Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра радіотехніки та телекомунікацій
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
магістра
(ступінь вищої освіти)

на тему **ПРОЕКТУВАННЯ ВІДМОВОСТІЙКОЇ, З МОЖЛИВІСТЮ МАСШТАБУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ КАФЕДРИ РТТ**

Виконав: студент 2 курсу, групи БК-912м

Спеціальності

172 «Телекомунікації та радіотехніка»
(код і найменування спеціальності)

Освітня програма (спеціалізація)

«Інформаційні мережі зв'язку»

ЗУЄВ Даніїл Володимирович
(прізвище та ініціали)

Керівник МОРЩАВКА С.В.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

2023 рік

Форма № 25

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування закладу вищої освіти)

Факультет *Інформаційної безпеки та електронних комунікацій*
Кафедра *Радіотехніки та телекомунікацій*
Ступінь вищої освіти *магістр*
Спеціальність *172 «Телекомунікації та радіотехніка»*
(код і найменування)
Освітня програма (спеціалізація) *Інформаційні мережі зв'язку*
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри *РТТ*
к.ф.-м.н., доц. Сергій САМОЙЛИК
«_____» грудня 2023 року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА

ЗУЄВУ Даніілу Володимировичу
(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи *Проектування відмовостійкої, з можливістю масштабування комп'ютерної мережі для кафедри РТТ*
керівник проєкту (роботи) *к.т.н., доц. МОРЩАВКА Сергій Володимирович*
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові,)
затверджені наказом закладу вищої освіти від *14 листопада 2023* року №*443*
2. Строк подання студентом проєкту (роботи) *15 грудня 2023 року*
3. Вихідні дані до проєкту (роботи) *Здійснити моделювання комп'ютерної мережі кафедри РТТ*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) *Розробити та змоделювати відмовостійкі кластери L3 комутаторів, міжмережевих екранів ASA та VoIP телефонії.*

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Презентація роботи в Microsoft PowerPoint

6. Консультанти розділів проєкту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1-9	*МОРЩАВКА С.В., к.т.н., доцент, доцент каф. РТТ*		
	МОРОЗ Г.В., ст. викладач каф. РТТ		
Нормоконт-роль	*МОРОЗ Г.В., ст. викладач каф. РТТ*		

7. Дата видачі завдання «*05*» *вересня* *2023* року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	*Огляд літератури та постановка задачі*	*2 тижні*	*виконано*
2	*Вибір необхідного обладнання під різні задачи*	*3 тижні*	*виконано*
3	*Налаштування L2 комутаторів та кінцевих пристроїв*	*1 тижні*	*виконано*
4	*Розробка відмовостійкого кластеру L3 комутаторів*	*2 тиждень*	*виконано*
5	*Розробка відмовостійкого кластеру міжмережевих екранів*	*1 тиждень*	*виконано*
6	*Розробка відмовостійкого кластеру VoIP телефонії*	*1 тиждень*	*виконано*
7	*Тестування макету мережі*	*1 тиждень*	*виконано*
8	*Оформлення ПЗ і презентації*	*1 тиждень*	*виконано*
9	*Захист роботи*	*1 день*	*виконано*

Студент (ка) _____ *Даніїл ЗУЄВ*
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ *Сергій МОРЩАВКА*
(підпис) (Ім'я ПРІЗВИЩЕ)

РЕФЕРАТ

Пояснювальна записка до магістерської роботи: 85 с., 8 табл., 38 рис., 11 джерел.

КОНСОЛЬНИЙ ПОРТ, ТОПОЛОГІЯ, ІНТЕРФЕЙС, КОМУТАТОР, ЛОКАЛЬНА МЕРЕЖА, ПРОТОКОЛ, МАРШРУТИЗАТОР.

Створення комп'ютерних мереж визначається практичною необхідністю забезпечення взаємодії користувачів, які розташовані на віддалених пристроях, в обміні інформацією та спільній роботі над загальними проектами. Мережі відкривають широкі можливості для оперативного обміну даними та спільної взаємодії з різноманітними кінцевими пристроями.

Для відповідності потребам кафедри «Радіотехніка та телекомунікації» (РТТ) була розроблена локальна мережа, яка має забезпечити ефективний та швидкий обмін даними між всіма підключеними пристроями та забезпечити доступ до глобальної мережі.

Створення мережі включає в себе використання різноманітних елементів, спрямованих на оптимізацію процесу передачі даних. До необхідних елементів входять комутатори для швидкого і ефективного пересилання інформації, міжмережеві екрани для забезпечення безпеки даних, сервери для зберігання та обробки інформації, а також точки доступу, які дозволяють бездротовий доступ до мережі.

Створення мережі локального рівня є важливим етапом для підвищення продуктивності та зручності роботи співробітників та студентів, які використовують різноманітні комп'ютерні ресурси для досягнення своїх професійних та навчальних цілей.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

DHCP	–	(Dynamic Host Configuration Protocol) протокол динамічної конфігурації хоста
HSRP	–	(Hot Standby Router Protocol) протокол високої доступності маршрутизатора
LAN	–	(Local Area Network) локальна мережа
Local Area Network	–	віртуальна локальна мережа
NAT	–	(Network Address Translation) трансляція мережевих адрес
OSPF	–	(Open Shortest Path First) – протокол динамічної маршрутизації
RSTP	–	(Rapid Spanning Tree Protocol) – швидкий протокол кістякового дерева
SIP	–	(Session Initiation Protocol) протокол ініціювання сеансів
VPN	–	(Virtual Private Network) – віртуальна приватна мережа
VTP	–	(VLAN Trunking Protocol) – протокол переносу VLAN
WAN	–	(Wide Area Network) – глобальна мережа

ВСТУП

Архітектура комп’ютерної мережі для кафедри визначається застосуванням різноманітних мережевих пристроїв, які оптимізують ефективність та безпеку зв’язку. Однією з основних складових цієї мережі є L2 комутатор [1], що працює на канальному рівні семирівневої моделі OSI і використовує MAC-адреси для адресації. Приєднання великої кількості кінцевих пристроїв до L2 комутатора дозволяє забезпечити швидкий та надійний обмін даними в локальній мережі.

Для оптимізації і розширення мережі було використано L3 комутатори, які фактично є маршрутизаторами. Вони реалізують механізми маршрутизації, використовуючи логічну адресацію та вибір шляху для доставки даних. Завдяки великій пропускній здатності L3 комутатори [2] дозволяють ефективно об’єднувати багато L2 комутаторів в єдину інфраструктуру.

Для забезпечення доступу до глобальної мережі використовується міжмережевий екран, основною функцією якого є ефективний захист інформації в локальній мережі. Міжмережевий екран служить бар’єром для зовнішніх загроз і забезпечує безпеку даних під час обміну інформацією із глобальною мережею.

Важливою частиною роботи є використання програмного забезпечення Cisco Packet Tracer та EVE-NG, що дозволяє моделювати та тестувати мережеві конфігурації перед їх впровадженням у реальному середовищі. Це сприяє оптимізації роботи та забезпеченню найвищої ефективності комп’ютерної інфраструктури. Топології мереж двох програм дещо відрязняється, так Cisco Packet Tracer використовується для симуляції більш простих пристроїв через обмежений функціонал, а саме L2 та L3 комутаторів. В той час EVE-NG потрібен для емуляції міжмережевих екранів та L3 комутаторів, на яких в повній мірі доступні усі налаштування. Топологія

мережі Cisco Packet Tracer зображена на рисунку 1, а топологія мережі EVE-NG на рисунку 2.

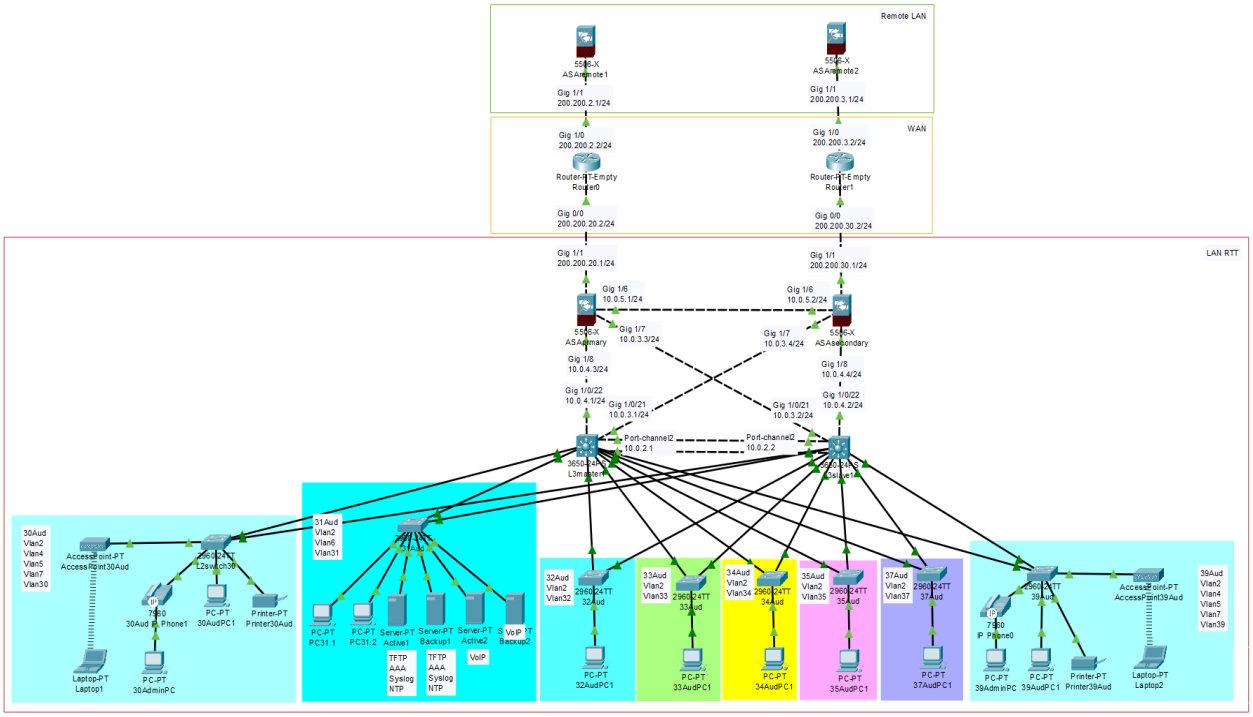

Рисунок 1 – Топологія локальної мережі побудована в Cisco Packet Tracer

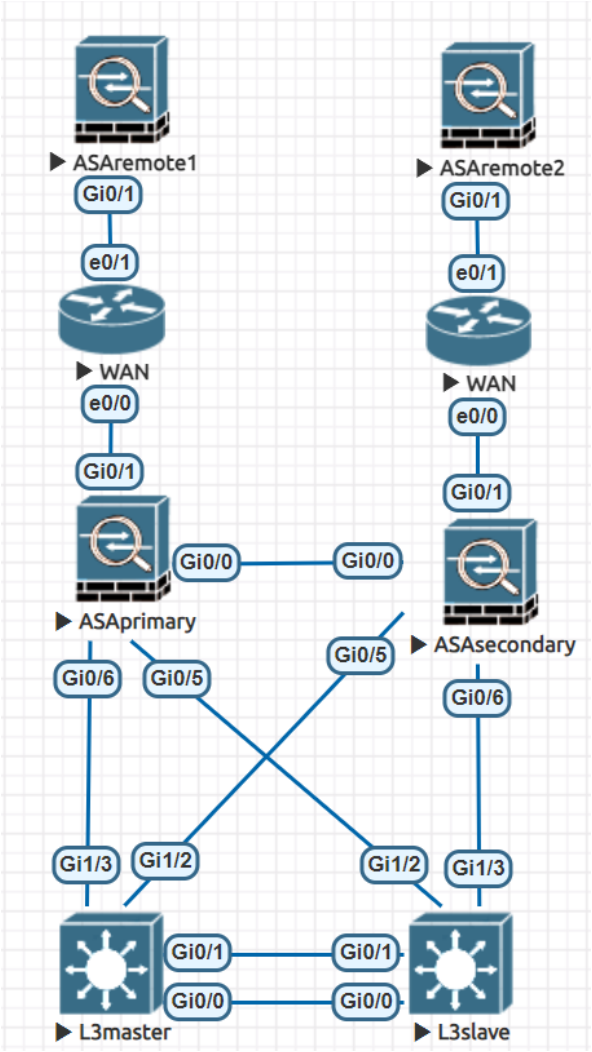

Рисунок 2 – Топологія локальної мережі побудованої в EVE-NG

1 ПРОЕКТУВАННЯ LAN

LAN – мережа, яка об’єднує комп’ютери та інші пристрої в обмеженій географічній області, такій як офіс, будинок, навчальний заклад чи компанія. Це робить LAN ефективним рішенням для внутрішньоорганізаційного зв’язку та обміну даними, ресурсами і послугами між різними пристроями в обмеженому просторі.

При проектуванні LAN були враховані наступні базові компоненти, які дозволили створити повноцінну локальну мережу:

а) комп’ютери та пристрої, серед яких робочі станції, ноутбуки, сервери, принтери, телефони, планшети та інші кінцеві пристрої, які підключені до локальної мережі;

б) мережеве обладнання LAN складається з комутаторів різних рівнів (switches L2, L3), міжмережевих екрани (Firewall) та точок доступу Wi-Fi;

в) сабелі та бездротові технології необхідні для підключення кінцевих пристроїв та мережевого обладнання за допомогою використання стандартів Ethernet і технологій на основі IEEE 802.11 (WI-FI). Ethernet використано для усіх мережевих пристроїв та комп’ютерів із переферійним обладнанням через стабільність та надійність сигналу в поєднанні із високою швидкістю передачі даних коли WI-FI використовується будь-якими пристроями що його підтримують;

г) мережеві протоколи є невідмінною частиною будь-якої комп’ютерної мережі і виконують ключові функції, які забезпечують ефективну та надійну комунікацію між пристроями в мережі. Серед протоколів важливо виділити TCP/IP, який є основним для будь-яких мереж та інтернету вцілому;

д) безпека мережі включає ряд заходів від встановлення та налаштування Firewall до антивірусного захисту кожного кінцевого пристрою окремо. Виділити окремо потрібно використання механізмів аутентифікації та шифрування даних, які є пріоритетом у питаннях безпеки мережі в цілому.

1.1 Обладнання

Для реалізації запропонованої локальної мережі необхідно використати багато пристроїв, серед них: вісім комутаторів другого рівня (Layer 2) Cisco Catalyst 2960 [3] (різних конфігурацій в залежності від аудиторії), два комутатори третього рівня (Layer 3) Cisco Catalyst 3650, два міжмережевих екрани Cisco Asa 5525-X, дві бездротові точки доступу для забезпечення Wi-Fi доступу (Cisco серії Aironet або будь-яка інша), чотири фізичні сервери для виконання різних задач, кабельна інфраструктура (роз'єми, панелі підключення, розподільчі панелі та інші елементи, які використовуються для створення мережевого з'єднання). За необхідності можливо використати джерела безперебійного живлення UPS.

2 ТОПОЛОГІЯ 30 ТА 39 АУДИТОРІЇ

Мережа 30 аудиторії є частиною рівня доступу (access layer) в ієрархічній моделі мережі Cisco, основною функцією якого є підключення кінцевих пристроїв до коммутатора L2. Рівень доступу виконує і ряд інших важливих функцій: комутація рівня 2, висока доступність (High Availability), безпека портів (Port security), класифікація та маркування QoS, списки контролю доступу (ACL), кістякове дерево (Spanning tree).

Кінцеві пристрої, такі як комп'ютери, принтери, телефони та інші зазвичай підключаються до локальної мережі за допомогою L2 комутаторів, тому основою локальної мережі 30 аудиторії стане Cisco Catalyst 2960-24TT-L [3] на 24 порти Fast Ethernet (10/100 Mbps) та 2 порти Gigabit Ethernet (10/100/1000 Mbps). У ролі кінцевих пристроїв виступають звичайні комп'ютери, точка доступу, IP-телефон та принтер. Їх з'єднання із комутатором відбувається за допомогою стандарту FastEthernet (IEEE 802.3u) та кабелю UTP 5 (CAT 5). Підключення комутатору до рівня розподілу відбувається за стандартом GigabitEthernet (IEEE 802.3ab) та кабелю UTP 5e (CAT 5e).

Топології окремих аудиторій реалізовані та розглянуті в програмному додатку Cisco Packet Tracer через достатню функціональність для налаштування необхідних функцій L2 комутаторів та простих мережевих пристроїв. Топологія 30 аудиторії зображена на рисунку 2.1.

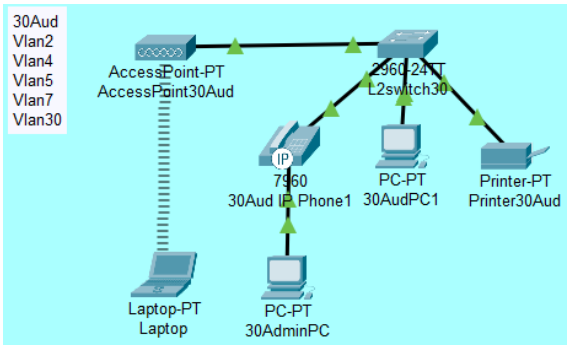

Рисунок 2.1 – Топологія мережі 30 аудиторії

2.1 Налаштування L2 комутатора 30 аудиторії

L2Switch – пристрій для комутації даних на другому рівні моделі OSI. Комутатор другого рівня став стандартом для LAN з кількох ключових причин, серед яких: ефективність комутації (комутація за допомогою MAC-адрес лише до портів призначення), розділення доменів колізії, підтримка VLAN та ефективності керування багатьма одночасними обмінами даних. Ці характеристики роблять L2 комутатор ефективним та надійним рішенням для локальних мереж, де ефективність та продуктивність є ключовими факторами.

2.1.1 Консольний порт

Консольний порт (Console port) – фізичний порт, який використовується для підключення до комутатора за допомогою спеціального консольного кабелю та термінальної програми (PuTTY для Windows або Terminal для macOS та Linux). З одного боку він має роз'єм RJ45, а з іншого роз'єм DB9 або USB. Цей порт дозволяє адміністратору взаємодіяти з комутатором для налаштування, моніторингу та діагностики. Через нього і буде відбуватися початкове налаштування усіх мережевих пристроїв.

Налаштування паролю для консольного порту є важливим елементом безпеки, що захистить від несанкціонованого доступу. Налаштовуємо Console port на L2switch30 наступним чином:

Задаємо пароль для консольного доступу до мережевого пристрою:

switch(config)# line console 0

switch(config-line)# password Y3zxKa79

Встановлюємо вимогу автентифікації при вході:

switch(config-line)# login

Визначаємо час допустимої бездіяльності та автоматичного відключення на 5 хвилин і 0 секунд:

switch(config-line)# exec-timeout 5 0

Обмежуємо кількості невірних спроб входу після 3 на 5 хвилин:

switch(config-line)# login block-for 5 attempts 3

2.1.2 Ім’я L2 комутатора

Зміна стандартного імені комутатора вирішує ряд важливих питань, а саме:

а) безпека, де зміна стандартного імені зробить мережу менш вразливою до атак, оскільки зловмисники часто використовують стандартні імена для виявлення конкретних моделей пристроїв та їх вразливостей;

б) полегшене управління та адміністрування мережою вцілому завдяки іменам, які відображають місце розташування чи функціональність пристрою та допомагають у налаштуванні моніторингу та відладці проблем де ім’я комутатора може бути корисним при аналізі журналів подій (logs).

У проектованій локальній мережі ім’я кожного мережевого містить його тип, місце розташування або призначення для легшої ідентифікації при пошуку проблем або для додаткових налаштувань. Наприклад L2 комутатор 30 аудиторії має ім’я L2switch30 а основний L3 комутатор L3master.

На більшості мережевих пристроїв Cisco зміна стандартного імені пристрою виконується за допомогою команди hostname в конфігураційному режимі:

Switch(config)# hostname L2switch30

L2switch30(config)#

2.1.3 VLAN’и на L2 комутаторі

VLAN (Virtual LAN або Віртуальна Локальна Мережа) [1] – технологія що дозволяє розділити одну фізичну локальну мережу на кілька логічних сегментів, які знаходяться в різних фізичних мережах. Використовуючи VLAN буде створено кілька незалежних мережевих сегментів на одному комутаторі L2. Створення багатьох VLAN у локальній мережі надає важливі переваги і буде використовуватися для досягнення наступних цілей:

а) розділення трафіку – VLAN дозволить об’єднати пристрої в один сегмент мережі, незалежно від їх фізичного розташування, так для ком’ютерів адміністраторів що знаходяться в різних аудиторіях використано окремий VLAN;

б) безпека – VLAN можуть служити для ізоляції трафіку між різними частинами мережі, що може покращити безпеку та уникнути несанкціонованого доступу до чутливої інформації (наприклад доступу із комп’ютера користувача до серверу даних);

в) оптимізація Пропускної Здатності – розділення трафіку на різні VLAN може покращити пропускну здатність мережі та зменшить широкомовний (broadcast) трафік;

г) управління Мережею – VLAN можуть спростити адміністрування мережі, оскільки дозволяють легко змінювати конфігурацію мережі, розміщуючи пристрої відповідно до логічних груп. Кожна аудиторія має окремий VLAN відповідно до її назви і використовує його для кінцевих пристрів користувачів, тому за необхідності можливо керувати усім трафіком одразу.

Усі вищеперераховані переваги актуальні і для Voice VLAN, що буде використовуватися для розділення трафіку VoIP і даних LAN. Основна мета – забезпечити якісну передачу голосу та уникнути затримок чи втрати пакетів, які можуть впливати на якість голосового зв’язку.

У 30 аудиторії використано 5 VLAN’ів, частина з яких буде зустрічатися в інших частинах LAN. VLAN2 завжди присутній на L2 комутаторах і необхідний віддаленого доступу, VLAN4 належить комп’ютерам адміністраторів, VLAN5 належить до access point’ів а VLAN7 необхідний для IP-телефонів. VLAN30 використовується лише в 30 аудиторії і необхідний для персональних комп’ютерів.

Кожен VLAN має своє ім’я для полегшення розуміння функції та призначення конкретного віртуального локального мережевого сегменту. Це допоможе адміністраторам та інженерам легко ідентифікувати призначення

кожного VLAN та спрощує розуміння мережевої топології одночасно зробивши її керування більш зручним. Повний перелік VLAN'ів що були використані у 30 аудиторії наведені у таблиці 2.1.

Таблиця 2.1 – VLAN'и 30 аудиторії та інтерфейси, на яких вони налаштовані

Номер VLAN	Ім'я VLAN	Призначення VLAN	interfas'и прив'язані до VLAN
vlan 2	L2switchVLAN	Віддалений доступ	Vlan2
vlan 4	adminVLAN	комп'ютер адміністратора	fastEthernet 0/20
vlan 5	wifiVLAN	access point	fastEthernet 0/22
vlan 7	voiceVLAN	IP-телефон	fastEthernet 0/20
vlan 30	30Aud	кінцеві пристрої 30 аудиторії	fastEthernet 0/1-19

Налаштовуємо VLAN'и на L2switch30 відповідно до таблиці 1. Вибираємо необхідний VLAN і задаємо ім'я відповідно до призначення:

L2switch30(config)# vlan 2

L2switch30(config-vlan)# name L2switchVLAN

Налаштовуємо аналогічно інші VLAN.

Зберігаємо поточну конфігурацію у пам'яті пристрою командою write memory. Це дозволить зберегти всі внесені зміни і забезпечити їх виконання навіть після перезавантаження пристрою.

L2switch30# write memory

2.1.4 Налаштування інтерфейсів

На комутаторах інтерфейс – фізично або логічно з'єднаний порт, через який комутатор "спілкується" з іншими пристроями у мережі. Інтерфейси на комутаторі мають кілька режимів роботи і майже усі були використані в локальній мережі:

а) Access Mode (режим доступу) – у цьому режимі інтерфейс призначається певному VLAN, і всі пакети, які надходять через цей інтерфейс, автоматично відносяться до цього VLAN. Це використовується для пристроїв, які не підтримують VLAN tagging;

б) Trunk Mode (режим магістралі) – у цьому режимі інтерфейс може передавати дані для декількох VLAN одночасно, використовуючи технологію VLAN tagging. Використовується для з'єднання комутаторів або інших пристроїв, які підтримують VLAN tagging;

в) Hybrid Mode (гібридний режим) – гібридний режим дозволяє поєднувати можливості режиму доступу і режиму магістралі для одного порту;

г) Voice VLAN (голосовий VLAN) – цей режим призначений для голосового трафіку в VoIP мережах. Інтерфейс, налаштований як голосовий VLAN, може ідентифікувати та керувати голосовим трафіком окремо.

Access Mode використано на інтерфейсах, що під'єданні до кінцевих пристроїв, кожен з яких окремо належить до одного VLAN'у, окрім випадків де буде одночасно використовуватися разом із Voice VLAN. Налаштування відбувається у режимі глобальної конфігурації. Визначаємо необхідні інтерфейси, вмикаємо порти, вибираємо режим роботи та прив'язуємо VLAN (окрім VLAN7) згідно таблиці 1:

```
L2switch30(config)# interface range fastEthernet 0/1-19
L2switch30(config-if-range)# no shutdown
L2switch30(config-if-range)# switchport mode access
L2switch30(config-if-range)# switchport access vlan 30
L2switch30(config)# interface fastEthernet 0/20
L2switch30(config-if)# switchport access vlan 4
L2switch30(config)# interface  fastEthernet 0/22
L2switch30(config-if)# switchport access vlan 5
```

Voice VLAN (VLAN7) налаштовується на інтерфейсі FastEthernet0/20 що одночасно належить і до VLAN4 наступним чином:

L2switch30(config)# interface fastEthernet 0/20

L2switch30(config-if)# switchport voice vlan 7

Для перевірки налаштування VLAN використаємо команду show vlan brief. Результат виводу команди показаний на рисунку 2.2.

```
L2switch30#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/21, Fa0/23, Fa0/24, Gig0/1
                                                Gig0/2
2    L2switchVLAN                     active
4    adminVLAN                        active    Fa0/20
5    wifiVLAN                         active    Fa0/22
7    voiceVLAN                        active    Fa0/20
30   30Aud                            active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Рисунок 2.2 – Результат виводу команди show vlan brief в Cisco packet tracer

Наступним кроком налаштовуємо порти що йдуть до рівня розподілу. Для цього використовуємо режим trunk (802.1Q) який дозволяє передавати декілька VLAN’ів одним портом. Це необхідно через наявність різних VLAN’ів на L2switch30.

L2switch30(config)# interface range gigabitEthernet 0/1-2

L2switch30(config-if-range)# no shutdown

L2switch30(config-if-range)# switchport mode trunk

Остання команда автоматично дозволяє всі доступні VLAN на порту. За необхідності можливо дозволити тільки певні VLAN для більшої сегментації мережі за допомогою команди:

L2switch30 (config-if-range)#switchport trunk allowed vlan (№VLAN)

Важливим кроком є присвоєння IP-адреси віртуальному інтерфесу L2 комутатору для подальшої можливості віддаленого доступу за допомогою використання протоколів SSH або telnet.

L2switch30(config)# interface vlan 2

L2switch30(config-if)# ip address 192.168.2.30 255.255.255.0

L2switch30(config)# ip default-gateway 192.168.2.254

2.1.5 RSTP

Налаштування STP (Spanning Tree Protocol) [1] важливе для усіх мережевих пристроїв, особливо де є можливість створення петель у топології. STP допомагає уникнути цих петель та гарантує відсутність циклічних маршрутів у мережі. RSTP (Rapid Spanning Tree Protocol) – покращена версія Spanning STP, яка була створена для більш швидкого виявлення змін у топології мережі та швидшого відновлення роботи мережі після змін.

Налаштування на L2 switch вимагає введення однієї команди:

L2switch30(config)# spanning-tree mode rapid-pvst

2.1.6 DHCP Snooping

DHCP Snooping – технологія безпеки мережі, яку використовують для захисту від атак із використанням DHCP-протоколу (DHCP spoofing або DHCP poisoning). Також технологія необхідна для захисту від атак Man-in-the-Middle, де зловмисник може видаляти або змінювати DHCP-відповіді. В нашій топлогії необхідна через наявність DHCP-серверів, що налаштовані на L3 комутаторах.

При налаштуванні DHCP Snooping на L2switch30 дозволяємо наступні VLAN:

а) усі VLAN’и, на яких розташовані кінцеві пристрої, що використовують DHCP для отримання IP-адрес, повинні бути дозволені. Це важливо для забезпечення того, щоб клієнти в усіх VLAN’ах могли успішно отримати необхідні IP-адреси від DHCP-серверів;

б) VLAN’и, на яких розташовані DHCP-сервери, повинні бути дозволені. Це особливо важливо, оскільки DHCP-сервери відповідають на

запити клієнтів, і тому VLAN'и, на яких розташовані ці сервери, повинні бути налаштовані як довірені.

Інші VLAN'и, на яких немає клієнтів DHCP, будуть незадіяними для DHCP Snooping. Правильне налаштування портів, підключених до DHCP-серверів також є важливою частиною налаштувань DHCP Snooping. Це дозволить DHCP Snooping довіряти тільки DHCP-серверам на цих портах і відбирати DHCP-відповіді, що надходять з інших портів.

Налаштовується DHCP Snooping на L2switch30:

Вмикаємо DHCP Snooping на комутаторі:

L2switch30(config)# ip dhcp snooping

Вказуємо довірені порти (trusted port), що йдуть до DHCP серверів:

L2switch30(config)# int range gigabitEthernet 0/1-2

L2switch30(config-if-range)# ip dhcp snooping trust

Вказуємо які VLAN слід перевіряти. Для 30 аудиторії DHCP необхідний для 5, 7 та 30 VLAN. Пристрої з 2 та 4 VLAN мають статичну адресу:

L2switch30(config)# ip dhcp snooping vlan 5, 7, 30

Вимикаємо опцію збереження інформації DHCP в пакеті, вона блокує можливість отримання IP-адреси:

L2switch30(config)# no ip dhcp snooping information option

Встановлюємо обмеження швидкості для DHCP Snooping до 10 пакетів на секунду. Це допомагає запобігти атакам, спрямованим на перевантаження мережі DHCP запитами:

L2switch30(config)# ip dhcp snooping limit rate 10

Для перевірки налаштування DHCP Snooping використаємо команду show ip dhcp snooping. Результат виводу команди показаний на рисунку 2.3.

```
L2switch30#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,7,30
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
GigabitEthernet0/1         yes        unlimited
GigabitEthernet0/2         yes        unlimited
FastEthernet0/20           no         unlimited
FastEthernet0/22           no         unlimited
```

Рисунок 2.3 – Результат виводу команди show ip dhcp snooping в Cisco packet tracer

2.1.7 IP Source Guard

IP Source Guard (IPSG) – функція безпеки, яка використовується на комутаторах Cisco для захисту від IP-підміни (IP spoofing) в локальних мережах. IPSG перевіряє відправника IP-пакета і зрівнює, чи відповідає його джерело IP-адресі, який був наданий на основі DHCP або статично вручну.

IPSG допомагає уникнути ситуацій, коли злоумисники намагаються ввести неправдиві IP-адреси для обходу безпеки мережі, шляхом перевірки відповідності IP-адреси наявному MAC-адресу порту комутатора. Це особливо корисно в мережах, де використовується динамічна настройка IP через DHCP.

Вмикаємо IPSG на довірених портах:

L2switch30(config)# interface range gigabitEthernet 0/1-2

L2switch30(config-if-range)# ip verify source

2.1.8 Dynamic ARP inspection

Dynamic ARP Inspection (DAI) – функція безпеки, яка використовується в комутаторах для захисту від атак, пов’язаних із зміною ARP-таблиць. Атаки ARP, такі як ARP Spoofing або ARP Poisoning, можуть бути використані зловмисниками для введення фальшивих мережевих шляхів і отримання неправомірного доступу до конфіденційних даних в мережі. DAI перевіряє відповідність між IP-адресами та фізичними MAC-адресами в ARP-пакетах,

які надходять на комутатор, і блокує або відхиляє пакети, якщо вони не відповідають дійсним зв'язкам в мережі. Це допомагає запобігти атакам, спрямованим на зловживання ARP-протоколом і забезпечує безпеку та цілісність мережевого з’єднання.

При нашалтування DAI необхідно встановити довірені порти (trusted ports), які пов’язані зі справжніми DHCP-серверами та іншими надійними пристроями. Порти, через які під’єднані кінцеві пристрої є недовіреними (untrusted ports). Налаштовуємо DAI наступними чином:

Активує DAI на 5, 7 та 30 VLAN:

L2switch30(config)# ip arp inspection vlan 5, 7, 30

Налаштовує інтерфейси GigabitEthernet 0/1-2 як довірені для DAI:

L2switch30(config)# interface range gigabitEthernet 0/1-2

L2switch30(config-if-range)# ip arp inspection trust

Для перевірки налаштування DAI використаємо команду show ip arp inspection interfaces. Результат виводу команди показаний на рисунку 2.4.

```
L2switch30#show ip arp inspection interfaces
Interface        Trust State     Rate(pps)    Burst Interval
---------------  -----------     ---------    --------------
Fa0/1            Untrusted              15                 1
Fa0/2            Untrusted              15                 1
Fa0/3            Untrusted              15                 1
Fa0/4            Untrusted              15                 1
Fa0/5            Untrusted              15                 1
Fa0/6            Untrusted              15                 1
Fa0/7            Untrusted              15                 1
Fa0/8            Untrusted              15                 1
Fa0/9            Untrusted              15                 1
Fa0/10           Untrusted              15                 1
Fa0/11           Untrusted              15                 1
Fa0/12           Untrusted              15                 1
Fa0/13           Untrusted              15                 1
Fa0/14           Untrusted              15                 1
Fa0/15           Untrusted              15                 1
Fa0/16           Untrusted              15                 1
Fa0/17           Untrusted              15                 1
Fa0/18           Untrusted              15                 1
Fa0/19           Untrusted              15                 1
Fa0/20           Untrusted              15                 1
Fa0/21           Untrusted              15                 1
Fa0/22           Untrusted              15                 1
Fa0/23           Untrusted              15                 1
Fa0/24           Untrusted              15                 1
Gig0/1           Trusted                15                 1
Gig0/2           Trusted                15                 1
```

Рисунок 2.4 – Результат виводу команди show ip arp inspection interfaces в Cisco packet tracer

2.1.9 Port security

Port Security – функція безпеки на L2 комутаторах що дозволяє обмежити кількість мережевих пристроїв, які можуть підключатися до конкретного порту. Це допомагає уникнути несанкціонованого доступу до мережі, зменшити можливість атак типу MAC flooding та ARP spoofing. Розглянемо налаштування Port Security для L2switch30:

Вибираємо діапазон портів, що належать комп'ютерам користувачів і обмежуємо максимальну кількість дозволених MAC-адрес на порту до 2:

L2switch30(config)# interface range fastEthernet 0/1-19

L2switch30(config-if-range)# switchport port-security

L2switch30(config-if-range)# switchport port-security maximum 2

Вказуємо як повинен реагувати комутатор на перевищення максимальної кількості дозволених адрес. Існує 3 режими:

Shutdown Mode: В цьому режимі порт буде вимкненний, як тільки буде виявлено порушення безпеки. Порт не буде пересилати трафік поки адміністратор не відновить його вручну.

Restrict Mode: У цьому режимі порт записуватиме порушення безпеки, але не вимикатиме його. Натомість порт продовжуватиме працювати та пересилати трафік, але кожне порушення буде реєструватися та/або може генерувати повідомлення.

Protect Mode: Цей режим подібний до режиму "Restrict", але він не реєструє порушення безпеки. Натомість він просто відкидає будь-який додатковий трафік, який порушує налаштування безпеки Port Security.

Найбільш оптимальним для нашої локальної мережі є варіант restrict:

L2switch30(config-if-range)# switchport port-security violation restrict

Для ком'ютера адміністратора значення збільшуємо до 5:

L2switch30(config)# int fastEthernet 0/20

L2switch30(config-if)# switchport port-security maximum 5

L2switch30(config-if)# switchport port-security violation restrict

До точки доступу може бути підключено багато пристроїв, через це вибираємо значення 50:

```
L2switch30(config)# interface fastEthernet 0/22
L2switch30(config-if)# switchport port-security maximum 50
L2switch30(config-if)# switchport port-security violation restrict
```

2.1.10 Storm Control

Storm control – функція, яка дозволяє обмежити обсяг надзвичайно великої та шкідливої мережевої активності, такої як broadcast, multicast або unknown unicast, що надходять на комутатор. Це може бути корисно для захисту мережі від надмірної навантаженості та забруднення мережі неправильними пакетами. Оптимальна пропускна здатності для різних типів трафіку у % може варіюватися. Зазвичай рекомендується встановлювати значення storm control на рівень, який забезпечить велику пропускну здатність для легітимного трафіку, але водночас обмежить потік broadcast, multicast або unknown unicast трафіку в разі надмірного навантаження на мережу. Найкраще встановити значення та спостерігати за мережевою активністю, щоб перевірити, чи вони відповідають вимогам мережі.

Налаштовуємо Storm Control на усіх інтрфейсах та вказуємо обмеження рівня broadcast, multicast та unicast трафіку у % від максимальної пропускної здатності порту:

```
L2switch30(config)#interface range fastEthernet 0/1-24
L2switch30(config-if-range)# storm-control broadcast level 10
L2switch30(config-if-range)# storm-control multicast level 5
L2switch30(config-if-range)# storm-control unicast level 1
L2switch30(config)#interface range gigabitEthernet 0/1-2
L2switch30(config-if-range)# storm-control broadcast level 10
L2switch30(config-if-range)# storm-control multicast level 5
L2switch30(config-if-range)# storm-control unicast level 1
```

Слід зазначити, що значення storm-control буде залежним від реальних умов мережі, і тому експерименти на реальному обладнанні будуть корисними для визначення оптимальних налаштувань у реальному середовищі.

2.1.11 Налаштування віддаленого доступу по SSH

SSH є шифрованим протоколом для безпечного віддаленого з'єднання з пристроями через мережу. SSH на відміну від telnet забезпечує шифрування даних під час передачі, і навіть у випадку перехоплення трафік буде неможливо розшифрувати.

Обов'язковим етапом налаштування SSH є встановлення доменного імені, без якого буде неможливо згенерувати RSA-ключі. За основу виберемо доменне ім'я "zp.edu.ua":

L2switch30(config)# ip domain name zp.edu.ua

Далі генеруємо на комутаторі ключову пару RSA з міткою "sshkeyL2" та розміром модуля 4096 біт:

L2switch30(config)# crypto key generate rsa usage-keys label sshkeyL2 modulus 4096

Створюємо користувача та встановлюємо пароль для SSH:

L2switch30(config)# username L2switch30 secret ku8S74g4JV

Налаштовуємо SSH для віртуальних терміналів (VTY) з номерами від 0 до 15, вказуємо другу версію протоколу та можливість віддаленого підключення лише із використанням SSH:

L2switch30(config)# ip ssh version 2

L2switch30(config)# line vty 0 15

L2switch30(config-line)# transport input ssh

Останнім кроком є перевірка можливості віддаленого доступу до L2switch30 з комп'ютера адміністратора 30 аудиторії, що зображено на рисунку 2.5.

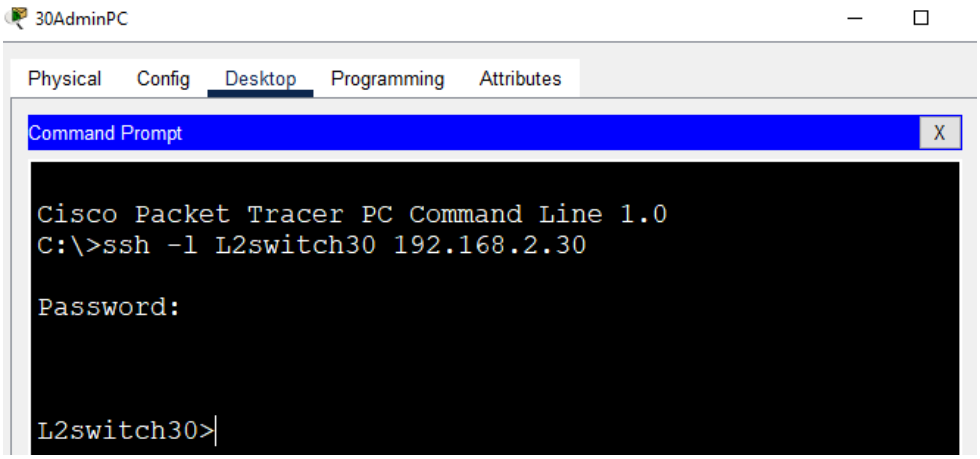

Рисунок 2.5 – Успішне віддалене підключення до L2switch30 із комп'ютера адміністратора

2.1.12 AAA

AAA (Authentication, Authorization, and Accounting) – фреймворк для реалізації механізмів аутентифікації, авторизації та обліку в мережевих пристроях. Використання цього фреймворку дозволяє налаштовувати політику доступу, визначати права користувачів і здійснювати облік подій для виявлення нроблем та проведення аудиту системи.

Наступні команди необхідні для налаштування TACACS+ (Terminal Access Controller Access Control System Plus) для аутентифікації на L2 комутаторі Cisco.

Вмикаємо журналювання подій на пристрої. Це дозволить реєструвати події і помилки для подальшого аналізу:

L2switch30(config)# logging on

Увімкнення нової моделі AAA:

L2switch30(config)# aaa new-model

Налаштовуємо аутентифікацію для режиму входу. Вказуємо що спочатку використовується TACACS+, а у випадку недоступності сервера TACACS+ використовується локальна аутентифікація:

L2switch30(config)# aaa authentication login default group tacacs+ local

Вказує IP-адресу сервера TACACS+, з яким буде встановлено з’єднання:

L2switch30(config)# tacacs-server host 192.168.6.100

L2switch30(config)# tacacs-server host 192.168.6.101

Задаємо ключ аутентифікації між пристроєм і сервером TACACS+:

L2switch30(config)# tacacs-server key 8DHxa8u6

2.1.13 Syslog

Syslog (System Logging) – стандартний протокол для відправлення та прийому журнальних подій чи повідомлень в мережевих системах. Syslog дозволяє пристроям записувати різноманітні події, такі як помилки, стан пристрою та інші важливі інформаційні повідомлення та відправляти їх на зазначений syslog-сервер для централізованого збору та аналізу.

Для синхронізації часу між серверами спочатку налаштуємо NTP (Network Time Protocol). Це дозволить точно визначати коли та в якому порядку сталися події. Вказуємо NTP-севрер до якого комутатор буде відправляти запити для отримання актуального часу наступною командою:

L2switch30(config)# ntp server 192.168.6.100

L2switch30(config)# ntp server 192.168.6.101

Встановлює розмір буфера для журнальних подій на 4096 байт, що необхідно для локального аналізу журналу на самому пристрої:

L2switch30(config)# logging buffered 4096

Встановлення рівня логування є важливим кроком для управління обсягом журнальних подій, які відправляються на централізований syslog-сервер. Щоб не переповнювати syslog-сервер непотрібними сповіщеннями виберемо 4 рівень логування (warnings):

L2switch30(config)# logging trap warnings

Вказуємо адресу Syslog-сервера, на який будуть відправлятися журнальні події:

L2switch30(config)# logging 192.168.6.100

L2switch30(config)# logging 192.168.6.101

Встановлює формат та часовий віджет для журнальних подій, “datetime” вказує, що в лог буде включено дату та час, а “msec” додає мілісекунди. Це дозволить точніше визначити час виникнення подій:

L2switch30(config)# service timestamps log datetime msec

2.1.14 Додаткові безпекові параметри L2 комутатора

Розглянемо декілька команд спрямованих на забезпечення безпеки конфігураційних режимів, управління доступом та фільтрацію трафіку для окремих пристроїв. Вони були об’єднані в групу параметрів безпеки, оскільки спільно призначені для захисту пристроїв від несанкціонованого доступу та забезпечують правильну обробку мережевого трафіку.

Зашифруємо всі паролі на пристрої (наприклад, паролі локальних користувачів або паролі для режимів доступу) алгоритмом типу MD5 у конфігураційному файлі наступною командою:

L2switch30(config)# service password-encryption

Встановимо пароль (secret) для доступу до режиму enable:

L2switch30(config)# enable secret yN9X9e

Дозволимо доступ лише певним IP адресам через віддалене підключення до комп’ютерів адміністраторів із 4 VLAN (adminVLAN):

L2switch30(config)# access-list 1 permit 192.168.4.0 0.0.0.255

L2switch30(config)# line vty 0 15

L2switch30(config-line)# access-class 1 in

2.2 Access Point

Access Point (AP) – бездротова точка доступу, яка дозволяє бездротовим пристроям підключатися до провідної мережі (Ethernet) через бездротове з’єднання (зазвичай Wi-Fi). Основні характеристики Access Point включають:

– провідне Підключення: AP зазвичай підключається до мережі за допомогою Ethernet-кабелю, що забузпечює зв’язок з комутатором або іншими мережевими пристроями;

– розширення Зони Покриття: AP використовується для розширення зони покриття мережі. Додавання нових Access Point може покращити якість сигналу та забезпечити бездротовий доступ в різних частинах будівлі або на території підприємства.

Для налаштування симуляції AP в Cisco Packet Tracer необхідно задати SSID та PSK Pass Phrase, що зображено на рисунку 2.6.

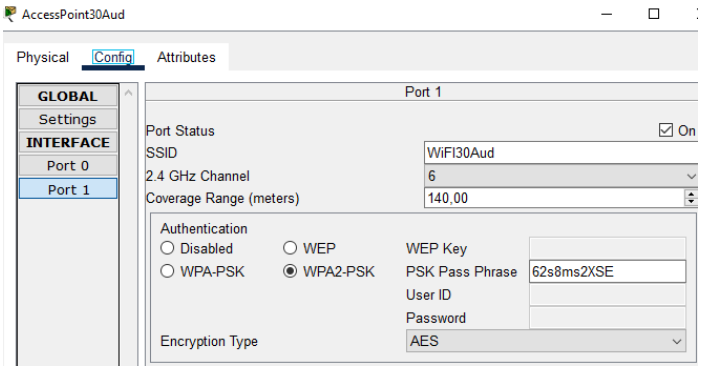

Рисунок 2.6 – Налаштування AP у Cisco Packet Tracer

Перевірити працездатність AP потрібно за допомогою пристрою, що підтримує бездротове з’єднання (в нашому випадку Laptop). Якщо все налаштовано правильно ми побачимо унікальний SSID що відноситься до цієї точки доступу як це показано на рисунку 2.7.

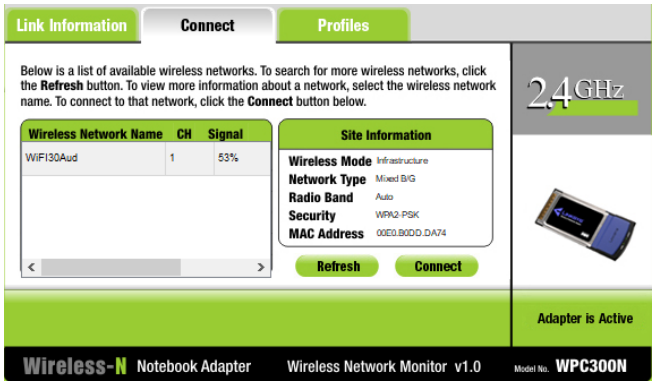

Рисунок 2.7 – SSID AP 30 аудиторії

3 ТОПОЛОГІЯ 39 АУДИТОРІЇ

Фізична топологія 39 аудиторії ідентична 30 аудиторії але є декілька важливих відмінностей у логічній. Основна відмінность – використання іншого VLAN для кінцевих пристроїв користувачів на L2 комутаторі, замість 30 використовуємо 39. Зміні також підлягає ім’я мережевого пристрою на L2switch39 відповідно до номеру аудиторії та інший користувач із паролем для SSH доступу:

L2switch30(config)# username L2switch39 secret kC282NZj2u

Для AP буде змінений SSID на WIFI39AUD та PSK Pass Phrase на 9UD7c2p8yF.

4 ТОПОЛОГІЯ 31 АУДИТОРІЇ

Топологія 31 аудиторії включає в себе L2 комутатор Cisco Catalyst 2960-12TC-L (12 FE + 2 GE порти) та кінцеві пристрої, серед яких 4 сервери під різні задачі (TFTP, AAA, Syslog, NTP, VoIP) і комп'ютери користувачів.

Топологія 31 аудиторії зображена на рисунку 4.1.

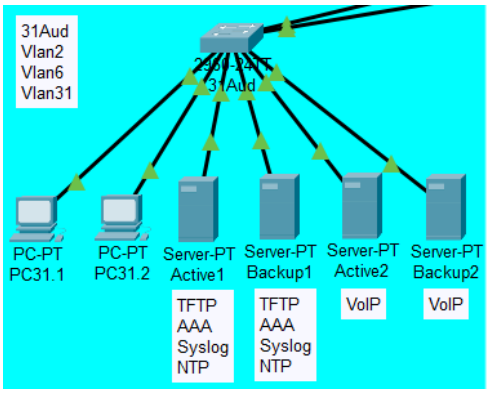

Рисунок 4.1 – Топологія 31 аудиторії

4.1 L2 комутатор 31 аудиторії

За основу налаштування L2 комутатора 31 аудиторії взяте налаштування L2 30 аудиторії, яке містить декілька значних змін, а саме:

а) ім'я пристрою

Змінюється відповідно до номеру аудиторії:

Switch(config)# hostname L2switch31

L2switch31(config)#

б) VLAN'и та інтерфейси.

На L2 комутаторі налаштовуються 3 різних VLAN: VLAN 2 для віддаленого доступу, VLAN 6 виділений тільки під сервери та VLAN 31 для кінцевих пристроїв 31 аудиторії. Номера VLAN з відповідними до них інтерфейсами та режимами роботи занесені до таблиці 4.1.

Таблиця 4.1 – VLAN’и та прив’язані до них інтерфейси 31 аудиторії

№ VLAN	Ім’я VLAN	№ фізичних інтерфейсів	Режим роботи
vlan 2	L2switchVLAN	Vlan2	-
vlan 6	serverVLAN	fastEthernet 0/8-11	Access
vlan 31	31Aud	fastEthernet 0/1-7	Access

Задаємо IP-адресу віртуальному інтерфейсу vlan 2:

L2switch31(config)# int vlan 2

L2switch31(config-if)# ip address 192.168.2.31 255.255.255.0

в) налаштування Dynamic ARP inspection

Активувати DAI необхідно лише для 31 VLAN, тому що це єдиний VLAN в аудиторії який має окремий DHCP pool на кластері L3 комутаторів:

L2switch31(config)# ip arp inspection vlan 31

г) налаштування Port security.

Змінюємо діапазон інтерфейсів відповідно до конфігурацаїї фізичного пристрою:

L2switch31(config)# interface range fastEthernet 0/1-12

L2switch31(config-if-range)# switchport port-security

L2switch31(config-if-range)# switchport port-security maximum 2

L2switch31(config-if-range)# switchport port-security violation restrict

д) Налаштування SSH

Змінюємо користувача та пароль у безпекових цілях:

L2switch31(config)# username L2switch31 secret rzP7XpL938

5 ТОПОЛОГІЯ 32, 33, 34, 35 ТА 37 АУДИТОРІЙ

Топології 32, 33, 34, 35 та 37 аудиторій було об’єднано в єдиний пункт через їхню подібність та простоту налаштування в порівнянні із 30 та 39 аудиторією. В аудиторіях 32, 33 та 37 основою мережі є Cisco Catalyst 2960-24TT-L (24 FE + 2 GE порти) коли для 34 та 35 це Cisco Catalyst 2960-12TC-L (12 FE + 2 GE порти). В якості кінцевих пристроїв виступають лише комп’ютери користувачів. Топології 32, 33, 34 та 37 аудиторії зображена на рисунку 5.1.

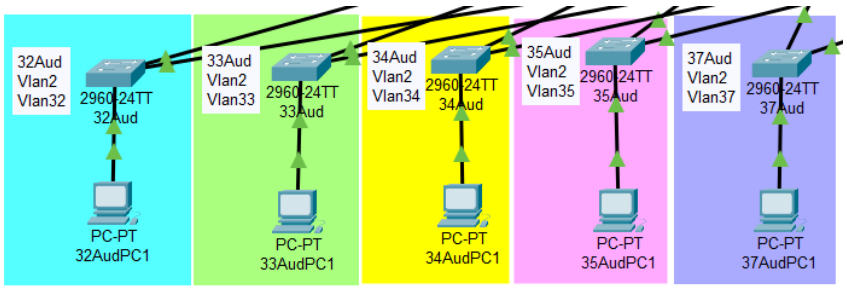

Рисунок 5.1 – Топологія мережі 32, 33 та 37 аудиторій

5.1 L2 комутатори 32, 33, 34, 35 та 37 аудиторій

За основу налаштування L2 комутаторів 32, 33, 34, 35 та 37 аудиторій взяте налаштування L2 30 аудиторії. Команди для налаштування комутатора в 30 аудиторії які є ідентичними, не будуть повторюватися, а будуть враховані лише ті, що відрізняються:

а) ім’я пристроїв

Змінюється відповідно до номеру аудиторії:

Switch(config)# hostname L2switch32

L2switch32(config)#

Switch(config)# hostname L2switch33

L2switch33(config)#

Switch(config)# hostname L2switch37

L2switch37(config)#

б) VLAN’и та інтерфейси

На комутаторах 32, 33, 34, 35 та 37 аудиторії налаштовуються по 2 VLAN, один з яких (VLAN2) буде спільний, а другий VLAN є унікальним для кожної аудиторії (32, 33, 34, 35, 37) і призначається лише для її кінцевих пристроїв. Номери комутаторів, VLAN’ів з відповідними до них інтерфейсами та їх режимом роботи занесені до таблиці 5.1.

Таблиця 5.1. VLAN’и та прив’язані до них інтерфейси 31 аудиторії

	№ VLAN	Ім’я VLAN	№ фізичних інтерфейсів	Режим роботи
L2switch32	vlan 2	L2switchVLAN	-	-
	vlan 32	32Aud	fastEthernet 0/1-24	Access
L2switch33	vlan 2	L2switchVLAN	-	-
	vlan 33	33Aud	fastEthernet 0/1-24	Access
L2switch34	vlan 2	L2switchVLAN	-	-
	vlan 34	34Aud	fastEthernet 0/1-12	Access
L2switch35	vlan 2	L2switchVLAN	-	-
	vlan 35	35Aud	fastEthernet 0/1-12	Access
L2switch37	vlan 2	L2switchVLAN	-	-
	vlan 37	37Aud	fastEthernet 0/1-24	Access

Задаємо IP-адреси віртуальним інтерфейсам vlan 2, дані заносимо до таблиці 5.2.

Таблиця 5.2 – IP-адреси віртулальних інтерфейсів для кожного пристрою

Ім’я пристрою	IP-адреса vlan 2
L2switch32	192.168.2.32/24
L2switch33	192.168.2.33/24
L2switch34	192.168.2.34/24
L2switch35	192.168.2.35/24
L2switch37	192.168.2.37/24

в) налаштування Dynamic ARP inspection

Активувати DAI необхідно лише для унікальних VLAN’ів кожної аудиторії на всіх L2 комутаторах наступним чином:

L2switch32(config)# ip arp inspection vlan 32

L2switch33(config)# ip arp inspection vlan 33

L2switch34(config)# ip arp inspection vlan 34

L2switch35(config)# ip arp inspection vlan 35

L2switch37(config)# ip arp inspection vlan 37

г) налаштування Port security.

Змінюємо діапазон інтерфейсів відповідно до конфігурацаїї фізичного пристрою.

Для L2switch32, L2switch33, L2switch37:

L2switch32(config)# interface range fastEthernet 0/1-24

L2switch32(config-if-range)# switchport port-security

L2switch32(config-if-range)# switchport port-security maximum 2

L2switch32(config-if-range)# switchport port-security violation restrict

Для L2switch34, L2switch35:

L2switch34(config)# interface range fastEthernet 0/1-24

L2switch34(config-if-range)# switchport port-security

L2switch34(config-if-range)# switchport port-security maximum 2

L2switch34(config-if-range)# switchport port-security violation restrict

д) Налаштування SSH

Змінюємо користувача та пароль на кожному комутаторі для безпекових цілей, заносимо дані до таблиці 5.3.

Таблиця 5.3 – Відповідність користувачів та паролей для SSH на L2 комутаторах

Ім’я пристрою	Ім’я SSH користувача	Пароль SSH користувача
L2switch32	L2switch32	NH5cmpV996
L2switch33	L2switch33	7G7HeP24sn
L2switch34	L2switch34	gnT76L4Bb4
L2switch35	L2switch35	jh23pBD37Z
L2switch37	L2switch37	4cg9KN67kG

6 ВІДМОВОСТІЙКИЙ КЛАСТЕР КОМУТАТОРІВ L3 ЯК ОСНОВА LAN

Відмовостійкий кластер (failover cluster) – група пов’язаних пристроїв, яка дозволяє продовжувати роботу в разі відмови одного або кількох пристроїв у групі.

Формування відмовостійкого кластеру надасть наступні переваги:

– відмовостійкість (High Availability) – кластер дозволяє застосунку або сервісу продовжувати роботу навіть у випадку відмови одного з пристроїв;

– автоматичне виявлення відмов (Automatic Failover) – система автоматично виявляє відмову одного з пристроїв та переносить роботу на інший активний пристрій;

– резервування ресурсів (Resource Redundancy) – кластер може мати дубльовані ресурси (наприклад, дубльовані сервери), які можуть взаємозамінювати один одного у випадку відмови.

Відмовостійкий кластер кафедри РТТ складається із двох комутаторів L3 та двох міжмережевих екранів Cisco Asa. Проектування розглядається відразу у двох программах: EVE-NG та Cisco Packet Tracer. EVE-NG – емулятор, який дозволяє створювати віртуальні мережі, емулюючи роботу мережевого обладнання через що має набагато ширший спект функцій та краще підходить для моделювання складних мережевих пристроїв та топологій. В деяких пунктах розписані команди для налаштування окремо до кожного програмного додатка через відмінності у фізичних назвах використаних інтерфейсів.

6.1 Налаштування L3 комутаторів

Комутатор L3 – мережевий пристрій, який об’єднує в собі функціональні можливості комутатора другого рівня (L2) та маршрутизатора третього рівня (L3). Функції L3 комутатора також може виконувати

маршрутизатор, але за однакову продуктивність маршрутизатор буде незрівнянно дорожчим і економічно невигідним для спектру задач що проектованої LAN. Слід зазначити що без використання маршрутизатору чи міжмережевого екрану із локальної мережі буде неможливо потрапити до глобальної мережі (WAN).

В проектуємій LAN L3 комутатори працюють на рівні розподілу (distribution layer), забезпечать відмовостійкість, поліпшать продуктивності мережі. Також вони необхідні для маршрутизації між VLAN'ами та підмережами, керуванням трафіку (QoS) і для покращення безпеки за допомогою Access Control Lists.

За основу LAN взяті два L3 комутатори Catalyst 3650-24TD на 24 порти Gigabit Ethernet (10/100/1000 Mbps), відповідно для з'єднання між собою та L2 комутаторами використовується цей стандарт та кабель UTP 5e (CAT 5e).

В усіх наступних пунктах спочатку розглядається налаштування в Cisco Packet Tracer а потім EVE-NG, за винятком ідентичних конфігурацій.

Топологія рівня розподілу L3 комутаторів зображена на рисунку 6.1.

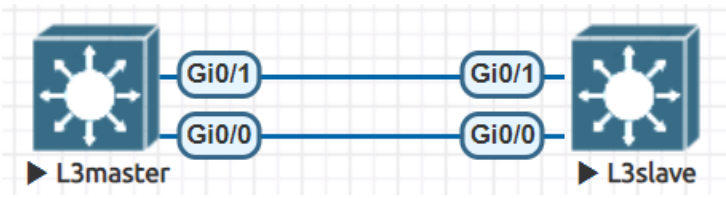

Рисунок 6.1 – Рівень розподілу L3 комутаторів

6.1.1 Імена L3 комутаторів

Для легшої ідентифікації пристроїв задамо імена відповідно до їх ролі у локальній мережі [1], де перший комутатор є основним (L3master), а другий додатковим (L3slave):

Switch(config)# hostname L3master

L3master(config)#

Switch(config)# hostname L3slave

L3slave(config)#

6.1.2 Консольного порту

Пароль на консольний порт використовується для підвищення рівня безпеки та контролю доступу до мережевого обладнання.

```
L3master(config)# line console 0
L3master(config-line)# password t2T7sBf52E
L3master(config-line)# login
L3master(config)# line console 0
L3slave(config-line)# password RymM877d7Y
L3master(config-line)# login
```

6.1.3 EtherChannel

EtherChannel [3] використовується для об’єднання (агрегації) кількох фізичних інтерфейсів в один логічний канал з метою підвищення пропускної здатності, надійності та управляючої гнучкості мережі.

Через L3master та L3slave йде найбільший трафік у локальній мережі тому одне фізичне з’єднання є ненадійним та низькопродуктивним на відміну від декількох фізичних об’єднаних в один логічний канал за допомогою EtherChannel, що дозволяє збільшити пропускну спроможність пропорційно продуктивності фізичних каналів, спрощує налаштування інтерфейсів та підвищує надійність локальної мережі у цілому.

Налаштування EtherChannel відбуваєть в режимі Layer 3 аналогічно на L3master і L3slave. Єдина відмінність – різні IP-адреси port-channel 2.

```
L3master(config)# interface range gigabitEthernet 1/0/23-24
L3master(config-if-range)# shutdown
L3master(config-if-range)# no switchport
L3master(config-if-range)# channel-group 2 mode on
L3master(config-if-range)# no shutdown
L3master(config)# interface port-channel 2
L3master(config-if)# ip address 10.0.2.1 255.255.255.0
```

Змінюємо IP-адресу на L3slave:

L3slave(config-if)# ip address 10.0.2.2 255.255.255.0

В EVE-NG налаштування дещо відрізняється, об’єднуємо фізичні інтерфейси GigabitEthernet 0/0 та GigabitEthernet 0/1 в один логічний.

Для перевірки налаштування EtherChannel в EVE-NG використаємо команду show etherchannel summary. Результат виводу команди показаний на рисунку 6.2.

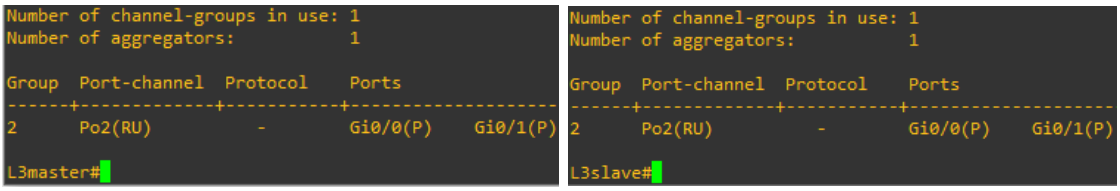

Рисунок 6.2 – Результат виводу команди show etherchannel summary на L3master та L3slave

6.1.4 OSPF

Для локальної мережі із великою кількістю підмереж оптимальним є вибір динамічної маршрутизації яка забезпечить автоматичне оновлення таблиці маршрутизації та баланс навантаження, що дозволить більш ефективно використовувати ресурси пристроїв. Основними представниками є протоколи вектора відстані (Distance Vector Protocols): RIP, EIGRP; протоколи вектора посилання (Link-State Protocols): OSPF, IS-IS та протокол вектора маршрутів (Path Vector Protocols): BGP.

Найбільш оптимальним для нашої мережі є OSPF [3]. Він підтримується усіма мережевими пристроями (на відміну від EIGRP що працює лише на обладнанні Cisco), має багато налаштуванні та може ефективно керувати великим обсягом маршрутів. Недоліками є велике споживання ресурсів пристроїв та швидкість збереження інформації, через що оновлення топології в може займати значний час, особливо у великих мережах з багатьма маршрутизаторами.

OSPF налаштовується на кожному пристрої, що підтримує маршрутизацію рівня 3. Для L3master та L3slave усі налаштування будуть ідентичними окрім router-id, для L3master 1.1.1.1, для L3slave 2.2.2.2.

Перед налаштуванням OSPF потрібно активувати IP-маршрутизацію:

L3master(config)# ip routing

Налаштовуємо процесс OSPF під номером 1:

L3master(config)# router ospf 1

Задаємо унікальний ідентифікатор мережевого пристрою:

L3master(config-router)# router-id 1.1.1.1

Перераховуємо усі підмережі що під'єднанні до L3 комутаторів напряму, їх wildcard mask'и (інвертована маска мережі) та зони, в яких буде маршрутизуватися трафік:

L3master(config-router)# network 10.0.2.0 0.0.0.255 area 1

L3master(config-router)# network 192.168.2.0 0.0.0.255 area 1

L3master(config-router)# network 192.168.3.0 0.0.0.255 area 1

L3master(config-router)# network 192.168.4.0 0.0.0.255 area 1

L3master(config-router)# network 192.168.5.0 0.0.0.255 area 1

L3master(config-router)# network 192.168.6.0 0.0.0.255 area 1

L3master(config-router)# network 192.168.7.0 0.0.0.255 area 1

L3master(config-router)# network 192.168.30.0 0.0.0.255 area 1

L3master(config-router)# network 192.168.31.0 0.0.0.255 area 1

L3master(config-router)# network 192.168.32.0 0.0.0.255 area 1

L3master(config-router)# network 192.168.33.0 0.0.0.255 area 1

L3master(config-router)# network 192.168.34.0 0.0.0.255 area 1

L3master(config-router)# network 192.168.35.0 0.0.0.255 area 1

L3master(config-router)# network 192.168.37.0 0.0.0.255 area 1

L3master(config-router)# network 192.168.39.0 0.0.0.255 area 1

Перевірка з'єднання OSPF відбувається за допомогою команди show ip ospf neighbor, результат виведення команди на L3 комутаторах показано на рисунку 6.3.

```
L3master#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:35    10.0.2.2        Port-channel2

L3slave#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/BDR        00:00:33    10.0.2.1        Port-channel2
```

Рисунок 6.3 – Результат виводу команди show ip ospf neighbor

6.1.5 VTP

VTP (VLAN Trunking Protocol) [6] – протокол який використовується для спрощенного процесу додавання, зміни і видалення VLAN на кількох мережевих пристрояї одночасно. Це дозволяє спростити адміністрування, уникати помилок та швидко змінювати топологію мережі.

Налаштовуємо VTP на L3 комутаторах із використанням другої версії протоколу:

L3master(config)# vtp version 2

Встановлюємо основний L3-комутатор у режим сервера VTP, що дозволить конфігурувати VLAN’и та надсилатиме інформацію про це іншим пристроям:

L3master(config)# vtp mode server

Встановлюємо другу версію протоколу VTP:

L3master(config)# vtp version 2

Встановлює домен (і’мя групи пристроїв, які взаємодіють між собою) VTP на “Basic” та задаємо пароль:

L3master(config)# vtp domain Basic

L3master(config)# vtp password BASIC

На L3slave змінюємо режим роботи з server на client:

L3slave(config)# vtp mode client

L3slave(config)# vtp version 2

L3slave (config)# vtp domain Basic

L3slave (config)# vtp password BASIC

Перевірка VTP відбувається за допомогою команди show vtp status, результат виведення команди показано на рисунку 6.4.

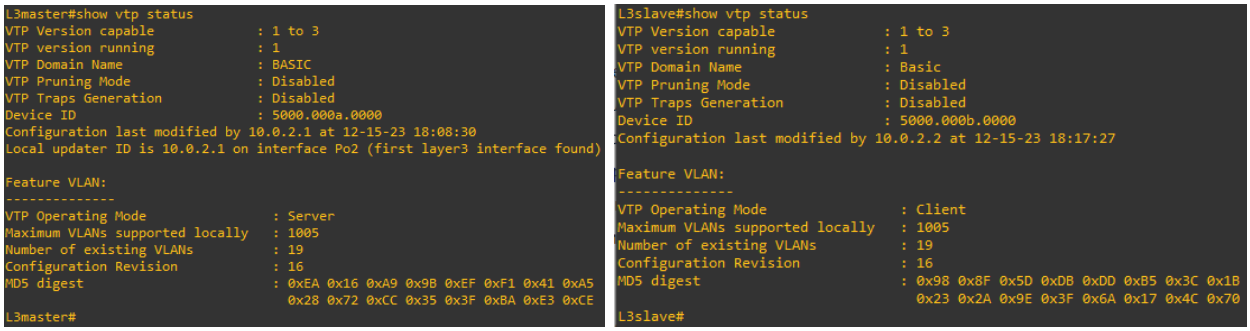

Рисунок 6.4 – Результат виводу конмади show vtp status

6.1.6 Vlan

Наступним кроком після налаштування VTP є налаштування VLAN'ів на L3master. Номери VLAN'ів та їх імена занесені до таблиці 6.1.

Таблиця 6.1 – VLAN'и L3 комутаторів

№ VLAN	Ім'я VLAN	№ VLAN	Ім'я VLAN
2	L2switchVLAN	31	31Aud
3	L3switchVLAN	32	32Aud
4	adminVLAN	33	33Aud
5	wifiVLAN	34	34Aud
6	serverVLAN	35	35Aud
7	voiceVLAN	37	37Aud
30	30Aud	39	39Aud

Налаштування VLAN'ів ніяк не відрізняється від L2 комутаторів і ідентично до пункту "Створення VLAN'ів на L2 комутаторі". Перевіримо налаштування VLAN'ів за допомогою команди show vlan brief, вивід якої зображено на рисунку 6.5.

```
L3master#show vlan brief

VLAN Name                             Status
---- -------------------------------- -------
1    default                          active

2    L2switchVLAN                     active
3    L3switchVLAN                     active
4    adminVLAN                        active
5    wifiVLAN                         active
6    serverVLAN                       active
7    voiceVLAN                        active
30   30Aud                            active
31   31Aud                            active
32   32Aud                            active
33   33Aud                            active
34   34Aud                            active
35   35Aud                            active
37   37Aud                            active
39   39Aud                            active
```

```
L3slave#show vlan brief

VLAN Name                             Status
---- -------------------------------- -------
1    default                          active

2    L2switchVLAN                     active
3    L3switchVLAN                     active
4    adminVLAN                        active
5    wifiVLAN                         active
6    serverVLAN                       active
7    voiceVLAN                        active
30   30Aud                            active
31   31Aud                            active
32   32Aud                            active
33   33Aud                            active
34   34Aud                            active
35   35Aud                            active
37   37Aud                            active
39   39Aud                            active
```

Рисунок 6.5 – Результат виводу команди show vlan brief

Ця конфігурація VLAN’ів тепер акутальна для L3slave через роботу протоколу VTP.

6.1.7 Налаштування HSRP і балансування трафіку між пристроями

HSRP (Hot Standby Router Protocol) [4] – протокол високої доступності для мережевих пристроїв. Використовується для створення відмовостійких кластерів, де один маршрутизатор (Master) використовується для обробки трафіку, а інший маршрутизатор (Slave) очікує на можливий випадок відмови активного маршрутизатора і у цьому випадку автоматично стає активним і продовжує обробку трафіку.

HSRP використовує віртуальну IP-адресу та віртуальну MAC-адресу, які визначаються в межах групи HSRP. Ці адреси використовуються як адреси за замовчуванням для пристроїв в мережі, так що зміни статусу маршрутизатора незамітні для кінцевих користувачів.

Для нашої локальної мережі HSRP є невід’ємним протоколом, що дозволить працювати усій мережі навіть у випадку несправності одного із центральних L3 комутаторів. HSRP буде налаштовуватися для майже усіх

існуючих віртуальних інтерфейсів, а відповідність IP-адрес та інтерфейсів занесена до таблиці 6.2.

Таблиця 6.2 – IP-адреси віртуальних інтерфейсів та пріоритети для налаштування HSRP

№ int vlan	IP int vlan (*) на L3 master	IP int vlan (*) на L3 slave	Virtual IP	Пріоритетний комутатор
2	192.168.2.1/24	192.168.2.2/24	192.168.2.254/24	L3master
3	192.168.3.1/24	192.168.3.2/24	192.168.3.254/24	L3slave
4	192.168.4.1/24	192.168.4.2/24	192.168.4.254/24	L3master
5	192.168.5.1/24	192.168.5.2/24	192.168.5.254/24	L3slave
6	192.168.6.1/24	192.168.6.2/24	192.168.6.254/24	L3master
7	192.168.7.1/24	192.168.7.2/24	192.168.7.254/24	L3slave
30	192.168.30.1/24	192.168.30.2/24	192.168.30.254/24	L3master
31	192.168.31.1/24	192.168.31.2/24	192.168.31.254/24	L3slave
32	192.168.32.1/24	192.168.32.2/24	192.168.32.254/24	L3master
33	192.168.33.1/24	192.168.33.2/24	192.168.33.254/24	L3slave
34	192.168.34.1/24	192.168.34.2/24	192.168.34.254/24	L3master
35	192.168.35.1/24	192.168.35.2/24	192.168.35.254/24	L3slave
37	192.168.37.1/24	192.168.37.2/24	192.168.37.254/24	L3master
39	192.168.39.1/24	192.168.39.2/24	192.168.39.254/24	L3slave

Розглянемо налаштування HSRP L3master на прикладі віртуальних інтерфейсів vlan 2 та vlan 3, що мають різні пріоритети для розподілу трафіку між L3 комутаторами.

Задаємо ip адреси для віртуальних інтерфейсів відповідно до таблиці:

L3master(config)# interface vlan 2

L3master(config-if)# ip address 192.168.2.1 255.255.255.0

Вказуємо віртуальну IP-адресу HSRP, яка буде використовуватися кінцевими пристроями як стандартний шлюз, 2 – номер групи HSRP:

L3master(config-if)# standby 2 ip 192.168.2.254

Встановлюємо пріоритет HSRP. L3master має більший пріоритет (110), тому він буде активним маршрутизатором за замовчуванням. На vlan 2 L3slave нижчий пріоритет (100), тому він перебуватиме у резерві.

L3master(config-if)# standby 2 priority 110

Наступна команда дозволить маршрутизатору з більш високим пріоритетом стати активним у випадку використання багатьох мережевих пристроїв у кластері HSRP або при поверненні активного пристрою у кластер:

L3master(config-if)# standby 2 preempt

Розгляенмо налаштування vlan 3 на L3master, де зміни торкнулись номера групи HSRP, IP-адрес та пріоритету:

L3master(config)# interface vlan 3

L3master(config-if)# ip address 192.168.3.1 255.255.255.0

L3master(config-if)# standby 3 ip 192.168.3.254

L3master(config-if)# standby 3 priority 100

Розглянемо налаштування ідентичних віртуальних інтерфейсів vlan 2 та vlan 3 на L3slave:

L3slave(config)# int vlan 2

L3slave(config-if)# ip address 192.168.2.2 255.255.255.0

L3slave(config-if)# standby 2 ip 192.168.2.254

L3slave(config-if)# standby 2 priority 100

L3slave(config)# int vlan 3

L3slave(config-if)# ip address 192.168.3.2 255.255.255.0

L3slave(config-if)# standby 3 ip 192.168.3.254

L3slave(config-if)# standby 3 priority 110

L3slave(config-if)# standby 3 preempt

Для перевірки налаштувань використаємо команду show standby brief, вивід якої зображено на рисунку 6.6.

```
L3master#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl2         2    110 P Active   local           192.168.2.2     192.168.2.254
Vl3         3    100   Standby  192.168.3.2     local           192.168.3.254
Vl4         4    110 P Active   local           192.168.4.2     192.168.4.254
Vl5         5    100   Standby  192.168.5.2     local           192.168.5.254
Vl6         6    110 P Active   local           192.168.6.2     192.168.6.254
Vl30        30   110 P Active   local           192.168.30.2    192.168.30.254
Vl31        31   100   Standby  192.168.31.2    local           192.168.31.254
Vl32        32   110 P Active   local           192.168.32.2    192.168.32.254
Vl33        33   100   Standby  192.168.33.2    local           192.168.33.254
Vl34        34   110 P Active   local           192.168.34.2    192.168.34.254
Vl35        35   100   Standby  192.168.35.2    local           192.168.35.254
Vl37        37   110 P Active   local           192.168.37.2    192.168.37.254
Vl39        39   100   Standby  192.168.39.2    local           192.168.39.254
Vl7         7    100   Standby  192.168.7.2     local           192.168.7.254
L3master#
```

```
L3slave#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl2         2    100   Standby  192.168.2.1     local           192.168.2.254
Vl3         3    110 P Active   local           192.168.3.1     192.168.3.254
Vl4         4    100   Standby  192.168.4.1     local           192.168.4.254
Vl5         5    110 P Active   local           192.168.5.1     192.168.5.254
Vl6         6    100   Standby  192.168.6.1     local           192.168.6.254
Vl30        30   100   Standby  192.168.30.1    local           192.168.30.254
Vl31        31   110 P Active   local           192.168.31.1    192.168.31.254
Vl32        32   100   Standby  192.168.32.1    local           192.168.32.254
Vl33        33   110 P Active   local           192.168.33.1    192.168.33.254
Vl34        34   100   Standby  192.168.34.1    local           192.168.34.254
Vl35        35   110 P Active   local           192.168.35.1    192.168.35.254
Vl37        37   100   Standby  192.168.37.1    local           192.168.37.254
Vl39        39   110 P Active   local           192.168.39.1    192.168.39.254
Vl7         7    110 P Active   local           192.168.7.1     192.168.7.254
L3slave#
```

Рисунок 6.6 – Результат виводу команди show standby brief на L3 комутаторах

6.1.8 DHCP

DHCP (Dynamic Host Configuration Protocol) [5] є протоколом мережевого рівня, який використовується для автоматичної отримання мережевих параметрів для пристроїв в комп'ютерних мережах. Налаштування DHCP дозволяє пристроям отримувати IP-адреси, підмережеві маски, шлюзи, DNS-сервери та інші конфігураційні параметри автоматично від DHCP-сервера. В проектуємій локальній мережі L3 комутатори виступають в ролі DHCP-серверів.

DHCP налаштований для окремих підмереж, на яких знаходиться велика кількість кінцевих пристроїв, тобто для VLAN’ів аудиторій та VLAN’у точок доступу.

Для роботи DHCP необхідно задати пул адрес, із якого будуть видаватися IP, шлюзи та інші параметри. Розглянемо варінт для пристроїв, що під’єднанні до AP.

Спершу створюємо пул wifiVLAN відповідно до призначення:

L3master(config)# ip dhcp pool wifiVLAN

Визначаємо діапазон IP-адрес, які можуть надаватися DHCP-клієнтам у цьому пулі:

L3master(dhcp-config)# network 192.168.5.0 255.255.255.0

Вказуємо IP-адресу, яку DHCP-клієнти використовуватимуть як шлюз за замовчуванням:

L3master(dhcp-config)# default-router 192.168.5.254

Визначаємо IP-адресу DNS-сервера, яку DHCP-клієнти отримають для використання при вирішенні доменних імен

L3master(dhcp-config)# dns-server 8.8.8.8

Виключаємо із пулу адреси що вже були використані як статичні та не можуть бути присвоєні іншим пристроям:

L3master(config)# ip dhcp excluded-address 192.168.5.1, 192.168.5.2, 192.168.5.254

Усі команди ідентичні на обох L3 комутаторах. Кінцеві пристрої будуть отримувати адреси від активних комутаторів, які визначаються відповідно до налаштувань HSRP. Якщо один із комутаторів недоступний – інший виконає його функції.

Занесемо дані про налаштування інших DHCP пулів до таблиці 6.3.

Таблиця 6.3 – Конфігураційні дані DHCP пулів

dhcp pool	network	default-router	dhcp excluded-address
wifiVLAN	192.168.5.0	192.168.5.254	192.168.5.1 192.168.5.2 192.168.5.254
30Aud	192.168.30.0	192.168.30.254	192.168.30.1 192.168.30.2 192.168.30.254
31Aud	192.168.31.0	192.168.31.254	192.168.31.1 192.168.31.2 192.168.31.254
32Aud	192.168.32.0	192.168.32.254	192.168.32.1 192.168.32.2 192.168.23.254
33Aud	192.168.33.0	192.168.33.254	192.168.33.1 192.168.33.2 192.168.33.254
34Aud	192.168.34.0	192.168.34.254	192.168.34.1 192.168.34.2 192.168.34.254
35Aud	192.168.35.0	192.168.35.254	192.168.35.1 192.168.35.2 192.168.35.254
37Aud	192.168.37.0	192.168.37.254	192.168.37.1 192.168.37.2 192.168.37.254
39Aud	192.168.39.0	192.168.39.254	192.168.39.1 192.168.39.2 192.168.39.254

Окремо розглянемо налаштування DHCP пулу для VoiceVLAN.

L3master(config)# ip dhcp pool voiceVLAN

L3master(dhcp-config)# network 192.168.7.0 255.255.255.0

L3master(dhcp-config)# default-router 192.168.7.254

L3master(dhcp-config)# dns-server 8.8.8.8

Вказуємо IP-адресу TFTP-сервера для Cisco IP телефонів:

L3master(dhcp-config)# option 150 ip 192.168.6.100

Вказуємо альтернативну IP-адресу TFTP-сервера:

L3master(dhcp-config)# option 66 ip 192.168.6.101

Детальну інформацію про налаштовані DHCP пули можливо отримати командою show ip dhcp pool.

6.1.9 DHCP Snooping

DHCP snooping використовується для перевірки і валідації DHCP-відповідей [5], які надходять через порти комутатора. Це допоможе запобігти використанню фальшивих або підроблених DHCP-відпові. Більш детально особливості налаштування DHCP Snooping розписані у пункті 2.1.6.

Для активації DHCP Snooping на L3 комутаторах вводимо наступну команду:

L3master(config)# ip dhcp snooping

Перераховуємо усі VLAN’и, які використовуються для присвоєння динамічних адрес (5, 7, 30, 31, 32, 33, 34, 35, 37, 39):

L3master(config)# ip dhcp snooping vlan 5

L3master(config)# ip dhcp snooping vlan 7

L3master(config)# ip dhcp snooping vlan 30-35

L3master(config)# ip dhcp snooping vlan 37

L3master(config)# ip dhcp snooping vlan 39

Налаштовуємо фізичні інтерфейси на яких DHCP-сервер отримує запити від клієнтів як довірені:

L3master(config)# interface range gigabitEthernet 1/0/1-20

L3master(config-if)# ip dhcp snooping trust

В EVE-NG не розглядалось налаштування L2 комутаторів, тому заданий діапазон інтерфейсів визначається інтерфейсами, що напряму з’єднують активний та резервний DHCP сервер:

L3master(config)# interface range gigabitEthernet 0/0-1

L3master(config-if)# ip dhcp snooping trust

В кожному програмному додатку L3slave налаштовується ідентично до L3master.

Отримати більш детальну інформацію про DHCP Snooping потрібно за допомогою команди show ip dhcp snooping.

6.1.10 IP Source Guard

IP Source Guard контролює відповідность IP-адрес інтерфейсів мережевих пристроїв до DHCP binding таблиці комутатора. Це не дозволяє пакетам з підробленими або невірними IP-адресами надходити на мережеві порти.

Вмикаємо IPSG на довірених портах:

L3master(config)# interface range gigabitEthernet 1/0/1-20

L3master(config-if)# ip verify source dhcp-snooping

Змінюємо діапазон інтерфейсів в EVE-NG відповідно до пункту 6.1.9:

L3master(config)# interface range gigabitEthernet 0/0-1

L3master(config-if)# ip verify source dhcp-snooping

В кожному програмному додатку L3slave налаштовується ідентично до L3master.

6.1.11 ARP Inspection

ARP inspection використвоується для перевірки та валідації ARP-запитів та відповідей на комутаторі. Це допомагає запобігти атакам, які використовують підроблені ARP-пакети.

Налаштовуємо наступним чином:

Перераховуємо усі VLAN’и, які використвоуються для присвоєння динамічних адрес (5, 7, 30, 31, 32, 33, 34, 35, 37, 39)

L3master(config)# ip arp inspection vlan 5

L3master(config)# ip arp inspection vlan 5

L3master(config)# ip arp inspection vlan 7

L3master(config)# ip arp inspection vlan 30-35

L3master(config)# ip arp inspection vlan 37

L3master(config)# ip arp inspection vlan 39

L3master(config)# interface range gigabitEthernet 1/0/1-20

L3master(config-if)# ip arp inspection trust

Змінюємо діапазон інтерфейсів в EVE-NG відповідно до пункту 6.1.9:

L3master(config)# interface range gigabitEthernet 0/0-1

L3master(config-if)# ip arp inspection trust

В кожному програмному додатку L3slave налаштовується ідентично до L3master.

Для отримання більш детальної інформації про налашування arp inspection необхідно використати декілька команд, а саме: show ip arp inspection та show ip arp inspection interfaces.

6.1.12 Налаштування з’єднання та маршрутизації між L3switch та кластером Cisco ASA

Усі інтерфейси що під’єднанні до міжмережевих екранів ASA мають власні IP-адреси та налаштовуються на 3 рівні. Ці інтерфейси створюють додаткові підмережі які слід занести до протоколу динамичніої маршрутизавції OSPF [2].

Перший крок – налаштовуємо інтерфейси L3switch:

L3master(config)# interface gigabitEthernet 1/0/21

L3master(config-if)# no switchport

L3master(config-if)# ip address 10.0.3.1 255.255.255.0

L3master(config)# interface gigabitEthernet 1/0/22

L3master(config-if)# no switchport

L3master(config-if)# ip address 10.0.4.1 255.255.255.0

Другим кроком додамо нові підмережі до OSPF:

L3master(config)# router ospf 1

L3master(config-router)# network 10.0.3.0 0.0.0.255 area 1

L3master(config-router)# network 10.0.4.0 0.0.0.255 area 1

Налаштовуємо L3slave ідентично, але зі зміною IP-адрес GigabitEthernet 1/0/21 та GigabitEthernet 1/0/22 відповідно на 10.0.3.2 та 10.0.4.2.

Ідентичні налаштування потрібні для емуляції в EVE-NG, єдина відміннсть – замінити інтерфейси GigabitEthernet 1/0/21 та GigabitEthernet 1/0/22 на GigabitEthernet 1/2 і GigabitEthernet 1/3 відповідно на двох L3 комутаторах одразу.

7 ВІДМОВОСТІЙКИЙ КЛАСТЕР CISCO ASA

Cisco ASA (Adaptive Security Appliance) [7] – серія мережевих пристроїв, розроблених компанією Cisco, які використовуються для забезпечення мережевої безпеки. Cisco ASA надає комплексний захист від різних загроз за допомогою файрволу, системи виявлення вразливостей та підписів (IDS та IPS), VPN, можливості аналізувати трафік на рівні пакетів приймаючи рішення відповідно до заданих правил безпеки. Міжмережевий екран ASA забезпечує широкий функціонал та високу продуктивність.

Кластер, який складається із двох міжмережевих екранів побудовано на основі двох ASA 5525-X

ASA Failover Cluster буде використовуватися для встановлення високодоступної архітектури, де два пристрої ASA працюють як партнери. Якщо один з пристроїв виявляє відмову або проблему, то управління автоматично переходить на інший пристрій, забезпечуючи продовження роботи без втрати доступу до мережі та служб безпеки.

В усіх наступних пунктах розглядається налаштування лише в EVE-NG через незрівнянно більші можливості налаштування міжмережевих екранів у порівнянні із Cisco Packet Tracer.

Відмовостійкий кластер ASA формується у парі із кластером L3 комутаторів, що зображено на рисинку 7.1.

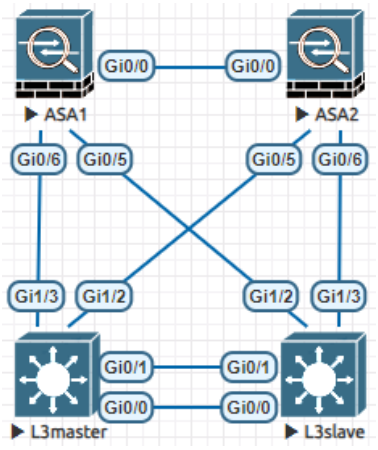

Рисунок 7.1 – Відмовостійкий кластер Cisco ASA

7.1 Налаштування інтерфейсів

Однією з найважливіших особливостей налаштування інтерфейсів Cisco ASA є параметр рівня безпеки (Security Level). Це числове значення в діапазоні від 0 до 100, де 100 є найвищим рівнем безпеки, а 0 – найнижчим. Рівень безпеки використовується для визначення довірливості інтерфейсу та контролю потоку трафіку між різними зонами мережі. Ключові слова, такі як inside та outside можуть використовуватися для створення читабельних та легко зрозумілих конфігурацій. Розглянемо налаштування інтерфейсів на міжмережевих екранах.

Першим буде налаштований екран ASA1. Вибираємо інтерфейс та задаємо IP-адресу:

```
asa(config)# interface gigabitEthernet 0/5
asa(config-if)# no shutdown
asa(config-if)# ip address 10.0.3.3 255.255.255.0
```

Встановлюємо ім’я (nameif) інтерфейсу відповідно до його призначення. GigabitEthernet0/5 під’єднаний до L3 комутатору тому він є одним із внутрішніх інтерфейсів:

```
asa(config-if)# nameif inside1
```

Встановлюємо максимальний рівень безпеки для інтерфейсу:

```
asa(config-if)# security-level 100
```

Аналогічно налаштовується GigabitEthernet 0/6 який також є внутрішнім інтерфейсом. Необхідно лише змінити IP-адресу та ім’я інтерфесу на inside2:

```
asa(config)# interface gigabitEthernet 0/6
asa(config-if)# no shutdown
asa(config-if)# ip address 10.0.4.3 255.255.255.0
asa(config-if)# nameif inside2
asa(config-if)# security-level 100
```

GigabitEthernet 0/1 є зовнішнім інтерфейсом, який веде до провайдера, відповідно змінюємо IP-адресу, назву та параметр рівня безпеки на мінімальний:

```
asa(config)# interface gigabitEthernet 0/1
asa(config-if)# no shutdown
asa(config-if)# ip address 200.200.20.1 255.255.255.0
asa(config-if)# nameif outside1
asa(config-if)# security-level 0
```

Налаштування ASA2 ідентичне по всім параметрам окрім IP-адрес інтерфейсів, так GigabitEthernet 0/5 має адресу 10.0.3.4/24, GigabitEthernet 0/6 10.0.4.4/24, GigabitEthernet 0/1 200.200.30.1/24.

7.2 Налаштування маршрутизації

Мережа запроектована як однорівнева, і весь мережевий трафік має пройти через один шлях до оператора мережі. Тому ми встановлюємо статичний маршрут, який визначає, що весь трафік із зовнішньої мережі повинен пройти через інтерфейс, який має IP-адресу 200.200.20.2.

```
asa(config)# route outside1 0.0.0.0 0.0.0.0 200.200.20.2
```

Налаштовуємо динамічну маршрутизацію OSPF вибравши унікальний ідентифікатор маршрутизатора для нашої локальної мережі:

```
asa(config)# router ospf 1
asa(config-router)# router-id 3.3.3.3
```

Вказуємо OSPF процесу які мережі повинні бути анонсовані:

```
asa(config-router)# network 10.0.3.0 255.255.255.0 area 1
asa(config-router)# network 10.0.4.0 255.255.255.0 area 1
```

Для коректної роботи динамічної та статичної маршрутизації одночасно необхідно ввести команду default-information originate яка вказує маршрутизатору генерувати стандартний маршрут за замовчуванням (0.0.0.0) і розповсюджувати його всередині OSPF області. Генерація маршруту за

замовчуванням спрощує конфігурацію та надає простий спосіб направлення трафіку за межі OSPF області.

asa(config-router)# default-information originate

7.3 NAT

NAT (Network Address Translation) – технологія мережевого протоколу, яка дозволяє приховати внутрішні IP-адреси комп'ютерів в локальній мережі за однією або декількома глобальними IP-адресами при виході в Інтернет. Головна мета NAT – забезпечити заміну IP-адреси одного пристрою в мережі іншою адресою при проходженні через маршрутизатор або файрвол.

Існує декілька видів NAT а саме: Static NAT, Dynamic NAT, PAT (Port Address Translation). Головним недоліком Static та Dynamic NAT є необхідність використовувати велику кількість глобальних адрес, тому в нашій мережі перевагу було віддано PAT, який дозволить всім внутрішнім IP-адресам використовувати один і той же зовнішній IP-адрес, але з різними портами.

В проектованій мережі налаштування PAT (NAT Overload) на кожному міжмережевому екрані є ідентичним.

Для налаштування PAT необхідно створити два об'єкти для кожної внутрішньої мережі, перший з ім'ям IN1OUT1 (скорочення від Inside1Outside1) та другий IN2OUT1 (Inside2Outside1). Розглянемо налаштування IN1OUT1:

asa(config)# object network IN1OUT1

Встановлюємо підмережу для об'єкта мережі IN1OUT1. В нашому випадку вказано 0.0.0.0 0.0.0.0 що означає будь-яку IP-адресу:

asa(config-network-object)# subnet 0.0.0.0 0.0.0.0

Встановлюємо правило NAT для об'єкта мережі IN1OUT1. В нашому випадку зазначено dynamic interface, що вказує на використання динамічного NAT і зазначення інтерфейсу outside1 в якості глобального інтерфейсу:

asa(config-network-object)# nat (inside1,outside1) dynamic interface

Налаштування об’єкта IN2OUT1 ідентичне, лише змінюємо внутрішній інтерфейс на inside2:

```
asa(config-network-object)# object network IN2OUT1
asa(config-network-object)# subnet 0.0.0.0 0.0.0.0
asa(config-network-object)# nat (inside2,outside1) dynamic interface
```

7.4 Налаштування політик

На Cisco ASA політики відносяться до правил і налаштувань, які визначають, як пристрій поводиться стосовно обробки мережевого трафіку. У контексті безпеки, політики дозволяють налаштовувати фільтрацію трафіку, аутентифікацію, авторизацію, інспекцію пакетів та інші правила.

Для проектуємої локальної мережі необхідно увімкнути інспекцію стандартних протоколів які використовуються усіма пристроями у локальній мережі, серед них: SSH, telnet, icmp, http, https. Реалізувати це потрібно наступним чином:

Створюємо нову політику обробки трафіку з іменем global_policy. У policy-map визначаються правила обробки різних класів трафіку та інструкції які слід виконати для кожного класу трафіку.

```
asa(config)# policy-map global_policy
```

Створюємо клас з іменем inspection_default в межах створеної політики. global_policy:

```
asa(config-pmap)# class inspection_default
```

Додаємо інспекцію для протоколів в межах створеного класу:

```
asa(config-pmap-c)# inspect SSH
asa(config-pmap-c)# inspect telnet
asa(config-pmap-c)# inspect icmp
asa(config-pmap-c)# inspect http
asa(config-pmap-c)# inspect https
```

Встановлюємо глобальну політику обробки трафіку що дозволить застосовувати визначену політику до всіх інтерфейсів пристрою:

```
asa(config)# service-policy global_policy global
```

7.5 Active-Backup ASA Cluster

Active-Backup ASA Cluster – тип конфігурації, в якій два міжмережевих екрана ASA працюють в групі, де один пристрій є активним, а інший є резервним. Це відноситься до технології Failover, яка забезпечує високу доступність і надійність мережевого обладнання. Active-Backup ASA Cluster дозволяє організувати резервне копіювання та переключення між пристроями так, щоб забезпечити безперервну роботу мережі в умовах відмови чи обслуговування. В цьому режимі роботи обидва пристрої повинні бути з'єднані через відведений інтерфейс для передачі інформації Failover LAN.

На відміну від режиму Active-Active є можливість налаштування VPN, що є дуже важливим аспектом для багатьох локальних мереж.

Розглянемо налаштування активного міжмережевого екрану ASA.

Першим кроком надамо відповідне до призначення ім'я міжмережевому екрану:

asa(config)# hostname ASAprimary

Вказуємо що пристрій буде основним (Primary) у парі, які працюють в режимі Failover:

ASAprimary(config)# failover lan unit primary

Визначаємо який інтерфейс буде використовуватися для передачі трафіку Failover між пристроями та даємо йому ім'я FAILLAN:

ASAprimary(config)# interface gigabitEthernet 0/0

ASAprimary(config-if)# no shutdown

ASAprimary(config)# failover lan interface FAILLAN gigabitEthernet0/0

Визначаємо IP-адресу та маску підмережі для інтерфейсу FAILLAN на активному пристрої (10.0.5.1/24) та IP-адресу резервного пристрою (10.0.5.2).

ASAprimary(config-if)# failover interfaces ip FAILLAN 10.0.5.1 255.255.255.0 standby 10.0.5.2

Встановлюємо ключ для забезпечення аутентифікації між активним і резервним пристроєм:

ASAprimary(config)# failover key Eu2Ldj94

Вказуємо що інтерфейс LANFAIL буде використовуватися для передачі даних Failover:

ASAprimary(config)# failover link FAILLAN

Внесемо зміни до конфігурацій інтерфейсів за допомогою додаткових IP-адрес резервного пристрою наступним чином:

ASAprimary(config)# interface gigabitEthernet 0/1

ASAprimary(config-if)# ip address 200.200.20.1 255.255.255.0 standby 200.200.30.1

ASAprimary(config)# interface gigabitEthernet 0/5

ASAprimary(config-if)# ip address 10.0.3.3 255.255.255.0 standby 10.0.3.4

ASAprimary(config)# interface gigabitEthernet 0/6

ASAprimary(config-if)# ip address 10.0.4.3 255.255.255.0 standby 10.0.4.4

Налаштовуємо резервний пристрій Cisco ASA:

asa(config)# hostname ASAsecondary

ASAsecondary(config)# failover lan unit secondary

ASAsecondary(config)# interface gigabitEthernet 0/0

ASAsecondary(config-if)# no shutdown

ASAsecondary(config)# failover lan interface FAILLAN gigabitEthernet0/0

ASAsecondary(config-if)# failover interface ip FAILLAN 10.0.5.1 255.255.255.0 standby 10.0.5.2

ASAsecondary(config)# failover key Eu2Ldj94

ASAsecondary(config)# failover link FAILLAN

Перевіряємо поточну конфігурацію та стан системи аварійного переключення (failover) за допомогою команди show failover, вивід якої зображено на рисунку 7.2.

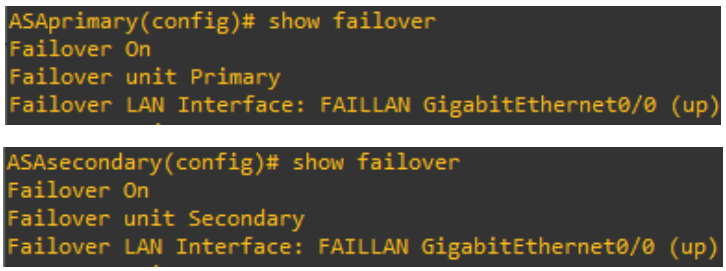

Рисунок 7.2 – Вивід команди show failover

7.6 ASA Site-to-Site VPN

VPN Site-to-Site [9] на Cisco ASA є одним з типів VPN який забезпечує безпечне з'єднання між двома або більше мережами та дозволяє об'єднати їх в єдину віртуальну мережу.

VPN Site-to-Site має свої унікальні переваги в порівнянні з іншими видами VPN, такими як Remote Access VPN або MPLS (Multiprotocol Label Switching). Однією з ключових переваг є можливість створювати постійні тунельні з'єднання між двома або більше корпоративними мережами що забезпечує передачу великих об'ємів даних. Це робить VPN Site-to-Site ідеальним варіантом для організацій з відділеннями або віддаленими офісами та найкраще підходить до нашої локальної мережі. У випадку масштабування проекту це дозволить з'єднати між собою відокремлені географічно LAN.

Безпека та шифрування є ще однією важливим аспектом. Трафік, який проходить через VPN Site-to-Site шифрується, що забезпечує високий рівень безпеки. Це надзвичайно важливо для захисту конфіденційної інформації.

Розглянемо налаштування VPN Site-to-Site у проектованый локальній мережі. Тунель буде "будуватися" до іншого мережевого (ASAremote) пристрою з IP 200.200.2.1 на зовнішньому інтерфейсі.

Підготовлюємо IKEv1 (Internet Key Exchange version 1) [9] для використання на зовнішньому інтерфейсі та вводимо в режим конфігурації політику IKEv1 з ідентифікатором 1:

ASAprimary(config)#crypto ikev1 enable outside1

ASAprimary(config)#crypto ikev1 policy 1

Для новоствореної політики ikev1 необхідно задати наступні парамтри: метод шифрування AES (Advanced Encryption Standard) для ініціюючого етапу обміну ключами, алгоритм хешування SHA (Secure Hash Algorithm) для генерації хеш-кодів в процесі обміну ключами, групу обміну ключами (DH Group) з номером 1, використання методу аутентифікації на основі спільного ключа та таймер «lifetime» що визначає як довго буде активний ключ обмінюватися між двома сторонами під час установки VPN-з'єднання (86400 секунд або 24 години):

ASAprimary(config-ikev1-policy)#encryption aes

ASAprimary(config-ikev1-policy)#hash sha

ASAprimary(config-ikev1-policy)#group 1

ASAprimary(config-ikev1-policy)#authentication pre-share

ASAprimary(config-ikev1-policy)#lifetime 86400

Створюємо IPsec LAN-to-LAN (L2L) тунель для групи тунелю (tunnel-group) де 200.200.2.1 – адреса віддаленого пристрою, з якою будується VPN-тунель:

ASAprimary(config)#tunnel-group 200.200.2.1 type ipsec-l2l

Визначаємо атрибути IPsec для групи тунелю 200.200.2.1:

ASAprimary(config)#tunnel-group 200.200.2.1 ipsec-attributes

Вказує використання методу аутентифікації на основі спільного ключа (pre-shared key) для IKEv1 тунелю:

ASAprimary(config-tunnel-ipsec)#ikev1 pre-shared-key 6xHS88p7Fz

Встановлюємо набір трансформацій для IPsec, який включає в себе шифрування AES-256 та хешування SHA:

ASAprimary(config-tunnel-ipsec)#crypto ipsec ikev1 transform-set vpn-transform-set esp-aes-256 esp-sha-hmac

Створюємо ACL [8] для визначення трафіку, що буде пересилатися через тунель, це підмережі 192.168.0.0/16 та 10.0.0.0/16 трафік яких направлено до хосту 200.200.2.1:

ASAprimary(config)# access-list 1 extended permit ip 192.168.0.0 255.255.0.0 host 200.200.2.1

ASAprimary(config)# access-list 1 extended permit ip 10.0.0.0 255.255.0.0 host 200.200.2.1

Встановлюємо відповідність між IPsec картою (crypto map) з ім’ям “RTT” та номером 1:

ASAprimary(config)#crypto map RTT-remote 1 match address 1

Встановлюємо параметри IPsec тунелю для crypto map з іменем "RTT" та номером 1:

ASAprimary(config)#crypto map RTT-remote 1 set peer 200.200.2.1

Вказуємо набір трансформацій, які використовуються для шифрування трафіку в тунелі:

ASAprimary(config)#crypto map RTT-remote 1 set transform-set vpn-transform-set

Вмикаємо Perfect Forward Secrecy (PFS) що надає додатковий рівень безпеки до процесу генерації ключів:

ASAprimary(config)#crypto map RTT-remote 1 set pfs

Вказуємо, що карта криптографічного відображення (crypto map) "RTT" буде використовуватися на зовнішньому інтерфейсі:

ASAprimary(config)#crypto map RTT-remote interface outside1

Конфігуруємо NAT для дозволу трафіку з мережі "Inside" досягати мережі "Remote" за допомогою двох додаткових об’єктів.

ASAprimary(config)# object network Inside

ASAprimary(config-network-object)# subnet 192.168.0.0 255.255.0.0

ASAprimary(config-network-object)# subnet 10.0.0.0 255.255.0.0

ASAprimary(config)# object network Remote

ASAprimary(config-network-object)# subnet 0.0.0.0 0.0.0.0

ASAprimary(config)# nat (inside1,outside1) source static Inside Inside destinatination static Remote Remote no-proxy-arp

Для коректної роботи VPN тунелю необхідний ідентичний список команд на пристрої із яким будується тунель. Зміни торкнуться IP адрес та ACL (через наявність відімінних локальних підмережі та різної політики маршрутизації трафіку). Розпишемо необхідну конфігурацію для віддаленого пристрою ASAremote:

ASAremote1(config)#crypto ikev1 enable outside1

ASAremote1(config)#crypto ikev1 policy 1

ASAremote1(config-ikev1-policy)#encryption aes

ASAremote1(config-ikev1-policy)#hash sha

ASAremote1(config-ikev1-policy)#group 1

ASAremote1(config-ikev1-policy)#authentication pre-share

ASAremote1(config-ikev1-policy)#lifetime 86400

ASAremote1(config)#tunnel-group 200.200.20.1 type ipsec-l2l

ASAremote1(config)#tunnel-group 200.200.20.1 ipsec-attributes

ASAremote1(config-tunnel-ipsec)#ikev1 pre-shared-key 6xHS88p7Fz

ASAremote(config-tunnel-ipsec)#crypto ipsec ikev1 transform-set vpn-transform-set esp-aes-256 esp-sha-hmac

ASAremote1(config)#access-list 1 extended permit ip 192.168.0.0 255.255.0.0 host 200.200.20.1

ASAremote1(config)#access-list 1 extended permit ip 0.0.0.0 0.0.0.0 host 200.200.20.1

ASAremote1(config)#crypto map RTT-remote 1 match address 1

ASAremote1(config)#crypto map RTT-remote 1 set peer 200.200.20.1

ASAremote1(config)#crypto map RTT-remote 1 set transform-set vpn-transform-set

ASAremote1(config)#crypto map RTT-remote 1 set pfs

ASAremote1(config)#crypto map RTT-remote interface outside1

Перевіяємо стан l2l VPN-тунелю командою show crypto ikev1 sa, що зображено на рисунку 7.3.

Рисунок 7.3 – Вивід команди show crypto ikev1 sa

Налаштування ASAsecondary та ASAremote2 відрізняється від ASAprimary та ASAremote1 лише IP-адресою віддаленого хосту із яким буде формуватися VPN-тунель та попередньо визначеним ключем. Розглянемо лише ті команди, які зазнали змін.

ASAsecondary:

ASAsecondary(config)# tunnel-group 200.200.3.1 type ipsec-l2l

ASAsecondary(config)# tunnel-group 200.200.3.1 ipsec-attributes

ASAsecondary(config-tunnel-ipsec)# ikev1 pre-shared-key g9D4ZnDt99

ASAsecondary(config)# access-list 1 extended permit ip 192.168.0.0 255.255.0.0 host 200.200.3.1

ASAsecondary(config)#access-list 1 extended permit ip 10.0.0.0 255.255.0.0 host 200.200.3.1

ASAsecondary(config)# crypto map RTT-remote 1 set peer 200.200.3.1

ASAremote2:

ASAremote2(config)# tunnel-group 200.200.30.1 type ipsec-l2l

ASAremote2(config)# tunnel-group 200.200.30.1 ipsec-attributes

ASAremote2(config-tunnel-ipsec)# ikev1 pre-shared-key g9D4ZnDt99

ASAremote2(config)# access-list 1 extended permit ip 192.168.0.0 255.255.0.0 host 200.200.30.1

ASAremote2(config)# access-list 1 extended permit ip 0.0.0.0 0.0.0.0 host 200.200.30.1

ASAremote2(config)# crypto map RTT-remote 1 set peer 200.200.30.1

8 ASTERISK ЯК ОСНОВА VOIP ЛОКАЛЬНОЇ МЕРЕЖІ

Asterisk – програмна система з відкритим кодом для реалізації IP-телефонії та інших послуг зв'язку через мережу IP. В першу чергу Asterisk використовується для створення IP-телефонних систем, де голосові дані передаються через Інтернет замість традиційних телефонних ліній. Asterisk має переваги порівняно з іншими VoIP програмами і вони пов'язані з гнучкістю та можливістю налаштування.

В запропонованій локальній мережі Asterisk буде налаштований на двох окремих серверах із використанням Keepalived, що дозволить створити відмовостійкий клатер та автоматично буде виявляти недоступність активного сервера та перенапрявляти трафік на резервний сервер для забезпечення неперервної роботи.

8.1 Завантаження Asterisk

Перед інсталяцією Asterisk рекомендується оновити системні пакети на сервері, що забезпечить загальну стабільність системи та актуалізує безпекові параметри. Зробити це потрібно двома командами:

root@ServerActive:/home/daniil# apt-get update

root@ServerActive:/home/daniil# apt-get upgrade

Необхідно також встановити build-essential [10], він містить базові інструменти для компіляції програмного забезпечення на системах, що використовують пакетний менеджер Advanced Package Tool (APT). Завантажуєжмо build-essential та інсталюємо:

root@ServerActive:/home/daniil# apt-get install build-essential

Мінімальний набір програмних пакетів, який необхідно встановити для коректної роботи Asterisk, включає в себе такі пакети, як: wget (отримання файлів з мережі), subversion (система контролю версій), git-core (встановлення Git), libjansson-dev (розробницькі файли для бібліотеки Jansson), sqlite (вбудовану систему управління базами даних), та пакети що

стосуються інструментів і бібліотек для автоматизації процесу компіляції програмного забезпечення з відкритим вихідним кодом: automake, autoconf, libncurses5-dev libtool, libxml2-dev. Інсталяюємо ці програмні засоби на кожен

root@ServerActive:/home/daniil# apt-get install wget subversion git-core libjansson-dev sqlite automake autoconf libncurses5-dev libtool libxml2-dev

Завантажуємо останню версію Asterisk 21 у стандартний каталог /usr/src/ командою wget, що була інстальована раніше:

root@ServerActive:/home/daniil# cd /usr/src/ && wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-21-current.tar.gz

Витягаємо архів інструментом tar:

root@ServerActive:/usr/src# tar zxf asterisk-21-current.tar.gz

8.2 Встановлення залежностей Asterisk

Перед інсталяцією Asterisk потрібно встановити залежності, що забезпечать належний функціонал та сумісність програми з різними середовищами. Наявності всіх необхідних залежностей є важливим етапом перед компіляцією та встановленням Asterisk.

Перед встановленням залежностей перейдемо до вихідного каталог Asterisk:

root@ServerActive:/home/daniil# cd /usr/src/asterisk-*/

Завантажимо скриптом contrib/scripts/get_mp3_source.sh аудіофайли у форматі MP3, які є необхідними для збирання модуля MP3 та корисні для роботи з MP3-файлами в Asterisk. Це надасть додаткові можливості Asterisk, наприклад відтворення аудіо-повідомлень або музики на утриманні під час очікування на лінії. Щоб виконати скрипт вводимо назву скрипта contrib/scripts/get_mp3_source.sh в директорії /usr/src/asterisk-21.0.0.

Скриптом contrib/scripts/install_prereq install встановлюємо залежності (пререквізити) Asterisk у системі. Це автоматизований спосіб встановити необхідні бібліотеки та інші компоненти, які необхідні для компіляції та правильної роботи Asterisk.

root@ServerActive:/usr/src/asterisk-21.0.0# contrib/scripts/install_prereq install

Скрипт виконано успішно, тому отримаємо вивід зображений на рисунку 8.1.

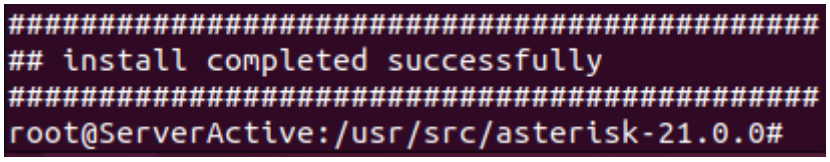

Рисунок 8.1 – Вивід успішно виконаного скрипту з встановлення залежностей

8.3 Інсталяція Asterisk

Після завантаження вихідних файлів для MP3 Asterisk необхідно збудував модуль MP3. Зробити це можливо вибравши формат format_mp3 в графічному інтерфейсі, що визивається командою make menuselect, як зображено на рисунку 8.2.

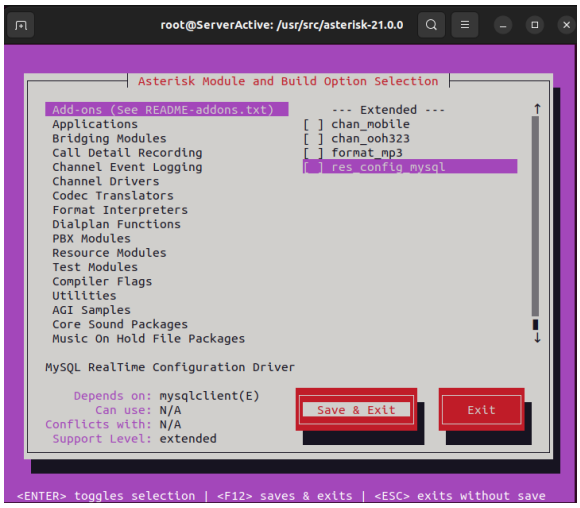

Рисунок 8.2 – Необхідні команди для MP3 модулю в графічному інтерфейсі

Починаємо процес компіляції Asterisk за допомогою інструменту make:

root@ServerActive:/usr/src/asterisk-21.0.0# make -j4

Значення -j залежить від кількості фізичних ядер на сервері та дозволяє прискорити процес компіляції. В нашому випадку їх 4.

Якщо компіляція завершена успішно, отримаємо вікно, зображене на рисунку 8.3.

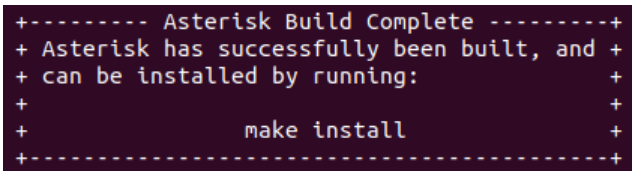

Рисунок 8.3 – Результат успішної компіляції Asterisk

Після успішної компіляції використаємо команду make install для встановлення скомпільованих бінарних файлів, файлів конфігурації та інших необхідних компонентів у відповідні каталоги:

root@ServerActive:/usr/src/asterisk-21.0.0# make install

Після успішного встановлення отримуємо вікно, зображене на рисунку 8.4.

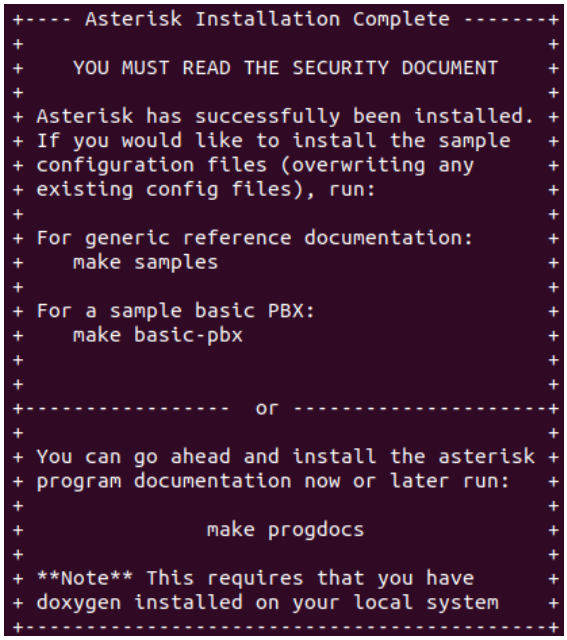

Рисунок 8.4 – Результат успішного встановлення Asterisk

Перед тим, як приступити до подальшого налаштування Asterisk, необхідно ввести три команди: make samples, make config, та ldconfig.

Команда make samples встановлює набір файлів, які містять базові налаштування та приклади конфігурацій для різних аспектів системи Asterisk.

Ці файли прикладів можуть включати конфігурації для різних типів підключень, телефонів, голосових послуг та інших аспектів системи.

Команда make config встановлює init-скрипт для Asterisk. Init-скрипт використовується для керування запуском, зупинкою та перезапуском Asterisk. Це дозволяє легко керувати життєвим циклом служби Asterisk на системі, забезпечуючи автоматичний запуск при старті системи та інші операції управління службою.

Команда ldconfig є необхідною для оновлення та налаштування системного кешу об’єктів динамічного виклику (shared libraries). Вона допомагає системі правильно визначати шляхи до бібліотек та їх версії під час виконання програм, поліпшуючи ефективність та стабільність системи.

8.4 Створення користувача Asterisk

За замовчуванням Asterisk працює як користувач root. З міркувань безпеки необхідно створити нового користувача і налаштувати Asterisk для запуску від його імені. Створюємо системного користувача з ім'ям “asterisk”, який буде використовуватися для виконання служб Asterisk PBX (Private Branch Exchange) наступною командою:

root@ServerActive:/home/daniil# adduser --system --group --home /var/lib/asterisk --no-create-home --gecos “Asterisk PBX” asterisk

Щоб налаштувати Asterisk для запуску від імені користувача asterisk, редагуємо файл /etc/default/asterisk і розкоментуємо (видаляємо #) наступні 2 рядки, як зображено на рисунку 8.5.

AST_USER="asterisk"

AST_GROUP="asterisk"

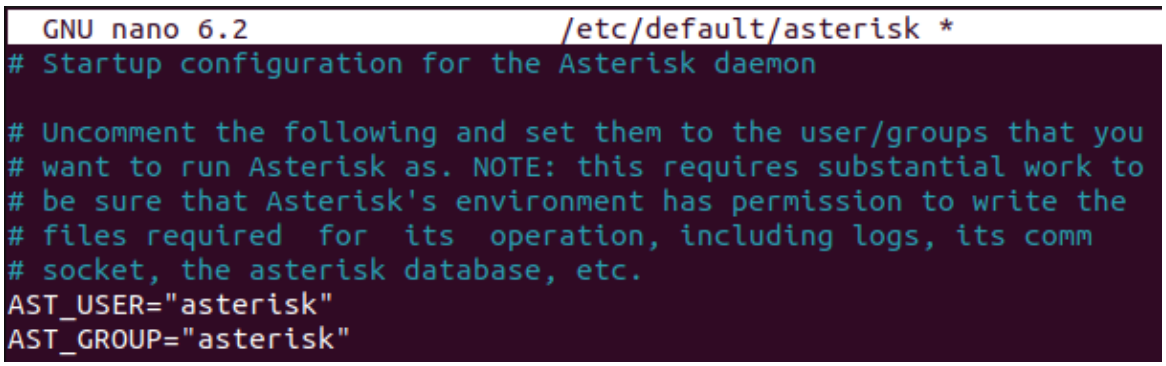

Рисунок 8.5 – Відредагований файл /etc/default/asterisk

Додаємо користувача asterisk до груп dialout та audio що є необхідним для забезпечення правильного доступу до портів зв'язку (USB-портів для модемів) та аудіо-пристроїв за допомогою наступної команди:

root@ServerActive:/home/daniil# usermod -a -G dialout,audio asterisk

Змінюємо власника та дозволи для всіх файлів і каталогів Asterisk, після чого Asterisk матиме доступ до них:

root@ServerActive:/home/daniil# sudo chown -R asterisk: /var/{lib,log,run,spool}/asterisk /usr/lib/asterisk /etc/asterisk

root@ServerActive:/home/daniil# sudo chmod -R 750 /var/{lib,log,run,spool}/asterisk /usr/lib/asterisk /etc/asterisk

8.5 Запуск Asterisk

Запускаємо Asterisk, використовуючи команду systemctl start asterisk, та перевіряємо його статус за допомогою команди systemctl status asterisk. Інший способом перевірити роботу Asterisk – через командний рядок. Використовуємо команду core show uptime після входу до Astersik CLI. Результати перевірки працездатності Asterisk зображено на рисунках 8.6 та 8.7.

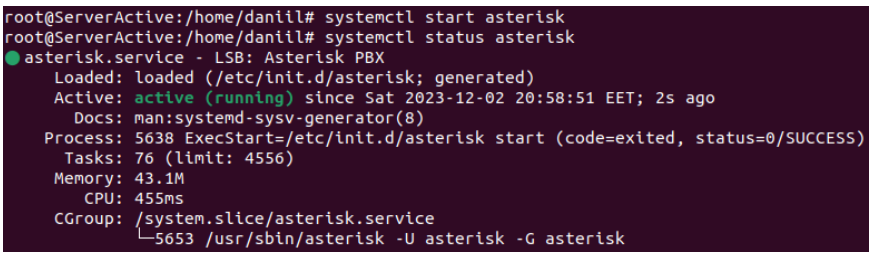

Рисунок 8.6 – Перевірка статусу Asterisk через systemctl

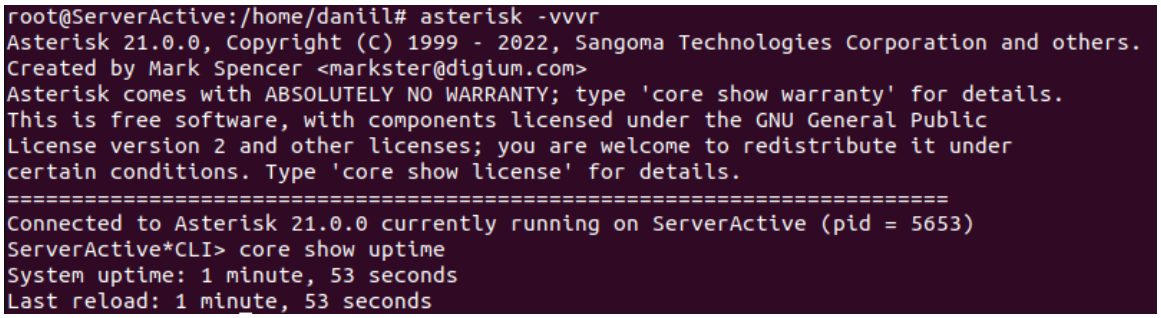

Рисунок 8.7 – Перевірка статусу Asterisk через Astersik CLI

Також необхідно налаштувати автоматичний запуск служби Asterisk під час завантаження системи за допомогою systemd та команди systemctl enable asterisk, що зображено на рисунку 8.8.

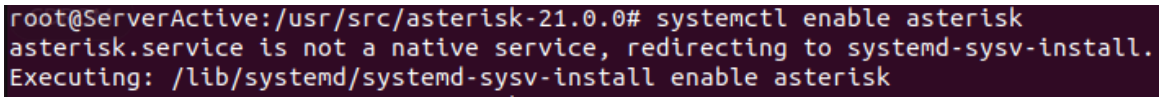

Рисунок 8.8 – Активація автоматичного запуску служби Asterisk

8.6 Налаштування конфігураційного файлу sip.conf

Файл sip.conf є одним з найважливіших конфігураційних файлів Asterisk, який використовується для налаштування параметрів SIP (Session Initiation Protocol) – протоколу для установки, управління та розриву аудіо та відеозв'язку через Інтернет. Файл містить параметри для SIP-клієнтів і серверів Asterisk та дозволяє визначати різні аспекти конфігурації, такі як імена користувачів, їх паролі, хостинг, кодеки, контексти та інше. Налаштування sip.conf зображено на рисунку 8.9.

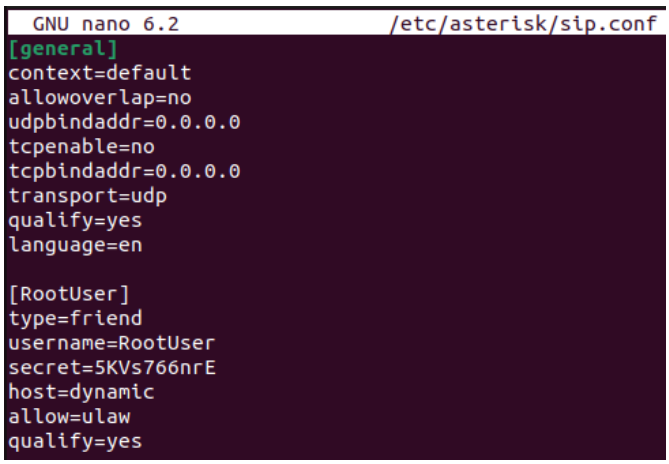

Рисунок 8.9 – Конфігураційні параметри файлу sip.conf

Розглянемо кожний параметр файлу окремо.

[general] – розділ, який містить загальні налаштування для всього програмного файлу;

context=default – стандартний контекст для SIP-з'єднань;

allowoverlap=no – забороняємо накладення дзвінків;

udpbindaddr=0.0.0.0 – прив'язуємо UDP-сокет до Asterisk;

tcpenable=no – вимикаємо TCP;

tcpbindaddr=0.0.0.0 – прив'язуємо TCP-сокет до Asterisk;

transport=udp – вказуємо UDP як транспортний протокол;

qualify=yes – встановлюємо, що Asterisk періодично робить тест доступності для користувачів;

language=en – задаємо англійську мову за замовчуванням для користувачів SIP;

[RootUser] – ідентифікатор користувача;

type=friend – визначає тип користувача;

username= RootUser – вказуємо ім'я користувача SIP;

secret=5KVs766nrE – встановлюємо пароль для користувача SIP;

host=dynamic – визначаємо що користувач може підключатися з будь-якої IP-адреси.

allow=ulaw – вказуємо жозволений аудіокодек ulaw;

qualify=yes – включаємо тест тест доступності користувача.

Додатково встановлюємо обмеження на кількість спроб авторизації для SIP-каналу, що допоможе уникнути brute force атаки. Налаштовується в /etc/asterisk/sip.conf як зображено на рисунку 8.10.

Рисунок 8.10 – Налаштування захисту від brute force атак

8.7 Налаштування Firewall

Налаштування файрвола для правильної роботи Asterisk на Ubuntu включає в себе встановлення необхідних правил для дозволу трафіку, який використовується для забезпечення зв’язку через протоколи SIP та RTP.

Відкриваємо порти, які використовуються для SIP-сигналізації та RTP-потоків. Зазвичай це порти 5060 (SIP) та діапазон портів для RTP (від 10000 до 20000).

root@ServerActive:/home/daniil# ufw allow 5060/udp

root@ServerActive:/home/daniil# ufw allow 10000:20000/udp

9 KEEPALIVED ЯК ОСНОВА ВІДМОВОСТІЙКОГО КЛАСТЕРУ ASTERISK

Keepalived – програмне забезпечення для лінукс-систем, яке надає можливість створювати відмовостійкі конфігурації для мережевих сервісів. Переважно використовується для забезпечення високої доступності (High Availability) для систем, таких як веб-сервери, бази даних, електронна пошта і т.д. У випадку Asterisk, який є програмним комутатором телефонії (PBX), Keepalived буде використаний для забезпечення відмовостійкості телефонної системи. Основні компоненти Keepalived, які використовуються для цього – Virtual IP (VIP) та Virtual Router Redundancy Protocol (VRRP).

Налаштовуватися Keepaliverd на двох серверах Ubuntu 22.04.3 LTS з попередньо всстановленим Asterisk. Перевіримо IP-адреси на Active та Backup серверах і наявність зв’язку між ними, результати наведені на рисунку 9.1.

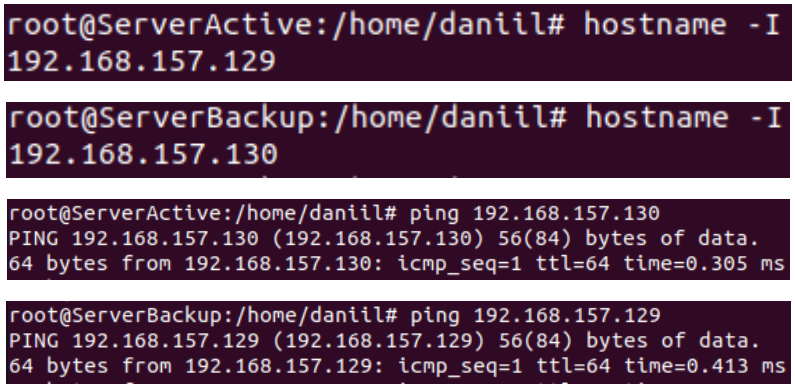

Рисунок 9.1 – перевірка доступності серверів VoIP

Виберемо IP-адресу 192.168.157.254 як Virtual IP для обох машин. Ця IP-адреса використовується як вхідна точка для обслуговування трафіку, і вона може бути перенаправлена між різними серверами в групі в залежності від їхнього стану (активний або пасивний).

9.1 Встановлення Keepalived

Встановимо на сервери ubuntu Keepalived та додамо сервіс в автозавантаження [11]:

root@ServerActive:/home/daniil# apt install keepalived

root@ServerActive:/home/daniil# systemctl enable keepalived

9.2 Налаштування конфігураційного файлу keepalived

Конфігураційний файл Keepalived – текстовий файл, який містить параметри та налаштування для правильної роботи програми Keepalived. Цей файл визначає різні аспекти конфігурації, такі як параметри VRRP (Virtual Router Redundancy Protocol), налаштування служб, віртуальні IP-адреси та інші параметри, необхідні для забезпечення високостійкості та надійності мережі. Коректна конфігурація є ключовою для успішної інтеграції та роботи Keepalived у локальній мережі.

Перед налаштування конфігураційного файлу через текстовий редактор nano визначимо інтерфейси та їх IP адреси за допомогою команди ip a, що показано на рисунку 9.2.

```
root@ServerActive:/home/daniil# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:79:8e:a3 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.157.129/24 brd 192.168.157.255 scope global dynamic noprefixroute ens33
       valid_lft 1201sec preferred_lft 1201sec
    inet6 fe80::6503:f1dc:59c6:6235/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
root@ServerBackup:/home/daniil# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:83:4f:97 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.157.130/24 brd 192.168.157.255 scope global dynamic noprefixroute ens33
       valid_lft 1781sec preferred_lft 1781sec
    inet6 fe80::1697:b354:8bd6:9192/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Рисунок 9.2 – Детальна інформація про існуючи інтерфейси

9.2.1 Налаштування конфігураційного файлу на ServerActive

Конфігураційний файл keepalived.conf містить параметри та налаштування, які визначають як буде працювати Keepalived. В проектуємій локальный мережі файл keepalived.conf описує параметри конфігурації для відмовостійкого кластера Asterisk. Повний код наведений на рисунку 9.3.

```
root@ServerActive:/home/daniil# cat /etc/keepalived/keepalived.conf
vrrp_script asterisk_self {
       script "/usr/bin/killall -0 asterisk"
       interval 1
       fall 5
       rise 3
       weight -15
}
vrrp_instance AsteriskVRRP {
    state MASTER
    interface ens33
    virtual_router_id 2
    priority 101
    unicast_src_ip 192.168.157.129
    unicast_peer {
    192.168.157.130
        }
   advert_int 1
   authentication {
        auth_type PASS
        auth_pass 2rFYhx35E2
        }
    virtual_ipaddress {
        192.168.157.254/24
        }
        track_script {
            asterisk_self
     }
}
```

Рисунок 9.3 – Конфігураційний файл keepalived.conf активного серверу

Розглянемо кожну частину цього файлу:

vrrp_script asterisk_self { ... } – створюємо сценарій VRRP з назвою “asterisk_self”;

script "/usr/bin/killall -0 asterisk" – сценарій для перевірки того, чи запущений Asterisk. Використовує команду killall з сигналом 0, який фактично не відправляє сигнал, але використовується для перевірки існування процесу;

interval 2 – частота виконання сценарію (1 секунда);

fall 5 – кількість послідовних невдач, необхідних для спричинення зміни стану на резервний;

rise 3 – кількість послідовних успіхів, необхідних для спричинення зміни стану назад на головний;

weight -15 – вага, надана сценарію. Негативна вага означає, що невдача зменшить пріоритет екземпляра VRRP;

vrrp_instance AsteriskVRRP { ... } – створюємо сценарій VRRP з назвою "AsteriskVRRP";

state MASTER – вказуємо що цей сервер починає як майстер (має вищий пріоритет);

interface ens33 – визначає мережевий інтерфейс, на якому відбуватиметься обмін пакетами;

virtual_router_id 2 – унікальний ідентифікатор екземпляра VRRP у межах домену трансляції;

priority 101 – пріоритет сервера. Чим вище значення, тим вищий пріоритет. Майстром стає сервер з найвищим пріоритетом;

unicast_src_ip 192.168.157.129 – IP-адреса джерела для unicast комунікації між серверами;

unicast_peer { 192.168.157.130 } – IP-адрес сервера, з яким відбувається unicast комунікація;

advert_int 1 – інтервал відправлення анонсів (advertisement) в секундах;

authentication { auth_type PASS auth_pass 2rFYhx35E2 } – налаштування аутентифікації за допомогою пароля;

virtual_ipaddress { 192.168.157.254/24 } – віртуальна IP-адреса, яку ділять головний і резервний вузли;

track_script { asterisk_self } – асоціює раніше визначений сценарій "asterisk_self" з цим екземпляром VRRP. Якщо сценарій не вдасться, це вплине на пріоритет екземпляра VRRP.

9.2.2 Налаштування конфігураційного файлу на ServerBackup

Головною відмінністю налаштування другого (резервного) сервера є відсутність сценарію VRRP з назвою “asterisk_self”. В сценарії "AsteriskVRRP" сервер встановлюється як BACKUP, а значення пріоритету

нижче, ніж на MASTER. Для unicast запитів міняємо місцями IP-адреси. Всі інші налаштування ідентичні до ServerActive. Скрипт наведено на рисунку 9.4.

```
root@ServerBackup:/home/daniil# cat /etc/keepalived/keepalived.conf
vrrp_instance AsteriskVRRP {
    state BACKUP
    interface ens33
    virtual_router_id 2
    priority 100
    unicast_src_ip 192.168.157.130
    unicast_peer {
    192.168.157.129
        }
   advert_int 1
   authentication {
        auth_type PASS
        auth_pass 2rFYhx35E2
        }
    virtual_ipaddress {
        192.168.157.254/24
        }
}
```

Рисунок 9.4 – Конфігураційний файл keepalived.conf резервного серверу

9.2.3 Перевірка працездатності Keepalived на кластері VoIP

Для перевірки стану інтерфейсів та конфігурації Keepalived використаємо команду ip a. Якщо Keepalived працює коректно та головний сервер (Active) переадресовує віртуальну IP-адресу на себе як додаткову, в той час як на резервному залишається лише одна, що зображено на рисунку 9.5.

```
root@ServerActive:/home/daniil# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:79:8e:a3 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.157.129/24 brd 192.168.157.255 scope global dynamic noprefixroute ens33
       valid_lft 1425sec preferred_lft 1425sec
    inet 192.168.157.254/24 scope global secondary ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::6503:f1dc:59c6:6235/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
root@ServerBackup:/home/daniil# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:83:4f:97 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.157.130/24 brd 192.168.157.255 scope global dynamic noprefixroute ens33
       valid_lft 1050sec preferred_lft 1050sec
    inet6 fe80::1697:b354:8bd6:9192/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Рисунок 9.5 – Перевірка Keepalived для штатної роботи VoIP кластеру

Перевіримо як кластер відреагує на припинення роботи Asterisk на основному сервері, для цього зупинимо процес командою systemctl stop asterisk. Як і очікувалось, якщо зупини процес Asterisk на активному пристрої то віртуальна IP-адреса “переїде” до резервного серверу, що зображено на рисунку 9.6.

```
root@ServerActive:/home/daniil# systemctl stop asterisk
root@ServerActive:/home/daniil# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:79:8e:a3 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.157.129/24 brd 192.168.157.255 scope global dynamic noprefixroute ens33
       valid_lft 1008sec preferred_lft 1008sec
    inet6 fe80::6503:f1dc:59c6:6235/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
root@ServerBackup:/home/daniil# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:83:4f:97 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.157.130/24 brd 192.168.157.255 scope global dynamic noprefixroute ens33
       valid_lft 1682sec preferred_lft 1682sec
    inet 192.168.157.254/24 scope global secondary ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::1697:b354:8bd6:9192/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Рисунок 9.6 – Перевірка Keepalived для позаштатної роботи VoIP кластеру

Також для коректної роботи Asterisk необхідно дадати декілька правил до iptables. При використанні multicast правила однакові для Active та Backup, і виглядають наступним чином:

root@ServerActive:/home/daniil# iptables -A INPUT -i ens33 -d 224.0.0.0/8 -j ACCEPT

root@ServerActive:/home/daniil# iptables -A INPUT -p vrrp -i ens33 -j ACCEPT

Для unicast правила між серверами будуть відрізнятися. Правила для Active:

root@ServerActive:/home/daniil# iptables -A INPUT -i ens33 -d 192.168.157.129/24 -j ACCEPT

root@ServerActive:/home/daniil# iptables -A INPUT -p vrrp -i ens33 -j ACCEPT

Правила для Backup:

root@ServerActive:/home/daniil# iptables -A INPUT -i ens33 -d 192.168.157.130/24 -j ACCEPT

root@ServerActive:/home/daniil# iptables -A INPUT -p vrrp -i ens33 -j ACCEPT

ВИСНОВКИ

У ході виконання дипломного проекту була ретельно розглянута та успішно реалізована задача проектування відмовостійкої локальної мережі для кафедри «Радіотехніка та телекомунікації». Для забезпечення високої доступності та стабільності мережевої інфраструктури було вирішено використовувати відмовостійкі кластери L3-комутаторів та ASA.

Однією з ключових складових відмовостійкої архітектури є використання відмовостійких кластерів L3-комутаторів. Ці кластери забезпечують неперервну роботу мережі у випадку відмови одного з комутаторів. Алгоритми кластеризації дозволяють розподіляти трафік та переключати його на інший активний комутатор у випадку виявлення відмови. Це сприяє зменшенню впливу відмов на роботу мережі та забезпеченню стабільності мережі вцілому.

Крім того, для забезпечення безпеки та доступності інтернет-з’єднання на кафедрі, був використаний відмовостійкий кластер ASA. ASA виступає в ролі брандмауера та VPN-концентратора, а використання кластеру дозволяє забезпечити неперервну роботу безпекових параметрів навіть у випадку відмови одного з пристроїв.

Загальна відмовостійкість системи досягається завдяки впровадженню дублювання ключових елементів мережі та механізмів автоматичного відновлення в разі відмови. Це робить отриману мережеву інфраструктуру надійною, ефективною та готовою відповідати високим стандартам доступності та безпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Cisco CCENT/CCNA ICND1 100-101 Академическое издание, Уэнделл Одом, 2015. – 903 с.

2. Cisco CCNA ICND2 200-101 Маршрутизация и коммутация Академическое издание, Уэнделл Одом, – 2015. – 737 с.

3. Cisco. (n.d.). Cisco Catalyst 2960 Series Switches Software Configuration Guide, Release 12.2(40)SE. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_40_se/configuration/guide/scg.pdf (дата звернення 29.09.2023). – Назва з екрану.

4. Cisco. HSRP Configuration Guide. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/9234-hsrpguidetoc.html (дата звернення 29.09.2023). – Назва з екрану.

5. Cisco. Configuring DHCP Server. [Електронний ресурс] – Режим доступу: //www.cisco.com/en/US/docs/ios/12_4t/ip_addr/configuration/guide/htdhcpsv.html (дата звернення 29.09.2023). – Назва з екрану.

6. Cisco. Understanding VLAN Trunk Protocol (VTP). [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html (дата звернення 15.10.2023). – Назва з екрану.

7. Cisco. ASDM 7.8 Configuration Guide - General. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/general/asdm-78-general-config.html (дата звернення 29.09.2023). – Назва з екрану.

8. Cisco. ASDM 7.8 Configuration Guide - Firewall. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/security/

asa/asa98/asdm78/firewall/asdm-78-firewall-config.html (дата звернення 28.10.2023). – Назва з екрану.

9. Cisco. ASDM 7.8 Configuration Guide - VPN. [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/vpn/asdm-78-vpn-config.html (дата звернення 14.11.2023). – Назва з екрану.

10. Asterisk Documentation - Getting Started. [Електронний ресурс] – Режим доступу: https://docs.asterisk.org/Getting-Started/Hello-World/#configure-chan_sip (дата звернення 29.11.2023). – Назва з екрану.

11. Keepalived Documentation. [Електронний ресурс] – Режим доступу: https://keepalived.readthedocs.io/en/latest/installing_keepalived.html (дата звернення 30.11.2023). – Назва з екрану.