

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

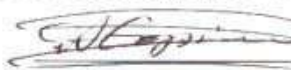
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект захищеної локальної комутованої
мережі організації, побудованої на базі обладнання
компанії Huawei»

Виконав: студент 4-го курсу групи КБ-21-1
спеціальності 125 «Кібербезпека»

 Андрій ДЕМЧУК

Керівник: завідувач кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук, доцент

 Андрій ЄФІМЕНКО

Рецензент: професор кафедри комп'ютерної інженерії та
кібербезпеки, доктор технічних наук, доцент

 Володимир ВОРОТНИКОВ

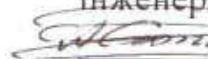
Житомир – 2025

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

30 квітня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Демчук Андрій Сергійович

Тема роботи: «Проект захищеної локальної комутованої мережі організації, побудованої на базі обладнання компанії Huawei»

затверджена Наказом університету від 3 березня 2025 р. №80/с.

Термін здачі студентом закінченої роботи 16 червня 2025 р.

Вихідні дані роботи:

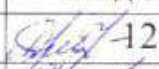
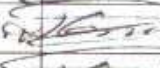
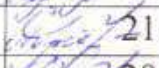
Вимоги до продуктивності, надійності та безпеки мережевої інфраструктури IT-компанії, а також функціональні можливості мережевого обладнання Huawei, що моделюється в програмному середовищі eNSP.

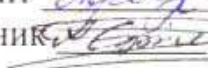
Обладнання та програмне забезпечення:

Huawei eNSP (Enterprise Network Simulation Platform): Використовується як основний інструмент для моделювання та тестування проєктованої локальної комутованої мережі.

Microsoft Windows: Використовується як операційна система для робочої станції, на якій встановлено та функціонує програмне забезпечення Huawei eNSP.

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

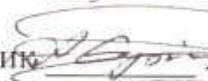
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	 12.05.2025	 12.05.2025
2	Єфіменко А.А.	 21.05.2025	 21.05.2025
3	Єфіменко А.А.	 29.05.2025	 29.05.2025

Студент  Андрій ДЕМЧУК
Керівник  Андрій ЄФІМЕНКО

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	03.03.2025	Виконано
2	Формулювання технічного завдання	14.03.2025	Виконано
3	Проведення аналізу літературних мереж	15.03.2025	Виконано
4	Розробка плану	02.05.2025	Виконано
5	Проектування структури системи	09.05.2025	Виконано
6	Побудова локальної мережі в програмному додатку	20.05.2025	Виконано
7	Проведення тестувань побудованої мережі	25.05.2025	Виконано
8	Оформлення пояснювальної записки	08.06.2025	Виконано
9	Підготовка доповіді та створення презентації	16.06.2025	Виконано
10	Захист		Виконано

Студент  Андрій ДЕМЧУК

Керівник  Андрій ЄФІМЕНКО

АНОТАЦІЯ

Випускна кваліфікаційна робота складається з проєкту захищеної локальної комутованої мережі, розробленого в середовищі симуляції, та пояснювальної записки. Пояснювальна записка до кваліфікаційної роботи містить текстову частину, викладену на 72 сторінках друкованого тексту. Список використаних джерел містить 19 найменувань і займає 2 сторінки. У роботі наведено 56 рисунків та 13 таблиць. Загальний обсяг роботи – 94 сторінки.

Метою роботи є розробка комплексного проєкту захищеної, надійної та високопродуктивної локальної комутованої мережі для сучасної ІТ-компанії на базі мережевого обладнання компанії Huawei.

Проєктування захищеної корпоративної мережі включало аналіз теоретичних аспектів сучасних комутованих мереж, розробку ієрархічної архітектури з логічною сегментацією на основі VLAN, обґрунтування вибору обладнання Huawei, а також детальне налаштування протоколів надійності (RSTP, VRRP), динамічної маршрутизації (OSPF) та механізмів безпеки (ACL, SSH). Для практичної реалізації та перевірки розроблених рішень було використано програмний симулятор Huawei eNSP.

Спроектована мережа пройшла комплексне тестування, що підтвердило її функціональність та відповідність поставленим вимогам безпеки та надійності.

Ключові слова: ЛОКАЛЬНА МЕРЕЖА, КОМУТАЦІЯ, МАРШРУТИЗАЦІЯ, БЕЗПЕКА МЕРЕЖІ, HUAWEI, VLAN, ACL, OSPF, VRRP, RSTP, ENSP.

					KKKB.KP.B – 125 – 03 – ПЗ		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.	Демчук А.С.			16.06.25	Проект захищеної локальної комутованої мережі організації, побудованої на базі обладнання компанії Huawei	Літ.	Арк.
Керівник	Єфіменко А.А.			16.06.25			4
Реценз.	Вороніков В.В.			16.06.25			94
Н. контр.	Єфіменко А.А.			16.06.25		ФІКТ, Гр. КБ-21-1	
Затверд.	Єфіменко А.А.			16.06.25			

ANNOTATION

The bachelor's thesis consists of a project for a secure local switched network developed in a simulation environment and an explanatory note. The explanatory note to the thesis contains a text section of 72 pages of printed text. The list of references contains 19 items and occupies 2 pages. The thesis contains 56 figures and 13 tables. The total volume of the thesis is 94 pages.

The purpose of the work is to develop a comprehensive project for a secure, reliable, and highly productive local switched network for a modern IT company based on Huawei network equipment.

The design of a secure corporate network included an analysis of the theoretical aspects of modern switched networks, the development of a hierarchical architecture with logical segmentation based on VLAN, justification for the choice of Huawei equipment, as well as detailed configuration of reliability protocols (RSTP, VRRP), dynamic routing (OSPF), and security mechanisms (ACL, SSH). The Huawei eNSP software simulator was used for the practical implementation and testing of the developed solutions.

The designed network underwent comprehensive testing, which confirmed its functionality and compliance with the set security and reliability requirements.

Keywords: LOCAL AREA NETWORK, SWITCHING, ROUTING, NETWORK SECURITY, HUAWEI, VLAN, ACL, OSPF, VRRP, RSTP, ENSP.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ СУЧАСНИХ КОМУТОВАНИХ ЛОКАЛЬНИХ МЕРЕЖ	10
1.1 Принципи та моделі побудови комутованої локальної мережі.....	10
1.2 Принципи та технології забезпечення продуктивності локальної мережі.	17
1.3 Принципи та протоколи забезпечення надійності	19
1.4 Принципи, протоколи та технології канального рівня для забезпечення безпеки локальної мережі	20
1.5 Принципи, протоколи та технології канального рівня для забезпечення безпеки локальної мережі	21
1.6 Постановка технічного завдання	22
РОЗДІЛ 2. ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ ЛОКАЛЬНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ	24
2.1 Розробка топології локальної мережі.....	24
2.2 Розробка схеми адресації мережі.....	33
2.3 Проект базових сервісів мережі.....	40
2.4 Розробка підсистеми захисту мережі	41
2.5 Вибір програмного забезпечення для реалізації проєкту	47
РОЗДІЛ 3. ВИБІР ОБЛАДНАННЯ, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ФУНКЦІОНАЛУ МЕРЕЖІ.....	50
3.1 Вибір обладнання	50
3.2 Базове налагодження пристроїв мережі.....	56
3.3 Налаштування засобів та протоколів мережного захисту	60
3.4 Тестування функціоналу мережного захисту	65
ВИСНОВКИ.....	69
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	71
ДОДАТКИ.....	73

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ЛМ / LAN – Local Area Network, локальна мережа

VLAN – Virtual Local Area Network, Віртуальна локальна мережа

ACL – Access Control List, список контролю доступу

IP – Internet Protocol, міжмережевий протокол

DHCP – Dynamic Host Configuration Protocol, протокол динамічної конфігурації хоста

DNS – Domain Name System, система доменних імен

ARP – Address Resolution Protocol, протокол визначення адреси

OSPF – Open Shortest Path First, протокол вибору найкоротшого шляху

VRRP – Virtual Router Redundancy Protocol, протокол резервування віртуальних маршрутизаторів

RSTP – Rapid Spanning Tree Protocol, протокол для запобігання петлям комутації з покращеним часом конвергенції

SSH – Secure Shell, мережевий протокол для безпечного віддаленого доступу

NAT – Network Address Translation, трансляція мережесих адрес

ISP – Internet Service Provider, інтернет-провайдер

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. В умовах сучасної цифрової економіки, що характеризується глобалізацією ринків, стрімким зростанням обсягів даних та тотальною цифровізацією бізнес-процесів, корпоративна мережева інфраструктура перетворилася з допоміжного інструменту на стратегічно важливий актив будь-якої організації. Локальна мережа (ЛМ) є фундаментом, на якому функціонують усі інформаційні системи підприємства: від корпоративної пошти та систем управління ресурсами (ERP) до хмарних додатків, IP-телефонії та систем відеоспостереження. Від її продуктивності, надійності та, що найважливіше, безпеки безпосередньо залежить безперервність операційної діяльності, конфіденційність комерційної інформації та загальна конкурентоспроможність компанії.

Водночас зі зростанням залежності від мережевих технологій експоненційно зростає і кількість кіберзагроз. Сучасні атаки стають все більш витонченими та спрямованими не лише на зовнішній периметр мережі, але й на її внутрішні компоненти. Вразливості на каналному рівні, несанкціонований доступ, відмови в обслуговуванні та крадіжки даних становлять реальну загрозу для будь-якої компанії. За таких умов просте забезпечення зв'язності вже не є достатнім. Виникає гостра потреба у побудові комплексних, багаторівневих систем захисту, інтегрованих безпосередньо в архітектуру локальної мережі.

Таким чином, завдання проєктування сучасної локальної комутованої мережі, яка б гармонійно поєднувала високу продуктивність, відмовостійкість та надійні механізми захисту, є надзвичайно актуальним. Використання для цього обладнання від провідних світових виробників, яким є компанія Huawei, дозволяє реалізувати проєкт на базі перевірених та функціонально багатих рішень, що додає даній роботі практичної значущості.

Метою даної кваліфікаційної роботи є розробка комплексного проєкту захищеної, надійної та високопродуктивної локальної комутованої мережі для сучасної ІТ-компанії на базі мережевого обладнання компанії Huawei.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

Для досягнення поставленої мети необхідно вирішити такі основні завдання: Провести системний аналіз теоретичних основ побудови сучасних комутованих мереж. Дослідити ієрархічні моделі проєктування, технології віртуальних локальних мереж (VLAN), методи забезпечення продуктивності (агрегація каналів, QoS), протоколи відмовостійкості (STP/RSTP, VRRP) та ключові механізми безпеки на каналному та мережевому рівнях.

Розробити архітектуру корпоративної мережі, враховуючи специфічні вимоги та структуру ІТ-компанії. Створити детальну фізичну та логічну топологію, розробити схему IP-адресації з урахуванням сегментації, а також спроектувати розміщення базових мережевих сервісів та політик безпеки.

На основі розробленої архітектури здійснити обґрунтований вибір конкретних моделей мережевого обладнання Huawei та розробити детальні інструкції з їх конфігурації для реалізації запланованого функціоналу.

Виконати практичну реалізацію спроектованої мережі в програмному середовищі симуляції Huawei eNSP. Провести комплексне тестування для перевірки базової зв'язності, коректності роботи протоколів надійності та ефективності впроваджених механізмів мережевого захисту.

Об'єктом дослідження є процес проєктування та впровадження сучасних захищених локальних комутованих мереж.

Предметом дослідження є моделі, технології та протоколи для побудови захищеної локальної мережі організації з використанням мережевого обладнання компанії Huawei.

У процесі виконання кваліфікаційної роботи було розроблено проєкт захищеної корпоративної мережі для ІТ-компанії. Проєкт включає ієрархічну топологію, логічну сегментацію за допомогою VLAN та багаторівневу систему безпеки, реалізовану на базі обладнання Huawei.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПОБУДОВИ СУЧАСНИХ КОМУТОВАНИХ ЛОКАЛЬНИХ МЕРЕЖ

1.1 Принципи та моделі побудови комутованої локальної мережі

Локальна мережа (ЛМ), або Local Area Network (LAN) – це комунікаційна система, що з'єднує комп'ютери та інші периферійні пристрої в межах обмеженої географічної території, такої як одна будівля, офіс або академічний кампус. У сучасній інформаційній екосистемі будь-якої організації ЛМ є не просто допоміжним інструментом, а критично важливою інфраструктурою, що лежить в основі всіх бізнес-процесів. Вона забезпечує спільний доступ до даних, програмних додатків, мережевих принтерів та інших ресурсів, а також слугує платформою для корпоративної комунікації, включаючи електронну пошту, IP-телефонію та відеоконференцз'язок. Ефективність, надійність та безпека локальної мережі безпосередньо впливають на продуктивність праці співробітників та загальну конкурентоспроможність організації.

Еволюція технологій локальних мереж пройшла декілька ключових етапів. Ранні реалізації, такі як ARCNET та Token Ring, використовували детерміновані методи доступу до середовища. Однак технологія Ethernet, розроблена компанією Херох у 1970-х роках, завдяки своїй простоті та низькій вартості швидко завоювала домінуюче положення. Перші покоління Ethernet базувалися на використанні розділюваного середовища передачі даних. У таких мережах, побудованих на коаксіальному кабелі (топології "спільна шина") або з використанням концентраторів (hub) на основі витой пари (топологія "зірка"), всі підключені пристрої знаходилися в одному домені колізій. Це означало, що в будь-який момент часу лише один пристрій міг успішно передавати дані. Якщо два або більше пристроїв намагалися передавати одночасно, виникала колізія — зіткнення сигналів, що призводило до пошкодження даних. Для вирішення цієї проблеми використовувався метод доступу CSMA/CD (Carrier Sense Multiple Access with Collision Detection), який вимагав від пристроїв "прослуховувати" середовище перед передачею та виявляти колізії. Зі

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

зростанням кількості вузлів та інтенсивності трафіку, кількість колізій стрімко зростала, що призводило до експоненційного падіння реальної пропускної здатності мережі.

Револьюційним кроком, що дозволив подолати обмеження розділюваного середовища, став перехід до комутованих мереж. Основою таких мереж є комутатор (switch) — інтелектуальний пристрій, що працює на каналному рівні (Layer 2) еталонної моделі OSI. На відміну від концентратора, який просто повторював отриманий електричний сигнал на всі свої порти, комутатор аналізує кожен вхідний кадр даних (frame). Він зчитує MAC-адресу (Media Access Control address) призначення, що міститься в заголовку кадру, і пересилає цей кадр виключно на той порт, до якого підключений пристрій-одержувач. Цей процес називається мікросегментацією, оскільки кожен порт комутатора, по суті, стає окремим, ізольованим доменом колізій. Таким чином, колізії можуть виникати лише на з'єднанні між комутатором і кінцевим пристроєм, якщо вони працюють у напівдуплексному режимі. При використанні повнодуплексного режиму (full-duplex), коли пристрій може одночасно передавати та приймати дані, колізії усуваються повністю. Це дозволило кардинально підвищити ефективність використання пропускної здатності мережі.

Принцип роботи комутатора базується на веденні та динамічному оновленні спеціальної таблиці MAC-адрес. Процес обробки кадрів комутатором включає три основні логічні операції, що виконуються послідовно:

- Навчання (Learning).
- Фільтрація та пересилання (Filtering and Forwarding).
- Затоплення (Flooding).

Навчання відбувається в момент, коли кадр надходить на один із портів. Комутатор аналізує MAC-адресу джерела і, якщо запису для неї ще немає в таблиці, створює новий, пов'язуючи цю адресу з номером порту, на який надійшов кадр. Таким чином, комутатор "дізнається" про розташування пристроїв у мережі. Кожен запис у таблиці має певний час життя (aging time), після закінчення якого він видаляється, що дозволяє таблиці залишатися актуальною при зміні топології мережі.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

Фільтрація та пересилання є основною інтелектуальною функцією комутатора. Після аналізу MAC-адреси джерела, пристрій перевіряє MAC-адресу призначення. Він здійснює пошук цієї адреси у своїй таблиці комутації. Якщо відповідний запис знайдено, комутатор пересилає кадр лише на той порт, що вказаний у записі, фільтруючи його від усіх інших портів, де він не потрібен.

Затоплення є необхідною операцією у випадках, коли MAC-адреса призначення відсутня в таблиці комутації (що трапляється, коли до цього пристрою ще не було передачі даних) або якщо адреса є широкомовною (broadcast) чи груповою (multicast). У такій ситуації комутатор змушений розіслати кадр на всі свої порти, окрім того, з якого він був отриманий, щоб гарантувати доставку та забезпечити роботу сервісних протоколів, таких як ARP та DHCP.

Для проєктування масштабованих, надійних та керованих корпоративних мереж застосовується ієрархічний підхід [1]. Цей підхід структурує мережу у вигляді логічних рівнів, кожен з яких виконує чітко визначені функції. Існують дві основні моделі ієрархічного проєктування:

- Трирівнева ієрархічна модель.
- Дворівнева ієрархічна модель

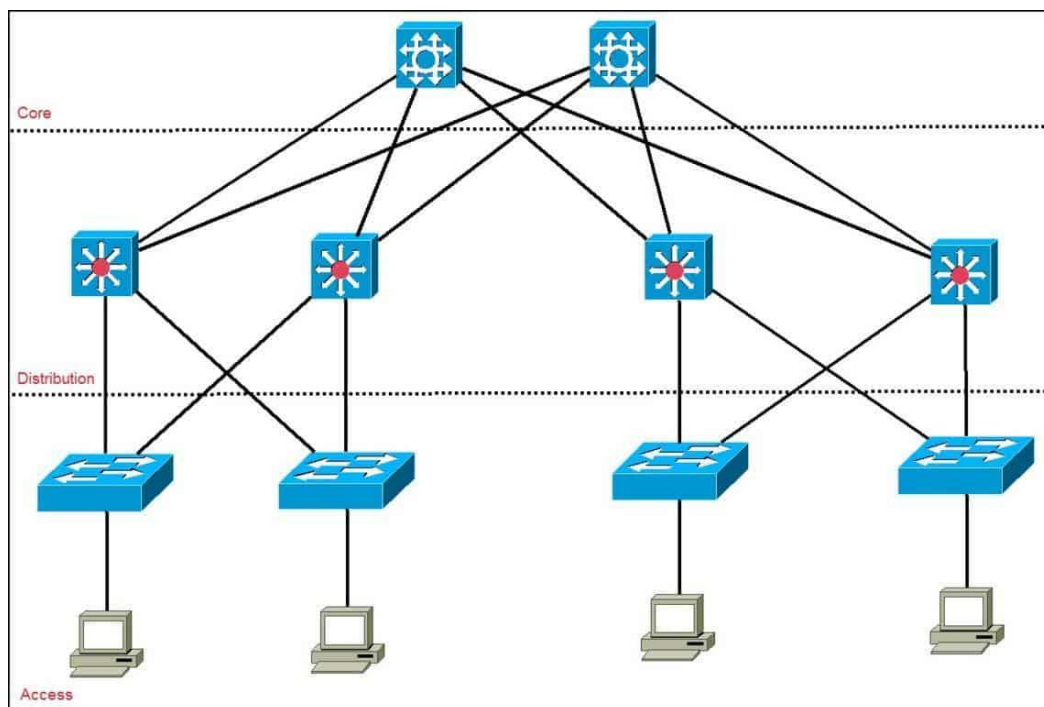


Рисунок 1.1 – Трирівнева ієрархічна модель комп'ютерної мережі

Трирівнева ієрархічна модель є класичним та найбільш повним підходом до проектування великих корпоративних мереж. Вона передбачає чіткий поділ на три функціональні рівні. Рівень доступу (Access Layer) забезпечує підключення кінцевих пристроїв. Рівень розподілу (Distribution Layer) агрегує трафік з рівня доступу, виконує маршрутизацію між VLAN та застосовує політики безпеки. Рівень ядра (Core Layer) слугує високошвидкісною магістраллю для пересилання трафіку між різними сегментами рівня розподілу.

До переваг трирівневої моделі можна віднести наступні пункти:

- Висока масштабованість
- Максимальна надійність та доступність
- Прогнозованість та керованість

Модель дозволяє легко розширювати мережу шляхом додавання нових комутаторів на рівні доступу без суттєвого впливу на ядро та розподіл. Чітке розділення функцій дозволяє реалізувати високий ступінь резервування на кожному рівні, особливо на рівнях розподілу та ядра. Подібна ієрархія спрощує планування пропускної здатності, пошук несправностей та управління мережею. Потоки трафіку є передбачуваними, що полегшує діагностику.

Водночас, до недоліків цієї моделі варто зарахувати:

- Висока вартість та підтримка
- Надлишкова складність для невеликих комп'ютерних мереж

Розгортання та підтримка трьох окремих рівнів обладнання потребує значних капіталовкладень, що може бути невиправданим для малих та середніх організацій. Також для організацій, де кількість користувачів та обсяги трафіку невеликі, трирівнева архітектура може бути надто складною в управлінні та конфігурації.

Дворівнева ієрархічна модель, також відома як модель зі згорнутим ядром (Collapsed Core), є модифікацією трирівневої моделі, в якій функції рівнів ядра та розподілу об'єднуються в одному наборі пристроїв. Цей підхід зберігає ієрархічну структуру, але робить її більш компактною та економічно ефективною.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

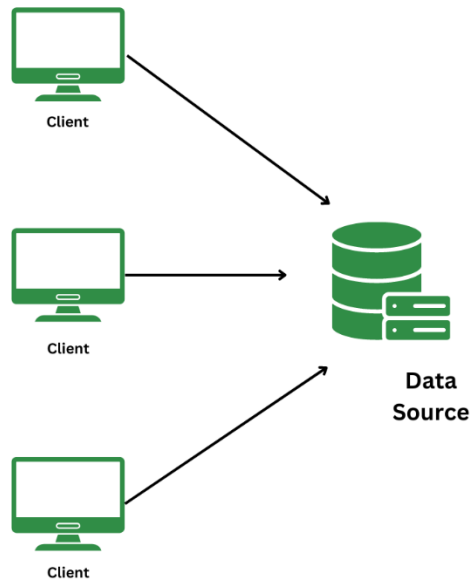


Рисунок 1.2 – Дворівнева ієрархічна модель комп’ютерної мережі

До переваг цієї моделі відносяться:

- Зниження вартості
- Достатня продуктивність для середніх мереж
- Спрощена конфігурація та управління подібними мережами

Об’єднання двох рівнів в один зменшує кількість необхідного обладнання та, відповідно, загальну вартість володіння мережею. Менша кількість пристроїв та рівнів ієрархії полегшує конфігурацію, моніторинг та пошук несправностей. Для більшості організацій середнього розміру продуктивності та надійності, яку забезпечує дворівнева модель, цілком достатньо.

Серед її обмежень можна виділити:

- Обмежена масштабованість
- Менший ступінь гранулярності політик

Хоча модель і є масштабованою, її можливості до розширення поступаються трирівневій архітектурі. Подальше зростання мережі може вимагати повної заміни обладнання згорнутого ядра. Об’єднання функцій ядра та розподілу може ускладнити застосування дуже гранулярних та складних політик безпеки та QoS.

Для даної дипломної роботи, що передбачає проєктування мережі для ІТ-компанії, було обрано повноцінну трирівневу ієрархічну модель. Незважаючи на потенційно вищу початкову вартість у порівнянні з дворівневим підходом, такий вибір

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

є стратегічно виправданим. Він забезпечує максимальну масштабованість для майбутнього зростання компанії, високий рівень надійності за рахунок чіткого резервування на кожному рівні, а також гранулярність у застосуванні політик безпеки, що є критично важливим для ІТ-організації, яка працює з конфіденційними даними та вимогливими додатками. Чітке розмежування функцій між рівнями доступу, розподілу та ядра створює прогнозовану та легко керовану інфраструктуру.

Рівень доступу є найнижчим в ієрархії, де відбувається безпосереднє підключення кінцевих користувацьких пристроїв до мережі. Основні функції цього рівня — надання портів для підключення комп'ютерів, IP-телефонів, принтерів, точок доступу Wi-Fi, а також реалізація політик безпеки на рівні порту (Port Security, 802.1X) та логічна сегментація за допомогою VLAN.

Рівень розподілу є проміжним і виконує функцію агрегації трафіку від комутаторів рівня доступу. Він слугує кордоном між доменами комутації (Layer 2) та доменами маршрутизації (Layer 3). Ключові функції рівня розподілу — маршрутизація між VLAN, застосування політик на основі списків контролю доступу (ACL), реалізація політик QoS та забезпечення надлишковості.

Рівень ядра — це "хребет" або магістраль корпоративної мережі. Його єдине завдання — максимально швидке та надійне пересилання великих обсягів трафіку між різними сегментами рівня розподілу. Головними вимогами до обладнання рівня ядра є найвища пропускна здатність, низька затримка та максимальна надійність, яка досягається шляхом високого ступеня резервування.

Фундаментальною технологією для логічної організації сучасних комутованих мереж є віртуальні локальні мережі (VLAN), стандартизовані протоколом IEEE 802.1Q [3]. Впровадження VLAN надає низку значних переваг, що комплексно покращують архітектуру та керованість мережі:

- Зменшення розміру широкомовних доменів.
- Підвищення безпеки.
- Гнучкість та спрощення адміністрування.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

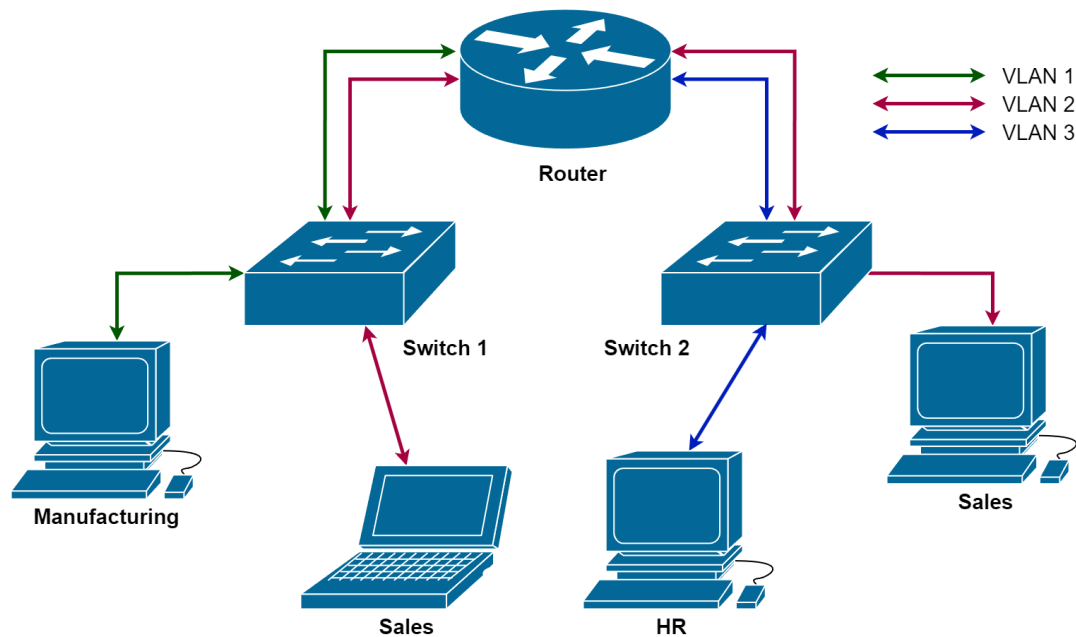


Рисунок 1.3 – Приклад сегментації за допомогою VLAN

Зменшення розміру широкомовних доменів досягається завдяки тому, що широкомовний трафік, який генерується протоколами ARP, DHCP та іншими, обмежується межами своєї VLAN. Він не поширюється на пристрої в інших віртуальних мережах, що значно знижує непродуктивне навантаження на мережеві пристрої та канали зв'язку.

Підвищення безпеки є наслідком логічної ізоляції трафіку. Пристрої, що знаходяться в різних VLAN, за замовчуванням не можуть взаємодіяти між собою на каналному рівні. Для організації комунікації між ними потрібен пристрій третього рівня (маршрутизатор або L3-комутатор), на якому можна застосувати списки контролю доступу (ACL) для суворої регламентації та фільтрації трафіку.

Гнучкість та спрощення адміністрування проявляються у можливості групувати користувачів за функціональним призначенням (наприклад, відділами) незалежно від їхнього фізичного розташування. При переміщенні співробітника в інший кабінет достатньо переналаштувати порт комутатора на відповідну VLAN без необхідності зміни IP-адреси чи фізичної перекомутації кабелів, що значно спрощує управління мережею.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

1.2 Принципи та технології забезпечення продуктивності локальної мережі

Забезпечення високої продуктивності є однією з ключових задач при проектуванні сучасних локальних мереж, особливо в середовищах з інтенсивним трафіком, як-от ІТ-компанії. Продуктивність мережі визначається не лише швидкістю окремих каналів, але й ефективністю роботи комутаційного обладнання. Сучасні комутатори використовують низку технологій для максимізації швидкості обробки трафіку, серед яких варто виділити:

- Високошвидкісні інтерфейси.
- Методи комутації.
- Агрегація каналів

Високошвидкісні інтерфейси є базовим елементом продуктивності. Сучасні мережі активно використовують стандарти Gigabit Ethernet (1 Гбіт/с) для підключення кінцевих пристроїв та 10 Gigabit Ethernet і вище для магістральних з'єднань між комутаторами (аплінків). Використання високошвидкісних аплінків є критично важливим для уникнення "вузьких місць" при агрегації трафіку з великої кількості користувачьких портів.

Методи комутації визначають, як комутатор обробляє кадри, що надходять на його порти. Існує два основних підходи. Наскрізна комутація забезпечує мінімальну затримку, оскільки комутатор починає пересилати кадр відразу після зчитування MAC-адреси призначення, не чекаючи його повного отримання. Це корисно для додатків, надзвичайно чутливих до затримок, але цей метод не виконує перевірку кадру на помилки. На противагу, метод комутації з проміжним зберіганням (Store-and-Forward) передбачає, що комутатор спочатку повністю приймає, буферизує кадр і перевіряє його контрольну суму (CRC). Лише після перевірки на відсутність помилок кадр пересилається далі. Цей метод вносить дещо більшу затримку, але гарантує, що пошкоджені кадри не будуть поширюватися по мережі, що є кращим підходом для більшості корпоративних середовищ.

Агрегація каналів (Link Aggregation), стандартизована як IEEE 802.3ad (LACP), є потужною технологією, що використовується в проєкті для підвищення

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

продуктивності та надійності магістральних з'єднань. Вона дозволяє об'єднати кілька фізичних каналів Ethernet в один логічний канал, який називається Eth-Trunk в термінології Huawei. Це дає дві ключові переваги: сумарну пропускну здатність, що дорівнює сумі пропускних здатностей фізичних каналів, та відмовостійкість — у разі виходу з ладу одного з фізичних каналів, трафік автоматично перерозподіляється між рештою каналів без розриву з'єднання. Для динамічного узгодження параметрів агрегованого каналу між пристроями використовується протокол LACP (Link Aggregation Control Protocol) [11].

Найпотужнішим інструментом управління продуктивністю є Якість обслуговування (Quality of Service, QoS) [6]. Це набір механізмів, які дозволяють мережі надавати різним класам трафіку різний рівень обслуговування, що є абсолютно необхідним у конвергентних мережах. Впровадження QoS є багатоетапним процесом, що включає наступні ключові механізми:

- Класифікація та маркування.
- Управління чергами та планування.
- Запобігання перевантаженням.
- Політика та формування трафіку (Policing and Shaping)..

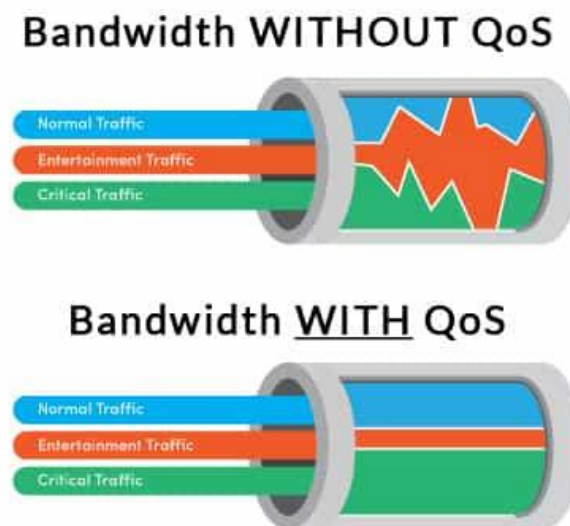


Рисунок 1.5 – Приклад роботи QoS

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

1.3 Принципи та протоколи забезпечення надійності

Забезпечення безперебійної роботи мережі є критичним для будь-якого бізнесу. Основним принципом побудови надійних мереж є надлишковість (резервування) на всіх рівнях. Однак створення надлишкових фізичних шляхів на каналному рівні (Layer 2) призводить до утворення петель комутації. Для боротьби з цією проблемою в проєкті використовується протокол RSTP, проте існують і альтернативні підходи. Для забезпечення надійності шлюзу за замовчуванням у проєкті застосовується VRRP, який також має свої аналоги.

Щодо альтернатив протоколам Spanning Tree, можна виділити наступні технології:

- Transparent Interconnection of Lots of Links (TRILL)
- Shortest Path Bridging (SPB)

Хоча протоколи родини STP (STP, RSTP, MSTP) є галузевим стандартом, їхнім основним недоліком є те, що для запобігання петлям вони блокують надлишкові шляхи, не дозволяючи використовувати їх для передачі даних у штатному режимі. Сучасніші технології, такі як TRILL та SPB, вирішують цю проблему, дозволяючи використовувати всі доступні шляхи одночасно. Вони інкапсулюють кадри Ethernet у власні заголовки та використовують протоколи маршрутизації стану каналу (схожі на IS-IS) для побудови оптимальних шляхів без петель. Це забезпечує балансування навантаження та значно ефективніше використання пропускної здатності мережі. Однак ці технології є більш складними і зазвичай застосовуються у великих центрах обробки даних. Для корпоративної мережі середнього розміру, як у даному проєкті, простоти та швидкості конвергенції RSTP цілком достатньо [12].

Іншим критичним елементом надійності є резервування шлюзу за замовчуванням. Якщо маршрутизатор, що слугує шлюзом для цілого сегмента, виходить з ладу, цей сегмент втрачає зовнішній зв'язок. Для усунення цієї єдиної точки відмови використовуються протоколи резервування першого хопу (First Hop Redundancy Protocols, FHRP), найпоширенішим з яких є Virtual Router Redundancy Protocol (VRRP) [2][9].

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				19
Змн.	Арк.	№ докум.	Підпис	Дата		

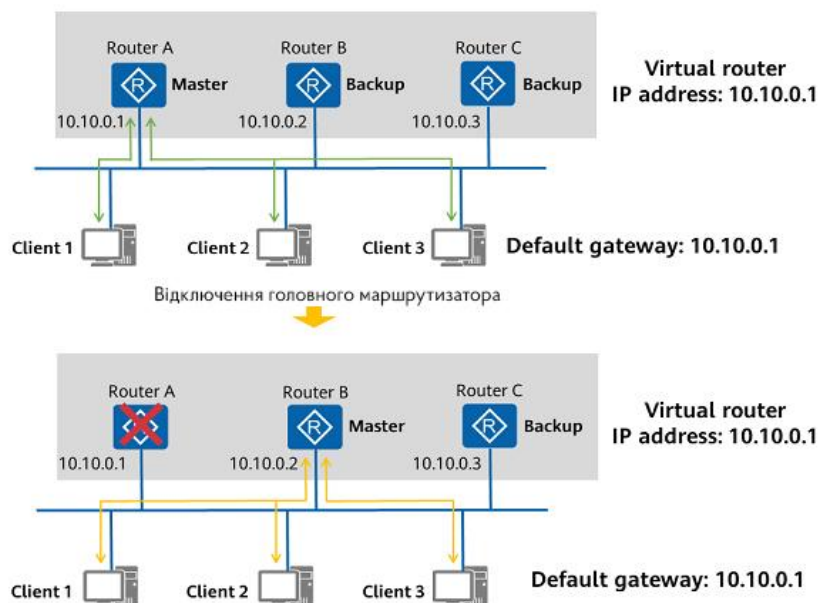


Рисунок 1.6 – Принцип роботи протоколу VRRP

VRRP дозволяє групі фізичних маршрутизаторів об'єднатися в одну віртуальну групу, яка представляється для кінцевих пристроїв як єдиний віртуальний маршрутизатор з унікальною віртуальною IP- та MAC-адресою. Один з фізичних маршрутизаторів обирається як основний (Master) і активно обробляє трафік. Решта знаходяться в резервному стані (Backup) і постійно моніторять стан основного. У разі відмови Master-маршрутизатора, один з Backup-пристроїв за лічені секунди перебирає на себе його роль, забезпечуючи практично безперебійну роботу шлюзу.

1.4 Принципи, протоколи та технології канального рівня для забезпечення безпеки локальної мережі

Безпека на канальному рівні є фундаментом загальної захищеності мережі. Окрім захисту від типових атак, важливо звернути увагу на протоколи управління VLAN та їх роль у безпеці.

Технологія VLAN як основа безпеки. Як було зазначено раніше, віртуальні локальні мережі (VLAN) є першим і найважливішим кроком у забезпеченні безпеки. Створюючи окремі логічні сегменти для різних відділів (ІТ-відділ, бухгалтерія, гості), ми ізолюємо їхній трафік один від одного. Навіть якщо один із сегментів буде скомпрометовано, атака не зможе автоматично поширитися на інші частини

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				20
Змн.	Арк.	№ докум.	Підпис	Дата		

мережі. Контроль взаємодії між VLAN здійснюється на пристрої 3-го рівня за допомогою списків контролю доступу (ACL), що дозволяє створити гранулярну політику безпеки "заборонено все, що не дозволено явно".

Протоколи динамічного управління VLAN. Для автоматизації процесу створення та поширення інформації про VLAN у великих мережах було розроблено протокол GVRP (GARP VLAN Registration Protocol) [10]. Він дозволяв комутаторам динамічно створювати VLAN та додавати порти до них на основі інформації, отриманої від сусідніх пристроїв. Це спрощувало адміністрування, але створювало певні ризики безпеки, оскільки несанкціоноване підключення могло спровокувати небажані зміни в конфігурації VLAN по всій мережі. Через ці недоліки та складність контролю, GVRP сьогодні практично не використовується, і стандартом де-факто є статична конфігурація VLAN та транкових каналів, що забезпечує повний контроль адміністратора над логічною структурою мережі.

Окрім цього, для комплексного захисту канального рівня необхідно застосовувати й інші технології. До таких технологій можна віднести захист протоколу Spanning Tree, що включає механізми BPDU Guard та Root Guard для запобігання атакам, спрямованим на маніпуляцію топологією STP, а також функцію ізоляції портів (Port Isolation), яка дозволяє ізолювати порти в межах однієї VLAN один від одного, щоб пристрої могли спілкуватися лише зі шлюзом, а не між собою.

1.5 Принципи, протоколи та технології канального рівня для забезпечення безпеки локальної мережі

Для стабільного, автоматизованого та керованого функціонування будь-якої локальної мережі необхідна низка фундаментальних мережевих сервісів та протоколів підтримки. У контексті спроектованої мережі ключову роль відіграють як серверні служби, так і протоколи, що забезпечують її функціонування та безпеку.

У спроектованій мережі передбачено виділену серверну ферму, що надає ключові бізнес-сервіси для організації. До них належать:

- Web-Server.
- Database Server.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

- File Server.
- Backup Server.

Web-Server надає доступ до внутрішніх корпоративних порталів, веб-додатків та систем документообігу. Database Server централізовано зберігає та обробляє дані, що використовуються різними корпоративними системами (наприклад, CRM, бухгалтерське ПЗ). File Server слугує централізованим сховищем для робочих файлів та документів, забезпечуючи спільний доступ та версійність. Backup Server відповідає за регулярне резервне копіювання критично важливих даних з інших серверів та робочих станцій для забезпечення їх відновлення у випадку збоїв чи атак.

Крім серверних служб, функціонування та безпека мережі підтримується низкою протоколів та технологій, налаштованих на активному обладнанні. Базові сервіси (DHCP та DNS) забезпечують автоматичну IP-адресацію та перетворення доменних імен. Протоколи надійності (RSTP, VRRP) гарантують безперебійність роботи мережі шляхом запобігання петлям та резервування шлюзів. Протокол динамічної маршрутизації (OSPF) слугує для автоматизації процесу обміну маршрутною інформацією, забезпечуючи оптимальну доставку трафіку. Безпека кінцевих точок (система автентифікації) виконує функції безпечного управління обладнанням використовується автентифікація через локальну базу даних користувачів за протоколом SSH. Списки контролю доступу (ACL) є ключовим інструментом реалізації політики безпеки, фільтруючи трафік між різними VLAN [12].

1.6 Постановка технічного завдання

Метою кваліфікаційної роботи є проектування комплексної мережевої інфраструктури, що відповідає високим вимогам до продуктивності, надійності, безпеки та керованості.

Основні вимоги до проєктованої мережі можна згрупувати за наступними напрямками:

У спроектованій мережі передбачено виділену серверну ферму, що надає ключові бізнес-сервіси для організації. До них належать:

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				22
Змн.	Арк.	№ докум.	Підпис	Дата		

– Проєктування мережі на основі трирівневої ієрархічної моделі. Забезпечення логічної сегментації мережі завдяки технології VLAN для ізоляції трафіку різних підрозділів. Архітектура повинна мати потенціал для подальшого розширення без кардинальної перебудови

– Забезпечення належної пропускної здатності для підключення кінцевих робочих станцій. Для магістральних каналів, що з'єднують ключові комутатори, задіяти технології агрегації каналів для збільшення пропускної здатності та проведення балансування навантаження мережі

– Реалізація резервування всіх критично важливих компонентів мережі. Використання протоколу RSTP для запобігання петлям комутації та забезпечення швидкої конвергенції мережі. Забезпечення відмовостійкого підключення до мережі Інтернет через двох незалежних провайдерів.

– Розробка та впровадження політики безпеки за допомогою списків контролю доступу (ACL) для контролю трафіку між різними VLAN. Проведення дій щодо ізоляції гостьового Wi-Fi трафік від корпоративних ресурсів. Забезпечення безпечного віддаленого управління всім активним мережевим обладнанням виключно за протоколом SSH.

– Реалізація централізованого надання IP-адрес за допомогою DHCP-сервера. Забезпечення стабільної роботи сервісу DNS. Створення окремої VLAN для управління мережевими пристроями.

Виконання даного технічного завдання дозволить створити сучасну, ефективну та захищену мережеву інфраструктуру.

Висновок до 1-го розділу:

У першому розділі було викладено основи комутованих локальних мереж: принципи роботи комутаторів та VLAN. Розглянуто забезпечення продуктивності (Ethernet, агрегація, QoS) та надійності (надлишковість, STP/RSTP, VRRP). Окрему увагу приділено безпеці на каналному рівні та безпечному управлінню. Ці відомості створюють підґрунтя для проєктування сучасних захищених та продуктивних мереж.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

РОЗДІЛ 2. ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ ЛОКАЛЬНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

2.1 Розробка топології локальної мережі

Для цілей даної дипломної роботи була розглянута невелика ІТ-компанія, що займається розробкою програмного забезпечення. Компанія розміщена в офісному приміщенні, яке включає кілька кабінетів різного розміру. Штат компанії складається з працівників різних підрозділів, що вимагає логічної ізоляції трафіку та застосування специфічних політик безпеки для кожного відділу. До основних підрозділів організації відносяться:

- ІТ-відділ розробки (IT DEV)
- ІТ-відділ підтримки (IT SUPPORT)
- Серверна ферма (SERVERS)
- Бухгалтерія (ACCOUNTING)
- Юридичний відділ
- Адміністрація та заступники
- Гостьовий підрозділ

ІТ-відділ розробки (IT DEV) відповідає за розробку програмного забезпечення. Потребує високої пропускнуєї здатності, низької затримки та доступу до тестових середовищ.

ІТ-відділ підтримки (IT SUPPORT) відповідає за підтримку мережевої інфраструктури, серверів, робочих станцій. Потребує високого рівня доступу до мережевого обладнання та серверної ферми.

Бухгалтерія працює з фінансовою інформацією, вимагає високого рівня безпеки та обмеженого доступу до специфічних ресурсів.

Юридичний відділ: Працює з конфіденційною юридичною інформацією, також вимагає високого рівня безпеки та ізоляції трафіку.

Щодо адміністрації та заступників, то керівний склад може мати специфічні вимоги до доступу та пропускнуєї здатності, а також вимагає високого рівня безпеки.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Гостьовий підрозділ призначений для відвідувачів, має обмежений доступ до внутрішніх ресурсів компанії та доступ лише до мережі Інтернет. Повинен бути повністю ізольований від внутрішньої корпоративної мережі.

Приймальня може включати робоче місце секретаря та зону очікування для відвідувачів.

Додатково розглянемо і інші вимоги до створенної мережі:

- Висока доступність та надійність мережевої інфраструктури.
- Висока швидкість та продуктивність для підтримки роботи додатків розробки та передачі великих обсягів даних.
- Забезпечення безпеки на всіх рівнях, особливо на каналному рівні.
- Можливість легкого масштабування мережі при зростанні штату співробітників.
- Централізоване управління та моніторинг мережевого обладнання.

Зважаючи на сформульовані вимоги, зокрема щодо масштабованості, надійності та керованості, для проєктування мережі ІТ-компанії було обрано трирівневу ієрархічну модель. Таке рішення забезпечує чіткий розподіл функціональних обов'язків між мережевими пристроями, дозволяє ефективно впроваджувати сегментацію трафіку за допомогою технології VLAN та застосовувати відповідні політики безпеки. Крім того, обрана модель надає необхідний рівень надлишковості ключових компонентів мережі.

Фізична структура мережі реалізована за принципом "розширеної зірки". У такій топології кінцеві пристрої користувачів підключаються до комутаторів рівня доступу, які, у свою чергу, агрегуються на маршрутизаторах рівня ядра/розподілу, що виконують центральні функції комутації та маршрутизації.

Логічна топологія мережі базується на широкому використанні віртуальних локальних мереж (VLAN), що дозволяє здійснити сегментацію трафіку відповідно до функціональних підрозділів організації. Кожен підрозділ виділяється в окрему, логічно ізольовану VLAN. Маршрутизацію між цими VLAN забезпечують маршрутизатори рівня ядра/розподілу.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

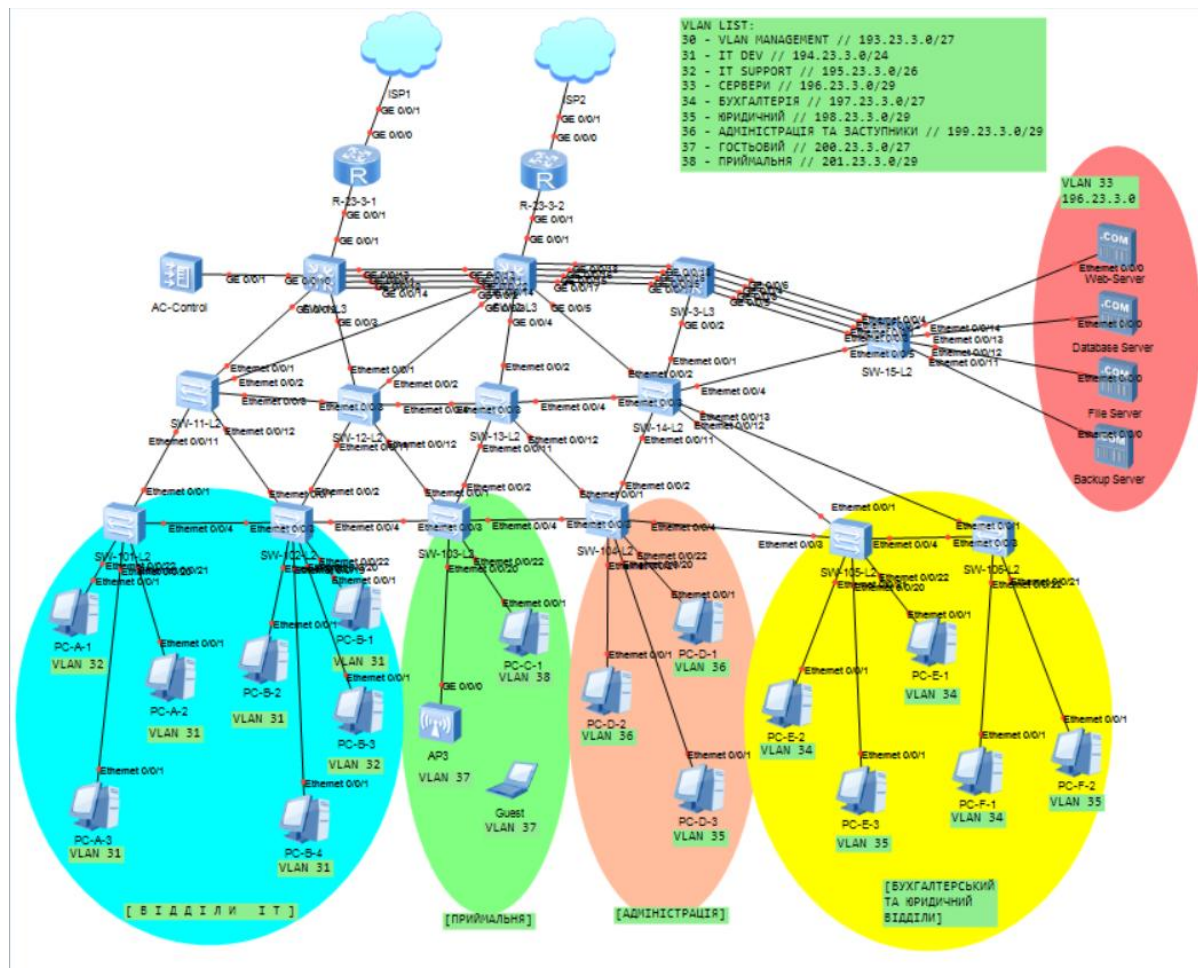


Рисунок 2.1 – Загальний вигляд топології мережі

Важливим елементом інфраструктури є серверна ферма, яка розміщується у виділеній VLAN 33. Окрім того, для управління всім активним мережевим обладнанням використовується окрема Management VLAN 30, доступ до якої суворо обмежується.

На основі детального аналізу поточної чисельності співробітників у кожному підрозділі та врахування перспектив зростання компанії було проведено розрахунок необхідного адресного простору та визначено відповідні VLAN для кожного сегменту. Дані цих розрахунків наведені у таблицях 2.1 та 2.2.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				26
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 2.1 – Поточна та прогнозована кількість клієнтів VLAN

Назва підрозділу	Поточна кількість клієнтів	Відсоток резерву (%)	Загальна сума можливих клієнтів (з урахуванням резерву)
ІТ-відділ розробки (IT DEV)	30	~233	100
ІТ-відділ підтримки (IT SUPPORT)	15	~166	40
Серверна ферма (СЕРВЕРИ)	4 (сервери) + 6 (запас)	150	10
Бухгалтерія	10	50	15
Юридичний відділ	8	50	12
Адміністрація та заступники	5	100	10
Гостьовий підрозділ	20 (оцінка пікового)	100	40
Приймальня	5	100	10
Management VLAN	~15 (пристрої) + 10 (запас)	~66	25
ВСЬОГО			~256

Таблиця 2.2 – Призначення VLAN та оцінка розмірів підмереж

Назва підрозділу	VLAN ID	Кількість користувачів (загальна з резервом)	Необхідний розмір підмережі (мін. кількість IP)	Обраний префікс IPv4	Максимальна кількість IP-адрес в підмережі
Management VLAN	30	25	27	/27	30
ІТ-відділ розробки (IT DEV)	31	100	102	/24	254
ІТ-відділ підтримки (IT SUPPORT)	32	40	42	/26	62

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Серверна ферма (СЕРВЕРИ)	33	10	12	/28	14
Бухгалтерія	34	15	17	/27	30
Юридичний відділ	35	12	14	/28	14
Адміністрація та заступники	36	10	12	/28	14
Гостьовий підрозділ	37	40	42	/26	62
Приймальня	38	10	12	/28	14

Розглянемо детальніше функції кожного рівня ієрархічної моделі на основі розробленої топології.

Рівень доступу (Access Layer) є першою точкою підключення до мережі для кінцевих пристроїв. У проєктованій мережі він представлений комутаторами L2 (на схемі позначені як SW-11-L2, SW-12-L2, SW-101-L2 і т.д.), які фізично розташовані в кабінетах або поблизу груп пристроїв. До цих комутаторів підключаються робочі станції користувачів (ПК), віртуальні ПК (VPCS), бездротові точки доступу (AP1), а також сервери у відповідній VLAN. Основні функції, що реалізуються на цьому рівні, включають комутацію на другому рівні (Layer 2), призначення портів доступу до відповідних VLAN, підтримку транкінгових з'єднань за стандартом 802.1Q на аплінк-портах до рівня розподілу, а також реалізацію початкових політик безпеки (наприклад, Port Security)

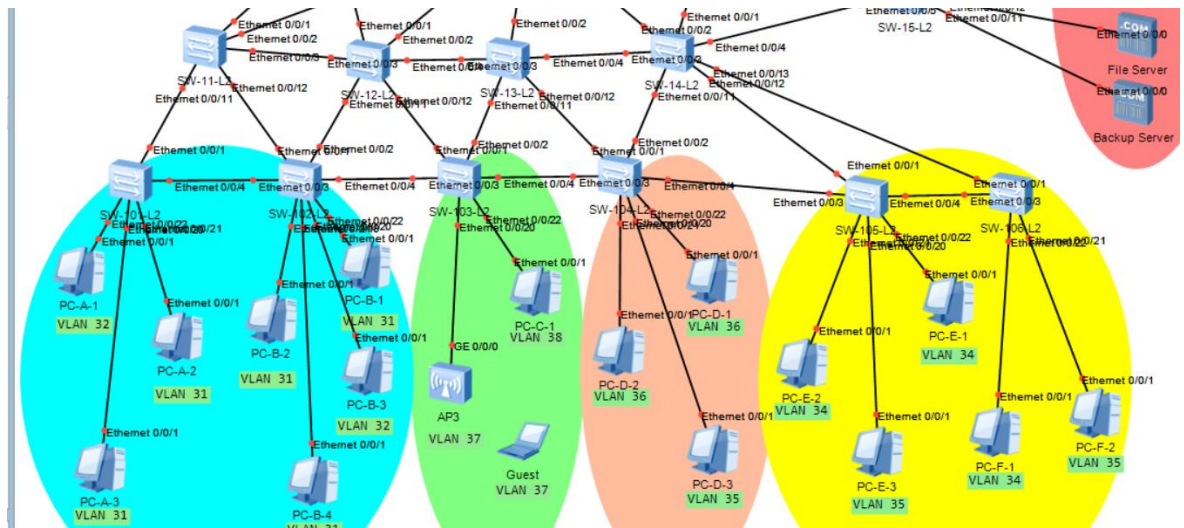


Рисунок 2.2 - Приклад сегменту рівня доступу

Рівень розподілу (Distribution Layer) слугує проміжною ланкою, що агрегує трафік з рівня доступу та застосовує політики. У даній топології цей рівень представлений потужними L3-комутаторами (SW-1-L3, SW-2-L3, SW-3-L3). Вони агрегують з'єднання від комутаторів рівня доступу та виконують ключові функції: агрегацію трафіку, маршрутизацію між різними VLAN (Inter-VLAN routing), застосування списків контролю доступу (ACL) для фільтрації трафіку між підрозділами та підтримку протоколів надійності, таких як RSTP/MSTP для запобігання петлям. Також на цьому рівні реалізується агрегація каналів (Eth-Trunk) для підвищення пропускної здатності та надійності з'єднань як до рівня доступу, так і до рівня ядра.

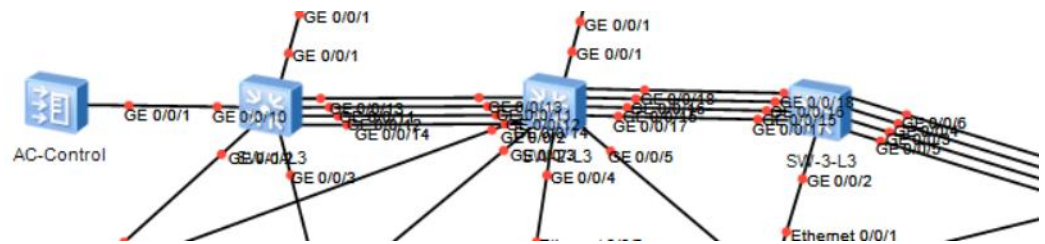


Рисунок 2.3 - Приклад сегменту рівня розподілу

Рівень ядра (Core Layer) є центральною високошвидкісною магістраллю мережі, що забезпечує зв'язок з зовнішніми мережами та об'єднує рівень розподілу. У цьому проєкті він представлений маршрутизаторами R-23-3-1 та R-23-3-2. Основні функції цього рівня — це максимально швидке пересилання трафіку, зв'язок з Інтернет-провайдерами (WAN), а також реалізація протоколів резервування шлюзів, таких як VRRP. Саме тут працюють протоколи динамічної маршрутизації, зокрема OSPF, для обміну маршрутною інформацією з рівнем розподілу та провайдерами.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

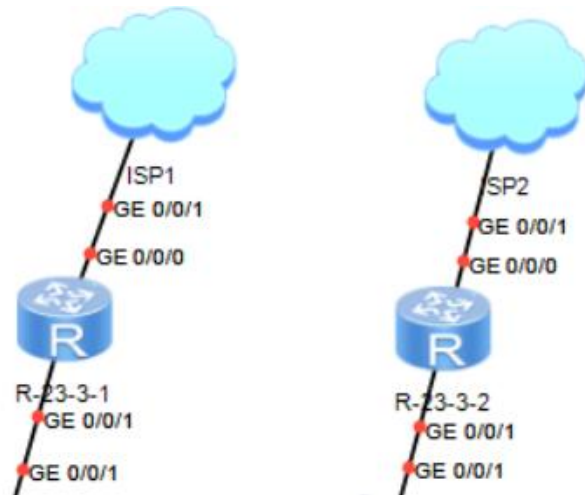


Рисунок 2.4 - Приклад сегменту рівня ядра

Надійна та високошвидкісна схема підключення до мережі Інтернет є критично важливою для сучасної ІТ-компанії. Існує кілька типових варіантів реалізації такого підключення, кожен з яких має свої переваги та недоліки.

Найпростішим варіантом є схема "Один провайдер – Один маршрутизатор". Її головними перевагами є простота реалізації та низька вартість. Однак такий підхід є найменш надійним, оскільки створює єдину точку відмови: вихід з ладу маршрутизатора або каналу провайдера призведе до повної втрати зв'язку. Крім того, пропускна здатність обмежується одним каналом.



Рисунок 2.5 – Приклад схеми «Один провайдер – Один маршрутизатор»

Схема "Два провайдери – Один маршрутизатор" забезпечує резервування на рівні каналів зв'язку. До переваг цього підходу можна віднести підвищення надійності, оскільки при відмові одного каналу трафік автоматично перемикається на інший, а також з'являється можливість балансування навантаження між двома провайдерами. Проте недоліком залишається наявність єдиної точки відмови у вигляді самого маршрутизатора.

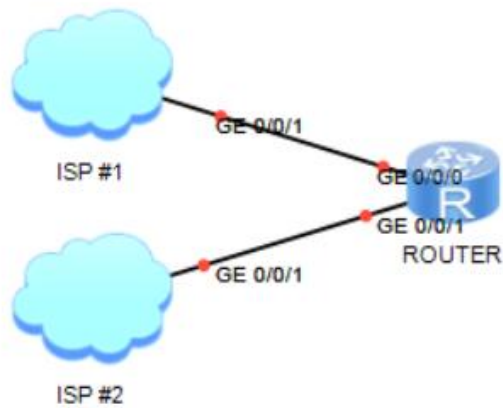


Рисунок 2.6 – Приклад схеми «Два провайдери – Один маршрутизатор»

Варіант "Один провайдер – Два маршрутизатори – Один комутатор" забезпечує резервування на рівні мережевого обладнання. Перевагою такої схеми є резервування пристроїв ядра, що дозволяє використовувати протоколи резервування першого хопу (наприклад, VRRP). Водночас, недоліком є наявність єдиної точки відмови на рівні каналу провайдера та комутатора, до якого підключені маршрутизатори.

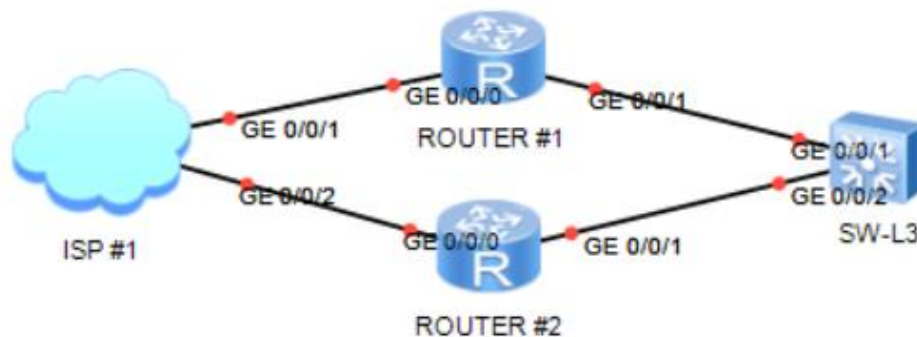


Рисунок 2.7 – Приклад схеми «Один провайдер – Два маршрутизатори – Один комутатор»

Для даного проєкту було обрано найбільш надійну та продуктивну схему "Два провайдери – Два маршрутизатори – комутатор", яка зображена на відповідній топології.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				31
Змн.	Арк.	№ докум.	Підпис	Дата		

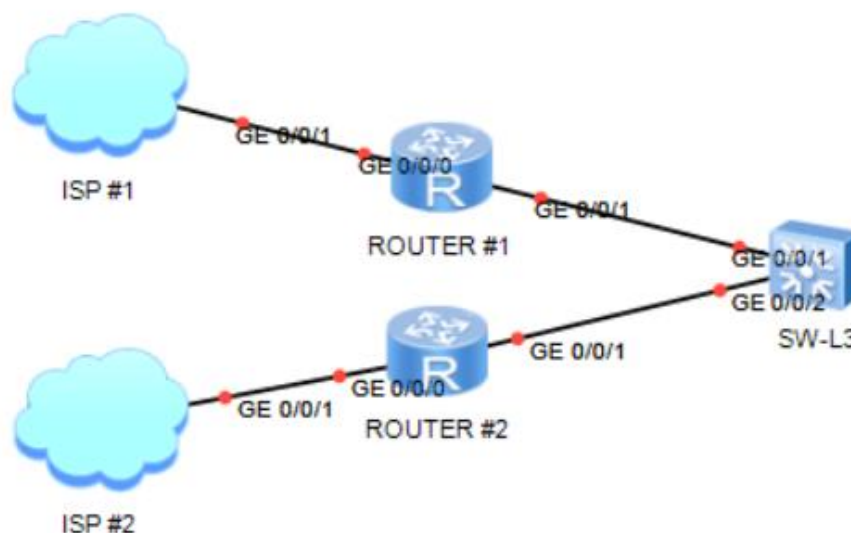


Рисунок 2.8 – Приклад схеми «Два провайдери- два маршрутизатори – комутатор»

До переваг цього варіанту належать найвищий рівень надійності та відмовостійкості завдяки повному резервуванню як каналів провайдерів, так і маршрутизаторів рівня ядра. Такий підхід надає можливість гнучкого балансування навантаження між двома провайдерами та двома маршрутизаторами, а також забезпечує високу сукупну пропускну здатність. Єдиним суттєвим недоліком є вища вартість реалізації порівняно з простішими схемами.

Для ІТ-компанії, де безперебійний доступ до Інтернету та висока швидкість є критично важливими для бізнес-процесів (розробка, комунікації, доступ до хмарних сервісів), схема з двома провайдерами та двома маршрутизаторами є найбільш оптимальною. Вона забезпечує максимальний рівень надійності та продуктивності за рахунок надлишковості на всіх ключових елементах підключення до глобальної мережі. Використання агрегації каналів (Eth-Trunk/LACP) між маршрутизаторами та комутаторами, а також між комутаторами та провайдерами додатково підвищує пропускну здатність та стійкість до відмов.

Для задоволення вимог до високої пропускну здатності на магістральних ділянках, що з'єднують ключові комутатори, передбачено використання технології агрегації каналів (Eth-Trunk). Це дозволяє об'єднати кілька фізичних ліній в один

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

логічний канал, збільшуючи загальну пропускну здатність та забезпечуючи відмовостійкість з'єднань.

2.2 Розробка схеми адресації мережі

Розробка схеми IP-адресації є критично важливим етапом проектування мережі, що забезпечує унікальність адрес, ефективне використання адресного простору та спрощує маршрутизацію. В даному проекті використовується приватний адресний простір IPv4, що базується на діапазонах 193.23.3.xxx - 204.23.3.xxx.

Схема адресації розробляється для всіх активних пристроїв (маршрутизаторів, комутаторів, серверів, робочих станцій) та мережевих сегментів (VLAN).

Таблиця 2.3 – Загальна схема IP-адресації мережі

Мережа/Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска	Префікс
Management VLAN (VLAN 30)		193.23.3.0	255.255.255.224	/27
	Шлюз за замовчуванням (VRRP VIP)	193.23.3.1	255.255.255.224	/27
R-23-3-1	VLAN 30 Interface	193.23.3.2	255.255.255.224	/27
R-23-3-2	VLAN 30 Interface	193.23.3.3	255.255.255.224	/27
... (інші пристрої у Management VLAN)	VLAN 30 Interface	193.23.3.4-193.23.3.30	255.255.255.224	/27
ІТ-відділ розробки (VLAN 31)		194.23.3.0	255.255.255.0	/24
	Шлюз за замовчуванням (VRRP VIP)	194.23.3.1	255.255.255.0	/24
R-23-3-1	VLAN 31 Interface	194.23.3.2	255.255.255.0	/24
R-23-3-2	VLAN 31 Interface	194.23.3.3	255.255.255.0	/24
PC-A-1, PC-B-1, ... (IT DEV)	Мережний адаптер	194.23.3.10-194.23.3.109	255.255.255.0	/24

Продовження таблиці 2.3

ІТ-відділ підтримки (VLAN 32)		195.23.3.0	255.255.255.192	/26
	Шлюз за замовчуванням (VRRP VIP)	195.23.3.1	255.255.255.192	/26
R-23-3-1	VLAN 32 Interface	195.23.3.2	255.255.255.192	/26
R-23-3-2	VLAN 32 Interface	195.23.3.3	255.255.255.192	/26
PC-B-1, PC-B-3, ... (IT SUPPORT)	Мережний адаптер	195.23.3.10-195.23.3.50	255.255.255.192	/26
Серверна ферма (VLAN 33)		196.23.3.0	255.255.255.240	/28
	Шлюз за замовчуванням (VRRP VIP)	196.23.3.1	255.255.255.240	/28
R-23-3-1	VLAN 33 Interface	196.23.3.2	255.255.255.240	/28
R-23-3-2	VLAN 33 Interface	196.23.3.3	255.255.255.240	/28
Web-Server	Мережний адаптер	196.23.3.10	255.255.255.240	/28
Database Server	Мережний адаптер	196.23.3.11	255.255.255.240	/28
File Server	Мережний адаптер	196.23.3.12	255.255.255.240	/28
Backup Server	Мережний адаптер	196.23.3.13	255.255.255.240	/28
Бухгалтерія (VLAN 34)		197.23.3.0	255.255.255.224	/27
	Шлюз за замовчуванням (VRRP VIP)	197.23.3.1	255.255.255.224	/27
R-23-3-1	VLAN 34 Interface	197.23.3.2	255.255.255.224	/27
R-23-3-2	VLAN 34 Interface	197.23.3.3	255.255.255.224	/27
PC-C-1, PC-D-1, ... (Бух.)	Мережний адаптер	197.23.3.10-197.23.3.24	255.255.255.224	/27
Юридичний відділ (VLAN 35)		198.23.3.0	255.255.255.240	/28
	Шлюз за замовчуванням (VRRP VIP)	198.23.3.1	255.255.255.240	/28
R-23-3-1	VLAN 35 Interface	198.23.3.2	255.255.255.240	/28
R-23-3-2	VLAN 35 Interface	198.23.3.3	255.255.255.240	/28

Продовження таблиці 2.3

PC-B-2, PC-E-1, ... (Юр.)	Мережний адаптер	198.23.3.10-198.23.3.21	255.255.255.240	/28
Адміністрація та заступники (VLAN 36)		199.23.3.0	255.255.255.240	/28
	Шлюз за замовчуванням (VRRP VIP)	199.23.3.1	255.255.255.240	/28
R-23-3-1	VLAN 36 Interface	199.23.3.2	255.255.255.240	/28
R-23-3-2	VLAN 36 Interface	199.23.3.3	255.255.255.240	/28
PC-F-1, PC-F-2, ... (Адм.)	Мережний адаптер	199.23.3.10-199.23.3.19	255.255.255.240	/28
Гостьовий під- розділ (VLAN 37)		200.23.3.0	255.255.255.192	/26
	Шлюз за замовчуванням (VRRP VIP)	200.23.3.1	255.255.255.192	/26
R-23-3-1	VLAN 37 Interface	200.23.3.2	255.255.255.192	/26
R-23-3-2	VLAN 37 Interface	200.23.3.3	255.255.255.192	/26
Гостьові ПК, AP1	Мережний адаптер	200.23.3.10-200.23.3.50	255.255.255.192	/26
Приймальня (VLAN 38)		201.23.3.0	255.255.255.240	/28
	Шлюз за замовчуванням (VRRP VIP)	201.23.3.1	255.255.255.240	/28
R-23-3-1	VLAN 38 Interface	201.23.3.2	255.255.255.240	/28
R-23-3-2	VLAN 38 Interface	201.23.3.3	255.255.255.240	/28
PC-C-2, ... (Приймальня)	Мережний адаптер	201.23.3.10-201.23.3.19	255.255.255.240	/28
Підмережа ISP1	-	204.23.3.0	255.255.255.252	/29
R-23-3-1	GE0/0/0	204.23.3.1	255.255.255.252	/29
ISP1	GE0/0/0	-	-	-
Підмережа ISP2	-	204.23.3.4	255.255.255.252	/29
R-23-3-2	GE0/0/0	204.23.3.5	255.255.255.252	/29
ISP2	GE0/0/0	-	-	-

Для кожної визначеної підмережі складається детальна таблиця, що включає адресу мережі, маску, інвертовану маску, діапазон доступних для хостів адрес, широкомовну адресу та адресу шлюзу за замовчуванням.

Вся інформація щодо адресації кожної гілки VLAN зображено у таблицях 2.4 – 2.12. Для кожної визначеної підмережі складено окрему таблицю, що включає адресу мережі, маску, інвертовану маску, діапазон доступних для хостів адрес, широкомовну адресу та адресу шлюзу за замовчуванням. Це дозволяє точно визначити параметри для налаштування мережевих інтерфейсів та DHCP-сервісів.

Таблиця 2.4 – Деталізація IP-адресації VLAN 30

Призначення	IP-адреси
Адреса мережі	193.23.3.0
Маска мережі	255.255.255.224
Префікс	/27
Інвертована маска	0.0.0.31
Мінімальна адреса	193.23.3.1
Максимальна адреса	193.23.3.30
Широкомовна адреса	193.23.3.31
Шлюз по замовчуванню	193.23.3.1
Діапазон адрес пристроїв	193.23.3.2 – 193.23.3.30

Таблиця 2.5 – Деталізація IP-адресації VLAN 31

Призначення	IP-адреси
Адреса мережі	194.23.3.0
Маска мережі	255.255.255.0
Префікс	/24
Інвертована маска	0.0.0.255
Мінімальна адреса	194.23.3.1
Максимальна адреса	194.23.3.254
Широкомовна адреса	194.23.3.255
Шлюз по замовчуванню	194.23.3.1

Діапазон адрес DHCP	194.23.3.10 – 194.23.3.109
Діапазон статичних IP	194.23.3.200 – 194.23.3.210

Таблиця 2.6 – Деталізація IP-адресації VLAN 32

Призначення	IP-адреси
Адреса мережі	195.23.3.0
Маска мережі	255.255.255.192
Префікс	/26
Інвертована маска	0.0.0.63
Мінімальна адреса	195.23.3.1
Максимальна адреса	195.23.3.62
Широкомовна адреса	195.23.3.63
Шлюз по замовчуванню	195.23.3.1
Діапазон адрес DHCP	195.23.3.10 – 195.23.3.50

Таблиця 2.7 – Деталізація IP-адресації VLAN 33

Призначення	IP-адреси
Адреса мережі	196.23.3.0
Маска мережі	255.255.255.240
Префікс	/28
Інвертована маска	0.0.0.15
Мінімальна адреса	196.23.3.1
Максимальна адреса	196.23.3.14
Широкомовна адреса	196.23.3.15
Шлюз по замовчуванню	196.23.3.1
Діапазон адрес серверів	196.23.3.10 – 196.23.3.13

Таблиця 2.8 – Деталізація IP-адресації VLAN 34

Призначення	IP-адреси
Адреса мережі	197.23.3.0
Маска мережі	255.255.255.224

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Префікс	/27
Інвертована маска	0.0.0.31
Мінімальна адреса	197.23.3.1
Максимальна адреса	197.23.3.30
Широкомовна адреса	197.23.3.31
Шлюз по замовчуванню	197.23.3.1
Діапазон адрес DHCP	197.23.3.10 – 197.23.3.24

Таблиця 2.9 – Деталізація IP-адресації VLAN 35

Призначення	IP-адреси
Адреса мережі	198.23.3.0
Маска мережі	255.255.255.240
Префікс	/28
Інвертована маска	0.0.0.15
Мінімальна адреса	198.23.3.1
Максимальна адреса	198.23.3.14
Широкомовна адреса	198.23.3.15
Шлюз по замовчуванню	198.23.3.1
Діапазон адрес DHCP	198.23.3.10 - 198.23.3.21

Таблиця 2.10 – Деталізація IP-адресації VLAN 36

Призначення	IP-адреси
Адреса мережі	199.23.3.0
Маска мережі	255.255.255.240
Префікс	/28
Інвертована маска	0.0.0.15
Мінімальна адреса	199.23.3.1
Максимальна адреса	199.23.3.14
Широкомовна адреса	199.23.3.15
Шлюз по замовчуванню	199.23.3.1

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				38
Змн.	Арк.	№ докум.	Підпис	Дата		

Діапазон адрес DHCP	199.23.3.10 - 199.23.3.19
---------------------	---------------------------

Таблиця 2.11 – Деталізація IP-адресації VLAN 37

Призначення	IP-адреси
Адреса мережі	200.23.3.0
Маска мережі	255.255.255.192
Префікс	/26
Інвертована маска	0.0.0.63
Мінімальна адреса	200.23.3.1
Максимальна адреса	200.23.3.62
Широкомовна адреса	200.23.3.63
Шлюз по замовчуванню	200.23.3.1
Діапазон адрес DHCP	200.23.3.10 - 200.23.3.50

Таблиця 2.12 – Деталізація IP-адресації VLAN 38

Призначення	IP-адреси
Адреса мережі	201.23.3.0
Маска мережі	255.255.255.240
Префікс	/28
Інвертована маска	0.0.0.15
Мінімальна адреса	201.23.3.1
Максимальна адреса	201.23.3.14
Широкомовна адреса	201.23.3.15
Шлюз по замовчуванню	201.23.3.1
Діапазон адрес DHCP	201.23.3.10 - 201.23.3.19

2.3 Проект базових сервісів мережі

Для забезпечення повноцінного функціонування, управління та підтримки користувачів у проєктованій мережі передбачається використання базових мережевих сервісів. Згідно з топологією, в ІТ-відділі розміщено серверну ферму, яка включає кілька ключових серверів:

- Web-Server.
- Database Server.
- File Server.
- Backup Server.

Web-Server призначений для розміщення внутрішніх вебдодатків компанії, таких як корпоративний портал, системи управління проєктами та внутрішня документація. Доступ до нього може надаватися співробітникам компанії згідно з політиками безпеки.

Database Server використовується для зберігання та управління базами даних, необхідних для роботи внутрішніх додатків, систем обліку, CRM тощо. Він є критично важливим ресурсом, що вимагає високого рівня захисту та надійності.

File Server надає централізоване сховище файлів для спільного доступу співробітників до документів, проєктних матеріалів та інших даних. Це дозволяє організувати структуру файлів, керувати правами доступу та забезпечувати резервне копіювання.

Backup Server призначений для створення та зберігання резервних копій даних з інших серверів та, можливо, критично важливих робочих станцій. Він є ключовим елементом стратегії відновлення після збоїв та забезпечення безперервності бізнесу.

Окрім серверів у фермі, для функціонування мережі також необхідні інші служби:

- DHCP-сервер.
- DNS-сервер.
- Syslog-сервер.
- RADIUS-сервер

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

DHCP-сервер необхідний для автоматичного призначення IP-адрес кінцевим пристроям у VLAN користувачів різних підрозділів. Налаштування DHCP будуть налаштовані на одному маршрутизаторі для кожної підмережі. VLAN корпоративної мережі отримуватимуть DHCP від R-23-3-1

DNS-сервер забезпечує перетворення доменних імен у IP-адреси. Може бути внутрішнім сервером компанії або використовуватись зовнішній публічний DNS (наприклад, 8.8.8.8).

Syslog-сервер слугує для централізованого збору логів з мережевих пристроїв, що є важливим для моніторингу, пошуку несправностей та аналізу подій безпеки.

RADIUS-сервер є обов'язковим, у випадку реалізації автентифікації на портах доступу за протоколом 802.1X, оскільки він виконує роль сервера автентифікації.

Важливо зазначити, що в рамках роботи основний акцент робиться на проектуванні мережевої інфраструктури та її безпеки на каналному та мережевому рівнях. Детальне налаштування та конфігурація операційних систем та специфічних ролей серверів (веб, база даних тощо) виходить за рамки даного проєкту, але їх наявність, базові налаштування та правильне розміщення в мережі є необхідною умовою для функціонування організації. Налаштуванням та обслуговуванням цих серверів буде займатися персонал відділу IT-підтримки.

2.4 Розробка підсистеми захисту мережі

Підсистема захисту спроектованої локальної мережі є багатокомпонентною та спрямована на забезпечення безпеки на різних рівнях. Вона включає логічну сегментацію трафіку, захист від петель комутації, резервування ключових вузлів, контроль доступу та безпечне управління мережевими обладнаннями.

Фундаментом підсистеми захисту є використання технології віртуальних локальних мереж (VLAN). Застосування VLAN дозволяє логічно розділити фізичну мережу на декілька ізольованих широкомовних доменів. У даному проєкті кож-

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

ному функціональному підрозділу організації, а також для специфічних потреб, таких як управління обладнанням (VLAN 30 Management) та розміщення серверів (VLAN 33 Servers), призначено окрему VLAN. Це забезпечує ізоляцію трафіку між підрозділами, обмежуючи потенційну зону ураження у випадку інцидентів безпеки та зменшуючи обсяг непотрібного широкомовного трафіку. Взаємодія між різними VLAN контролюється на рівні маршрутизації, де можуть бути застосовані списки контролю доступу.

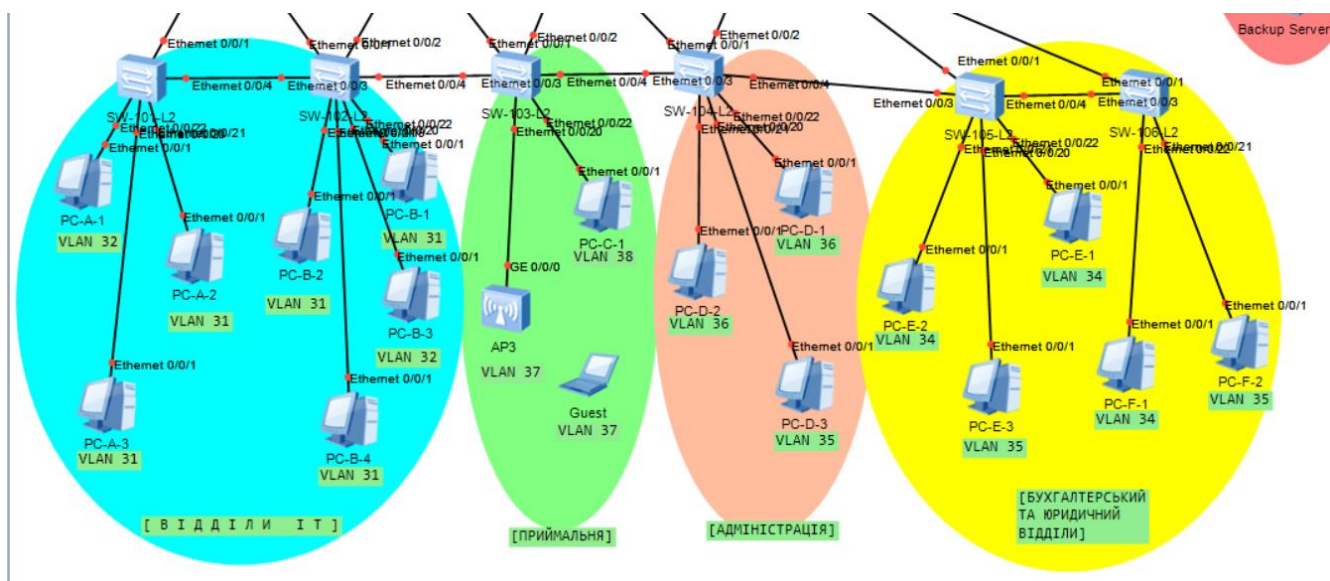


Рисунок 2.9 – Розподіл кінцевих пристроїв між різними відділами (VLAN)

Для забезпечення стабільності роботи мережі на каналному рівні та запобігання утворенню петель комутації, що можуть виникнути при наявності надлишкових фізичних зв'язків між комутаторами, впроваджено протокол Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w). RSTP динамічно визначає топологію мережі без петель, блокуючи надлишкові шляхи, та забезпечує швидку конвергенцію (протягом декількох секунд) у випадку зміни топології, наприклад, при відмові одного з каналів. Всі комутатори в мережі налаштовані на використання RSTP, а на портах, до яких підключені кінцеві пристрої, активовано функцію `stp edged-port enable` для прискорення їх переходу в стан пересилання.

Висока доступність шлюзу за замовчуванням для всіх користувацьких та сервісних VLAN реалізована за допомогою протоколу Virtual Router Redundancy Protocol (VRRP). Маршрутизатори R-23-3-1 та R-23-3-2 налаштовані як учасники VRRP груп для кожного логічного інтерфейсу `Vlanif`, що відповідає певній VLAN.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

Для кожної такої групи визначено унікальну віртуальну IP-адресу, яка використовується кінцевими пристроями як шлюз. Один з маршрутизаторів (R-23-3-1) функціонує як основний (Master) завдяки вищому пріоритету, тоді як інший (R-23-3-2) перебуває в режимі резервного (Backup). У випадку відмови основного маршрутизатора, резервний автоматично перебирає на себе роль активного шлюзу, забезпечуючи безперервність мережевого трафіку.

Для автоматизації процесу призначення IP-конфігурацій кінцевим пристроям та спрощення адміністрування мережі, на маршрутизаторі R-23-3-1 реалізовано функціонал DHCP-сервера. Для кожної VLAN, що потребує динамічної IP-адресації (VLAN 31, 32, 34, 35, 36, 37, 38), створено окремий пул IP-адрес. Ці пули включають діапазон доступних адрес, адресу шлюзу за замовчуванням (що відповідає віртуальній IP-адресі VRRP), адресу DNS-сервера та параметри часу оренди. IP-адреси, зарезервовані для мережевих пристроїв та серверів, виключені з діапазонів DHCP. Для сегментів Management VLAN (VLAN 30) та Server VLAN (VLAN 33) використовується виключно статична IP-адресація. Теоретично, для посилення захисту від неавторизованих DHCP-серверів, на комутаторах рівня доступу рекомендується впровадження DHCP Snooping.

Захист бездротового доступу для гостей користувачів, які підключатимуться через точку доступу AP-Guest забезпечується за допомогою протоколу WPA2-PSK (Wi-Fi Protected Access 2 with Pre-Shared Key). Цей механізм використовує надійний алгоритм шифрування AES для захисту даних, що передаються, та вимагає введення попередньо встановленого спільного ключа для підключення до бездротової мережі. Гостьовий SSID (GuestWiFi-AP4050) налаштовується для роботи у виділеній VLAN 37, що забезпечує ізоляцію гостьового трафіку від основної корпоративної мережі. Хоча стандарт WPA3 пропонує більш сучасні механізми захисту, WPA2-PSK залишається прийнятним рішенням для гостьових мереж за умови використання складного та регулярно змінюваного пароля.

Для ефективного обміну маршрутною інформацією між ключовими маршрутизуючими пристроями мережі (R-23-3-1, R-23-3-2, SW-1-L3, SW-2-L3, SW-3-L3) використовується протокол динамічної маршрутизації OSPF (Open Shortest Path

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

First). Всі ці пристрої налаштовані як члени OSPF процесу 1 в межах єдиної зони (area 0.0.0.0), що спрощує конфігурацію для мережі даного розміру. Кожен маршрутизатор має унікальний Router ID. OSPF автоматично визначає оптимальні шляхи для передачі даних між різними підмережами та забезпечує швидку адаптацію до змін у топології мережі. Внутрішні підмережі, представлені інтерфейсами Vlanif, анонсуються в OSPF, забезпечуючи їх доступність у всій маршрутизованій частині мережі. Для виходу в Інтернет використовуються статичні маршрути за замовчуванням, які можуть редистрибутуватися в OSPF.

```
ospf 1 router-id 1.1.1.1
area 0.0.0.0
network 193.23.3.0 0.0.0.31
network 194.23.3.0 0.0.0.255
network 195.23.3.0 0.0.0.63
network 196.23.3.0 0.0.0.15
network 197.23.3.0 0.0.0.31
network 198.23.3.0 0.0.0.15
network 199.23.3.0 0.0.0.15
network 200.23.3.0 0.0.0.63
network 201.23.3.0 0.0.0.15
#
```

Рисунок 2.10 – Приклад налаштування OSPF на одному із пристроїв мережі

Центральним елементом реалізації гранулярної політики безпеки та контролю доступу між різними VLAN є списки контролю доступу (Access Control Lists, ACL). Вони налаштовуються на маршрутизаторах R-23-3-1 та R-23-3-2, які виконують функцію Inter-VLAN маршрутизації. ACL застосовуються до логічних інтерфейсів Vlanif у напрямку inbound, що дозволяє фільтрувати трафік, який надходить з певної VLAN і прямує до інших сегментів мережі або в Інтернет. У випадку обмежень симулятора eNSP щодо прямого застосування ACL до Vlanif, альтернативним підходом може бути використання зон безпеки (firewall zones) з прив'язкою ACL до політик між зонами.

Реалізація політики доступу за допомогою списків контролю доступу буде поступовою із проведенням тестувань на кожному рівні налаштувань задля забезпечення безпомилкової роботи комп'ютерної мережі.

Трафік з VLAN 31 (IT DEV) та VLAN 32 (IT SUPPORT) має дозвіл на доступ до серверної VLAN 33 та до мережі Інтернет; доступ до інших внутрішніх VLAN

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		44

для них обмежується, за винятком того, що VLAN 32 (IT SUPPORT) має доступ до VLAN 30 (Management) для управління мережевим обладнанням.

Гостьова VLAN 37 повністю ізольована від усіх внутрішніх корпоративних VLAN (30-36, 38), маючи дозвіл на доступ виключно до ресурсів мережі Інтернет.

Для VLAN 34 (Бухгалтерія) та VLAN 35 (Юридичний відділ) дозволено доступ до серверів (VLAN 33) та Інтернету, однак доступ до VLAN Адміністрації (VLAN 36) та VLAN Management (VLAN 30) для них заборонений.

VLAN 36 (Адміністрація) має повний доступ до всіх внутрішніх VLAN та до мережі Інтернет, що відображає потреби керівного складу.

Пристрої з VLAN 38 (Приймальня) можуть взаємодіяти лише з VLAN Адміністрації (VLAN 36), серверною VLAN 33 та мають доступ до Інтернету, тоді як доступ до інших внутрішніх сегментів для них заблокований.

Захист VLAN 30 (Management) забезпечується шляхом явних заборон на доступ до неї з усіх інших VLAN, окрім VLAN 32 (IT SUPPORT).

```
#
acl number 3101
description Controls outbound traffic from IT-DEV (VLAN 31)
rule 10 permit ip source 194.23.3.0 0.0.0.255 destination 196.23.3.0 0.0.0.15
rule 20 deny ip source 194.23.3.0 0.0.0.255 destination 193.23.3.0 0.0.0.31
rule 21 deny ip source 194.23.3.0 0.0.0.255 destination 195.23.3.0 0.0.0.63
rule 22 deny ip source 194.23.3.0 0.0.0.255 destination 197.23.3.0 0.0.0.31
rule 23 deny ip source 194.23.3.0 0.0.0.255 destination 198.23.3.0 0.0.0.15
rule 24 deny ip source 194.23.3.0 0.0.0.255 destination 199.23.3.0 0.0.0.15
rule 25 deny ip source 194.23.3.0 0.0.0.255 destination 200.23.3.0 0.0.0.63
rule 26 deny ip source 194.23.3.0 0.0.0.255 destination 201.23.3.0 0.0.0.15
rule 100 permit ip source 194.23.3.0 0.0.0.255
#
```

Рисунок 2.11 – Приклад налаштування ACL для однієї із VLAN

Нижче приведено таблицю, що візуалізує дозволи та заборони на доступ між різними VLAN згідно з налаштованими ACL. "+" означає дозвіл, "-" означає заборону. "Інтернет" означає доступ до зовнішніх мереж.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		45

Таблиця 2.13 – Таблиця доступу дозволів між різними підмережами VLAN

3 VLAN	30	31	32	33	34	35	36	37	38
30 (MGMT)	+	–	+	+	–	–	+	–	+
31 (IT DEV)	–	+	–	+	–	–	–	–	–
32 (IT SUP)	+	–	+	+	–	–	–	–	–
33 (SRV)	–	+	+	+	+	+	+	–	+
34 (ACC)	–	–	–	+	+	–	–	–	–
35 (LEG)	–	–	–	+	–	+	–	–	–
36 (ADM)	+	+	+	+	+	+	+	+	+
37 (GST)	–	–	–	–	–	–	–	+	–
38 (REC)	–	–	–	+	–	–	+	–	+

Безпека доступу до управління мережевим обладнанням є критично важливою. У спроектованій мережі для віддаленого доступу до командного рядка (CLI) всіх керованих пристроїв – маршрутизаторів, L3-комутаторів, L2-комутаторів та точки доступу AP-Guest – використовується протокол Secure Shell (SSH). Протокол Telnet, через передачу даних, включаючи облікові дані, у відкритому вигляді, вимкнено або не використовується для цілей управління. На кожному пристрої створено локального користувача-адміністратора з високим рівнем привілеїв та захищено надійним паролем. Доступ до ліній віртуального терміналу (VTY) обмежено виключно протоколом SSH, а аутентифікація користувачів здійснюється через механізм AAA з використанням локальної бази даних користувачів. Такий підхід мінімізує ризик несанкціонованого доступу до конфігурації пристроїв та перехоплення адміністративних сесій.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		46

2.5 Вибір програмного забезпечення для реалізації проєкту

Реалізація та тестування спроектованої захищеної корпоративної мережі проводилися з використанням програмного симулятора мереж Huawei eNSP (Enterprise Network Simulation Platform). eNSP є графічним інструментом, розробленим компанією Huawei, що дозволяє створювати віртуальні мережеві топології та симулювати роботу різноманітних мережевих пристроїв цього виробника, таких як маршрутизатори, комутатори, точки доступу та міжмережеві екрани.

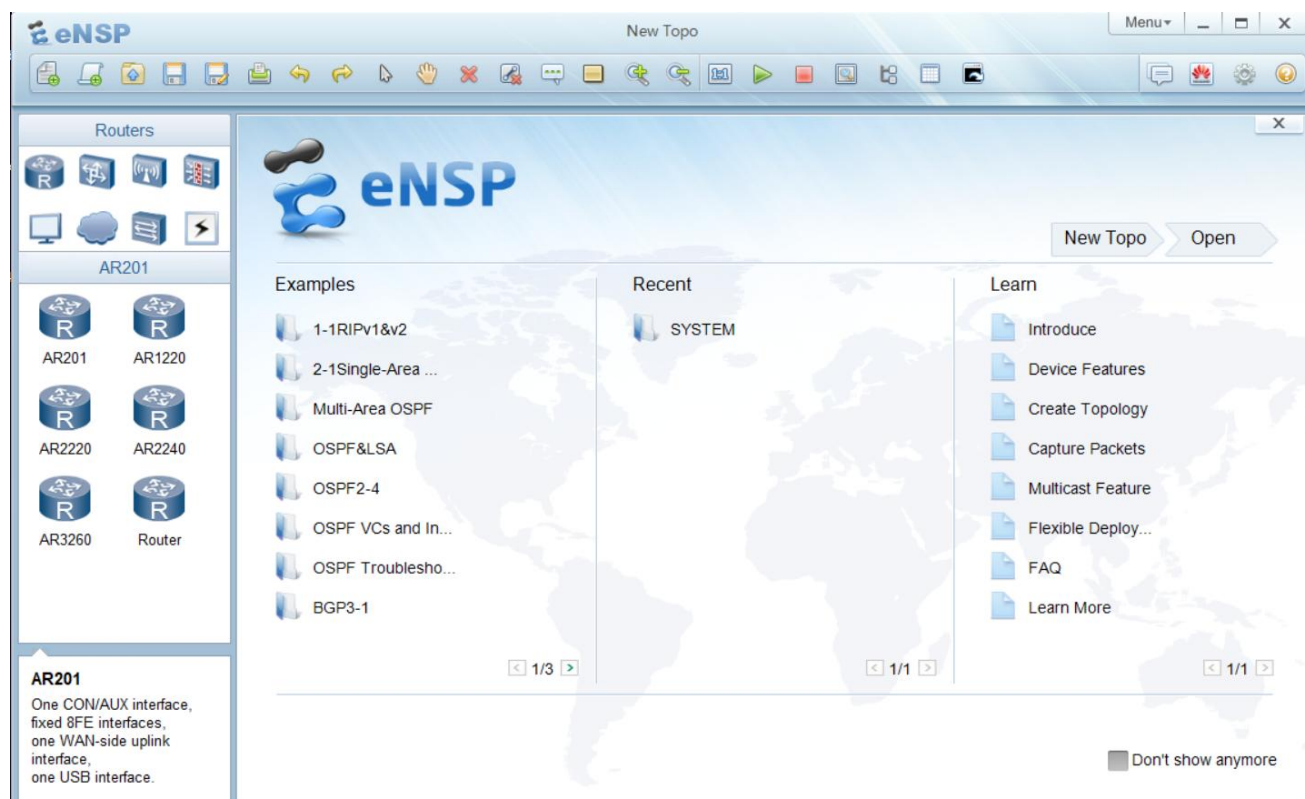


Рисунок 2.12 – Програмне забезпечення eNSP

Використання eNSP для даного проєкту має низку переваг. По-перше, це безкоштовний та широкодоступний інструмент, що робить його зручним для освітніх цілей, навчання та підготовки до професійної сертифікації Huawei. По-друге, інтуїтивно зрозумілий графічний інтерфейс дозволяє легко конструювати складні мережеві топології шляхом простого перетягування віртуальних пристроїв та їх з'єднання. Третьою важливою перевагою є симуляція реального командного рядка (CLI) пристроїв Huawei, що дає можливість практикувати налаштування та відлагодження мережевих протоколів та сервісів в середовищі, наближеному до реаль-

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

ного. Симулятор підтримує значну кількість моделей пристроїв та ключових мережевих технологій, таких як VLAN, STP/RSTP, OSPF, VRRP, ACL, NAT, DHCP та основи WLAN, що є достатнім для реалізації більшості аспектів дипломного проєкту. Крім того, інтеграція з аналізатором трафіку Wireshark надає цінні можливості для дослідження та відлагодження мережевої взаємодії.

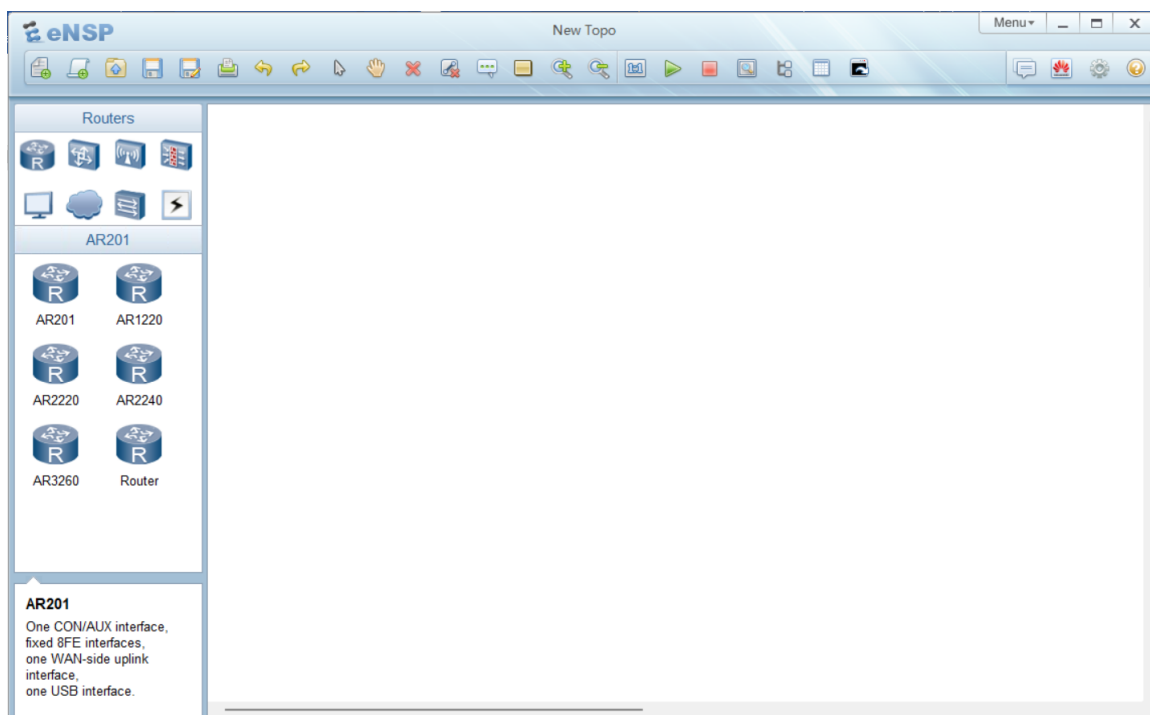


Рисунок 2.13 – Головна оболонка проектування мережі в eNSP

Водночас, важливо усвідомлювати й певні недоліки та обмеження eNSP. Як симулятор, він не завжди може ідеально відтворити всі нюанси роботи реального апаратного забезпечення або найновіших версій операційної системи VRP. Функціонал деяких симульованих пристроїв, особливо точок доступу в автономному режимі або специфічних модулів, може бути обмеженим, а деякі команди CLI можуть бути недоступними або працювати з відхиленнями від поведінки реального обладнання, що було виявлено в ході даної роботи. Симуляція великих та складних топологій також може вимагати значних ресурсів від комп'ютера. Оскільки активна розробка та підтримка eNSP компанією Huawei була значною мірою припинена, нові моделі обладнання та оновлення програмного забезпечення в симуляторі не з'являються.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

Незважаючи на вказані обмеження, eNSP залишається ефективним інструментом для моделювання мережевих сценаріїв, вивчення технологій Huawei та реалізації проєктів рівня даної дипломної роботи. Усвідомлення його сильних та слабких сторін дозволяє коректно інтерпретувати результати симуляції та доповнювати отриманий досвід вивченням офіційної документації та, за можливості, практикою на реальному обладнанні.

Висновок до 2-го розділу:

У другому розділі розроблено проєкт захищеної локальної мережі для ІТ-компанії на основі ієрархічної моделі. Створено детальну фізичну та логічну топології з сегментацією трафіку через VLAN, а також розроблено комплексну схему IP-адресації з резервуванням шлюзів (VRRP) та визначено ключові сервіси (DHCP, DNS).

Основну увагу приділено багаторівневій підсистемі захисту. Описано застосування протоколів RSTP, OSPF та SSH, а центральним елементом стала гранулярна політика доступу між VLAN, реалізована за допомогою ACL та візуалізована у матриці доступу. Також обґрунтовано вибір симулятора Huawei eNSP для побудови комп'ютерної мережі. Розроблені рішення є міцним підґрунтям для подальшого вибору обладнання, його налаштування та тестування.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

РОЗДІЛ 3. ВИБІР ОБЛАДНАННЯ, НАЛАГОДЖЕННЯ ТА ТЕСТУ- ВАННЯ ФУНКЦІОНАЛУ МЕРЕЖІ

3.1 Вибір обладнання

Для реалізації спроектованої мережевої топології в середовищі eNSP було обрано наступні моделі віртуальних пристроїв Huawei, які за своїми характеристиками та підтримуваним функціоналом відповідають вимогам кожного рівня спроектованої мережі.

Для кожного типу обладнання проведемо детальний підбір обладнання, що є оптимальним для подальшої роботи при побудові мережі. На даному етапі розглянемо вибір маршрутизаторів рівня ядра (R-23-3-1, R-23-3-2).

Для виконання ключових функцій маршрутизації між VLAN, забезпечення підключення до двох незалежних Інтернет-провайдерів, реалізації трансляції мережевих адрес (NAT), функціонування DHCP-сервера для клієнтських VLAN, забезпечення надлишковості шлюзів за допомогою VRRP, а також для застосування списків контролю доступу (ACL), було обрано універсальні маршрутизатори серії Huawei AR G3. Конкретна модель в eNSP, наприклад AR2220 або аналогічна, що підтримує необхідний набір команд та функцій, є придатною для цих завдань. Маршрутизатори цієї серії характеризуються достатньою продуктивністю для мережі даного масштабу, підтримують широкий спектр протоколів маршрутизації, включаючи OSPF, необхідні сервіси (DHCP, NAT, VRRP) та гнучкі механізми фільтрації трафіку. Наявність гігабітних Ethernet-портів є важливою для забезпечення високошвидкісних з'єднань з комутаційною інфраструктурою та зовнішніми каналами.



Рисунок 3.1 – Маршрутизатор Huawei AR2220

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 3.1 – Основні характеристики Huawei AR2220

Категорія	Характеристика	Значення
Основні апаратні характеристики	Процесор	4-ядерний, 600 МГц
	Оперативна пам'ять (RAM)	2 ГБ
	Флеш-пам'ять (Flash)	16 МБ (також 2 ГБ Micro SD карта за замовчуванням)
	Слоти розширення	4 x SIC (Smart Interface Card) 2 x WSIC (Wide Smart Interface Card) 1 x DSP (Digital Signal Processor)
Фізичні інтерфейси	Фіксовані WAN-порти	3 x GE (Gigabit Ethernet) • 2 x GE (електричні, RJ45) 1 x GE Combo (може працювати як електричний RJ45 або оптичний SFP)
	Інтерфейси управління	1 x Console/AUX (RJ45) • 2 x USB 2.0
	Підтримувані стандарти та протоколи	Мережеві протоколи (L2/L3) Ethernet: IEEE 802.1Q (VLAN), IEEE 802.1p (QoS), IEEE 802.3 (Ethernet), STP/RSTP/MSTP • Маршрутизація: Static Routes, RIP, OSPF, BGP, IS-IS
	Протоколи безпеки	Контроль доступу: ACL (списки контролю доступу), 802.1x, MAC-аутентифікація, AAA, RADIUS, HWTACACS VPN: IPsec VPN, GRE VPN, L2TP VPN Захист: Вбудований Firewall, захист від ARP-атак, DHCP Snooping, URPF, IP Source Guard
	Управління та моніторинг	CLI (командний рядок), SSH, SNMP (v1/v2c/v3), NTP, NetConf, CWMP, TR-069
Фізичні параметри	Максимальна потужність	150 Вт (блок живлення змінного струму)
	Габарити (В x Ш x Г)	44.5 мм x 442.0 мм x 420.0 мм
	Вага	7 кг

Для агрегації трафіку, що надходить від комутаторів рівня доступу, та участі в процесі динамічної маршрутизації OSPF, було обрано керовані L3-комутатори серії Huawei S5700, наприклад, модель S5700-28P-LI-AC або її аналог, доступний в eNSP. Ці комутатори підтримують розширений набір функцій рівня 2, таких як VLAN, RSTP, агрегація каналів LACP, а також необхідні функції рівня 3, включаючи підтримку інтерфейсів Vlanif, статичну та динамічну маршрутизацію, та можливість застосування ACL. Висока щільність портів Gigabit Ethernet забезпечує достатню кількість підключень.



Рисунок 3.2 – L3-комутатор Huawei S5700

Таблиця 3.2 – Основні характеристики Huawei S5700

Категорія	Характеристика	Значення
Продуктивність	Комутаційна ємність	До 598 Гбіт/с
	Швидкість пересилання пакетів	До 216 млн пакетів/с (Mpps)
	Таблиця MAC-адрес	16 000 - 32 000 записів
	Кількість VLAN	4000
Порти та інтерфейси	Низхідні порти (Downlink)	24 або 48 портів 10/100/1000BASE-T (RJ45) Часто з підтримкою PoE/PoE+
	Висхідні порти (Uplink)	2 або 4 порти GE SFP, або 2/4 порти 10GE SFP+
	Інтерфейси управління	1 x Console (RJ45) 1 x USB
	Стекування (iStack)	Підтримується на більшості моделей, дозволяє об'єднувати до 9 комутаторів в єдиний логічний пристрій
Підтримувані стандарти та протоколи	Рівень 2 (L2)	Стандарти: IEEE 802.1Q (VLAN), 802.1p (QoS), 802.1d (STP), 802.1w (RSTP), 802.1s (MSTP), 802.3ad (LACP) Інше: IGMP Snooping, MLD Snooping
	Рівень 3 (L3)	Статична маршрутизація Динамічна маршрутизація: RIP, OSPF, BGP, IS-IS (підтримується на старших моделях серій EI/HI)
	Протоколи безпеки	Аутентифікація: 802.1x, RADIUS, HWTACACS Захист: Списки контролю доступу (ACL), Port Security, DHCP Snooping, ARP-spoofing protection, захист від DoS-атак
	Управління та моніторинг	CLI (командний рядок), SSH v2, SNMP (v1/v2c/v3), RMON, Telnet
Фізичні параметри	Живлення	Модулі змінного (AC) або постійного (DC) струму, часто з можливістю резервування (RPS або подвійні БЖ)
	Форм-фактор	1U, для монтажу в 19-дюймову стійку

Для підключення кінцевих користувацьких пристроїв (робочих станцій, принтерів), серверів та точки доступу до мережі, а також для забезпечення сегментації трафіку за допомогою VLAN та реалізації базових функцій безпеки на портах, було обрано керовані L2-комутатори. Серед всіх запропонованих варіантів, вибір

зупинився на моделі серії S3700. Ці пристрої забезпечують необхідну кількість портів Gigabit Ethernet, повноцінну підтримку VLAN та RSTP, а також мають можливість налаштування Port Security.

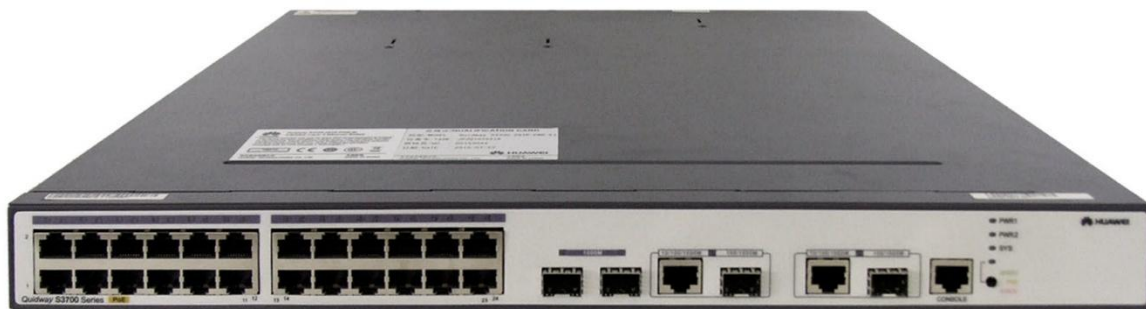


Рисунок 3.3 – L2-комутатор Huawei S3700

Таблиця 3.3 – Основні характеристики Huawei S3700

Категорія	Характеристика	Значення (типові для серії)
Продуктивність	Комутаційна ємність	32 Гбіт/с - 64 Гбіт/с
	Швидкість пересилання пакетів	9.6 млн пакетів/с - 13.2 млн пакетів/с (Mpps)
	Таблиця MAC-адрес	8 000 - 16 000 записів
	Кількість VLAN	до 4 000
Порти та інтерфейси	Низхідні порти (Downlink)	24 або 48 портів 10/100BASE-TX (Fast Ethernet, RJ45) Деякі моделі підтримують PoE/PoE+
	Висхідні порти (Uplink)	2 або 4 порти GE SFP, часто в комбінації з 2 портами 10/100/1000BASE-T (Combo)
	Інтерфейси управління	1 x Console (RJ45)
	Стекування (iStack)	Підтримується, дозволяє об'єднувати комутатори в єдиний логічний пристрій
Підтримувані стандарти та протоколи	Рівень 2 (L2)	Стандарти: IEEE 802.1Q (VLAN), 802.1p (QoS), 802.1d (STP), 802.1w (RSTP), 802.1s (MSTP), 802.3ad (LACP)
	Протоколи безпеки	Аутентифікація: 802.1x, RADIUS, MAC-аутентифікація Захист: Списки контролю доступу (ACL), DHCP Snooping, Port Security, захист від ARP- та DoS-атак
	Управління та моніторинг	CLI (командний рядок), SSH, SNMP (v1/v2c/v3), RMON, Telnet, Web-інтерфейс
Фізичні параметри	Живлення	Вбудовані блоки живлення змінного (AC) або постійного (DC) струму
	Форм-фактор	1U, для монтажу в 19-дюймову стійку

Враховуючи обмеження симуляції eNSP щодо повноцінного налаштування автономних точок доступу, розглядається сценарій з використанням бездротового контролера та керованих точок доступу.

В ролі бездротового контролера було обрано модель Huawei AC6005. Це спеціалізований пристрій, призначений для централізованого управління великою

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

кількістю точок доступу Huawei, конфігурації параметрів WLAN, політик безпеки, забезпечення роумінгу та моніторингу бездротової мережі.



Рисунок 3.4 – Контролер Huawei AC6005

Таблиця 3.4 – Основні характеристики Huawei AC6005

Категорія	Характеристика	Значення
Продуктивність та ємність	Пропускна здатність (Forwarding Capacity)	4 Гбіт/с
	Макс. кількість керованих точок доступу (AP)	128
	Макс. кількість користувачів доступу	2000
	Таблиця MAC-адрес	4 000 записів
	Кількість VLAN	4000
Порти та інтерфейси	Сервісні порти	Всього 8 портів GE: 6 x 10/100/1000BASE-T (RJ45) з підтримкою PoE/PoE+ 2 x Combo GE (RJ45/SFP) з підтримкою PoE/PoE+
	Інтерфейси управління	1 x Console (RJ45) 1 x USB
Живлення через Ethernet (PoE)	Підтримувані стандарти	IEEE 802.3af (PoE) та 802.3at (PoE+)
	Кількість портів з PoE	8 (усі сервісні порти)
Фізичні параметри та живлення	Живлення	1 вбудований блок живлення змінного струму (AC)
	Максимальна споживана потужність	114.7 Вт
	Габарити (В x Ш x Г)	43.6 мм x 320 мм x 233.6 мм
	Вага	2.5 кг
	Охолодження	Примусове, з вентиляторами

В якості точки доступу виступає Huawei AP4050DN. Це сучасна дводіапазонна (2.4 ГГц та 5 ГГц) точка доступу, що підтримує актуальні стандарти Wi-Fi (наприклад, 802.11a/b/g/n/ac) і призначена для роботи в режимі "Fit AP" під управлінням контролера AC6005.



Рисунок 3.5 – Точка доступу Huawei AP4050DN

Таблиця 3.5 – Основні характеристики Huawei AP4050DN

Категорія	Характеристика	Значення
Бездротові характеристики	Підтримувані стандарти	IEEE 802.11a/b/g/n/ac/ac Wave 2
	Частотні діапазони	2.4 ГГц та 5 ГГц (одночасна робота)
	MIMO	2x2 MIMO, 2 просторові потоки (Spatial Streams)
	Максимальна швидкість	400 Мбіт/с на 2.4 ГГц 867 Мбіт/с на 5 ГГц
	Режими роботи	Fat AP (автономний), Fit AP (керований контролером), Cloud-managed
Антенa	Тип антени	Вбудована всеспрямована антена
	Коефіцієнт підсилення	2.4 ГГц: 4 дБі 5 ГГц: 5 дБі
Порти та інтерфейси	Ethernet порти	1 x 10/100/1000M Ethernet (RJ45)
	Інтерфейси управління	1 x Console (RJ45)
Фізичні параметри та живлення	Живлення	PoE: IEEE 802.3at (PoE+) Локальне: Адаптер 12В DC
	Максимальна споживана потужність	12.95 Вт
	Габарити (В x Ш x Г)	53 мм x 220 мм x 220 мм
	Вага	1.1 кг

Обрані моделі або їх аналоги в середовищі eNSP дозволяють реалізувати більшість запланованих функцій та протоколів, необхідних для створення та тестування захищеної корпоративної мережі в рамках даного дипломного проєкту.

3.2 Базове налагодження пристроїв мережі

Базове налагодження є першочерговим етапом конфігурації мережевого обладнання. Воно включає в себе встановлення унікальних імен для кожного пристрою (hostname) для полегшення їх ідентифікації в мережі, налаштування IP-адрес для інтерфейсів управління згідно з розробленою схемою адресації, створення необхідних VLAN на комутаторах та маршрутизаторах, а також конфігурацію транкових портів для передачі трафіку декількох VLAN між пристроями та портів доступу для підключення кінцевих пристроїв до конкретних VLAN. Невід'ємною частиною базового налаштування є забезпечення безпечного віддаленого доступу до пристроїв за допомогою протоколу SSH.

Для маршрутизаторів R-23-3-1 та R-23-3-2 виконується встановлення імені хоста, наприклад, sysname R-23-3-1. Створюються всі необхідні VLAN (з 30 по 38) за допомогою команди vlan batch 30 to 38.

```
#
sysname R-23-3-1
#
undo info-center enable
#
vlan batch 30 to 38
#
```

Рисунок 3.6 – Проведення базових налаштувань на R-23-3-1

Далі налаштовуються IP-адреси на логічних інтерфейсах Vlanif для кожної VLAN, наприклад, для Vlanif30 призначається IP-адреса 193.23.3.2 з маскою 255.255.255.224.

```
interface Vlanif30
description VLAN-30-MANAGEMENT
ip address 193.23.3.2 255.255.255.224
```

Рисунок 3.7 – Приклад проведення налаштувань VLAN на R-23-3-1

Також конфігуруються IP-адреси на фізичних WAN-інтерфейсах, що підключаються до Інтернет-провайдерів (наприклад, GigabitEthernet0/0/0). Фізичний LAN-інтерфейс маршрутизатора (наприклад, GigabitEthernet0/0/1), що з'єднується з L3-комутатором, переводиться в режим L2-транку командами portswitch, port link-type trunk та port trunk allow-pass vlan 30 to 38.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

```
#
interface GigabitEthernet0/0/0
description LINK-TO-ISP1
ip address 204.23.3.1 255.255.255.252
nat outbound 3000
#
interface GigabitEthernet0/0/1
portswitch
description TRUNK-TO-SW-1-L3-GE0/0/1
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 38
#
```

Рисунок 3.8 – Фрагмент конфігурації на R-23-3-1

Для безпечного управління створюється локальний користувач admin з відповідним паролем та максимальним рівнем привілеїв (15), вмикається SSH-сервер (stelnet server enable), а лінії VTY налаштовуються для доступу виключно за протоколом SSH. За необхідності, налаштовується статичний маршрут за замовчуванням до відповідного ISP.

```
#
stelnet server enable
#
header login information "WELCOME TO R-23-3-1"
#
user-interface con 0
authentication-mode password
set authentication password cipher ~3;Hj'/0Fani^>"qh^;TW,#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
```

Рисунок 3.9 – Фрагмент конфігурації R-23-3-1

Аналогічним чином були проведені базові налаштування на пристрої R-23-3-2.

Для L3-комутаторів, таких як SW-1-L3, SW-2-L3 та SW-3-L3, базове налаштування включає встановлення унікального імені хоста. Створюються всі необхідні VLAN, включаючи VLAN для користувачів та сервісів (VLAN 30-38). Для управління кожним L3-комутатором налаштовується IP-адреса на інтерфейсі Vlanif30. Аналогічно, IP-адреси призначаються інтерфейсам Vlanif транзитних VLAN. Порти, що використовуються для з'єднання L3-комутаторів між собою (ча-

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

сто агреговані в Eth-Trunk), а також порти, що ведуть до маршрутизаторів та комутаторів рівня доступу, конфігуруються як транкові з дозволом передачі відповідного набору VLAN. Налаштування безпечного доступу через SSH виконується аналогічно до маршрутизаторів, включаючи створення користувача admin та конфігурацію VTY-ліній. Також встановлюється статичний маршрут за замовчуванням, що вказує на IP-адресу шлюзу у Management VLAN.

```
sysname SW-1-L3
#
undo info-center enable
#
vlan batch 30 to 38 100
#
```

Рисунок 3.10 – Фрагмент базової конфігурації SW-1-L3

```
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher XJUN8<9N-:5NZPO3JBXBHA!!
 local-user admin privilege level 15
 local-user admin service-type telnet ssh http
#
interface Vlanif1
#
interface Vlanif30
 description MANAGEMENT-SW-1-L3
 ip address 193.23.3.4 255.255.255.224
 ospf enable 1 area 0.0.0.0
#
```

Рисунок 3.11 – Фрагмент базової конфігурації SW-1-L3

```
#
interface Eth-Trunk1
 description L3-AGG-TO-SW-2-L3
 port link-type trunk
 port trunk allow-pass vlan 30 to 38 100
 mode lacp-static
#
interface GigabitEthernet0/0/1
 description L2-TRUNK-TO-R-23-3-1
 port link-type trunk
 port trunk pvid vlan 30
 port trunk allow-pass vlan 30 to 38
#
```

Рисунок 3.12 – Фрагмент базової конфігурації SW-1-L3

На прикладі комутатора доступу SW-11-L2 та SW-101-L2 базове налаштування включає встановлення імені sysname SW-11-L2. Створюються лише ті

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

VLAN, які використовуються на даному комутаторі (наприклад, VLAN 30, 31, 32). Налаштовується IP-адреса на Vlanif30 для управління. Аплінк-порти до L3-комутаторів конфігуруються як транкові. Порти, до яких підключаються кінцеві пристрої, налаштовуються як порти доступу командою port link-type access з прив'язкою до відповідної VLAN (наприклад, port default vlan 31). Налаштування SSH та статичного маршруту за замовчуванням виконується аналогічно до L3-комутаторів.

```
sysname SW-11-L2
#
undo info-center enable
#
vlan batch 30 to 32 37 to 38
#
stp mode rstp
stp instance 0 priority 16384
#
```

Рисунок 3.13 – Фрагмент базової конфігурації SW-11-L2

```
#
interface Vlanif30
description MANAGEMENT-SW-11-L2
ip address 193.23.3.7 255.255.255.224
#
```

Рисунок 3.14 – Фрагмент базової конфігурації SW-11-L2

```
#
interface Ethernet0/0/1
description UPLINK-TRUNK-TO-SW-1-L3_GE0/0/2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
#
interface Ethernet0/0/2
description UPLINK-TRUNK-TO-SW-2-L3_GE0/0/2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
#
interface Ethernet0/0/3
description LINK-TO-SW-12-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
#
```

Рисунок 3.15 – Фрагмент базової конфігурації SW-11-L2

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				59
Змн.	Арк.	№ докум.	Підпис	Дата		

```
sysname SW-101-L2
#
undo info-center enable
#
vlan batch 30 to 32
#
```

Рисунок 3.16 – Фрагмент базової конфігурації SW-101-L2

```
interface Vlanif30
description MANAGEMENT_SW-101-L2
ip address 193.23.3.12 255.255.255.224
#
```

Рисунок 3.17 – Фрагмент базової конфігурації SW-101-L2

```
#
interface Ethernet0/0/20
description TO-PC-A-3-VLAN31
port link-type access
port default vlan 31
stp edged-port enable
#
```

Рисунок 3.18 – Фрагмент базової конфігурації SW-101-L2

3.3 Налаштування засобів та протоколів мережного захисту

Після виконання базового налагодження пристроїв здійснюється конфігурація ключових протоколів та технологій, що забезпечують надійність та безпеку мережевої інфраструктури. Цей процес включає налаштування відмовостійкості на каналному та мережевому рівнях, конфігурацію динамічної маршрутизації для ефективного обміну даними, розгортання сервісів для автоматизації роботи мережі та реалізацію політик доступу.

Для забезпечення відмовостійкості та запобігання петлям комутації на всіх комутаторах мережі (як L2, так і L3) активується протокол RSTP за допомогою команди `stp mode rstp`. Для створення передбачуваної та стабільної топології Spanning Tree, на комутаторі SW-1-L3, який виконує роль центрального вузла агрегації для значної частини мережі, встановлюється найвищий пріоритет (`stp instance 0 priority 4096`), що робить його кандидатом у кореневі мости для інстансу STP 0. На інших

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				60
Змн.	Арк.	№ докум.	Підпис	Дата		

L3-комутаторах встановлюються менші пріоритети, а на L2-комутаторах – ще менші, що створює чітку ієрархію. На портах, що підключають кінцеві пристрої, активується функція stp edged-port enable, що дозволяє їм швидше переходити в стан пересилання.

```
stp mode rstp
stp instance 0 priority 4096
```

Рисунок 3.19 – Налаштування RSTP на комутаторі SW-1-L3

```
stp mode rstp
stp instance 0 priority 8192
```

Рисунок 3.20 – Налаштування RSTP на комутаторі SW-2-L3

Висока доступність шлюзів за замовчуванням реалізується за допомогою протоколу VRRP на маршрутизаторах R-23-3-1 та R-23-3-2. Для кожного інтерфейсу Vlanif (з 30 по 38), що представляє окрему підмережу, створюється відповідна VRRP-група. Наприклад, для Vlanif31 на обох маршрутизаторах конфігурується група 31 з віртуальною IP-адресою 194.23.3.1. На маршрутизаторі R-23-3-1 встановлюється вищий пріоритет (120), що робить його основним (Master) для всіх груп, тоді як R-23-3-2 з пріоритетом 100 стає резервним (Backup). Це забезпечує безшовне перемикання у випадку відмови основного маршрутизатора.

```
#
interface Vlanif31
description VLAN-31-IT-DEV
ip address 194.23.3.2 255.255.255.0
vrrp vrid 31 virtual-ip 194.23.3.1
vrrp vrid 31 priority 120
ospf enable 1 area 0.0.0.0
#
interface Vlanif32
description VLAN-32-IT-SUPPORT
ip address 195.23.3.2 255.255.255.192
vrrp vrid 32 virtual-ip 195.23.3.1
vrrp vrid 32 priority 120
ospf enable 1 area 0.0.0.0
_
```

Рисунок 3.21 – Налаштування VRRP на VLAN 31-32 маршрутизатора R-23-3-1

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		61

```

interface Vlanif31
description VLAN31_IT-DEV
ip address 194.23.3.3 255.255.255.0
vrrp vrid 31 virtual-ip 194.23.3.1
ospf enable 1 area 0.0.0.0
#
interface Vlanif32
description VLAN32_IT-SUPPORT
ip address 195.23.3.3 255.255.255.192
vrrp vrid 32 virtual-ip 195.23.3.1
ospf enable 1 area 0.0.0.0
#

```

Рисунок 3.22 – Налаштування VRRP на VLAN 31-32 маршрутизатора R-23-3-2

Для автоматичного обміну маршрутною інформацією між ключовими вузлами мережі налаштовується протокол динамічної маршрутизації OSPF. Процес OSPF 1 створюється на маршрутизаторах R-23-3-1, R-23-3-2 та L3-комутаторах SW-1-L3, SW-2-L3, SW-3-L3, і всі вони включаються в єдину зону (area 0). На кожному пристрої за допомогою команди network анонсуються всі внутрішні підмережі, представлені інтерфейсами Vlanif, а також транзитні мережі, що використовуються для зв'язку між самими L3-пристроями. Це дозволяє мережі автоматично адаптуватися до змін у топології та ефективно визначати найкращі шляхи для передачі даних.

```

ospf 1 router-id 10.0.0.1
silent-interface Vlanif30
area 0.0.0.0
network 10.20.3.0 0.0.0.3
network 193.23.3.0 0.0.0.31
#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#

```

Рисунок 3.23 – Налаштування OSPF на L3-комутаторі SW-1-L3

```

ospf 1 router-id 10.0.0.2
silent-interface Vlanif30
area 0.0.0.0
network 10.20.3.0 0.0.0.3
network 10.20.4.0 0.0.0.3
network 193.23.3.0 0.0.0.31
#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#

```

Рисунок 3.24 – Налаштування OSPF на L3-комутаторі SW-2-L3

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

Важливим елементом є налаштування трансляції мережевих адрес (NAT). Для цього на маршрутизаторі R-23-3-1 створюється розширений ACL з номером 3000, який дозволяє трафік з усіх внутрішніх підмереж (193.23.3.0/27, 194.23.3.0/24 і т.д.). Цей ACL потім застосовується до зовнішнього WAN-інтерфейсу GigabitEthernet0/0/0 за допомогою команди nat outbound 3000 для забезпечення доступу внутрішніх користувачів до Інтернету. Аналогічні налаштування з ACL 3001 виконуються на R-23-3-2.

```
#
acl number 3000
 rule 10 permit ip source 193.23.3.0 0.0.0.31
 rule 20 permit ip source 194.23.3.0 0.0.0.255
 rule 30 permit ip source 195.23.3.0 0.0.0.63
 rule 40 permit ip source 196.23.3.0 0.0.0.15
 rule 50 permit ip source 197.23.3.0 0.0.0.31
 rule 60 permit ip source 198.23.3.0 0.0.0.15
 rule 70 permit ip source 199.23.3.0 0.0.0.15
 rule 80 permit ip source 200.23.3.0 0.0.0.63
 rule 90 permit ip source 201.23.3.0 0.0.0.15
#
```

Рисунок 3.25 - ACL 3000 для NAT та його застосування до WAN-інтерфейсу R-23-3-1

```
interface GigabitEthernet0/0/0
 description LINK-TO-ISP1
 ip address 204.23.3.1 255.255.255.252
 nat outbound 3000
#
```

Рисунок 3.26 - ACL 3000 для NAT та його застосування до WAN-інтерфейсу R-23-3-1

Сервіс DHCP для автоматизації IP-адресації клієнтських пристроїв централізовано налаштовується на основному маршрутизаторі R-23-3-1. Для кожної VLAN, що потребує динамічної конфігурації (31-32, 34-38), створюється окремий пул IP-адрес. Наприклад, для VLAN 31 створюється пул VLAN31_IT_DEV, в якому визначається мережа, шлюз за замовчуванням (який відповідає VRRP VIP), адреса DNS-сервера та діапазони IP-адрес, виключені з роздачі для статичних призначень.

```
#
ip pool VLAN31_IT_DEV
gateway-list 194.23.3.1
network 194.23.3.0 mask 255.255.255.0
excluded-ip-address 194.23.3.2 194.23.3.3
excluded-ip-address 194.23.3.200 194.23.3.210
lease day 7 hour 0 minute 0
dns-list 8.8.8.8
#
ip pool VLAN32_SUPPORT
gateway-list 195.23.3.1
network 195.23.3.0 mask 255.255.255.192
excluded-ip-address 195.23.3.2 195.23.3.3
lease day 7 hour 0 minute 0
dns-list 8.8.8.8
#
```

Рисунок 3.27 – Налаштування DHCP пулу для VLAN на R-23-3-1

Політика безпеки між VLAN реалізується за допомогою Списків контролю доступу (ACL). На маршрутизаторах R-23-3-1 та R-23-3-2 створюється набір розширених ACL (наприклад, acl number 3101, acl number 3701 тощо) з правилами permit та deny, що відповідають розробленій матриці доступу.

```
#
acl number 3101
description Controls outbound traffic from IT-DEV (VLAN 31)
rule 10 permit ip source 194.23.3.0 0.0.0.255 destination 196.23.3.0 0.0.0.15
rule 20 deny ip source 194.23.3.0 0.0.0.255 destination 193.23.3.0 0.0.0.31
rule 21 deny ip source 194.23.3.0 0.0.0.255 destination 195.23.3.0 0.0.0.63
rule 22 deny ip source 194.23.3.0 0.0.0.255 destination 197.23.3.0 0.0.0.31
rule 23 deny ip source 194.23.3.0 0.0.0.255 destination 198.23.3.0 0.0.0.15
rule 24 deny ip source 194.23.3.0 0.0.0.255 destination 199.23.3.0 0.0.0.15
rule 25 deny ip source 194.23.3.0 0.0.0.255 destination 200.23.3.0 0.0.0.63
rule 26 deny ip source 194.23.3.0 0.0.0.255 destination 201.23.3.0 0.0.0.15
rule 100 permit ip source 194.23.3.0 0.0.0.255
#
```

Рисунок 3.28 – Створена ACL 3101 для VLAN 31 на маршрутизаторі

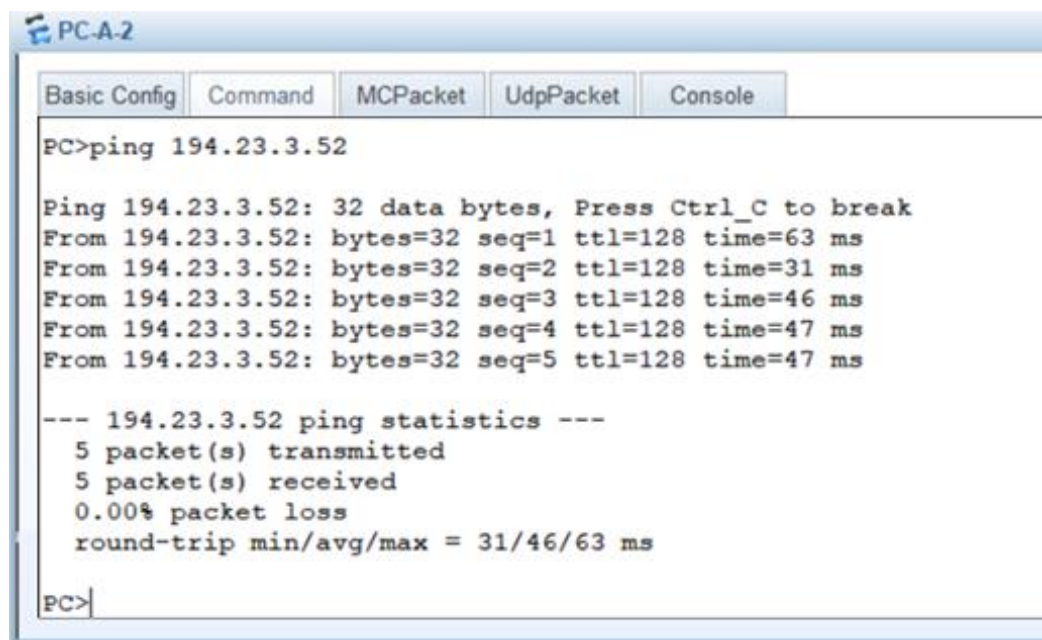
```
acl number 3701
description Allow only Internet for GUEST (VLAN37)
rule 10 deny ip source 200.23.3.0 0.0.0.63 destination 193.23.3.0 0.0.0.31
rule 11 deny ip source 200.23.3.0 0.0.0.63 destination 194.23.3.0 0.0.0.255
rule 12 deny ip source 200.23.3.0 0.0.0.63 destination 195.23.3.0 0.0.0.63
rule 13 deny ip source 200.23.3.0 0.0.0.63 destination 196.23.3.0 0.0.0.15
rule 14 deny ip source 200.23.3.0 0.0.0.63 destination 197.23.3.0 0.0.0.31
rule 15 deny ip source 200.23.3.0 0.0.0.63 destination 198.23.3.0 0.0.0.15
rule 16 deny ip source 200.23.3.0 0.0.0.63 destination 199.23.3.0 0.0.0.15
rule 17 deny ip source 200.23.3.0 0.0.0.63 destination 201.23.3.0 0.0.0.15
rule 100 permit ip source 200.23.3.0 0.0.0.63
#
```

Рисунок 3.29 – Створена ACL 3701 для VLAN 37 на маршрутизаторі

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		64

3.4 Тестування функціоналу мережного захисту

Після завершення налаштування всіх компонентів мережі та протоколів захисту проводиться комплексне тестування для перевірки працездатності та відповідності спроектованої системи поставленим вимогам. Цей процес включає перевірку базової IP-зв'язності як всередині окремих VLAN, так і між ними. Наприклад, з комп'ютера PC-A-2 (VLAN 31) виконуються команди ping на інший пристрій у тій же VLAN (PC-A-3) та на шлюз за замовчуванням для цієї VLAN (194.23.3.1), що дозволяє переконатися в коректності налаштувань комутації на рівнях доступу та розподілу. Аналогічно перевіряється зв'язність між IP-адресами управління комутаторів та маршрутизаторів у Management VLAN 30.



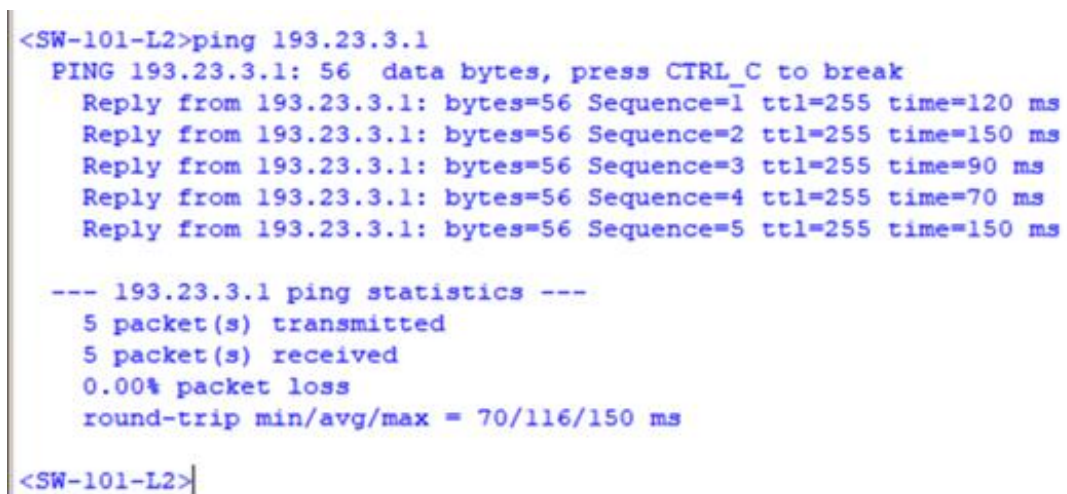
```
PC-A-2
Basic Config Command MCPacket UdpPacket Console
PC>ping 194.23.3.52

Ping 194.23.3.52: 32 data bytes, Press Ctrl_C to break
From 194.23.3.52: bytes=32 seq=1 ttl=128 time=63 ms
From 194.23.3.52: bytes=32 seq=2 ttl=128 time=31 ms
From 194.23.3.52: bytes=32 seq=3 ttl=128 time=46 ms
From 194.23.3.52: bytes=32 seq=4 ttl=128 time=47 ms
From 194.23.3.52: bytes=32 seq=5 ttl=128 time=47 ms

--- 194.23.3.52 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 31/46/63 ms

PC>
```

Рисунок 3.30 – Перевірка з'єднання PC-A-2 – PC-A-3 (VLAN 31)



```
<SW-101-L2>ping 193.23.3.1
PING 193.23.3.1: 56 data bytes, press CTRL_C to break
Reply from 193.23.3.1: bytes=56 Sequence=1 ttl=255 time=120 ms
Reply from 193.23.3.1: bytes=56 Sequence=2 ttl=255 time=150 ms
Reply from 193.23.3.1: bytes=56 Sequence=3 ttl=255 time=90 ms
Reply from 193.23.3.1: bytes=56 Sequence=4 ttl=255 time=70 ms
Reply from 193.23.3.1: bytes=56 Sequence=5 ttl=255 time=150 ms

--- 193.23.3.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 70/116/150 ms

<SW-101-L2>
```

Рисунок 3.31 – Перевірка з'єднання SW-101-L2 – R-23-3-1 (VLAN 30)

Далі тестується працездатність протоколів надійності шляхом імітації різних сценаріїв відмов. Робота RSTP перевіряється аналізом стану портів на комутаторах (display stp brief); у штатному режимі надлишкові шляхи мають бути заблоковані. Потім імітується відмова основного каналу зв'язку, після чого спостерігається час конвергенції RSTP та автоматичне перемикання на резервний шлях. Для VRRP імітується відмова основного маршрутизатора R-23-3-1, після чого R-23-3-2 має перебрати на себе роль Master, що перевіряється командою display vrrp brief. Аналогічно тестується робота агрегованих каналів LACP (Eth-Trunk) шляхом перевірки їх стану та імітації відмови одного з фізичних каналів в агрегації.

```
<R-23-3-2>display vrrp brief
VRID  State      Interface      Type      Virtual IP
-----
30     Master      Vlanif30      Normal    193.23.3.1
31     Backup      Vlanif31      Normal    194.23.3.1
32     Backup      Vlanif32      Normal    195.23.3.1
33     Backup      Vlanif33      Normal    196.23.3.1
34     Backup      Vlanif34      Normal    197.23.3.1
35     Backup      Vlanif35      Normal    198.23.3.1
36     Backup      Vlanif36      Normal    199.23.3.1
37     Backup      Vlanif37      Normal    200.23.3.1
38     Backup      Vlanif38      Normal    201.23.3.1
-----
Total:9      Master:1      Backup:8      Non-active:0
<R-23-3-2>
```

Рисунок 3.32 – Вивід команди display vrrp brief на R-23-3-2

```
<R-23-3-2>display vrrp brief
VRID  State      Interface      Type      Virtual IP
-----
30     Master      Vlanif30      Normal    193.23.3.1
31     Master      Vlanif31      Normal    194.23.3.1
32     Master      Vlanif32      Normal    195.23.3.1
33     Master      Vlanif33      Normal    196.23.3.1
34     Master      Vlanif34      Normal    197.23.3.1
35     Master      Vlanif35      Normal    198.23.3.1
36     Master      Vlanif36      Normal    199.23.3.1
37     Master      Vlanif37      Normal    200.23.3.1
38     Master      Vlanif38      Normal    201.23.3.1
-----
Total:9      Master:9      Backup:0      Non-active:0
<R-23-3-2>
```

Рисунок 3.33 – Вивід команди display vrrp brief на R-23-3-2 після відмови R-23-3-1

Важливою частиною тестування є перевірка коректності роботи мережевих сервісів. Функціонування DHCP-сервера перевіряється шляхом аналізу IP-конфігурацій, отриманих клієнтськими пристроями у відповідних VLAN. Доступ до ресурсів мережі Інтернет з внутрішніх VLAN перевіряється для підтвердження працездатності NAT.

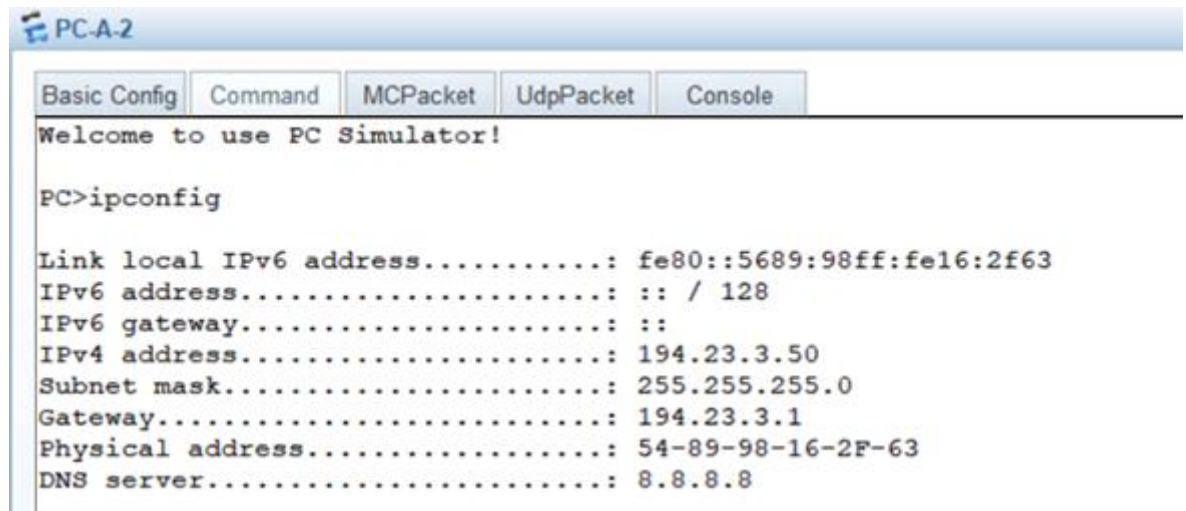


Рисунок 3.34 – Результат команди ipconfig на PC-A-2 (VLAN 31)

Ефективність налаштованих списків контролю доступу (ACL) перевіряється шляхом виконання тестових ping-запитів між різними VLAN відповідно до розробленої матриці доступу. Наприклад, з ПК у VLAN 31 виконується ping на сервер у VLAN 33 (має бути дозволено) та на ПК у VLAN 34 (має бути заборонено).

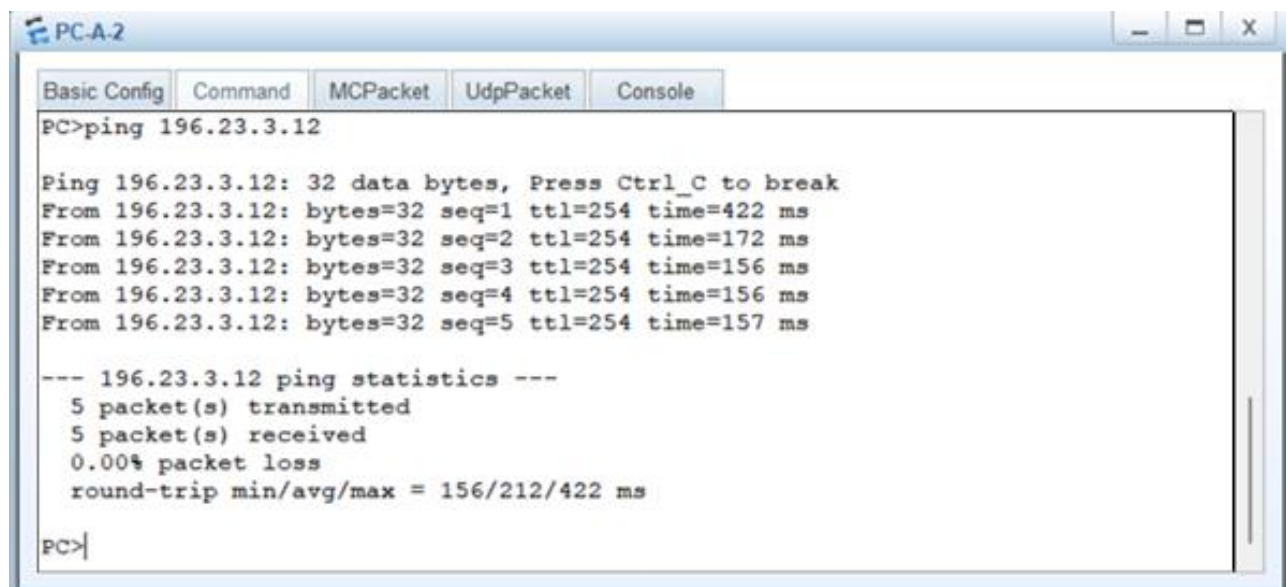


Рисунок 3.35 – Перевірка з'єднання VLAN 31 – VLAN 33

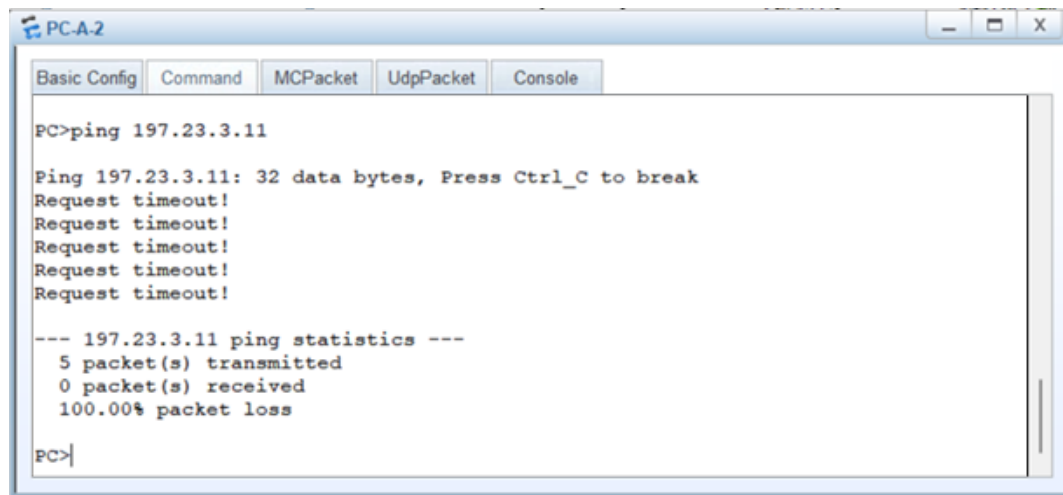


Рисунок 3.36 – Перевірка з'єднання VLAN 31 – VLAN 34

Нарешті, перевіряється безпека віддаленого доступу до мережевих пристроїв шляхом спроби підключення за протоколом SSH.

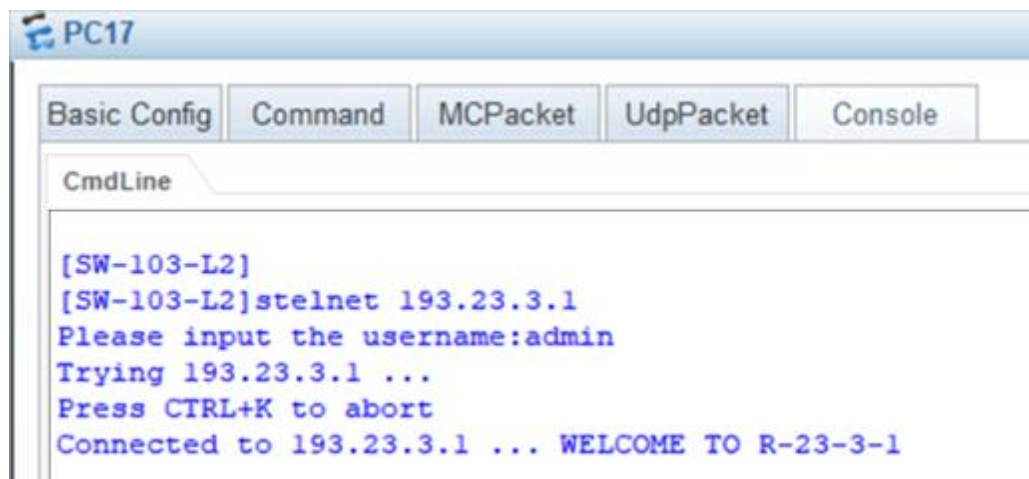


Рисунок 3.37 – Успішна спроба SSH-з'єднання з маршрутизатором R-23-3-1

Результати всіх проведених тестів фіксуються та аналізуються для підтвердження працездатності та безпеки спроектованої мережевої інфраструктури.

Висновок до розділу 3:

У даному розділі було виконано практичну реалізацію спроектованої мережі, що включала вибір обладнання, його базове налагодження та конфігурацію протоколів захисту. Було детально описано налаштування VLAN, RSTP, VRRP, OSPF та списків контролю доступу (ACL). Проведене тестування підтвердило, що реалізовані рішення забезпечують необхідний рівень надійності, продуктивності та безпеки, відповідаючи поставленим у проєкті вимогам.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

ВИСНОВКИ

У кваліфікаційній роботі було розроблено, спроектовано та теоретично обґрунтовано конфігурацію захищеної локальної комутованої мережі для ІТ-компанії з використанням сучасних мережевих технологій та протоколів. Основною метою було створення надійної, продуктивної та безпечної інфраструктури, що відповідає потребам організації та забезпечує гнучкість для подальшого масштабування.

На першому етапі було проведено детальний аналіз теоретичних аспектів побудови сучасних локальних мереж, включаючи принципи комутації, ієрархічні моделі проектування, технології віртуальних локальних мереж (VLAN), методи забезпечення продуктивності (агрегація каналів, QoS), протоколи надійності (STP/RSTP, VRRP) та ключові механізми безпеки на каналному та мережевому рівнях (Port Security, ACL), а також базові мережеві сервіси (DHCP, DNS, SSH).

На основі цих теоретичних знань та з урахуванням специфічних вимог ІТ-компанії, у другому розділі було розроблено комплексну архітектуру мережі. Було обрано трирівневу ієрархічну модель з об'єднаними рівнями ядра та розподілу, що забезпечує оптимальний баланс між продуктивністю, вартістю та керованістю для організації даного розміру. Розроблено детальну фізичну та логічну топологію, включаючи схему підключення до двох незалежних Інтернет-провайдерів для забезпечення відмовостійкості. Ключовим елементом проекту стала розробка схеми IP-адресації з використанням VLAN для сегментації мережі на окремі логічні домени для різних підрозділів (ІТ-розробка, ІТ-підтримка, сервери, бухгалтерія, юридичний відділ, адміністрація, гостьовий доступ, приймальня) та виділення окремої VLAN для управління мережевим обладнанням. Визначено розташування та функціонал базових мережевих сервісів, зокрема DHCP-сервера, реалізованого на центральних маршрутизаторах.

Особливу увагу приділено розробці підсистеми захисту, що включає використання VLAN для ізоляції, RSTP для запобігання петлям, VRRP для резервування шлюзів, детально розроблені списки контролю доступу (ACL) для гранулярного контролю трафіку між різними VLAN відповідно до визначеної політики безпеки.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		69

Обґрунтовано вибір симулятора Huawei eNSP для реалізації проєкту, враховуючи його переваги та обмеження.

У третьому розділі було здійснено вибір конкретних моделей обладнання Huawei, доступних у симуляторі eNSP, та детально описано процес їх базового налаштування, включаючи IP-адресацію, конфігурацію VLAN, транкових та доступних портів, агрегацію каналів. Наведено приклади налаштування ключових протоколів, таких як OSPF для динамічної маршрутизації, VRRP для резервування шлюзів, DHCP-сервера. Теоретично описано налаштування Wi-Fi та детально розроблено застосування списків контролю доступу (ACL) для реалізації політики безпеки між VLAN. Запропоновано комплексну методику тестування функціоналу мережі та її захисних механізмів, включаючи перевірку зв'язності, працездатності протоколів надійності, мережевих сервісів та ефективності ACL.

В результаті виконання кваліфікаційної роботи було створено комплексний проєкт захищеної корпоративної мережі, що відповідає сучасним вимогам до продуктивності, надійності та інформаційної безпеки. Реалізовані рішення, такі як сегментація за допомогою VLAN, резервування ключових компонентів та гранулярний контроль доступу за допомогою ACL, дозволяють забезпечити стабільну та безпечну роботу IT-інфраструктури організації, а також створюють основу для її подальшого розвитку та модернізації.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

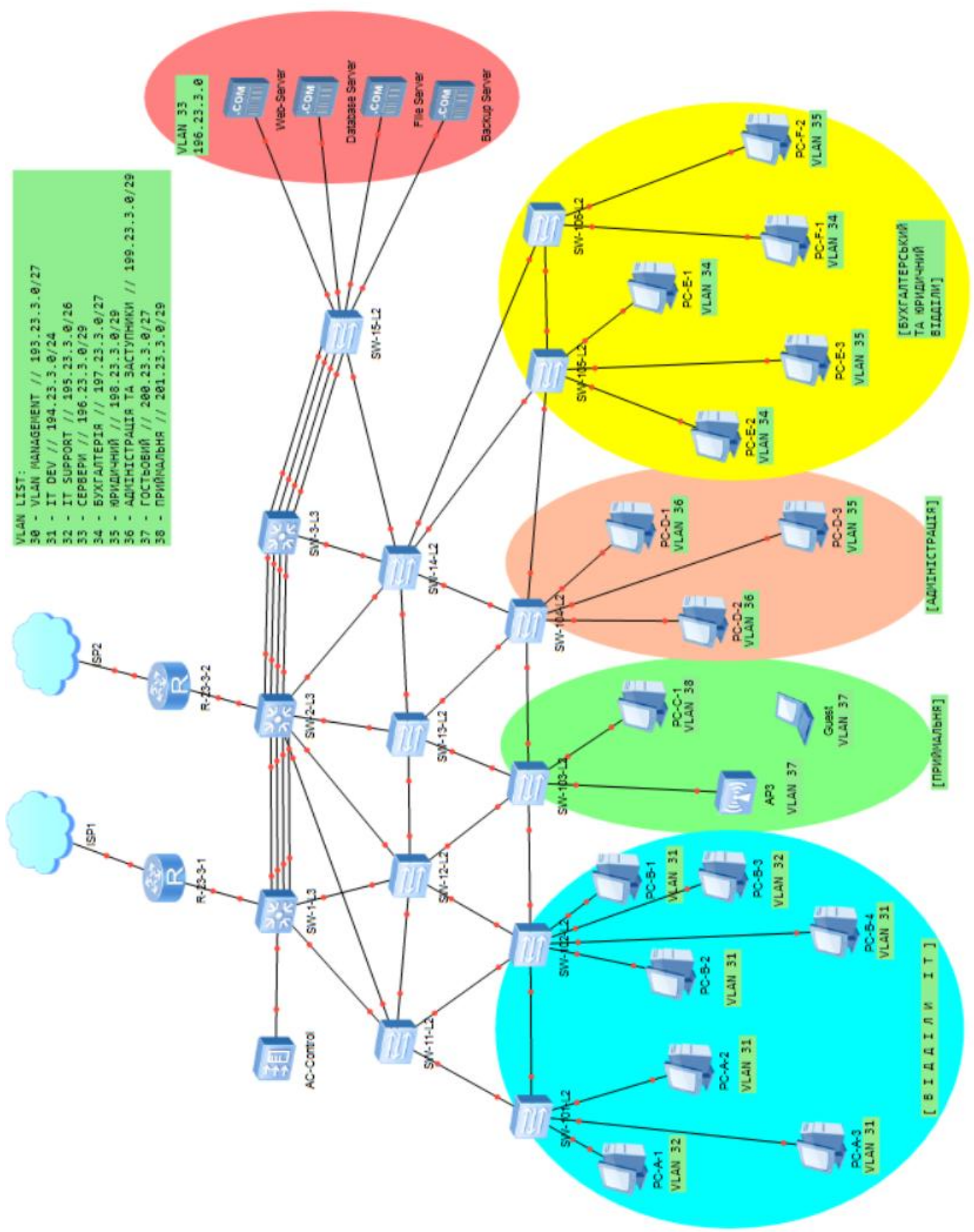
1. *Geeksforgeeks. Difference Between Two-Tier And Three-Tier Database Architecture.* URL: <https://www.geeksforgeeks.org/dbms/difference-between-two-tier-and-three-tier-database-architecture/>.
2. *Huawei Support. What Is VRRP?.* URL: <https://info.support.huawei.com/info-finder/encyclopedia/en/VRRP.html>.
3. *Mosse Cyber Security Institute. Network Segmentation.* URL: <https://library.mosse-institute.com/articles/2023/08/network-segmentation.html>.
4. *Huawei Support. CloudEngine S8700 V600R023C10 Configuration Guide.* URL: <https://support.huawei.com/enterprise/en/doc/EDOC1100366613/541e0175/gvrp-configuration>.
5. *Huawei Support. AP4050DN-E Access Point.* URL: <https://e.huawei.com/hu/products/wlan/ap4050dn-e>.
6. *WebSentra. What is QOS? Quality of Service.* URL: <https://www.websentra.com/what-is-qos/>.
7. Архітектурні принципи побудови комп'ютерних мереж. *Комп'ютерні мережі: підручник* / Є. В. Буров. Львів : Магнолія 2006, 2010. С. 30–65.
8. Технології локальних мереж. *Комп'ютерні мережі: підручник* / Є. В. Буров. Львів : Магнолія 2006, 2010. С. 135–175.
9. *PyNetLabs. VRRP in Networking || Virtual Router Redundancy Protocol.* URL: <https://www.pynetlabs.com/what-is-vrrp-in-networking/>.
10. *Huawei Support. Overview of GVRP.* URL: <https://support.huawei.com/enterprise/en/doc/EDOC1100366613/231931e3/overview-of-gvrp>.
11. *Grandmetric. LACP configuration (Huawei).* URL: https://www.grandmetric.com/knowledge-base/design_and_configure/how-to-configure-lacp-on-huawei-switch/.
12. *Huawei Support. Understanding STP/RSTP/MSTP.* URL: <https://support.huawei.com/enterprise/en/doc/EDOC1100290921/81c7095f/understanding-stp-rstp-mstp>.

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

13. *Huawei Support. Configuring a Basic ACL.* URL: <https://support.huawei.com/enterprise/en/doc/EDOC1000178177/d8968298/configuring-a-basic-acl>.
14. *Huawei Support. WLAN Product Description.* URL: <https://support.huawei.com/enterprise/en/doc/EDOC1100101736/e84a67a4/hardware-information-ac6005-8>.
15. *Huawei Support. S5700 Series Switches Product Description (V200).* URL: <https://support.huawei.com/enterprise/en/doc/EDOC1000027454>.
16. *Huawei Support. AR100, AR120, AR150, AR160, AR200, AR1200, AR2200, AR3200, and AR3600 Hardware Description.* URL: <https://support.huawei.com/enterprise/en/doc/EDOC1000009848/dbb34edd/ar2220-ac>.
17. *Practical Networking. Routing Between VLANs & Layer 3 Switches.* URL: <https://www.practicalnetworking.net/stand-alone/routing-between-vlans/>.
18. *Chapter 20: IP Security. Cryptography and Network Security: Principles and Practice (8th Edition) / W. Stallings.* Hoboken, NJ : Pearson, 2020. C. 621–654.
19. *Huawei Support. S3700 Product Description.* URL: <https://info.support.huawei.com/info-finder/vue/searchcenter/en/enterprise/wlan/S3700-pid-6691596>.

ДОДАТКИ

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				73
Змн.	Арк.	№ докум.	Підпис	Дата		



		Демчук А.С.		
		Єфіменко А.А.		
Змн.	Арк.	№ докум.	Підпис	Дата

R-23-3-1:

```

sysname R-23-3-1
#
vlan batch 30 to 38
#
undo nap slave enable
#
dhcp enable
#
acl number 3000
 rule 10 permit ip source 193.23.3.0 0.0.0.31
 rule 20 permit ip source 194.23.3.0 0.0.0.255
 rule 30 permit ip source 195.23.3.0 0.0.0.63
 rule 40 permit ip source 196.23.3.0 0.0.0.15
 rule 50 permit ip source 197.23.3.0 0.0.0.31
 rule 60 permit ip source 198.23.3.0 0.0.0.15
 rule 70 permit ip source 199.23.3.0 0.0.0.15
 rule 80 permit ip source 200.23.3.0 0.0.0.63
 rule 90 permit ip source 201.23.3.0 0.0.0.15
#
acl number 3101
 description Controls outbound traffic from IT-DEV
 (VLAN 31)
 rule 10 permit ip source 194.23.3.0 0.0.0.255 destination
 196.23.3.0 0.0.0.15
 rule 20 deny ip source 194.23.3.0 0.0.0.255 destination
 193.23.3.0 0.0.0.31
 rule 21 deny ip source 194.23.3.0 0.0.0.255 destination
 195.23.3.0 0.0.0.63
 rule 22 deny ip source 194.23.3.0 0.0.0.255 destination
 197.23.3.0 0.0.0.31
 rule 23 deny ip source 194.23.3.0 0.0.0.255 destination
 198.23.3.0 0.0.0.15
 rule 24 deny ip source 194.23.3.0 0.0.0.255 destination
 199.23.3.0 0.0.0.15
 rule 25 deny ip source 194.23.3.0 0.0.0.255 destination
 200.23.3.0 0.0.0.63
 rule 26 deny ip source 194.23.3.0 0.0.0.255 destination
 201.23.3.0 0.0.0.15
 rule 100 permit ip source 194.23.3.0 0.0.0.255
#
acl number 3201
 description Controls outbound traffic from IT_SUP-
 PORT (VLAN32)
 rule 10 permit ip source 195.23.3.0 0.0.0.63 destination
 196.23.3.0 0.0.0.15
 rule 11 permit ip source 195.23.3.0 0.0.0.63 destination
 193.23.3.0 0.0.0.31
 rule 20 deny ip source 195.23.3.0 0.0.0.63 destination
 194.23.3.0 0.0.0.255
 rule 21 deny ip source 195.23.3.0 0.0.0.63 destination
 197.23.3.0 0.0.0.31
 rule 22 deny ip source 195.23.3.0 0.0.0.63 destination
 198.23.3.0 0.0.0.15
 rule 23 deny ip source 195.23.3.0 0.0.0.63 destination
 199.23.3.0 0.0.0.15
 rule 24 deny ip source 195.23.3.0 0.0.0.63 destination
 200.23.3.0 0.0.0.63
 rule 25 deny ip source 195.23.3.0 0.0.0.63 destination
 201.23.3.0 0.0.0.15
 rule 100 permit ip source 195.23.3.0 0.0.0.63

```

```

#
acl number 3401
 description Controls outbound traffic from ACCOUNT-
 ING (VLAN34)
 rule 10 permit ip source 197.23.3.0 0.0.0.31 destination
 196.23.3.0 0.0.0.15
 rule 20 deny ip source 197.23.3.0 0.0.0.31 destination
 199.23.3.0 0.0.0.15
 rule 21 deny ip source 197.23.3.0 0.0.0.31 destination
 193.23.3.0 0.0.0.31
 rule 100 permit ip source 197.23.3.0 0.0.0.31
#
acl number 3501
 description Controls outbound traffic from LEGAL
 (VLAN35)
 rule 10 permit ip source 198.23.3.0 0.0.0.15 destination
 196.23.3.0 0.0.0.15
 rule 20 deny ip source 198.23.3.0 0.0.0.15 destination
 199.23.3.0 0.0.0.15
 rule 21 deny ip source 198.23.3.0 0.0.0.15 destination
 193.23.3.0 0.0.0.31
 rule 100 permit ip source 198.23.3.0 0.0.0.15
#
acl number 3601
 description Allows full access for ADMIN (VLAN36)
 rule 10 permit ip source 199.23.3.0 0.0.0.15
#
acl number 3701
 description Allow only Internet for GUEST (VLAN37)
 rule 10 deny ip source 200.23.3.0 0.0.0.63 destination
 193.23.3.0 0.0.0.31
 rule 11 deny ip source 200.23.3.0 0.0.0.63 destination
 194.23.3.0 0.0.0.255
 rule 12 deny ip source 200.23.3.0 0.0.0.63 destination
 195.23.3.0 0.0.0.63
 rule 13 deny ip source 200.23.3.0 0.0.0.63 destination
 196.23.3.0 0.0.0.15
 rule 14 deny ip source 200.23.3.0 0.0.0.63 destination
 197.23.3.0 0.0.0.31
 rule 15 deny ip source 200.23.3.0 0.0.0.63 destination
 198.23.3.0 0.0.0.15
 rule 16 deny ip source 200.23.3.0 0.0.0.63 destination
 199.23.3.0 0.0.0.15
 rule 17 deny ip source 200.23.3.0 0.0.0.63 destination
 201.23.3.0 0.0.0.15
 rule 100 permit ip source 200.23.3.0 0.0.0.63
#
acl number 3801
 description Controls outbound traffic from RECEP-
 TION (VLAN38)
 rule 10 permit ip source 201.23.3.0 0.0.0.15 destination
 199.23.3.0 0.0.0.15
 rule 11 permit ip source 201.23.3.0 0.0.0.15 destination
 196.23.3.0 0.0.0.15
 rule 20 deny ip source 201.23.3.0 0.0.0.15 destination
 193.23.3.0 0.0.0.31
 rule 21 deny ip source 201.23.3.0 0.0.0.15 destination
 194.23.3.0 0.0.0.31
 rule 22 deny ip source 201.23.3.0 0.0.0.15 destination
 195.23.3.0 0.0.0.63

```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				75
Змн.	Арк.	№ докум.	Підпис	Дата		

```

rule 24 deny ip source 201.23.3.0 0.0.0.15 destination
197.23.3.0 0.0.0.31
rule 25 deny ip source 201.23.3.0 0.0.0.15 destination
198.23.3.0 0.0.0.15
rule 26 deny ip source 201.23.3.0 0.0.0.15 destination
200.23.3.0 0.0.0.63
rule 100 permit ip source 201.23.3.0 0.0.0.15
#
ip pool VLAN31_IT_DEV
gateway-list 194.23.3.1
network 194.23.3.0 mask 255.255.255.0
excluded-ip-address 194.23.3.2 194.23.3.3
excluded-ip-address 194.23.3.200 194.23.3.210
lease day 7 hour 0 minute 0
dns-list 8.8.8.8
#
ip pool VLAN32_SUPPORT
gateway-list 195.23.3.1
network 195.23.3.0 mask 255.255.255.192
excluded-ip-address 195.23.3.2 195.23.3.3
lease day 7 hour 0 minute 0
dns-list 8.8.8.8
#
ip pool VLAN33_SERVERS
gateway-list 196.23.3.1
network 196.23.3.0 mask 255.255.255.240
excluded-ip-address 196.23.3.2 196.23.3.3
excluded-ip-address 196.23.3.10 196.23.3.13
lease day 7 hour 0 minute 0
dns-list 8.8.8.8
#
ip pool VLAN34_ACCOUNTING
gateway-list 197.23.3.1
network 197.23.3.0 mask 255.255.255.224
excluded-ip-address 197.23.3.2 197.23.3.3
lease day 7 hour 0 minute 0
dns-list 8.8.8.8
#
ip pool VLAN35_LEGAL
gateway-list 198.23.3.1
network 198.23.3.0 mask 255.255.255.240
excluded-ip-address 198.23.3.2 198.23.3.3
lease day 7 hour 0 minute 0
dns-list 8.8.8.8
#
ip pool VLAN36_ADMIN
gateway-list 199.23.3.1
network 199.23.3.0 mask 255.255.255.240
excluded-ip-address 199.23.3.2 199.23.3.3
lease day 7 hour 0 minute 0
dns-list 8.8.8.8
#
ip pool VLAN37_GUEST
gateway-list 200.23.3.1
network 200.23.3.0 mask 255.255.255.192
excluded-ip-address 200.23.3.2 200.23.3.3
lease day 7 hour 0 minute 0
dns-list 8.8.8.8
#
ip pool VLAN38_RECEPTION
gateway-list 201.23.3.1
network 201.23.3.0 mask 255.255.255.240
excluded-ip-address 201.23.3.2 201.23.3.3

```

```

lease day 7 hour 0 minute 0
dns-list 8.8.8.8
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher
zEv9:lwChK@X,k6.EVZ,.m(#
local-user admin service-type ssh
#
firewall zone IT_DEV
#
firewall zone Local
priority 16
#
interface Vlanif30
description VLAN-30-MANAGEMENT
ip address 193.23.3.2 255.255.255.224
vrrp vrid 30 virtual-ip 193.23.3.1
vrrp vrid 30 priority 120
vrrp vrid 30 preempt-mode timer delay 20
ospf enable 1 area 0.0.0.0
#
interface Vlanif31
description VLAN-31-IT-DEV
ip address 194.23.3.2 255.255.255.0
vrrp vrid 31 virtual-ip 194.23.3.1
vrrp vrid 31 priority 120
ospf enable 1 area 0.0.0.0
#
interface Vlanif32
description VLAN-32-IT-SUPPORT
ip address 195.23.3.2 255.255.255.192
vrrp vrid 32 virtual-ip 195.23.3.1
vrrp vrid 32 priority 120
ospf enable 1 area 0.0.0.0
#
interface Vlanif33
description VLAN-33-SERVERS
ip address 196.23.3.2 255.255.255.240
vrrp vrid 33 virtual-ip 196.23.3.1
vrrp vrid 33 priority 120
ospf enable 1 area 0.0.0.0
#
interface Vlanif34
description VLAN-34-ACCOUNTING
ip address 197.23.3.2 255.255.255.224
vrrp vrid 34 virtual-ip 197.23.3.1
vrrp vrid 34 priority 120
ospf enable 1 area 0.0.0.0
#
interface Vlanif35
description VLAN-35-LEGAL
ip address 198.23.3.2 255.255.255.240
vrrp vrid 35 virtual-ip 198.23.3.1
vrrp vrid 35 priority 120
ospf enable 1 area 0.0.0.0
#
interface Vlanif36
description VLAN-36-ADMIN

```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

ip address 199.23.3.2 255.255.255.240
vrrp vrid 36 virtual-ip 199.23.3.1
vrrp vrid 36 priority 120
ospf enable 1 area 0.0.0.0
#
interface Vlanif37
description VLAN-37-GUEST
ip address 200.23.3.2 255.255.255.192
vrrp vrid 37 virtual-ip 200.23.3.1
vrrp vrid 37 priority 120
ospf enable 1 area 0.0.0.0
interface Vlanif38
#description VLAN-38-RECEPTION
ip address 201.23.3.2 255.255.255.240
vrrp vrid 38 virtual-ip 201.23.3.1
vrrp vrid 38 priority 120
ospf enable 1 area 0.0.0.0
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Serial0/0/0
link-protocol ppp
#
interface Serial0/0/1
link-protocol ppp
#
interface Serial0/0/2
link-protocol ppp
#
interface Serial0/0/3
link-protocol ppp
#
interface GigabitEthernet0/0/0
description LINK-TO-ISP1
ip address 204.23.3.1 255.255.255.252
nat outbound 3000
#
interface GigabitEthernet0/0/1
portswitch
description TRUNK-TO-SW-1-L3-GE0/0/1

```

```

sysname R-23-3-2
#
vlan batch 30 to 38
#
undo nap slave enable
#
dhcp enable
#
acl number 3001
description NAT for internal user and server VLANs via ISP2
rule 10 permit ip source 193.23.3.0 0.0.0.31
rule 20 permit ip source 194.23.3.0 0.0.0.255
rule 30 permit ip source 195.23.3.0 0.0.0.63
rule 40 permit ip source 196.23.3.0 0.0.0.15
rule 50 permit ip source 197.23.3.0 0.0.0.31
rule 60 permit ip source 198.23.3.0 0.0.0.15
rule 70 permit ip source 199.23.3.0 0.0.0.15
rule 80 permit ip source 200.23.3.0 0.0.0.63
rule 90 permit ip source 201.23.3.0 0.0.0.15

```

```

port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 38
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
ospf 1 router-id 1.1.1.1
area 0.0.0.0
network 193.23.3.0 0.0.0.31
network 194.23.3.0 0.0.0.255
network 195.23.3.0 0.0.0.63
network 196.23.3.0 0.0.0.15
network 197.23.3.0 0.0.0.31
network 198.23.3.0 0.0.0.15
network 199.23.3.0 0.0.0.15
network 200.23.3.0 0.0.0.63
network 201.23.3.0 0.0.0.15
#
snmp-agent
snmp-agent local-engineid 800007DB03548998B92A2D
snmp-agent sys-info version v3
#
stelnet server enable
#
header login information "WELCOME TO R-23-3-1"
#
user-interface con 0
authentication-mode password
set authentication password cipher
~=>3;Hj'/0Fani^>"qh^;TW,#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
user-interface vty 16 20
#
return

```

R-23-3-2:

```

#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher
0MnL7meMt2;BH^68NhwO2qF#
local-user admin service-type ssh
#
firewall zone Local
priority 16
#
interface Vlanif30
description VLAN30_MANAGEMENT
ip address 193.23.3.3 255.255.255.224
vrrp vrid 30 virtual-ip 193.23.3.1
vrrp vrid 30 preempt-mode timer delay 20
ospf enable 1 area 0.0.0.0

```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

```
#
interface Vlanif31
description VLAN31_IT-DEV
ip address 194.23.3.3 255.255.255.0
vrrp vrid 31 virtual-ip 194.23.3.1
ospf enable 1 area 0.0.0.0
#
interface Vlanif32
description VLAN32_IT-SUPPORT
ip address 195.23.3.3 255.255.255.192
vrrp vrid 32 virtual-ip 195.23.3.1
ospf enable 1 area 0.0.0.0
#
interface Vlanif33
description VLAN33-SERVERS
ip address 196.23.3.3 255.255.255.240
vrrp vrid 33 virtual-ip 196.23.3.1
ospf enable 1 area 0.0.0.0
#
interface Vlanif34
description VLAN34-ACCOUNTING
ip address 197.23.3.3 255.255.255.224
vrrp vrid 34 virtual-ip 197.23.3.1
ospf enable 1 area 0.0.0.0
#
interface Vlanif35
description VLAN35-LEGAL
ip address 198.23.3.3 255.255.255.240
vrrp vrid 35 virtual-ip 198.23.3.1
ospf enable 1 area 0.0.0.0
#
interface Vlanif36
description VLAN36-ADMIN
ip address 199.23.3.3 255.255.255.240
vrrp vrid 36 virtual-ip 199.23.3.1
ospf enable 1 area 0.0.0.0
#
interface Vlanif37
description VLAN37-GUEST
ip address 200.23.3.3 255.255.255.192
vrrp vrid 37 virtual-ip 200.23.3.1
ospf enable 1 area 0.0.0.0
#
interface Vlanif38
description VLAN38-RECEPTION
ip address 201.23.3.3 255.255.255.240
vrrp vrid 38 virtual-ip 201.23.3.1
ospf enable 1 area 0.0.0.0
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Serial0/0/0
link-protocol ppp
#
interface Serial0/0/1
link-protocol ppp

#
sysname SW-1-L3
#
vlan batch 30 to 38 100
```

```
#
interface Serial0/0/2
link-protocol ppp
#
interface Serial0/0/3
link-protocol ppp
#
interface GigabitEthernet0/0/0
description LINK-TO-ISP2
ip address 204.23.3.5 255.255.255.252
nat outbound 3001
#
interface GigabitEthernet0/0/1
portswitch
description TO-SW-2-L3-GE0/0/1-VLAN30-38
port link-type trunk
port trunk allow-pass vlan 30 to 38
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
wlan
#
interface NULL0
#
ospf 1 router-id 2.2.2.2
area 0.0.0.0
network 193.23.3.0 0.0.0.31
network 194.23.3.0 0.0.0.255
network 195.23.3.0 0.0.0.63
network 196.23.3.0 0.0.0.15
network 197.23.3.0 0.0.0.31
network 198.23.3.0 0.0.0.15
network 199.23.3.0 0.0.0.15
network 200.23.3.0 0.0.0.63
network 201.23.3.0 0.0.0.15
#
snmp-agent
snmp-agent local-engineid 800007DB035489980227C6
snmp-agent sys-info version v3
#
stelnet server enable
#
header login information "WELCOME TO R-23-3-2"
#
user-interface con 0
authentication-mode password
set authentication password cipher
{}|SY^bRuYECB7Ie7/)adB#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
user-interface vty 16 20
#
return

#
stp mode rstp
stp instance 0 priority 4096
#
```

SW-1-L3:

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

cluster enable
ntdp enable
ndp enable
#
undo nap slave enable
#
drop illegal-mac alarm
#
dhcp enable
#
diffserv domain default
#
drop-profile default
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher XJUN8<9N-
:5NZPO3JBXBHA!!
local-user admin privilege level 15
local-user admin service-type telnet ssh http
#
interface Vlanif1
#
interface Vlanif30
description MANAGEMENT-SW-1-L3
ip address 193.23.3.4 255.255.255.224
ospf enable 1 area 0.0.0.0
#
interface Vlanif100
description L3-INTERFACE-TO-SW-2-L-3-VIA-ETH-
TRUNK-1
ip address 10.23.3.1 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface MEth0/0/1
#
interface Eth-Trunk1
description L3-AGG-TO-SW-2-L3
port link-type trunk
port trunk allow-pass vlan 30 to 38 100
mode lacp-static
#
interface GigabitEthernet0/0/1
description L2-TRUNK-TO-R-23-3-1
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 38
#
interface GigabitEthernet0/0/2
description L2-TRUNK-TO-SW-11-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
#
interface GigabitEthernet0/0/3
description L2-TRUNK-TO-SW-12-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38

```

```

#
interface GigabitEthernet0/0/4
#
interface GigabitEthernet0/0/5
#
interface GigabitEthernet0/0/6
#
interface GigabitEthernet0/0/7
#
interface GigabitEthernet0/0/8
#
interface GigabitEthernet0/0/9
#
interface GigabitEthernet0/0/10
#
interface GigabitEthernet0/0/11
description MEMBER-TRUNK-SW-2-L3
eth-trunk 1
#
interface GigabitEthernet0/0/12
description MEMBER-TRUNK-SW-2-L3
eth-trunk 1
#
interface GigabitEthernet0/0/13
description MEMBER-TRUNK-SW-2-L3
eth-trunk 1
#
interface GigabitEthernet0/0/14
description MEMBER-TRUNK-SW-2-L3
eth-trunk 1
#
interface GigabitEthernet0/0/15
#
interface GigabitEthernet0/0/16
#
interface GigabitEthernet0/0/17
#
interface GigabitEthernet0/0/18
#
interface GigabitEthernet0/0/19
#
interface GigabitEthernet0/0/20
#
interface GigabitEthernet0/0/21
#
interface GigabitEthernet0/0/22
#
interface GigabitEthernet0/0/23
#
interface GigabitEthernet0/0/24
#
interface NULL0
#
ospf 1 router-id 10.0.0.1
silent-interface Vlanif30
area 0.0.0.0
network 10.20.3.0 0.0.0.3
network 193.23.3.0 0.0.0.31
#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#
stelnet server enable
#

```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

header login information "WELCOME TO SW-1-L3"
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
}:/ $J{,Lk>`S/0Rb{DzNmVF#

```

```

user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return

```

SW-2-L3:

```

ghgh sysname SW-2-L3
#
vlan batch 30 to 38 100 200
#
stp mode rstp
stp instance 0 priority 8192
#
cluster enable
ntdp enable
ndp enable
#
undo nap slave enable
#
drop illegal-mac alarm
#
dhcp enable
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher XJUN8<9N-
:5NZPO3JBXBHA!!
 local-user admin privilege level 15
 local-user admin service-type ssh
#
interface Vlanif1
#
interface Vlanif30
 description MANAGEMENT-SW-2-L3
 ip address 193.23.3.5 255.255.255.224
 ospf enable 1 area 0.0.0.0
#
interface Vlanif100
 description L3-INTERFACE-TO-SW-1-L3-VIA-ETH-
TRUNK1
 ip address 10.20.3.2 255.255.255.252
 ospf enable 1 area 0.0.0.0
#
interface Vlanif200
 description L3-INTERFACE-TO-SW-3-L3-VIA-ETH-
TRUNK2
 ip address 10.20.4.1 255.255.255.252
 ospf enable 1 area 0.0.0.0
#
interface MEth0/0/1
#
interface Eth-Trunk1
 description L2-AGG-TRUNK-TO-SW-1-L3-TRANSIT-
VLAN100

```

```

port link-type trunk
port trunk allow-pass vlan 30 to 38 100
mode lacp-static
#
interface Eth-Trunk2
 description L2-AGG-TRUNK-TO-SW-3-L3-TRANSIT-
VLAN200
port link-type trunk
port trunk allow-pass vlan 30 to 38 200
mode lacp-static
#
interface GigabitEthernet0/0/1
 description TRUNK-TO-R-23-3-2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 38
#
interface GigabitEthernet0/0/2
 description L2-TRUNK-TO-SW-11-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
#
interface GigabitEthernet0/0/3
 description L2-TRUNK-TO-SW-12-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
#
interface GigabitEthernet0/0/4
 description L2-TRUNK-TO-SW-13-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 34 to 38
#
interface GigabitEthernet0/0/5
 description L2-TRUNK-TO-SW-14-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 33 to 36
#
interface GigabitEthernet0/0/6
#
interface GigabitEthernet0/0/7
#
interface GigabitEthernet0/0/8
#
interface GigabitEthernet0/0/9
#
interface GigabitEthernet0/0/10
#
interface GigabitEthernet0/0/11
 description MEMBER-TRUNK-SW-1-L3
 eth-trunk 1
#
interface GigabitEthernet0/0/12

```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				6
Змн.	Арк.	№ докум.	Підпис	Дата		

```

description MEMBER-TRUNK-SW-1-L3
eth-trunk 1
#
interface GigabitEthernet0/0/13
description MEMBER-TRUNK-SW-1-L3
eth-trunk 1
#
interface GigabitEthernet0/0/14
description MEMBER-TRUNK-SW-1-L3
eth-trunk 1
#
interface GigabitEthernet0/0/15
description MEMBER-TRUNK-SW-3-L3
eth-trunk 2
#
interface GigabitEthernet0/0/16
description MEMBER-TRUNK-SW-3-L3
eth-trunk 2
#
interface GigabitEthernet0/0/17
description MEMBER-TRUNK-SW-3-L3
eth-trunk 2
#
interface GigabitEthernet0/0/18
description MEMBER-TRUNK-SW-3-L3
eth-trunk 2
#
interface GigabitEthernet0/0/19
#
interface GigabitEthernet0/0/20
#

```

```

sysname SW-3-L3
#
vlan batch 30 to 38 200
#
stp mode rstp
stp instance 0 priority 8192
#
cluster enable
ntdp enable
ndp enable
#
undo nap slave enable
#
drop illegal-mac alarm
#
dhcp enable
#
diffserv domain default
#
drop-profile default
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher XJUN8<9N-
:5NZPO3JBXBHA!!
local-user admin privilege level 15
local-user admin service-type ssh

```

```

interface GigabitEthernet0/0/21
#
interface GigabitEthernet0/0/22
#
interface GigabitEthernet0/0/23
#
interface GigabitEthernet0/0/24
#
interface NULL0
#
ospf 1 router-id 10.0.0.2
silent-interface Vlanif30
area 0.0.0.0
network 10.20.3.0 0.0.0.3
network 10.20.4.0 0.0.0.3
network 193.23.3.0 0.0.0.31
#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#
stelnet server enable
#
header login information "WELCOME TO SW-2-L3"
#
user-interface con 0
authentication-mode password
set authentication password cipher
<Z0n5Q=A_~^QW:LZJi;=A**#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#

```

SW-3-L3:

```

#
interface Vlanif1
#
interface Vlanif30
description MANAGEMENT-SW-3-L3
ip address 193.23.3.6 255.255.255.224
ospf enable 1 area 0.0.0.0
#
interface Vlanif200
description L3-INTERFACE-TO-SW-2-L3-VIA-ETH-
TRUNK2
ip address 10.20.4.2 255.255.255.252
ospf enable 1 area 0.0.0.0
#
interface MEth0/0/1
#
interface Eth-Trunk2
description L2-AGG-TRUNK-TO-SW-2-L3-TRANSIT-
VLAN200
port link-type trunk
port trunk allow-pass vlan 30 to 38 200
mode lacp-static
#
interface Eth-Trunk3
description L2-AGG-TRUNK-TO-SW-15-L2-SERV-
ERS
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 33
mode lacp-static
#

```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
description L2-TRUNK-TO-SW-14-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 33 to 36
#
interface GigabitEthernet0/0/3
description MEMBER-TRUNK-SW-15-L2
eth-trunk 3
#
interface GigabitEthernet0/0/4
description MEMBER-TRUNK-SW-15-L2
eth-trunk 3
#
interface GigabitEthernet0/0/5
description MEMBER-TRUNK-SW-15-L2
eth-trunk 3
#
interface GigabitEthernet0/0/6
description MEMBER-TRUNK-SW-15-L2
eth-trunk 3
#
interface GigabitEthernet0/0/7
#
interface GigabitEthernet0/0/8
#
interface GigabitEthernet0/0/9
#
interface GigabitEthernet0/0/10
#
interface GigabitEthernet0/0/11
#
interface GigabitEthernet0/0/12
#
interface GigabitEthernet0/0/13
#
interface GigabitEthernet0/0/14
#
interface GigabitEthernet0/0/15
description MEMBER-TRUNK-SW-2-L3
eth-trunk 2
#
interface GigabitEthernet0/0/16
description MEMBER-TRUNK-SW-2-L3

```

```

sysname SW-11-L2
#
vlan batch 30 to 32 37 to 38
#
stp mode rstp
stp instance 0 priority 16384
#
cluster enable
ntdp enable
ndp enable
#
undo nap slave enable
#
drop illegal-mac alarm
#
dhcp enable

```

```

eth-trunk 2
#
interface GigabitEthernet0/0/17
description MEMBER-TRUNK-SW-2-L3
eth-trunk 2
#
interface GigabitEthernet0/0/18
description MEMBER-TRUNK-SW-2-L3
eth-trunk 2
#
interface GigabitEthernet0/0/19
#
interface GigabitEthernet0/0/20
#
interface GigabitEthernet0/0/21
#
interface GigabitEthernet0/0/22
#
interface GigabitEthernet0/0/23
#
interface GigabitEthernet0/0/24
#
interface NULL0
#
ospf 1 router-id 10.0.0.3
silent-interface Vlanif30
area 0.0.0.0
network 10.20.4.0 0.0.0.3
network 193.23.3.0 0.0.0.31
#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#
stelnet server enable
#
header login information "WELCOME TO SW-3-L3"
#
user-interface con 0
authentication-mode password
set authentication password cipher
YWr*D)%NIYy~t+Byca8Yq:(#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
return

```

SW-11-L2:

```

#
diffserv domain default
#
drop-profile default
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher XJUN8<9N-
:5NZPO3JBXBHA!!
local-user admin privilege level 15
local-user admin service-type ssh
#

```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Vlanif1
#
interface Vlanif30
description MANAGEMENT-SW-11-L2
ip address 193.23.3.7 255.255.255.224
#
interface MEth0/0/1
#
interface Ethernet0/0/1
description UPLINK-TRUNK-TO-SW-1-L3_GE0/0/2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
#
interface Ethernet0/0/2
description UPLINK-TRUNK-TO-SW-2-L3_GE0/0/2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
#
interface Ethernet0/0/3
description LINK-TO-SW-12-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
#
interface Ethernet0/0/4
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface Ethernet0/0/8
#
interface Ethernet0/0/9
#
interface Ethernet0/0/10
#
interface Ethernet0/0/11
description DOWNLINK-TO-SW-101-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32
#
interface Ethernet0/0/12

```

```

#sysname SW-12-L2
#
vlan batch 30 to 38
#
stp mode rstp
stp instance 0 priority 16384
#
cluster enable
ntdp enable
ndp enable
#
undo nap slave enable
#
drop illegal-mac alarm
#

```

```

description DOWNLINK-TO-SW-102-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32
#
interface Ethernet0/0/13
#
interface Ethernet0/0/14
#
interface Ethernet0/0/15
#
interface Ethernet0/0/16
#
interface Ethernet0/0/17
#
interface Ethernet0/0/18
#
interface Ethernet0/0/19
#
interface Ethernet0/0/20
#
interface Ethernet0/0/21
#
interface Ethernet0/0/22
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#
stelnet server enable
#
header login information "WELCOME TO SW-11-L2"
#
user-interface con 0
authentication-mode password
set authentication password cipher
BWT'95|#.Z'eKRQqbl+ODD@#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
Return

```

SW-12-L2:

```

dhcp enable
#
diffserv domain default
#
drop-profile default
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher XJUN8<9N-
:5NZPO3JBXBHA!!
local-user admin privilege level 15

```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

local-user admin service-type ssh
#
interface Vlanif1
#
interface Vlanif30
description MANAGEMENT_SW-12-L2
ip address 193.23.3.8 255.255.255.224
#
interface MEth0/0/1
#
interface Ethernet0/0/1
description UPLINK-TO-SW-1-L3_GE0/0/3
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
#
interface Ethernet0/0/2
description UPLINK-TO-SW-2-L3_GE0/0/3
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
#
interface Ethernet0/0/3
description LINK-TO-SW-11-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
#
interface Ethernet0/0/4
description LINK-TO-SW-13-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 34 to 38
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface Ethernet0/0/8
#
interface Ethernet0/0/9
#
interface Ethernet0/0/10
#
interface Ethernet0/0/11
description DOWNLINK-TO-SW-102-L2
port link-type trunk

```

```

ghf sysname SW-13-L2
#
vlan batch 30 to 38
#
stp mode rstp
stp instance 0 priority 16384
#
cluster enable
ntdp enable
ndp enable
#
undo nap slave enable
#

```

```

port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
#
interface Ethernet0/0/12
description DOWNLINK-TO-SW-103-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 37 to 38
#
interface Ethernet0/0/13
#
interface Ethernet0/0/14
#
interface Ethernet0/0/15
#
interface Ethernet0/0/16
#
interface Ethernet0/0/17
#
interface Ethernet0/0/18
#
interface Ethernet0/0/19
#
interface Ethernet0/0/20
#
interface Ethernet0/0/21
#
interface Ethernet0/0/22
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#
stelnet server enable
#
user-interface con 0
authentication-mode password
set authentication password cipher
PrN\WzKkT:u:|l#3M^#3ILL#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
return

```

SW-13-L2:

```

drop illegal-mac alarm
#
dhcp enable
#
diffserv domain default
#
drop-profile default
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default

```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

domain default_admin
local-user admin password cipher XJUN8<9N-
:5NZPO3JBXBHA!!
local-user admin privilege level 15
local-user admin service-type ssh
#
interface Vlanif1
#
interface Vlanif30
description MANAGEMENT_SW-13-L2
ip address 193.23.3.9 255.255.255.224
#
interface MEth0/0/1
#
interface Ethernet0/0/1
#
interface Ethernet0/0/2
description UPLINK-TRUNK-TO-SW-2-L3_GE0/0/4
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 34 to 38
#
interface Ethernet0/0/3
description LINK-TO-SW-12-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
#
interface Ethernet0/0/4
description LINK-TO-SW-14-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 33 to 36
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface Ethernet0/0/8
#
interface Ethernet0/0/9
#
interface Ethernet0/0/10
#
interface Ethernet0/0/11
description DOWNLINK-TO-SW-103-L2
port link-type trunk
port trunk pvid vlan 30

```

```

sysname SW-14-L2
#
vlan batch 30 to 38
#
stp mode rstp
stp instance 0 priority 16384
#
cluster enable
ntdp enable
ndp enable
#
undo nap slave enable

```

```

port trunk allow-pass vlan 30 37 to 38
#
interface Ethernet0/0/12
description DOWNLINK-TO-SW-104-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 35 to 36
#
interface Ethernet0/0/13
#
interface Ethernet0/0/14
#
interface Ethernet0/0/15
#
interface Ethernet0/0/16
#
interface Ethernet0/0/17
#
interface Ethernet0/0/18
#
interface Ethernet0/0/19
#
interface Ethernet0/0/20
#
interface Ethernet0/0/21
#
interface Ethernet0/0/22
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#
stelnet server enable
#
header login information "WELCOME TO SW-13-L2"
#
user-interface con 0
authentication-mode password
set authentication password cipher czvN-
~UmP/u:|l#3M^#3$C#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
return

```

SW-14-L2:

```

#
drop illegal-mac alarm
#
dhcp enable
#
diffserv domain default
#
drop-profile default
#
aaa
authentication-scheme default
authorization-scheme default

```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

```

accounting-scheme default
domain default
domain default_admin
local-user admin password cipher XJUN8<9N-
:5NZPO3JBXBHA!!
local-user admin privilege level 15
local-user admin service-type ssh
#
interface Vlanif1
#
interface Vlanif30
description MANAGEMENT_SW-14-L2
ip address 193.23.3.10 255.255.255.224
#
interface MEth0/0/1
#
interface Ethernet0/0/1
description UPLINK-TRUNK-TO-SW-3-L3_GE0/0/2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 33 to 36
#
interface Ethernet0/0/2
description UPLINK-TRUNK-TO-SW-2-L3_GE0/0/5
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 33 to 36
#
interface Ethernet0/0/3
description LINK-TO-SW-13-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 34 to 38
#
interface Ethernet0/0/4
description LINK-TO-SW-15-L2-SERVERS
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 33
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface Ethernet0/0/8
#
interface Ethernet0/0/9
#
interface Ethernet0/0/10
#
interface Ethernet0/0/11
description DOWNLINK-TO-SW-104-L2
port link-type trunk

```

```

sysname SW-15-L2
#
vlan batch 30 33
#
stp mode rstp
stp instance 0 priority 20480
#

```

```

port trunk pvid vlan 30
port trunk allow-pass vlan 30 35 to 36
#
interface Ethernet0/0/12
description DOWNLINK-TO-SW-105-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 34 to 35
#
interface Ethernet0/0/13
description DOWNLINK-TO-SW-106-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 34 to 35
#
interface Ethernet0/0/14
#
interface Ethernet0/0/15
#
interface Ethernet0/0/16
#
interface Ethernet0/0/17
#
interface Ethernet0/0/18
#
interface Ethernet0/0/19
#
interface Ethernet0/0/20
#
interface Ethernet0/0/21
#
interface Ethernet0/0/22
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#
stelnet server enable
#
header login information "WELCOME TO SW-14-L2"
#
user-interface con 0
authentication-mode password
set authentication password cipher rW=i/<aV-
VVHj<w)JO!C@1cl#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
return

```

SW-15-L2:

```

cluster enable
ntdp enable
ndp enable
#
undo nap slave enable
#
drop illegal-mac alarm

```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```
#
dhcp enable
#
diffserv domain default
#
drop-profile default
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher XJUN8<9N-
:5NZPO3JBXBHA!!
local-user admin privilege level 15
local-user admin service-type ssh
#
interface Vlanif1
#
interface Vlanif30
description MANAGEMENT_SW-15-L2
ip address 193.23.3.11 255.255.255.224
#
interface MEth0/0/1
#
interface Eth-Trunk3
description UPLINK-L2AGG-TO-SW-3-L3-ETH-
TRUNK3
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 33
mode lacp-static
#
interface Ethernet0/0/1
description MEMBER-SW-3-L3
eth-trunk 3
#
interface Ethernet0/0/2
description MEMBER-SW-3-L3
eth-trunk 3
#
interface Ethernet0/0/3
description MEMBER-SW-3-L3
eth-trunk 3
#
interface Ethernet0/0/4
description MEMBER-SW-3-L3
eth-trunk 3
#
interface Ethernet0/0/5
description LINK-TO-SW-14-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 33
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface Ethernet0/0/8
#
interface Ethernet0/0/9
```

```
#
interface Ethernet0/0/10
#
interface Ethernet0/0/11
description TO-BACKUP-SERVER
port link-type access
port default vlan 33
stp edged-port enable
#
interface Ethernet0/0/12
description TO-FILE-SERVER
port link-type access
port default vlan 33
stp edged-port enable
#
interface Ethernet0/0/13
description TO-DATABASE-SERVER
port link-type access
port default vlan 33
stp edged-port enable
#
interface Ethernet0/0/14
description TO-WEB-SERVER
port link-type access
port default vlan 33
stp edged-port enable
#
interface Ethernet0/0/15
#
interface Ethernet0/0/16
#
interface Ethernet0/0/17
#
interface Ethernet0/0/18
#
interface Ethernet0/0/19
#
interface Ethernet0/0/20
#
interface Ethernet0/0/21
#
interface Ethernet0/0/22
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#
stelnet server enable
#
header login information "WELCOME TO SW-15-L2"
#
user-interface con 0
authentication-mode password
set authentication password cipher
TM\~+3Skd$:.`&R&e7S(2&)#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

SW-101-L2:

```
sysname SW-101-L2
#
vlan batch 30 to 32
#
stp mode rstp
#
cluster enable
ntdp enable
ndp enable
#
undo nap slave enable
#
drop illegal-mac alarm
#
dhcp enable
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher XJUN8<9N-
:5NZPO3JBXBHA!!
 local-user admin privilege level 15
 local-user admin service-type ssh
#
interface Vlanif1
#
interface Vlanif30
 description MANAGEMENT_SW-101-L2
 ip address 193.23.3.12 255.255.255.224
#
interface MEth0/0/1
#
interface Ethernet0/0/1
 description UPLINK-TRUNK-TO-SW-11-
L2_ETH0/0/11
 port link-type trunk
 port trunk pvid vlan 30
 port trunk allow-pass vlan 30 to 32
#
interface Ethernet0/0/2
#
interface Ethernet0/0/3
#
interface Ethernet0/0/4
 description LINK-TO-SW-102-L2_ETH0/0/3
 port link-type trunk
 port trunk pvid vlan 30
 port trunk allow-pass vlan 30 to 32
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
```

```
interface Ethernet0/0/8
#
interface Ethernet0/0/9
#
interface Ethernet0/0/10
#
interface Ethernet0/0/11
#
interface Ethernet0/0/12
#
interface Ethernet0/0/13
#
interface Ethernet0/0/14
#
interface Ethernet0/0/15
#
interface Ethernet0/0/16
#
interface Ethernet0/0/17
#
interface Ethernet0/0/18
#
interface Ethernet0/0/19
#
interface Ethernet0/0/20
 description TO-PC-A-3-VLAN31
 port link-type access
 port default vlan 31
 stp edged-port enable
#
interface Ethernet0/0/21
 description TO-PC-A-2-VLAN31
 port link-type access
 port default vlan 31
 stp edged-port enable
#
interface Ethernet0/0/22
 description TO-PC-A-1-VLAN32
 port link-type access
 port default vlan 32
 stp edged-port enable
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#
stelnet server enable
#
header login information "WELCOME TO SW-101-L2"
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
w7B'LcT:@Pu:|l#3M^#3(2&#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		4

SW-102-L2:

```
sysname SW-102-L2
#
vlan batch 30 to 32 37 to 38
#
stp mode rstp
#
cluster enable
ntdp enable
ndp enable
#
undo nap slave enable
#
drop illegal-mac alarm
#
dhcp enable
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher XJUN8<9N-
:5NZPO3JBXBHA!!
 local-user admin privilege level 15
 local-user admin service-type ssh
#
interface Vlanif1
#
interface Vlanif30
 description MANAGEMENT_SW-102-L2
 ip address 193.23.3.13 255.255.255.224
#
interface MEth0/0/1
#
interface Ethernet0/0/1
 description UPLINK-TO-SW-11-L2_ETH0/0/12
 port link-type trunk
 port trunk pvid vlan 30
 port trunk allow-pass vlan 30 to 32
#
interface Ethernet0/0/2
 description UPLINK-TO-SW-12-L2_ETH0/0/11
 port link-type trunk
 port trunk pvid vlan 30
 port trunk allow-pass vlan 30 to 32 37 to 38
#
interface Ethernet0/0/3
 description LINK-TO-SW-101-L3_ETH0/0/4
 port link-type trunk
 port trunk pvid vlan 30
 port trunk allow-pass vlan 30 to 32
#
interface Ethernet0/0/4
 description LINK-TO-SW-103-L2_ETH0/0/3
 port link-type trunk
 port trunk pvid vlan 30
 port trunk allow-pass vlan 30 to 32 37 to 38
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface Ethernet0/0/8
#
interface Ethernet0/0/9
#
interface Ethernet0/0/10
#
interface Ethernet0/0/11
#
interface Ethernet0/0/12
#
interface Ethernet0/0/13
#
interface Ethernet0/0/14
#
interface Ethernet0/0/15
#
interface Ethernet0/0/16
#
interface Ethernet0/0/17
#
interface Ethernet0/0/18
#
interface Ethernet0/0/19
 description TO-PC-B-4-VLAN31
 port link-type access
 port default vlan 31
 stp edged-port enable
#
interface Ethernet0/0/20
 description TO-PC-B-3-VLAN32
 port link-type access
 port default vlan 32
 stp edged-port enable
#
interface Ethernet0/0/21
 description TO-PC-B-2-VLAN31
 port link-type access
 port default vlan 31
 stp edged-port enable
#
interface Ethernet0/0/22
 description TO-PC-B-1-VLAN31
 port link-type access
 port default vlan 31
 stp edged-port enable
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#
stelnet server enable
```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		4

```
#
header login information "WELCOME TO SW-102-L2"
#
user-interface con 0
authentication-mode password
set authentication password cipher
4bw0I<^dJ6sPddVIN=17]=-#
```

```
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
return
```

SW-103-L2:

```
sysname SW-103-L2
#
vlan batch 30 to 32 35 to 38
#
stp mode rstp
#
cluster enable
ntdp enable
ndp enable
#
undo nap slave enable
#
drop illegal-mac alarm
#
diffserv domain default
#
drop-profile default
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher XJUN8<9N-
:5NZPO3JBXBHA!!
local-user admin privilege level 15
local-user admin service-type ssh
#
interface Vlanif1
#
interface Vlanif30
description MANAGEMENT_SW-103-L2
ip address 193.23.3.14 255.255.255.224
#
interface MEth0/0/1
#
interface Ethernet0/0/1
description Uplink1-trunk-to-SW-12-L2_ETH0/0/12
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
#
interface Ethernet0/0/2
description UPLINK-TRUNK-TO-SW-13-L2-
ETH0/0/11
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 35 to 38
#
interface Ethernet0/0/3
description LINK-TO-SW-102-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 to 32 37 to 38
```

```
#
interface Ethernet0/0/4
description LINK-TO-SW-104-L2-ETH0/0/3
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 35 to 38
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface Ethernet0/0/8
#
interface Ethernet0/0/9
#
interface Ethernet0/0/10
#
interface Ethernet0/0/11
#
interface Ethernet0/0/12
#
interface Ethernet0/0/13
#
interface Ethernet0/0/14
#
interface Ethernet0/0/15
#
interface Ethernet0/0/16
#
interface Ethernet0/0/17
#
interface Ethernet0/0/18
#
interface Ethernet0/0/19
#
interface Ethernet0/0/20
port link-type access
port default vlan 37
stp edged-port enable
#
interface Ethernet0/0/21
description TO-AP-GUEST-VLAN37
shutdown
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 37
stp edged-port enable
#
interface Ethernet0/0/22
description TO-PC-C-1-VLAN38
port link-type access
port default vlan 38
stp edged-port enable
```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#
stelnet server enable
#

sysname SW-104-L2
#
undo info-center enable
#
vlan batch 30 34 to 38
#
stp mode rstp
#
cluster enable
ntdp enable
ndp enable
#
undo nap slave enable
#
drop illegal-mac alarm
#
dhcp enable
#
diffserv domain default
#
drop-profile default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher XJUN8<9N-
:5NZPO3JBXBHA!!
 local-user admin privilege level 15
 local-user admin service-type ssh
#
interface Vlanif1
#
interface Vlanif30
 description MANAGEMENT_SW-104-L2
 ip address 193.23.3.15 255.255.255.224
#
interface MEth0/0/1
#
interface Ethernet0/0/1
 description UPLINK-TRUNK-TO-SW-13-L2-
ETH0/0/12
 port link-type trunk
 port trunk pvid vlan 30
 port trunk allow-pass vlan 30 35 to 38
#
interface Ethernet0/0/2
 description UPLINK-TO-SW-14-L2_ETH0/0/11
 port link-type trunk

```

```

header login information "WELCOME TO SW-103-L2"
#
user-interface con 0
 authentication-mode password
 set authentication password cipher
B0"wQn)\]O:.`&R&e7S(gSz#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
return

```

SW-104-L2:

```

port trunk pvid vlan 30
port trunk allow-pass vlan 30 34 to 36
#
interface Ethernet0/0/3
 description LINK-TO-SW-103-L2
 port link-type trunk
 port trunk pvid vlan 30
 port trunk allow-pass vlan 30 35 to 38
#
interface Ethernet0/0/4
 description LINK-TO-SW-105-L2
 port link-type trunk
 port trunk pvid vlan 30
 port trunk allow-pass vlan 30 34 to 36
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface Ethernet0/0/8
#
interface Ethernet0/0/9
#
interface Ethernet0/0/10
#
interface Ethernet0/0/11
#
interface Ethernet0/0/12
#
interface Ethernet0/0/13
#
interface Ethernet0/0/14
#
interface Ethernet0/0/15
#
interface Ethernet0/0/16
#
interface Ethernet0/0/17
#
interface Ethernet0/0/18
#
interface Ethernet0/0/19
#
interface Ethernet0/0/20
 description TO-PC-D-3-VLAN35
 port link-type access
 port default vlan 35
 stp edged-port enable
#

```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Ethernet0/0/21
description TO-PC-D-2-VLAN36
port link-type access
port default vlan 36
stp edged-port enable
#
interface Ethernet0/0/22
description TO-PC-D-1-VLAN36
port link-type access
port default vlan 36
stp edged-port enable
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface NULL0

```

```

#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#
stelnet server enable
#
header login information "WELCOME TO SW-104-L2"
#
user-interface con 0
authentication-mode password
set authentication password cipher
B0"wQn\)OsPddVIN=178[|#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
return

```

SW-105-L2:

```

sysname SW-105-L2
#
undo info-center enable
#
vlan batch 30 34 to 36
#
stp mode rstp
#
cluster enable
ntdp enable
ndp enable
#
undo nap slave enable
#
drop illegal-mac alarm
#
dhcp enable
#
diffserv domain default
#
drop-profile default
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher XJUN8<9N-
:5NZPO3JBXBHA!!
local-user admin privilege level 15
local-user admin service-type ssh
#
interface Vlanif1
#
interface Vlanif30
description MANAGEMENT_SW-105-L2
ip address 193.23.3.16 255.255.255.224
#
interface MEth0/0/1
#
interface Ethernet0/0/1
description UPLINK-TRUNK-TO-SW-14-L2-
ETH0/0/12
port link-type trunk

```

```

port trunk pvid vlan 30
port trunk allow-pass vlan 30 34 to 36
#
interface Ethernet0/0/2
#
interface Ethernet0/0/3
description LINK-TO-SW-104-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 34 to 36
#
interface Ethernet0/0/4
description LINK-TO-SW-106-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 34 to 35
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface Ethernet0/0/8
#
interface Ethernet0/0/9
#
interface Ethernet0/0/10
#
interface Ethernet0/0/11
#
interface Ethernet0/0/12
#
interface Ethernet0/0/13
#
interface Ethernet0/0/14
#
interface Ethernet0/0/15
#
interface Ethernet0/0/16
#
interface Ethernet0/0/17
#
interface Ethernet0/0/18
#

```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

interface Ethernet0/0/19
#
interface Ethernet0/0/20
description TO-PC-E-3-VLAN35
port link-type access
port default vlan 35
stp edged-port enable
#
interface Ethernet0/0/21
description TO-PC-E-2-VLAN34
port link-type access
port default vlan 34
stp edged-port enable
#
interface Ethernet0/0/22
description TO-PC-E-1-VLAN34
port link-type access
port default vlan 34
stp edged-port enable
#
interface GigabitEthernet0/0/1

```

```

#
sysname SW-106-L2
#
undo info-center enable
#
vlan batch 30 34 to 35
#
stp mode rstp
#
cluster enable
ntdp enable
ndp enable
#
undo nap slave enable
#
drop illegal-mac alarm
#
dhcp enable
#
diffserv domain default
#
drop-profile default
#
aaa
authentication-scheme default
authorization-scheme default
accounting-scheme default
domain default
domain default_admin
local-user admin password cipher XJUN8<9N-
:5NZPO3JBXBHA!!
local-user admin privilege level 15
local-user admin service-type ssh
#
interface Vlanif1
#
interface Vlanif30
description MANAGEMENT_SW-106-L2
ip address 193.23.3.17 255.255.255.224
#
interface MEth0/0/1

```

```

#
interface GigabitEthernet0/0/2
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#
stelnet server enable
#
header login information "WELCOME TO SW-105-L2"
#
user-interface con 0
authentication-mode password
set authentication password cipher
l0GsEQmcK7EBi%T]n/.I+cR#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
Return

```

SW-106-L2:

```

#
interface Ethernet0/0/1
description UPLINK-TRUNK-TO-SW-14-
L2_ETH0/0/13
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 34 to 35
#
interface Ethernet0/0/2
#
interface Ethernet0/0/3
description LINK-TO-SW-105-L2
port link-type trunk
port trunk pvid vlan 30
port trunk allow-pass vlan 30 34 to 35
#
interface Ethernet0/0/4
#
interface Ethernet0/0/5
#
interface Ethernet0/0/6
#
interface Ethernet0/0/7
#
interface Ethernet0/0/8
#
interface Ethernet0/0/9
#
interface Ethernet0/0/10
#
interface Ethernet0/0/11
#
interface Ethernet0/0/12
#
interface Ethernet0/0/13
#
interface Ethernet0/0/14
#
interface Ethernet0/0/15
#
interface Ethernet0/0/16

```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

```

#
interface Ethernet0/0/17
#
interface Ethernet0/0/18
#
interface Ethernet0/0/19
#
interface Ethernet0/0/20
#
interface Ethernet0/0/21
description TO-PC-F-2-VLAN35
port link-type access
port default vlan 35
stp edged-port enable
#
interface Ethernet0/0/22
description TO-PC-F-1-VLAN34
port link-type access
port default vlan 34
stp edged-port enable
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/2
#
interface NULL0
#
ip route-static 0.0.0.0 0.0.0.0 193.23.3.1
#
stelnet server enable
#
header login information "WELCOME TO SW-106-L2"
#
user-interface con 0
authentication-mode password
set authentication password cipher
MO)\CJJ>FYJIDGI>zbS=FjO#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
return

```

		Демчук А.С.			ККІКБ.КР.Б – 125 – 03 – ПЗ	Арк.
		Єфіменко А.А.				5
Змн.	Арк.	№ докум.	Підпис	Дата		