інформація, що вводиться користувачами через нього всередину, а результат, що видається комп'ютером, виходить через нього назад. Система автентифікації працює правильно доти, доки зломисник не зламає периметр безпеки. Прикладом локальної аутентифікації є переносні комп'ютери. З погляду адміністрування кожен пристрій є окремим пунктом обслуговування.

Пряма автентифікація

Дана типова модель заснована на простій архітектурі системи автентифікації віддалених користувачів. Користувачі не використовують систему безпосередньо - вони вводять автентифікаційні дані у віддаленого клієнта, які (часто у зашифрованому вигляді) надсилаються до БД авторизованих користувачів системи для порівняння. Такий підхід реалізується, якщо підтримується єдина точка обслуговування або кожна точка обслуговування має окрему спільноту користувачів. Власник кожної точки

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

обслуговування заздалегідь знає, кому слід дозволити їм користуватися. Механізм паролів ОС Unix якраз і забезпечує пряму автентифікацію. Іншими прикладами є одноточкові мережеві сервери, аналогічні початковому варіанту мережного менеджера LAN Manager Microsoft, та сервер старої ОС Novell NetWare 3.

Суть моделі прямої аутентифікації у тому, що обчислювальні служби перебувають у одному фізично захищеному місці, а точки їх використання (клієнти) необов'язково захищені. Назва «пряма» пояснюється тим, що точка обслуговування приймає рішення про автентифікацію сама. Механізми автентифікації та управління доступом, а також самі служби знаходяться в одному пристрої. Адміністратори підтримують БД користувачів у кожній системі.

Підхід найкраще застосовується, коли адмініструється одна система чи група систем із незалежними користувачами. А якщо ні, то може знадобитися внести кожного користувача в кілька БД. Під час створення додаткової точки обслуговування проблема загострюється.

Істотним мінусом прямої моделі є недостатня стійкість до збоїв, оскільки все централізоване. Крім того, оскільки користувачам не обов'язково взаємодіяти з системою із захищеного місця, то зломщики можуть вибрати в якості своєї мішені віддалені користувальницькі робочі станції або їх канали зв'язку. Через ризик активної розвідки системи з прямою аутентифікацією зазвичай вимагають криптозахисту (зазвичай буває достатньо шифрування паролів, а не всього трафіку).

Непряма автентифікація

Рішення з урахуванням непрямой аутентифікації вирішують завдання масштабованості на обчислювальних центрах, які мають одна група користувачів, але кілька точок обслуговування. Навіть на майданчику всього з двома серверами важко підтримувати сумісність двох окремих БД аутентифікації. Якщо два попередні методи передбачають об'єднання механізмів аутентифікації та управління доступом, то в даній моделі механізм

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

аутентифікації з точки обслуговування переходить на сервер аутентифікації, що колективно використовується, з єдиною базою даних записів про користувачів. Всі інші компоненти надають послуги або керують доступом до ресурсів, але не ухвалюють рішення про автентифікацію.

Непряма автентифікація знайшла застосування в багатьох додатках, що керують трафіком на межах мереж/підмереж і використовують одноразові паролі та ресурси мережної ОС.

У першому випадку автентифікацією займається сервер мережного доступу (Network Access Server, NAS), який працює з протоколами тунелювання (вони розглянуті у шостому розділі підручника). Коли компанія Cisco почала випускати сервери мережного доступу, для аутентифікації з'єднань по комутованих каналах зв'язку був обраний протокол TACACS та його вдосконалені версії XTACACS і TACACS+.

Іншим відкритим стандартом для реалізації непрямої аутентифікації користувачів телефонними лініями є протокол RADIUS. Сервери віддаленого доступу, які підтримують останні версії цього протоколу, зазвичай працюють із системами одноразових паролів.

Для виконання запитів на серверах Windows-доменів та верифікації особи користувачів використовуються різні варіанти протоколу SMB. Таку ж роль грає і протокол Kerberos, реалізований у сучасних ОС Windows і вирішує головним чином завдання керування ключами.

У загальному випадку протокол непрямої автентифікації починає свою роботу, коли хтось намагається зареєструватися у точці обслуговування з віддаленого місця, яким може бути, наприклад, робоча станція. Коли точка обслуговування приймає запит на реєстрацію, вона пересилає ім'я користувача та пароль, біометричні або інші характеристики сервера автентифікації. Якщо він підтверджує аутентифікацію, він посилає в точку обслуговування відповідне підтвердження. Отримавши його, точка обслуговування приймає до виконання спробу користувача зареєструватися. Якщо сервер надсилає відмову, то точка обслуговування відкидає запит. Щоправда, є небезпека того, що

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

зловмисник для обману зможе згенерувати повідомлення «автентифікацію підтверджено». Тому між сервером аутентифікації та точкою обслуговування рекомендується застосовувати шифрування.

Деякі системи непрямої автентифікації можуть мати високий рівень відмови стійкості, підтримуючи автономну реплікацію БД на різні хости для розподілу автентифікаційного навантаження між кількома віддаленими системами.

Автономна автентифікація

Автономна модель призначена для вирішення внутрішньої суперечності, властивій розподіленої аутентифікації: власник не може довіряти кожному пристрою, що потребує аутентифікації. Деякі програми настільки великі або розподілені (або ізольовані), що вони не можуть покладатися на централізований сервер для аутентифікації в реальному часі. Але при цьому власник хоче зберегти централізоване керування автентифікацією. Реальні приклади - електронна комерція або пересилання електронної пошти.

Цей підхід поєднує особливості перших трьох моделей. Як у локальному випадку, аутентифікації може виконуватися на автономній системі без створення мережного з'єднання реального часу. Як при локальному і прямому випадках, механізм аутентифікації розміщується на тому ж пристрої, що і механізм управління доступом. Подібно до непрямих рішень, власник може підтримувати один централізований список авторизованих користувачів.

Важливою особливістю автономної аутентифікації є її відмовостійкість.

Реалізують автономну аутентифікацію, наприклад, інфраструктури відкритих ключів, де аутентифікація здійснюється в два етапи з використанням відкритих ключів для підтвердження аутентифікаційних даних окремих користувачів або інших об'єктів. Власник не повинен створювати, підтримувати та адмініструвати записи про користувачів за допомогою доступної системи. Це робить ПЗ управління видачею сертифікатів. Зловмисники не можуть безпосередньо проникнути в механізм реєстрації, оскільки він недоступний в інтерактивному режимі.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

Для даної мережі було створено такі користувачі, як:

- admin – має максимальні права та привілеї (15)
- employee – має середні права та привілеї (7)
- tech – має права та привілеї вище середнього (12)
- quest – має мінімальні права та привілеї (3)

А також створено backup користувача cisco, який буде працювати лише коли не буде доступу до серверу. Кінцеві точки доступу PC1 та PC2 в нашій системі є суплікантами.

2.3. Розробка схеми журналювання подій системи аутентифікації

Журналювання - це процес запису в хронологічному порядку подій, що відбуваються з якимсь об'єктом. В інформаційних технологіях як такий об'єкт може представлятися файлова система, операційна система або окрема програма. Запис може здійснюватися у файл або базу даних. За цими записами можна зрозуміти, що зараз відбувається з об'єктом, що спостерігається, або ж відновити, що з ним відбувалося в якийсь цікавий для нас момент часу.

Завдяки записам в журналах можна дізнатися про те, що якийсь інцидент відбувається прямо зараз, або ж розслідувати вже інцидент, знайти передумови до нього, відновити хід подій, що передують його виникненню, і виявити ті елементи, взаємодія з якими зробило його можливим.

Припустимо, перестав відповідати сервер, на якому працює певний веб-додаток. У відповідь на запити сервер повертає код 404 або 500 (а то взагалі мовчить) і належним чином працювати не бажає. У такому випадку можна переглянути журнали реєстрації подій цього сервера, які зазвичай являють собою всі одержувані сервером запити. Їх можна подивитися і знайти той із них, що передував припиненню роботи сервера, який до цього міг призвести.

Окрім одержуваних веб-сервером запитів журналювати можна події в операційній системі, на серверах баз даних, у різних засобах безпеки, в програмах користувача, на зовнішньому проксі-сервері та інші. Якщо нас цікавить лише веб-сервер і те, що відбувається з ним, то і події нас цікавитимуть лише його. Якщо ж нас цікавить загальний стан захищеності та

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

працездатності інформаційної системи, то є сенс стежити за подіями на різних її вузлах, а також на мережному обладнанні. Це дозволить відстежувати складніші взаємодії всередині системи. Наприклад, у системі з'явився вірус — за журналами можна спробувати визначити, як і куди він далі розповсюджується і звідки взагалі з'явився. Або якщо відбувається DoS-атака, можна зрозуміти, з якого пристрою. І так далі.

Приклади подій, що журналюються:

- успішний або неуспішний вхід користувача до системи;
- вихід користувача із системи;
- додавання, видалення або зміна даних користувача;
- додавання, видалення чи зміна файлів;
- запити до сервера;
- заблоковані мережеві пакети;
- дозволені мережеві пакети;
- передача файлів;
- та інше.

Але журнали потрібно захищати. Адже при найменшому сумніві в цілісності та справжності записів журналу такому ж сумніву піддається вся інформація, що отримується з нього. Відповідно, ставиться під питання використання журналу як достовірне джерело. Так само й зацікавлений свідок у суді лише заплутує слідство. Зазвичай це вирішується призначенням прав доступу, які дозволяють запис і редагування нікому крім системи. На випадок якщо зломиснику все ж таки вдасться модифікувати журнал, добре б мати його резервну копію. Ця копія може зберігатися на віддаленому сервері або на тому самому, але в зашифрованому вигляді і, можливо, в іншій директорії.

Журнал — незамінний інструмент для моніторингу стану системи та розслідування інцидентів безпеки.

З технічних причин додавання і налаштування серверу журналювання стало неможливим, тому було вирішено його не додавати, а його теоретичне налаштування пред'явлено нижче.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

Ввімкнення ведення журналу:

(config)# logging on

(config)# logging buffered

(config)# logging trap <0-7>

0 - мінімальне, 7- записувати всі повідомлення

Додати системний час в повідомлення:

(config)# service timestamps log datetime msec localtime show-timezone

Збір даних на syslog-сервер:

(config)# logging facility local7

(config)# logging trap info

(config)# logging <servername.com>

Увімкнути сервіс нумерації повідомлень та запису історії відвідування:

(config)# service sequence-numbers

(config)# login on failure log

(config)# login on success log

Висновки до другого розділу

В данному розділі було проаналізовано топологію мережі, розглянено типові схеми аутентифікації пристроїв, а саме, такі як локальна автентифікація, пряма автентифікація, непряма автентифікація та автономна автентифікація. Було проаналізовано журналювання подій системи аутентифікації, приклади подій які журналюються і визначено, що журнал – незамінний інструмент для моніторингу стану системи та розслідування інцидентів безпеки, але він має і свої мінуси, такі як обов’язкова необхідність його захисту.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. ВИБІР ТА НАЛАГОДЖЕННЯ ОБЛАДНАННЯ, ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ТУСТУВАННЯ ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ

3.1. Вибір обладнання та програмного забезпечення

При виборі моделі маршрутизатора необхідно враховувати як він маршрутизує пакети в складній мережі з різними видами топологій. Маршрутизатор повинен містити достатню кількість портів, забезпечувати легке розширення мережі, забезпечувати необхідну швидкість передачі даних та швидкість їх обробки.

В данному випадку було взято за основу один із маршрутизаторів Cisco 7600 Series, який використовує програмне забезпечення Cisco IOS v15.6.



Рисунок 3.1 - Маршрутизатори Cisco 7600 Series

Програмне забезпечення Cisco IOS (Internetworking Operating System) — це платформа, яка надає мережеві послуги та підтримує мережеві програми. На маршрутизаторах і серверах доступу Cisco працює провідне програмне забезпечення Cisco IOS. Програмне забезпечення Cisco IOS плавно зв'язує різноманітні носії та пристрої через найширший набір протоколів. Сервіси керування, властиві програмному забезпеченню Cisco IOS, надають необхідні інструменти, які дозволяють розширити вашу мережу, щоб не відставати від вимог бізнесу, що швидко змінюються.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

Серія маршрутизаторів відповідає вимогам сучасних офісів. Модульна архітектура призначена для підтримки зростаючих вимог клієнтів, збільшення пропускної спроможності і установки модулів для розподілу потужності.

Всі великі IT-компанії ґрунтують свою діяльність на використанні мережеских можливостей. Ні для кого не є секретом того, що інтернет і мережескі технології займають у розвитку будь-якого підприємства дуже важливу роль. Багато замовників отримують або відправляють завдання за допомогою доступу до мережі. Але метою перед компанією є не тільки вихід до глобальної паутини, немало важливим залишається питання з побудовою локальної мережі, по магістралям якої будуть відправлятися потоки інформації.

Маршрутизатори серії 7600 є основою, яка служить платформою для подальшого розвитку підприємства. Надійний і в тей же час високоефективний протокол IP був використаний багатьма вимірними центрами, як засіб отримання зв'язку. На його базі будуються послуги інтернет-провайдерів, чия клієнтська база може розраховувати більше мільйонів користувачів. Лінійка маршрутизаторів серії 7600 може використовуватися і великими компаніями. Зручність використання даних продуктів полягає в тому, що вони підтримують різні інтерфейси, здатні адаптуватися до завантажених мереж і продовжувати виконувати свої обов'язки. Сімейство маршрутизаторів Series 7600 отримало всезагальне звання за рахунок своїх високих показників не тільки при початкових тестуваннях на території компанії – розробника, але також під час виконання серйозних завдань. Маршрутизатори серії 7600 прийшли на заміну версії 7500, але вмістили в себе набагато більше можливостей. Аналогічно минулому поколінню з'явилася підтримка швидкої комутації даних, а також швидкісної маршрутизації інформаційних пакетів.

При використанні одного слота користувач отримує пропускну здатність в 1 Гбіт в секунду. Що для одного підключеного порту достатньо. Щоб істотно збільшити дані показники, необхідно прибігти до оснащення декількох роз'ємів. Лінійка маршрутизаторів серії 7600 часто використовується інтернет-провайдерами в містах для побудови надійної клієнтської мережі, де будь-яка

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

комірка буде отримувати постійний дохід, тим самим повертати вкладені гроші. Сімейство маршрутизаторів Series 7600 легко налаштовується, користувач при виборі може вибирати низькошвидкісний або високошвидкісний потік передачі даних.

В якості комутатору було взято за основу стандартно влаштований Ethernet Switch, так як в програмному середовищі GNS3 відсутня можливість емулювати комутатори, так як в них влаштовані спеціалізовані мікросхеми, які не можна емулювати на ПК.

3.2. Налагодження підсистеми аутентифікації

Спочатку налаштуємо адресацію маршрутизаторам, комутаторам та серверам. Лістинг коду налаштування буде представлений на скріншотах нижче, рисунки 3.2 – 3.6.

```
root@AAA-1:~# nano /etc/network/interfaces
root@AAA-1:~# cat /etc/network/interfaces
#
# This is a sample network config, please uncomment lines to configure the network
#
# Uncomment this line to load custom interface files
# source /etc/network/interfaces.d/*
#
# Static config for eth0
auto eth0
iface eth0 inet static
    address 192.168.122.201
    netmask 255.255.255.0
    gateway 192.168.122.1
    up echo nameserver 192.168.122.1 > /etc/resolv.conf
```

Рисунок 3.2 – Налаштування IP-адреси для серверу

Було вирішено використовувати IP-адресу 192.168.122.0, так як цю підмережу використовує за замовчуванням мережа ISP.

```
Router(config)#int gig0/1
Router(config-if)#ip add
Router(config-if)#ip address 192.168.122.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#no shutdown
Router(config-if)#ex
*Apr 11 09:32:23.232: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, change
e to up
*Apr 11 09:32:24.232: %LINEPROTO-5-UPDOWN: Line protocol on Interface Giga
ernet0/1, changed state to up
Router(config-if)#ex
Router(config)#int gig0/0
Router(config-if)#ip address 192.168.122.10 255.255.255.0
% 192.168.122.0 overlaps with GigabitEthernet0/1
% 192.168.122.0 overlaps with GigabitEthernet0/1
Router(config-if)#ip address 192.168.10.10 255.255.255.0
Router(config-if)#no shut
Router(config-if)#no shutdown
Router(config-if)#ex
```

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

Рисунок 3.3 - Налаштування IP-адреси маршрутизатора R1

```
R2(config)#int gig0/0
R2(config-if)#ip add
R2(config-if)#ip address 192.168.100.10 255.255.255.0
R2(config-if)#no shut
R2(config-if)#no shutdown
R2(config-if)#ex
R2(config-if)#exit
R2(config)#
*Apr 11 13:07:51.639: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Apr 11 13:07:52.639: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R2(config)#int gig0/1
R2(config-if)#ip address 192.168.122.11 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#ex
R2(config-if)#exit
```

Рисунок 3.4 - Налаштування IP-адреси маршрутизатора R2

```
PC1> ip 192.168.122.5/24 192.168.122.4
Checking for duplicate address...
PC1 : 192.168.122.5 255.255.255.0 gateway 192.168.122.4
```

Рисунок 3.5 - Налаштування IP-адреси PC1 та PC2

```
PC2> ip 192.168.122.6/24 192.168.122.4
Checking for duplicate address...
PC2 : 192.168.122.6 255.255.255.0 gateway 192.168.122.4
```

Рисунок 3.6 - Налаштування IP-адреси PC1 та PC2

Перед початком налаштування маршрутизаторів потрібно перевірити зв'язок між сусідніми пристроями.

```
root@AAA:~# ping 192.168.122.1
PING 192.168.122.1 (192.168.122.1) 56(84) bytes of data.
64 bytes from 192.168.122.1: icmp_seq=1 ttl=255 time=1.73 ms
64 bytes from 192.168.122.1: icmp_seq=2 ttl=255 time=1.40 ms
64 bytes from 192.168.122.1: icmp_seq=3 ttl=255 time=1.24 ms
^C
--- 192.168.122.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.241/1.458/1.734/0.210 ms
```

Рисунок 3.7 – Виконання команди ping між сервером та комутатором

```
Router#ping 192.168.122.201
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.122.201, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Рисунок 3.8 – Виконання команди ping між маршрутизатором та сервером

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

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

Рисунок 3.9 – Перевірка наявних користувачів та їх паролів

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

```

root@AAA:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.122.201 netmask 255.255.255.0 broadcast 0.0.0.0
    inet6 fe80::60eb:62ff:fela:36b9 prefixlen 64 scopeid 0x20<link>
    ether 62:eb:62:1a:36:b9 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 656 (656.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Рисунок 3.10 – Виконання команди ifconfig на сервері

Тепер можна розпочати налаштування моделі AAA на пристроях та створення бекуп користувача cisco.

```

R1 - PuTTY
Router(config)#aaa new-model
Router(config)#username cisco pass
Router(config)#username cisco password cisco
Router(config)#enable pass
Router(config)#enable password cisco
Router(config)#radius server radius1
Router(config-radius-server)#add
Router(config-radius-server)#address ipv4 192.168.122.201 au
Router(config-radius-server)#address ipv4 192.168.122.201 auth-port 1812 acc
Router(config-radius-server)#$4 192.168.122.201 auth-port 1812 acct-port 1813
Router(config-radius-server)#key gns3
Router(config-radius-server)#end

```

Рисунок 3.11 – Налаштування маршрутизатора R1

```

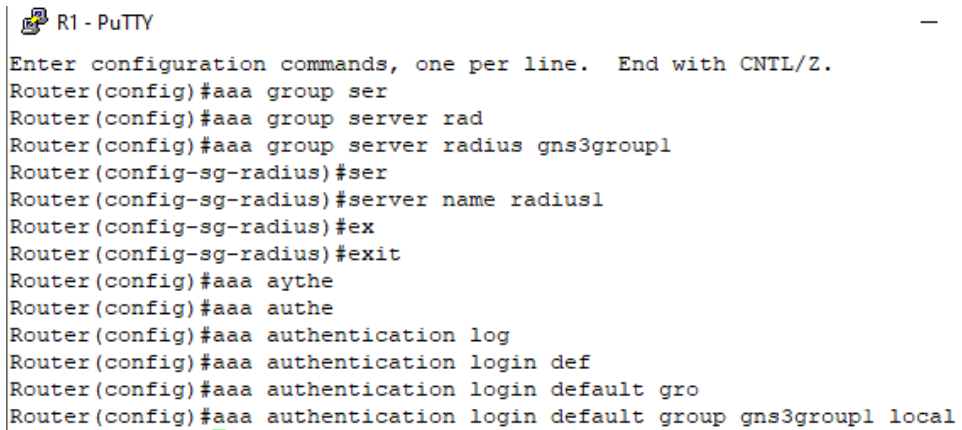
R2(config)# aaa new-model
R2(config)#userna
R2(config)#username cisco pass
R2(config)#username cisco password cisco
R2(config)#enable password cisco
R2(config)#radius server radius1
R2(config-radius-server)#address ipv4 192.168.122.201 au
R2(config-radius-server)#address ipv4 192.168.122.201 auth-port 1821 acc
R2(config-radius-server)#$4 192.168.122.201 auth-port 1812 acct-port 1813
R2(config-radius-server)#key gns3

```

Рисунок 3.12 – Налаштування маршрутизатора R2

Наступним кроком нам потрібно створити AAA групу, щоб вказати підмножину серверів RADIUS для використання як метод автентифікації входу.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		



```

R1 - PuTTY
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#aaa group ser
Router(config)#aaa group server rad
Router(config)#aaa group server radius gns3group1
Router(config-sg-radius)#ser
Router(config-sg-radius)#server name radius1
Router(config-sg-radius)#ex
Router(config-sg-radius)#exit
Router(config)#aaa aythe
Router(config)#aaa authe
Router(config)#aaa authentication log
Router(config)#aaa authentication login def
Router(config)#aaa authentication login default gro
Router(config)#aaa authentication login default group gns3group1 local

```

Рисунок 3.13 – Створення gns3group1 на R1

```

R2(config-sg-radius)#server name radius1
R2(config-sg-radius)#exit
R2(config)#aaa auth
R2(config)#aaa authe
R2(config)#aaa authentication log
R2(config)#aaa authentication login def
R2(config)#aaa authentication login default group gns3group2
R2(config)#aaa authentication login default group gns3group2 local
R2(config)#
R2(config)#
R2(config)#aaa authe
R2(config)#aaa authentication ena
R2(config)#aaa authentication enable def
R2(config)#aaa authentication enable default enable

```

Рисунок 3.14 – Створення gns3group1 на R2

Далі включимо telnet, це мережевий протокол для реалізації текстового інтерфейсу по мережі (у сучасній формі — за допомогою транспорту TCP).

```

Router(config)#line vty 0 4
Router(config-line)#tr
Router(config-line)#transport inp
Router(config-line)#transport input all
Router(config-line)#end

```

Рисунок 3.15 – Ввімкнення telnet на R1

```

R2(config)#line vty 0 4
R2(config-line)#rt
R2(config-line)#tr
R2(config-line)#transport inp
R2(config-line)#transport input all
R2(config-line)#end

```

Рисунок 3.16 – Ввімкнення telnet на R2

Наступним кроком створимо декілька користувачів з різним рівнем доступу для підсистеми.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

```
Router(config)#username admin password cisco
Router(config)#username admin privilege 15
Router(config)#username employee password 123
Router(config)#username employee privilege 7
Router(config)#end
```

Рисунок 3.17 – Створення користувачів на R1

```
R2 (config)#username admin password cisco
R2 (config)#username admin privilege 15
R2 (config)#username tech password 1234
R2 (config)#username tech privilege 12
R2 (config)#username quest password 12
R2 (config)#username quest privilege 3
```

Рисунок 3.18 – Створення користувачів на R2

Далі налаштуємо протокол dot1x на маршрутизаторах.

```
Router(config)#aaa new-model
Router(config)#dot1x system-auth-control
Router(config)#aaa group server radius dot1x
Router(config-sg-radius)#server 192.168.122.201
Router(config-sg-radius)#erx
      ^
% Invalid input detected at '^' marker.

Router(config-sg-radius)#ex
Router(config)#aaa authe
Router(config)#aaa authentication dot1x default group dot1x
```

Рисунок 3.19 – Налаштування протоколу dot1x на R1

```
R2 (config)#aaa new-model
R2 (config)#dot1x system-auth-control
R2 (config)#aaa group server radius dot1x
R2 (config-sg-radius)#server 192.168.122.201
R2 (config-sg-radius)#
*Apr 14 10:58:27.213: %RADIUS-4-NOSERV: Warning: Server 192.168.12
6 is not defined.
R2 (config-sg-radius)#ex
R2 (config)#aaa auth`
R2 (config)#aaa auth
R2 (config)#aaa authe
R2 (config)#aaa authentication dot1x default group dot1x
```

Рисунок 3.20 – Налаштування протоколу dot1x на R2

3.3. Тестування роботи підсистеми аутентифікації

В попередньому пункті було налаштована повністю дану мережу. В даному пункті перевіримо налаштування.

Для початку перевіримо зв'язок між пристроями.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Router#ping 192.168.122.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.122.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
Router#ping 192.168.122.201
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.122.201, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

```

Рисунок 3.21 – Виконання команди ping R1

```

R2#ping 192.168.122.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.122.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R2#ping 192.168.122.201
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.122.201, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
R2#ping 192.168.122.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.122.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 2/2/3 ms

```

Рисунок 3.22 – Виконання команди ping R2

```

PC1> ping 192.168.122.201

84 bytes from 192.168.122.201 icmp_seq=1 ttl=64 time=0.608 ms
84 bytes from 192.168.122.201 icmp_seq=2 ttl=64 time=0.724 ms
84 bytes from 192.168.122.201 icmp_seq=3 ttl=64 time=0.424 ms
84 bytes from 192.168.122.201 icmp_seq=4 ttl=64 time=0.334 ms
84 bytes from 192.168.122.201 icmp_seq=5 ttl=64 time=0.398 ms

PC1> ping 192.168.122.1

84 bytes from 192.168.122.1 icmp_seq=1 ttl=255 time=1.382 ms
84 bytes from 192.168.122.1 icmp_seq=2 ttl=255 time=1.133 ms
84 bytes from 192.168.122.1 icmp_seq=3 ttl=255 time=1.331 ms
84 bytes from 192.168.122.1 icmp_seq=4 ttl=255 time=1.599 ms
84 bytes from 192.168.122.1 icmp_seq=5 ttl=255 time=1.414 ms

PC1> ping 192.168.122.11

84 bytes from 192.168.122.11 icmp_seq=1 ttl=255 time=1.453 ms
84 bytes from 192.168.122.11 icmp_seq=2 ttl=255 time=1.316 ms
84 bytes from 192.168.122.11 icmp_seq=3 ttl=255 time=1.108 ms
84 bytes from 192.168.122.11 icmp_seq=4 ttl=255 time=1.504 ms
84 bytes from 192.168.122.11 icmp_seq=5 ttl=255 time=1.251 ms

```

Рисунок 3.23– Виконання команди ping на PC1

Далі спробуємо увійти до підмережі за допомогою команди telnet, використовуючи стандартних користувачів AAA серверу, це користувачі alice та bob, пароль gns3 для кожного з них.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Router#telnet 192.168.122.1
Trying 192.168.122.1 ... Open

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's    *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any      *
* purposes is expressly prohibited except as otherwise authorized by    *
* Cisco in writing.                                                       *
*****

User Access Verification

Username: alice
Password:
Hello, alice

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's    *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any      *
* purposes is expressly prohibited except as otherwise authorized by    *
* Cisco in writing.                                                       *
*****

```

Рисунок 3.24 – Вхід до системи з R1, користувач alice

```

Router#telnet 192.168.122.1
Trying 192.168.122.1 ... Open

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's    *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any      *
* purposes is expressly prohibited except as otherwise authorized by    *
* Cisco in writing.                                                       *
*****

User Access Verification

Username: bob
Password:
Hello, bob

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's    *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any      *
* purposes is expressly prohibited except as otherwise authorized by    *
* Cisco in writing.                                                       *
*****

Router>
Router>en
Password:

```

Рисунок 3.25 – Вхід до системи з R1, користувач bob

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

```

Router#show line
  Tty Typ      Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns  Int
*    0 CTY          -    -        -    -    -     1       0      0/0      -
  1 AUX    9600/9600  -    -        -    -    -     0       0      0/0      -
*   578 VTY          -    -        -    -    -     2       0      0/0      -
  579 VTY          -    -        -    -    -     1       0      0/0      -
  580 VTY          -    -        -    -    -     0       0      0/0      -
  581 VTY          -    -        -    -    -     0       0      0/0      -
  582 VTY          -    -        -    -    -     0       0      0/0      -

Line(s) not in async mode -or- with no hardware support:
2-577

Router#exit

[Connection to 192.168.122.1 closed by foreign host]
Router#show line
  Tty Typ      Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns  Int
*    0 CTY          -    -        -    -    -     1       0      0/0      -
  1 AUX    9600/9600  -    -        -    -    -     0       0      0/0      -
  578 VTY          -    -        -    -    -     2       0      0/0      -
  579 VTY          -    -        -    -    -     1       0      0/0      -
  580 VTY          -    -        -    -    -     0       0      0/0      -
  581 VTY          -    -        -    -    -     0       0      0/0      -
  582 VTY          -    -        -    -    -     0       0      0/0      -

Line(s) not in async mode -or- with no hardware support:
2-577

```

Рисунок 3.26 – Виконання команди show line на R1

```

R2#telnet 192.168.122.11
Trying 192.168.122.11 ... Open

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****

User Access Verification

Username: alice
Password:
Hello, alice

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****

R2>enable
Password:
% Access denied

R2>en
Password:
R2#

```

Рисунок 3.27 – Вхід до системи з R2, користувач alice

```

R2#show line
  Tty Typ      Tx/Rx    A Modem  Roty AccO AccI   Uses   Noise  Overruns  Int
*    0 CTY          -    -        -    -    -     1       0      0/0      -
  1 AUX    9600/9600  -    -        -    -    -     0       0      0/0      -
*   578 VTY          -    -        -    -    -     1       0      0/0      -
  579 VTY          -    -        -    -    -     0       0      0/0      -
  580 VTY          -    -        -    -    -     0       0      0/0      -
  581 VTY          -    -        -    -    -     0       0      0/0      -
  582 VTY          -    -        -    -    -     0       0      0/0      -

Line(s) not in async mode -or- with no hardware support:
2-577

```

Рисунок 3.28 – Виконання команди show line на R2

Тепер перевіримо користувачів, що було створено, а саме користувач admin, з паролем cisco та користувач employee з паролем 123, створені на R1.

```
Username: admin
Password:

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****
Router>en
Router>enable
Password:
% Access denied

Router>en
Password:
Router#tel
```

Рисунок 3.29 – Вхід до системи з R1, користувач admin

```
Username: employee
Password:
*Apr 14 13:07:04.912: %RADIUS-4-RADIUS_DEAD: RADIUS server 192.168.122.201:1812,
1813 is not responding.
*Apr 14 13:07:04.912: %RADIUS-4-RADIUS_ALIVE: RADIUS server 192.168.122.201:1812
,1813 is being marked alive.

*****
* IOSv is strictly limited to use for evaluation, demonstration and IOS *
* education. IOSv is provided as-is and is not supported by Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any *
* purposes is expressly prohibited except as otherwise authorized by *
* Cisco in writing. *
*****
Router>en
Password:
Router#
```

Рисунок 3.30 – Вхід до системи з R1, користувач employee

Далі виконаємо команду show running config на маршрутизаторах для перегляду поточних налаштувань кожного з них.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

```

hostname Router
!
boot-start-marker
boot-end-marker
!
!
enable password cisco
!
aaa new-model
!
!
aaa group server radius gns3group1
server name radius1
!
aaa authentication login default group gns3group1 local
aaa authentication enable default enable
aaa authentication dot1x default group radius

dot1x system-auth-control
username cisco password 0 cisco
username admin privilege 15 password 0 cisco
username employee privilege 7 password 0 123

radius server radius1
address ipv4 192.168.122.201 auth-port 1812 acct-port 1813
key gns3

```

Рисунок 3.31 – Результат виконання команди show running config на R1

```

hostname R2
!
boot-start-marker
boot-end-marker
!
!
enable password cisco
!
aaa new-model
!
!
aaa group server radius gns3group2
server name radius1
!
aaa authentication login default group gns3group2 local
aaa authentication enable default enable
aaa authentication dot1x default group radius

dot1x system-auth-control
username cisco password 0 cisco
username admin privilege 15 password 0 cisco
username tech privilege 12 password 0 1234
username ques privilege 3 password 0 12

radius server radius1
address ipv4 192.168.122.201 auth-port 1812 acct-port 1813
key gns3

```

Рисунок 3.32 – Результат виконання команди show running config на R2

					Арк.
Змн.	Арк.	№ докум.	Підпис	Дата	

Висновки до третього розділу

В данному розділі було обрано яке саме обладнання та пристрої ми будемо використовувати в нашій мережі, визначено програмне забезпечення яке використовує обладнання, а саме, Cisco IOS v15.6. Далі було поетапно налаштовано підмережу аутентифікації на пристроях.

В останньому пункті розділу було виконано команди для перевірки налаштувань пристроїв.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

В першому розділі було розглянено поняття аутентифікації, та з чого вона складається, навели декілька прикладів та чинники аутентифікації. Ми з'ясували, що аутентифікація – це підтвердження того, ким є користувач на вході. Далі ми розглянули модель AAA (Authentication, Authorization and Accounting) та три протоколи, з яких вона складається, таких як RADIUS, TACACS+ та LDAP. В основному AAA використовується для керування доступом до різних ІТ-ресурсів, таких як мережа, служби, сервери і т.д. Далі ми дізнались про особливості і принцип роботи протоколу взаємної аутентифікації Kerberos.

В другому пункті цього ж розділу ми розглянули детальніше протокол RADIUS та його ключові характеристики. А також порівняння протоколів RADIUS та TACACS+ і з'ясували, що RADIUS підтримується практично будь-яким мережевим обладнанням, чого не скажеш про TACACS+, а який протокол використовувати для AAA-сервера, необхідно обирати в залежності від завдання. Якщо це адміністрування пристроїв, то TACACS+ стане найкращим варіантом, а якщо доступ до мережі, то універсальніший і швидший – RADIUS.

В останньому пункті було розглянено технологію 802.1X, основні її компоненти, особливості застосування. А також механізм автентифікації з загальною назвою EAP (Extensible Authentication Protocol), який дозволив зробити аутентифікацію прозорою для серверів доступу різних виробників.

В другому розділі було проаналізовано топологію побудованої мережі, розглянено типові схеми аутентифікації пристроїв, такі як локальна аутентифікація, пряма аутентифікація, непряма аутентифікація та автономна аутентифікація.

Далі було проаналізовано журналювання подій системи аутентифікації, приклади подій які журналюються і визначено, що журнал – незамінний інструмент для моніторингу стану системи та розслідування інцидентів безпеки, але він має і свої мінуси, такі як обов'язкова необхідність його захисту.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

В останньому розділі кваліфікаційної роботи було обрано яке саме обладнання ми будемо використовувати в нашій мережі і вибір впав на серію маршрутизаторів Cisco 7600 Series. Наступним кроком було визначено програмне забезпечення яке використовує саме це обладнання, це виявилось Cisco IOS v15.6. В наступному пункті було поетапно налаштовано підмережу аутентифікації на пристроях мережі. В останньому пункті розділу ми виконали команди для перевірки налаштувань пристроїв та перевірили працездатність підмережі.

Отже, в результаті роботи над кваліфікаційною роботою було досягнуто її мети, побудовано та налаштовано пісистему аутентифікації кампусної мережі організації.

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Authorization, Authentication, Accounting [Електронний ресурс] – Режим доступу:
<https://networkradius.com/doc/current/concepts/introduction/AAA.html>
2. Аутентифікація в Cisco IOS [Електронний ресурс] – Режим доступу:
<https://habr.com/ru/companies/pt/articles/192668/>
3. Что такое AAA [Електронний ресурс] – Режим доступу:
<https://itsecforu.ru/2020/09/29/□-что-такое-aaa-аутентификация-авториз/>
4. RADIUS [Електронний ресурс] – Режим доступу:
<https://www.itperfection.com/network-administration/radius-server-network-security-nas-authentication-aaa-authorization-accounting/>
5. ПРАКТИЧНА БЕЗПЕКА МЕРЕЖ [Електронний ресурс] – Режим доступу: <http://blog.netskills.ru/2017/01/network-security13.html>
6. Налаштування RADIUS-серверу [Електронний ресурс] – Режим доступу: <https://www.dlink.ru/ru/faq/487/2095.html>
7. Аутентифікація, авторизація та облік (AAA) – RADIUS або TACACS+ [Електронний ресурс] – Режим доступу:
<https://vasexperts.ru/blog/tehnologii/autentifikacziya-avtorizacziya-i-uchet-aaa-radius-ili-tacacs/>
8. TACACS и Radius сервери [Електронний ресурс] – Режим доступу:
<https://forum.huawei.com/enterprise/ru/tacacs-и-radius-серверы-сравнение/thread/787955-100335>
9. Порівняння протоколів TACACS+ и RADIUS [Електронний ресурс] – Режим доступу:
https://studbooks.net/2411296/informatika/sravnienie_protokolov_tacacs_radius
10. Configuring AAA on Cisco Devices – RADIUS and TACACS+ [Електронний ресурс] – Режим доступу: <https://study-ccna.com/aaa-cisco-configuration/>

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

						Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R2#show run
Building configuration...

Current configuration : 3618 bytes
!
version 15.6
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
enable password cisco
!
aaa new-model
!
!
aaa group server radius gns3group2
server name radius1
!
aaa authentication login default group gns3group2 local
aaa authentication enable default enable
aaa authentication dot1x default group radius
!
!
!
!
aaa session-id common
ethernet lmi ce
!
!
!
no process cpu autoprofile hog
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
dot1x system-auth-control
username cisco password 0 cisco

!
redundancy
!
no cdp log mismatch duplex
no cdp run
!
ip tcp synwait-time 5
!
interface GigabitEthernet0/0
ip address 192.168.100.10 255.255.255.0
duplex auto
speed auto
media-type rj45
no cdp enable
!
interface GigabitEthernet0/1
ip address 192.168.122.11 255.255.255.0
duplex auto
speed auto
media-type rj45
no cdp enable
!
interface GigabitEthernet0/2
no ip address
shutdown
duplex auto
speed auto
media-type rj45
no cdp enable
!
interface GigabitEthernet0/3
no ip address
shutdown
duplex auto
speed auto
media-type rj45
no cdp enable
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
radius server radius1
address ipv4 192.168.122.201 auth-port 1812 acct-port 1813
key gns3
!
!
control-plane
!
banner exec ^C
*****
*****
* IOSv is strictly limited to use for evaluation, demonstration
and IOS *
* education. IOSv is provided as-is and is not supported by
Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole
or in part, *

```

```

* of the IOSv Software or Documentation to any third party
for any *
* purposes is expressly prohibited except as otherwise
authorized by *
* Cisco in writing. *
*****
*****^C
banner incoming ^C
*****
*****
* IOSv is strictly limited to use for evaluation, demonstration
and IOS *
* education. IOSv is provided as-is and is not supported by
Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole
or in part, *
* of the IOSv Software or Documentation to any third party
for any *
* purposes is expressly prohibited except as otherwise
authorized by *
* Cisco in writing. *
*****
*****^C
banner login ^C
*****
*****
* IOSv is strictly limited to use for evaluation, demonstration
and IOS *
* education. IOSv is provided as-is and is not supported by
Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole
or in part, *
* of the IOSv Software or Documentation to any third party
for any *
* purposes is expressly prohibited except as otherwise
authorized by *
* Cisco in writing. *
*****
*****^C
!
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 all
!
no scheduler allocate
!
end

Router#show run
Building configuration...

Current configuration : 3710 bytes
!
version 15.6
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!

```

```

!
enable password cisco
!
aaa new-model
!
!
aaa group server radius gns3group1
server name radius1
!
aaa authentication login default group gns3group1 local
aaa authentication enable default enable
aaa authentication dot1x default group radius
!
!
!
aaa session-id common
ethernet lmi ce
!
!
!
no process cpu autoprofile hog
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
no ip icmp rate-limit unreachable
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
dot1x system-auth-control
username cisco password 0 cisco
username admin privilege 15 password 0 cisco
username employee privilege 7 password 0 123
!
redundancy
!
no cdp log mismatch duplex
no cdp run
!
ip tcp synwait-time 5
!
!
!
interface GigabitEthernet0/0
ip address 192.168.10.10 255.255.255.0
duplex auto
speed auto
media-type rj45
no cdp enable
!
interface GigabitEthernet0/1
ip address 192.168.122.1 255.255.255.0
duplex auto
speed auto
media-type rj45

```

```

no cdp enable
!
interface GigabitEthernet0/2
no ip address
shutdown
duplex auto
speed auto
media-type rj45
no cdp enable
!
interface GigabitEthernet0/3
no ip address
shutdown
duplex auto
speed auto
media-type rj45
no cdp enable
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
!
radius server radius1
address ipv4 192.168.122.201 auth-port 1812 acct-port 1813
key gns3
!
!
control-plane
!
banner exec ^C
*****
*****

* IOSv is strictly limited to use for evaluation, demonstration
and IOS *
* education. IOSv is provided as-is and is not supported by
Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole
or in part, *
* of the IOSv Software or Documentation to any third party
for any *
* purposes is expressly prohibited except as otherwise
authorized by *
* Cisco in writing. *
*****
*****^C

banner incoming ^C
*****
*****

* IOSv is strictly limited to use for evaluation, demonstration
and IOS *
* education. IOSv is provided as-is and is not supported by
Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole
or in part, *
* of the IOSv Software or Documentation to any third party
for any *
* purposes is expressly prohibited except as otherwise
authorized by *
* Cisco in writing. *
*****
*****^C

```

```

banner login ^C
*****
*****

* IOSv is strictly limited to use for evaluation, demonstration
and IOS *
* education. IOSv is provided as-is and is not supported by
Cisco's *
* Technical Advisory Center. Any use or disclosure, in whole
or in part, *
* of the IOSv Software or Documentation to any third party
for any *
* purposes is expressly prohibited except as otherwise
authorized by *
* Cisco in writing. *
*****
*****^C

```

```

!
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 all
!
no scheduler allocate
!
End
PC1> show ip

```

```

NAME      : PC1[1]
IP/MASK    : 192.168.122.5/24
GATEWAY    : 192.168.122.4
DNS        :
MAC        : 00:50:79:66:68:00
LPORT      : 20008
RHOST:PORT : 127.0.0.1:20009
MTU        : 1500

```

PC2> show ip

```

NAME      : PC2[2]
IP/MASK    : 192.168.122.6/24
GATEWAY    : 192.168.122.4
DNS        :
MAC        : 00:50:79:66:68:00
LPORT      : 20008
RHOST:PORT : 127.0.0.1:20009
MTU        : 1500

```

PC2> show ip

```

NAME      : PC2[1]
IP/MASK    : 192.168.122.6/24
GATEWAY    : 192.168.122.4
DNS        :
MAC        : 00:50:79:66:68:01
LPORT      : 20016
RHOST:PORT : 127.0.0.1:20017
MTU        : 1500

```