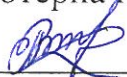


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми аутентифікації користувачів
корпоративної мережі на базі моделі AAA та протоколу
TACACS+»

Виконала студентка 4-го курсу групи КІ-4
спеціальності 123 «Комп'ютерна інженерія»

 Анжеліка Русятинська

Керівник зав. кафедри КІ та КБ, к.т.н., доцент

 Андрій Єфіменко

Рецензент проф. кафедри КІ та КБ, д.т.н., доцент

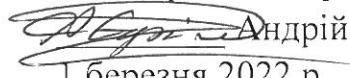
 Володимир Воротніков

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Русятинська Анжеліка Олегівна

Тема роботи: «Проект підсистеми аутентифікації користувачів корпоративної мережі на базі моделі AAA та протоколу TACACS+»

затверджена Наказом університету від 1 березня 2022 р. № 127/с

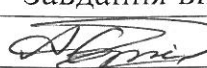
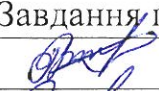
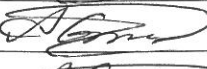
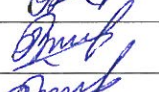
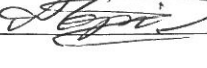
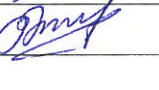
Термін здачі студентом закінченої роботи 10 червня 2022 р.

Вихідні дані роботи: об'єктом дослідження є процес побудови підсистеми аатентифікації користувачів мережі з використання моделі AAA та забезпечення їх безпеки; предметом дослідження є побудова підсистеми аутентифікації мережі на базі протоколу Tacacs+ та сервера TacacsGui.

Обладнання та програмне забезпечення:

1. GNS3
2. GNS VM
3. Vitrual Box
4. Ubuntu Desktop
5. Tacacs server GUI

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

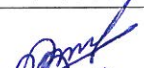
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	 1.03.22	 01.03.22
2	Єфіменко А.А.	 1.03.22	 01.03.22
3	Єфіменко А.А.	 1.03.22	 01.05.22

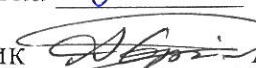
Студентка  Анжеліка Русятинська

Керівник  Андрій Єфіменко

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Аналіз теоретичних основ моделі AAA	02.03.2022 – 07.03.2022	
2	Аналіз протоколів AAA та їх безпеки	08.03.2022 – 13.03.2022	
3	Вивчення протоколу Tascacs+ та способів його реалізації	14.03.2022 – 20.03.2022	
4	Вивчення статичної та динамічної маршрутизації, редистрибуції	21.03.2022 – 26.03.2022	
5	Розробка топології мережі, аналіз побудови мереж	27.03.2022 – 11.04.2022	
6	Розробка адресації мережі з використанням CIDR та VLSM	11.04.2022 – 20.04.2022	
7	Аналіз та вибір обладнання та побудова мережі	21.04.2022 – 26.04.2022	
8	Розробка моделі AAA на базі протоколу Tascacs+	27.04.2022 – 02.05.2022	
9	Налаштування статичної та динамічної адресації, редистрибуції, моделі AAA	03.05.2022 – 20.05.2022	
10	Тестування працездатності схеми	21.05.2022 – 27.05.2022	
11	Написання пояснювальної записки	28.05.2022 – 15.06.2022	
12	Захист	22.06.2022	

Студентка  Анжеліка Русятинська

Керівник  Андрій Єфіменко

АНОТАЦІЯ

Випускна кваліфікаційна робота бакалавра складається з пояснювальної записки, що нараховує загальний обсяг 105 сторінок, 35 рисунків та 5 таблиць. Список використаної літератури налічує 23 найменування та розміщений на 2 сторінках.

Метою кваліфікаційної роботи є розробка підсистеми аутентифікації користувачів корпоративної мережі на базі моделі AAA та протоколу TACACS+.

В результаті виконання випускної кваліфікаційної роботи бакалавра було визначено основні завдання для розробки системи аутентифікації користувачів на базі моделі AAA та протоколу TACACS+, проаналізовано базові поняття та приклади налаштування протоколу, розроблено топологію мережі та її адресація, побудована та налаштована схема. Також розроблено систему авторизації, автентифікації та обліку. Результат роботи протестований та відповідає поставленим вимогам.

Ключові слова: AAA, TACACS+, МЕРЕЖА, СХЕМА, АДРЕСАЦІЯ, ТОПОЛОГІЯ, EIGHT, РЕДИСТРИБУЦІЯ.

					КІК.КР.Б – 123 – 19 – ПЗ		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.	Рустинська А.О.		10.06		Літ.	Арк.	Аркушів
Керівник	Сфіменко А.А.		20.06.22	Проект підсистеми аутентифікації		4	105
Реценз.	Воротніков В.В.		20.06.22	користувачів корпоративної мережі на	ФІКТ, Гр. КІ-4		
Н. контр.	Сфіменко А.А.		20.06.22	базі моделі AAA та протоколу TACACS+			
Затверд.	Сфіменко А.А.		20.06.22				

ANNOTATION

The final qualifying work of the bachelor consists of an explanatory note, which has a total volume of 105 pages, 35 figures and 5 tables. The list of used literature includes 23 titles and is placed on 2 pages.

The purpose of the qualification work is to develop a subsystem for authentication of corporate network users based on the AAA model and the TACACS + protocol.

As a result of the bachelor's degree qualification, the main tasks for the development of user authentication system based on the AAA model and TACACS + protocol were identified, basic concepts and examples of protocol configuration were analyzed, network topology and addressing were developed, and a scheme was built and configured. An authorization, authentication and accounting system has been developed. The result of the work is tested and meets the requirements.

Keywords: AAA, TACACS+, NETWORK, SCHEME, ADDRESSING, TOPOLOGY, EIGHT, REDISTRIBUTION.

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ СИСТЕМ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ МЕРЕЖ	10
1.1 Модель AAA як основа сучасних систем аутентифікації	10
1.2 Аналіз функцій та безпеки протоколів моделі AAA.....	13
1.3 Аналіз сучасних серверних рішень на базі протоколу TACACS+	21
Висновки до першого розділу	23
РОЗДІЛ 2 РОЗРОБКА ПРОЕКТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ.....	24
2.1 Розробка загального проекту комп'ютерної мережі	24
2.2 Розробка схеми IP-адресації	29
2.3 Розробка проекту підсистеми аутентифікації на базі протоколу TACACS+ ..	32
Висновки до другого розділу.....	34
РОЗДІЛ 3 ВИБІР ОБЛАДНАННЯ, ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ МЕРЕЖІ ТА ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ.....	36
3.1 Вибір обладнання та програмного забезпечення для побудови мережі та її підсистеми аутентифікації	36
3.2 Налагодження обладнання мережі.....	38
3.3 Налаштування підсистеми аутентифікації на базі протоколу TACACS+	43
3.4 Тестування виконаних налаштувань	46
Висновки до третього розділу	50
ВИСНОВКИ.....	51
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	52
ДОДАТКИ.....	54

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІКС – Інформаційно-комунікаційна система

ЛКМ – Локальна комп'ютерна мережа

ГКМ – Глобальна комп'ютерна мережа

FE – Fast Ethernet

GE – Gigabit Ethernet

EIGR - Enhanced Interior Gateway Routing Protocol

RID – Router Identifier – Ідентифікатор маршрутизатора

IP – Internet Protocol

AAA – Accounting Authorization Audit

ACS – Access Control System

DES – Data Encryption Standard

PAP – Password Authentication Protocol

CHAP – Challenge Handshake Authentication Protocol

UDP – User Datagram Protocol

TCP – Transmission Control Protocol

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Основою сучасного життя є інформація, з якою ми зустрічаємося кожного дня. Інформація проникає у всі частинки людського життя і суспільства, а життя неможливе в інформаційному вакуумі. Все більше всі види людської роботи переходять до інформаційних технологій.

Мережева павутина охоплює світ і через декілька десятків років взагалі жодна людина не зможе уникнути цього простору і роботи в ньому. Все це утворює комп'ютерну мережу, що являє собою систему розподіленої обробки інформації, що складає як мінімум із двох комп'ютерів, взаємодіючих між собою за допомогою спеціальних засобів зв'язку. Або іншими словами мережа являє собою сукупність з'єднаних один з одним ПК і інших обчислювальних пристроїв, таких як принтери, факсимільні апарати й модеми. Мережа дає можливість окремим співробітникам організації взаємодіяти один з одним і звертатися до спільно використовуваних ресурсів; дозволяє їм одержувати доступ до даних, що зберігається на персональних комп'ютерах у видалених офісах, і встановлювати зв'язок з постачальниками.

Для того, щоб робота у мережі була безпечною використовується багато протоколів та способів захисту. Оскільки, у багатьох компаній щодня з'являються нові користувачі, тому краще розробляти глобальні мережі з необмеженою кількістю користувачів. А також важливо передбачати створення додаткових можливостей, які будуть необхідні для потреб користувачів.

Розробка підсистеми аутентифікації користувачів корпоративної мережі на базі моделі AAA та протоколу TACACS+ дозволяє побудувати структуровану, безпечну та адміністровану мережу, яка надасть змогу керувати правами користувачів, виконувати їх розмежування та контроль обліку процесів аутентифікації та авторизації.

Метою кваліфікаційної роботи є розробка підсистеми аутентифікації користувачів корпоративної мережі на базі моделі AAA та протоколу TACACS+.

Визначена мета обумовлює наступні завдання:

— Аналіз теоретичних основ моделі AAA, протоколів та реалізація безпеки;

		Русакинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

- Розробка мережі та її налаштування;
- Встановлення та налаштування серверу TascacsGui;
- Адміністрування мережі з використанням протоколу Tascacs+.

Об'єктом дослідження є процес побудови підсистеми аутентифікації користувачів мережі з використання моделі AAA та забезпечення їх безпеки.

Предметом дослідження є побудова підсистеми аутентифікації мережі на базі протоколу Tascacs+ та сервера TascacsGui.

У процесі виконання кваліфікаційної роботи було розроблено проект з використанням двох типів маршрутизації (статичної та динамічної) об'єднаних за допомогою редистрибуції та створена підсистема аутентифікації користувачів мережі на базі протоколу Tascacs+ та сервера TascacsGui .

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ СИСТЕМ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Модель AAA як основа сучасних систем аутентифікації

Налаштування безпеки мережі повинне забезпечувати можливість контролю доступу, а також розподілення різних прав в залежності від ролі користувача. Ці параметри складають політику мережевої безпеки. Для забезпечення використовують різні методи, протоколи з метою налаштування мережі. Незважаючи на розмір мережі варто завжди пам'ятати про необхідність налаштування параметрів безпеки для неї.

Для більш великих корпоративних організацій вимагається більш масштабоване рішення аутентифікації. Маршрутизатори та комутатори Cisco IOS можна налаштувати таким чином, щоб вони використовували AAA для аутентифікації в систему Cisco Secure Access Control System. Cisco ACS гарно масштабуються, тому що всі інфраструктурні пристрої мають доступ до центрального сервера. Дана система відрізняється відмовостійкістю, тому що дозволяє налаштовувати декілька серверів.

За замовчуванням пристрій Cisco IOS виконує автентифікацію на основі пароля лінії та авторизацію на основі пароля ввімкнення рівня 15. Це проблема для будь-якої організації, яка бажає деталізації або можливості відстежувати діяльність одного з кількох користувачів. Рішенням цього є AAA, аббревіатура від аутентифікації, авторизації та обліку. Це дозволяє адміністратору налаштувати детальний доступ і можливість аудиту до пристрою IOS.

Служби безпеки мережі AAA забезпечують базову інфраструктуру налаштування контролю доступу на мережевому пристрої. AAA дозволяє контролювати, кому дозволено доступ до мережі (authentication) і що дозволено робити (authorization), а також перевіряти дії при доступі до мережі (accounting).

Система мережевої та адміністративної безпеки AAA в середовищі Cisco має три функціональних компонента:

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

Аутентифікація – користувачі та адміністратори повинні довести, що вони – саме ті, за кого самі себе видають. Аутентифікація здійснюється за допомогою комбінації імені користувача та пароля, питань та відповідей, токен-карт та інше.

Авторизація – після аутентифікації користувача, служби авторизації визначають, яким користувачам ресурсу можна отримати доступ і які операції вони мають право виконувати.

Облік і аудит – система записує дії користувача, включаючи ресурси, якими від отримувач доступу, тривалість доступу до певного ресурсу та будь-які внесені зміни. Система обліку відстежує спосіб використання мережевих ресурсів.

В системі управління доступом Cisco Secure Access Control System (ACS) підтримуються два основних протокола, які використовуються в пристроях безпеки, маршрутизаторах і комутаторах для реалізації AAA: Tacacs+ та Radius.

Централізована безпека доступу до мережі AAA від Cisco надає багато переваг для організації та мережевого адміністратора, зокрема:

- підвищена гнучкість;
- підвищена безпека;
- масштабованість;
- стандартні методи аутентифікації;
- кілька систем резервного копіювання.

Підвищена гнучкість моделі AAA полягає в підтримці AAA авторизації, на додаток до аутентифікації, означає, що доступ можна підтримувати на основі «необхідності», тобто підтримувати кілька паролів. Підтримка обліку означає, що аудит користувачів і політика розподілу витрат можуть бути реалізовані та бути корисним для усунення проблем мережі.

Підвищена безпека моделі реалізується в тому що декілька пристроїв з однаковим іменем користувача/паролем, що керується локально, забезпечують низький рівень безпеки. Кожен, хто має доступ до всього, незалежно від потреби, також невиправдано збільшує ризик. Здається, що кілька локально адміністрованих паролів підвищують безпеку, але можуть призвести до того, що співробітники

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

будуть записувати паролі, якщо їх занадто багато, щоб їх запам'ятати. Ситуація посилилася б, якщо б були реалізовані складні паролі.

AAA з його централізованою базою даних безпеки та функціями авторизації дозволяє використовувати єдину безпечну комбінацію імені користувача та пароля для кожного співробітника, але при цьому дозволяє обмежувати доступ за принципом «потреба». У той же час AAA дозволяє швидко вирішити зламані паролі або видалення записів для звільнених співробітників.

Важливим моментом є масштабованість AAA — це шаблонний підхід до управління безпекою, який залишається надійним і гнучким, оскільки мережа стає більшою і складнішою. Завдяки централізації баз даних безпеки та підтримці авторизації AAA уникає керування багатьма комбінаціями імені користувача/пароля у зростаючому середовищі або альтернативної «слабкої» безпеки використання невеликої кількості комбінацій. Локально збережена автентифікація означає, що в будь-який момент, коли є ймовірність скомпрометованого імені користувача/паролю або звільнення співробітника, кожен пристрій має бути переналаштованим. Чим більше пристроїв існує, тим більше зусиль.

Стандартна модель AAA підтримує протоколи безпеки RADIUS, TACACS+ і Kerberos для захисту сеансів підключення. Ці протоколи забезпечують безпечну автентифікацію, включаючи зашифровані комунікації та взаємодію з системами безпеки мережевого сервера. Далі буде розглянуто кожний протокол більш детально.

З метою забезпечення безперервної роботи AAA підтримує кілька серверів безпеки в одній мережі (TACACS+), для забезпечення резервування в разі відмови пристрою або перевантаження каналів. Крім того, AAA дозволяє вказати кілька методів автентифікації, тому, якщо перший з них недоступний, можна використовувати другий або третій варіант. Наприклад, якщо вказаний сервер TACACS+ перебуває в автономному режимі, може використовуватися локально збережена база даних імен користувачів/паролів або навіть пароль увімкнення. Ці альтернативи мають бути визначені заздалегідь, інакше доступ може бути заблокований, доки не буде відновлено вказану службу.

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2 Аналіз функцій та безпеки протоколів моделі AAA

Модель AAA підтримує три протоколи безпеки для контролю комутованого доступу до мереж:

- Kerberos;
- RADIUS;
- TACACS+.

Cisco підтримує Kerberos як застарілий протокол безпеки для тих мереж, які вже підключені до нього. Сервер безпечного контролю доступу Cisco (ACS), реалізує лише TACACS+ і RADIUS.

На найбільш очевидному рівні кожен з цих трьох протоколів виконує те саме. Кожен із них забезпечує безпечний процес аутентифікації, який дозволяє віддаленим користувачам отримати доступ до мережевих ресурсів організації.

Розглянемо кожний з протоколів більш детально:

Kerberos отримав свою назву від триголового собаки, що охороняє ворота Аїда в грецькій міфології. Kerberos (протокол безпеки) — це система аутентифікації, розроблена в Массачусетському технологічному інституті (MIT), яка використовує криптографічний алгоритм стандарту шифрування даних (DES) для шифрування та аутентифікації. Kerberos ґрунтується на припущенні, що внутрішні користувачі за своєю природою не є більш надійними, ніж зовнішні користувачі, і застосовує безпеку та зашифровані комунікації для таких служб, як Telnet, для всіх користувачів.

Kerberos розроблено для того, щоб дозволити двом сторонам обмінюватися особистою інформацією через відкриту мережу, як-от Інтернет, призначаючи унікальний ключ, кожному користувачеві, який входить у мережу. Потім ключ вбудовується в повідомлення, щоб ідентифікувати відправника повідомлення. Kerberos заснований на концепції надійної третьої сторони, яка називається центром розподілу ключів (KDC), сервером аутентифікації Kerberos (AS), що виконує безпечну перевірку всіх користувачів і служб у мережі. Ця перевірка передбачає обмін зашифрованими повідомленнями аутентифікації без передачі пароля користувача.

		Русаїтинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

Протокол Kerberos в своїй роботі для забезпечення доступу користувача до мережі передбачає виконання наступних кроків

- 1) Віддалений користувач відкриває з'єднання PPP з маршрутизатором NAS організації.
- 2) Маршрутизатор запитує у користувача ім'я користувача та пароль.
- 3) Тоді маршрутизатор використовує лише ім'я користувача для запиту ключа або облікових даних, які підтверджують ідентичність користувача (TGT) від центру розподілу ключів (KDC).
- 4) Якщо припустити, що ім'я користувача відоме KDC, зашифрований TGT надсилається назад на маршрутизатор, який містить (серед іншого) ідентичність користувача. Термін дії ключа становить вісім годин, щоб зменшити ризик несанкціонованого захоплення та повторного відтворення.
- 5) Маршрутизатор використовує пароль з кроку 2, для розшифрування TGT. Після цього, якщо розшифровка успішна, віддалений користувач аутентифікується на маршрутизаторі та для нього надається доступ до мережі.
- 6) Коли віддалений користувач успішно аутентифікується на граничному маршрутизаторі, користувач і машина користувача стають частиною мережі. Інший TGT від KDC необхідний для доступу до мережеслужб, оскільки оригінальний TGT зберігається на маршрутизаторі і не використовується для додаткової аутентифікації, якщо користувач фізично не увійде на цей маршрутизатор.
- 7) Захист мережеслужби передбачає подвійне шифрування. Коли користувач запитує доступ до мережеслужби, наприклад, доступ до принтера або Telnet до хоста, KDC створює облікові дані служби. Ці облікові дані служби містять особу клієнта, ідентичність бажаної мережеслужби та обмеження часу. Облікові дані служби спочатку шифруються за допомогою пароля, наданого KDC і службою. Результат знову шифрується з використанням TGT користувача як ключа.

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

- 8) Цільова служба використовує TGT, наданий користувачем, для виконання першого дешифрування. Якщо результат можна успішно розшифрувати за допомогою пароля, наданого KDC і службою, значить, служба доступна.

Починаючи з Cisco IOS 11.2, організації, які вже використовують безпеку Kerberos 5, можуть використовувати свої існуючі сервери аутентифікації для автентифікації своїх маршрутизаторів і комутаторів. Можливості аутентифікації Kerberos програмного забезпечення IOS підтримують такі мережеві служби:

- Telnet;
- rlogin;
- rsh;
- rcp.

Вважається, що попередні програми були Kerberized, програми та служби, які були модифіковані для підтримки інфраструктури облікових даних Kerberos та зашифрованого зв'язку.

Служба віддаленої автентифікації Dial-In User Service (RADIUS) — це протокол автентифікації, авторизації та обліку сервера доступу, розроблений Livingston Enterprises, Inc., нині підрозділом Lucent Technologies. RADIUS — це система розподіленої безпеки, яка захищає віддалений доступ до мереж і мережевих служб від несанкціонованого доступу.

RADIUS — це повністю відкритий протокол, розповсюджений у форматі вихідного коду, який можна змінити для роботи з будь-якою системою безпеки, доступною на ринку. Численні реалізації коду сервера RADIUS є комерційно та вільно доступними. Сервери Cisco включають CiscoSecure ACS для Windows, CiscoSecure UNIX і Cisco Access Registrar. Кілька RFC IETF визначають протокол RADIUS, але наразі це все ще є запропонованим стандартом.

Реалізація RADIUS складається з трьох наступних компонентів:

- 1) Протокол з використанням UDP/IP зв'язку.
- 2) RADIUS-сервер — служба, що працює на центральному сервері Windows або UNIX, як правило, на сайті клієнта.

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				15
Змн.	Арк.	№ докум.	Підпис	Дата		

3) Клієнт RADIUS — служба, що знаходиться на серверах комутованого доступу, яка може бути поширена по всій мережі. Cisco додала підтримку клієнта RADIUS, починаючи з IOS версії 11.1.

Протокол RADIUS у своєму функціонуванні використовує модель сервер клієнт. Маршрутизатор NAS, на якому працює клієнтська служба RADIUS, передає інформацію про користувача визначеному серверу(ам) RADIUS, а потім діє на основі отриманої відповіді. Сервер RADIUS відповідає на всі запити на підключення користувача, аутентифікуючи користувача, а потім пересилаючи всю інформацію про конфігурацію, необхідну клієнту для надання послуги користувачеві. Сервери RADIUS можуть діяти як проксі-клієнти для інших типів серверів аутентифікації.

Після перевірки облікових даних сервер RADIUS відповідає клієнту однією з таких відповідей:

- прийняти – користувач пройшов автентифікацію;
- відхилити – користувач не автентифікований, і доступ заборонено. Користувачеві буде запропоновано повторно ввести ім'я користувача/пароль;
- виклик – запит на отримання додаткової інформації від користувача для підтвердження особи;
- змінити пароль – користувач повинен змінити свій пароль.

Технологія безпеки мережі полягає в тому, що клієнти та сервери RADIUS використовують спільну секретну технологію для всіх транзакцій аутентифікації. Спільний секретний ключ ніколи не надсилається по мережі. Щоб виключити можливість того, що хтось успішно перевірить пароль користувача в незахищеній мережі, будь-які передані паролі користувача надсилаються зашифрованими між клієнтом і RADIUS-сервером.

Одніє з переваг є гнучкість використання, оскільки сервер RADIUS підтримує різноманітні методи автентифікації користувача, включаючи PPP PAP або CHAP, MS-CHAP, логін UNIX та інші.

Інша сторона будь-якого відкритого стандарту полягає в тому, що він не

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

завжди гарантує взаємодію з реалізаціями інших виробників. Реалізації RADIUS у різних постачальників можуть відрізнятися, оскільки стандарт RADIUS спеціально дозволяє постачальникам пропонувати власні функції або атрибути в так званих парах AV. Якщо пристрій постачальника не розпізнає AV-пару, він ігнорує її. Щоб продемонструвати варіації, реалізація IETF підтримує атрибути, тоді як Ascend підтримує 254. Зараз Cisco підтримує 58 атрибутів у Cisco Secure ACS, серверах доступу, комутаторах Ethernet, брандмауерах PIX та концентраторах VPN 3000.

Контролер доступу до терміналів Access Control System Plus (TACACS+) — це протокол аутентифікації, який дозволяє NAS спілкуватися з сервером аутентифікації, щоб визначити, чи має користувач доступ до мережі.

TACACS+, новий протокол, розроблений Cisco, замінює два попередні галузеві стандарти: TACACS і XTACACS (система контролю доступу до розширеного термінального контролера доступу). TACACS+ несумісний із двома старішими протоколами. Cisco подала специфікацію протоколу TACACS+ у проекті RFC до IETF для розробки стандарту та для тих клієнтів, які зацікавлені в розробці власного програмного забезпечення TACACS+.

Серверні служби TACACS+ зберігаються в базі даних на демоні TACACS+, що працює на хості Windows 2000/NT або UNIX. Сервери Cisco, які підтримують TACACS+, включають CiscoSecure ACS для Windows, CiscoSecure UNIX і Cisco Access Registrar. Сервери доступу Cisco (Cisco Secure ACS) можуть реалізувати як TACACS+, так і RADIUS. Основна архітектура протоколу TACACS+ доповнює архітектуру AAA.

TACACS+ забезпечує окремі сервіси AAA. Відділення сервісів AAA забезпечує гнучкість реалізації, дозволяючи використовувати протокол TACACS+ для авторизації та урахування при цьому використання іншого методу аутентифікації.

Розширення протоколу TACACS+ дають додаткові типи запитів аутентифікації та коди відповідей відповідно до вихідної специфікації TACACS. TACACS+ забезпечує підтримку різноманітних протоколів, включаючи IP та застарілий протокол AppleTalk. В звичайних операціях TACACS+ для найбільшої

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

безпеки зв'язку шифрується все тіло пакету і використовується порт TCP 49.

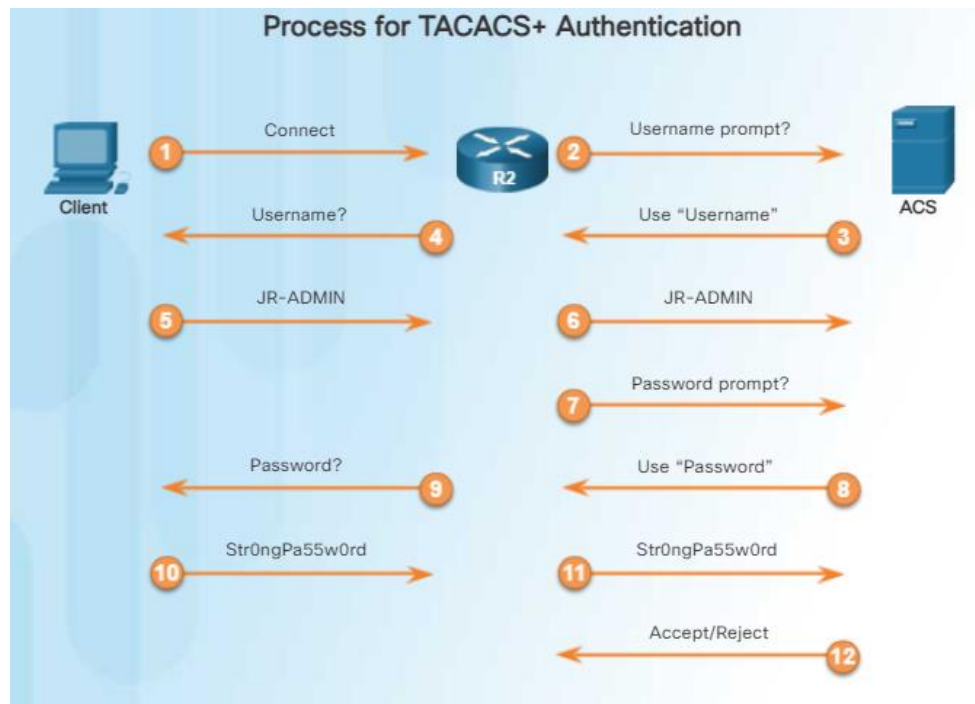


Рисунок 1.1 – Процес Тасас+ аутентифікації

Протокол TACACS+ використовується для зв'язку між клієнтами та серверами безпеки AAA.

Щоб налаштувати сервер TACACS+, необхідно глобально увімкнути AAA за допомогою команди `aaa new-model`. Далі скористатися командою `tacacs server name`. У режимі конфігурації сервера TACACS+ налаштувати IPv4-адресу сервера TACACS+ за допомогою команди `address ipv4`. Команда `address ipv4` дозволяє змінити порт аутентифікації та порт обліку.

Далі скористатися командою `single-connection`, щоб підвищити продуктивність TCP, підтримуючи єдине TCP-з'єднання протягом усього сеансу. В іншому випадку за замовчуванням TCP-з'єднання відкривається та закривається для кожного сеансу. Якщо потрібно, кілька серверів TACACS+ можна ідентифікувати, ввівши відповідні IPv4-адреси за допомогою команди `tacacs server name`.

Команда `key key` використовується для налаштування спільного секретного ключа для шифрування передачі даних між сервером TACACS+ і маршрутизатором з підтримкою AAA. Цей ключ має бути налаштований точно так само як на маршрутизаторі, так і на сервері TACACS+.

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

Коли сервери безпеки AAA ідентифіковані, вони повинні бути включені до списку методів команди аутентифікації AAA. Сервери AAA ідентифікуються за допомогою ключових слів group tacacs+.

Щоб налаштувати список методів для входу, за замовчуванням, для аутентифікації за допомогою сервера TACACS+ з локальною базою даних імен користувачів, необхідно вказати порядок за допомогою команди аутентифікації входу за замовчуванням.

Порівняння TACACS+ і RADIUS можна здійснити за такими параметрами, як список наведений нижче:

- аутентифікація та авторизація;
- UDP/TCP;
- виклик/відповідь;
- багатопроTOCOLна підтримка.

RADIUS поєднує служби аутентифікації та авторизації. Пакети доступу-прийняття, надіслані сервером RADIUS у відкритому тексті клієнту, містять інформацію про авторизацію.

TACACS+ повністю підтримує архітектуру AAA, розділяючи аутентифікацію, авторизацію та облік. Це дозволяє гнучко використовувати іншу службу, наприклад Kerberos, для аутентифікації, але при цьому використовувати TACACS+ для авторизації.

TACACS+ використовує TCP для орієнтованого на з'єднання транспортування між клієнтами та серверами. TCP-порт 49 зарезервований для TACACS+.

RADIUS використовує UDP для максимальної доставки, що вимагає визначення додаткових змінних, таких як спроби повторної передачі та тайм-аути для компенсації.

Підтвердження (TCP ACK) вказує на те, що запит було отримано протягом (приблизно) часу обертання мережі (RTT). Цей самий процес TCP використовує пакети RST (скидання), щоб забезпечити негайну індикацію невдалого (або автономного) сервера аутентифікації. UDP не може відрізнити несправний сервер, повільний сервер і неіснуючий сервер.

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

Пакети TCP Keepalive можна використовувати для спостереження за невдалими серверами та для швидкого перемикання збоїв між кількома підключеними серверами аутентифікації.

TCP краще масштабується та краще адаптується до зростаючих мереж.

RADIUS підтримує лише односпрямований виклик/відповідь від сервера RADIUS до клієнта RADIUS. TACACS+ підтримує двонаправлений виклик/відповідь, як CHAP, між двома NAS.

I TACACS+, і RADIUS підтримують протоколи інкапсуляції SLIP і PPP, але RADIUS не підтримує такі протоколи, які підтримуються TACACS+, що є значною перевагою:

- інтерфейс асинхронних служб Novell (NASI);
- підключення X.25 PAD;
- протокол керування Net BIOS Frame Protocol;
- протокол віддаленого доступу AppleTalk (ARAP).

RADIUS шифрує лише пароль у пакеті запиту доступу від клієнта до сервера, використовуючи хешування MD5 для безпеки. Інша частина пакета міститься у відкритому тексті, що відкриває таку інформацію, як ім'я користувача, авторизовані послуги та облікові дані, які слід відстежувати.

TACACS+ шифрує всю корисну інформацію пакету, залишаючи лише стандартний заголовок TACACS+ у відкритому тексті. Хоча тіло пакетів залишається незашифрованим для цілей налагодження, нормальна робота повністю шифрує тіло для більш безпечного зв'язку. Поле в заголовку вказує, чи зашифровано тіло.

RADIUS не підтримує обмеження доступу користувача до певних команд маршрутизатора як інструменту для керування маршрутизатором або служб терміналів.

TACACS+ підтримує два методи контролю авторизації команд маршрутизатора для кожного користувача або для групи.

Для узагальнення та виокремлення переваг та недоліків кожного з протоколів створено порівняльну таблицю (табл.1.1).

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 1.1 – Порівняльна таблиця протоколів

	TACACS+	RADIUS	Kerberos
Використання UDP	-	+	-
Використання TCP	+	-	+
Шифрування	Все крім заголовка	Лише пароль	Все крім заголовка
Підтримка мультипротоколів	+	-	-
Управління обліковим записом маршрутизатора	+	-	+
Управління авторизацією маршрутизатора	+	-	+
Підтримка LEAP	-	+	-
Підтримка XAUTH	+	+	+

Отже, в результаті порівняння вдалося виокремити переваги та недоліки кожного з протоколів. В результаті аналізу можна зробити висновки, що протокол TACACS+ більш надійний, оскільки використовує TCP, окрім цього TACACS+ забезпечує більший контроль команд авторизації та всі пакети AAA зашифровані на відміну від Radius, тому для створення підсистеми аутентифікації користувачів на підприємстві буде використано протокол TACACS+.

1.3 Аналіз сучасних серверних рішень на базі протоколу TACACS+

Протокол TACACS+ є пропрієтарним протоколом Cisco, тому основним сервером для реалізації протоколу є TACACS+ GUI. Основні можливості використання TacsacsGUI:

1) Вміє створювати конфігурацію для демона tacacs, це основна мета створення проекту. TacsacsGUI не просто створює конфігурацію, він спрощує налаштування tacacs – автоматичне шифрування паролів (tac_pwd вміє лише des), налаштування правил доступу для групи користувачів, попередній перегляд та міні-debug, на випадок помилок у конфігурації. На даний момент немає підтримки LDAP,

груп і ще деяких корисних додатків;

2) TacsacsGUI також оснащений деякими корисними утилітами, всі вони працюють з базою даних пристроїв, яка використовується для створення конфігураційного файлу tacsacs. Кожна утиліта має свого користувача, з певними правами доступу, за замовчуванням, користувачі вимкнені. Почнемо з першої утиліти – Backup Maker. Відразу з назви можна здогадатися, навіщо призначена ця утиліта. Слід зазначити, що вона працює виключно з Cisco пристроями (як і всі інші утиліти). Backup Maker створює резервне копіювання з періодичним налаштуванням, на обладнанні виконується команда `copy startup-config tftp:`, при цьому є можливість зберегти конфігурацію перед резервним копіюванням. На жаль, поки що TFTP-сервером має виступати сам сервер TacsacsGUI, який збирає всі бекапи у зручну базу даних (IMXO);

3) Subnet Searcher — ще одна утиліта, яка допомагає визначити налаштовані підмережі на пристроях, також є можливість визначення номеру Vlan для підмережі. Subnet Searcher заходить на пристрій та виконує команду `show runn | in (rface|dress|encap)`, ґрунтуючись на інформації про ір адресу та маску підмережі (secondary ір так само враховуються) обчислюється номер підмережі, якщо інтерфейс називається Vlan або є рядок encapsulation, то визначається vlan. В результаті, отримується база даних відомих підмереж у мережі + номер Vlan (якщо був помічений) + для кожної підмережі є список учасників;

4) CDP MapMaker — утиліта, яка будує топологію мережі, базуючись на інформації, отриманій від CDP. Ця утиліта використовує ту ж саму JavaScript бібліотеку (jsPlumb), що і UNetLab. Насправді ця утиліта ділиться на два «движки»: CDP Search та MapMaker. CDP Search збирає інформацію з усіх пристроїв та створює тимчасову базу даних, яку надалі використовує MapMaker. Крім автоматичного створення топології, існує можливість ручного додавання елементів мережі та встановлення зв'язків. Також є експорт, але тільки в XML файл, який можна відкрити за допомогою сервісу draw.io;

5) Є можливість створення користувачів для керування TacsacsGUI поки що без розмежування прав доступу. Ведеться логування дій користувача та спроб

		Русакинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

несанкціонованого доступу. Також можна робити резервну копію всіх налаштувань, файлу конфігурації tacacs і всіх резервних копій, зроблених за допомогою Backup Maker, при цьому є вибір куди (FTP, SCP, Win Share) і коли видаляти backup;

б) Звичайно інформація, яка зберігається на цьому сервері, повинна передаватися між користувачем і сервером по https. Щоб https був коректно налаштованим та відповідно позначався "зеленим" кольором, треба зробити DNS запис для сервера - tacacs.gui і встановити кореневий сертифікат.

Висновки до першого розділу

У першому розділі було виконано аналіз моделі AAA, як основи сучасних систем аутентифікації, розглянуто основні функції та рішення безпеки. Розроблені основні завдання роботи. Проаналізовано теоретичні основи моделі та протоколи AAA, а саме TACACS+, RADIUS та Kerberos. Виокремлено переваги та недоліки кожного з них та дійдено до висновку що протокол TACACS+ більш надійний, оскільки використовує TCP, окрім цього TACACS+ забезпечує більший контроль команд авторизації та всі пакети AAA зашифровані на відміну від Radius, тому для створення підсистеми аутентифікації користувачів на підприємстві буде використано протокол TACACS+. Всі налаштування будуть побудовані на базі сервера TacacsGui, оскільки він вміє створювати конфігурацію, підтримує додаткові утиліти, простий та доступний у використанні.

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				23
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 РОЗРОБКА ПРОЕКТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

2.1 Розробка загального проекту комп'ютерної мережі

Будь-яке проектування, як відомо являє собою моделювання з певним ступенем спрощення. Саме тому, щоб передбачити всі можливі фактори, врахувати всі потреби, які можуть виникнути в майбутньому, виконується попередній розрахунок необхідних параметрів та проектування відповідно них.

При проектування мережі необхідно враховувати:

- необхідний розмір мережі;
- необхідну структуру, ієрархію і основні частини;
- основні напрями та інтенсивність використання;
- вимоги до програмних засобів.

І це ще не весь список необхідних параметрів. Під структурою мережі розуміється спосіб поділу мережі на частини, а також спосіб сполучення цих сегментів між собою. Мережа може містити робочі групи комп'ютерів, мережі підрозділів, опорні мережі, засоби зв'язку з іншими мережами. В ідеалі структура мережі має відповідати структурі будинку або комплексу будинків.

Під час проектування та вибору топології власної мережі було використано трирівнева ієрарічна модель мережі, що складається з рівня ядра, рівня розподілу та рівня доступу. Модель даної ієрархії відображена на рис.2.1.

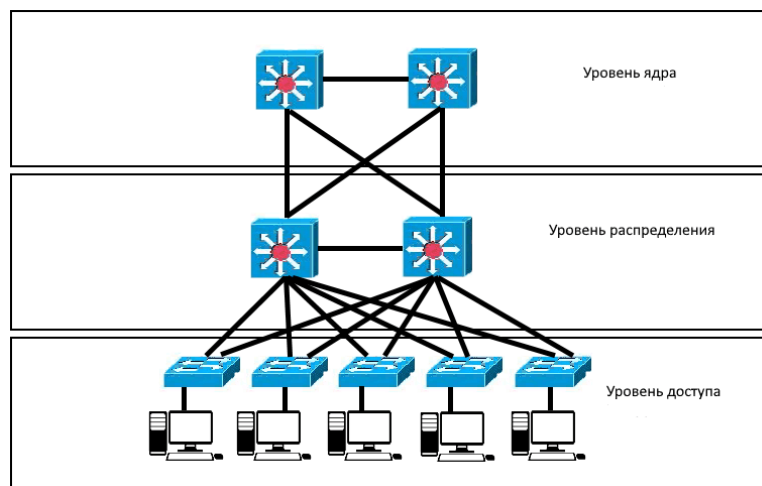


Рисунок 2.1 - Трирівнева ієрархічна модель мережі

		Русаїтинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				24
Змн.	Арк.	№ докум.	Підпис	Дата		

Відповідно до рис.2.1 була створена власна модель мережі, яка відображена на рис.2.2. Дана модель мережі містить в собі дві підмережі двох компаній, в першій використовується статична маршрутизація (плаваюча), в іншій динамічна (EIGRP), також схема має два ядра, які з'єднані між собою, та налаштовані за допомогою редистрибуції.

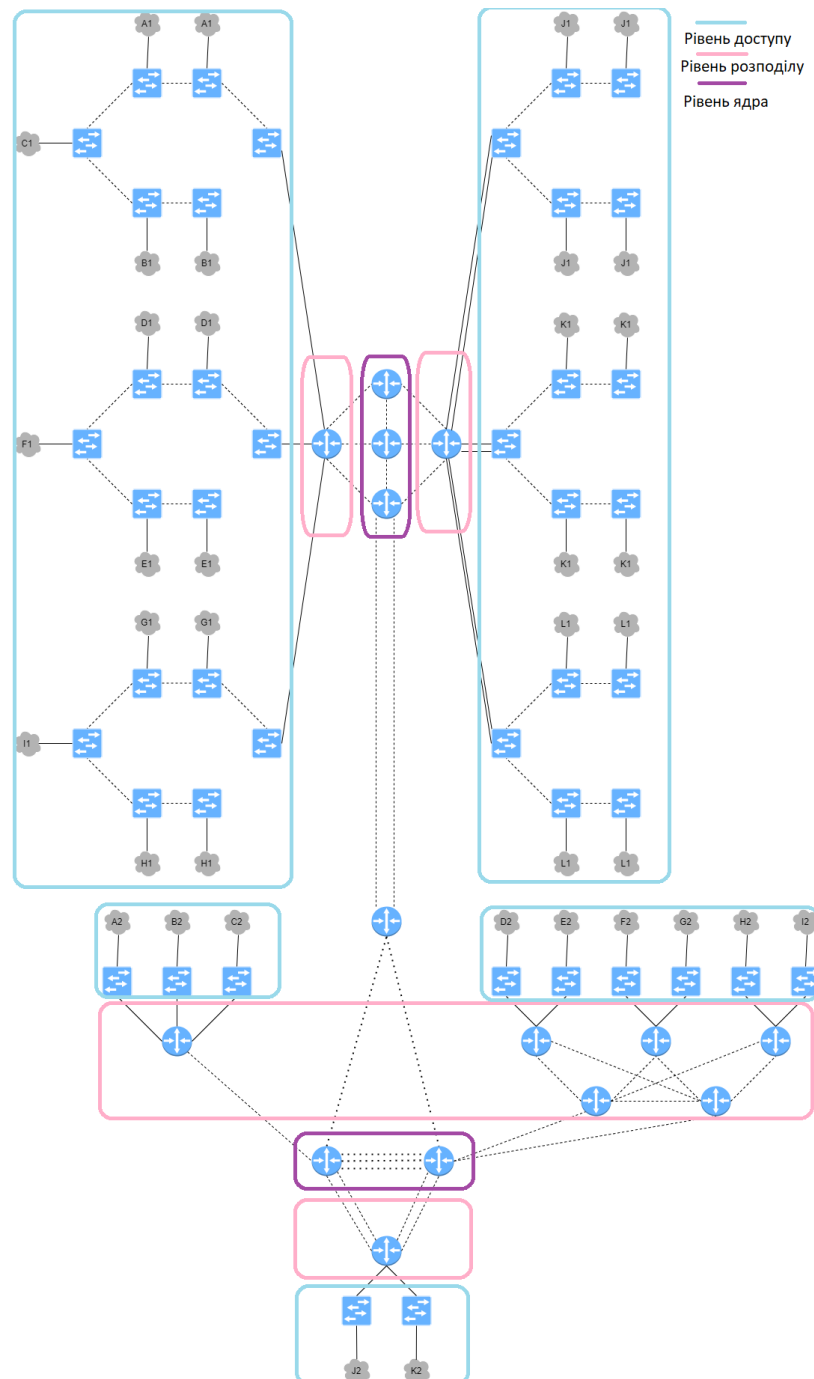


Рисунок 2.2 - Проект корпоративної мережі

Розпочнемо розбір корпоративної мережі по частинам. Спершу розглянемо першу частину, що відображена рис.2.3.

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				25
Змн.	Арк.	№ докум.	Підпис	Дата		

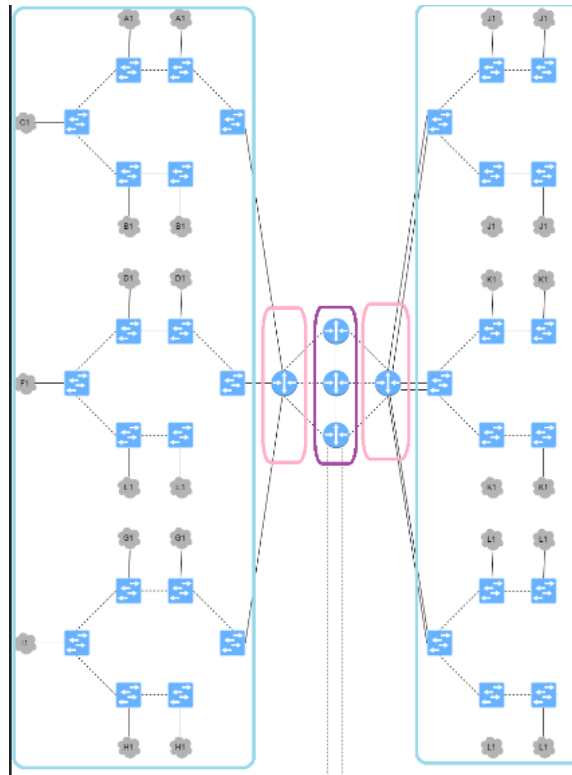


Рисунок 2.3 - Проект першої частини мережі

Перша частина мережі складається з 5 маршрутизаторів, 3 з яких складають рівень ядра, а 2 – рівень розподілу. Взагалом на рівні доступу використовується 36 комутаторів, а також 12 окремих мереж. Маршрутизатори з'єднані між собою за допомогою витії пари Gigabit Ethernet. Всі решта елементів мережі з'єднані між собою за допомогою витії пари Ethernet.

Наступною на рис.2.4 відображений проект другої частини загальної мережі.

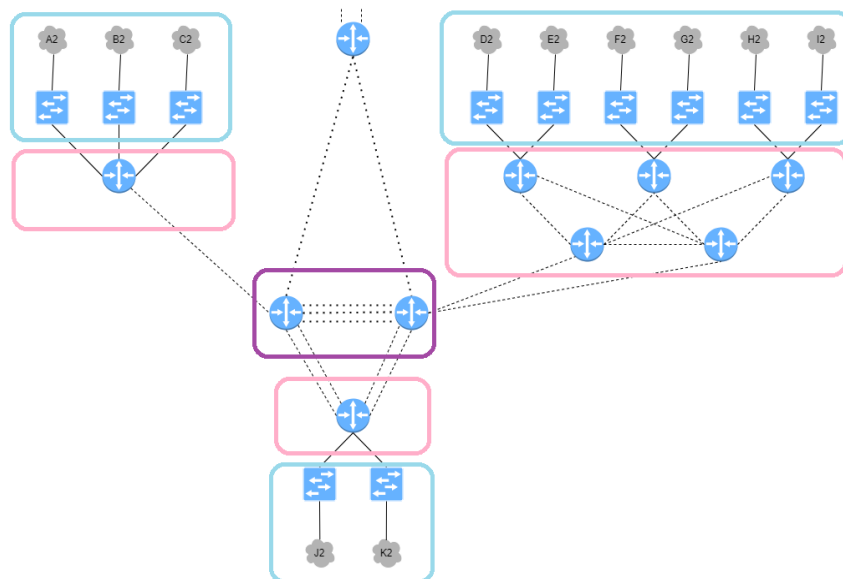


Рисунок 2.4 - Проект другої частини мережі

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

Друга частина мережі складається з 9 маршрутизаторів, 2 з яких складаються рівень ядра, а 7 – рівень розподілу. Взагалом на рівні доступу використовується 11 комутаторів, а також 11 окремих мереж. Маршрутизатори з'єднані між собою за допомогою витії пари Gigabit Ethernet. Всі решта елементів мережі з'єднані між собою за допомогою витії пари Ethernet.

Детально розглянемо деякі частини підмереж.

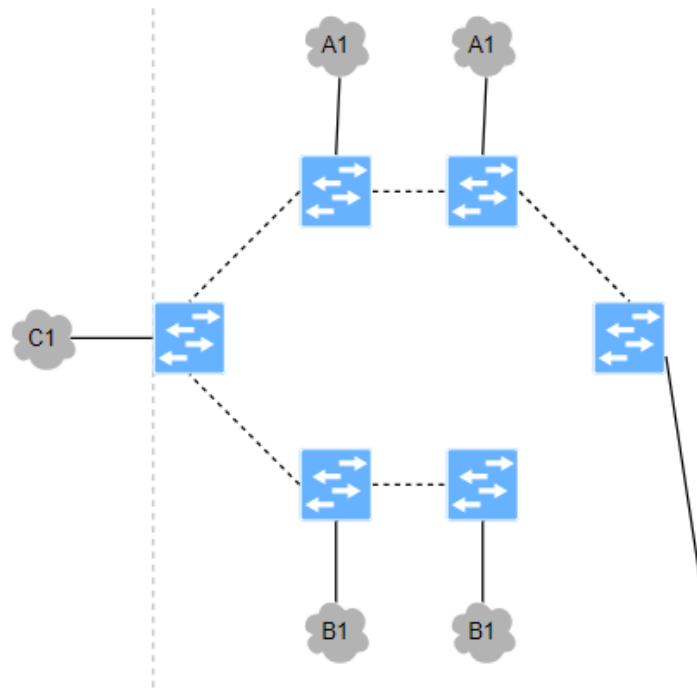


Рисунок 2.5 - Частина 1 першої підмережі

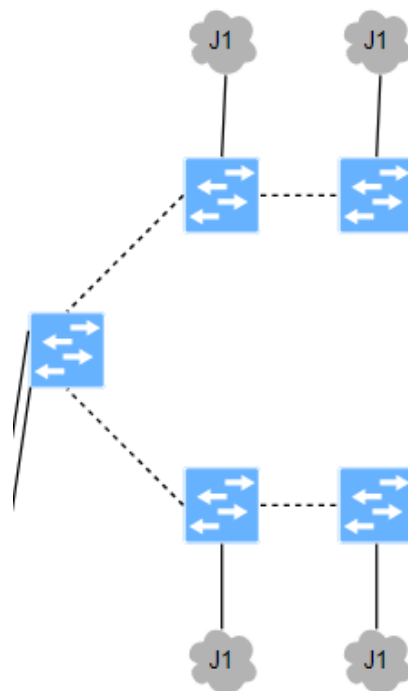


Рисунок 2.6 - Частина 2 першої підмережі

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				27
Змн.	Арк.	№ докум.	Підпис	Дата		

Перша підмережа всієї мережі складається з трьох складових що відображені на рис.2.5, а також трьох, що відображені на рис.2.6. Дві частини складаються з 6 комутаторів, які з'єднані між собою за допомогою виті пари Ethernet, відрізняються лише способом з'єднання між собою комутаторів, перша містить в собі 3 мережі, а наступна 1 відповідно.

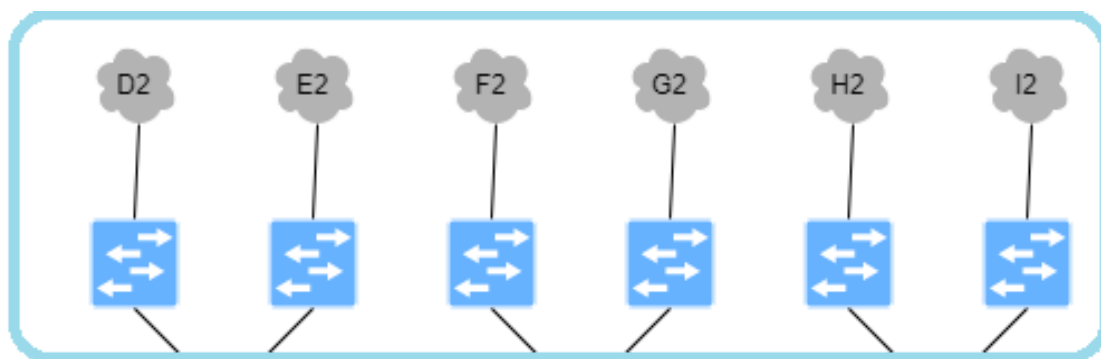


Рисунок 2.7 - Частина другої підмережі

На рис.2.7 відображено підмережу, що складається з 6 комутаторів, що з'єднані між собою за допомогою виті пари Ethernet, а також 6 мереж. Аналогічним чином виконано побудована вся друга частина мережі.

Для детального опису кожної з мереж виконаємо побудову узагальнюючої таблиці (табл.2.1)

Таблиця 2.1 - Узагальнююча таблиця моделі мережі

Мережа	Кількість робочих станцій	Кількість серверів	Кількість комутаторів	Підключення до маршрутизатора
1	2	3	4	5
A1	60	2	2	R_4_20_1
B1	64	0	2	R_4_20_1
C1	40	0	1	R_4_20_1
D1	60	2	2	R_4_20_1
E1	64	0	2	R_4_20_1
F1	40	0	1	R_4_20_1
G1	60	2	2	R_4_20_1
H1	64	0	2	R_4_20_1

1	2	3	4	5
I1	40	0	1	R_4_20_1
J1	150	2	5	R_4_20_2
K1	150	2	5	R_4_20_2
L1	150	2	5	R_4_20_2
A2	40	0	1	R_4_20_6
B2	40	0	1	R_4_20_6
C2	40	0	1	R_4_20_6
D2	40	0	1	R_4_20_7
E2	40	0	1	R_4_20_7
F2	40	0	1	R_4_20_7
G2	40	0	1	R_4_20_7
H2	40	0	1	R_4_20_7
I2	40	0	1	R_4_20_7
J2	0	40	1	R_4_20_8
K2	0	40	1	R_4_20_8

Отже, після побудови та розрахунку відповідної кількості елементів та моделей мережі, можна переходити до розрахунку адресації мережі.

2.2 Розробка схеми IP-адресації

Адресація мережі може бути реалізована класова та безкласова, в кожній з них є свої переваги та недоліки. Оскільки мережа є досить об'ємною і складається з підмереж, то в такому випадку варто перехід від класової до безкласової адресації – адже у цьому випадку клас мережі дещо втрачає свій зміст, оскільки за ним вже не можна визначити, яка частина IP-адреси відповідає за номер вузла, а яка – за номер мережі. При використанні підмереж і безкласової адресації наявність маски є обов'язковою, оскільки лише з її допомогою можна визначити, до якої мережі належить вузол.

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

Підмережі створюються за рахунок запозичення біт з поля номера вузла адреси певного класу. Враховуючи, що у кожній підмережі повинно бути 2 зарезервовані адреси (адреса мережі та ширококомовна адреса, як і у класовій адресації), можна визначити мінімальну та максимальну кількість біт, які можна запозичити: $N_{\min}=2$, на основі чого можна створити 2 підмережі (рахується за тією ж формулою, що і кількість вузлів у мережі); $N_{\max}=n-2$ (повинно залишитися достатня кількість біт для адресації щонайменше 2-х вузлів, враховуючи 2 зарезервовані адреси). Адреса підмережі та ширококомовна адреса визначаються за тими ж правилами, що і для класових мереж; правила використання маски теж однакові. Але при записі маски слід враховувати, що у ній в 1 виставляються не лише ті біти, які належать номеру мережі, а і ті, які належать номеру підмережі. За допомогою використання безкласової адресації є можливість економити IP-адресний простір.

Спершу виконаємо побудову узагальнюючої таблиці по-кількості вузлів в мережі, а також враховуючи запас адресації в разі збільшення мережі, або для потреб адміністратора.

Таблиця 2.2 - Розподіл вузлів по мережам

Мережа	Кількість вузлів	Загальна кількість вузлів з запасом
1	2	3
A1	62	70
B1	64	70
C1	40	45
D1	62	70
E1	64	70
F1	40	45
G1	62	70
H1	64	70
I1	40	45
J1	152	160
K1	152	160

1	2	3
L1	152	160
A2	40	45
B2	40	45
C2	40	45
D2	40	45
E2	40	45
F2	40	45
G2	40	45
H2	40	45
I2	40	45
J2	45	45
K2	45	45

Окрім наведених у заданій таблиці пристроїв і відповідних мереж, необхідно також врахувати мережі, які сполучають маршрутизатори між собою.

AA1 – R_4_20_1 – R_4_20_3: 2 вузла мережі;

BB1 – R_4_20_1 – R_4_20_4: 2 вузла мережі;

CC1 – R_4_20_1 – R_4_20_5: 2 вузла мережі;

DD1 – R_4_20_3 – R_4_20_2: 2 вузла мережі;

EE1 – R_4_20_3 – R_4_20_4: 2 вузла мережі;

FF1 – R_4_20_4 – R_4_20_2: 2 вузла мережі;

GG1 – R_4_20_4 – R_4_20_5: 2 вузла мережі;

HH1 – R_4_20_2 – R_4_20_5: 2 вузла мережі;

Додаткові мережі: II1, JJ1, KK1.

AA2 – R_4_20_6 – R_4_20_7: 2 вузла мережі;

BB2 – R_4_20_7 – R_4_20_8: 2 вузла мережі;

CC2 – R_4_20_7 – R_4_20_9: 2 вузла мережі;

DD2 – R_4_20_8 – R_4_20_9: 2 вузла мережі;

		Русаїтинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

EE2 – R_4_20_13 – R_4_20_14: 2 вузла мережі;
 FF2 – R_4_20_7 – R_4_20_13: 2 вузла мережі;
 GG2 – R_4_20_7 – R_4_20_14: 2 вузла мережі;
 HH2 – R_4_20_10 – R_4_20_13: 2 вузла мережі;
 II2 – R_4_20_10 – R_4_20_14: 2 вузла мережі;
 JJ2 – R_4_20_11 – R_4_20_13: 2 вузла мережі;
 KK2 – R_4_20_11 – R_4_20_14: 2 вузла мережі;
 LL2 – R_4_20_12 – R_4_20_13: 2 вузла мережі;
 MM2 – R_4_20_12 – R_4_20_14: 2 вузла мережі;
 Додаткові мережі: NN2, OO2, PP2.

На основі цих даних, виконаємо розподіл підмереж. Результат виконання поділу першої мережі відображений у (Додатку А), а другої - у (Додатку Б).

Отже, в результаті поділу вдалося знайти оптимальні префікси для мереж:

Мережа №1: оптимальний префікс - /21, обрана IP-мережа: 201.128.0.0

Мережа №2: оптимальний префікс - /22, обрана IP-мережа: 202.128.0.0

Після обрання оптимальних префіксів, та вибору IP-мереж було проведено розрахунок адресації, для першої мережі наведений у (Додатку В, Г, Е), а для другої – у (Додатку Г, Д, Є).

2.3 Розробка проекту підсистеми аутентифікації на базі протоколу TACACS+

Для кожної мережі важливо виконати коректний розподіл прав доступу, адже від цього залежить безпека всієї системи. Саме для розмежування буде створено поділ всіх користувачів на основні групи, а також призначення відповідних прав для кожної групи. Розмежування буде відбуватися за таким принципом:

- Головний адміністратор
- Група адміністраторів
- Група менеджерів
- Група користувачів

Для кожної з наведених груп відповідно будуть розмежовані права доступу.

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				32
Змн.	Арк.	№ докум.	Підпис	Дата		

Але спершу необхідно розподілити всіх користувачів по відповідним групам. Поділ наведений у табл.2.3.

Таблиця 2.3 - Розподіл користувачів по групам

Група	Користувач
mainadmin	mainadmin (Cisco123)
admin	admin1 (Cisco123)
	admin2 (Cisco123)
	admin3 (Cisco123)
manager	manager1 (Cisco123)
	manager2 (Cisco123)
user	user1 (Cisco123)
	user2 (Cisco123)
	user3 (Cisco123)
	user4 (Cisco123)

Наступним кроком є розподіл прав та можливостей для кожної групи користувачів.

Таблиця 2.4 - Розподіл прав для кожної групи

Група користувачів	Права													
	conf t	show	interface	line vty	line console	line aux	ip addr	shutdown	copy run-con st-con	ping	hostname	маршрутизація	редистрибуція	all
mainadmin	+	+	+	+	+	+	+	+	+	+	+	+	+	+
admin	+	+/-	+	+	+	+	+	+	+	+	+	+	+	-
manager	+	+/-	+	-	-	-	+	+	+	+	+	-	-	-
user	+	+/-	+	-	-	-	-	+	+	+	+	-	-	-

З табл.2.4 можна зробити висновки, що для головного адміністратора дозволений повний доступний, адміністраторам менший, менеджерам та користувачам дозволені лише певні команди, що наведені у таблиці.

Окрім цього, також буде проведено налаштування Accounting, тобто обліку входу та виходу користувача, а також виконання обліку всіх команд, що використовує кожний користувач. Дані налаштування можна виконати застосувавши певні команди.

1) Налаштування сервера TACACS.

```
aaa authentication-server tacacs <ім'я_сервера>  
хост <IP_адреса>  
ключ <спільний_секрет>
```

2) Налаштування групи для серверів TACACS.

```
aaa server-group <ім'я_групи_сервера>  
auth-server <name_of_tacacs_server>
```

3) Увімкнення обліку TACACS.

```
aaa accounting command <priv-lvl> start-end default group tacacs+
```

В результаті даних налаштувань буде виконуватися облік в log file.

Для забезпечення доступу до пристроїв буде налаштований ssh – мережевий протокол прикладного рівня, що дозволяє виконувати віддалене управління операційними системами, а також пристроями. На відміну від telnet шифрує весь трафік, включаючи і паролі, які передаються.

Висновки до другого розділу

В результаті виконання другого розділу вдалося обрати топологію мережі, розглянути основні вузли та побудувати мережу в цілому. Після цього було проведено розподіл підмереж на основі цих даних. В результаті поділу вдалося знайти оптимальні префікси для мереж: мережа №1: оптимальний префікс - /21, обрана IP-мережа: 201.128.0.0; мережа №2: оптимальний префікс - /22, обрана IP-мережа: 202.128.0.0. Після вибору оптимальних префіксів, та вибору IP-мереж було проведено розрахунок адресації для мереж. Також було обрано обладнання мережі,

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

виокремлено переваги та недоліки кожної категорії пристроїв мережі. В результаті аналізу для побудови мережі були обрані такі пристрої: маршрутизатор C7200VXR та стандартний комутатор, оскільки образи цих пристроїв наявні в GNS. Для реалізації системи аутентифікації користувачів було обрано Tacsacs server with GUI. Також розроблено групи користувачів та розподілені відповідні права між ними, наведені основні команди для налаштування обліку всіх дій користувачів на пристроях.

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 ВИБІР ОБЛАДНАННЯ, ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ МЕРЕЖІ ТА ПІДСИСТЕМИ АУТЕНТИФІКАЦІЇ

3.1 Вибір обладнання та програмного забезпечення для побудови мережі та її підсистеми аутентифікації

Мережеве обладнання являє собою пристрої, які необхідні для функціонування мережі. Тому вибір апаратного забезпечення це важлива складова розробки мережі. Оскільки, обраний пристрій повинен виконувати всі необхідні функції, що були розроблені та спланові перед побудовою мережі.

При виборі маршрутизатора важливими параметрами, стало те що він повинен підтримувати досить велику кількість підключених пристроїв, функціонувати досить швидко, адже з нього в майбутньому складатиметься не лише рівень розподілу, а ще й рівень ядра.

На рівні розподілу від маршрутизатора вимагались такі основні параметри, як підтримка технології Ethernet та FastEthernet. Можливість підключення підключення до 8 портів. Підтримка протоколу маршрутизації EIGRP, статичної IPv4 маршрутизації, а також підтримка редистрибуції мережа, окрім цього важливими параметрами стало те, що він повинен підтримувати агрегування та транкування каналів, а також протоколи для реалізації моделі AAA.

В результаті пошуку за вказаними параметрами, вдалося підібрати маршрутизатор моделі Cisco ISR4331/K9. Він відноситься до серії маршрутизаторів 4000, що включають в себе моделі Cisco ISR4300 і Cisco ISR4400. Ці пристрої відрізняються в порівнянні з іншими високою швидкістю від 50 Мбіт/с до 2 Гбіт/с, вбудованими WAN портами Ethernet і SPF портами. Окрім наведених параметрів він підтримує всі протоколи маршрутизації та методи каналів, які необхідні для коректного функціонування і не лише.

Тому в подальшому, якщо буде необхідність налагодження або додавання певних протоколів чи параметрів даний маршрутизатор надасть цю можливість. Оскільки вибір був зупинено на моделі Cisco ISR4331/K9, тому було розглянуто

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				36
Змн.	Арк.	№ докум.	Підпис	Дата		

технічні характеристики, що наведені у додатку Ж, а також загальний вигляд представлений на рис.3.1.



Рисунок 3.1 - Маршрутизатор Cisco ISR4331/K9

Наведена модель маршрутизатора досить практична у використанні та універсальна.

Наступним не менш важливим елементом мережі є комутатор. Комутатори містяться на рівні розподілу. У створеній мережі не передбачено налаштування безпроводних зв'язків, тому комутатор необхідно було обрати з досить великою кількістю портів. А також щоб підтримував функції, що необхідні для налаштування схеми.

Оптимальним варіантом було знайдено комутатор моделі WS-C2960+24TC-L. Він являє собою лінійний комутатор з фіксованою конфігурацією та портами Fast Ethernet та Gigabit Ethernet, підтримує розширення LAN. Дозволяє підключити достатню кількість мереж, підтримує агрегування та транкування каналів мережі. Також комутатори даної моделі підтримують передачу голосу, даних та відео, а також безпечний доступ. Можна виконувати масштабування відповідно до необхідно створеної мережі. Окрім цього можна додавати резервні джерела живлення мережі. Детальна технічна характеристика описана у додатку И та продемонстрована на рис.3.2.

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				37
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 3.2 - Комутатор Cisco

Для реалізації побудови системи аутентифікації користувачів на базі протоколу Tacsacs+ та моделі AAA буде використовуватися Tacsacs+ server with GUI, який надає можливість створення користувачів, груп користувачів, додавання пристроїв, а також об'єднання їх за допомогою груп, налаштування рівня привілеїв, а також дозволи та заборони на виконання певних типів команд.

3.2 Налагодження обладнання мережі

Базове налагодження мережі передбачає налагодження фізичних інтерфейсів мережі, налагодження параметрів адресації, налагодження протоколів маршрутизації, налагодження віддаленого доступу SSH. Це налагодження здійснюється за відповідними сценарями. Сценарій налагодження ір-адресації наведений на рис.3.3, а результат наведений в 3.3 пункті.

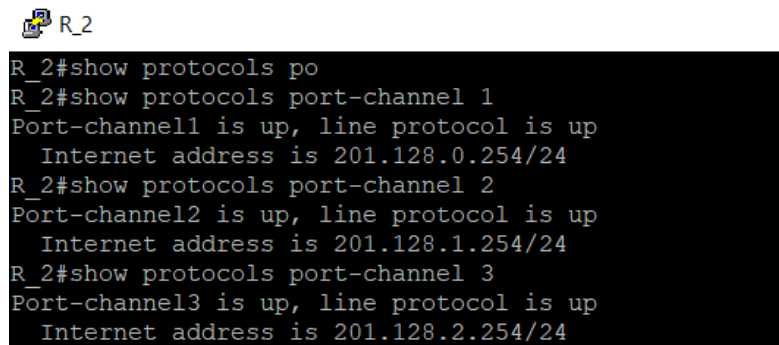
```

R_13
R_13#show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 202.128.2.222/30
FastEthernet0/1 is up, line protocol is up
  Internet address is 202.128.2.230/30
FastEthernet1/0 is up, line protocol is up
  Internet address is 202.128.2.238/30
FastEthernet1/1 is up, line protocol is up
  Internet address is 202.128.2.209/30
FastEthernet2/0 is up, line protocol is up
  Internet address is 202.128.2.213/30
FastEthernet2/1 is administratively down, line protocol is down
FastEthernet3/0 is administratively down, line protocol is down
FastEthernet3/1 is administratively down, line protocol is down
FastEthernet4/0 is administratively down, line protocol is down
FastEthernet4/1 is administratively down, line protocol is down
GigabitEthernet5/0 is administratively down, line protocol is down
GigabitEthernet6/0 is administratively down, line protocol is down
  
```

Рисунок 3.3 – Налаштування ір-адресації

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

На рис.3.4 відображено результат налаштування агрегованих каналів на маршрутизаторі R_2.

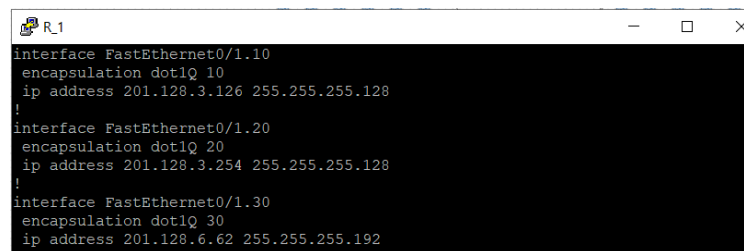


```

R_2#show protocols po
R_2#show protocols port-channel 1
Port-channel1 is up, line protocol is up
Internet address is 201.128.0.254/24
R_2#show protocols port-channel 2
Port-channel2 is up, line protocol is up
Internet address is 201.128.1.254/24
R_2#show protocols port-channel 3
Port-channel3 is up, line protocol is up
Internet address is 201.128.2.254/24
  
```

Рисунок 3.4 - Результат налаштування агрегації каналів

На рис.3.5 відображено результат налаштування транкових каналів на маршрутизаторі R_1.

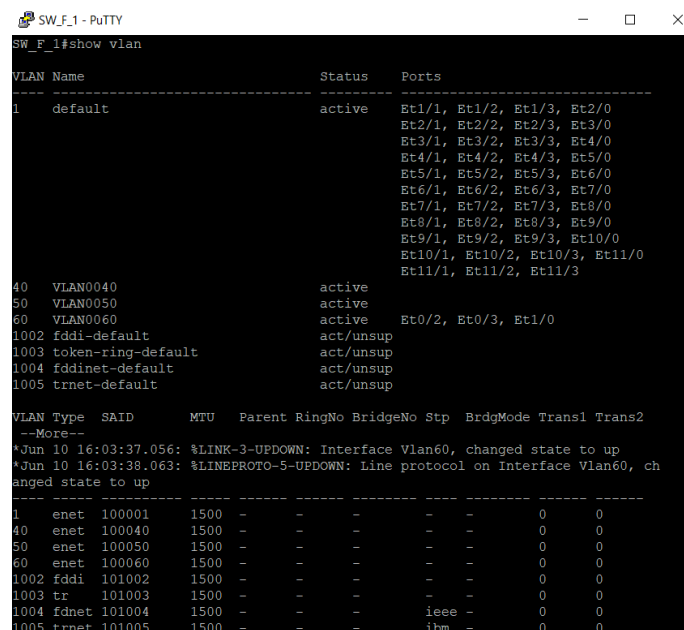


```

interface FastEthernet0/1.10
encapsulation dot1Q 10
ip address 201.128.3.126 255.255.255.128
!
interface FastEthernet0/1.20
encapsulation dot1Q 20
ip address 201.128.3.254 255.255.255.128
!
interface FastEthernet0/1.30
encapsulation dot1Q 30
ip address 201.128.6.62 255.255.255.192
  
```

Рисунок 3.5 - Результат налаштування транкових каналів

На рис.3.6 відображено результат налаштування інтерфейсів VLAN на комутаторі SW_F_1.



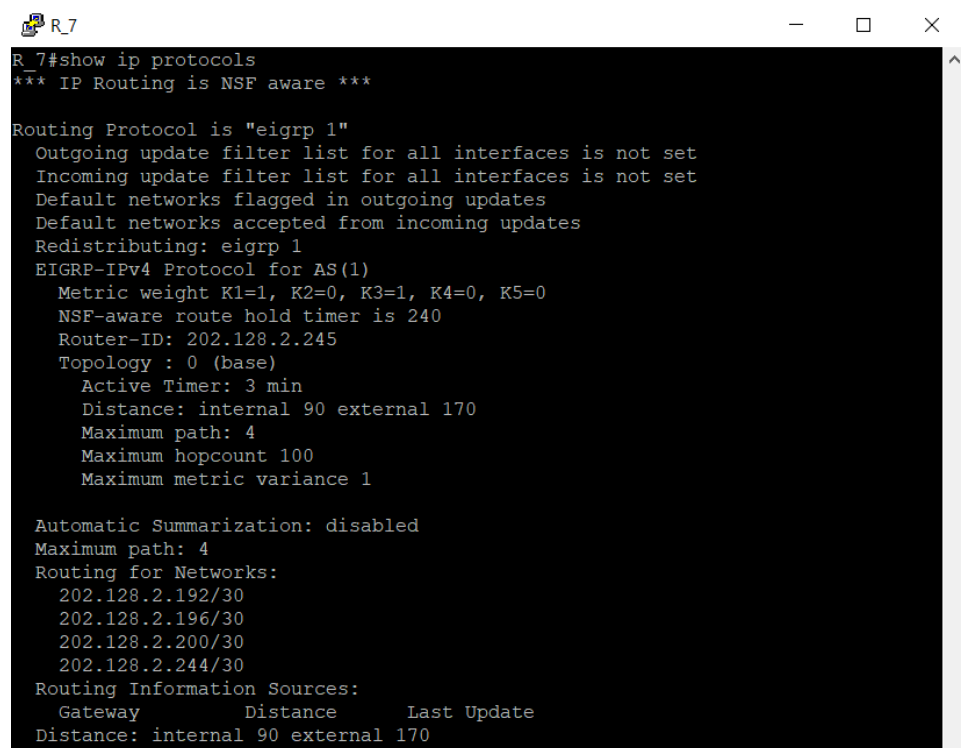
```

SW_F_1#show vlan
VLAN Name                Status    Ports
-----
1    default                active    Et1/1, Et1/2, Et1/3, Et2/0
                                           Et2/1, Et2/2, Et2/3, Et3/0
                                           Et3/1, Et3/2, Et3/3, Et4/0
                                           Et4/1, Et4/2, Et4/3, Et5/0
                                           Et5/1, Et5/2, Et5/3, Et6/0
                                           Et6/1, Et6/2, Et6/3, Et7/0
                                           Et7/1, Et7/2, Et7/3, Et8/0
                                           Et8/1, Et8/2, Et8/3, Et9/0
                                           Et9/1, Et9/2, Et9/3, Et10/0
                                           Et10/1, Et10/2, Et10/3, Et11/0
                                           Et11/1, Et11/2, Et11/3
40   VLAN0040                active
50   VLAN0050                active
60   VLAN0060                active    Et0/2, Et0/3, Et1/0
1002 fddi-default          act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default       act/unsup
1005 trnet-default         act/unsup

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp    BrdgMode Trans1 Trans2
--More--
*Jun 10 16:03:37.056: %LINK-3-UPDOWN: Interface Vlan60, changed state to up
*Jun 10 16:03:38.063: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan60, changed state to up
1    enet  100001  1500   -      -      -      -      -      0      0
40   enet  100040  1500   -      -      -      -      -      0      0
50   enet  100050  1500   -      -      -      -      -      0      0
60   enet  100060  1500   -      -      -      -      -      0      0
1002 fddi  101002  1500   -      -      -      -      -      0      0
1003 tr    101003  1500   -      -      -      -      -      0      0
1004 fdnet 101004  1500   -      -      -      -      -      0      0
1005 trnet 101005  1500   -      -      -      -      -      0      0
  
```

Рисунок 3.6 - Налаштування інтерфейсів VLAN

На рис.3.7 відображено результат налаштування динамічного протоколу маршрутизації EIGRP.



```

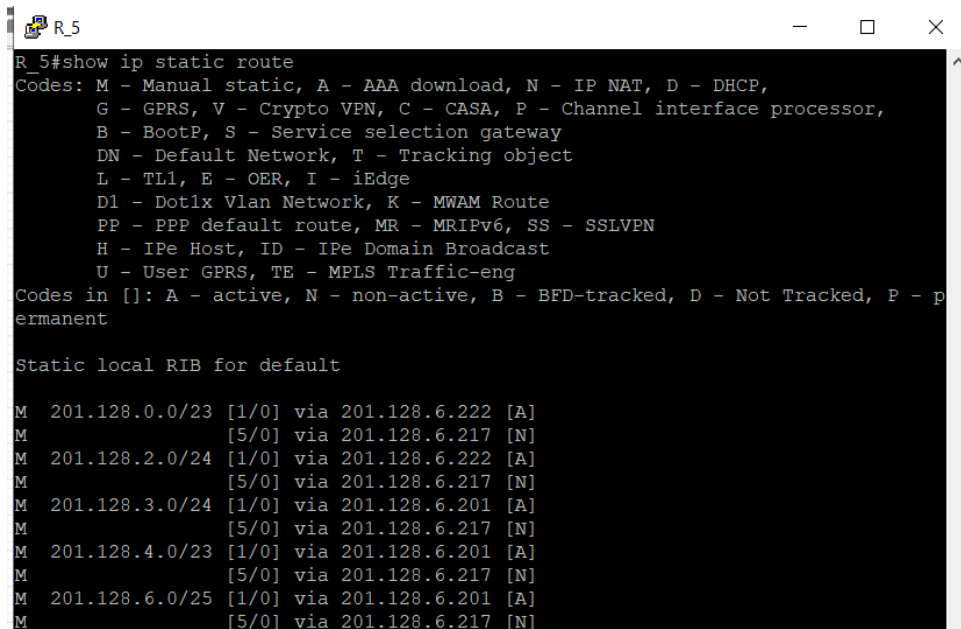
R_7#show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  Redistributing: eigrp 1
    EIGRP-IPv4 Protocol for AS(1)
      Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
      NSF-aware route hold timer is 240
      Router-ID: 202.128.2.245
      Topology : 0 (base)
        Active Timer: 3 min
        Distance: internal 90 external 170
        Maximum path: 4
        Maximum hopcount 100
        Maximum metric variance 1

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    202.128.2.192/30
    202.128.2.196/30
    202.128.2.200/30
    202.128.2.244/30
  Routing Information Sources:
    Gateway         Distance         Last Update
  Distance: internal 90 external 170
  
```

Рисунок 3.7 - Результат налаштування протоколу EIGRP

На рис.3.8 відображено результат налаштування статичної IPv4 маршрутизації.



```

R_5#show ip static route
Codes: M - Manual static, A - AAA download, N - IP NAT, D - DHCP,
       G - GPRS, V - Crypto VPN, C - CASA, P - Channel interface processor,
       B - BootP, S - Service selection gateway
       DN - Default Network, T - Tracking object
       L - TL1, E - OER, I - iEdge
       DL - Dot1x Vlan Network, K - MWAM Route
       PP - PPP default route, MR - MRIPv6, SS - SSLVPN
       H - IPe Host, ID - IPe Domain Broadcast
       U - User GPRS, TE - MPLS Traffic-eng
Codes in []: A - active, N - non-active, B - BFD-tracked, D - Not Tracked, P - p
ermanent

Static local RIB for default

M 201.128.0.0/23 [1/0] via 201.128.6.222 [A]
M                               [5/0] via 201.128.6.217 [N]
M 201.128.2.0/24 [1/0] via 201.128.6.222 [A]
M                               [5/0] via 201.128.6.217 [N]
M 201.128.3.0/24 [1/0] via 201.128.6.201 [A]
M                               [5/0] via 201.128.6.217 [N]
M 201.128.4.0/23 [1/0] via 201.128.6.201 [A]
M                               [5/0] via 201.128.6.217 [N]
M 201.128.6.0/25 [1/0] via 201.128.6.201 [A]
M                               [5/0] via 201.128.6.217 [N]
  
```

Рисунок 3.8 - Результат налаштування статичної маршрутизації

На рис.3.9 відображено зв'язок між вузлами мережі (цілісність схеми не порушена).

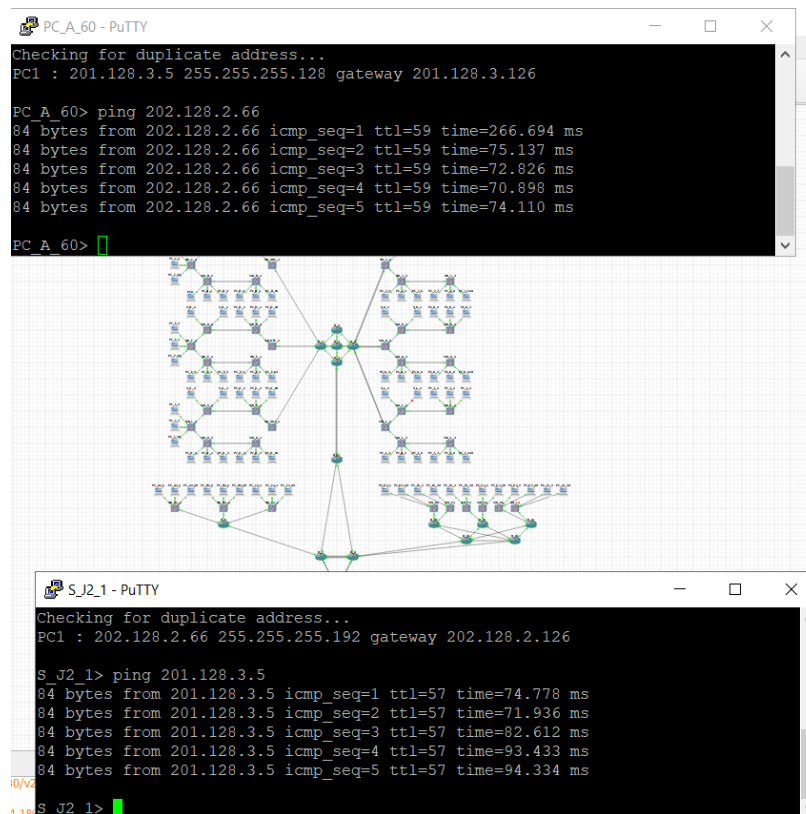


Рисунок 3.9 - Перевірка наявності зв'язку між вузлами мережі (цілісність схеми не порушена)

На рис.3.10 зв'язок між вузлами мережі (цілісність схеми порушена).

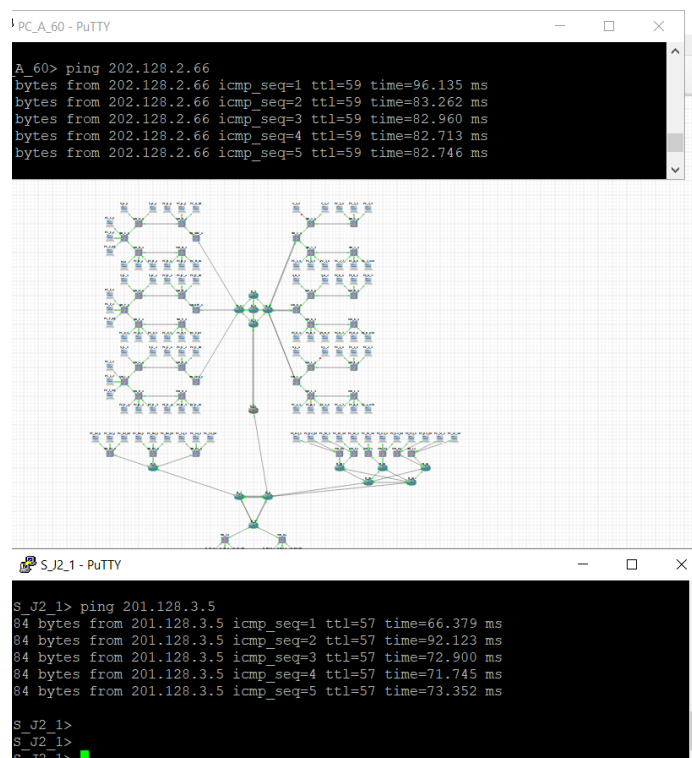


Рисунок 3.10 - Перевірка наявності зв'язку між вузлами мережі (цілісність схеми порушена)

		Руса́тинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфі́менко А.А.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

На рис.3.11 та рис.3.12 виведена загальна таблиця маршрутизації, на цьому маршрутизаторі налаштована редистрибуція, щоб об'єднує мережі.

```

R15#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

S    201.128.0.0/23 [1/0] via 201.128.6.226
S    201.128.2.0/24 [1/0] via 201.128.6.226
S    201.128.3.0/24 [1/0] via 201.128.6.226
S    201.128.4.0/23 [1/0] via 201.128.6.226
S    201.128.6.0/24 is variably subnetted, 12 subnets, 4 masks
S    201.128.6.0/25 [1/0] via 201.128.6.226
S    201.128.6.128/26 [1/0] via 201.128.6.226
S    201.128.6.192/30 [1/0] via 201.128.6.226
S    201.128.6.196/30 [1/0] via 201.128.6.226
S    201.128.6.200/30 [1/0] via 201.128.6.226
S    201.128.6.204/30 [1/0] via 201.128.6.226
S    201.128.6.208/30 [1/0] via 201.128.6.226
S    201.128.6.212/30 [1/0] via 201.128.6.226
S    201.128.6.216/30 [1/0] via 201.128.6.226
S    201.128.6.220/30 [1/0] via 201.128.6.226
C    201.128.6.224/30 is directly connected, Port-channel1
L    201.128.6.225/32 is directly connected, Port-channel1
S    202.128.0.0/24 is variably subnetted, 5 subnets, 2 masks
S    202.128.0.0/25 [1/0] via 202.128.2.245
D    202.128.0.0/26
     [90/30976] via 202.128.2.245, 00:00:07, GigabitEthernet5/0
D    202.128.0.64/26
     [90/30976] via 202.128.2.245, 00:00:08, GigabitEthernet5/0
S    202.128.0.128/26 [1/0] via 202.128.2.245
S    202.128.0.192/26 [1/0] via 202.128.2.245
S    202.128.1.0/26 is subnetted, 4 subnets
S    202.128.1.0 [1/0] via 202.128.2.245
S    202.128.1.64 [1/0] via 202.128.2.245
S    202.128.1.128 [1/0] via 202.128.2.245
S    202.128.1.192 [1/0] via 202.128.2.245
S    202.128.2.0/24 is variably subnetted, 20 subnets, 3 masks
S    202.128.2.0/26 [1/0] via 202.128.2.245
S    202.128.2.64/26 [1/0] via 202.128.2.245
S    202.128.2.128/26 [1/0] via 202.128.2.245
S    202.128.2.192/30 [1/0] via 202.128.2.245
S    202.128.2.196/30 [1/0] via 202.128.2.245
S    202.128.2.200/30 [1/0] via 202.128.2.245

```

Рисунок 3.11 - Таблиця маршрутизації (частина 1)

```

R15#
S    202.128.2.64/26 [1/0] via 202.128.2.245
S    202.128.2.128/26 [1/0] via 202.128.2.245
S    202.128.2.192/30 [1/0] via 202.128.2.245
S    202.128.2.196/30 [1/0] via 202.128.2.245
S    202.128.2.200/30 [1/0] via 202.128.2.245
S    202.128.2.204/30 [1/0] via 202.128.2.245
S    202.128.2.208/30 [1/0] via 202.128.2.245
S    202.128.2.212/30 [1/0] via 202.128.2.245
S    202.128.2.216/30 [1/0] via 202.128.2.245
S    202.128.2.220/30 [1/0] via 202.128.2.245
S    202.128.2.224/30 [1/0] via 202.128.2.245
S    202.128.2.228/30 [1/0] via 202.128.2.245
S    202.128.2.232/30 [1/0] via 202.128.2.245
S    202.128.2.236/30 [1/0] via 202.128.2.245
S    202.128.2.240/30 [1/0] via 202.128.2.245
C    202.128.2.244/30 is directly connected, GigabitEthernet5/0
L    202.128.2.246/32 is directly connected, GigabitEthernet5/0
C    202.128.2.248/30 is directly connected, GigabitEthernet6/0
L    202.128.2.250/32 is directly connected, GigabitEthernet6/0

```

Рисунок 3.12 - Таблиця маршрутизації (частина 2)

		Русацька А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

3.3 Налаштування підсистеми аутентифікації на базі протоколу TACACS+

Налагодження системи аутентифікації згідно за розробленою схемою передбачає налагодження роботи сервера аутентифікації, створення груп користувачів, надавання їм певних привілеїв, створення груп пристроїв, а також додавання пристроїв.

Спочатку було виконано налаштування пристроїв, що будуть використовуватися для налаштування AAA. Результат налаштування наведений на рис.3.13.

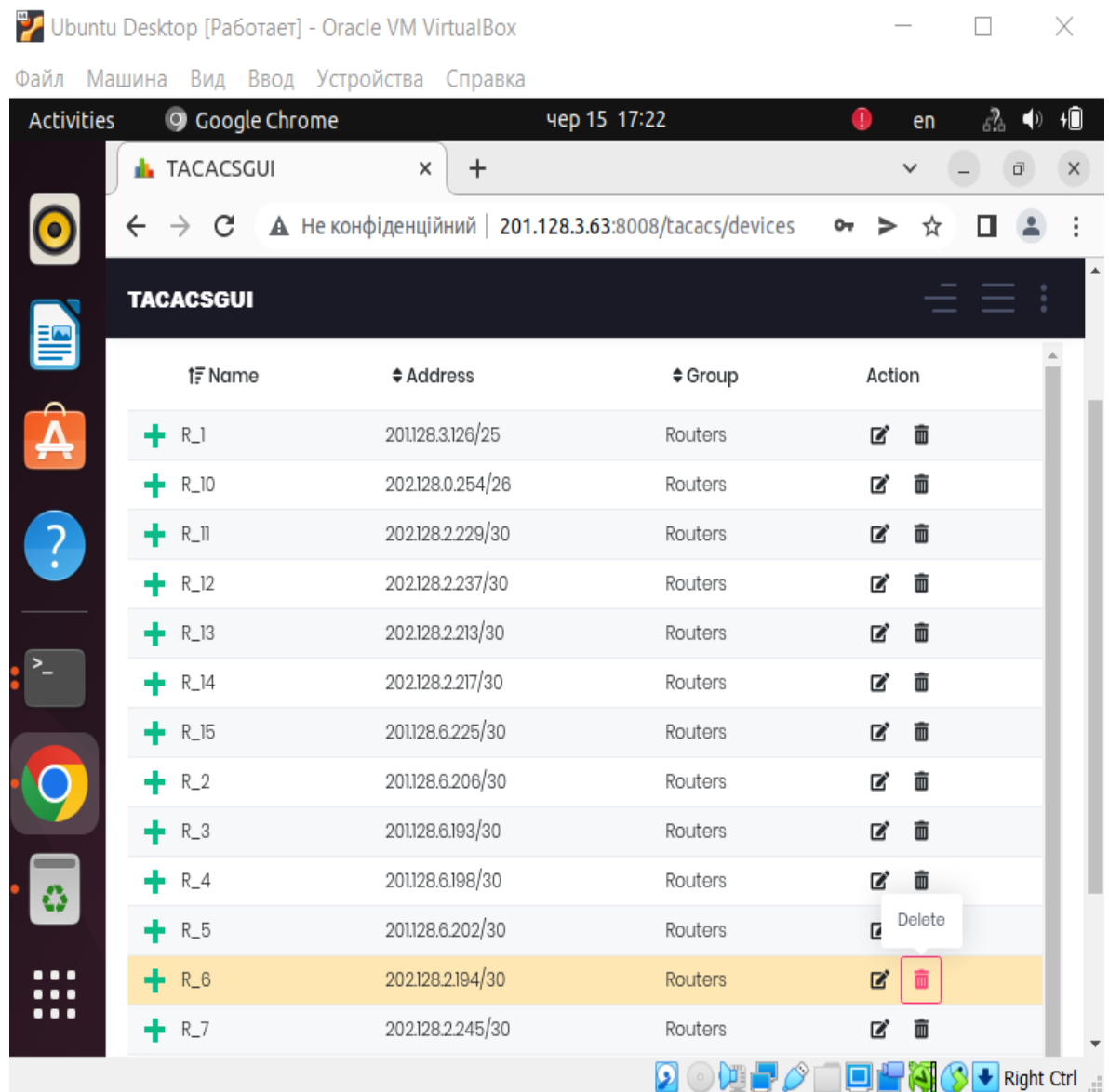


Рисунок 3.13 - Результат створення пристроїв

На рис.3.14 відображений результат створення груп користувачів, відповідно до розподілу прав, наведених у розділі.

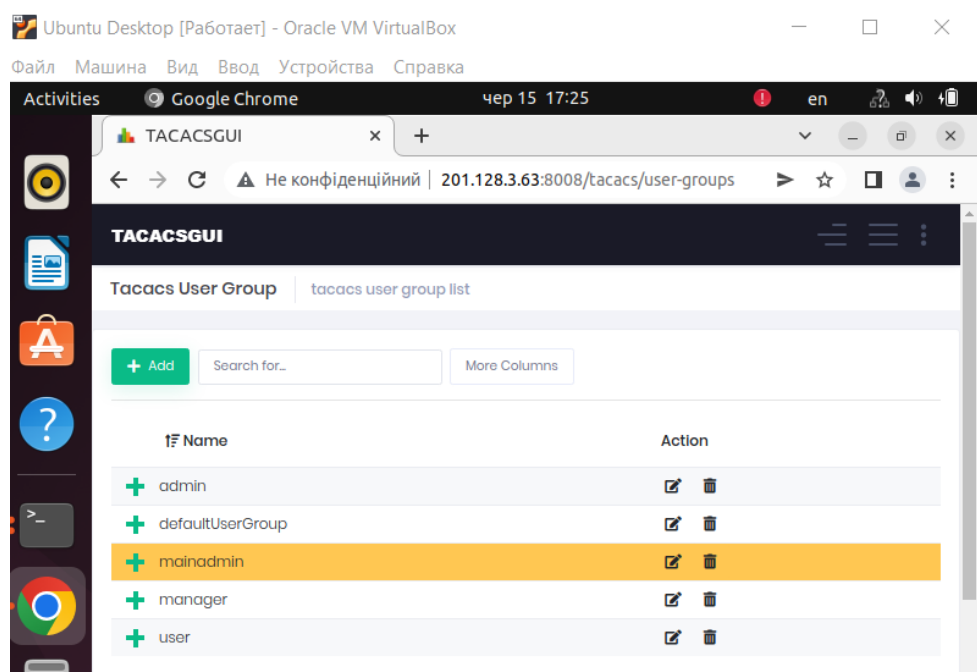


Рисунок 3.14 - Результат створення груп

На рис.3.15 відображений результат створення користувачів та додавання їх до відповідних груп.

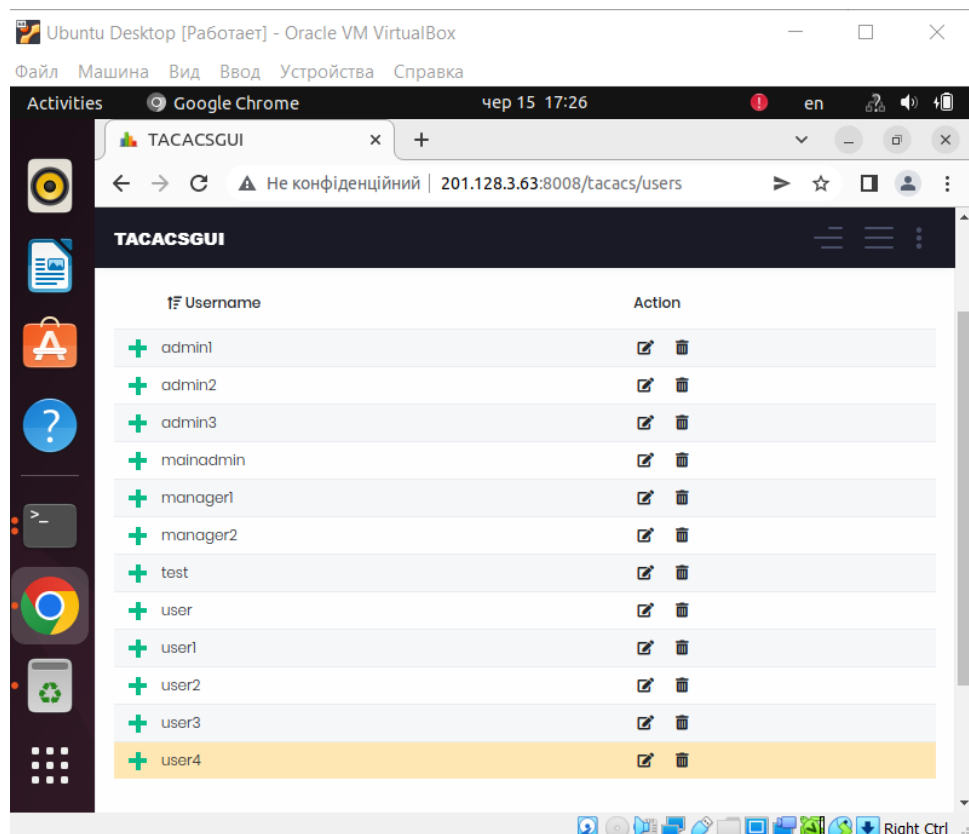


Рисунок 3.15 - Список створених користувачів

Після проведених операцій на tacacsgui виконується налаштування AAA на пристроях мережі. На рис.3.16 наведений приклад налаштування.

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R_1
!
aaa group server tacacs+ Routers
server 201.128.3.63
!
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
action-type start-stop
group tacacs+
!
aaa accounting commands 15 default
action-type start-stop
group tacacs+

```

Рисунок 3.16 - Результат налаштування AAA на маршрутизаторі

На рис.3.17 наведений приклад налаштування прав для відповідного типу привілеїв групи.

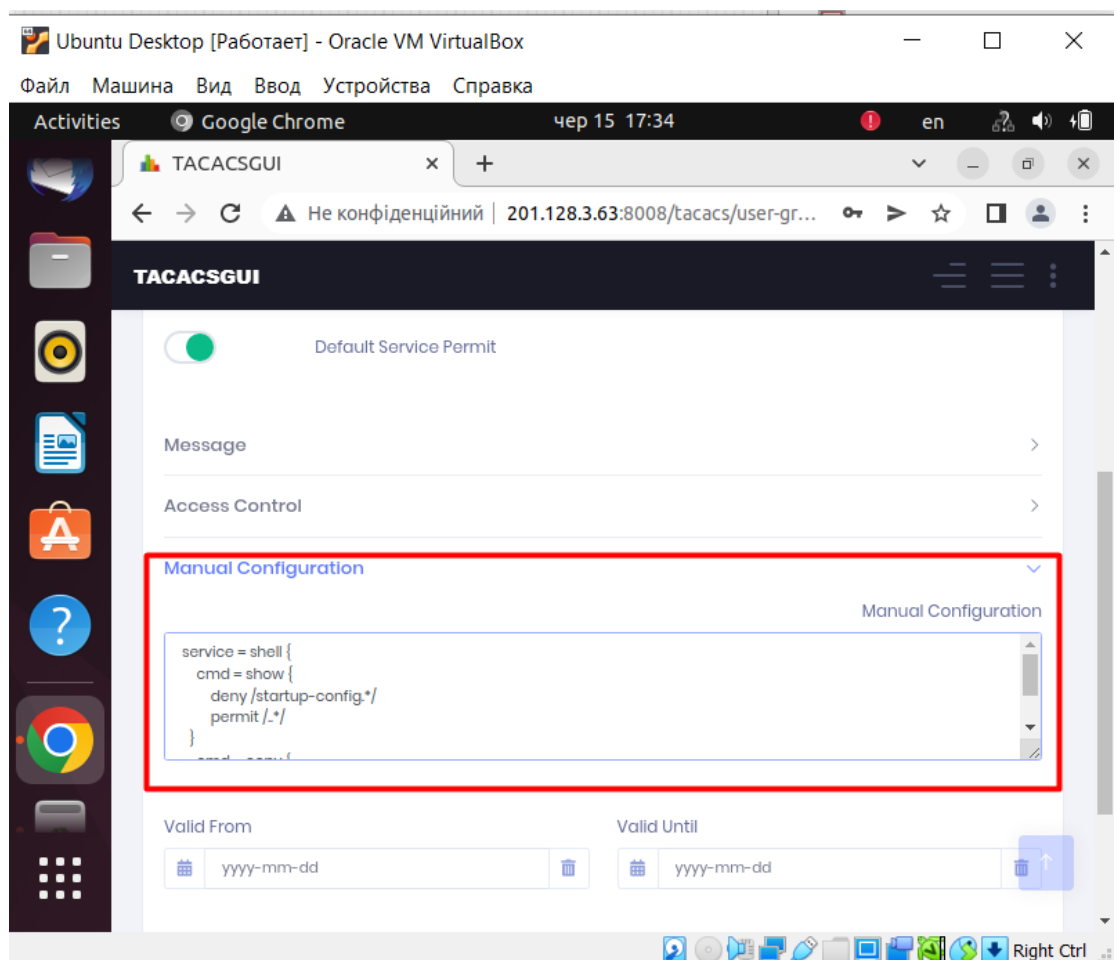


Рисунок 3.17 - Налаштування прав для кожного типу привілеїв

Також був налаштований доступ за допомогою ssh. Виконанні налаштування наведені на рис.3.18.

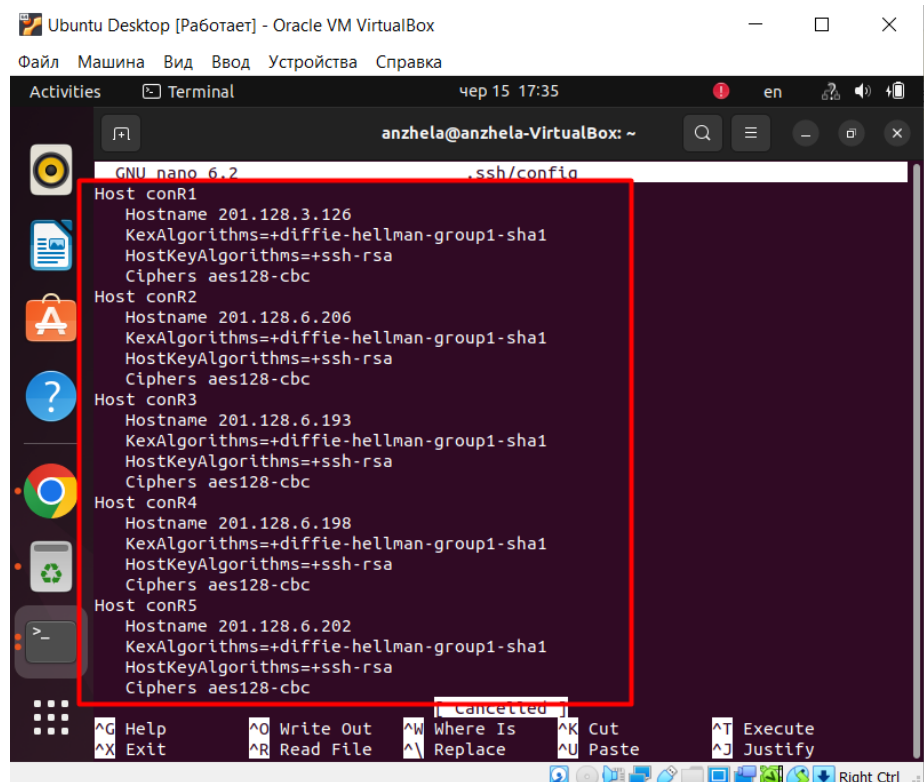


Рисунок 3.18 - Налаштування ssh

3.4 Тестування виконаних налаштувань

Спершу виконуємо перевірку доступу до пристроїв, що були налаштовані вище за допомогою користувачів:

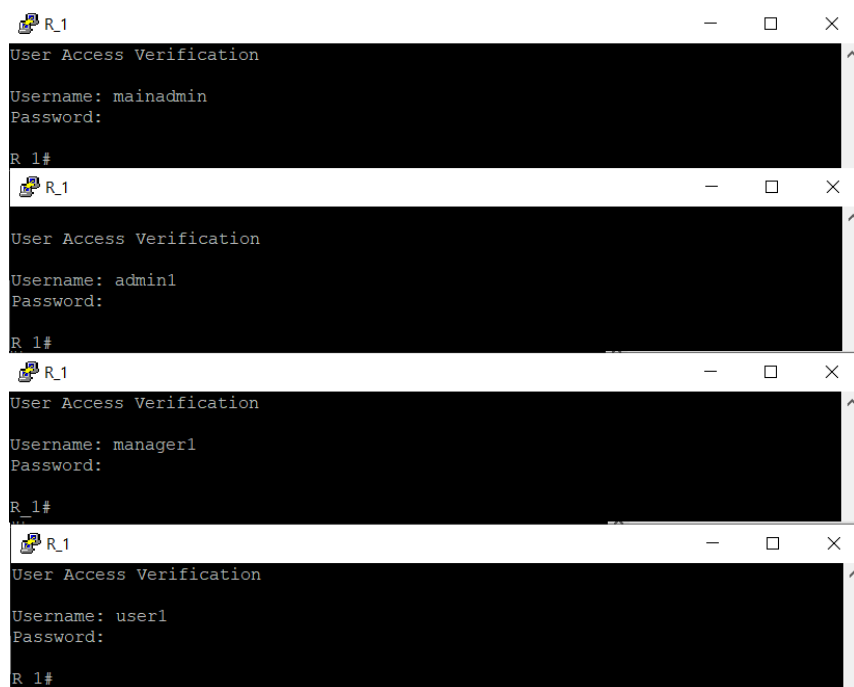
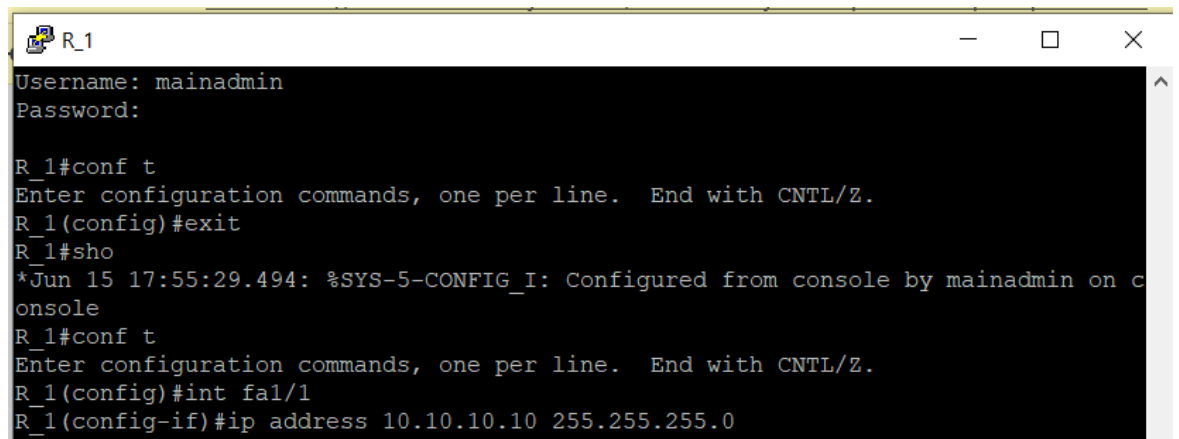


Рисунок 3.19 – Перевірка доступу до пристроїв для користувачів різних груп

		Рустинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				46
Змн.	Арк.	№ докум.	Підпис	Дата		

Перевірка застосування дозволів та заборон для користувачів з різних груп:

- mainadmin1 (permit all) рис.3.20:

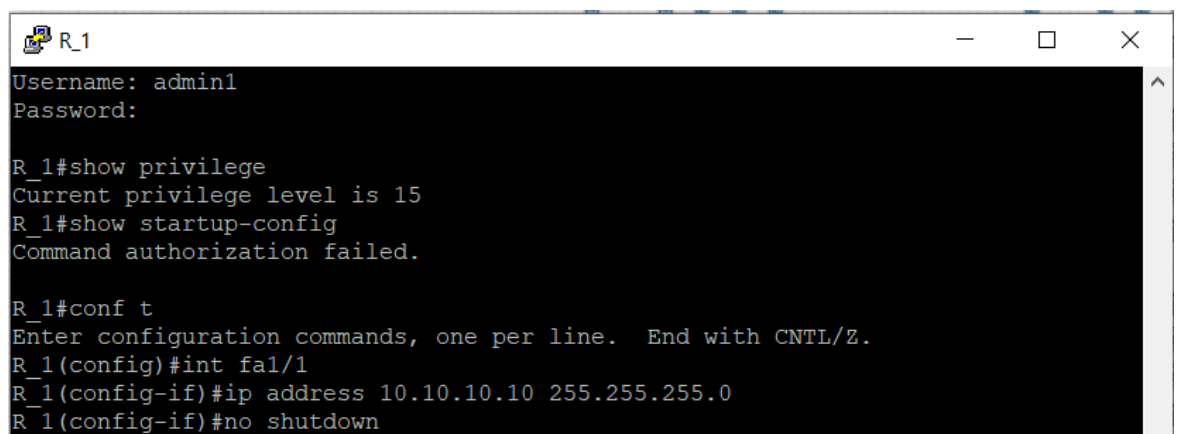


```
R_1
Username: mainadmin
Password:

R_1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R_1(config)#exit
R_1#sho
*Jun 15 17:55:29.494: %SYS-5-CONFIG_I: Configured from console by mainadmin on c
onsole
R_1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R_1(config)#int fa1/1
R_1(config-if)#ip address 10.10.10.10 255.255.255.0
```

Рисунок 3.20 – Перевірка дозволів та заборон для користувача mainadmin1 (група: mainadmin)

- admin1 (admin) рис.3.21:



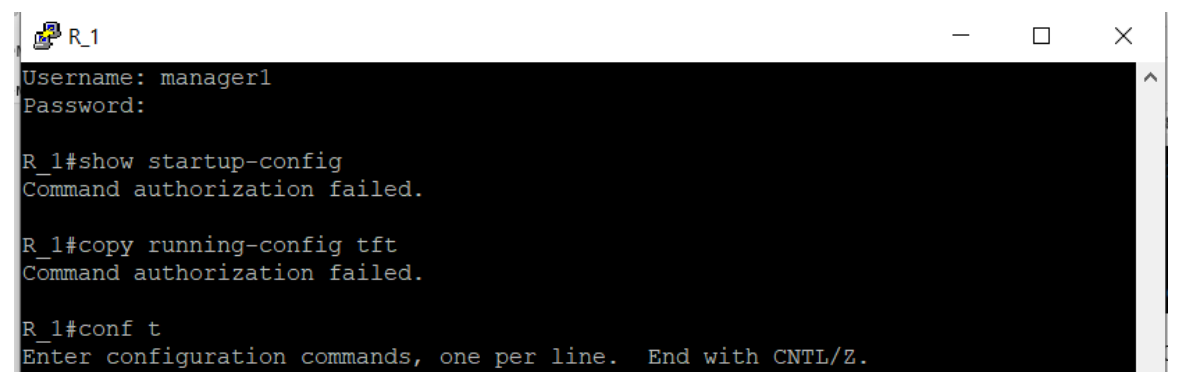
```
R_1
Username: admin1
Password:

R_1#show privilege
Current privilege level is 15
R_1#show startup-config
Command authorization failed.

R_1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R_1(config)#int fa1/1
R_1(config-if)#ip address 10.10.10.10 255.255.255.0
R_1(config-if)#no shutdown
```

Рисунок 3.21 – Перевірка дозволів та заборон для користувача admin1 (група: admin)

- manager1 (manager) рис.3.22:



```
R_1
Username: manager1
Password:

R_1#show startup-config
Command authorization failed.

R_1#copy running-config tft
Command authorization failed.

R_1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
```

Рисунок 3.22 – Перевірка дозволів та заборон для користувача manager1 (група: manager)

- user1 (user) рис.3.23:

```

R_1
User Access Verification

Username: user1
Password:

R_1#show startup-config
Command authorization failed.

R_1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R_1(config)#int fa1/1
R_1(config-if)#ip address 10.10.10.10 255.255.255.0
Command authorization failed.

R_1(config-if)#exit
  
```

Рисунок 3.23 – Перевірка дозволів та заборон для користувача manager1 (група: manager)

Окрім груп, також можна задавати дозволи та заборони для виконання користувачів окремо.

Для можливості управління пристроями з одного пристрою було виконано налаштування ssh, тому виконуємо перевірку доступу:

```

anzhela@anzhela-VirtualBox: ~
$ ssh conR4 -l user1
The authenticity of host '201.128.6.198 (201.128.6.198)' can't be established.
RSA key fingerprint is SHA256:CMRoTaSf0afqt6hkhintqIaY5N8JNU/t02pcEyq4px4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '201.128.6.198' (RSA) to the list of known hosts.
(user1@201.128.6.198)
Password:

R_4#exit
Connection to 201.128.6.198 closed.

anzhela@anzhela-VirtualBox: ~
$ ssh conR1 -l user1
The authenticity of host '201.128.3.126 (201.128.3.126)' can't be established.
RSA key fingerprint is SHA256:fw70ZzXVDW9dU8oQDj7XLI2Zip3vebJrqiAVsMoY2V4.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '201.128.3.126' (RSA) to the list of known hosts.
(user1@201.128.3.126)
Password:

R_1#exit
Connection to 201.128.3.126 closed by remote host.
Connection to 201.128.3.126 closed.

anzhela@anzhela-VirtualBox: ~
$ ssh conR7 -l admin1
The authenticity of host '202.128.2.245 (202.128.2.245)' can't be established.
RSA key fingerprint is SHA256:Z6G+2exoEWq+SvB6EEUJxlu0T3mj5YTVFgQaIdyVTjs.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '202.128.2.245' (RSA) to the list of known hosts.
  
```

Рисунок 3.24 – Перевірка підключення до SSH

Тасacs GUI також надає можливість обліку та аудиту дій користувачів, що виконують певні дії на пристрої, звіти наведені на рис.3.25-3.27:

Date	Server	Nas	Username	Nac	Action
2022-06-15 21:54:34	localhost	201128.2.217	manager1	201128.3.64	shell login succeeded
2022-06-15 21:54:30	localhost	201128.2.217	manager1	201128.3.64	shell login failed
2022-06-15 21:52:31	localhost	201128.2.245	admin1	201128.3.64	shell login succeeded
2022-06-15 21:52:27	localhost	201128.2.245	admin1	201128.3.64	shell login failed
2022-06-15 21:52:03	localhost	201128.3.126	user1	201128.3.64	shell login succeeded
2022-06-15 21:51:50	localhost	201128.6.198	user1	201128.3.64	shell login succeeded
2022-06-15 21:49:51	localhost	201128.3.126	user1	201128.3.64	shell login succeeded
2022-06-15 21:45:07	localhost	201128.3.126	user1	async	shell login succeeded
2022-06-15 21:41:39	localhost	201128.3.126	manager1	async	shell login succeeded
2022-06-15 21:37:44	localhost	201128.3.126	admin1	async	shell login succeeded
2022-06-15 21:37:19	localhost	201128.3.126	admin1	async	shell login succeeded
2022-06-15 21:34:55	localhost	201128.3.126	admin1	async	shell login succeeded
2022-06-15 21:32:37	localhost	201128.3.126	admin1	async	shell login succeeded

Рисунко 3.25 – Звіт authentication

Date	Server	Nas	Username	Nac	Action	Command
2022-06-15 21:46:02	localhost	201128.3.126	user1	async	deny	ip address 10.10.10.10 255.255.255.0
2022-06-15 21:45:52	localhost	201128.3.126	user1	async	permit	interface FastEthernet 1/1
2022-06-15 21:45:40	localhost	201128.3.126	user1	async	permit	configure terminal
2022-06-15 21:45:37	localhost	201128.3.126	user1	async	deny	show startup-config
2022-06-15 21:42:54	localhost	201128.3.126	manager1	async	permit	configure terminal
2022-06-15 21:42:39	localhost	201128.3.126	manager1	async	deny	copy running-config tftp
2022-06-15 21:42:18	localhost	201128.3.126	manager1	async	deny	show startup-config
2022-06-15 21:39:19	localhost	201128.3.126	admin1	async	permit	no shutdown
2022-06-15 21:39:10	localhost	201128.3.126	admin1	async	permit	ip address 10.10.10.10 255.255.255.0
2022-06-15 21:38:18	localhost	201128.3.126	admin1	async	permit	interface FastEthernet 1/1
2022-06-15 21:38:12	localhost	201128.3.126	admin1	async	permit	configure terminal
2022-06-15 21:38:07	localhost	201128.3.126	admin1	async	deny	show startup-config
2022-06-15 21:37:28	localhost	201128.3.126	admin1	async	permit	show running-config

Рисунок 3.26 – Звіт authorization

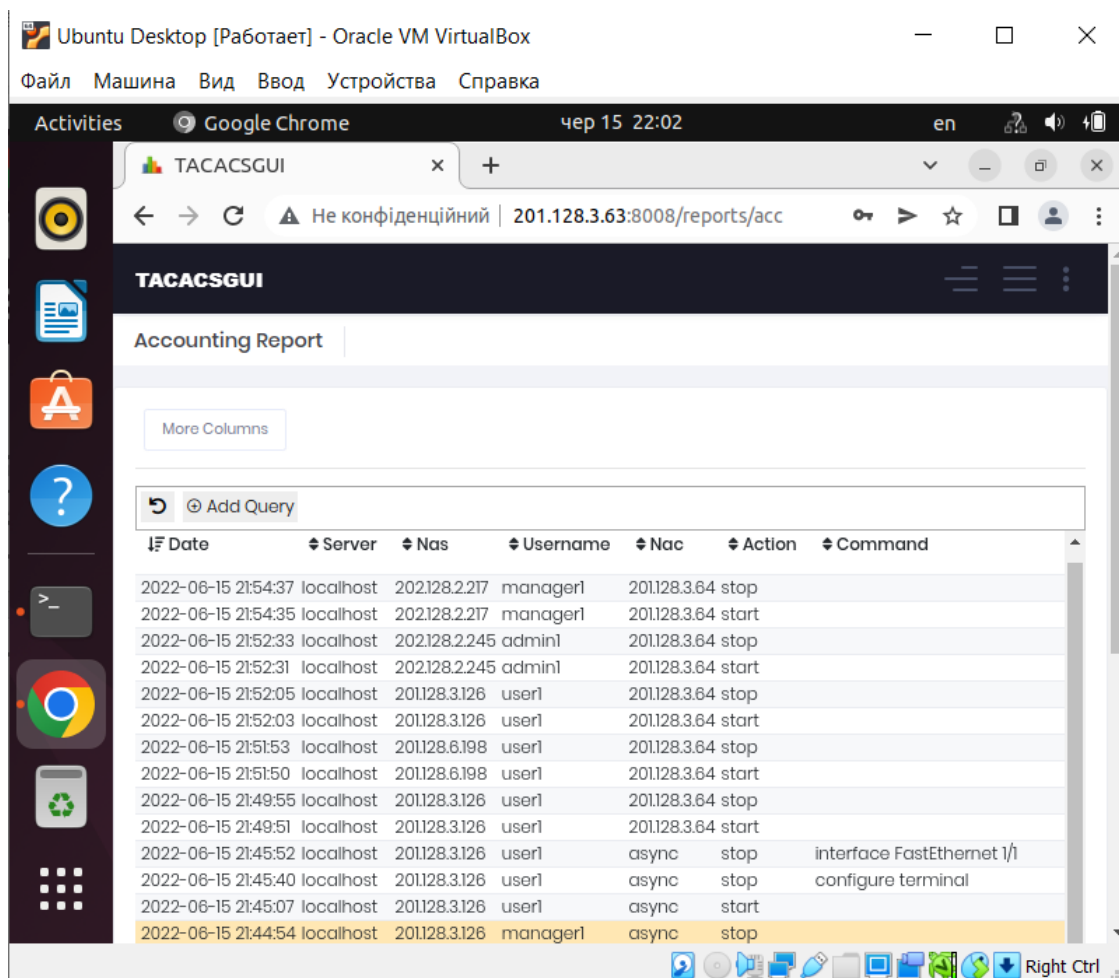


Рисунок 3.27 – Звіт accounting

Висновки до третього розділу

В результаті виконання третього розділу вдалося виконати налаштування пристроїв мережі, а саме налаштувати ір адресацію, статичну та динамічну маршрутизацію між пристроями, а також редистрибуцію. Вдалося реалізувати дію моделі AAA за допомогою протоколу Тасас+. Користувачі були поділені по групах та отримували відповідні права для виконання чи заборони певних дій на мережевих пристроях. Під час тестування помилок не було знайдено, пристрою працюють відповідно до розроблених цілей.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи бакалавра у першому розділі було виконано аналіз моделі AAA, як основи сучасних систем аутентифікації, розглянуто основні функції та рішення безпеки. Проаналізовано теоретичні основи моделі та протоколи AAA, а саме TACACS+, RADIUS та Kerberos. Виокремлено переваги та недоліки кожного з них та дійдено до висновку що протокол TACACS+ більш надійний, оскільки використовує TCP, окрім цього TACACS+ забезпечує більший контроль команд авторизації та всі пакети AAA зашифровані на відміну від Radius, тому для створення підсистеми аутентифікації користувачів на підприємстві буде використано протокол TACACS+.

В результаті виконання другого розділу вдалося обрати топологію мережі, розглянути основні вузли та побудувати мережу в цілому. Після цього було проведено розподіл підмереж на основі цих даних. В результаті поділу вдалося знайти оптимальні префікси для мереж: мережа №1: оптимальний префікс - /21, обрана IP-мережа: 201.128.0.0; мережа №2: оптимальний префікс - /22, обрана IP-мережа: 202.128.0.0. Після вибору оптимальних префіксів, та вибору IP-мереж було проведено розрахунок адресації для мереж. Також було обрано обладнання мережі, виокремлено переваги та недоліки кожної категорії пристроїв мережі. В результаті аналізу для побудови мережі були обрані такі пристрої: маршрутизатор C7200VXR та стандартний комутатор. Для реалізації системи аутентифікації користувачів було обрано Tacacs server with GUI. Також розроблено групи користувачів та розподілені відповідні права між ними, наведені основні команди для налаштування обліку всіх дій користувачів на пристроях.

В результаті виконання третього розділу вдалося виконати налаштування пристроїв мережі, а саме налаштувати ip адресацію, статичну та динамічну маршрутизацію між пристроями, а також редистрибуцію. Вдалося реалізувати модель AAA за допомогою протоколу Tacacs+. Користувачі були поділені по групах та отримували відповідні права для виконання чи заборони певних дій на мережевих пристроях. Під час тестування помилок не було знайдено.

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Буров Є.В. Комп'ютерні мережі. Підручник. Том 1. / Є.В. Буров, М.М. Митник. – Львів: «Магнолія 2006», 2021. – 334 с.
2. Комп'ютерні мережі : навчальний посібник / [Азаров О. Д., Захарченко С. М., Кадук О. В. та ін.] — Вінниця : ВНТУ, 2013. — 371 с
3. Навчальний курс CCNAv7: Introduction to Networks [Електронний ресурс] – Режим доступу: www.netacad.com.
4. Навчальний курс CCNA Routing and Switching: Routing and Switching Essentials [Електронний ресурс] – Режим доступу: www.netacad.com.
5. Навчальний курс CCNA Routing and Switching: Scaling Networks [Електронний ресурс] – Режим доступу: www.netacad.com.
6. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РОБОТИ ПРОТОКОЛУ МАРШРУТИЗАЦІЇ EIGRP. [Електронний ресурс]. – Режим доступу: https://learn.ztu.edu.ua/pluginfile.php/156823/mod_resource/content/1/KM_KI_LR-23-2020-2021_KI-4.pdf
7. НАЛАГОДЖЕННЯ ТА ДОСЛІДЖЕННЯ РЕДИСТРИБУЦІЇ МАРШРУТІВ У МЕРЕЖІ. [Електронний ресурс]. – Режим доступу: https://learn.ztu.edu.ua/pluginfile.php/160433/mod_resource/content/1/KM_KI_LR-27-2020-2021_KI-4.pdf
8. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. Юбилейное издание: учебник для вузов. – 6-е изд. / В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2020 – 1008 с.
9. Одом Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация, акад. изд. / пер. с англ. Уэнделл Одом. – М.: ООО „И.Д. Вильямс”, 2015. – 736 с.
10. AAA Local Command Authorization. [Електронний ресурс]. – Режим доступу: <https://networklessons.com/cisco/ccie-routing-switching/aaa-local-command-authorization>
11. Authentication, Authorization, Accounting. [Електронний ресурс]. – Режим

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

доступу: <https://contenthub.netacad.com/legacy/CCNAS/en/3.0.1.1>

12. Basic Route Redistribution. Cisco Academy Conference. [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/dam/en_us/training-events/le21/le34/downloads/689/academy/2005/BRK-105.pdf

13. Enterprise Networking, Security, and Automation Course. [Електронний ресурс]. – Режим доступу: <https://contenthub.netacad.com/ensa>

14. Switching, Routing, and Wireless Essentials Course. [Електронний ресурс]. – Режим доступу: <https://contenthub.netacad.com/srwe>

15. Cisco IOS – Privilege Levels. [Електронний ресурс]. – Режим доступу: <https://learningnetwork.cisco.com/s/blogs/a0D3i000002eeWTEAY/cisco-ios-privilege-levels>

16. Configure SSH on Routers and Switches. [Електронний ресурс]. – Режим доступу: <https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-shell-ssh/4145-ssh.html>

17. Enhanced Interior Gateway Routing Protocol. [Електронний ресурс]. – Режим доступу: <https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/16406-eigrp-toc.html>

18. Odom Wendell. CCNA 200-301 Official Cert Guide. Volume 2. / Wendell Odom. Cisco Press, 2020 – 1444 p.

19. TACACS+. [Електронний ресурс]. – Режим доступу: https://www.pro-bono-publico.de/projects/tac_plus.html

20. Tacacs+ Authentication. [Електронний ресурс]. – Режим доступу: <https://contenthub.netacad.com/legacy/CCNAS/2.0/en/index.html#3.3.2.2>.

21. TACACSGUI. [Електронний ресурс]. – Режим доступу: <https://tacacsgui.com/>

22. TACACSGUI. Documentation. [Електронний ресурс]. – Режим доступу: <https://tacacsgui.com/documentation/>

23. Tacacs + LDAP + Huawei. [Електронний ресурс]. – Режим доступу: <https://netdotwork.github.io/tacacs-plus/>

		Русаїтинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Руса́тинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфі́менко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

Таблиця розподілу підмереж першої мережі

ІР-адреса та префікс	ІР-адреса в двійковому вигляді	Робоча підмережа
201.128.0.0/21	11001001.10000000.00000 000.00000000	-
201.128.0.0/24	11001001.10000000.00000000 .00000000	J1
201.128.1.0/24	11001001.10000000.00000001 .00000000	K1
201.128.2.0/24	11001001.10000000.00000010 .00000000	L1
201.128.3.0/25	11001001.10000000.00000011.0 00000000	A1
201.128.3.128/25	11001001.10000000.00000011.1 00000000	B1
201.128.4.0/25	11001001.10000000.00000100.0 00000000	D1
201.128.4.128/25	11001001.10000000.00000100.1 00000000	E1
201.128.5.0/25	11001001.10000000.00000101.0 00000000	G1
201.128.5.128/25	11001001.10000000.00000101.1 00000000	H1
201.128.6.0/26	11001001.10000000.00000110.00 00000000	C1
201.128.6.64/26	11001001.10000000.00000110.01 00000000	F1
201.128.6.128/26	11001001.10000000.00000110.10 00000000	I1
201.128.6.192/30	11001001.10000000.00000110.110000 00	AA1
201.128.6.196/30	11001001.10000000.00000110.110001 00	BB1
201.128.6.200/30	11001001.10000000.00000110.110010 00	CC1
201.128.6.204/30	11001001.10000000.00000110.110011 00	DD1
201.128.6.208/30	11001001.10000000.00000110.110100 00	EE1
201.128.6.212/30	11001001.10000000.00000110.110101 00	FF1
201.128.6.216/30	11001001.10000000.00000110.110110 00	GG1
201.128.6.220/30	11001001.10000000.00000110.110111 00	HH1
201.128.6.224/30	11001001.10000000.00000110.111000 00	II1
201.128.6.228/30	11001001.10000000.00000110.111001 00	JJ1
201.128.6.232/30	11001001.10000000.00000110.111010 00	KK1

Таблиця розподілу підмереж другої мережі

ІР-адреса та префікс	ІР-адреса в двійковому вигляді	Робоча підмережа
202.128.0.0/22	11001010.10000000.00000000 00.00000000	-
202.128.0.0/26	11001010.10000000.00000000.00 000000	A2
202.128.0.64/26	11001010.10000000.00000000.01 000000	B2
202.128.0.128/26	11001010.10000000.00000000.10 000000	C2
202.128.0.192/26	11001010.10000000.00000000.11 000000	D2
202.128.1.0/26	11001010.10000000.00000001.00 000000	E2
202.128.1.64/26	11001010.10000000.00000001.01 000000	F2
202.128.1.128/26	11001010.10000000.00000001.10 000000	G2
202.128.1.192/26	11001010.10000000.00000001.11 000000	H2
202.128.2.0/26	11001010.10000000.00000010.00 000000	I2
202.128.2.64/26	11001010.10000000.00000010.01 000000	J2
202.128.2.128/26	11001010.10000000.00000010.10 000000	K2
202.128.2.192/30	11001010.10000000.00000010.110000 00	AA2
202.128.2.196/30	11001010.10000000.00000010.110001 00	BB2
202.128.2.200/30	11001010.10000000.00000010.110010 00	CC2
202.128.2.204/30	11001010.10000000.00000010.110011 00	DD2
202.128.2.208/30	11001010.10000000.00000010.110100 00	EE2
202.128.2.212/30	11001010.10000000.00000010.110101 00	FF2
202.128.2.216/30	11001010.10000000.00000010.110110 00	GG2
202.128.2.220/30	11001010.10000000.00000010.110111 00	HH2
202.128.2.224/30	11001010.10000000.00000010.111000 00	II2
202.128.2.228/30	11001010.10000000.00000010.111001 00	JJ2
202.128.2.232/30	11001010.10000000.00000010.111010 00	KK2
202.128.2.236/30	11001010.10000000.00000010.111011 00	LL2
202.128.2.240/30	11001010.10000000.00000010.111100 00	MM2
202.128.2.244/30	11001010.10000000.00000010.111101 00	NN2
202.128.2.248/30	11001010.10000000.00000010.111110 00	OO2
202.128.2.252/30	11001010.10000000.00000010.111111 00	PP2

Параметри IP-адресації першої мережі

Мережа	Маска мережі	Мін. адреса	Макс. адреса	Широк. адр.
(J1) 201.128.0.0/24	255.255.255.0	201.128.0.1	201.128.0.254	201.128.0.255
(K1) 201.128.1.0/24	255.255.255.0	201.128.1.1	201.128.1.254	201.128.1.255
(L1) 201.128.2.0/24	255.255.255.0	201.128.2.1	201.128.2.254	201.128.2.255
(A1) 201.128.3.0/25	255.255.255.128	201.128.3.1	201.128.3.126	201.128.3.127
(B1) 201.128.3.128/25	255.255.255.128	201.128.3.129	201.128.3.254	201.128.3.255
(D1) 201.128.4.0/25	255.255.255.128	201.128.4.1	201.128.4.126	201.128.4.127
(E1) 201.128.4.128/25	255.255.255.128	201.128.4.129	201.128.4.254	201.128.4.255
(G1) 201.128.5.0/25	255.255.255.128	201.128.5.1	201.128.5.126	201.128.5.127
(H1) 201.128.5.128/25	255.255.255.128	201.128.5.129	201.128.5.254	201.128.5.255
(C1) 201.128.6.0/26	255.255.255.192	201.128.6.1	201.128.6.62	201.128.6.63
(F1) 201.128.6.64/26	255.255.255.192	201.128.6.65	201.128.6.126	201.128.6.127
(I1) 201.128.6.128/26	255.255.255.192	201.128.6.129	201.128.6.190	201.128.6.191
(AA1) 201.128.6.192/30	255.255.255.252	201.128.6.193	201.128.6.194	201.128.6.195
(BB1) 201.128.6.196/30	255.255.255.252	201.128.6.197	201.128.6.198	201.128.6.199
(CC1) 201.128.6.200/30	255.255.255.252	201.128.6.201	201.128.6.202	201.128.6.203
(DD1) 201.128.6.204/30	255.255.255.252	201.128.6.205	201.128.6.206	201.128.6.207
(EE1) 201.128.6.208/30	255.255.255.252	201.128.6.209	201.128.6.210	201.128.6.211
(FF1) 201.128.6.212/30	255.255.255.252	201.128.6.213	201.128.6.214	201.128.6.215
(GG1) 201.128.6.216/30	255.255.255.252	201.128.6.217	201.128.6.218	201.128.6.219
(HH1) 201.128.6.220/30	255.255.255.252	201.128.6.221	201.128.6.222	201.128.6.223
(II1) 201.128.6.224/30	255.255.255.252	201.128.6.225	201.128.6.226	201.128.6.227
(JJ1) 201.128.6.228/30	255.255.255.252	201.128.6.229	201.128.6.230	201.128.6.231
(KK1) 201.128.6.232/30	255.255.255.252	201.128.6.233	201.128.6.234	201.128.6.235

Параметри IP-адресації другої мережі

Мережа	Маска мережі	Мін. адреса	Макс. адреса	Широк. адр.
(A2) 202.128.0.0/26	255.255.255.192	202.128.0.1	202.128.0.62	202.128.0.63
(B2) 202.128.0.64/26	255.255.255.192	202.128.0.65	202.128.0.126	202.128.0.127
(C2) 202.128.0.128/26	255.255.255.192	202.128.0.129	202.128.0.190	202.128.0.191
(D2) 202.128.0.192/26	255.255.255.192	202.128.0.193	202.128.0.254	202.128.0.255
(E2) 202.128.1.0/26	255.255.255.192	202.128.1.1	202.128.1.62	202.128.1.63
(F2) 202.128.1.64/26	255.255.255.192	202.128.1.65	202.128.1.126	202.128.1.127
(G2) 202.128.1.128/26	255.255.255.192	202.128.1.129	202.128.1.190	202.128.1.191
(H2) 202.128.1.192/26	255.255.255.192	202.128.1.193	202.128.1.254	202.128.1.255
(I2) 202.128.2.0/26	255.255.255.192	202.128.2.1	202.128.2.62	202.128.2.63
(J2) 202.128.2.64/26	255.255.255.192	202.128.2.65	202.128.2.126	202.128.2.127
(K2) 202.128.2.128/26	255.255.255.192	202.128.2.129	202.128.2.190	202.128.2.191
(AA2) 202.128.2.192/30	255.255.255.252	202.128.2.193	202.128.2.194	202.128.2.195
(BB2) 202.128.2.196/30	255.255.255.252	202.128.2.197	202.128.2.198	202.128.2.199
(CC2) 202.128.2.200/30	255.255.255.252	202.128.2.201	202.128.2.202	202.128.2.203
(DD2) 202.128.2.204/30	255.255.255.252	202.128.2.205	202.128.2.206	202.128.2.207
(EE2) 202.128.2.208/30	255.255.255.252	202.128.2.209	202.128.2.210	202.128.2.211
(FF2) 202.128.2.212/30	255.255.255.252	202.128.2.213	202.128.2.214	202.128.2.215
(GG2) 202.128.2.216/30	255.255.255.252	202.128.2.217	202.128.2.218	202.128.2.219
(HH2) 202.128.2.220/30	255.255.255.252	202.128.2.221	202.128.2.222	202.128.2.223
(II2) 202.128.2.224/30	255.255.255.252	202.128.2.225	202.128.2.226	202.128.2.227
(JJ2) 202.128.2.228/30	255.255.255.252	202.128.2.229	202.128.2.230	202.128.2.231
(KK2) 202.128.2.232/30	255.255.255.252	202.128.2.233	202.128.2.234	202.128.2.235
(LL2) 202.128.2.236/30	255.255.255.252	202.128.2.237	202.128.2.238	202.128.2.239
(MM2) 202.128.2.240/30	255.255.255.252	202.128.2.241	202.128.2.242	202.128.2.243
(NN2) 202.128.2.244/30	255.255.255.252	202.128.2.245	202.128.2.246	202.128.2.247
(OO2) 202.128.2.248/30	255.255.255.252	202.128.2.249	202.128.2.250	202.128.2.251
(PP2) 202.128.2.252/30	255.255.255.252	202.128.2.253	202.128.2.254	202.128.2.255

Адресація пристроїв для першої мережі

Мережа	Комутатор (и)	Робоча станція (ї)	Сервер (и)	Шлюз за замовчуванням	Вільний простір
A1	201.128.3.1- 201.128.3.2	201.128.3.3- 201.128.3.62	201.128.3.63- 201.128.3.64	201.128.3.126	201.128.3.65- 201.128.3.125
B1	201.128.3.129- 201.128.3.130	201.128.3.131- 201.128.3.194	-	201.128.3.254	201.128.3.195- 201.128.3.253
C1	201.128.6.1, 201.128.6.42	201.128.6.2- 201.128.6.41	-	201.128.6.62	201.128.6.43- 201.128.6.61
D1	201.128.4.1- 201.128.4.2	201.128.4.3- 201.128.4.62	201.128.4.63- 201.128.4.64	201.128.4.126	201.128.4.65- 201.128.4.125
E1	201.128.4.129- 201.128.4.130	201.128.4.131- 201.128.4.194	-	201.128.4.254	201.128.4.195- 201.128.4.253
F1	201.128.6.65, 201.128.6.106	201.128.6.66- 201.128.6.105	-	201.128.6.126	201.128.6.107- 201.128.6.125
G1	201.128.5.1- 201.128.5.2	201.128.5.3- 201.128.5.62	201.128.5.63- 201.128.5.64	201.128.5.126	201.128.5.65- 201.128.5.125
H1	201.128.5.129- 201.128.5.130	201.128.5.131- 201.128.5.194	-	201.128.5.254	201.128.5.195- 201.128.5.253
I1	201.128.6.129, 201.128.6.170	201.128.6.130- 201.128.6.169	-	201.128.6.190	201.128.6.171- 201.128.6.189
J1	201.128.0.1- 201.128.0.5	201.128.0.6- 201.128.0.155	201.128.0.156- 201.128.0.157	201.128.0.254	201.128.0.158- 201.128.0.253
K1	201.128.1.1- 201.128.1.5	201.128.1.6- 201.128.1.155	201.128.1.156- 201.128.1.157	201.128.1.254	201.128.1.158- 201.128.1.253
L1	201.128.2.1- 201.128.2.5	201.128.2.6- 201.128.2.155	201.128.2.156- 201.128.2.157	201.128.2.254	201.128.2.158- 201.128.2.253

Адресація пристроїв для першої мережі

Мережа	Комутатор (и)	Робоча станція (ї)	Сервер (и)	Шлюз за замовчуванням	Вільний простір
A2	202.128.0.1	202.128.0.2- 202.128.0.41	-	202.128.0.62	202.128.0.42- 202.128.0.61
B2	202.128.0.65	202.128.0.66- 202.128.0.105	-	202.128.0.126	202.128.0.106- 202.128.0.125
C2	202.128.0.129	202.128.0.130- 202.128.0.169	-	202.128.0.190	202.128.0.170- 202.128.0.189
D2	202.128.0.193	202.128.0.194- 202.128.0.233	-	202.128.0.254	202.128.0.234- 202.128.0.253
E2	202.128.1.1	202.128.1.2- 202.128.1.41	-	202.128.1.62	202.128.1.42- 202.128.1.61
F2-	202.128.1.65	202.128.1.66- 202.128.1.105	-	202.128.1.126	202.128.1.106- 202.128.1.125
G2	202.128.1.129	202.128.1.130- 202.128.1.169	-	202.128.1.190	202.128.1.170- 202.128.1.189
H2	202.128.1.193	202.128.1.194- 202.128.1.233	-	202.128.1.254	202.128.1.234- 202.128.1.253
I2	202.128.2.1	202.128.2.2- 202.128.2.41	-	202.128.2.62	202.128.2.42- 202.128.2.61
J2	202.128.2.65	-	202.128.2.66- 202.128.2.105	202.128.2.126	202.128.2.106- 202.128.2.125
K2	202.128.2.129	-	202.128.2.130- 202.128.2.169	202.128.2.190	202.128.2.170- 202.128.2.189

Технічна характеристика маршрутизатора Cisco ISR4331/K9

Тип пристроя	Маршрутизатор
Технологія доступу	Ethernet
Типи WAN-з'єднань	L2TP, PPPoE, PPTP, Динамічний IP, Статичний IP
Кількість LAN портів	3
Тип LAN портів	10/100/1000Base-TX(1000 мбит/с)
Наявність SFP (mini GBIC)	+
Кількість портів SFP (mini GBIC)	2
Максимальна швидкість передачі даних	1000 Мбіт/с
Протоколи Ethernet	IEEE 802.3, IEEE 802.3ab, IEEE 802.3u
Wi-Fi	-
Підтримка IPv6	+
Наявність USB портів	-
Підтримка 3G/4G модемів	-
Порт для SIM-карти	-
Підтримка IPTV	-
Підтримка PoE	-
Підтримка Auto-MDI/MDI-X	+
Об'єм оперативної пам'яті	4096 МБ
Об'єм Flash пам'яті	4096 МБ
Web-інтерфейс	+
Підтримка Telnet	+
NAT	+
DHCP-сервер	+
VPN	+
Колір	Чорний
Вага	6,2 кг

Технічна характеристика комутатора Cisco SF220-48

Особливості Cisco Catalyst 2960 Series:

- intelligent features (створення складних списків управління доступом, розширена безпека);
- порти подвійного призначення, що дозволяють використовувати підключення по мідній парі або оптоволокну, порти подвійного призначення має один 10/100/1000 Ethernet порт і один слот для модулів Small Form-Factor Pluggable (активним одночасно може бути тільки один порт).
- мережеве управління, оптимізація пропускної здатності використовуючи QoS, покроковий Rate Limiting, ACL та multicast services. Мережева безпека з використанням широкого діапазону методів ідентифікації, технологій кодування даних, та мережеве управління за користувачем, портом та MAC адресою. При використанні програмного забезпечення Cisco Network Assistant спрощується конфігурація, оновлення програмного забезпечення та пошук несправності. Комутатори Catalyst 2960 Series підтримують різні додаткові функції:
- підтримка передачі даних, бездротового та голосового зв'язку означає, що коли буде необхідність у розгортанні цих можливостей, буде єдина мережа, яка обслуговуватиме всі потреби підприємства;
- інтелектуальність полягає в можливості вказувати пріоритети для передачі голосу та обміну даними, щоб надання інформації відповідало потребам підприємства.
- поліпшений захист, а саме заборона незареєстрованим користувачам проникнути в мережу та забезпечте безперебійну роботу.
- надійність, а саме надання резервних джерела живлення для підвищення надійності.

Комутатор пропонує інтелектуальне керування трафіком, що забезпечує безперебійну роботу. Гнучкі механізми маркування, класифікації та планування забезпечують чудову продуктивність для передачі даних, голосу та відео та функціонування.

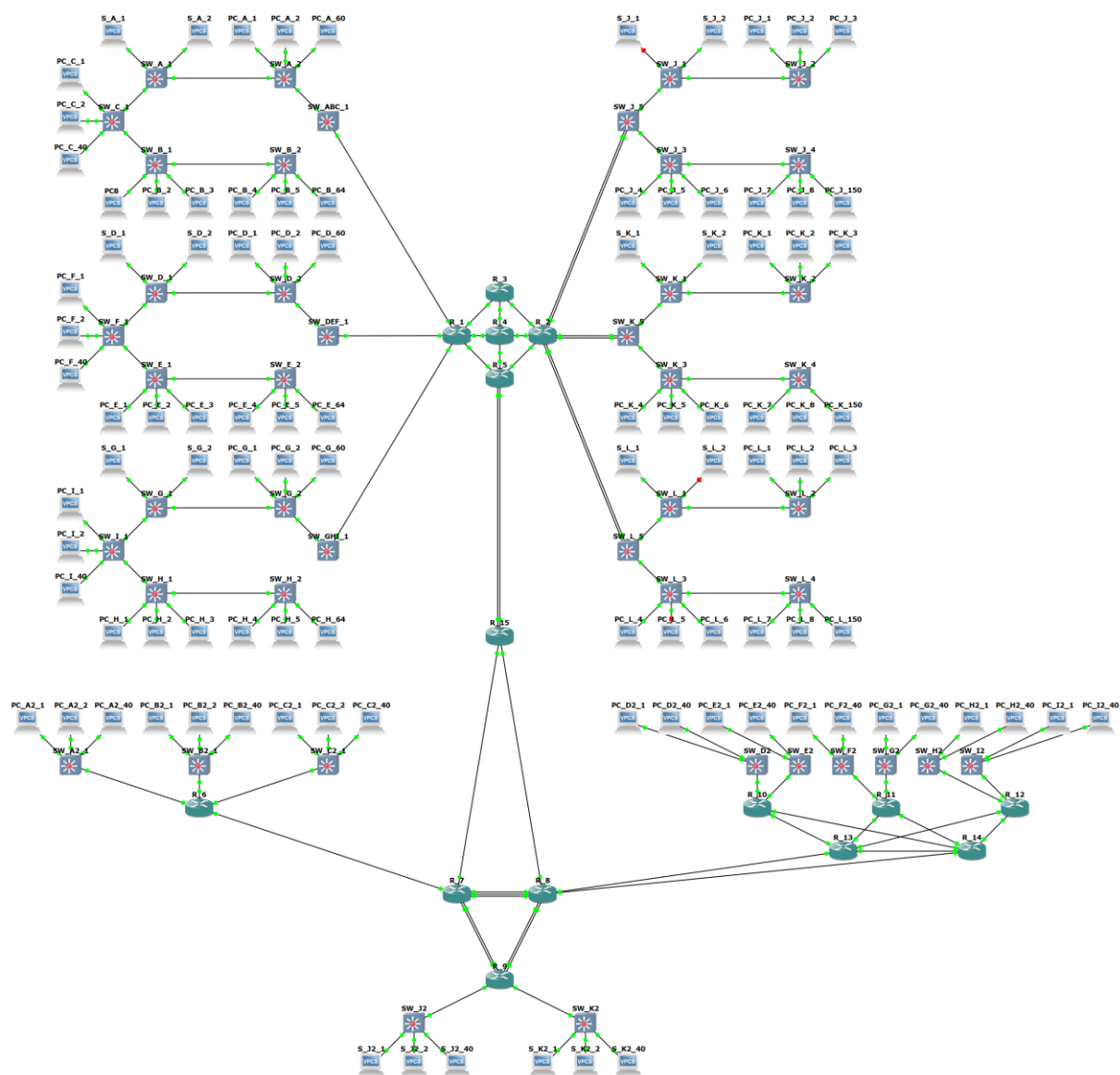
		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				64
Змн.	Арк.	№ докум.	Підпис	Дата		

Основні характеристики комутатора:

Тип пристроя	Комутатор
Виборник	Cisco
Тип комутатора	Керований 2 рівня
Тип портів	Fast Ethernet, Gigabit Ethernet
Загальна кількість портів	24 шт.
Швидкість LAN портів	100 Мбіт/с
Наявність бездротових можливостей	-
Наявність USB портів	-
Колір	Сірий
Вага	3,6 кг

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				65
Змн.	Арк.	№ докум.	Підпис	Дата		

Загальний схема мережі у середовищі GNS3



Русагинська А.О.

Єфіменко А.А.

Змн.

Арк.

№ докум.

Підпис

Дата

КІК.КР.Б – 123 – 19 – ПЗ

Арк.

66

Лістинг налаштування основних пристроїв

```

hostname R_1
interface FastEthernet0/1.10
encapsulation dot1Q 10
ip address 201.128.3.126 255.255.255.128
interface FastEthernet0/1.20
encapsulation dot1Q 20
ip address 201.128.3.254 255.255.255.128
interface FastEthernet0/1.30
encapsulation dot1Q 30
ip address 201.128.6.62 255.255.255.192
interface FastEthernet1/0.40
encapsulation dot1Q 40
ip address 201.128.4.126 255.255.255.128
interface FastEthernet1/0.50
encapsulation dot1Q 50
ip address 201.128.4.254 255.255.255.128
interface FastEthernet1/0.60
encapsulation dot1Q 60
ip address 201.128.6.126 255.255.255.192
interface FastEthernet2/0.70
encapsulation dot1Q 70
ip address 201.128.5.126 255.255.255.128
interface FastEthernet2/0.80
encapsulation dot1Q 80
ip address 201.128.5.254 255.255.255.128
interface FastEthernet2/0.90
encapsulation dot1Q 90

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				67
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip address 201.128.6.190 255.255.255.192
interface FastEthernet3/0
ip address 201.128.6.197 255.255.255.252
interface FastEthernet3/1
ip address 201.128.6.194 255.255.255.252
interface FastEthernet4/1
ip address 201.128.6.201 255.255.255.252
aaa group server tacacs+ Routers
server 201.128.3.63
!
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
action-type start-stop
group tacacs+
!
aaa accounting commands 15 default
action-type start-stop
group tacacs+
*****

hostname R_2
interface Port-channel1
description pc-swj5-r2
ip address 201.128.0.254 255.255.255.0
interface Port-channel2
description pc-swk5-r2
ip address 201.128.1.254 255.255.255.0

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Port-channel3
description pc-sw15-r2
ip address 201.128.2.254 255.255.255.0
interface FastEthernet0/0
ip address 201.128.6.206 255.255.255.252
interface FastEthernet0/1
ip address 201.128.6.222 255.255.255.252
interface FastEthernet1/0
ip address 201.128.6.213 255.255.255.252
ip route 0.0.0.0 0.0.0.0 201.128.6.205
ip route 0.0.0.0 0.0.0.0 201.128.6.214 5
ip route 0.0.0.0 0.0.0.0 201.128.6.221 6
aaa group server tacacs+ Routers
server 201.128.3.63
!
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
action-type start-stop
group tacacs+
!
aaa accounting commands 15 default
action-type start-stop
group tacacs+
*****

hostname R_3
interface FastEthernet0/0

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip address 201.128.6.205 255.255.255.252
interface FastEthernet0/1
ip address 201.128.6.209 255.255.255.252
interface FastEthernet3/1
ip address 201.128.6.193 255.255.255.252
ip route 201.128.3.0 255.255.255.0 201.128.6.194
ip route 201.128.4.0 255.255.254.0 201.128.6.194
ip route 201.128.6.0 255.255.255.128 201.128.6.194
ip route 201.128.6.128 255.255.255.192 201.128.6.194
ip route 201.128.0.0 255.255.254.0 201.128.6.206
ip route 201.128.2.0 255.255.255.0 201.128.6.206
ip route 201.128.3.0 255.255.255.0 201.128.6.210 5
ip route 201.128.4.0 255.255.254.0 201.128.6.210 5
ip route 201.128.6.0 255.255.255.128 201.128.6.210 5
ip route 201.128.6.128 255.255.255.192 201.128.6.210 5
ip route 201.128.0.0 255.255.254.0 201.128.6.210 5
ip route 201.128.2.0 255.255.255.0 201.128.6.210 5
ip route 201.128.6.196 255.255.255.252 201.128.6.210
ip route 201.128.6.196 255.255.255.252 201.128.6.194 5
ip route 201.128.6.212 255.255.255.252 201.128.6.210
ip route 201.128.6.212 255.255.255.252 201.128.6.206 5
ip route 201.128.6.216 255.255.255.252 201.128.6.210
ip route 201.128.6.216 255.255.255.252 201.128.6.194 5
ip route 201.128.6.200 255.255.255.252 201.128.6.194
ip route 201.128.6.200 255.255.255.252 201.128.6.210 5
ip route 201.128.6.220 255.255.255.252 201.128.6.206
ip route 201.128.6.220 255.255.255.252 201.128.6.210 5
!
ip route 202.128.0.0 255.255.255.128 201.128.6.210
ip route 202.128.0.128 255.255.255.192 201.128.6.210

```

		Русаїтинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip route 202.128.0.192 255.255.255.192 201.128.6.210
ip route 202.128.1.0 255.255.255.192 201.128.6.210
ip route 202.128.1.64 255.255.255.192 201.128.6.210
ip route 202.128.1.128 255.255.255.192 201.128.6.210
ip route 202.128.1.192 255.255.255.192 201.128.6.210
ip route 202.128.2.0 255.255.255.192 201.128.6.210
ip route 202.128.2.64 255.255.255.192 201.128.6.210
ip route 202.128.2.128 255.255.255.192 201.128.6.210
ip route 202.128.2.192 255.255.255.252 201.128.6.210
ip route 202.128.2.196 255.255.255.252 201.128.6.210
ip route 202.128.2.200 255.255.255.252 201.128.6.210
ip route 202.128.2.204 255.255.255.252 201.128.6.210
ip route 202.128.2.208 255.255.255.252 201.128.6.210
ip route 202.128.2.212 255.255.255.252 201.128.6.210
ip route 202.128.2.216 255.255.255.252 201.128.6.210
ip route 202.128.2.220 255.255.255.252 201.128.6.210
ip route 202.128.2.224 255.255.255.252 201.128.6.210
ip route 202.128.2.228 255.255.255.252 201.128.6.210
ip route 202.128.2.232 255.255.255.252 201.128.6.210
ip route 202.128.2.236 255.255.255.252 201.128.6.210
ip route 202.128.2.240 255.255.255.252 201.128.6.210
ip route 201.128.6.224 255.255.255.252 201.128.6.210
ip route 202.128.2.244 255.255.255.252 201.128.6.210
ip route 202.128.2.248 255.255.255.252 201.128.6.210
ip route 202.128.0.0 255.255.255.128 201.128.6.194 5
ip route 202.128.0.128 255.255.255.192 201.128.6.194 5
ip route 202.128.0.192 255.255.255.192 201.128.6.194 5
ip route 202.128.1.0 255.255.255.192 201.128.6.194 5
ip route 202.128.1.64 255.255.255.192 201.128.6.194 5
ip route 202.128.1.128 255.255.255.192 201.128.6.194 5

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip route 202.128.1.192 255.255.255.192 201.128.6.194 5
ip route 202.128.2.0 255.255.255.192 201.128.6.194 5
ip route 202.128.2.64 255.255.255.192 201.128.6.194 5
ip route 202.128.2.128 255.255.255.192 201.128.6.194 5
ip route 202.128.2.192 255.255.255.252 201.128.6.194 5
ip route 202.128.2.196 255.255.255.252 201.128.6.194 5
ip route 202.128.2.200 255.255.255.252 201.128.6.194 5
ip route 202.128.2.204 255.255.255.252 201.128.6.194 5
ip route 202.128.2.208 255.255.255.252 201.128.6.194 5
ip route 202.128.2.212 255.255.255.252 201.128.6.194 5
ip route 202.128.2.216 255.255.255.252 201.128.6.194 5
ip route 202.128.2.220 255.255.255.252 201.128.6.194 5
ip route 202.128.2.224 255.255.255.252 201.128.6.194 5
ip route 202.128.2.228 255.255.255.252 201.128.6.194 5
ip route 202.128.2.232 255.255.255.252 201.128.6.194 5
ip route 202.128.2.236 255.255.255.252 201.128.6.194 5
ip route 202.128.2.240 255.255.255.252 201.128.6.194 5
ip route 201.128.6.224 255.255.255.252 201.128.6.194 5
ip route 202.128.2.244 255.255.255.252 201.128.6.194 5
ip route 202.128.2.248 255.255.255.252 201.128.6.194 5
ip route 202.128.0.0 255.255.255.128 201.128.6.206 6
ip route 202.128.0.128 255.255.255.192 201.128.6.206 6
ip route 202.128.0.192 255.255.255.192 201.128.6.206 6
ip route 202.128.1.0 255.255.255.192 201.128.6.206 6
ip route 202.128.1.64 255.255.255.192 201.128.6.206 6
ip route 202.128.1.128 255.255.255.192 201.128.6.206 6
ip route 202.128.1.192 255.255.255.192 201.128.6.206 6
ip route 202.128.2.0 255.255.255.192 201.128.6.206 6
ip route 202.128.2.64 255.255.255.192 201.128.6.206 6
ip route 202.128.2.128 255.255.255.192 201.128.6.206 6

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip route 202.128.2.192 255.255.255.252 201.128.6.206 6
ip route 202.128.2.196 255.255.255.252 201.128.6.206 6
ip route 202.128.2.200 255.255.255.252 201.128.6.206 6
ip route 202.128.2.204 255.255.255.252 201.128.6.206 6
ip route 202.128.2.208 255.255.255.252 201.128.6.206 6
ip route 202.128.2.212 255.255.255.252 201.128.6.206 6
ip route 202.128.2.216 255.255.255.252 201.128.6.206 6
ip route 202.128.2.220 255.255.255.252 201.128.6.206 6
ip route 202.128.2.224 255.255.255.252 201.128.6.206 6
ip route 202.128.2.228 255.255.255.252 201.128.6.206 6
ip route 202.128.2.232 255.255.255.252 201.128.6.206 6
ip route 202.128.2.236 255.255.255.252 201.128.6.206 6
ip route 202.128.2.240 255.255.255.252 201.128.6.206 6
ip route 201.128.6.224 255.255.255.252 201.128.6.206 6
ip route 202.128.2.244 255.255.255.252 201.128.6.206 6
ip route 202.128.2.248 255.255.255.252 201.128.6.206 6
aaa group server tacacs+ Routers
server 201.128.3.63
!
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
action-type start-stop
group tacacs+
!
aaa accounting commands 15 default
action-type start-stop

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

group tacacs+

hostname R_4

interface FastEthernet0/0

ip address 201.128.6.217 255.255.255.252

interface FastEthernet0/1

ip address 201.128.6.210 255.255.255.252

interface FastEthernet1/0

ip address 201.128.6.214 255.255.255.252

interface FastEthernet3/0

ip address 201.128.6.198 255.255.255.252

ip route 201.128.3.0 255.255.255.0 201.128.6.197

ip route 201.128.4.0 255.255.254.0 201.128.6.197

ip route 201.128.6.0 255.255.255.128 201.128.6.197

ip route 201.128.6.128 255.255.255.192 201.128.6.197

ip route 201.128.0.0 255.255.254.0 201.128.6.213

ip route 201.128.2.0 255.255.255.0 201.128.6.213

ip route 201.128.3.0 255.255.255.0 201.128.6.209 5

ip route 201.128.4.0 255.255.254.0 201.128.6.209 5

ip route 201.128.6.0 255.255.255.128 201.128.6.209 5

ip route 201.128.6.128 255.255.255.192 201.128.6.209 5

ip route 201.128.0.0 255.255.254.0 201.128.6.209 5

ip route 201.128.2.0 255.255.255.0 201.128.6.209 5

ip route 201.128.3.0 255.255.255.0 201.128.6.218 6

ip route 201.128.4.0 255.255.254.0 201.128.6.218 6

ip route 201.128.6.0 255.255.255.128 201.128.6.218 6

ip route 201.128.6.128 255.255.255.192 201.128.6.218 6

ip route 201.128.0.0 255.255.254.0 201.128.6.218 6

ip route 201.128.2.0 255.255.255.0 201.128.6.218 6

ip route 201.128.6.192 255.255.255.252 201.128.6.209

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip route 201.128.6.192 255.255.255.252 201.128.6.197 5
ip route 201.128.6.204 255.255.255.252 201.128.6.209
ip route 201.128.6.204 255.255.255.252 201.128.6.213 5
ip route 201.128.6.200 255.255.255.252 201.128.6.218
ip route 201.128.6.200 255.255.255.252 201.128.6.197 5
ip route 201.128.6.220 255.255.255.252 201.128.6.218
ip route 201.128.6.220 255.255.255.252 201.128.6.213 5
!
ip route 202.128.0.0 255.255.255.128 201.128.6.218
ip route 202.128.0.128 255.255.255.192 201.128.6.218
ip route 202.128.0.192 255.255.255.192 201.128.6.218
ip route 202.128.1.0 255.255.255.192 201.128.6.218
ip route 202.128.1.64 255.255.255.192 201.128.6.218
ip route 202.128.1.128 255.255.255.192 201.128.6.218
ip route 202.128.1.192 255.255.255.192 201.128.6.218
ip route 202.128.2.0 255.255.255.192 201.128.6.218
ip route 202.128.2.64 255.255.255.192 201.128.6.218
ip route 202.128.2.128 255.255.255.192 201.128.6.218
ip route 202.128.2.192 255.255.255.252 201.128.6.218
ip route 202.128.2.196 255.255.255.252 201.128.6.218
ip route 202.128.2.200 255.255.255.252 201.128.6.218
ip route 202.128.2.204 255.255.255.252 201.128.6.218
ip route 202.128.2.208 255.255.255.252 201.128.6.218
ip route 202.128.2.212 255.255.255.252 201.128.6.218
ip route 202.128.2.216 255.255.255.252 201.128.6.218
ip route 202.128.2.220 255.255.255.252 201.128.6.218
ip route 202.128.2.224 255.255.255.252 201.128.6.218
ip route 202.128.2.228 255.255.255.252 201.128.6.218
ip route 202.128.2.232 255.255.255.252 201.128.6.218
ip route 202.128.2.236 255.255.255.252 201.128.6.218

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip route 202.128.2.240 255.255.255.252 201.128.6.218
ip route 201.128.6.224 255.255.255.252 201.128.6.218
ip route 202.128.2.244 255.255.255.252 201.128.6.218
ip route 202.128.2.248 255.255.255.252 201.128.6.218
ip route 202.128.0.0 255.255.255.128 201.128.6.202 5
ip route 202.128.0.128 255.255.255.192 201.128.6.202 5
ip route 202.128.0.192 255.255.255.192 201.128.6.202 5
ip route 202.128.1.0 255.255.255.192 201.128.6.202 5
ip route 202.128.1.64 255.255.255.192 201.128.6.202 5
ip route 202.128.1.128 255.255.255.192 201.128.6.202 5
ip route 202.128.1.192 255.255.255.192 201.128.6.202 5
ip route 202.128.2.0 255.255.255.192 201.128.6.202 5
ip route 202.128.2.64 255.255.255.192 201.128.6.202 5
ip route 202.128.2.128 255.255.255.192 201.128.6.202 5
ip route 202.128.2.192 255.255.255.252 201.128.6.202 5
ip route 202.128.2.196 255.255.255.252 201.128.6.202 5
ip route 202.128.2.200 255.255.255.252 201.128.6.202 5
ip route 202.128.2.204 255.255.255.252 201.128.6.202 5
ip route 202.128.2.208 255.255.255.252 201.128.6.202 5
ip route 202.128.2.212 255.255.255.252 201.128.6.202 5
ip route 202.128.2.216 255.255.255.252 201.128.6.202 5
ip route 202.128.2.220 255.255.255.252 201.128.6.202 5
ip route 202.128.2.224 255.255.255.252 201.128.6.202 5
ip route 202.128.2.228 255.255.255.252 201.128.6.202 5
ip route 202.128.2.232 255.255.255.252 201.128.6.202 5
ip route 202.128.2.236 255.255.255.252 201.128.6.202 5
ip route 202.128.2.240 255.255.255.252 201.128.6.202 5
ip route 201.128.6.224 255.255.255.252 201.128.6.202 5
ip route 202.128.2.244 255.255.255.252 201.128.6.202 5
ip route 202.128.2.248 255.255.255.252 201.128.6.202 5

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				77
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip route 202.128.0.0 255.255.255.128 201.128.6.221 6
ip route 202.128.0.128 255.255.255.192 201.128.6.221 6
ip route 202.128.0.192 255.255.255.192 201.128.6.221 6
ip route 202.128.1.0 255.255.255.192 201.128.6.221 6
ip route 202.128.1.64 255.255.255.192 201.128.6.221 6
ip route 202.128.1.128 255.255.255.192 201.128.6.221 6
ip route 202.128.1.192 255.255.255.192 201.128.6.221 6
ip route 202.128.2.0 255.255.255.192 201.128.6.221 6
ip route 202.128.2.64 255.255.255.192 201.128.6.221 6
ip route 202.128.2.128 255.255.255.192 201.128.6.221 6
ip route 202.128.2.192 255.255.255.252 201.128.6.221 6
ip route 202.128.2.196 255.255.255.252 201.128.6.221 6
ip route 202.128.2.200 255.255.255.252 201.128.6.221 6
ip route 202.128.2.204 255.255.255.252 201.128.6.221 6
ip route 202.128.2.208 255.255.255.252 201.128.6.221 6
ip route 202.128.2.212 255.255.255.252 201.128.6.221 6
ip route 202.128.2.216 255.255.255.252 201.128.6.221 6
ip route 202.128.2.220 255.255.255.252 201.128.6.221 6
ip route 202.128.2.224 255.255.255.252 201.128.6.221 6
ip route 202.128.2.228 255.255.255.252 201.128.6.221 6
ip route 202.128.2.232 255.255.255.252 201.128.6.221 6
ip route 202.128.2.236 255.255.255.252 201.128.6.221 6
ip route 202.128.2.240 255.255.255.252 201.128.6.221 6
aaa group server tacacs+ Routers
server 201.128.3.63
!
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				78
Змн.	Арк.	№ докум.	Підпис	Дата		

```

aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
  action-type start-stop
group tacacs+
!
aaa accounting commands 15 default
  action-type start-stop
group tacacs+
*****

hostname R_5
interface Port-channel1
ip address 201.128.6.226 255.255.255.252
interface FastEthernet0/0
ip address 201.128.6.218 255.255.255.252
interface FastEthernet0/1
ip address 201.128.6.221 255.255.255.252
interface FastEthernet4/1
ip address 201.128.6.202 255.255.255.252
!
ip route 201.128.3.0 255.255.255.0 201.128.6.201
ip route 201.128.4.0 255.255.254.0 201.128.6.201
ip route 201.128.6.0 255.255.255.128 201.128.6.201
ip route 201.128.6.128 255.255.255.192 201.128.6.201
ip route 201.128.0.0 255.255.254.0 201.128.6.222
ip route 201.128.2.0 255.255.255.0 201.128.6.222
ip route 201.128.3.0 255.255.255.0 201.128.6.217 5
ip route 201.128.4.0 255.255.254.0 201.128.6.217 5
ip route 201.128.6.0 255.255.255.128 201.128.6.217 5
ip route 201.128.6.128 255.255.255.192 201.128.6.217 5
ip route 201.128.0.0 255.255.254.0 201.128.6.217 5

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				79
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip route 201.128.2.0 255.255.255.0 201.128.6.217 5
ip route 201.128.6.196 255.255.255.252 201.128.6.217
ip route 201.128.6.196 255.255.255.252 201.128.6.201 5
ip route 201.128.6.212 255.255.255.252 201.128.6.217
ip route 201.128.6.212 255.255.255.252 201.128.6.222 5
ip route 201.128.6.208 255.255.255.252 201.128.6.217
ip route 201.128.6.208 255.255.255.252 201.128.6.222 5
ip route 201.128.6.192 255.255.255.252 201.128.6.201
ip route 201.128.6.192 255.255.255.252 201.128.6.217 5
ip route 201.128.6.204 255.255.255.252 201.128.6.222
ip route 201.128.6.204 255.255.255.252 201.128.6.217 5
ip route 202.128.0.0 255.255.255.128 201.128.6.225
ip route 202.128.0.128 255.255.255.192 201.128.6.225
ip route 202.128.0.192 255.255.255.192 201.128.6.225
ip route 202.128.1.0 255.255.255.192 201.128.6.225
ip route 202.128.1.64 255.255.255.192 201.128.6.225
ip route 202.128.1.128 255.255.255.192 201.128.6.225
ip route 202.128.1.192 255.255.255.192 201.128.6.225
ip route 202.128.2.0 255.255.255.192 201.128.6.225
ip route 202.128.2.64 255.255.255.192 201.128.6.225
ip route 202.128.2.128 255.255.255.192 201.128.6.225
ip route 202.128.2.192 255.255.255.252 201.128.6.225
ip route 202.128.2.196 255.255.255.252 201.128.6.225
ip route 202.128.2.200 255.255.255.252 201.128.6.225
ip route 202.128.2.204 255.255.255.252 201.128.6.225
ip route 202.128.2.208 255.255.255.252 201.128.6.225
ip route 202.128.2.212 255.255.255.252 201.128.6.225
ip route 202.128.2.216 255.255.255.252 201.128.6.225
ip route 202.128.2.220 255.255.255.252 201.128.6.225
ip route 202.128.2.224 255.255.255.252 201.128.6.225

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				80
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip route 202.128.2.228 255.255.255.252 201.128.6.225
ip route 202.128.2.232 255.255.255.252 201.128.6.225
ip route 202.128.2.236 255.255.255.252 201.128.6.225
ip route 202.128.2.240 255.255.255.252 201.128.6.225
ip route 202.128.2.244 255.255.255.252 201.128.6.225
ip route 202.128.2.248 255.255.255.252 201.128.6.225
aaa group server tacacs+ Routers
server 201.128.3.63
!
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
action-type start-stop
group tacacs+
!
aaa accounting commands 15 default
action-type start-stop
group tacacs+
*****

hostname R_6
interface FastEthernet0/0
ip address 202.128.0.62 255.255.255.192
interface FastEthernet0/1
ip address 202.128.0.126 255.255.255.192
interface FastEthernet1/0
ip address 202.128.0.190 255.255.255.192
interface FastEthernet1/1

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				81
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip address 202.128.2.194 255.255.255.252
router eigrp 1
network 202.128.0.0 0.0.0.63
network 202.128.0.64 0.0.0.63
network 202.128.0.128 0.0.0.63
network 202.128.2.192 0.0.0.3
passive-interface FastEthernet0/0
passive-interface FastEthernet0/1
passive-interface FastEthernet1/0
*****

hostname R_7
interface Port-channel1
description pc-r7-r9
ip address 202.128.2.202 255.255.255.252
interface Port-channel2
description pc-r7-r8
ip address 202.128.2.198 255.255.255.252
interface FastEthernet0/0
interface FastEthernet3/0
ip address 202.128.2.193 255.255.255.252
interface GigabitEthernet5/0
ip address 202.128.2.245 255.255.255.252
negotiation auto
router eigrp 1
network 202.128.2.192 0.0.0.3
network 202.128.2.196 0.0.0.3
network 202.128.2.200 0.0.0.3
network 202.128.2.244 0.0.0.3
aaa group server tacacs+ Routers
server 201.128.3.63

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				82
Змн.	Арк.	№ докум.	Підпис	Дата		

!

aaa authentication login default group tacacs+ local

aaa authorization console

aaa authorization config-commands

aaa authorization exec default group tacacs+ local

aaa authorization commands 15 default group tacacs+ local

aaa accounting exec default

action-type start-stop

group tacacs+

!

aaa accounting commands 15 default

action-type start-stop

group tacacs+

hostname R_8

interface Port-channel1

description pc-r8-r7

ip address 202.128.2.197 255.255.255.252

interface Port-channel2

description pc-r8-r9

ip address 202.128.2.205 255.255.255.252

interface FastEthernet3/0

ip address 202.128.2.214 255.255.255.252

interface FastEthernet3/1

ip address 202.128.2.218 255.255.255.252

interface GigabitEthernet6/0

ip address 202.128.2.249 255.255.255.252

router eigrp 1

network 202.128.2.196 0.0.0.3

network 202.128.2.204 0.0.0.3

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				83
Змн.	Арк.	№ докум.	Підпис	Дата		

```

network 202.128.2.212 0.0.0.3
network 202.128.2.216 0.0.0.3
network 202.128.2.248 0.0.0.3
aaa group server tacacs+ Routers
server 201.128.3.63
!
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
action-type start-stop
group tacacs+
!
aaa accounting commands 15 default
action-type start-stop
group tacacs+
*****
hostname R_9
interface Port-channel1
description pc-r9-r8
ip address 202.128.2.206 255.255.255.252
interface Port-channel2
description pc-r9-r7
ip address 202.128.2.201 255.255.255.252
interface FastEthernet0/0
channel-group 2
interface FastEthernet0/1
channel-group 2

```

		Русаїтинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				84
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface FastEthernet1/0
channel-group 1
interface FastEthernet1/1
channel-group 1
interface FastEthernet2/0
ip address 202.128.2.126 255.255.255.192
interface FastEthernet2/1
ip address 202.128.2.190 255.255.255.192
interface FastEthernet3/0
router eigrp 1
network 202.128.2.64 0.0.0.63
network 202.128.2.128 0.0.0.63
network 202.128.2.200 0.0.0.3
network 202.128.2.204 0.0.0.3
passive-interface FastEthernet2/0
passive-interface FastEthernet2/1
aaa group server tacacs+ Routers
server 201.128.3.63
!
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
action-type start-stop
group tacacs+
!
aaa accounting commands 15 default
action-type start-stop

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				85
Змн.	Арк.	№ докум.	Підпис	Дата		

```

group tacacs+
*****

hostname R_10
interface FastEthernet0/0
ip address 202.128.0.254 255.255.255.192
interface FastEthernet0/1
ip address 202.128.1.62 255.255.255.192
interface FastEthernet1/0
ip address 202.128.2.221 255.255.255.252
interface FastEthernet1/1
ip address 202.128.2.225 255.255.255.252
router eigrp 1
network 202.128.0.192 0.0.0.63
network 202.128.1.0 0.0.0.63
network 202.128.2.220 0.0.0.3
network 202.128.2.224 0.0.0.3
passive-interface FastEthernet0/0
passive-interface FastEthernet0/1
aaa group server tacacs+ Routers
server 201.128.3.63
!
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
action-type start-stop
group tacacs+
!
```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				86
Змн.	Арк.	№ докум.	Підпис	Дата		

```

aaa accounting commands 15 default
action-type start-stop
group tacacs+
*****

hostname R_11
interface FastEthernet0/0
ip address 202.128.1.126 255.255.255.192
interface FastEthernet0/1
ip address 202.128.1.190 255.255.255.192
interface FastEthernet1/0
ip address 202.128.2.229 255.255.255.252
interface FastEthernet1/1
ip address 202.128.2.233 255.255.255.252
router eigrp 1
network 202.128.1.64 0.0.0.63
network 202.128.1.128 0.0.0.63
network 202.128.2.228 0.0.0.3
network 202.128.2.232 0.0.0.3
passive-interface FastEthernet0/0
passive-interface FastEthernet0/1
aaa group server tacacs+ Routers
server 201.128.3.63
!
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
action-type start-stop

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				87
Змн.	Арк.	№ докум.	Підпис	Дата		

```

group tacacs+
!
aaa accounting commands 15 default
action-type start-stop
group tacacs+
*****

hostname R_12
interface FastEthernet0/0
ip address 202.128.1.254 255.255.255.192
interface FastEthernet0/1
ip address 202.128.2.62 255.255.255.192
interface FastEthernet1/0
ip address 202.128.2.237 255.255.255.252
interface FastEthernet1/1
ip address 202.128.2.241 255.255.255.252
router eigrp 1
network 202.128.1.192 0.0.0.63
network 202.128.2.0 0.0.0.63
network 202.128.2.236 0.0.0.3
network 202.128.2.240 0.0.0.3
passive-interface FastEthernet0/0
passive-interface FastEthernet0/1
aaa group server tacacs+ Routers
server 201.128.3.63
!
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				88
Змн.	Арк.	№ докум.	Підпис	Дата		

```

aaa accounting exec default
  action-type start-stop
  group tacacs+
!
aaa accounting commands 15 default
  action-type start-stop
  group tacacs+
*****

hostname R_13
interface FastEthernet0/0
ip address 202.128.2.222 255.255.255.252
interface FastEthernet0/1
ip address 202.128.2.230 255.255.255.252
interface FastEthernet1/0
ip address 202.128.2.238 255.255.255.252
interface FastEthernet1/1
ip address 202.128.2.209 255.255.255.252
interface FastEthernet2/0
ip address 202.128.2.213 255.255.255.252
router eigrp 1
network 202.128.2.208 0.0.0.3
network 202.128.2.212 0.0.0.3
network 202.128.2.220 0.0.0.3
network 202.128.2.228 0.0.0.3
network 202.128.2.236 0.0.0.3
aaa group server tacacs+ Routers
  server 201.128.3.63
!
aaa authentication login default group tacacs+ local
aaa authorization console

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				89
Змн.	Арк.	№ докум.	Підпис	Дата		

```

aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
  action-type start-stop
  group tacacs+
!
aaa accounting commands 15 default
  action-type start-stop
  group tacacs+
*****

hostname R_14
interface FastEthernet0/0
ip address 202.128.2.226 255.255.255.252
interface FastEthernet0/1
ip address 202.128.2.234 255.255.255.252
interface FastEthernet1/0
ip address 202.128.2.242 255.255.255.252
interface FastEthernet1/1
ip address 202.128.2.210 255.255.255.252
interface FastEthernet2/0
ip address 202.128.2.217 255.255.255.252
router eigrp 1
network 202.128.2.208 0.0.0.3
network 202.128.2.216 0.0.0.3
network 202.128.2.224 0.0.0.3
network 202.128.2.232 0.0.0.3
network 202.128.2.240 0.0.0.3
aaa group server tacacs+ Routers
server 201.128.3.63

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				90
Змн.	Арк.	№ докум.	Підпис	Дата		

!

aaa authentication login default group tacacs+ local

aaa authorization console

aaa authorization config-commands

aaa authorization exec default group tacacs+ local

aaa authorization commands 15 default group tacacs+ local

aaa accounting exec default

action-type start-stop

group tacacs+

!

aaa accounting commands 15 default

action-type start-stop

group tacacs+

hostname R_15

interface Port-channel1

ip address 201.128.6.225 255.255.255.252

interface GigabitEthernet3/0

no ip address

negotiation auto

channel-group 1

interface GigabitEthernet4/0

channel-group 1

interface GigabitEthernet5/0

ip address 202.128.2.246 255.255.255.252

interface GigabitEthernet6/0

ip address 202.128.2.250 255.255.255.252

router eigrp 1

network 201.128.6.224 0.0.0.3

network 202.128.2.244 0.0.0.3

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				91
Змн.	Арк.	№ докум.	Підпис	Дата		

```

network 202.128.2.248 0.0.0.3

redistribute static metric 1000 100 255 1 255

ip route 201.128.0.0 255.255.254.0 201.128.6.226
ip route 201.128.2.0 255.255.255.0 201.128.6.226
ip route 201.128.3.0 255.255.255.0 201.128.6.226
ip route 201.128.4.0 255.255.254.0 201.128.6.226
ip route 201.128.6.0 255.255.255.128 201.128.6.226
ip route 201.128.6.128 255.255.255.192 201.128.6.226
ip route 201.128.6.192 255.255.255.252 201.128.6.226
ip route 201.128.6.196 255.255.255.252 201.128.6.226
ip route 201.128.6.200 255.255.255.252 201.128.6.226
ip route 201.128.6.204 255.255.255.252 201.128.6.226
ip route 201.128.6.208 255.255.255.252 201.128.6.226
ip route 201.128.6.212 255.255.255.252 201.128.6.226
ip route 201.128.6.216 255.255.255.252 201.128.6.226
ip route 201.128.6.220 255.255.255.252 201.128.6.226
ip route 202.128.0.0 255.255.255.128 202.128.2.245
ip route 202.128.0.0 255.255.255.128 202.128.2.249 5
ip route 202.128.0.128 255.255.255.192 202.128.2.245
ip route 202.128.0.128 255.255.255.192 202.128.2.249 5
ip route 202.128.0.192 255.255.255.192 202.128.2.245
ip route 202.128.0.192 255.255.255.192 202.128.2.249 5
ip route 202.128.1.0 255.255.255.192 202.128.2.245
ip route 202.128.1.0 255.255.255.192 202.128.2.249 5
ip route 202.128.1.64 255.255.255.192 202.128.2.245
ip route 202.128.1.64 255.255.255.192 202.128.2.249 5
ip route 202.128.1.128 255.255.255.192 202.128.2.245
ip route 202.128.1.128 255.255.255.192 202.128.2.249 5
ip route 202.128.1.192 255.255.255.192 202.128.2.245
ip route 202.128.1.192 255.255.255.192 202.128.2.249 5

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				92
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip route 202.128.2.0 255.255.255.192 202.128.2.245
ip route 202.128.2.0 255.255.255.192 202.128.2.249 5
ip route 202.128.2.64 255.255.255.192 202.128.2.245
ip route 202.128.2.64 255.255.255.192 202.128.2.249 5
ip route 202.128.2.128 255.255.255.192 202.128.2.245
ip route 202.128.2.128 255.255.255.192 202.128.2.249 5
ip route 202.128.2.192 255.255.255.252 202.128.2.245
ip route 202.128.2.192 255.255.255.252 202.128.2.249 5
ip route 202.128.2.196 255.255.255.252 202.128.2.245
ip route 202.128.2.196 255.255.255.252 202.128.2.249 5
ip route 202.128.2.200 255.255.255.252 202.128.2.245
ip route 202.128.2.200 255.255.255.252 202.128.2.249 5
ip route 202.128.2.204 255.255.255.252 202.128.2.245
ip route 202.128.2.204 255.255.255.252 202.128.2.249 5
ip route 202.128.2.208 255.255.255.252 202.128.2.245
ip route 202.128.2.208 255.255.255.252 202.128.2.249 5
ip route 202.128.2.212 255.255.255.252 202.128.2.245
ip route 202.128.2.212 255.255.255.252 202.128.2.249 5
ip route 202.128.2.216 255.255.255.252 202.128.2.245
ip route 202.128.2.216 255.255.255.252 202.128.2.249 5
ip route 202.128.2.220 255.255.255.252 202.128.2.245
ip route 202.128.2.220 255.255.255.252 202.128.2.249 5
ip route 202.128.2.224 255.255.255.252 202.128.2.245
ip route 202.128.2.224 255.255.255.252 202.128.2.249 5
ip route 202.128.2.228 255.255.255.252 202.128.2.245
ip route 202.128.2.228 255.255.255.252 202.128.2.249 5
ip route 202.128.2.232 255.255.255.252 202.128.2.245
ip route 202.128.2.232 255.255.255.252 202.128.2.249 5
ip route 202.128.2.236 255.255.255.252 202.128.2.245
ip route 202.128.2.236 255.255.255.252 202.128.2.249 5

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				93
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip route 202.128.2.240 255.255.255.252 202.128.2.245
ip route 202.128.2.240 255.255.255.252 202.128.2.249 5
aaa group server tacacs+ Routers
server 201.128.3.63
!
aaa authentication login default group tacacs+ local
aaa authorization console
aaa authorization config-commands
aaa authorization exec default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default
action-type start-stop
group tacacs+
!
aaa accounting commands 15 default
action-type start-stop
group tacacs+

```

SW-A-1

```

interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
interface Ethernet0/1
switchport access vlan 10
switchport mode access
interface Ethernet1/1
switchport trunk encapsulation dot1q
switchport mode trunk
interface Ethernet1/2
switchport access vlan 10

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				94
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport mode access
interface Vlan10
ip address 201.128.3.2 255.255.255.128
ip default-gateway 201.128.3.126
*****

```

SW-A-2

```

interface Ethernet0/0
switchport access vlan 10
switchport mode access
interface Ethernet0/3
switchport access vlan 10
switchport mode access
interface Ethernet1/1
switchport trunk encapsulation dot1q
switchport mode trunk
interface Ethernet1/2
switchport access vlan 10
switchport mode access
interface Ethernet1/3
switchport trunk encapsulation dot1q
switchport mode trunk
interface Vlan10
ip address 201.128.3.1 255.255.255.128
ip default-gateway 201.128.3.126
*****

```

SW-C-1

```

interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
interface Ethernet0/1

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				95
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport trunk encapsulation dot1q
switchport mode trunk
interface Ethernet0/2
switchport access vlan 30
switchport mode access
interface Ethernet0/3
switchport access vlan 30
switchport mode access
interface Ethernet1/0
switchport access vlan 30
switchport mode access
interface Vlan30
ip address 201.128.6.1 255.255.255.192
ip default-gateway 201.128.3.254

```

SW-B-1

```

interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20,30
switchport mode trunk
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10,20,30
switchport mode trunk
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet1/0
interface Ethernet1/1
switchport access vlan 20
switchport mode access

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				96
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Ethernet1/2
switchport access vlan 20
switchport mode access
interface Ethernet1/3
switchport access vlan 20
switchport mode access
interface Vlan20
ip address 201.128.3.129 255.255.255.128
ip default-gateway 201.128.3.254

```

```

SW-B-2
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
interface Ethernet1/1
switchport access vlan 20
switchport mode access
interface Ethernet1/2
switchport access vlan 20
switchport mode access
interface Ethernet1/3
switchport access vlan 20
switchport mode access

```

```

SW-D-1
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 40,50,60
switchport mode trunk
interface Ethernet0/1

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				97
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport access vlan 40
switchport mode access
interface Ethernet1/0
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 40,50,60
switchport mode trunk
interface Ethernet1/2
switchport access vlan 40
switchport mode access
interface Vlan40
ip address 201.128.4.2 255.255.255.128
ip default-gateway 201.128.4.254
*****

```

```

SW-D-2
interface Ethernet0/0
switchport access vlan 40
switchport mode access
interface Ethernet0/3
switchport access vlan 40
switchport mode access
interface Ethernet1/0
switchport trunk encapsulation dot1q
switchport mode trunk
interface Ethernet1/2
switchport access vlan 40
switchport mode access
interface Ethernet1/3
switchport trunk encapsulation dot1q
switchport mode trunk
*****

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				98
Змн.	Арк.	№ докум.	Підпис	Дата		

SW-F-1

interface Ethernet0/0

switchport trunk encapsulation dot1q

switchport mode trunk

interface Ethernet0/1

switchport trunk encapsulation dot1q

switchport mode trunk

interface Ethernet0/2

switchport access vlan 60

switchport mode access

interface Ethernet0/3

switchport access vlan 60

switchport mode access

interface Ethernet1/0

switchport access vlan 60

switchport mode access

SW-E-1

interface Ethernet0/0

switchport trunk encapsulation dot1q

switchport mode trunk

interface Ethernet0/1

switchport trunk encapsulation dot1q

interface Ethernet1/0

switchport trunk encapsulation dot1q

switchport mode trunk

interface Ethernet1/1

switchport access vlan 50

switchport mode access

interface Ethernet1/2

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				99
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport access vlan 50
switchport mode access
interface Ethernet1/3
switchport access vlan 50
switchport mode access
interface Vlan50
ip address 201.128.4.129 255.255.255.128
ip default-gateway 201.128.4.254

```

```

SW-E-2
interface Ethernet1/0
switchport trunk encapsulation dot1q
switchport mode trunk interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
duplex auto
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
interface Ethernet0/2
switchport access vlan 90
switchport mode access
interface Ethernet0/3
switchport access vlan 90
switchport mode access
interface Ethernet1/0
switchport access vlan 90
switchport mode access
interface Vlan90
ip address 201.128.6.129 255.255.255.192

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				100
Змн.	Арк.	№ докум.	Підпис	Дата		

!

```
ip default-gateway 201.128.6.190
```

```
interface Ethernet1/1
```

```
switchport access vlan 50
```

```
switchport mode access
```

```
interface Ethernet1/2
```

```
switchport access vlan 50
```

```
switchport mode access
```

```
interface Ethernet1/3
```

```
switchport access vlan 50
```

```
switchport mode access
```

```
interface Vlan50
```

```
ip address 201.128.4.130 255.255.255.128
```

```
ip default-gateway 201.128.4.254
```

SW-G-1

```
nterface Ethernet0/0
```

```
switchport trunk encapsulation dot1q
```

```
switchport mode trunk
```

```
interface Ethernet0/1
```

```
switchport access vlan 70
```

```
switchport mode access
```

```
interface Ethernet1/0
```

```
switchport trunk encapsulation dot1q
```

```
switchport mode trunk
```

```
interface Ethernet1/2
```

```
switchport access vlan 70
```

```
switchport mode access
```

```
interface Vlan70
```

```
ip address 201.128.5.2 255.255.255.128
```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				101
Змн.	Арк.	№ докум.	Підпис	Дата		

ip default-gateway 201.128.5.126

*****SW-G-2

interface Ethernet0/0

switchport access vlan 70

switchport mode access

interface Ethernet0/3

switchport access vlan 70

switchport mode access

interface Ethernet1/0

switchport trunk encapsulation dot1q

switchport mode trunk

interface Ethernet1/2

switchport access vlan 70

switchport mode access

interface Ethernet1/3

switchport trunk encapsulation dot1q

switchport mode trunk

interface Vlan70

ip address 201.128.5.1 255.255.255.128

ip default-gateway 201.128.5.126

SW-I-1

interface Ethernet0/0

switchport trunk encapsulation dot1q

switchport mode trunk

interface Ethernet0/1

switchport trunk encapsulation dot1q

switchport mode trunk

interface Ethernet0/2

switchport access vlan 90

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				102
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport mode access
interface Ethernet0/3
switchport access vlan 90
switchport mode access
interface Ethernet1/0
switchport access vlan 90
switchport mode access
interface Vlan90
ip address 201.128.6.129 255.255.255.192
ip default-gateway 201.128.6.190

```

```

SW-H-1
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
interface Ethernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
interface Ethernet1/1
switchport access vlan 80
switchport mode access
interface Ethernet1/2
switchport access vlan 80
switchport mode access
interface Ethernet1/3
switchport access vlan 80
switchport mode access
interface Vlan80
ip address 201.128.5.129 255.255.255.128
ip default-gateway 201.128.5.254

```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				103
Змн.	Арк.	№ докум.	Підпис	Дата		

SW-H-2

```
interface Ethernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
interface Ethernet1/1
switchport access vlan 80
switchport mode access
interface Ethernet1/2
switchport access vlan 80
switchport mode access
interface Ethernet1/3
switchport access vlan 80
switchport mode access
interface Vlan80
ip address 201.128.5.130 255.255.255.128
ip default-gateway 201.128.5.254
```

SW-J-1

```
interface Vlan1
ip address 201.128.0.5 255.255.255.0
ip default-gateway 201.128.0.254
```

SW-J-2

```
interface Vlan1
ip address 201.128.0.2 255.255.255.0
ip default-gateway 201.128.0.254
```

SW-J-3

```
interface Vlan1
```

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				104
Змн.	Арк.	№ докум.	Підпис	Дата		

ip address 201.128.0.3 255.255.255.0

ip default-gateway 201.128.0.254

SW-J-4

interface Vlan1

ip address 201.128.0.3 255.255.255.0

ip default-gateway 201.128.0.254

		Русятинська А.О.			КІК.КР.Б – 123 – 19 – ПЗ	Арк.
		Єфіменко А.А.				105
Змн.	Арк.	№ докум.	Підпис	Дата		