

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту інфраструктури
локальної IPv4/IPv6 мережі компанії»

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

Термін здачі студентом закінченої роботи 30 червня 2022 р.

Вихідні дані роботи:

1. Cisco Packet Tracer

2. Схема мережі

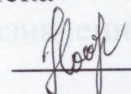
3. Маршрутизатори Cisco ISR433

4. Комутатори Cisco

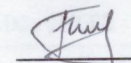
5. Багаторівневі ком

Виконав студент 4-го курсу групи КБ-2

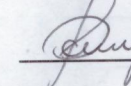
спеціальності 125 «Кібербезпека»

 Носов Є.С.

Керівник старший викладач КІ та КБ

 Покотило О.А.

Рецензент старший викладач КІ та КБ

 Байлюк Є.М.

Житомир – 2022

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
1 березня 2022 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Носов Євгеній Станіславович

Тема роботи: «Проект підсистеми захисту інфраструктури локальної IPv4/IPv6 мережі компанії»

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

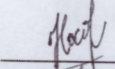
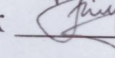
Термін здачі студентом закінченої роботи 30 червня 2022 р.

Вихідні дані роботи:

1. Cisco Packet Tracer
2. Схема мережі
3. Маршрутизатори Cisco ISR433
4. Комутатори Cisco Catalyst 2960
5. Багаторівневі комутатори Cisco Catalyst 3650

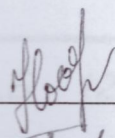
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

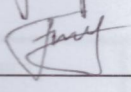
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Покотило О.А.	 06.03.2022	 06.03.2022
2	Покотило О.А.	 20.04.2022	 20.04.2022
3	Покотило О.А.	 11.05.2022	 11.05.2022

Студент  Носов Є.С.
Керівник  Покотило О.А.

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	6 березня 2022 – 7 березня 2022	Виконано
2	Пошук та аналіз інформації щодо топології локальних мереж	8 березня 2022 – 16 березня 2022	Виконано
3	Розгляд поширених атак на мережу	17 березня 2022 – 20 березня 2022	Виконано
4	Вибір обладнання для побудови мережі	21 березня 2022 – 25 березня 2022	Виконано
5	Розробка проекту мережі	26 березня 2022 – 2 квітня 2022	Виконано
6	Проектування підсистем захисту мережі	3 квітня 2022 – 6 квітня 2022	Виконано
7	Налаштування пристроїв мережі	7 квітня 2022 – 12 квітня 2022	Виконано
8	Тестування й аналіз роботи мережі	20 квітня 2022 – 24 квітня 2022	Виконано
9	Написання пояснювальної записки	22 травня 2022 – 29 травня 2022	Виконано
10	Підготовка доповіді та презентації	30 травня 2022 – 1 червня 2022	Виконано
11	Отримання відгуку та рецензії на кваліфікаційну роботу	29 червня	
12	Захист	30 червня	

Студент  Носов Є.С.

Керівник  Покотило О.А.

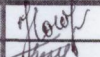
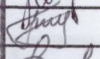
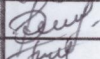
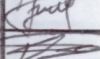
АНОТАЦІЯ

Кваліфікаційна робота складається з проєкту підсистеми захисту інфраструктури локальної IPv4/IPv6 мережі компанії та пояснювальної записки до нього. Пояснювальна записка містить 43 сторінки, 25 ілюстрацій та 1 таблицю.

Метою роботи є розробка проєкту підсистеми захисту інфраструктури локальної IPv4/IPv6 мережі компанії.

В роботі було розглянуто теоретичні відомості про локальні мережі, технології їх побудови та захисту. Проаналізовано можливі загрози та наведено можливі засоби та методи захисту мережі від них. Також в роботі було обґрунтовано вибір мережевих пристроїв Cisco, надана основна інформація про використовувані комутатори та маршрутизатори. Розроблено та налагоджено проєкт мережі та були проведені налаштування захисту. Схема мережі була розроблена в Cisco Packet Tracer. Також наведено результати тестування працездатності системи.

Ключові слова: МЕРЕЖА, ЛОКАЛЬНА, ЗАХИСТ, ЗАГРОЗИ, CISCO

					КІК.КР.Б – 125 – 15 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми захисту інфраструктури локальної IPv4/IPv6 мережі компанії	Літ.	Арк.	Аркушів
Розроб.		Носов Є.С.		20.06				
Керівник		Покотило О.А.		20.06				
Реценз.		Байлюк Є.М.		20.06				
Ч. Кадров		Покотило О.А.		20.06				
Затверд.		Єфіменко А.А.		20.06		ФІКТ, Гр. КБ-2		

ANNOTATION

The qualification work consists of the project of the infrastructure protection subsystem of the company's local IPv4 / IPv6 network and an explanatory note to it. The explanatory note contains 43 pages, 25 illustration and 1 table.

The purpose of the work is to develop a subsystem for the protection of the infrastructure of the local IPv4 / IPv6 network of the company.

Theoretical information about local networks, technologies of their construction and protection was poured into the work. Possible threats are analyzed and possible means and methods of network protection from them are given. The paper also substantiated the choice of Cisco network devices, provided basic information about the switches and routers used. The network project was developed and adjusted and security settings were made. The network scheme was developed in Cisco Packet Tracer. The results of system performance testing are also presented.

Keywords: NETWORK, LOCAL, PROTECTION, THREATS, CISCO

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				4
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	7
РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ТА ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ.....	8
1.1 Топологія локальних мереж	8
1.2 Аналіз технологій побудови локальної мережі.....	11
1.3 Аналіз мережевих атак	17
РОЗДІЛ 2 ПРОЄКТ ПОБУДОВИ ТА ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ.....	20
2.1 Вибір обладнання для організації роботи мережі.....	20
2.2 Розробка топології комп'ютерної мережі	22
2.3 Розробка схеми адресації мережі.....	27
РОЗДІЛ 3 НАЛАГОДЖЕННЯ ЛОКАЛЬНОЇ МЕРЕЖІ.....	34
3.1 Базове налагодження пристроїв.....	34
ВИСНОВКИ	41
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	42
ДОДАТКИ	44

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

LAN – Local Area Networks

MAC – Media Access Control

VLAN – Virtual Local Area Networks

VRRP – (англ. Virtual Router Redundancy Protocol) – Протокол резервування віртуального маршрутизатора.

DHCPv6 – Dynamic Host Configuration Protocol version 6 — протокол динамічної конфігурації вузла для IPv6.

IPv6 – Internet Protocol version 6.

STP – spanning-tree protocol – протокол кістякового дерева.

TCP – Transmission Control Protocol – протокол керування передачею.

OSPF – Open Shortest Path First.

LACP – (англ. Link Aggregation Control Protocol) – Протокол управління агрегацією каналів.

HSRP – (англ. Hot Standby Router Protocol) – Протокол маршрутизатора гарячого режиму очікування.

MST – (англ. Multiple Spanning Tree) – протокол множинного сполучного дерева.

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Обрана тема є дуже важливою, так як питання забезпечення безпеки мережі на сьогоднішній день як ніколи актуальні в організації будь-якого масштабу і області роботи. Ми можемо бачити швидкий розвиток інформаційних технологій, тому завжди потрібно думати про те чи захищена ваша мережа.

Актуальність теми. Дуже важливо, щоб в мережі дані, які зберігаються на комп'ютерах чи інших пристроях були захищені. Більшість цих даних є конфіденційними, тому для них несанкціонований доступ або викриття – недопустимі.

Метою кваліфікаційної роботи є розробка проєкту захисту інфраструктури локальної IPv4/IPv6 мережі компанії.

Визначена мета обумовлює наступні завдання:

- Огляд теоретичних основ побудови та захисту локальних мереж
- Розробка проєкту мережі
- Базове налаштування , та налаштування захисту мережі

Об'єктом дослідження є захист локальних мереж компаній.

Предметом дослідження є процес захисту локальної мережі

У процесі виконання кваліфікаційної роботи було розроблено проєкт підсистеми захисту інфраструктури локальної IPv4/IPv6 мережі компанії.

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ТА ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ

1.1 Топологія локальних мереж

Локальні мережі (**Local Area Networks, LAN**) – це об'єднання комп'ютерів, зосереджених на невеликій території, зазвичай в радіусі не більше 1-2 км. У загальному випадку локальна мережа є комунікаційною системою, що належить одній організації [1].

Склад локальної мережі :

1. Комп'ютери – програмно-керовані пристрої для проведення обчислень, а також приймання, оброблення, зберігання і передачі інформації.
2. Мережеві адаптери – периферійний пристрій, що дозволяє ком'ютеру взаємодіяти з іншими пристроями мережі.
3. Периферійний пристрій – частина апаратного забезпечення , призначена для передавання інформації від і до комп'ютера.
4. Передавальне середовище – фізичне середовище, у якому можливе передавання інформаційних сигналів у вигляді електричних, світлових та інших імпульсів.
5. Мережеві пристрої – необхідні пристрої для роботи комп'ютерної мережі. В локальних мережах використовуються: концентратори, комутатори, мости та маршрутизатори[2].

Найпоширенішими реалізаціями локальних мереж є Ethernet, Token Ring, FDDI.

Ethernet – найпоширеніший протокол у сучасних локальних комп'ютерних мережах, він тісно пов'язаний з моделлю TCP/IP, оскільки у більшості випадків використовується для передачі IP-пакетів[3].

Термін Ethernet відноситься до сімейства продуктів локальної мережі (LAN), які охоплюються стандартом IEEE 802.3, який визначає те, що широко відоме як протокол CSMA/CD. Наразі визначено чотири швидкості передачі даних для роботи по оптичному волокну та кабелю з витою парою:

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

- 10 Мбіт/с—10Base-T Ethernet
- 100 Мбіт/с — Fast Ethernet
- 1000 Мбіт/с — Gigabit Ethernet
- 10 000 Мбіт/с—10 Gigabit Ethernet

Технологія Ethernet є основною технологією локальної мережі через наступні характеристики:

- Легкий для розуміння, реалізування, керування та обслуговування
- Відносно низька вартість
- Забезпечує широку топологічну гнучкість для встановлення мережі
- Гарантує успішне взаємо з'єднання та роботу продукції, що відповідає стандартам

Token-Ring (англ. «маркерне кільце») — архітектура мереж з кільцевою логічною топологією і детермінованим методом доступу, заснованому на передачі маркера.

Розроблялася Token-Ring як надійна альтернатива Ethernet. Уже той факт, що її підтримує компанія IBM, найбільший виробник комп'ютерної техніки, говорить про те, що їй необхідно приділити особливу увагу. Але не менш важливо й те, що Token-Ring є в цей час міжнародним стандартом IEEE 802.5 (хоча між Token-Ring й IEEE 802.5 є незначні відмінності). Це ставить дану мережу на один рівень по статусі з Ethernet. І хоча зараз Ethernet витісняє всі інші мережі, Token-Ring не можна вважати безнадійно застарілою. Більше 10 мільйонів комп'ютерів в усьому світі об'єднані цією мережею.

Основні технічні характеристики класичного варіанта мережі Token-Ring:

- Максимальна кількість концентраторів типу IBM 8228 MAU – 12
- Максимальна кількість абонентів у мережі – 96
- Максимальна довжина кабелю між абонентом і концентратором – 45 метрів
- Максимальна довжина кабелю між концентраторами – 45 метрів

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

- Максимальна довжина кабелю, що з'єднує всі концентратори – 120 метрів
- Швидкість передачі даних – 4 Мбіт/с й 16 Мбіт/с

Мережа FDDI (від англійського Fiber Distributed Data Interface, оптоволоконний розподілений інтерфейс даних) – це одна з новітніх розробок стандартів локальних мереж.

За основу стандарту FDDI був узятий метод маркерного доступу, передбачений міжнародним стандартом IEEE 802.5 (Token-Ring). Несуттєві відмінності від цього стандарту визначаються необхідністю забезпечити високу швидкість передачі інформації на великі відстані. Топологія мережі FDDI – це кільце, найбільш підходяща топологія для оптоволоконного кабелю. У мережі застосовується два різнонаправлених оптоволоконних кабелі, один із яких звичайно перебуває в резерві, однак таке рішення дозволяє використати й повнодуплексну передачу інформації (одночасно у двох напрямках) з подвоєною ефективною швидкістю в 200 Мбіт/с (при цьому кожний із двох каналів працює на швидкості 100 Мбіт/с). Застосовується й зірково-кільцева топологія з концентраторами, включеними в кільце (як в Token-Ring)[4].

Основні технічні характеристики мережі FDDI:

- Максимальна кількість абонентів мережі – 1000.
- Максимальна довжина кільця мережі – 20 кілометрів.
- Максимальна відстань між абонентами мережі – 2 кілометри.
- Середовище передачі – многомодовий оптоволоконний кабель (можливе застосування електричної крученої пари).
- Метод доступу – маркерний.
- Швидкість передачі інформації – 100 Мбіт/с (200 Мбіт/с для дуплексного режиму передачі).

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2 Аналіз технологій побудови локальної мережі

IPv4 — це 32-розрядна адреса, яка зазвичай представлена в десятковому позначенні з точками, з десятковим значенням, що представляє кожен із чотирьох октетів (байтів), які складають адресу. Адреса IPv4 складається з *адреси мережі* та *адреси хоста*. В Інтернеті мережеві адреси призначаються центральним органом, *інформаційним центром мережі* (NIC). Частина адреси IPv4, яка використовується для кожної з цих адрес, визначається класом адреси.

Існує три часто використовувані класи IPv4-адрес:

- Клас А : 0.XXX.XXX.XXX - 127.XXX.XXX.XXX

Перший біт адреси дорівнює нулю, таким чином клас А займає половину всього адресного простору. Адреса мережі займає 7 біт, адреса вузла - 24 біти, отже клас А містить 128 підмереж по 16 777 216 адрес у кожній.

Наприклад, підмережа 10.0.0.0 (класу А містить більше 16,7 млн адрес від 10.0.0.0 по 10.255.255.255). За замовчуванням зарезервована, не маршрутизується в інтернеті та використовується для побудови локальних та корпоративних мереж.

- Клас В: 128.0.XXX.XXX - 191.255.XXX.XXX

Адреса починається з бітів 1,0, таким чином клас В займає чверть всього адресного простору. Адреса мережі займає 14 біт, адреса вузла - 16, отже клас В містить 16384 підмереж по 65536 адрес в кожній

Наприклад, мережа 169.254.XX класу В із 65536 адресами. Зарезервована для "каналних" адрес.

- Клас С: 192.0.0.XXX - 223.255.255.XXX

Адреса починається з бітів 1,1,0, таким чином клас С займає 1/8 адресного простору. Адреса мережі займає 21 біт, адреса вузла - 8 біт, отже клас С містить 2097152 мереж по 256 адрес в кожній.

IPv6 — нова версія протоколу IP, покликана вирішити проблеми, з якими зіткнулася попередня версія (IPv4) при її використанні в Інтернеті, за рахунок використання 128 бітної адресації замість 32 бітної. Протокол був розроблений

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

IETF. Згідно зі статистикою Google на січень 2020 року, частка IPv6 в мережевому трафіку становила близько 30%

При розробці нового протоколу IPv6 були враховані багато проблем і вузькі місця протоколу IPv4

Існує 3 типи IPv6-адрес:

Unicast (індивідуальний) - Служить для визначення інтерфейсу на пристрої під управлінням протоколу IPv6 .

Multicast (Груповий) - Використовується для відправки пакетів по декількох адресах призначення (Замінив собою Broadcast адреса, є IPv6- адреса для всіх узлів Б котрий дає аналогічний результат.)

Anycast (Довільний) - Будь-який індивідуальний адресу, який може бути призначений декільком пристроям. Пакет, що відправляється на адресу довільній розсилки, направляється до найближчого пристрою до цієї адреси.

Протокол IPv6 використовує довжину префікса для позначення частини префікса адреси. IPv6 не використовує для маски підмережі десяткове подання з розділовими точками. Довжина префікса позначає мережну частину IPv6-адреси за допомогою адреси або довжини IPv6-префікса. Діапазон довжини префікса може становити від 0 до 128. Традиційна довжина IPv6-префікса для локальних і інших типів мереж - /64. Це означає, що довжина префікса, або мережева частина адреси, становить 64 біта, а що залишилися 64 біта залишаються для ідентифікатора інтерфейсу (вузловий частини) адреси.

Пакети складаються з керуючої інформації, необхідної для доставки пакета адресату, і корисних даних, які потрібно переслати. Керуюча інформація ділиться на те, що міститься в основному фіксованому заголовку, і що міститься в одному з необов'язкових додаткових заголовків. Корисні дані, як правило, це дейтаграма або фрагмент протоколу більш високого транспортного рівня, але можуть бути і дані мережевого рівня (наприклад ICMPv6, OSPF)[5].

IPv6-пакети зазвичай передаються за допомогою протоколів канального рівня, таких як Ethernet, який інкапсулює кожен пакет в кадр.

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

- Version: версія протоколу; для IPv6 це значення рівно 6 (в бітах – 0110).
- Traffic Class: пріоритет пакета (8 біт). Це поле складається з двох значень. Старші 6 біт використовуються DSCP для класифікації пакетів. Два біти використовуються ECN для контролю перевантаження.
- Flow Label: мітка потоку.
- Payload Length: (16 біт) розмір даних в октетах, не включаючи цей заголовок, але включаючи всі розширені заголовки.
- Next Header: задає тип розширеного заголовка, який йде наступним. В останньому розширеному заголовку поле Next Header задає тип транспортного протоколу (TCP, UDP і т.д.).
- Hop Limit: аналог поля time to live в IPv4 (8 біт)
- Source Address і Destination Address: адреса відправника та одержувача відповідно; по 128 біт.

HSRP

HSRP був розроблений компанією Cisco Systems. У березні 1998 року стандартизований в документі RFC 2281, написаному представниками Cisco Systems і Juniper Networks. Надалі на основі HSRP був створений протокол VRRP, який не є пропрієтарним, але має патентні обмеження через те, що заснований на HSRP. Повністю вільної від патентних суперечок альтернативою протоколу HSRP є протокол CARP, розроблений в 2003 році командою розробників операційної системи OpenBSD.

Протокол HSRP призначений для того, щоб домогтися практично 100% доступності та відмовостійкості першого хопу від відправника («маршрут за замовчуванням», default gateway, також іноді званий «шлюз останньої надії»).

Це досягається шляхом використання у двох або більше маршрутизаторів або маршрутизуючих комутаторів третього рівня одного IP-адреси і MAC-адреси так званого віртуального маршрутизатора. Така група називається HSRP-групою.

У термінології HSRP-протоколу існують кілька основних понять (термінів):

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

- Активний маршрутизатор (Active Router) - маршрутизатор або маршрутизуючий комутатор третього рівня, що виконує роль віртуального маршрутизатора і забезпечує пересилку пакетів з однієї підмережі в іншу;
- Резервний маршрутизатор (Standby Router) - маршрутизатор або маршрутизуючий комутатор третього рівня, що виконує роль резервного віртуального маршрутизатора, що очікує відмови активного маршрутизатора в рамках однієї HSRP групи;
- Група резервування (Standby Group) - група маршрутизаторів або маршрутизуючих комутаторів третього рівня, які є членами однієї HSRP-групи і забезпечують роботу і відмовостійкість віртуального маршрутизатора;
- Таймер вітання (Hello Time) - проміжок часу, протягом якого маршрутизатори або маршрутизовані комутатори третього рівня, що знаходяться в рамках однієї HSRP групи, очікують пакети вітання (Hello Packet) від активного маршрутизатора;
- Таймер утримання (Hold Time) - проміжок часу, після закінчення якого резервний маршрутизатор посилає пакет, в якому міститься інформація про відмову активного маршрутизатора, тим самим здійснює пріоритетний переривання в групі і бере на себе роль активного маршрутизатора[8].

VLAN

У пристроях Cisco, протокол VTP (англ. VLAN Trunking Protocol) передбачає VLAN-домени для спрощення адміністрування. VTP також виконує «чистку» трафіку, направляючи VLAN трафік тільки на ті комутатори, які мають цільові VLAN-порти (функція VTP pruning). Комутатори Cisco в основному використовують протокол 802.1Q Trunk замість застарілого пропрієтарного ISL (англ. Inter-Switch Link) для забезпечення сумісності інформації.

За замовчуванням на кожному порту комутатора є мережа VLAN1 або VLAN управління. Мережа управління не може бути видалена, проте можуть бути створені додаткові мережі VLAN і цим альтернативним VLAN можуть бути додатково призначені порти.

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

Native VLAN - це параметр кожного порту, який визначає номер VLAN, який отримують всі непомічені (untagged) пакети.

В Cisco використовується наступна термінологія портів:

- access port - порт належить одному VLAN'у і передає нетегірований трафік. За специфікації cisco, access порт може належати тільки одному VLAN'у, за замовчуванням це перший (нетегірований) VLAN. Будь-кадр, який проходить через access порт, позначається номером, що належить цьому VLAN'у.

- trunk port - порт передає тежованих трафік одного або декількох VLAN'ов. Цей порт, навпаки, не змінює тег, а лише пропускає кадри з тегами, які дозволені на цьому порту.

- Для того щоб передати через порт трафік декількох VLAN, порт переводиться в режим транка.

Режими інтерфейсу (режим за замовчуванням залежить від моделі комутатора):

- auto - Порт знаходиться в автоматичному режимі і буде переведений в стан trunk, тільки якщо порт на іншому кінці знаходиться в режимі on або desirable. Тобто якщо порти на обох кінцях знаходяться в режимі «auto», то trunk застосовуватися не буде.

- desirable - Порт знаходиться в режимі «готовий перейти в стан trunk»; періодично передає DTP-кадри порту на іншому кінці, запитуючи віддалений порт перейти в стан trunk (стан trunk буде встановлено, якщо порт на іншому кінці знаходиться в режимі on, desirable, або auto).

- trunk - Порт постійно знаходиться в стані trunk, навіть якщо порт на іншому кінці не підтримує цей режим.

- nonegotiate - Порт готовий перейти в режим trunk, але при цьому не передає DTP-кадри порту на іншому кінці. Цей режим використовується для запобігання конфліктів з іншим "не-cisco" обладнанням. В цьому випадку комутатор на іншому кінці повинен бути вручну налаштований на використання trunk'a.

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

За замовчуванням в транки дозволені всі VLAN. Для того щоб через відповідний VLAN в транки передавалися дані, як мінімум, необхідно щоб VLAN був активним. Активним VLAN стає тоді, коли він створений на комутаторі і в ньому є хоча б один порт в стані up / up.

PVST+

PVST + відправляє BPDU для кожного екземпляра VLAN, щоб MST міг обробляти кожен BPDU окремо для кожного VLAN. MST, однак, не має примірника для кожної VLAN.

Коли область MST (MST region) підключена до топології PVST +, MST «імітує» PVST + за допомогою функції, званої PVST simulation mechanism. Ця функція дозволяє області MST відправити PVST + BPDU (по одному для кожної VLAN) на інтерфейси, підключені до комутаторів PVST +. Ці BPDU містять одну і ту ж інформацію і розсилають один і той же кореневої міст. Інтерфейси, які підключаються до топології PVST +, називаються граничними (boundary) інтерфейсами або портами.

VRST + (Rapid PVST +) також буде підтримуватися. Однак MST реалізує тільки функції PVST +, тому різниці в продуктивності не буде.

Оскільки тепер комутатори PVST+ отримують BPDU для кожної VLAN з MST, що несуть одну і ту ж інформацію, всі вони будуть приймати однакові рішення при виборі кореневого моста, кореневого порту і т.д.

Всі комутатори MST повинні узгоджувати одну і ту ж інформацію, тому для цього використовується інформація з IST (internal spanning tree). Кореневий міст в області MST, який вибирається як кореневої міст для IST, також буде використовуватися в BPDU для PVST +.

MST вибирає роль порту (кореневий, призначений, чи не призначений) для прикордонного інтерфейсу для всіх VLAN тільки шляхом перегляду інформації в BPDU VLAN 1.

Вибір ролі порту на прикордонному інтерфейсі для всіх VLAN є ризикованим, адже це означає, що передбачається, що всі VLAN використовують один і той же кореневий міст, кореневі порти і т.д. невідомо, чи згоден домен PVST

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

+ з роллю порту для всіх VLAN, яка вибирається на прикордонному інтерфейсі MST[7].

1.3 Аналіз мережевих атак

Захист локальної мережі проводиться з метою запобігання несанкціонованого доступу до комутаторів, робочих станцій тощо.

Для захисту підключення до мережевих пристроїв було налаштовано протокол віддаленого підключення SSH. Даний протокол здійснює шифрування повідомлення віддаленого доступу, а не передає його у відкритому вигляді. Більшої уваги при захисті мережі потребують комутатори, тому що вони є найбільш вразливі до атак. Найбільш поширеними атаками є:

- DHCP starvation;
- VLAN hopping;
- Rogue DHCP Server;
- CAM-table overflow.

DHCP starvation – проста та популярна атака, яка виконується за допомогою протоколу DHCP. Її суть в тому, що DHCP pool, з якого клієнти отримують IP-адреси, початково з обмеженим доступом. Наприклад, це може бути адреси 253 при використанні маски 255.255.255.0. Для нормальної роботи мережі цього має повністю вистачити всім клієнтам, проте «атака резервації» (DHCP starvation) прагне вичерпати цей пул і вивести легітимний сервер DHCP з гри.

Хронологія атаки є такою:

1. Атакуючий пристрій запитує IP-адресу, маску і шлюз за замовчуванням у сервера DHCP і отримує їх.
2. MAC-адреса атакуючого пристрою змінюється, і він запитує наступну, вже іншу IP-адресу, маскуючись під якогось нового клієнта, який з'явився в корпоративній мережі.
3. Попередні два пункти циклічно повторюються до тих пір, поки весь пул IP-адрес на сервері не буде вичерпано.

В залежності від того, чого добиваються атакуючі можуть бути такі наслідки:

		Носов Є.С.		
		Покотило О.А.		
Змн.	Арк.	№ докум.	Підпис	Дата

KIK.KP.B – 125 – 15 – ПЗ

Арк.

17

- Відмова в обслуговуванні. Сервери IP-адрес вичерпані і нові хости не можуть отримати їх , тобто їх взаємодія з мережею на цьому закінчиться
- Підміна DHCP. Атака чудово поєднується з атакою Rogue DHCP Server. Так як на основному сервері DHCP вільних адрес вже не залишилося, він вимикається, і всі 100% корпоративних клієнтів мережі дістаються ворожому атакуючому DHCP-серверу.

Rogue DHCP Server – атака підміни DHCP – сервера. Найпростіший спосіб захисту від атак класу Rogue DHCP Server - це включити на всіх комутаторах таку функцію, як DHCP snooping . Однак перед цим необхідно визначити два типи портів:

- довірені - порти комутатора, до яких підключається DHCP-сервер або інший легітимний комутатор;
- недовірені порти для клієнтських підключень, за якими DHCP-сервер перебувати не може.

DHCP snooping необхідний для того, щоб вказати комутатору, що слід звертати увагу на пакети DHCP offer і acknowledgment , що проходять крізь нього, і не допускати проходження таких пакетів з недовірених портів. Також широкомовні запити від клієнта (discover і request) тепер будуть перенаправлятися тільки на довірені порти.

VLAN hopping атака базується на можливості комутаторів автоматично узгоджувати тип свого порту – access або trunk.

Протокол 802.1Q спільно використовується у всіх сучасних мережах. Ідея полягає в тому, що протокол розширює ethernet кадр, додаючи декілька полів (зокрема поле VLAN Identifier, VID). На основі даного поля, комутатор в змозі визначити, якій групі портів адресований цей чи інший кадр.

При цьому можна виділити такі особливості:

- клієнти нічого не знають про свою приналежність до певного VLAN та працюють з нетегованими кадрами, заголовок 802.1Q з'являється тільки при проходженні кадру через access-порт;

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

- порт може бути не тегований (access) лише в одному VLAN;
- через тегований (trunk) порт можна передавати кадри, що належать до різних VLAN;
- існує так званий native VLAN - при попаданні на trunk-порт кадру без тега він автоматично буде зарахований до native VLAN. Як правило, native VLAN за умовчанням – це VLAN1 (але це можна змінити);
- при цьому кадри, що належать native VLAN і потрапили в access-порт, будуть передаватися через trunk-порт без тега.

CAM table overflow атака або переповнення локальної таблиці, реалізується, коли таблиця комутації заповнюється і після цього комутатор працює в режимі хаба. Іншими словами, підключившись до будь-якого порту комутатора після успішної атаки, можна перехоплювати весь трафік у межах широкомовного домену, якому належить цей порт. Атаку можна виконати, наприклад, за допомогою утиліти masof, яка входить до dsniff.

Щоб зрозуміти, як працює ця атака, потрібно знати принципи роботи сучасного комутатора. Давай уявімо комутатор з ім'ям SW, до якого підключені два рівнозначних хоста PC1 (MAC 0000.1111.1111) і PC2 (MAC 0000.2222.2222). На них уже налаштовані IP-адреси (10.0.0.1 та 10.0.0.2), і ці хости хочуть спілкуватися один з одним, як різностатеві підлітки у пубертатний період[6].

Висновки до першого розділу

В першому розділі було розглянуто топологію побудови локальних мереж, проведено аналіз технологій для їх побудови (IPv4, IPv6, HSRP, PVST+, VLAN) аналіз найбільш поширених мережевих атак (DHCP snooping, Rouge DHCP server, VLAN hopping та CAM table overflow)

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

РОЗДІЛ 2 ПРОЄКТ ПОБУДОВИ ТА ЗАХИСТУ ЛОКАЛЬНОЇ МЕРЕЖІ

2.1 Вибір обладнання для організації роботи мережі

Для забезпечення функціонування мережі організації було обрано оптимальне обладнання корпорації Cisco, котрі мають адаптованість під модернізацію модулями. Також потрібно приділити особливу увагу технологіям, котрі необхідні для мережі, зокрема це підтримка GigabitEthernet та Ethernet (FastEthernet).

На роль комутаторів обрано Cisco Catalyst 2960 серії, що є лінійкою комутаторів з фіксованою конфігурацією і портами Fast Ethernet і Gigabit Ethernet, що мають розширені LAN сервіси для підприємств початкового рівня і мереж віддаленого офісу. Комутатори Cisco Catalyst 2960 підтримують передачу голосу, даних і відео, а також безпечний доступ. Крім того, вони є масштабованим рішенням для управління в міру зміни потреб бізнесу.



Рисунок 2.1 – Комутатор Cisco Catalyst 2960

Комутатори Cisco Catalyst 2960 підтримують “розумні функції” (створення складних списків управління доступом, розширена безпека), комбіновані гігабітні порти (мідний 10/100 / 1000BASE-T Ethernet або SFP-модуль для переходу в інше середовище - Cisco 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX, 100BASE-FX, 100BASE-LX, CWDM SFP). Також, пристрої Catalyst 2960 підтримують QoS, покроковий Rate Limiting, ACL (на базі MAC або IP адрес, портів UDP / TCP) і multicast services, можливість регулювати швидкість передачі на кожному порту з кроком 64 Кбіт, Link Aggregation для організації більш швидкісних з'єднань між комутаторами і серверами, можливість організації транкових з'єднань на кожному

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

порту за допомогою тегів 802.1q, до 255 VLAN на комутатор, до 4000 VLAN ID і управління через Cisco Network Assistant (підтримує широкий спектр моделей комутаторів від Cisco Catalyst 2960 до Cisco Catalyst 4506).

Для ролі багаторівневих комутаторів було обрано Cisco Catalyst 3650. Комутатори Cisco Catalyst 3650 серії - це стекові пристрої для конвергації доступу з фіксованою конфігурацією і інтегрованим бездротовим контролером ASIC і працюють на базі модульної операційної системи IOS XE. Аналогічні ASIC використовуються в платформах Catalyst 3850 і Supervisor 8-Е для Catalyst 4500-Е. Комутатори Cisco Catalyst 3650 забезпечують політику безпеки і якості обслуговування QoS для трафіку дротових і бездротових клієнтів, а також моніторинг та оптимізацію цього трафіку на рівні доступу корпоративної мережі.



Рисунок 2.2 – Багаторівневий комутатор Cisco Catalyst 3650

До особливостей моделей Catalyst 3650 можна віднести фіксовану конфігурацію з 24 або 48 портів 10/100/1000 з можливістю підтримки PoE + (до 30 Вт на порт), інтегровані АПЛІНК 4 x Gigabit Ethernet, 2 x 10 Gigabit Ethernet або 4 x 10 Gigabit Ethernet з підтримкою трансиверів SFP iSFP +, можливість установки до 2 відмовостійких джерел живлення змінного струму різних потужностей і 3 вентиляторів охолодження. Також, в Catalyst 3650 є підтримка стека StackWise (до

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

9 пристроїв в стеку) при використанні опціональних модулів для стекирования з пропускною спроможністю 160Гб / с і технологією SSO (Stateful SwitchOver), пропускна здатність Wireless 40 Гб / с на базі ASIC UADP (Unified Access Data Plane) і операційної системи IOS XE і підтримка до 25 точок доступу і 1000 бездротових клієнтів на один комутатор 3650 або один стек StackWise з комутаторів 3650.

На роль маршрутизатора було обрано Cisco ISR 4331 . Ця модель є однією з найновіших та найпотужніших для корпоративного сегменту.



Рисунок 2.3 – Маршрутизатор Cisco ISR433

Модель маршрутизатора має пропускну швидкість до 7 Гбіт, 2 інтерфейси GigabitEthernet з форм-фактором RJ-45, 2 інтерфейси SFP та 1 USB 2.0. Два порти RJ-45, та два порти SFP. Також роутер має слот для модуля SM-X та декілька слотів для NIM (Network Interface Modules). Загальна пам'ять маршрутизатора становить 4 Гб у стандарті, та може бути розширена до 16 Гб, як і флеш-пам'ять[9].

2.2 Розробка топології комп'ютерної мережі

Мережу було спроектовано на базі трирівневої структури, що містить:

- рівень ядра;
- рівень розподілу;
- рівень доступу.

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

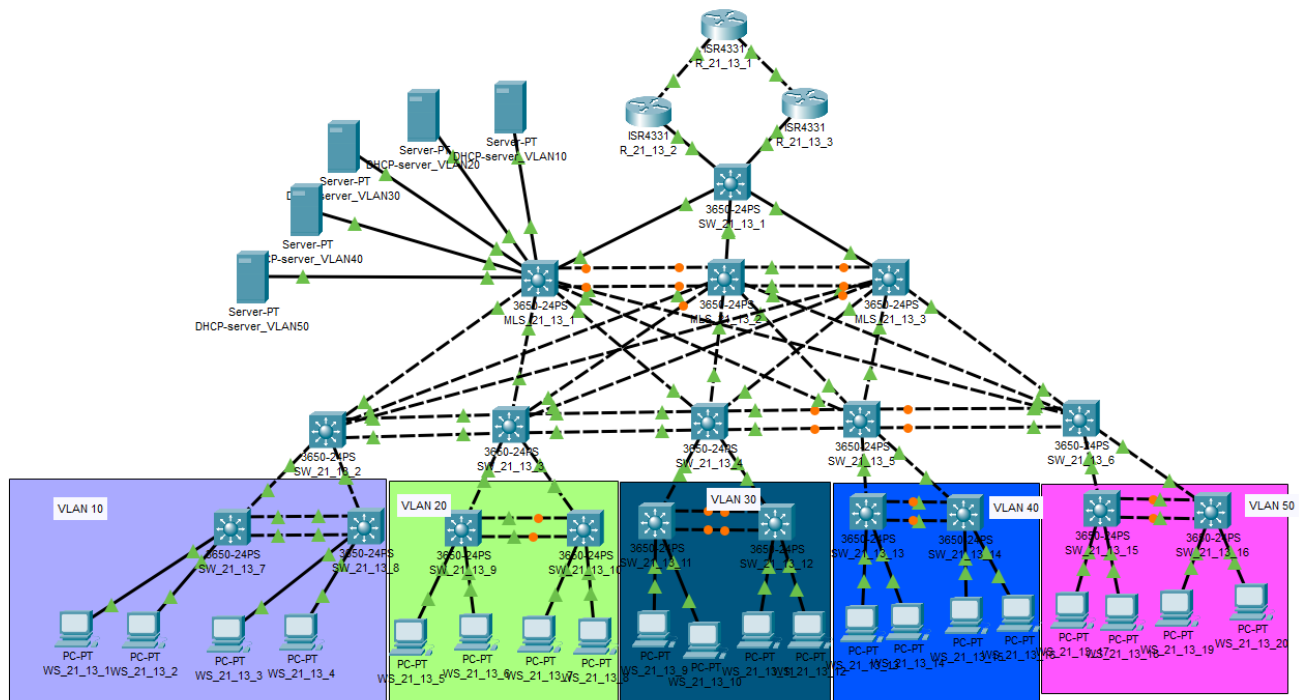


Рисунок 2.4 – Топологія мережі

Рівень ядра складається з 3 маршрутизаторів, 3 багаторівневих комутаторів та одного комутатора, з'єднаних між собою витою парою GigabitEthernet. Налаштована динамічна агрегація між багаторівневими комутаторами для підвищення надійності.

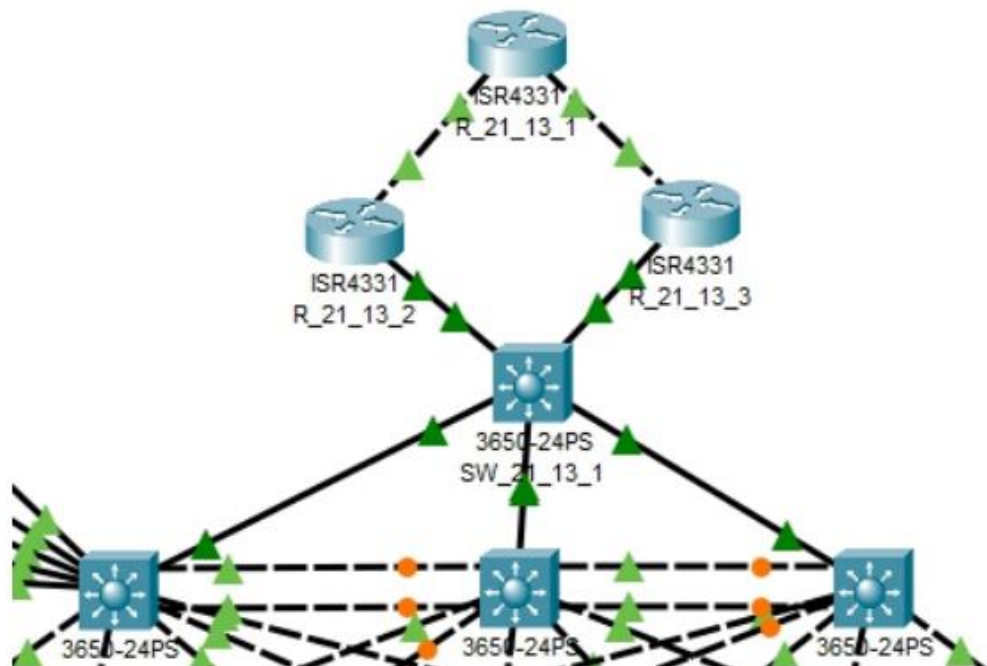


Рисунок 2.5 – Ядро мережі

Рівень розподілу представляє собою набір з 5 комутаторів, що під'єднані до ядра мережі. З'єднання з ядром мережі виконано за допомогою витої пари GigabitEthernet. Налаштована динамічна агрегація між комутаторами для підвищення надійності.

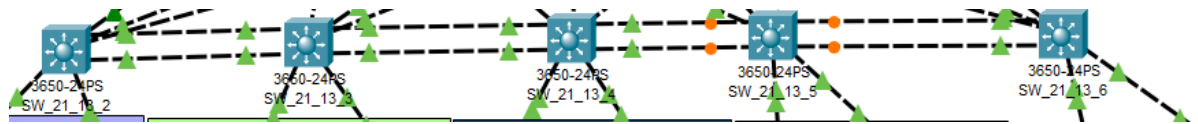


Рисунок 2.6 – Рівень розподілу

Рівень доступу складається з 10 комутаторів та 20 вузлів. Усюди використано з'єднання GigabitEthernet. Налаштована динамічна агрегація між комутаторами для підвищення надійності.

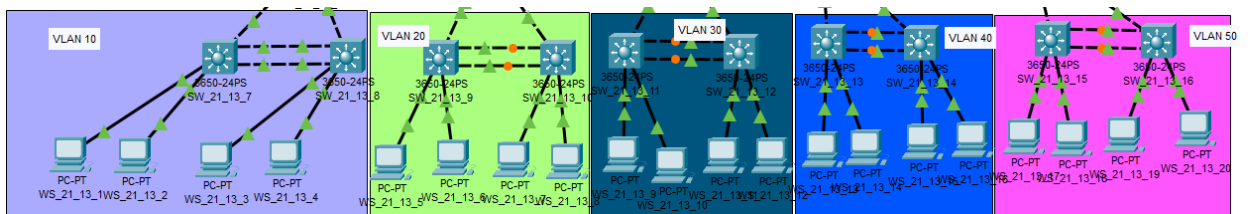


Рисунок 2.7 – Рівень доступу

Віртуальна мережа VLAN 10 складається з 2 комутаторів та 4 робочих станцій, що з'єднані витою парою GigabitEthernet. Також до неї входить віртуальна мережа для віддаленого керування VLAN 100.

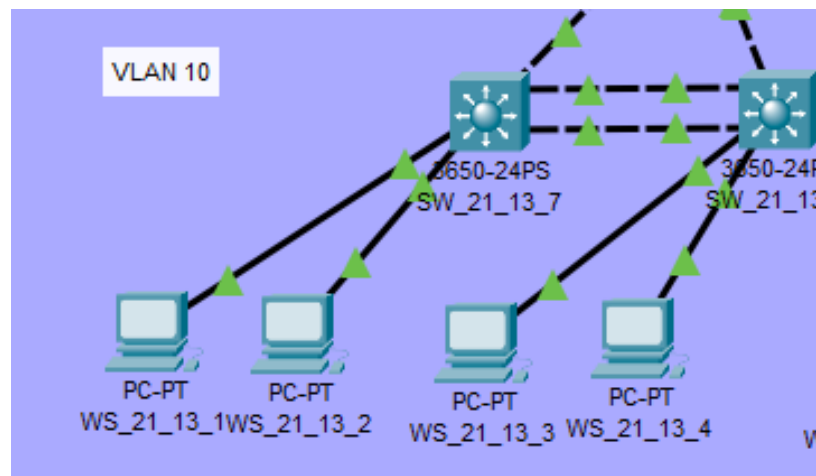


Рисунок 2.8 – Віртуальна мережа VLAN 10

Віртуальна мережа VLAN 20 складається з 2 комутаторів та 4 робочих станцій, що з'єднані витою парою GigabitEthernet. Також до неї входить віртуальна мережа для віддаленого керування VLAN 100.

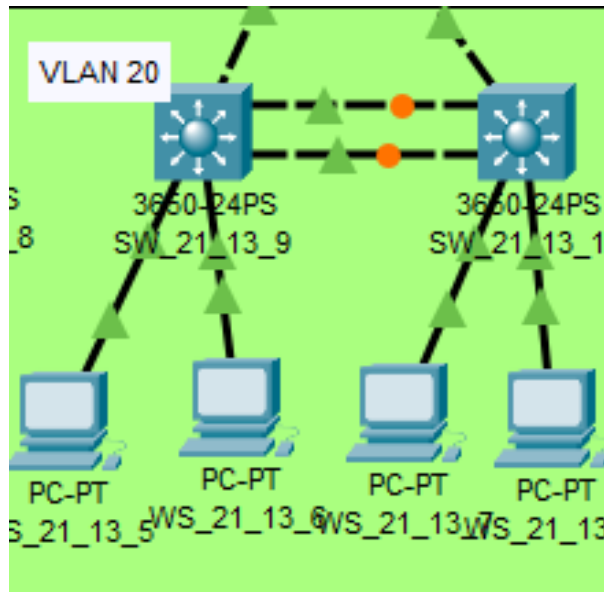


Рисунок 2.9 – Віртуальна мережа VLAN 20

Віртуальна мережа VLAN 30 складається з 2 комутаторів та 4 робочих станцій, що з'єднані витою парою GigabitEthernet. Також до неї входить віртуальна мережа для віддаленого керування VLAN 100.

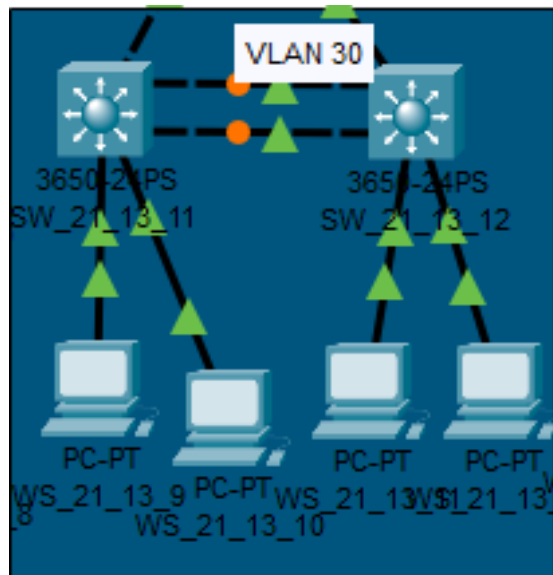


Рисунок 2.10 – Віртуальна мережа VLAN 30

Віртуальна мережа VLAN 40 складається з 2 комутаторів та 4 робочих станцій, що з'єднані витою парою GigabitEthernet. Також до неї входить віртуальна мережа для віддаленого керування VLAN 100.

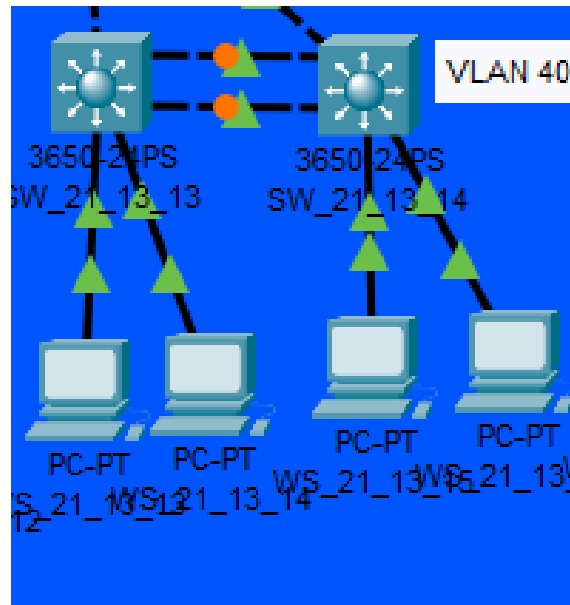


Рисунок 2.11 – Віртуальна мережа VLAN 40

Віртуальна мережа VLAN 50 складається з 2 комутаторів та 4 робочих станцій, що з'єднані витою парою GigabitEthernet. Також до неї входить віртуальна мережа для віддаленого керування VLAN 100.

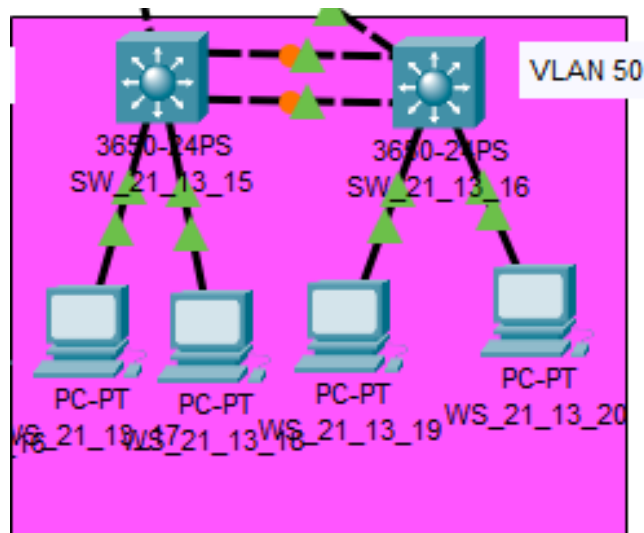


Рисунок 2.12 – Віртуальна мережа VLAN 50

Так як в Packet Tracer не підтримуються DHCPv6-сервери на багаторівневих комутаторах, то їх роль будуть виконувати фізичні сервери (для кожного VLAN окремий сервер).

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

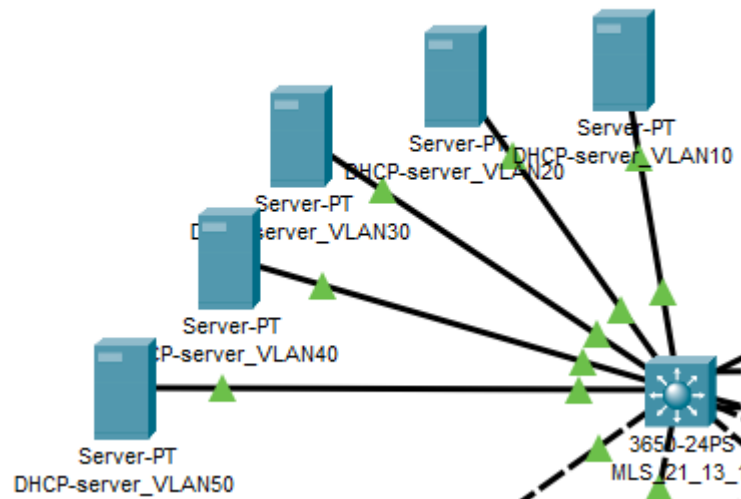


Рисунок 2.10 – DHCPv6 сервери

2.3 Розробка схеми адресації мережі

Для забезпечення функціонування мережі, перш за все були виконано розрахунок параметрів IP-адресації. Під час розрахунку параметрів IP-адресації особлива увага була приділена економії IP-адрес, тому мережі було розбито на підмережі з оптимальними масками, згідно кількості вузлів у кожній з них. Також було приділено увагу можливості розширення[10].

Таблиця 1

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/ Мережний адаптер/ Шлюз	IP-адреса	Маска префіксу	Пре - фікс
Підмережа А	—	2001:DB8:2113:10::	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Підмережа В	—	2001:DB8:2113:20::	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Підмережа С	—	2001:DB8:2113:30::	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/ Мережний адаптер/ Шлюз	IP-адреса	Маска префіксу	Пре - фікс
Підмережа D	—	2001:DB8:2113:40::	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Підмережа E	—	2001:DB8:2113:50::	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Підмережа F	—	2001:DB8:2113:100 ::	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Підмережа G	—	2001:DB8:2113:1::	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Підмережа H	—	2001:DB8:2113:2::	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Підмережа I	—	2001:DB8:2113:3::	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Маршрутизатор R_21_13_1	Gig0/0/0	2001:DB8:2113:1::1	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	Gig0/0/1	2001:DB8:2113:2::1	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Маршрутизатор R_21_13_2	Gig0/0/0	2001:DB8:2113:1::2	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	Gig0/0/1	2001:DB8:2113:3::1	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Маршрутизатор R_21_13_3	Gig0/0/0	2001:DB8:2113:2::2	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	Gig0/0/1	2001:DB8:2113:3::1	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/ Мережний адаптер/ Шлюз	ІР-адреса	Маска префіксу	Пре- фікс
Багаторівневий комутатор MLS_21_13_1	Gig1/0/1	2001:DB8:2113:3::4	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN10	2001:DB8:2113:10::1	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN20	2001:DB8:2113:20::1	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN30	2001:DB8:2113:30::1	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN40	2001:DB8:2113:40::1	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN50	2001:DB8:2113:50::1	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN100	2001:DB8:2113:100::1	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Багаторівневий комутатор MLS_21_13_2	Gig1/0/1	2001:DB8:2113:3::5	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN10	2001:DB8:2113:10::2	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN20	2001:DB8:2113:20::2	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN30	2001:DB8:2113:30::2	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN40	2001:DB8:2113:40::2	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/ Мережний адаптер/ Шлюз	ІР-адреса	Маска префіксу	Пре- фікс
Багаторівневий комутатор MLS_21_13_2	VLAN50	2001:DB8:2113:50:: 2	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN100	2001:DB8:2113:100 ::2	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Багаторівневий комутатор MLS_21_13_3	Gig1/0/1	2001:DB8:2113:3::6	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN10	2001:DB8:2113:10:: 3	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN20	2001:DB8:2113:20:: 3	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN30	2001:DB8:2113:30:: 3	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN40	2001:DB8:2113:40:: 3	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN50	2001:DB8:2113:50:: 3	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
	VLAN100	2001:DB8:2113:100 ::3	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Комутатор SW_21_13_2	VLAN100	2001:DB8:2113:100 ::4	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Комутатор SW_21_13_3	VLAN100	2001:DB8:2113:100 ::5	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Комутатор SW_21_13_4	VLAN100	2001:DB8:2113:100 ::6	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				30
Змн.	Арк.	№ докум.	Підпис	Дата		

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/ Мережний адаптер/ Шлюз	ІР-адреса	Маска префіксу	Пре- фікс
Комутатор SW_21_13_5	VLAN100	2001:DB8:2113:100 ::7	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Комутатор SW_21_13_6	VLAN100	2001:DB8:2113:100 ::8	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Комутатор SW_21_13_7	VLAN100	2001:DB8:2113:100 ::9	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Комутатор SW_21_13_8	VLAN100	2001:DB8:2113:100 ::10	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Комутатор SW_21_13_9	VLAN100	2001:DB8:2113:100 ::11	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Комутатор SW_21_13_10	VLAN100	2001:DB8:2113:100 ::12	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Комутатор SW_21_13_11	VLAN100	2001:DB8:2113:100 ::13	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Комутатор SW_21_13_12	VLAN100	2001:DB8:2113:100 ::14	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Комутатор SW_21_13_13	VLAN100	2001:DB8:2113:100 ::15	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Комутатор SW_21_13_14	VLAN100	2001:DB8:2113:100 ::16	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Комутатор SW_21_13_15	VLAN100	2001:DB8:2113:100 ::17	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/ Мережний адаптер/ Шлюз	ІР-адреса	Маска префіксу	Пре- фікс
Комутатор SW_21_13_16	VLAN100	2001:DB8:2113:100 ::18	FFFF:FFFF:FFFF:FFFF :0000:0000:0000:0000	/64
Робоча станція WS_21_13_1	Fa0	DHCPv6		
Робоча станція WS_21_13_2	Fa0	DHCPv6		
Робоча станція WS_21_13_3	Fa0	DHCPv6		
Робоча станція WS_21_13_4	Fa0	DHCPv6		
Робоча станція WS_21_13_5	Fa0	DHCPv6		
Робоча станція WS_21_13_6	Fa0	DHCPv6		
Робоча станція WS_21_13_7	Fa0	DHCPv6		
Робоча станція WS_21_13_8	Fa0	DHCPv6		
Робоча станція WS_21_13_9	Fa0	DHCPv6		
Робоча станція WS_21_13_10	Fa0	DHCPv6		
Робоча станція WS_21_13_11	Fa0	DHCPv6		
Робоча станція WS_21_13_12	Fa0	DHCPv6		
Робоча станція WS_21_13_13	Fa0	DHCPv6		
Робоча станція WS_21_13_14	Fa0	DHCPv6		

Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/ Мережний адаптер/ Шлюз	ІР-адреса	Маска префіксу	Пре- фікс
Робоча станція WS_21_13_15	Fa0	DHCPv6		
Робоча станція WS_21_13_16	Fa0	DHCPv6		
Робоча станція WS_21_13_17	Fa0	DHCPv6		
Робоча станція WS_21_13_18	Fa0	DHCPv6		
Робоча станція WS_21_13_19	Fa0	DHCPv6		
Робоча станція WS_21_13_20	Fa0	DHCPv6		

Висновки до другого розділу

При виконанні другого підрозділу було підібрано обладнання для організації роботи мережі, спираючись на наявне в продажі. Було описано чому саме це обладнання є найкращим доступним варіантом для побудови мережі. Розроблено проєкт мережі організації, структуру ядра локальної мережі, наведено загальну кількість необхідного обладнання. Також було розроблено схему адресації мережі.

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 НАЛАГОДЖЕННЯ ЛОКАЛЬНОЇ МЕРЕЖІ

3.1 Базове налагодження пристроїв

Розглянемо лістинги налаштування. Для зручності налаштування були змінені стандартні імена елементів мережі[11].

```
R_21_13_3(config)#int gig0/0/1
R_21_13_3(config-if)#sta
R_21_13_3(config-if)#standby version 2
R_21_13_3(config-if)#standby ipv6 au
R_21_13_3(config-if)#standby ll3 ipv6 autoconfig
R_21_13_3(config-if)#standby ll3 pri
R_21_13_3(config-if)#standby ll3 priority 150
R_21_13_3(config-if)#stan
R_21_13_3(config-if)#standby tra
R_21_13_3(config-if)#standby track gig0/0/0
R_21_13_3(config-if)#do write
```

Рисунок 3.1 – Налаштування HSRP на маршрутизаторі R_21_13_3

```
interface Vlan10
  mac-address 0090.0c81.3301
  no ip address
  ipv6 address 2001:DB8:2113:10::1/64
  ipv6 enable
!
interface Vlan20
  mac-address 0090.0c81.3302
  no ip address
  ipv6 address 2001:DB8:2113:20::1/64
  ipv6 enable
!
interface Vlan30
  mac-address 0090.0c81.3303
  no ip address
  ipv6 address 2001:DB8:2113:30::1/64
!
interface Vlan40
  mac-address 0090.0c81.3304
  no ip address
  ipv6 address 2001:DB8:2113:40::1/64
!
interface Vlan50
  mac-address 0090.0c81.3305
  no ip address
  ipv6 address 2001:DB8:2113:50::1/64
!
interface Vlan100
  mac-address 0090.0c81.3306
  no ip address
  ipv6 address 2001:DB8:2113:100::1/64
```

Рисунок 3.2 – Створені VLAN на багаторівневому комутаторі MLS_21_13_1

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

```

interface GigabitEthernet1/0/4
  switchport access vlan 10
  switchport mode access
  switchport nonegotiate
  spanning-tree portfast
  spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/5
  switchport access vlan 10
  switchport mode access
  switchport nonegotiate
  spanning-tree portfast
  spanning-tree bpduguard enable
!

```

Рисунок 3.3 – Налаштовані access-порти на комутаторах та налаштування PVST (portfast, bpduguard)

```

spanning-tree mode pvst
spanning-tree vlan 10,20,30,40,50,100 priority 24576
!

```

Рисунок 3.7 – Налаштування PVST+

Рисунок 3.4 – Налаштування DHCPv6-серверу для мережі VLAN 10

3.2 Налаштування безпеки у мережі

Захист від DHCP-starvation атаки.

Щоб захиститись від даної атаки потрібно обмежити кількість MAC-адрес на порті комутатора. Реалізовується це за допомогою активації режиму port-security[12].

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

```

SW_21_13_7(config)#interface GigabitEthernet1/0/4
SW_21_13_7(config-if)#switchport mode access
SW_21_13_7(config-if)#switchport port-security
SW_21_13_7(config-if)#switchport port-security maximum 2
SW_21_13_7(config-if)#switchport port-security mac-address sticky
SW_21_13_7(config-if)#switchport port-security violation restrict
SW_21_13_7(config-if)#ip dhcp snooping limit rate 10
SW_21_13_7(config-if)#

```

Рисунок 3.5 – Методи захисту від DHCP-starvation

Реалізація методу захисту є такою:

- за допомогою команди switchport mode access переведено порт у режим access;
- switchport port-security – вмикаємо port-security на інтерфейсі, що нас цікавить;
- switchport port-security maximum 2 – обмежуємо максимальну кількість MAC-адрес на інтерфейсі до 2;
- switchport port-security mac-address sticky – спосіб вивчення MAC-адрес. Функція sticky записує часто вживані адреси у конфігураційний файл, що спрощує роботу адміністратора.
- switchport port-security violation restrict – фінальний крок, де задається тип реагування на перевищення числа дозволених MAC-адрес. Обрано було функцію restrict, за допомогою якого після переповнення всі пакети, надіслані з інших MAC-адрес відкидаються з повідомленням в syslog або за SNMP. Таким чином, атакуючий вже не зможе вичерпати ліміт IP-адрес пулу DHCP, оскільки комутатор не дозволить йому нескінченно змінювати свою MAC-адресу.;
- Також використовується команда - ip dhcp snooping limit rate, яка обмежує кількість пакетів DHCP, що обробляються за секунду на заданому порту, а якщо обмеження перевищено, переводить порт у стан err-disable, тобто тимчасово вимикає його.

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Захист від атак класу Rogue DHCP Server.

```
SW_21_13_7#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW_21_13_7(config)#ip dhcp snooping
SW_21_13_7(config)#ip dhcp snooping vlan 10
SW_21_13_7(config)#ip dhcp snooping trust gig1/0/2 ,gig1/0/3
```

Рисунок 3.6 – Налаштування dhcp snooping

Реалізація методу захисту є такою:

- Для конфігурування DHCP snooping вмикаємо її на комутаторі за допомогою команди ip dhcp snooping;
- Вказуємо, для яких VLAN потрібно відстежувати DHCP-пакети за допомогою команди ip dhcp snooping vlan <номер VLAN>;
- Вказуємо довірені (порти комутатора, до яких підключається DHCP-сервер або інший легітимний комутатор) порти на комутаторі за допомогою команди ip dhcp snooping trust <номер довірених портів>.

Широкомовні запити від клієнта (discover і request) тепер будуть перенаправлятися тільки на довірені порти.

Захист від атаки VLAN hopping

Вирішення цієї проблеми дуже просте, але багато хто при конфігуруванні комутаторів забуває його використовувати. Однією короткою командою ми просто відключаємо можливість автоматичного узгодження та робимо атаку неможливою[13].

```
SW_21_13_7(config)#interface GigabitEthernet1/0/4
SW_21_13_7(config-if)#switchport nonegotiate
SW_21_13_7(config-if)#
```

Рисунок 3.7 – Команда switchport nonegotiate

Ще один потенційний вектор атаки VLAN hopping – використання native VLAN та додавання другого тега. Працює він тільки в тому випадку, якщо атакуючий пристрій знаходиться в native VLAN для trunk-порту.

Кадр, що прийшов на порт gig1/0/4 , що знаходиться в VLAN 10, передаватиметься через trunk-порт нетегованим. Але так як зловмисник PC1 привласнив йому два заголовки, на виході він опиниться з тегом VLAN 20 і дійде

посов С.С.				
Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата

KIK.KP.B – 125 – 15 – ПЗ

Арк.

37

до клієнта, що атакується, чого в нормі бути не повинно. Слід зауважити, що подібна атака односпрямована, тому що неможливо за такою ж схемою передати кадр назад[14].

Захиститися можна таким чином: призначаємо на всіх trunk-портах VLAN, що не використовується, як native :

```
SW_21_13_7(config)#interface GigabitEthernet1/0/4
SW_21_13_7(config-if)#swit
SW_21_13_7(config-if)#switchport trunk native vlan 999
SW_21_13_7(config-if)#interface GigabitEthernet1/0/5
SW_21_13_7(config-if)#switchport trunk native vlan 999
SW_21_13_7(config-if)#ex
SW_21_13_7(config)#
```

Рисунок 3.8– Спосіб захисту VLAN hooping

Тепер атака неможлива, оскільки VLAN 999 не відноситься до жодного з access-портів.

3.3 Тестування працездатності системи

В першу чергу перевіримо можливість підключення по захищеному протоколу SSH.

```
SW_21_13_7>enable
Password:
Password:
SW_21_13_7#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Рисунок 3.9 – Перевірка можливості підключення до SW_21_13_7

Важливим етапом тестування мережі є перевірка на розділення віртуальних підмереж.

```
MLS_21_13_1#show vlan
```

VLAN Name	Status	Ports
1 default	active	Po4, Gig1/0/2, Gig1/0/8, Gig1/0/9, Gig1/0/14, Gig1/0/15, Gig1/0/16, Gig1/0/18, Gig1/0/19, Gig1/0/20, Gig1/0/22, Gig1/0/24, Gig1/1/1, Gig1/1/2, Gig1/1/3, Gig1/1/4
10 VLAN_10	active	Gig1/0/23
20 VLAN_20	active	Gig1/0/10
30 VLAN_30	active	Gig1/0/11
40 VLAN_40	active	Gig1/0/12
50 VLAN_50	active	Gig1/0/13
100 MGMT_VLAN_100	active	

Рисунок 3.10 – Результат виконання команди show vlan на комутаторі

MLS_21_13_1

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

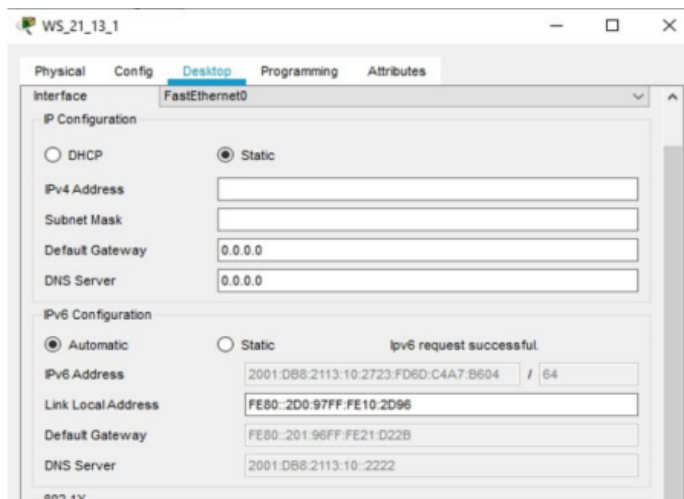


Рисунок 3.11 – Підтвердження отримання DHCPv6 адрес

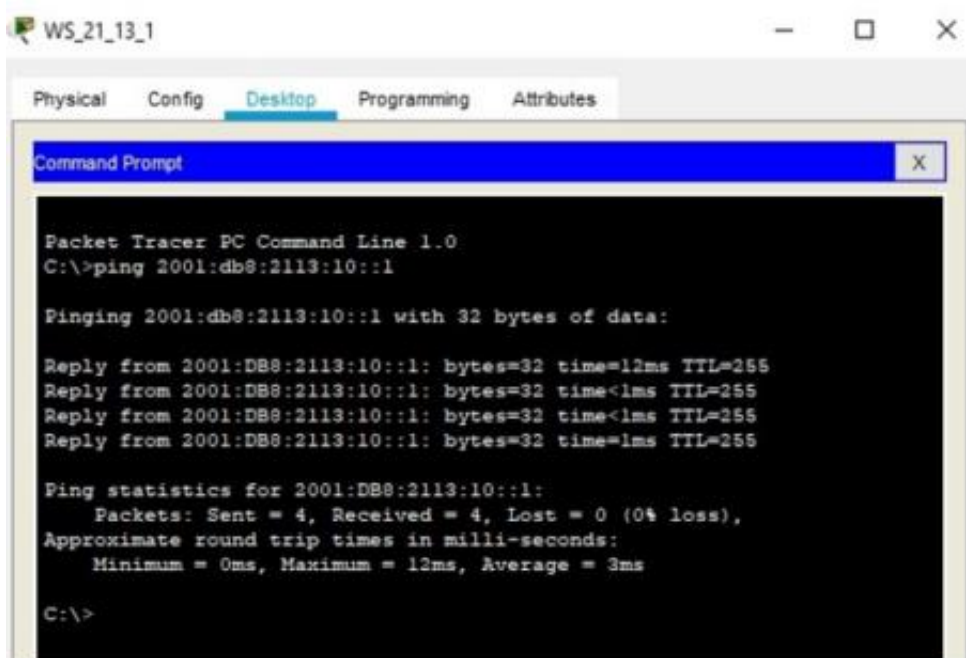


Рисунок 3.12 – Перевірка зв'язку між пристроями мережі

Висновки до третього розділу

В ході виконання третього розділу було проаналізовано основні вимоги технічного завдання, побудови та захисту мережі, проведено базові налаштування та налаштування для захисту мережі від атак. Було детально описано послідовність налаштувань безпеки від мережевих атак. Протестовано мережу на коректність налаштування та особливості роботи протоколу маршрутизації.

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

ВИСНОВКИ

У даній кваліфікаційній роботі розроблено проєкт підсистеми захисту інфраструктури локальної IPv4/IPv6 мережі компанії.

При виконанні кваліфікаційної роботи в першому підрозділі було проаналізовано особливості функціонування мережевих технологій локальних мереж з використанням IPv6 та такими технологіями як PVST+, HSRP, VLAN. Було проаналізовано деякі з поширених мережевих атак.

В другому розділі було підібрано обладнання для організації роботи мережі, спиравшись на наявне в продажі. Розроблено проєкт мережі організації, структуру ядра локальної мережі, наведено загальну кількість необхідного обладнання. Також було розроблено схему адресації мережі.

В третьому розділі, проаналізувавши основні вимоги технічного завдання, побудови та захисту мережі, проведено базові налаштування та налаштування для захисту мережі від атак. Протестовано мережу на коректність налаштування та особливості роботи протоколу маршрутизації.

Розроблений проєкт був реалізований в симуляторі мережі передачі даних Cisco Packet Tracer. Даний проєкт можна використовувати для створення малих організацій.

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Поняття про комп'ютерні мережі, їх призначення. Типи комп'ютерних мереж і мережної взаємодії [Електронний ресурс] / Режим доступу: http://elartu.tntu.edu.ua/bitstream/123456789/16930/5/Mykytyshyn_A_G_Mytnyk_M_M_Kompjuterni_merezhi_Knyga_1.pdf
2. Локальна мережа [Електронний ресурс] / Режим доступу: https://uk.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0
3. Протокол Ethernet [Електронний ресурс] / Режим доступу: <https://www.cisco.com/c/en/us/tech/lan-switching/ethernet/index.html>
4. Протоколи Token Ring та FDDI [Електронний ресурс] – Режим доступу до ресурсу: <https://ua5.org/lan/137-merezha-token-ring.html>
5. Протоколи IPv4 , IPv6 [Електронний ресурс] – Режим доступу до ресурсу: <https://www.ibm.com/docs/en/zos/2.2.0?topic=ipv6-internet-protocol-version-4>
6. Мережеві атаки та захист від них [Електронний ресурс] / Режим доступу до ресурсу: <https://tech-geek.ru/network-attacks/>
7. Протоколи MST, PVST+ та їх сумісність [Електронний ресурс] / Режим доступу до ресурсу: <https://blog.sedicomm.com/2020/10/22/protokoly-mst-pvst-i-ih-sovmestimost/>
8. Hot Standby Router Protocol (HSRP) [Електронний ресурс] – Режим доступу до ресурсу: <https://www.geeksforgeeks.org/hot-standby-router-protocol-hsrp/>
9. Безпека інформаційних систем [Електронний ресурс] – Режим доступу до ресурсу: https://pidru4niki.com/74227/informatika/bezpeka_informatsiynih_sistem.
10. Таненбаум Э. Компьютерные сети. 4-е изд. – СПб.: Питер, 2003. – 848 с.
11. Амато, Вито. Основы организации сетей Cisco, том 2. - Издательский дом "Вильямс", 2004. – 464 с.
12. Поділ на підмережі [Електронний ресурс] – Режим доступу до ресурсу: <https://studfile.net/preview/5199546/page:10/>

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

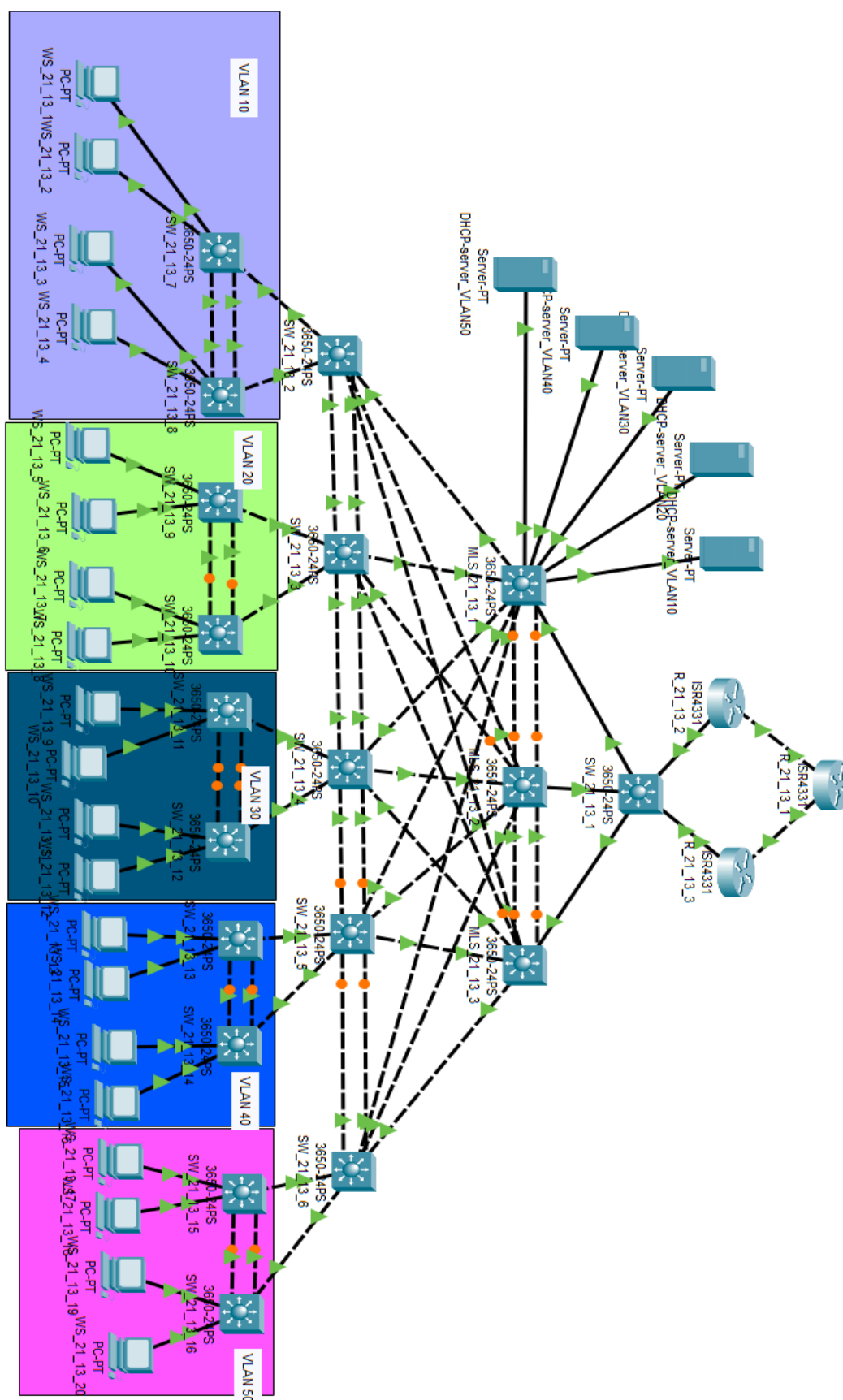
13. Безпека мережі [Електронний ресурс] – Режим доступу до ресурсу:
<https://www.eset.com/ua/support/information/entsiklopediya-ugroz/bezopasnost-seti/>
14. Захист мережі від атак [Електронний ресурс] – Режим доступу до ресурсу:
<https://sites.google.com/site/theocsic/technologies/securitynet>
15. Мережеве обладнання Cisco [Електронний ресурс] – Режим доступу до ресурсу:
<https://stack-systems.com.ua/brands/cisco>
16. Спортак Марк и др. Компьютерные сети. Книга 1. High-performance Networking. Энциклопедия пользователя. – К.: Изд-во “ДиаСофт”, 1998. – 432 с.

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

ДОДАТКИ

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				43
Змн.	Арк.	№ докум.	Підпис	Дата		

Схема мережі



		Носов Є.С.		
		Покотило О.А.		
Змн.	Арк.	№ докум.	Підпис	Дата

Лістинг конфігурацій пристроїв

Маршрутизатор R_21_13_1:

```

version 15.4 no service timestamps log
datetime msec no service timestamps
debug datetime msec
service password-encryption
hostname R_21_13_1
enable secret 5
$1$mERr$jru/RnXiM18dxqPMjj788.
ip cef
ipv6 unicast-routing
no ipv6 cef
username admin privilege 15 secret 5
$1$mERr$qnVcFVUraySLnKS3XOpTd.
username user password 7 08345F4B1B485744465E
ip ssh version 2
ip ssh authentication-
retries 5 ip ssh time-out
105 ip domain-name
nosov.local
spanning-tree mode pvst
interface GigabitEthernet0/0/0
no ip
address
duplex auto
speed auto
ipv6 address 2001:DB8:2113:1::1/64

ipv6 enable

ipv6 ospf 1 area 1 standby
version 2 standby 113 ipv6
autoconfig standby 113 priority 200
interface GigabitEthernet0/0/1
no ip address duplex auto speed auto
ipv6 address 2001:DB8:2113:2::1/64
ipv6 enable
ipv6 ospf 1 area 1 standby version 2
interface GigabitEthernet0/0/2
media-type sfp
no ip address
duplex auto
speed auto
shutdown
interface Vlan1
no ip address
shutdown
ipv6 router ospf 1
router-id 1.1.1.1 log-adjacency-changes
ip classless !
ip flow-export version 9
line con 0 logging synchronous
line aux 0
line vty 0 4 logging synchronous login local transport input ssh transport output ssh

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

Маршрутизатор R_21_13_2:

```
version 15.4
no service timestamps log datetime msec no
service timestamps debug datetime msec
service password-encryption
hostname R_21_13_2
enable secret 5 $1$mERr$jru/RnXiM18dxqPMjj788.
ip cef
ipv6 unicast-routing
no ipv6 cef
username admin privilege 15 secret 5 $1$mERr$qnVcFVUraySLnKS3XOpTd.
username user password 7 08345F4B1B485744465E
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 105 ip domain-
name nosov.local
spanning-tree mode pvst
interface GigabitEthernet0/0/0
no ip address
duplex auto speed
auto
ipv6 address 2001:DB8:2113:1::2/64
ipv6 enable ipv6 ospf 1 area 1
interface GigabitEthernet0/0/1
no ip address duplex auto speed auto
ipv6 address 2001:DB8:2113:3::1/64
ipv6 enable
ipv6 ospf 1 area 1 standby version 2 standby 0
ipv6 autoconfig standby 113
ipv6 autoconfig standby 113 priority 180
standby 113 track GigabitEthernet0/0/0
interface GigabitEthernet0/0/2
media-type sfp
no ip address
duplex auto
speed auto
shutdown
interface Vlan1
no ip address shutdown
ipv6 router ospf 1
router-id 2.2.2.2 log-adjacency-changes
! ip classless !
ip flow-export version 9
line con 0 logging synchronous
line aux 0
line vty 0 4 logging synchronous
login local
transport input ssh
transport output ssh
end
```

		Носов С.С.			КИК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

Маршрутизатор R_21_13_3:

```
!  
version 15.4  
no service timestamps log datetime msec no  
service timestamps debug datetime msec  
service password-encryption  
hostname R_21_13_3  
! enable secret 5 $1$mERr$jru/RnXiM18dxqPMjj788.  
ip cef  
ipv6 unicast-routing  
no ipv6 cef  
username admin privilege 15 secret 5 $1$mERr$qnVcFVUraySLnKS3XOpTd.  
username user password 7 08345F4B1B485744465E  
ip ssh version 2  
ip ssh authentication-retries 5  
ip ssh time-out 105 ip domain-  
name nosov.local  
spanning-tree mode pvst  
interface GigabitEthernet0/0/0  
  no ip address  
  duplex auto speed  
  auto  
  ipv6 address 2001:DB8:2113:2::2/64  
  ipv6 enable ipv6 ospf 1 area 1  
interface GigabitEthernet0/0/1  
  no ip address  
  duplex auto speed  
  auto  
  ipv6 address 2001:DB8:2113:3::2/64  
  ipv6 enable ipv6 ospf 1 area 1 standby  
  version 2  
  standby 0 track GigabitEthernet0/0/0  
  standby 113 ipv6 autoconfig standby  
  113 priority 150  
interface GigabitEthernet0/0/2  
  media-type sfp no  
  ip address duplex  
  auto speed auto  
  shutdown  
interface Vlan1  
  no ip address shutdown  
ipv6 router ospf 1  
  router-id 3.3.3.3 log-adjacency-changes  
! ip classless  
ip flow-export version 9  
line con 0 logging  
  synchronous  
line aux 0  
line vty 0 4 logging  
  synchronous  
  login local transport  
  input ssh transport  
  output ssh  
end
```

		Носов С.С.			КИК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

Багаторівневий комутатор MLS_21_13_1:

version 16.3.2

```
no service timestamps log datetime msec no
service timestamps debug datetime msec
service password-encryption
hostname MLS_21_13_1
enable secret 5 $1$mERr$jru/RnXiM18dxqPMjj788.
no ip cef ipv6
unicast-routing
no ipv6 cef
username admin privilege 15 secret 5 $1$mERr$qnVcFVUraySLnKS3XOpTd.
username user
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 105 ip domain-
name nosov.local
spanning-tree mode pvst
spanning-tree vlan 10,20,30,40,50,100 priority 24576
interface Port-channel4
interface GigabitEthernet1/0/1
    no switchport no
    ip address duplex
    auto speed auto
    ipv6 address 2001:DB8:2113:3::4/64
    ipv6 ospf 1 area 1
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/0/3
    switchport trunk allowed vlan 10,20,30,40,50,100
    switchport trunk encapsulation dot1q switchport
    mode trunk
!
interface GigabitEthernet1/0/4
    switchport trunk allowed vlan 10,20,30,40,50,100
    switchport trunk encapsulation dot1q switchport
    mode trunk
!
interface GigabitEthernet1/0/5
    switchport trunk allowed vlan 10,20,30,40,50,100
    switchport trunk encapsulation dot1q switchport
    mode trunk
!
interface GigabitEthernet1/0/6
    switchport trunk allowed vlan 10,20,30,40,50,100
    switchport trunk encapsulation dot1q switchport
    mode trunk
!
interface GigabitEthernet1/0/7
    switchport trunk allowed vlan 10,20,30,40,50,100
    switchport trunk encapsulation dot1q switchport
    mode trunk
!
interface GigabitEthernet1/0/8 channel-group
    4 mode active
!
```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

```

interface GigabitEthernet1/0/9 channel-group
 4 mode active
!
interface GigabitEthernet1/0/10
switchport access vlan 20
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/11
switchport access vlan 30
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/12
switchport access vlan 40
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/13
switchport access vlan 50
switchport mode access
switchport nonegotiate
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
switchport access vlan 10 switchport mode access switchport nonegotiate
!
interface GigabitEthernet1/0/24
! interface GigabitEthernet1/1/1
! interface GigabitEthernet1/1/2
! interface GigabitEthernet1/1/3
! interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address shutdown
!
interface Vlan10
mac-address 0090.0c81.3301 no ip address
ipv6 address 2001:DB8:2113:10::1/64 ipv6 enable

```

		Носов С.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

```

!
interface Vlan20
  mac-address 0090.0c81.3302 no ip address
  ipv6 address 2001:DB8:2113:20::1/64 ipv6 enable
!
interface Vlan30
  mac-address 0090.0c81.3303 no ip address
  ipv6 address 2001:DB8:2113:30::1/64
!
interface Vlan40
  mac-address 0090.0c81.3304 no ip address
  ipv6 address 2001:DB8:2113:40::1/64
!
interface Vlan50
  mac-address 0090.0c81.3305

  no ip address ipv6 address
  2001:DB8:2113:50::1/64
!
interface Vlan100
  mac-address 0090.0c81.3306 no ip
  address ipv6 address
  2001:DB8:2113:100::1/64
!
interface Vlan1000
  mac-address 0090.0c81.3307 no
  ip address
!
ipv6 router ospf 1
  router-id 4.4.4.4 log-adjacency-changes
! ip classless
!
ip flow-export version 9
line con 0 logging
  synchronous
!
line aux 0
!
line vty 0 4 logging
  synchronous login
  local transport input
  ssh transport output
  ssh
end

```

Багаторівневий комутатор MLS_21_13_2:

```

version 16.3.2
no service timestamps log datetime msec no
service timestamps debug datetime msec
service password-encryption
hostname MLS_21_13_2
  enable secret 5 $1$mERr$jru/RnXiM18dxqPMjj788.
no ip cef
ipv6 unicast-routing
no ipv6 cef

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

```

username admin privilege 15 secret 5 $1$mERr$qnVcFVUraySLnKS3XOpTd.
username user password 7 08345F4B1B485744465E
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 105 ip domain-
name nosov.local
spanning-tree mode pvst spanning-tree vlan
10,20,30,40,50,100 priority 28672
interface Port-channel4
interface Port-channel5
interface GigabitEthernet1/0/1
no switchport no
ip address duplex
auto speed auto
ipv6 address 2001:DB8:2113:3::5/64
ipv6 ospf 1 area 1
interface GigabitEthernet1/0/2
interface GigabitEthernet1/0/3
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk
interface GigabitEthernet1/0/4

switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk
!
interface GigabitEthernet1/0/5
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk
!
interface GigabitEthernet1/0/6
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk
!
interface GigabitEthernet1/0/7
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk
!
interface GigabitEthernet1/0/8 channel-group
4 mode active
!
interface GigabitEthernet1/0/9 channel-group
4 mode active
!
interface GigabitEthernet1/0/10 channel-group
5 mode active
!
interface GigabitEthernet1/0/11 channel-group
5 mode active
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				51
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
! interface GigabitEthernet1/1/1
! interface GigabitEthernet1/1/2
! interface GigabitEthernet1/1/3
! interface GigabitEthernet1/1/4
!
interface Vlan1
  no ip address shutdown
!
interface Vlan10
  mac-address 00d0.97e7.1101 no ip address ipv6 address 2001:DB8:2113:10::2/64
!
interface Vlan20
  mac-address 00d0.97e7.1102 no ip address ipv6 address 2001:DB8:2113:20::2/64
!
interface Vlan30
  mac-address 00d0.97e7.1103 no ip address ipv6 address 2001:DB8:2113:30::2/64
!
interface Vlan40
  mac-address 00d0.97e7.1104 no ip address ipv6 address 2001:DB8:2113:40::2/64
!
interface Vlan50
  mac-address 00d0.97e7.1105 no ip address
  ipv6 address 2001:DB8:2113:50::2/64
!
interface Vlan100
  mac-address 00d0.97e7.1106 no ip address
  ipv6 address 2001:DB8:2113:100::2/64
!
ipv6 router ospf 1
  router-id 5.5.5.5 log-adjacency-changes
! ip classless !
ip flow-export version 9
line con 0 logging
  synchronous
!

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

```

line aux 0
!
line vty 0 4 logging
  synchronous
  login local transport
  input  ssh  transport
  output ssh
end

```

```

line con 0 logging
  synchronous
!
line aux 0
!
line vty 0 4 logging
  synchronous
  login local transport
  input  ssh  transport
  output ssh
end

```

Багаторівневий комутатор MLS_21_13_3:

```

version 16.3.2
no service timestamps log datetime msec no
service timestamps debug datetime msec
service password-encryption
hostname MLS_21_13_3
enable secret 5 $1$mERr$jru/RnXiM18dxqPMjj788.
no ip cef
ipv6 unicast-routing
no ipv6 cef
username admin privilege 15 secret 5 $1$mERr$qnVcFVUraySLnKS3XOpTd.
username user password 7 08345F4B1B485744465E
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 105 ip domain-name nosov.local
spanning-tree mode pvst
interface Port-channel5
interface GigabitEthernet1/0/1
interface GigabitEthernet1/0/2
  no switchport no
  ip address duplex
  auto speed auto
  ipv6 address 2001:DB8:2113:3::6/64
  ipv6 ospf 1 area 1
!
interface GigabitEthernet1/0/3
  switchport trunk allowed vlan 10,20,30,40,50,100
  switchport trunk encapsulation dot1q switchport
  mode trunk
!
interface GigabitEthernet1/0/4
  switchport trunk allowed vlan 10,20,30,40,50,100
  switchport trunk encapsulation dot1q switchport
  mode trunk
!

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface GigabitEthernet1/0/5
  switchport trunk allowed vlan 10,20,30,40,50,100
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface GigabitEthernet1/0/6
  switchport trunk allowed vlan 10,20,30,40,50,100
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface GigabitEthernet1/0/7
  switchport trunk allowed vlan 10,20,30,40,50,100
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface GigabitEthernet1/0/8 channel-group
  5 mode active
!
interface GigabitEthernet1/0/9 channel-group
  5 mode active
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
! interface GigabitEthernet1/1/1
! interface GigabitEthernet1/1/2
! interface GigabitEthernet1/1/3
! interface GigabitEthernet1/1/4
!
interface Vlan1
  no ip address shutdown

```

		Носов С.С.			KIK.KP.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Vlan10
  mac-address 00d0.bc11.2501 no ip address
  ipv6 address 2001:DB8:2113:10::3/64
!
interface Vlan20
  mac-address 00d0.bc11.2502 no ip address
  ipv6 address 2001:DB8:2113:20::3/64
!
interface Vlan30
  mac-address 00d0.bc11.2503 no ip address ipv6 address 2001:DB8:2113:30::3/64
!
interface Vlan40
  mac-address 00d0.bc11.2504 no ip address ipv6 address 2001:DB8:2113:40::3/64
! interface Vlan50
  mac-address 00d0.bc11.2505 no ip
  address ipv6 address
  2001:DB8:2113:50::3/64
!
interface Vlan100
  mac-address 00d0.bc11.2506 no ip
  address ipv6 address
  2001:DB8:2113:100::3/64
!
ipv6 router ospf 1
  router-id 6.6.6.6 log-adjacency-changes
! ip classless
!
ip flow-export version 9
line con 0 logging
  synchronous
!
line aux 0
!
line vty 0 4 logging
  synchronous login
  local transport input
  ssh transport output
  ssh
end

```

Комутатор SW_21_13_1:

```

!
version 16.3.2 no service timestamps log
datetime msec no service timestamps debug
datetime msec
service password-encryption
!
hostname SW_21_13_1
! enable secret 5 $1$mERr$jru/RnXiM18dxqPMjj788.
no ip cef no
ipv6 cef
!
!
! username admin privilege 15 secret 5 $1$mERr$qnVcFVUraySLnKS3XOpTd.
username user

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 105 ip domain-
name nosov.local
spanning-tree mode pvst
! interface GigabitEthernet1/0/1
! interface GigabitEthernet1/0/2
! interface GigabitEthernet1/0/3
! interface GigabitEthernet1/0/4
! interface GigabitEthernet1/0/5
! interface GigabitEthernet1/0/6
! interface GigabitEthernet1/0/7
! interface GigabitEthernet1/0/8
! interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
! interface GigabitEthernet1/1/1
! interface GigabitEthernet1/1/2
! interface GigabitEthernet1/1/3
! interface GigabitEthernet1/1/4
!
interface Vlan1
  no ip address shutdown
! ip classless !
ip flow-export version 9
!
!
!
!

```

		Носов С.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

```

!
!
!
!
line con 0 logging synchronous
!
line aux 0
!
line vty 0 4 logging synchronous
  login local transport input ssh transport output ssh
!

!
!
!
end

```

Комутатор SW_21_13_2:

```

!
version 16.3.2 no service timestamps log
datetime msec no service timestamps debug
datetime msec
service password-encryption
!
hostname SW_21_13_2
!
! enable secret 5 $1$mERr$jru/RnXiM18dxqPMjj788.
!
!
!
!
!
!
no ip cef no
ipv6 cef
!
!
! username admin privilege 15 secret 5 $1$mERr$qnVcFVUraySLnKS3XOpTd.
username user password 7 08345F4B1B485744465E
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 105 ip domain-
name nosov.local
!
!
spanning-tree mode pvst
!

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
!
!
!
interface Port-channel1
  switchport trunk allowed vlan 10,20,30,40,50,100
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface GigabitEthernet1/0/1
  switchport trunk allowed vlan 10,20,30,40,50,100
  switchport trunk encapsulation dot1q switchport
  mode trunk
!
interface GigabitEthernet1/0/2
  switchport trunk allowed vlan 10,20,30,40,50,100
  switchport trunk encapsulation dot1q switchport
  mode trunk
!
interface GigabitEthernet1/0/3
  switchport trunk allowed vlan 10,20,30,40,50,100
  switchport trunk encapsulation dot1q switchport
  mode trunk
!
interface GigabitEthernet1/0/4
  switchport trunk allowed vlan 10,20,30,40,50,100
  switchport trunk encapsulation dot1q switchport
  mode trunk channel-group 1 mode active
!
interface GigabitEthernet1/0/5
  switchport trunk allowed vlan 10,20,30,40,50,100
  switchport trunk encapsulation dot1q switchport
  mode trunk channel-group 1 mode active
!
interface GigabitEthernet1/0/6
  switchport trunk allowed vlan 10,100
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
interface GigabitEthernet1/0/7
  switchport trunk allowed vlan 10,100
  switchport trunk encapsulation dot1q
  switchport mode trunk
! interface GigabitEthernet1/0/8
! interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

```

interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
    interface GigabitEthernet1/0/17
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
! interface GigabitEthernet1/1/1
! interface GigabitEthernet1/1/2
! interface GigabitEthernet1/1/3
! interface GigabitEthernet1/1/4
!
interface Vlan1
    no ip address shutdown
!
interface Vlan10
    mac-address 0090.0c98.4d01 no ip address
!
interface Vlan20
    mac-address 0090.0c98.4d02 no ip address
!
interface Vlan30
    mac-address 0090.0c98.4d03 no ip address
!
interface Vlan40
    mac-address 0090.0c98.4d04 no ip address
!
interface Vlan50
    mac-address 0090.0c98.4d05 no ip address
!
interface Vlan100
    mac-address 0090.0c98.4d06 no ip address
    ipv6 address 2001:DB8:2113:100::4/64 ipv6 enable
! ip classless !
ip flow-export version 9
!

line con 0 logging
    synchronous
!
line aux 0
!
line vty 0 4 logging
    synchronous

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

```

login local transport
input ssh transport
output ssh
!
!
!
!
end

```

Комутатор SW_21_13_3:

```

!
version 16.3.2
no service timestamps log datetime msec no
service timestamps debug datetime msec
service password-encryption
!
hostname SW_21_13_3
!
! enable secret 5 $1$mERr$jru/RnXiM18dxqPMjj788.
!
!
!
!
!
!
no ip cef no
ipv6 cef
!
!
! username admin privilege 15 secret 5 $1$mERr$qnVcFVUraySLnKS3XOpTd.
username user password 7 08345F4B1B485744465E
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 105 ip domain-
name nosov.local
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface Port-channel1
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk
!
interface Port-channel2
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk
!
interface GigabitEthernet1/0/1

```

		Носов С.С.			KIK.KP.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

```

switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk
!
interface GigabitEthernet1/0/2
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk
!
interface GigabitEthernet1/0/3
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk
!
interface GigabitEthernet1/0/4
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk channel-group 1 mode passive
!
interface GigabitEthernet1/0/5
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk channel-group 1 mode passive
!
interface GigabitEthernet1/0/6
switchport trunk allowed vlan 10,20,30,40,50,100

switchport trunk encapsulation dot1q

switchport mode trunk channel-group 2 mode active

interface GigabitEthernet1/0/7
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk channel-group 2 mode active
!
interface GigabitEthernet1/0/8
switchport trunk allowed vlan 20,100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/9
switchport trunk allowed vlan 20,100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

```

interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
! interface GigabitEthernet1/1/1
! interface GigabitEthernet1/1/2
! interface GigabitEthernet1/1/3
! interface GigabitEthernet1/1/4
!
interface Vlan1
  no ip address
  shutdown

interface Vlan10
  mac-address 00e0.a311.2401 no ip address
!
interface Vlan20
  mac-address 00e0.a311.2402 no ip address
!
interface Vlan30
  mac-address 00e0.a311.2403 no ip address
!
interface Vlan40
  mac-address 00e0.a311.2404 no ip address
!
interface Vlan50
  mac-address 00e0.a311.2405 no ip address
!
interface Vlan100
  mac-address 00e0.a311.2406 no ip address
  ipv6 address 2001:DB8:2113:100::5/64
! ip classless !
ip flow-export version 9
!
!
!
!
!
!
!
line con 0 logging synchronous
!
line aux 0

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		62

```

!
line vty 0 4 logging synchronous login local transport input ssh transport output ssh
!
!
!
!
end

```

Комутатор SW_21_13_4:

```

!
version 16.3.2

no service timestamps log datetime msec no
service timestamps debug datetime msec
service password-encryption
!
hostname SW_21_13_4
!
! enable secret 5 $1$mERr$jru/RnXiM18dxqPMjj788.
!
!
!
!
!
!
no ip cef no
ipv6 cef
!
!
! username admin privilege 15 secret 5 $1$mERr$qnVcFVUraySLnKS3XOpTd.
username user password 7 08345F4B1B485744465E
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 105 ip domain-
name nosov.local
!
!
spanning-tree mode pvst
!
!
!
!
!
!
!
interface Port-channel2

```

		Носов С.С.			KIK.KP.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		63

```

switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk
!
interface Port-channel3
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk
!
interface GigabitEthernet1/0/1
switchport trunk allowed vlan 10,20,30,40,50,100 switchport
trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/2
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk
!
interface GigabitEthernet1/0/3
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk
!
interface GigabitEthernet1/0/4
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk channel-group 2 mode passive
!
interface GigabitEthernet1/0/5
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk channel-group 2 mode passive
!
interface GigabitEthernet1/0/6
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk channel-group 3 mode active
!
interface GigabitEthernet1/0/7
switchport trunk allowed vlan 10,20,30,40,50,100
switchport trunk encapsulation dot1q switchport
mode trunk channel-group 3 mode active
!
interface GigabitEthernet1/0/8
switchport trunk allowed vlan 30,100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/9
switchport trunk allowed vlan 30,100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/10
!

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

```

interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
    interface GigabitEthernet1/0/15
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
! interface GigabitEthernet1/1/1
! interface GigabitEthernet1/1/2
! interface GigabitEthernet1/1/3
! interface GigabitEthernet1/1/4
!
interface Vlan1
    no ip address shutdown
!
interface Vlan10
    mac-address 0005.5ea1.6401 no ip address
!
interface Vlan20
    mac-address 0005.5ea1.6402 no ip address
!
interface Vlan30
    mac-address 0005.5ea1.6403 no ip address
!
interface Vlan40
    mac-address 0005.5ea1.6404 no ip address
!
interface Vlan50
    mac-address 0005.5ea1.6405 no ip address
!
interface Vlan100
    mac-address 0005.5ea1.6406 no ip address
    ipv6 address 2001:DB8:2113:100::6/64
!
    ip classless

ip flow-export version 9
!

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		65

```

!
!
!
!
!
!
!
line con 0 logging
    synchronous
!
line aux 0
!
line vty 0 4 logging
    synchronous
    login local transport
    input  ssh  transport
    output ssh
!
!
!
!
end

```

Комутатор SW_21_13_5:

```

!
version 16.3.2
no service timestamps log datetime msec no
service timestamps debug datetime msec
service password-encryption
!
hostname SW_21_13_5
!
! enable secret 5 $1$mERr$jru/RnXiM18dxqPMjj788.
!
!
!
!
!
!
no ip cef no
ipv6 cef
!
!
! username admin privilege 15 secret 5 $1$mERr$qnVcFVUraySLnKS3XOpTd.
username user password 7 08345F4B1B485744465E
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 105 ip domain-
name nosov.local
!
!
spanning-tree mode pvst
!
!
!
!

```

		Носов Є.С.			KIK.KP.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

```

!
!
interface Port-channel3
 switchport trunk allowed vlan 10,20,30,40,50,100
 switchport trunk encapsulation dot1q switchport
 mode trunk
!
interface Port-channel4
 switchport trunk allowed vlan 10,20,30,40,50,100
 switchport trunk encapsulation dot1q switchport
 mode trunk
!
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan 10,20,30,40,50,100
 switchport trunk encapsulation dot1q switchport
 mode trunk
!
interface GigabitEthernet1/0/2
 switchport trunk allowed vlan 10,20,30,40,50,100
 switchport trunk encapsulation dot1q switchport
 mode trunk
!
interface GigabitEthernet1/0/3
 switchport trunk allowed vlan 10,20,30,40,50,100
 switchport trunk encapsulation dot1q switchport
 mode trunk
!
interface GigabitEthernet1/0/4
 switchport trunk allowed vlan 10,20,30,40,50,100
 switchport trunk encapsulation dot1q switchport
 mode trunk channel-group 3 mode passive
!
interface GigabitEthernet1/0/5
 switchport trunk allowed vlan 10,20,30,40,50,100
 switchport trunk encapsulation dot1q switchport
 mode trunk channel-group 3 mode passive
!
interface GigabitEthernet1/0/6
 switchport trunk allowed vlan 10,20,30,40,50,100 switchport trunk encapsulation dot1q

 switchport mode trunk channel-group
 4 mode active
!
interface GigabitEthernet1/0/7
 switchport trunk allowed vlan 10,20,30,40,50,100
 switchport trunk encapsulation dot1q switchport
 mode trunk channel-group 4 mode active
! interface GigabitEthernet1/0/8
! interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

```

!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
! interface GigabitEthernet1/1/1
! interface GigabitEthernet1/1/2
! interface GigabitEthernet1/1/3
! interface GigabitEthernet1/1/4
!
interface Vlan1
  no ip address shutdown
!
interface Vlan10
  mac-address 00d0.9781.6701
  no ip address
!
interface Vlan20
  mac-address 00d0.9781.6702 no ip address
!
interface Vlan30
  mac-address 00d0.9781.6703 no ip address
!
interface Vlan40
  mac-address 00d0.9781.6704 no ip address
!
interface Vlan50
  mac-address 00d0.9781.6705 no ip address
!
interface Vlan100
  mac-address 00d0.9781.6706 no ip address
  ipv6 address 2001:DB8:2113:100::7/64
! ip classless !
ip flow-export version 9
!
!
!
!
!
!
!

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				68
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
line con 0 logging synchronous
!
line aux 0
!
line vty 0 4 logging synchronous
  login local transport input ssh transport output ssh
!
!
!
!
end

```

Комутатор SW_21_13_6:

```

!
version 16.3.2

  no service timestamps log datetime msec
  no service timestamps
  debug datetime ms service password-encryption

!
hostname SW_21_13_6
!
! enable secret 5 $1$mERr$jru/RnXiM18dxqPMjj788.
!
!
!
!
!
!
no ip cef no
ipv6 cef
!
!
! username admin privilege 15 secret 5 $1$mERr$qnVcFVUraySLnKS3XOpTd.
username user password 7 08345F4B1B485744465E
!
!
!
!
!
!
!
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 105 ip domain-
name nosov.local
!
!
spanning-tree mode pvst
!

```

		Носов С.С.			KIK.KP.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

```

!
!
!
!
!
interface Port-channel4
 switchport trunk allowed vlan 10,20,30,40,50,100
 switchport trunk encapsulation dot1q switchport
 mode trunk
!
interface GigabitEthernet1/0/1
 switchport trunk allowed vlan 10,20,30,40,50,100
 switchport trunk encapsulation dot1q switchport
 mode trunk
!
interface GigabitEthernet1/0/2
 switchport trunk allowed vlan 10,20,30,40,50,100
 switchport trunk encapsulation dot1q switchport
 mode trunk
!
interface GigabitEthernet1/0/3
 switchport trunk allowed vlan 10,20,30,40,50,100
 switchport trunk encapsulation dot1q switchport
 mode trunk
!
interface GigabitEthernet1/0/4
 switchport trunk allowed vlan 10,20,30,40,50,100
 switchport trunk encapsulation dot1q switchport
 mode trunk channel-group 4 mode passive
!
interface GigabitEthernet1/0/5
 switchport trunk allowed vlan 10,20,30,40,50,100
 switchport trunk encapsulation dot1q switchport
 mode trunk channel-group 4 mode passive
!
interface GigabitEthernet1/0/6
 switchport trunk allowed vlan 50,100
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/7
 switchport trunk allowed vlan 50,100
 switchport trunk encapsulation dot1q
 switchport mode trunk
! interface GigabitEthernet1/0/8
! interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
! interface GigabitEthernet1/1/1
! interface GigabitEthernet1/1/2
! interface GigabitEthernet1/1/3
! interface GigabitEthernet1/1/4
!
interface Vlan1
no ip address shutdown
!
interface Vlan10
mac-address 0060.702d.9801 no ip address
!
interface Vlan20
mac-address 0060.702d.9802 no ip address
!
interface Vlan30
mac-address 0060.702d.9803 no ip address
!
interface Vlan40
mac-address 0060.702d.9804 no ip address
!
interface Vlan50
mac-address 0060.702d.9805 no ip address
!
interface Vlan100
mac-address 0060.702d.9806 no ip address
ipv6 address 2001:DB8:2113:100::8/64
! ip classless !
ip flow-export version 9
!
!
!
!
!
!
!
!
line con 0 logging synchronous

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
line aux 0
!
line vty 0 4

logging synchronous
login local transport
input ssh transport
output ssh
!
!
!
!
end

```

Комутатор SW_21_13_7:

```

!
version 16.3.2 no service timestamps log
datetime msec no service timestamps debug
datetime msec
service password-encryption
!
hostname SW_21_13_7
!
! enable secret 5 $1$mERr$jru/RnXiM18dxqPMjj788.
!
!
!
!
!
!
no ip cef no
ipv6 cef
!
!
! username admin privilege 15 secret 5 $1$mERr$qnVcFVUraySLnKS3XOpTd.
username user password 7 08345F4B1B485744465E
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 105 ip domain-
name nosov.local
!
!
spanning-tree mode pvst
!
!
!
!

```

		Носов С.С.			КИК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
interface Port-channel1
  switchport trunk allowed vlan 10,100 switchport trunk encapsulation dot1q switchport mode trunk
!
interface GigabitEthernet1/0/1
  switchport trunk allowed vlan 10,100 switchport trunk encapsulation dot1q switchport mode trunk
!
interface GigabitEthernet1/0/2
  switchport trunk allowed vlan 10,100 switchport trunk encapsulation dot1q switchport mode trunk
  channel-group 1 mode active
!
interface GigabitEthernet1/0/3
  switchport trunk allowed vlan 10,100 switchport trunk encapsulation dot1q switchport mode trunk
  channel-group 1 mode active
!
interface GigabitEthernet1/0/4
  switchport access vlan 10 switchport mode access switchport nonegotiate spanning-tree portfast
  spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/5
  switchport access vlan 10 switchport mode access switchport nonegotiate spanning-tree portfast
  spanning-tree bpduguard enable
! interface GigabitEthernet1/0/6
! interface GigabitEthernet1/0/7
! interface GigabitEthernet1/0/8
! interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
  ! login local
  transport input ssh
  transport output ssh
!
!
!
!
End

```

Комутатор SW_21_13_8:

```

!
version 16.3.2
no service timestamps log datetime msec no
service timestamps debug datetime msec
service password-encryption
!
hostname SW_21_13_8
!
! enable secret 5 $1$mERr$jru/RnXiM18dxqPMjj788.

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

```

!
!
!
!
!
no ip cef no
ipv6 cef
!
!
! username admin privilege 15 secret 5 $1$mERr$qnVcFVUraySLnKS3XOpTd.
username user password 7 08345F4B1B485744465E
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 105 ip domain-
name nosov.local
!
!
spanning-tree mode pvst
!
!
!
!
!
! interface Port-channel1
switchport trunk allowed vlan 10,100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/1
switchport trunk allowed vlan 10,100
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet1/0/2
switchport trunk allowed vlan 10,100
switchport trunk encapsulation dot1q
switchport mode trunk channel-group 1 mode active
!
interface GigabitEthernet1/0/3
switchport trunk allowed vlan 10,100 switchport trunk
encapsulation dot1q switchport mode trunk
channel-group 1 mode active
!
interface GigabitEthernet1/0/4
switchport access vlan 10 switchport mode access
switchport nonegotiate spanning-tree portfast

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

```

spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/5
  switchport access vlan 10 switchport mode access switchport nonegotiate spanning-tree portfast
  spanning-tree bpduguard enable
! interface GigabitEthernet1/0/6
! interface GigabitEthernet1/0/7
! interface GigabitEthernet1/0/8
! interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
  interface GigabitEthernet1/0/17
  !
  interface GigabitEthernet1/0/18
  !
  interface GigabitEthernet1/0/19
  !
  interface GigabitEthernet1/0/20
  !
  interface GigabitEthernet1/0/21
  !
  interface GigabitEthernet1/0/22
  !
  interface GigabitEthernet1/0/23
  !
  interface GigabitEthernet1/0/24
! interface GigabitEthernet1/1/1
! interface GigabitEthernet1/1/2
! interface GigabitEthernet1/1/3
! interface GigabitEthernet1/1/4
!
interface Vlan1
  no ip address shutdown
!
interface Vlan10
  mac-address 0001.43c0.c801 no ip address
!
interface Vlan100
  mac-address 0001.43c0.c802 no ip address
ipv6 address 2001:DB8:2113:100::10/64
! ip classless !
ip flow-export version 9
!
!
!

```

		Носов С.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		75

```

!
!
!
!
!
line con 0 logging synchronous
!
line aux 0
!

```

Комутатор SW_21_13_9:

```
!
version 16.3.2 no service timestamps log
datetime msec no service timestamps debug
datetime msec
service password-encryption
!
hostname SW_21_13_9
!
! enable secret 5 $1$mERr$jru/RnXiM18dxqPMjj788.
!
!
!
!
!
!
!
no ip cef no
ipv6 cef
!
!
! username admin privilege 15 secret 5 $1$mERr$qnVcFVUraySLnKS3XOpTd.
username user password 7 08345F4B1B485744465E
!
!
!
!
!
!
!
!
!
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 105 ip domain-
name nosov.local
!
!
```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

```

spanning-tree mode pvst
!
!
!
!
!
interface Port-channel1
    switchport trunk allowed vlan 20,100
    switchport trunk encapsulation dot1q
    switchport mode trunk
!
interface GigabitEthernet1/0/1
    switchport trunk allowed vlan 20,100
    switchport trunk encapsulation dot1q
    switchport mode trunk
!
interface GigabitEthernet1/0/2
    switchport trunk allowed vlan 20,100
    switchport trunk encapsulation dot1q
    switchport mode trunk channel-group 1 mode active
!
interface GigabitEthernet1/0/3
    switchport trunk allowed vlan 20,100 switchport trunk
    encapsulation dot1q
    switchport mode trunk channel-group 1 mode active
!
interface GigabitEthernet1/0/4
    switchport access vlan 20
    switchport mode access
    switchport nonegotiate spanning-tree portfast
    spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/5
    switchport access vlan 20 switchport mode access
    switchport nonegotiate
    spanning-tree portfast
    spanning-tree bpduguard enable
! interface GigabitEthernet1/0/6
! interface GigabitEthernet1/0/7
! interface GigabitEthernet1/0/8
! interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
!
interface GigabitEthernet1/0/12
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16

```

		Носов Є.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		77

```

interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
! interface GigabitEthernet1/1/1
! interface GigabitEthernet1/1/2
! interface GigabitEthernet1/1/3
! interface GigabitEthernet1/1/4
!
interface Vlan1
  no ip address shutdown
!
interface Vlan20
  mac-address 0002.1613.d701 no ip address
!
interface Vlan100
  mac-address 0002.1613.d702 no ip address
ipv6 address 2001:DB8:2113:100::11/64
! ip classless !
ip flow-export version 9
!
!
!
!
!
!
!
!
!
line con 0 logging synchronous
!
line aux 0
!
line vty 0 4 logging synchronous login local transport input ssh

```

		Носов С.С.			КІК.КР.Б – 125 – 15 – ПЗ	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		78