МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

МЕРЕЖА ДЛЯ ОРГАНІЗАЦІЇ КІБЕРСПОРТ-АРЕНИ

Виконав: студент групи 2К-22
Спеціальності 123 Комп’ютерна інженерія
Володимир ЮРЧЕНКО
Керівник:
Маргарита МЕДОЛИЗ

Черкаси 2026

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ

Циклова комісія комп’ютерної інженерії та інформаційних технологій

Спеціальність 123 «Комп’ютерна інженерія»

Освітня програма Комп’ютерна інженерія

ЗАТВЕРДЖУЮ

Завідувачка циклової комісії КІ та ІТ

_____Наталя ФАЛЬЧЕНКО
(підпис)

«_____» _____2025 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Юрченку Володимиру Ігоровичу

1. Тема кваліфікаційної роботи Мережа для організації кіберспорт-арени. Керівник роботи Медолиз Маргарита Миколаївна, викладач вищої категорії, затверджені наказом закладу перевищої освіти від «__» ____2025 року №__у
2. Строк подання студентом кваліфікаційної роботи 05.06.2026
3. Вихідні дані до кваліфікацій роботи: Документація виробників обладнання, матеріали з мережевої безпеки, інформація про моніторинг і адміністрування мереж , вимоги до технічного забезпечення кіберзмагань
4. Зміст кваліфікаційної роботи: Технічні вимоги до мережі кіберспорт-арени з урахуванням специфіки ігрового, трансляційного та службового трафіку; визначення критеріїв працездатності та ефективності мережі для потреб кіберспорту; побудова структури мережі для кіберарени, тестування мережі
5. Дата видачі завдання 15.09.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання
1	Вступ	14.10.2025	
2	Розділ 1 Аспекти побудови мереж кіберспортивних	09.12.2025	
3	Розділ 2. Мережева інфраструктури кіберспортивної арени	10.03.2026	
4	Розділ 3 Експериментальне тестування та аналіз результатів проєктування	28.04.2026	
5	Висновки	12.05.2026	
6	Оформлення кваліфікаційної роботи (чистовий варіант)	26.05.2026	
7	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	02.06.2026	
8	Подання кваліфікаційної роботи на затвердження завідувачу ЦК (за 7 днів до захисту)	10.06.2026	

Студент _____ Володимир ЮРЧЕНКО
(підпис)

Керівник роботи _____ Маргарита МЕДОЛИЗ
(підпис)

АНОТАЦІЯ

Кваліфікаційну роботу присвячено розробці та дослідженню спеціалізованої мережевої інфраструктури, адаптованої під специфічні потреби кіберспортивної арени місткістю до 50 ігрових місць.

На основі ієрархічної моделі Collapsed Core спроєктовано фізичну та логічну топології мережі об'єкта. Застосовано технологію логічного розділення широкомовних доменів для повної ізоляції критично важливого ігрового контуру та студії відеотрансляцій від гостьової бездротової мережі та адміністративного сегмента. Для гарантування пріоритетної обробки ігрових пакетів розроблено та впроваджено гнучкі політики якості обслуговування на основі механізмів LLQ та CBWFQ.

Безпеку периметра та захист від цілеспрямованих DDoS-атак реалізовано за допомогою міжмережевого екрана нового покоління NGFW та інструментів канального рівня.

Працездатність та відмовостійкість запропонованих архітектурних рішень підтверджено шляхом імітаційного моделювання у середовищі Cisco Packet Tracer 8.2 під різними сценаріями навантаження. Результати експериментів демонструють утримання затримки в ігровому сегменті в межах 7–12 мс за умов 90%-го завантаження магістральних каналів зв'язку.

КЛЮЧОВІ СЛОВА: ІЄРАРХІЧНА АРХІТЕКТУРА МЕРЕЖІ, ЯКІСТЬ ОБСЛУГОВУВАННЯ, ВІРТУАЛЬНІ ЛОКАЛЬНІ МЕРЕЖІ, ЗАТРИМКА ПАКЕТА, ДЖИТТЕР, КІБЕРСПОРТИВНА ІНФРАСТРУКТУРА, CISCO PACKET TRACER.

ABSTRACT

The qualification work is devoted to the development and research of a specialized network infrastructure adapted to the specific needs of an eSports arena with a capacity of up to 50 gaming seats.

Based on the hierarchical Collapsed Core model, the physical and logical topology of the facility's network was designed. The technology of logical separation of broadcast domains was applied to completely isolate the critically important gaming circuit and video broadcast studio from the guest wireless network and the administrative segment. To guarantee priority processing of gaming packets, flexible quality of service policies based on the LLQ and CBWFQ mechanisms were developed and implemented.

Perimeter security and protection against targeted DDoS attacks were implemented using a new generation NGFW firewall and link-layer tools.

The operability and fault tolerance of the proposed architectural solutions were confirmed by simulation modeling in the Cisco Packet Tracer 8.2 environment under various load scenarios. The experimental results demonstrate that the latency in the gaming segment is maintained within 7–12 ms under conditions of 90% load of the backbone communication channels.

Keywords: hierarchical network architecture, quality of service, virtual local area networks, packet delay, jitter, esports infrastructure, Cisco Packet Tracer.

KEYWORDS: HIERARCHICAL NETWORK ARCHITECTURE, QUALITY OF SERVICE, VIRTUAL LOCAL AREA NETWORKS , ROUND-TRIP TIME, JITTER, E-SPORTS INFRASTRUCTURE, CISCO PACKET TRACER.

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

Скорочення	Пояснення
ACL	Access Control List
CBWFQ	Class-Based Weighted Fair Queuing
DiffServ	Differentiated Services
DPI	Deep Packet Inspection
DSCP	Differentiated Services Code Point
EF	Expedited Forwarding
IPS	Intrusion Prevention System
LACP	Link Aggregation Control Protocol
LLQ	Low Latency Queuing
NGFW	Next-Generation Firewall
QoS	Quality of Service
RSTP	Rapid Spanning Tree Protocol
RTT	Round-Trip Time
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SVI	Switched Virtual Interface
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network

ЗМІСТ

ВСТУП

Протягом останнього десятиліття кіберспорт стрімко трансформувався з аматорського хобі у глобальну високотехнологічну індустрію з багатомільйонними призовими фондами, професійними лігами та мільярдною аудиторією вболівальників. Проведення професійних кіберспортивних турнірів вимагає наявності спеціалізованих майданчиків – арен, які мають задовольняти найвищі технічні стандарти. Організація таких заходів, як турніри серій Intel Extreme Masters, ESL One, The International (Dota 2) або League of Legends World Championship, передбачає не лише створення комфортних умов для гравців та глядачів, але й забезпечення безперебійної, надійної та надшвидкої роботи всієї мережевої інфраструктури. Будь-яке відхилення від заданих параметрів якості обслуговування – збільшення затримки, поява джиттера або втрата пакетів – може призвести до порушення цілісності змагань, дискваліфікації учасників або технічних пауз, які негативно впливають на видовищність та довіру до кіберспорту як до виду спорту.

Як показують сучасні дослідження корпоративних мереж, традиційні моделі організації та захисту втрачають актуальність і не відповідають новим викликам, що особливо проявляється у сфері кіберспорту. Традиційні організації мереж, що часто використовуються в офісних середовищах, не забезпечують необхідного рівня пріоритезації трафіку, ізоляції критичних сервісів та стійкості до зовнішніх і внутрішніх загроз. Як показують сучасні дослідження, навіть затримка у 20 мс може суттєво впливати на якість ігрового процесу, тому для кіберспортивних арен критичною є мінімізація RTT до рівня менше 5 мс, а також велике значення надається надійному захисту від цілеспрямованих DDoS-атак, які можуть бути спрямовані на зрив показового матчу або фінальної гри.

Окрім того, сучасна кіберспортивна арена – це не лише ігрова зона з комп'ютерами учасників. Це ще й потужний медійний майданчик, де працюють десятки камер високої роздільної здатності, системи відеозахоплення, коментаторські позиції, сервери для обсерверів (спостерігачів), студії трансляцій з ефектами доповненої реальності, а також глядацький Wi-Fi, який має витримувати підключення сотень або навіть тисяч пристроїв одночасно. Кожен із цих типів трафіку має різні характеристики та рівень пріоритетності.

Саме тому розробка спеціалізованої, надійної та відмовостійкої архітектури комп'ютерної мережі, яка враховує всі ці вимоги, є надзвичайно важливою технічною задачею, що підтверджує актуальність та практичне значення виконання даної роботи для розвитку інформаційних та мережевих технологій.

Метою кваліфікаційної роботи є розробка надійної, високопродуктивної та безпечної мережевої інфраструктури для організації кіберспортивної арени, що забезпечить стабільне проведення професійних турнірів та покращить показники якості обслуговування ігрового трафіку.

Для досягнення поставленої мети необхідно дослідити теоретичні аспекти, специфіку та вимоги до мережевих інфраструктур у сфері професійного кіберспорту, зокрема, проаналізувати критичні параметри (затримка, джиттер, втрати пакетів, пропускна здатність) та обґрунтувати їх граничні значення. Далі потрібно провести порівняльний огляд існуючих мережевих рішень та підходів до організації турнірних локацій, включаючи плоску, гібридну та ієрархічну архітектури, виявивши їх переваги та недоліки для використання в кіберспорті.

Об'єктом дослідження є процес функціонування та організації комп'ютерних мереж високотехнологічних об'єктів для проведення масових заходів (зокрема, кіберспортивних арен), а також методи забезпечення їх надійності, продуктивності та безпеки.

Предметом дослідження є апаратно-програмні засоби, мережеві протоколи, технології сегментації, пріоритезації трафіку, резервування каналів та архітектурні рішення, що використовуються для розробки відмовостійкої комп’ютерної мережі кіберспорт-арени, здатної забезпечувати стабільну роботу в режимі реального часу.

Практичне значення отриманих результатів також полягає в тому, що розроблена мережева модель, схема IP-адресації, конфігурації VLAN та політик QoS, а також підібрана специфікація обладнання можуть бути безпосередньо використані при будівництві нових або модернізації існуючих комп’ютерних клубів, тренувальних баз та професійних кіберспортивних арен в Україні.

РОЗДІЛ 1 АСПЕКТИ ПОБУДОВИ МЕРЕЖ КІБЕРСПОРТИВНИХ АРЕН

1.1 Специфіка та критичні вимоги до мережевої інфраструктури

Сучасний розвиток кіберспорту як окремої високотехнологічної галузі інформаційних технологій зумовлює необхідність створення спеціалізованих мережевих інфраструктур, здатних забезпечувати стабільну роботу під час проведення професійних турнірів. На відміну від традиційних локальних або корпоративних мереж, мережі кіберспортивних арен функціонують в умовах постійного обміну даними в режимі реального часу, що висуває підвищені вимоги до швидкодії, надійності та відмовостійкості.

Кіберспортивна арена – це складний технологічний комплекс, який одночасно генерує кілька принципово різних типів трафіку. Кожен із цих типів має власні характеристики, вимоги до якості обслуговування та рівень пріоритетності.

До основних типів трафіку належать, перш за все, ігровий трафік, що являє собою обмін даними між ігровими клієнтами, ПК учасників, та ігровими серверами, локальними або віддаленими. Цей трафік базується переважно на протоколі UDP [1], оскільки він не потребує встановлення з'єднання та підтвердження доставки кожного пакета, що мінімізує затримки. Вибір протоколу UDP для ігрового трафіку обумовлений його архітектурними перевагами перед TCP у задачах реального часу. Оскільки TCP орієнтований на гарантовану доставку та використовує механізми повторного надсилання втрачених сегментів і контролю перевантаження, його застосування в кіберспорті призвело б до кумулятивного ефекту затримок. У разі втрати пакета, TCP зупинив би обробку всієї черги до моменту повторного отримання втрачених даних. Використання UDP дозволяє ігровим клієнтам ігнорувати поодинокі втрачені пакети та негайно обробляти найактуальніший стан ігрового світу, що надходить у наступних пакетах з високою частотою. Проте

це висуває безкомпромісні вимоги до фізичного та канального рівнів мережі: оскільки протокол не має вбудованих засобів відновлення втрат, сама мережева інфраструктура повинна гарантувати 0% втрат пакетів. Типовий розмір ігрового пакету становить від 30 до 300 байт, а частота оновлення складає 64, 128 або навіть 256 Гц, що означає передачу до 256 пакетів кожну секунду між клієнтом і сервером. Через це навіть незначне збільшення затримки або втрата окремих пакетів призводить до візуальних артефактів, «телепортації» персонажів, розсинхронізації дій гравців та, як наслідок, до поразки у змаганні.

Наступним типом є трафік відеотрансляцій, який охоплює потоки відео високої чіткості (1080p, 4K, 8K) з ігрових комп'ютерів від гравців або обсерверів на відеомікшери, сервери стрімінгу та студійні монітори. Для передачі нестисненого відео в цьому сегменті використовуються такі технології, як NDI або SDI over IP, які потребують стабільної пропускної здатності до 100–200 Мбіт/с на один потік [21].

Також виділяється адміністративний трафік, який забезпечує роботу системи турнірного управління, включаючи білінг та черги матчів, доступ до файлових серверів, електронну пошту, внутрішній документообіг та VoIP-зв'язок між суддями та організаторами. Хоча цей трафік не є критичним до затримок в реальному часі, його стабільна робота є необхідною для безперебійного функціонування турніру.

Нарешті, вагому частину складає гостьовий Wi-Fi, який надається глядачам, журналістам та іншим відвідувачам арени. Цей трафік є найменш пріоритетним, проте за кількістю підключених пристроїв, що може вимірюватися сотнями або тисячами, він здатний створювати найбільше навантаження на радіоканали та магістральні з'єднання.

Для забезпечення коректної роботи кіберспортивної інфраструктури необхідно контролювати чотири основних параметри: затримку, джиттер, втрати пакетів та пропускну здатність. У таблиці 1.1 наведено граничні

значення для кожного типу трафіку, визначені на основі аналізу вимог провідних турнірних операторів (Riot Games, Valve, ESL) та технічних рекомендацій виробників мережевого обладнання [18–20].

Таблиця 1.1 – Критичні параметри якості мережі для різних типів трафіку

Тип трафіку	Макс. затримка (RTT)	Макс. джиттер	Макс. втрати пакетів	Мін. пропускна здатність
Ігровий (UDP)	20 мс (оптимально 1–5 мс)	< 2 мс	0%	1 Мбіт/с на клієнта
Відеотрансляції (NDI)	< 50 мс	< 5 мс	< 0,1%	100 Мбіт/с на потік
Адміністративний	< 150 мс	не критично	< 1%	10 Мбіт/с (сумарно)
Гостьовий Wi-Fi	< 300 мс	не критично	< 5%	10 Мбіт/с на користувача

Затримка та час кругового шляху – це проміжок часу між відправленням пакета даних від клієнта до сервера та отриманням відповіді. У кіберспорті важливим є не лише середнє значення, а й його стабільність. Типові значення RTT для локальних змагань не повинні перевищувати 5 мс, в ідеалі – 1–2 мс. Для порівняння: при грі через Інтернет навіть у межах одного міста затримка може сягати 20–30 мс, що вже є відчутним для професійних гравців.

Джиттер – варіація затримки між послідовними пакетами. Високий джиттер спричиняє нерівномірне надходження даних, що проявляється як «смикання» об'єктів на екрані, навіть якщо середня затримка низька. Причиною джиттера може бути перевантаження черг на комутаторах, фрагментація пакетів або неякісні кабелі. Для ігрового трафіку допустимий джиттер не більше 2 мс.

Втрати пакетів – відсоток пакетів, які не досягли адресата. Оскільки ігрові додатки використовують UDP, втрачені пакети не пересилаються повторно. Навіть 1% втрат призводить до помітних «провалів» в оновленні ігрового світу, що для професійного гравця неприпустимо. Допустимим

рівнем вважається 0% — будь-які втрати мають бути відсутні. Протокол UDP не має вбудованих засобів відновлення даних , тому завдання мінімізації втрат та компенсації затримок у динамічних онлайн-іграх повністю покладається на оптимізацію мережевої інфраструктури [1].

Пропускна здатність – хоча окремі ігрові клієнти потребують лише 0,5–1 Мбіт/с, сукупне навантаження на мережу арени може сягати гігабітних значень через трансляції, завантаження оновлень ігор та гостьовий трафік. Особливістю є те, що навантаження має пульсуючий характер: під час старту матчу або паузи відбувається синхронне оновлення даних на всіх клієнтах, що створює короткочасні піки.

На практиці на якість мережі впливає безліч факторів, які не завжди очевидні на етапі проєктування. До них належить, перш за все, перевантаження буферів комутаторів, що виникає, коли комутатор накопичує велику кількість пакетів у чергах через перевантаження каналу, внаслідок чого затримка різко зростає. Іншим суттєвим фактором є електромагнітні завади, які створюються через потужне освітлення, аудіосистеми, камери та інше обладнання сцени, що спричиняє перешкоди, особливо для неекранованих кабелів. Крім того, небезпеку становить широкомовний шторм, коли у великих плоских мережах службовий широкомовний трафік може повністю паралізувати роботу всієї інфраструктури. Наостанок, важливим фактором є несанкціоноване підключення пристроїв, за якого глядачі або сторонні особи можуть спробувати підключитися до ізольованої ігрової мережі.

Кіберспортивний турнір – це подія, зупинка якої через технічні причини завдає репутаційних та фінансових збитків організаторам. Тому до апаратного забезпечення мережі висуваються суворі вимоги щодо резервування, серед яких першочерговим є резервування блоків живлення, що передбачає обов'язкову можливість підключення двох джерел живлення до комутаторів ядра та доступу або забезпечення підтримки PoE з резервним інжектором.

Крім того, важливу роль відіграє резервування каналів, згідно з яким між ядром та комутаторами доступу слід прокладати не менше двох фізичних ліній, об'єднаних в один агрегований канал за протоколом LACP. Наостанок, обов'язковим технічним рішенням є впровадження протоколів запобігання петлям, де критично важливим є використання RSTP для автоматичного блокування надлишкових з'єднань та забезпечення швидкого відновлення працездатності мережі у разі виникнення обриву.

Таким чином проведений аналіз свідчить, що мережа кіберспортивної арени повинна забезпечувати мінімальні затримки передавання даних (RTT < 20 мс, бажано 1–5 мс), високу стабільність з'єднання (джиттер < 2 мс, втрати пакетів 0%), ізоляцію різних типів трафіку (ігровий, відео, адмін, гостьовий) та гарантовану якість обслуговування навіть у пікових навантаженнях. Досягнення цих вимог потребує використання сучасних технологій сегментації мережі, пріоритезації трафіку, резервування каналів та захисту периметра.

1.2 Огляд існуючих ережевих рішень та підходів до турнірних локацій

Для задоволення критичних вимог, сформульованих раніше, а саме: затримка меньше 20 мс, нульові втрати пакетів, ізоляція трафіку, необхідно обрати архітектуру локальної мережі, яка б забезпечувала необхідну продуктивність, надійність та масштабованість. Історично підходи до побудови мережевих інфраструктур для ігрових заходів еволюціонували від найпростіших однорангових з’єднань до складних багаторівневих систем, що за своєю відмовостійкістю не поступаються мережам великих фінансових установ.

На ранніх етапах розвитку кіберспорту (кінець 1990-х – початок 2000-х років) турніри проводилися переважно в невеликих комп’ютерних клубах або на тимчасових майданчиках, де інфраструктура часто обмежувалася одним

некомутованим концентратором або найдешевшим комутатором, який об’єднував усі ігрові ПК в єдиний широкомовний домен. Зі зростанням популярності кіберспорту виникла потреба в структурованих кабельних системах і керованих комутаторах. Сьогодні професійні турніри (IEM Katowice, ESL One, The International, BLAST Premier) вимагають архітектур, які забезпечують не лише низькі затримки, але й безперервність роботи десятків відеопотоків, сотень ігрових станцій і тисяч глядацьких Wi-Fi-підключень. Аналіз технічних звітів [18–20] провідних турнірних операторів показує, що більшість сучасних кіберспортивних арен використовують ієрархічні моделі з централізованим ядром.

Одним із найпростіших підходів є плоска архітектура, яка передбачає об’єднання всіх пристроїв (ігрових ПК, серверів, точок доступу) в один широкомовний домен без логічного поділу на рівні L2/L3. Її переваги – мінімальна вартість, простота адміністрування та швидке підключення нових пристроїв. Однак для професійного кіберспорту вона має критичні недоліки: відсутність ізоляції трафіку (гостьовий Wi-Fi та стрімінгове обладнання знаходяться в одному сегменті з ігровими ПК, що призводить до широкомовних штормів), неможливість пріоритезації через FIFO-обробку пакетів, низьку безпеку (будь-який глядач може отримати доступ до ігрових серверів) та погану масштабованість. Такий підхід може застосовуватися лише для невеликих локальних змагань до 20 учасників без вимог до стрімінгу та безпеки.

Гібридна архітектура з віддаленим продакшеном передбачає розміщення локально на арені лише комутаторів доступу та клієнтських пристроїв, а всі сервери (ігрові, відеосервери, системи управління) виносяться у віддалений центр обробки даних або хмару. Зв’язок між ареною та ЦОД здійснюється через орендовані волоконно-оптичні канали або виділені VPN. Переваги – зменшення обсягу локального обладнання та централізоване адміністрування. Недоліки: критична залежність від зовнішніх каналів (будь-

яке погіршення зв’язку або DDoS-атака на провайдера зупиняє турнір), додаткова затримка в 10–20 мс на каналі до ЦОД, висока вартість оренди високошвидкісних каналів (від 1 Гбіт/с із гарантованим SLA) та ускладнення діагностики. Хоча деякі медійні продюсерські центри використовують такий підхід для пост-продакшену, для реального часу змагань він не рекомендується.

Найбільш ефективним рішенням для сучасних кіберспортивних арен є ієрархічна архітектура (Core–Distribution–Access або її спрощений варіант – Collapsed Core). У класичній трирівневій моделі рівень ядра відповідає за високошвидкісну комутацію між сегментами, рівень розподілу реалізує політики маршрутизації, ACL та QoS, а рівень доступу забезпечує підключення кінцевих пристроїв: ПК, камер, точок доступу, із підтримкою PoE та безпеки портів. Для арен з кількістю ігрових місць до 100–150 часто використовують спрощений варіант Collapsed Core, де функції L3-комутації, міжмережевої маршрутизації та реалізації політик виконує один потужний комутатор (або стек комутаторів), до якого безпосередньо підключаються комутатори рівня доступу. Це зменшує кількість пристроїв і спрощує адміністрування без втрати продуктивності.

Ієрархічна архітектура забезпечує повну підтримку VLAN [7] та маршрутизації між ними на апаратному рівні, що дозволяє ізолювати ігровий, медійний, адміністративний та гостьовий трафік. Вона дає можливість тонкого налаштування QoS – пріоритезації ігрових пакетів за допомогою LLQ та резервування смуги для відеотрансляцій через CBWFQ. Завдяки протоколам RSTP та LACP досягається висока відмовостійкість – навіть при виході з ладу окремих ліній або портів робота мережі не переривається. Крім того, архітектура легко масштабується: додавання нових ігрових місць або зон виконується підключенням додаткових комутаторів доступу без зміни конфігурації ядра. Захист периметра забезпечується списками контролю доступу на ядрі та механізмами Port Security на рівні доступу, а також

міжмережевим екраном нового покоління NGFW. Основним недоліком є вища вартість обладнання та складніша початкова конфігурація, однак для професійної кіберспортивної арени ці витрати виправдані вимогами до надійності та продуктивності. У таблиці 1.2 наведено порівняльний аналіз трьох описаних архітектур за ключовими критеріями.

Таблиця 1.2 Порівняння архітектурних підходів для мережі кіберспортивної арени

Критерій	Плоска архітектура	Гібридна	Ієрархічна Collapsed Core
Вартість реалізації	Низька	Висока (оренда каналів)	Середня
Складність налаштування	Низька	Висока	Середня
Підтримка VLAN / ізоляція трафіку	Немає	Часткова	Повна
Можливість QoS (LLQ, CBWFQ)	Немає	Обмежена	Повна
Відмовостійкість (LACP, RSTP)	Немає	Тільки на арені	Повна
Стійкість до DDoS-атак	Дуже низька	Середня	Висока (NGFW на периметрі)
Макс. кількість ігрових місць	До 20	Будь-яка (залежить від каналів)	До 200–300
Час відновлення після збою	Хвилини	Години (при обриві каналу)	Секунди (RSTP)
Затримка (RTT) у локальному сегменті	2–15 мс (нестабільна)	15–50 мс (з каналом)	1–5 мс (стабільна)

Як видно з таблиці 1.2, ієрархічна архітектура Collapsed Core забезпечує найкращий баланс між вартістю, продуктивністю та надійністю для кіберспортивних арен. Аналіз гібридної архітектури з віддаленим продакшеном виявив її критичну непридатність для проведення змагань найвищого рівня. Основним деструктивним фактором є збільшення часу кругового шляху (RTT) за рахунок потреби інкапсуляції трафіку в VPN-тунелі та проходження пакетів через мережі загального користування. Навіть за

наявності волоконно-оптичного лінійного тракту від провайдера з гарантованим SLA, географічна віддаленість ЦОД додає до базового локального пінгу 1–2 мс додаткові 15–30 мс, що робить неможливим досягнення цільового показника RTT менше 5 мс, необхідного для професійних гравців. Таким чином, локальна ієрархічна модель Collapsed Core є єдиним технічно виправданим рішенням, яке повністю усуває залежність ігрового процесу від транзитних затримок глобальної мережі. Вона дозволяє реалізувати всі ключові вимоги, визначені в підрозділі 1.1: ізоляцію трафіку через VLAN, гарантовану низьку затримку через LLQ, відмовостійкість через LACP/RSTP та безпеку через ACL/NGFW.

1.3 Аналіз факторів стабільності мережі та обґрунтування вибору технологій

Стабільність функціонування мережевої інфраструктури є одним із ключових факторів ефективної роботи кіберспортивної арени. На відміну від звичайних локальних мереж, де короткочасні перебої або незначні затримки можуть залишатися непомітними для користувачів, у кіберспорті навіть мінімальні порушення передачі даних здатні суттєво вплинути на результати гри та якість проведення турніру. Саме тому під час проєктування мережі необхідно враховувати не лише базову працездатність обладнання, а й здатність інфраструктури працювати стабільно при високому навантаженні та в умовах постійного обміну даними в режимі реального часу.

Однією з основних проблем у великих локальних мережах є перевантаження окремих сегментів та виникнення широкомовного трафіку, який може негативно впливати на швидкодію мережі. Якщо всі пристрої працюють у межах одного широкомовного домену, зростає кількість службових пакетів, що призводить до зайвого навантаження на комутатори та збільшення затримок передачі даних. Для кіберспортивної арени така ситуація

є критичною, оскільки ігрові застосунки потребують максимально швидкої та стабільної передачі пакетів.

Для вирішення цієї проблеми доцільно використовувати технологію VLAN, яка дозволяє логічно розділити мережу на окремі сегменти. Це дає можливість ізолювати ігровий трафік від адміністративного сегмента, систем відеотрансляції та гостьового Wi-Fi. У результаті зменшується обсяг широкомовного трафіку, підвищується рівень безпеки та покращується керованість мережею.

Важливим аспектом стабільної роботи мережі є забезпечення безперервності з’єднання у випадку виходу з ладу окремих каналів або обладнання. У мережах із великою кількістю комутаторів існує ризик виникнення петель комутації, які можуть спричинити широкомовний шторм і фактичну недоступність мережевих ресурсів. Для запобігання таким ситуаціям використовуються протоколи резервування та контролю топології мережі. Одним із найбільш ефективних рішень є застосування протоколу Rapid Spanning Tree Protocol, який дозволяє автоматично блокувати надлишкові канали та швидко відновлювати працездатність мережі у разі відмови основного з’єднання.

Крім того, для підвищення пропускної здатності магістральних з’єднань доцільно використовувати технологію агрегування каналів LACP. Вона дозволяє об’єднувати кілька фізичних каналів у єдиний логічний інтерфейс, що забезпечує не лише збільшення швидкості передачі даних, а й резервування з’єднань. У разі виходу одного з каналів із ладу передача даних автоматично продовжується через інші активні лінії.

Особливу увагу під час проєктування мережі кіберспорт-арени необхідно приділяти якості обслуговування трафіку. У межах однієї мережі можуть одночасно функціонувати ігрові сервери, відеотрансляції, системи моніторингу та користувацький доступ до Інтернету. Без механізмів

пріоритезації всі типи трафіку обробляються однаково, що може призвести до появи затримок у роботі ігрових сервісів під час пікових навантажень.

Для уникнення подібних ситуацій використовується технологія Quality of Service [13], яка дозволяє встановлювати пріоритет для критично важливого трафіку. Завдяки цьому ігрові пакети обробляються першочергово, а другорядний трафік, наприклад фонові оновлення або гостьовий доступ, не впливає на стабільність ігрового процесу.

Не менш важливим фактором є забезпечення інформаційної безпеки мережі. Під час проведення турнірів мережа кіберспорт-арени може бути об’єктом несанкціонованого доступу, DDoS-атак або внутрішніх порушень роботи. Для мінімізації ризиків необхідно використовувати комплексний підхід до захисту інфраструктури. Зокрема, доцільним є використання міжмережевих екранів нового покоління, списків контролю доступу ACL та механізмів Port Security. Додатково можуть застосовуватись DHCP Snooping та Dynamic ARP Inspection, які дозволяють запобігати підміні мережевих параметрів та несанкціонованому підключенню пристроїв.

Отже, проведений аналіз показав, що для забезпечення стабільної роботи кіберспортивної арени доцільним є використання ієрархічної мережевої архітектури із застосуванням VLAN, QoS, RSTP та LACP [4]. На основі отриманих результатів у наступному розділі буде виконано проєктування логічної та фізичної топології мережі.

РОЗДІЛ 2 МЕРЕЖЕВА ІНФРАСТРУКТУРИ КІБЕРСПОРТИВНОЇ АРЕНИ

2.1 Архітектура та розробка логічної і фізичної топології мережі

Проєктування мережевої інфраструктури кіберспортивної арени базується на принципах ієрархічності, масштабованості та забезпечення мінімальних затримок. Для досягнення поставленої мети обрано ієрархічну модель мережі Collapsed Core [4]. Графічне представлення розробленої фізичної топології мережі кіберспорт-арени у середовищі Cisco Packet Tracer 8.2 наведено на рисунку Б.1.

Вибір цієї архітектури замість ієрархічної архітектури мережі обумовлений можливістю локалізації помилок та широкомовних штормів у межах окремих VLAN. Завдяки використанню комутаторів 3-го рівня у ядрі, маршрутизація між сегментами відбувається на апаратній швидкості, що мінімізує затримки.

Фізична топологія визначає спосіб прокладання кабелів та розміщення обладнання. Для кіберспортивної арени обрано топологію «ієрархічна зірка» .

Центральний вузол розміщує головну телекомунікаційну шафу з комутаторами ядра та маршрутизатором периметра.

З’єднання між ядром мережі та комутаторами в ігрових зонах або глядацьких секторах виконується за допомогою волоконно-оптичних ліній зв'язку. Це гарантує швидкість 10 Гбіт/с і вище та захищає магістраль від електромагнітних завад потужного освітлювального обладнання арени.

Підключення кінцевих пристроїв: ігрових ПК, консолей, камер, здійснюється мідною крученою парою категорії Cat 6a. Використання екранованого кабелю є обов’язковим для запобігання наводкам від силових ліній на сцені. Максимальна довжина сегмента не перевищує 90 метрів. На рисунку 2.1 зображено логічну структуру розробленої мережі.

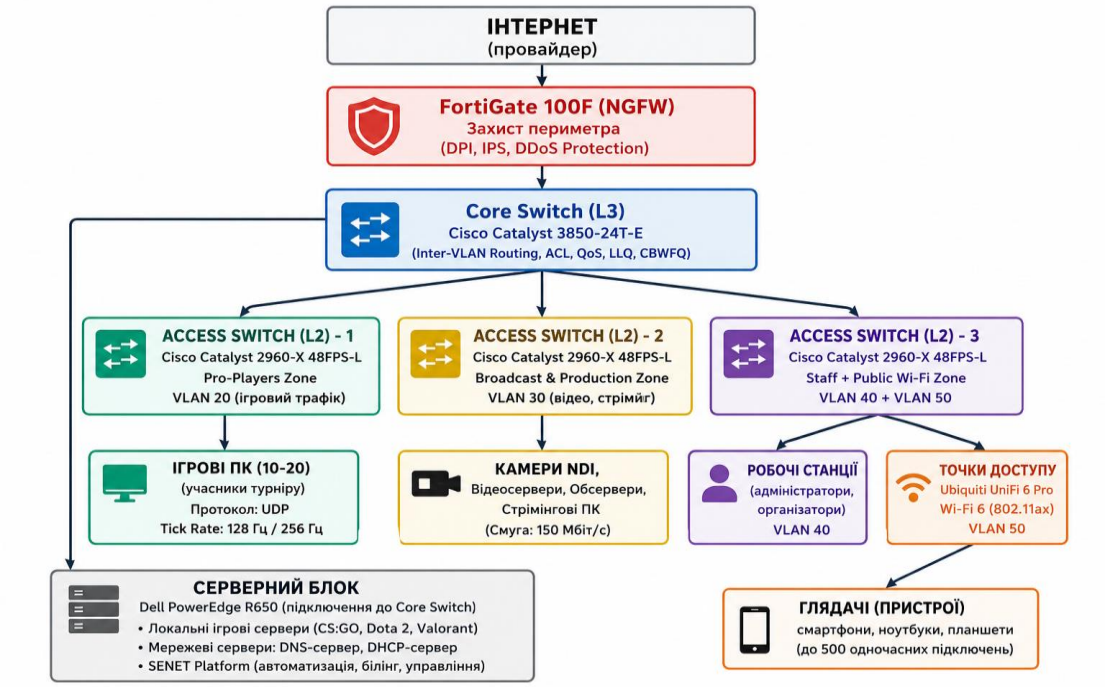

Рисунок 2.1 – Логічна структура мережі кібер-спорт арени

Логічна топологія визначає шлях проходження даних у мережі незалежно від фізичних з’єднань. Основою логічної структури є розподіл на зони відповідальності:

Турнірна зона - ізольований сегмент з прямим підключенням до ігрових серверів. Логічно налаштований на роботу з найвищим пріоритетом.

Зона трансляції - сегмент для передачі відеопотоків високої чіткості. Використовує окремі логічні канали для запобігання завантаженню загальної смуги пропускання.

Адміністративна зона для роботи персоналу арени, касових апаратів, систем контролю доступу.

Глядацька зона з Public Wi-Fi - логічно відокремлена від усіх критичних систем арени. Весь трафік цієї зони проходить через шейпер - обмежувач швидкості та ізолюється від внутрішніх ресурсів мережі.

Вибір ієрархічної моделі замість «плоскої» мережі обумовлений наступними перевагами:

Локалізація помилок: проблеми в одному сегменті (наприклад, несправна точка доступу в зоні глядачів) не поширюються на ігрову зону завдяки чіткому розділенню доменів колізій та широкомовних доменів.

Легкість масштабування: арена може легко збільшити кількість ігрових місць або глядацьких трибун, просто додавши комутатор рівня доступу без зміни конфігурації ядра мережі.

Оптимізація продуктивності: завдяки використанню комутаторів 3-го рівня у ядрі мережі, маршрутизація між сегментами відбувається на апаратній швидкості, що мінімізує затримки, критично важливі для кіберспорту.

2.2 Сегментація мережі (VLAN) та розробка схеми IP-адресації

Ефективне управління мережею кіберспортивної арени неможливе без логічного розділення ресурсів. Використання технології згідно зі стандартом IEEE 802.1Q [7] дозволяє створити кілька ізольованих широкомовних доменів у межах однієї фізичної інфраструктури.

На рисунку 2.3 зображена логічна структура сегментації мережі кіберспотривної арени.

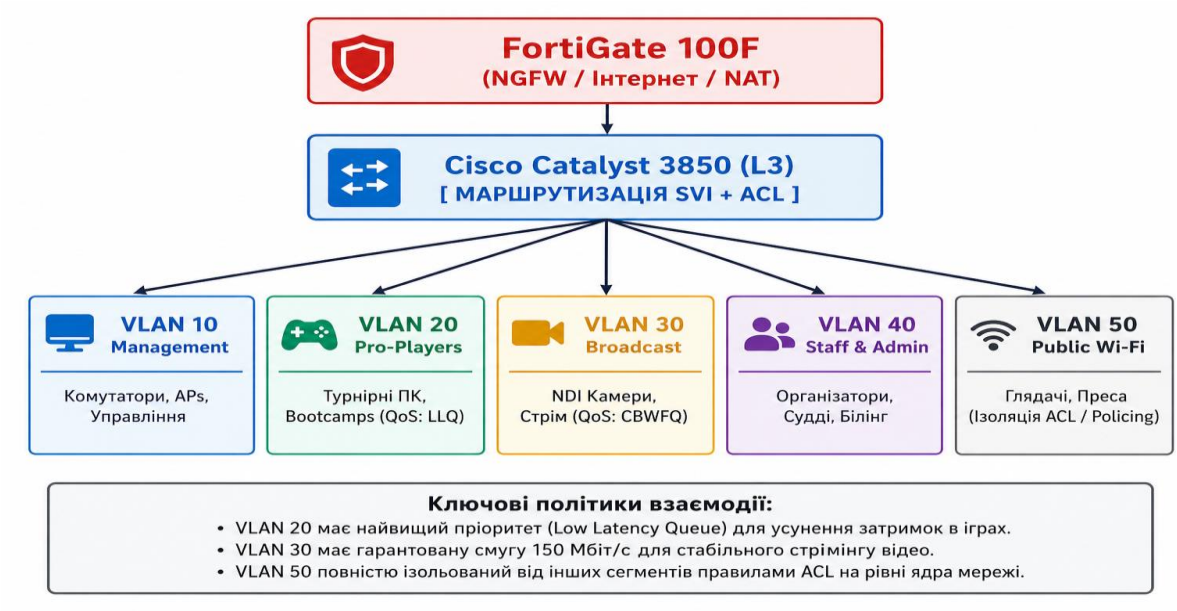

Рисунок 2.2 – Сегментація мережі VLAN

Для побудови мережевої інфраструктури арени обрано комбіновану схему адресації з використанням приватних діапазонів (RFC 1918) [12]. Основна частина внутрішніх сегментів базується на просторі 192.168.0.0/16, що дозволяє гнучко маніпулювати масками підмереж. Для сегмента Production (VLAN 30), зважаючи на велику кількість медіа-пристроїв (камери, обсервери, сервери), використовується мережа 192.168.30.0/24, що забезпечує до 253 вільних адрес. Для публічного сегмента Wi-Fi використано діапазон 172.16.0.0/20, що забезпечує масштабованість для великої кількості одночасних підключень. В таблиці 2.1 наведено розроблену схему IP-адресації мережі.

Обґрунтування розробленої схеми полягає в тому, що для критичних зон, якими є VLAN 20 та 30, використання маски /24 із ємністю 254 адреси є оптимальним рішенням для надійної ізоляції ігрових та стрімінгових пристроїв.

Таблиця 2.1 – Схема IP-адресації мережі

Назва сегмента	ID VLAN	Мережа / Маска	IP-адреса шлюзу	Діапазон для хостів	К-ть хостів	Призначення
Management	10	192.168.10.0/24	192.168.10.1	192.168.10.2–192.168.10.254	253	Комутатори, AP, ДБЖ
Pro-Players	20	192.168.20.0/24	192.168.20.1	192.168.20.2–192.168.20.254	253	Ігрові ПК гравців
Production	30	192.168.30.0/24	192.168.30.1	192.168.30.2–192.168.30.254	253	Стрімінг, ТБ, медіа
Staff	40	192.168.40.0/24	192.168.40.1	192.168.40.2–192.168.40.254	253	Організатори, адміністрація
Public Wi-Fi	50	172.16.0.0/20	172.16.0.1	172.16.0.2–172.16.15.254	4093	Глядачі та гості

Розробка схеми IP-адресації базується на принципі мінімально достатнього адресного простору для критичних зон та максимальної ізоляції широкомовного домену. Вибір маски /24 для сегментів Pro-Players (VLAN 20)

та Production (VLAN 30) аргументується тим, що обмеження розміру підмережі до 254 хостів штучно лімітує граничну кількість широкомовного трафіку (ARP-запитів, службових повідомлень ОС). Це гарантує, що процесори кінцевих ігрових станцій та комутаційні фабрики не будуть витрачати апаратні ресурси на обробку «сміттєвого» трафіку, що безпосередньо впливає на стабільність показників джиттера (< 2 мс). Натомість, для гостьової мережі (VLAN 50) застосування маски /20 (4093 адреси) є математично обґрунтованим кроком для запобігання вичерпання DHCP-пулу під час масових заходів, коли кожен глядач може одночасно мати кілька активних бездротових пристроїв.

Такий підхід суттєво спрощує подальший моніторинг мережевого трафіку та жорстко обмежує широкомовний домен, що є критично важливим фактором для забезпечення стабільності показників пінгу під час змагань. У глядацькій зоні, виділеній під VLAN 50, доцільно обрано маску /20 у діапазоні 172.16.0.0, оскільки це дозволяє одночасно підключити до 4093 клієнтських пристроїв, повністю задовольняючи технічні вимоги до організації масових заходів на кіберспортивних аренах. При цьому міжмережева маршрутизація між усіма створеними підмережами здійснюється безпосередньо на рівні ядра мережі за допомогою високопродуктивного L3-комутатора через Switched Virtual Interfaces, де кожен такий віртуальний інтерфейс функціонує як шлюз за замовчуванням для свого відповідного VLAN.

Для захисту цілісності ігрового процесу та конфіденційних даних на рівні L3-комутатора впроваджуються списки контролю доступу ACL, логіка взаємодії та обмежень яких графічно інтегрована у загальну структуру сегментації мережі. Відповідно до цих налаштувань, сегмент гостьового доступу VLAN 50 (Public) є повністю ізольованим, через що для нього діє сувора заборона на будь-який рух трафіку до внутрішніх мереж арени, включаючи Management, Players, Production та Staff, з одночасним дозволом виключно на вихід в інтернет.

Водночас ігровий контур VLAN 20 (Pro-Players) має чітко обмежений доступ, який дозволяє встановлювати зв’язок лише з локальними ігровими серверами та сегментом керування Management, до того ж в останньому випадку — виключно через визначені порти технічної підтримки, тоді як доступ гравців до глобальної мережі інтернет суворо регламентується через міжмережевий екран. Наостанок, виділена мережа керування VLAN 10 (Management) наділена повноваженнями доступу до всіх існуючих сегментів задля ефективного адміністрування активного обладнання, проте вхідний трафік до самого Management VLAN суворо обмежується і дозволяється лише з авторизованих робочих місць адміністраторів, розташованих у внутрішній мережі персоналу VLAN 40.

Повна топологія побудови, маркування трафіку, розподіл адресного простору та зони дії списків контролю доступу для кожного логічного сегмента кіберспортивної арени наочно представлені на рисунку 2.1.

2.3 Вибір програмного забезпечення та мережевого обладнання

Для реалізації високоефективної мережевої інфраструктури кіберспорт-арени обрано обладнання та програмне забезпечення корпоративного класу, що дозволяє мінімізувати затримки передачі даних та забезпечити високий рівень безпеки.

В основу проектування покладено трирівневу ієрархічну модель мережі, де центральним вузлом виступає комутатор ядра L3-рівня Cisco Catalyst 3850-24T-E, параметри якого деталізовано у Таблиці 2.3. Даний пристрій забезпечує апаратну маршрутизацію між VLAN-сегментами та централізоване керування трафіком.

Рівень доступу реалізовано на базі комутаторів Cisco Catalyst 2960-X, які дозволяють підключити ігрові ПК та стрімінгове обладнання на гігабітних швидкостях, а завдяки підтримці технології PoE+ — забезпечити живлення точок доступу та IP-камер без прокладання додаткових силових ліній.

Захист периметра мережі та фільтрація зовнішнього трафіку покладається на міжмережевий екран наступного покоління (NGFW) FortiGate 100F. Це рішення обрано через наявність спеціалізованих процесорів для протидії DDoS-атакам, що є критично важливим для стабільності ігрового процесу під час турнірів.

Для обґрунтування вибору апаратного міжмережевого екрана нового покоління у межах кваліфікаційної роботи було проведено порівняльний аналіз провідних рішень корпоративного класу від виробників Fortinet, Cisco та Palo Alto за ключовими технічними критеріями, що безпосередньо впливають на стабільність і безпеку функціонування ігрового контуру. Результати аналізу систематизовано та наведено в таблиці 2.2.

Аналіз даних таблиці 2.2 дозволяє зробити висновок, що модель Fortinet FortiGate 100F є найбільш раціональним технічним рішенням для об'єкта кіберспортивної інфраструктури. Ключовою перевагою обраного пристрою є використання спеціалізованих мікросхем апаратного прискорення ASIC, які дозволяють виконувати глибоку інспекцію пакетів (DPI) та активовувати систему запобігання вторгненням (IPS) без деградації загальної пропускної здатності каналу зв'язку.

Технічна перевага FortiGate 100F над аналогами (Cisco Firepower та Palo Alto) полягає в архітектурній реалізації обробки трафіку.

Таблиця 2.2 – Порівняльний аналіз міжмережевих екранів нового покоління (NGFW)

Критерій порівняння	Fortinet FortiGate 100F	Cisco Firepower 1010	Palo Alto PA-440
Номінальна пропускна здатність Firewall	20 Гбіт/с	3 Гбіт/с	3 Гбіт/с
Пропускна здатність Threat Protection / IPS	1 Гбіт/с / 1 Гбіт/с	650 Мбіт/с / 650 Мбіт/с	900 Мбіт/с / 900 Мбіт/с

Продовження таблиці 2.2

Апаратне прискорення обробки трафіку	Інтегровані со-процесори ASIC (SOC4)	Відсутнє (залежність від загального CPU)	Відсутнє (архітектурна оптимізація ОС)
Стійкість до апаратних збоїв	Наявність резервних блоків живлення	Зовнішній блок живлення	Зовнішній блок живлення
Економічна доцільність (Ціна / Продуктивність)	Оптимальна (найкращий показник у класі)	Висока вартість ліцензування	Максимальна вартість обладнання

Традиційні міжмережеві екрани використовують загальний центральний процесор як для маршрутизації, так і для важких обчислювальних операцій: глибокої інспекції пакетів та сигнатурного аналізу IPS. Під час масованої UDP-Flood або ICMP-Flood атаки це призводить до явища «CPU Exhaustion», через що пристрій починає затримувати або відкидати легітимні пакети, піднімаючи пінг гравців. FortiGate 100F завдяки спеціалізованим со-процесорам ASIC SOC4 переносить обробку безпекових сигнатур на апаратний уровень (Hardware Acceleration), залишаючи основний CPU вільним для базової комутації. Це забезпечує нульову деградацію пропускної здатності та стабільність RTT ігрового контуру навіть у моменти пікових зовнішніх атак.

Особливе значення для професійної ігрової арени має висока стійкість FortiGate 100F до спрямованих DDoS-атак (зокрема UDP та ICMP Flood). Завдяки обробці аномального інтернет-трафіку на рівні спеціалізованих чіпів, пристрій запобігає перевантаженню центрального процесора, нейтралізує загрози на периметрі та за умови коректного налаштування гарантує стабільність показників у локальному ігровому сегменті.

У розробленій архітектурі мережі міжмережевий екран FortiGate 100F інтегрується на рівні магістрального периметра (Edge Router / NGFW), виступаючи єдиною точкою розмежування між внутрішнім адресним простором арени та глобальною мережею Інтернет.

Схема фізичного та логічного позиціонування пристрою визначається кількома взаємопов'язаними аспектами, де вхідні магістральні лінії від інтернет-провайдерів підключаються безпосередньо до інтерфейсів WAN

пристрою FortiGate 100F. Водночас внутрішній LAN-інтерфейс міжмережевого екрана з'єднується з високопродуктивним L3-комутатором ядра Cisco Catalyst 3850-24T-E за допомогою волоконно-оптичної лінії зв'язку. При цьому розподіл функцій маршрутизації організовано таким чином, що внутрішня міжмережева маршрутизація між створеними сегментами, а саме VLAN 10, 20, 30 та 40, повністю покладається на апаратний рівень комутатора ядра через віртуальні інтерфейси SVI. Це дозволяє ефективно локалізувати внутрішній гігабітний трафік і не перевантажувати центральний процесор екрана периметра. Для забезпечення виходу в глобальну мережу на комутаторі ядра Cisco Catalyst 3850 конфігурується статичний маршрут за замовчуванням, який автоматично перенаправляє весь трафік, призначений для зовнішніх мереж, на IP-адресу внутрішнього інтерфейсу FortiGate 100F, що відповідає значенню 10.0.0.1, як детально визначено у таблиці маршрутизації у Додатку А.3

Така топологічна організація гарантує, що будь-який пакет, який прямує у глобальну мережу (ігровий трафік учасників, медіа-стріми або запити глядачів з Public Wi-Fi), обов'язково проходить через підсистему безпеки NGFW, де здійснюється DPI-моніторинг і забезпечується ізоляція публічного сегмента VLAN 50 від критично важливих внутрішніх ресурсів кіберспортивної арени.

Бездротовий сегмент для глядачів та персоналу базується на точках доступу Ubiquiti UniFi 6 Pro, які підтримують стандарт Wi-Fi 6 і здатні обслуговувати велику кількість одночасних сесій у щільному середовищі.

Серверна частина інфраструктури, представлена платформою Dell PowerEdge R650, призначена для розгортання віртуалізованих сервісів, таких як локальні ігрові сервери та системи кешування контенту, що також відображено у специфікації мережевого обладнання та ПЗ (Таблиця 2.3).

Програмне забезпечення мережі включає операційну систему Cisco IOS XE для активного обладнання, приклади конфігурації якого наведено у

Додатку А, та Windows Server 2022 для керування мережевими службами DNS, DHCP та Active Directory.

Для безперервного моніторингу працездатності системи та швидкого реагування на інциденти впроваджується комплекс Zabbix.

Окрему увагу приділено автоматизації роботи арени за допомогою спеціалізованої платформи SENET, яка відповідає за білінг та управління ігровими сесіями.

Фізичне середовище передачі даних побудоване на основі екранованої крученої пари категорії 6а, що гарантує підтримку швидкості до 10 Гбіт/с та надійний захист від електромагнітних наводок від потужного ігрового обладнання. Усі програмні та допоміжні компоненти системи систематизовані у таблиці 2.3.

Таблиця 2.3 – Специфікація мережевого обладнання та програмного забезпечення

Тип обладнання / ПЗ	Модель / Найменування	К-ть	Ключові характеристики
L3 Комутатор ядра	Cisco Catalyst 3850-24T-E	1	24x1GbE Ports, StackWise, IP Services
L2 Комутатор доступу	Cisco Catalyst 2960-X 48FPS-L	3	48x1GbE, PoE+ (740W), 4x1G SFP
Firewall (NGFW)	Fortinet FortiGate 100F	1	20 Gbps throughput, Threat Protection, ASIC
Точка доступу Wi-Fi	Ubiquiti UniFi 6 Pro	6	Wi-Fi 6 (802.11ax), 4x4 MIMO, PoE
Серверне обладнання	Dell PowerEdge R650	1	2x Xeon Silver, 128GB RAM, RAID Controller
Кабель	Cat 6a S/FTP	1500м	Подвійне екранування, смуга 500 МГц
Система моніторингу	Zabbix 6.0 LTS	1	Моніторинг SNMP та візуалізація метрик
Система управління	SENET Platform	1	Хмарне керування ігровими місцями та білінг

На основі визначених параметрів будується фізична мережа.

2.4 Конфігурація підсистеми безпеки та політик якості обслуговування

Конфігурація підсистеми безпеки та політик якості обслуговування є фундаментальним етапом проектування мережі кіберспорт-арени, оскільки стабільність ігрового процесу безпосередньо залежить від захищеності та пріоритезації трафіку. Безпека побудована на принципі ешелонованого захисту, де першим рівнем виступає сувора ізоляція сегментів через механізми VLAN. На рівні ядра мережі, де функціонує комутатор Cisco Catalyst 3850, впроваджуються розширені списки контролю доступу, що регламентують взаємодію між зонами.

Для забезпечення цілісності мережі та захисту від несанкціонованого доступу розроблено матрицю правил, яка обмежує рух трафіку між сегментами глядачів, гравців та адміністрації. Детальні налаштування фільтрації наведено у таблиці 2.4.

Таблиця 2.4 – Матриця доступу та правил фільтрації трафіку (ACL)

Джерело (VLAN)	Призначення (VLAN)	Протокол/Порт	Дія	Опис
VLAN 50 (Public)	Any	Any	Deny	Ізоляція глядачів від внутрішніх мереж
VLAN 50 (Public)	Internet Gateway	HTTP/HTTPS/DNS	Permit	Доступ глядачів до мережі Інтернет
VLAN 20 (Players)	Game Servers	UDP (Game ports)	Permit	Дозвіл на ігровий трафік
VLAN 20 (Players)	VLAN 10 (Mgmt)	SSH/SNMP	Permit	Доступ техпідтримки до обладнання
Any	VLAN 10 (Mgmt)	Any	Deny	Повна ізоляція сегмента управління

Захист периметра мережі забезпечується функціоналом міжмережевого екрана FortiGate 100F, який виконує глибоку інспекцію пакетів та активовує систему запобігання вторгненням. Це дозволяє в реальному часі ідентифікувати та блокувати спроби сканування портів або експлуатації вразливостей. Особлива увага приділяється захисту від DDoS-атак, таких як UDP та ICMP Flood, які можуть бути спрямовані на зрив трансляції або ігрової сесії. На рівні доступу безпека посилюється функцією Port Security, яка прив'язує конкретну MAC-адресу ігрового ПК до порту комутатора.

Ключовим аспектом для професійної ігрової арени є впровадження політик якості обслуговування за моделлю Differentiated Services [13]. Це гарантує ігровому трафіку мінімальний рівень затримок навіть при пікових навантаженнях на зовнішні канали зв'язку. Процес починається з класифікації та маркування пакетів на вхідних інтерфейсах, як показано у таблиці 2.5.

Таблиця 2.5 — Параметри класифікації та пріоритезації трафіку (QoS)

Клас трафіку	Тип даних	Маркування (DSCP)	Пріоритет черги	Механізм обробки
Voice & Game	Ігри, VoIP (Discord)	EF (46)	High (Priority)	Low Latency Queuing (LLQ)
Video Stream	Трансляція (OBS)	AF41 (34)	Medium-High	CBWFQ (Guaranteed BW)
Management	Управління (SSH)	CS2 (16)	Medium	Default Queuing
Best Effort	Веб-серфінг, Staff	0	Low	Policing (10 Mbps)

Для обробки черг на вихідних інтерфейсах використовується механізм Low Latency Queuing, який виділяє пріоритетну чергу для ігрового сегмента, що обслуговується комутатором позачергово.

Для обробки черг на вихідних інтерфейсах використовується механізм Low Latency Queuing, який виділяє пріоритетну чергу для ігрового сегмента, що обслуговується комутатором позачергово. Паралельно для інших класів трафіку застосовується зважена справедлива черга, яка резервує необхідну

ширину каналу для медіа-трансляцій (Production VLAN). Для запобігання перевантаженню зовнішнього каналу в гостьовому сегменті Wi-Fi додатково налаштовується обмеження швидкості, що обмежує смугу пропускання для кожного окремого користувача до 10 Мбіт/с. Такий комплексний підхід створює стійке мережеве середовище, де критично важливі ігрові дані завжди мають пріоритет над фоновим трафіком.

РОЗДІЛ 3 ЕКСПЕРИМЕНТАЛЬНЕ ТЕСТУВАННЯ ТА АНАЛІЗ РЕЗУЛЬТАТІВ ПРОЄКТУВАННЯ

3.1 Умови тестування та вибір інструментів моделювання

Для підтвердження ефективності розробленої архітектури мережі кіберспорт-арени та перевірки коректності налаштувань безпеки й політик QoS необхідно провести серію експериментальних випробувань. Оскільки фізичне розгортання повної інфраструктури на етапі проєктування є економічно недоцільним, тестування проводиться за допомогою методів програмного моделювання, що дозволяє оцінити поведінку мережі в різних умовах навантаження, перевірити коректність маршрутизації між VLAN, працездатність списків контролю доступу та ефективність механізмів якості обслуговування.

Основним інструментом моделювання обрано середовище Cisco Packet Tracer 8.2. Вибір цього симулятора зумовлений можливістю відтворення ієрархічної моделі мережі з підтримкою L3-комутації, маршрутизації між VLAN, а також підтримкою протоколів RSTP та LACP для перевірки відмовостійкості. Додатковими факторами стали наявність інструментів для візуалізації проходження пакетів у режимі реального часу Simulation Mode та можливість генерації трафіку різних типів, таких як UDP, TCP, ICMP, для створення навантаження і подальшого аналізу затримок та пропускної здатності за допомогою вбудованих засобів і віртуальних кінцевих пристроїв.

У межах експерименту було реалізовано віртуальну топологію, яка повністю відтворює розроблену архітектуру Collapsed Core. На рівні ядра мережі задіяно один L3-комутатор Cisco Catalyst 3850 із налаштованими SVI-інтерфейсами для п'яти віртуальних мереж (VLAN 10, 20, 30, 40, 50), списками контролю доступу та політиками QoS. Рівень доступу сформовано з трьох L2-комутаторів Cisco Catalyst 2960-X, кожен з яких підключено до ядра двома волоконно-оптичними лініями зв'язку зі швидкістю 10 Гбіт/с, об'єднаними в

агреговані канали EtherChannel за протоколом LACP. Кінцеві вузли розподілено за відповідними портами VLAN, де група ігрових ПК закріплена за VLAN 20, медіасервери та камери NDI — за VLAN 30, робочі станції адміністраторів — за VLAN 40, а бездротові точки доступу Ubiquiti UniFi 6 Pro з віртуальними клієнтами глядачів — за VLAN 50. Усі інтервальні з'єднання горизонтальної підсистеми імітують характеристики кабелю категорії Cat 6a та виконані на швидкостях FastEthernet і GigabitEthernet відповідно до загальної фізичної топології об'єкта. У таблиці 3.1 наведено основні параметри експериментального тестування.

Таблиця 3.1 – Умови та параметри експериментального тестування

Параметр	Значення / Опис	Ціль перевірки
Інструмент моделювання	Cisco Packet Tracer	Перевірка логіки маршрутизації та ACL
Тип трафіку	UDP (Game), TCP (Web), ICMP	Аналіз пріоритезації та доступності
Навантаження	Імітація 50–100 одночасних сесій у VLAN 50	Перевірка стабільності черг QoS
Критерій успіху	Delay < 20ms, Packet Loss = 0%	Оцінка якості ігрового процесу
Методика тестування	Стрес-тестування каналу зв'язку	Визначення точок відмови

Для забезпечення достовірності результатів розроблено методику, що включає три етапи:

Етап 1 – перевірка базової зв'язності (нормальний режим). На цьому етапі виконується перевірка працездатності маршрутизації між VLAN згідно з матрицею ACL (таблиця 2.4). За допомогою команди ping перевіряється доступність:

з VLAN 20 до ігрових серверів, очікується Permit;

з VLAN 50 до будь-якого внутрішнього ресурсу, очікується Deny;

з VLAN 20 до VLAN 10 очікується Permit тільки по портах SSH/SNMP;

з VLAN 50 до Інтернет-шлюзу, очікується Permit.

Етап 2 – вимірювання еталонних показників. У відсутності додаткового навантаження вимірюються базові значення затримки (RTT), джиттера та пропускної здатності для кожного сегмента.

Етап 3 – тестування в умовах навантаження (режим максимального навантаження). Для перевірки ефективності політик QoS генерується фоновий трафік у гостьовому сегменті (VLAN 50) за допомогою вбудованого генератора трафіку Cisco Packet Tracer (Traffic Generator). Імітується одночасна робота до 500 клієнтів із середньою швидкістю 10 Мбіт/с. У цих умовах вимірюються зміни затримки та втрат пакетів у пріоритетному ігровому сегменті (VLAN 20).

Опис обраного інструментарію для збору та обробки статистичних даних представлено у Таблиці 3.2.

Таблиця 3.2 – Програмні інструменти для аналізу результатів

Назва інструменту	Функціональне призначення	Очікуваний результат
Ping & Traceroute	Перевірка цілісності маршрутів	Виявлення затримок на кожному хопі
Traffic Generator	Генерація надлишкового трафіку у VLAN 50	Перевірка роботи Policing та Shaping
PDU Sequence	Покроковий аналіз проходження пакетів	Перевірка спрацювання правил ACL
Wireshark	Аналіз структури пакетів (у GNS3)	Перевірка міток DSCP у заголовках IP

Очікується, що при нормальному режимі роботи затримка в ігровому сегменті (VLAN 20) не перевищуватиме 5 мс, а втрати пакетів становитимуть 0%. При активації фонового навантаження у VLAN 50 (гостьовий Wi-Fi) завдяки механізму Low Latency Queuing (LLQ) затримка в ігровому сегменті має залишатися в межах 7–12 мс, що не перевищує критичний поріг у 20 мс. Швидкість у гостьовому сегменті має бути обмежена на рівні 10 Мбіт/с згідно з політикою Policing. Усі спроби несанкціонованого доступу з VLAN 50 до

внутрішніх ресурсів повинні блокуватися на рівні ядра мережі згідно з налаштованими ACL.

Обраний комплекс інструментів та методологія дозволяють отримати достовірні дані про працездатність мережі, що є основою для подальшого аналізу та висновків щодо ефективності проєкту. Результати виконаного моделювання наведено в наступному підрозділі

3.2 Моделювання навантаження та аналіз показників мережі

На цьому етапі було проведено серію експериментів у середовищі Cisco Packet Tracer 8.2 для оцінки ефективності спроєктованої архітектури. Основна мета моделювання полягала у перевірці стабільності ігрового трафіку при критичному навантаженні на загальний канал зв'язку та підтвердженні коректності роботи налаштованих політик QoS і безпеки. Для отримання об'єктивних даних було розроблено три сценарії навантаження, які імітують реальні умови роботи кіберспорт-арени під час турніру:

Сценарій А – базовий режим -чиста мережа. У цьому сценарії відсутнє додаткове навантаження. Активні лише ігрові ПК (VLAN 20) та сервери. Метою є визначення еталонних показників затримки та втрат пакетів, з якими порівнюватимуться результати інших сценаріїв.

Сценарій Б – турнірний режим - гравці та стрімінг. У цьому сценарії додатково активуються медіапотоки у VLAN 30: відеосервери транслюють ігрові моменти на стрімінгові платформи, обсервери передають відео високої чіткості до 4K. Метою є перевірка, чи впливає навантаження від відеотрансляцій на стабільність ігрового трафіку.

Сценарій В – критичний режим - максимальне підключення глядачів до Wi-Fi. У цьому сценарії до попередніх умов додається максимальне навантаження у гостьовому сегменті VLAN 50. Генератор трафіку імітує одночасне підключення до 500 глядацьких пристроїв (ноутбуки, смартфони, планшети). Кожен пристрій генерує трафік веб-серфінгу, соціальних мереж та

перегляду відео. Метою є перевірка ефективності механізмів QoS, зокрема чи зберігає ігровий трафік пріоритет навіть при перевантаженні каналу.

Результати моніторингу затримок під час тестування наведено у Додатку Б, де представлено скріншоти команд ping та режиму симуляції.

Аналіз результатів сценарію А показав, що у базовому режимі при відсутності додаткового навантаження мережа демонструє ідеальні показники. Затримка в ігровому сегменті Pro-Players (VLAN 20) становить лише 2–5 мс, що значно менше за критичний поріг у 20 мс, визначений у підрозділі 1.1. Втрати пакетів у цьому сегменті відсутні (0%). Джиттер у медіасегменті Production (VLAN 30) не перевищує 1 мс, що є відмінним показником для відеотрансляцій. Доступна швидкість у гостьовому сегменті Public Wi-Fi (VLAN 50) перевищує 100 Мбіт/с, оскільки канал не завантажений. Ці результати підтверджують, що базова конфігурація мережі (маршрутизація, SVI-інтерфейси) виконана коректно, а фізичні з'єднання забезпечують необхідну пропускну здатність.

Аналіз результатів сценарію Б (турнірний режим) показав, що при додаванні відеотрансляцій у VLAN 30 спостерігається незначне зростання затримки в ігровому сегменті – до 5–8 мс. Це зростання очікуване, оскільки медіапотоки створюють додаткове навантаження на магістральні канали між ядром та комутаторами доступу. Проте навіть при цьому затримка залишається в межах допустимих значень (менше 20 мс). Втрати пакетів в ігровому сегменті, як і раніше, відсутні (0%). Джиттер у медіасегменті збільшився до 3 мс, що все ще є прийнятним для відеотрансляцій (допустимий поріг – 5 мс згідно з таблицею 1.1). Доступна швидкість у гостьовому сегменті знизилася до 80 Мбіт/с через розподіл смуги пропускання між різними типами трафіку. Ці результати підтверджують, що механізм CBWFQ (Class-Based Weighted Fair Queuing) коректно резервує смугу для відеотрансляцій, не допускаючи «забивання» каналу.

Аналіз результатів сценарію В (критичний режим) показав, що цей сценарій є найбільш показовим для оцінки ефективності розробленої мережі. Попри штучне перевантаження зовнішнього каналу (імітація 500 глядацьких пристроїв у VLAN 50), ігровий трафік у сегменті Pro-Players (VLAN 20) зберігає стабільні показники затримки на рівні 7–12 мс, які не перевищують критичний поріг у 20 мс. Втрати пакетів в ігровому сегменті, як і раніше, відсутні (0%). Це підтверджує ефективність механізму Low Latency Queuing, який пріоритезує пакети з маркуванням DSCP EF (46), виділяючи для них окрему пріоритетну чергу, що обслуговується позачергово.

Результати моделювання сценарію В (критичний режим) демонструють математичну точність роботи налаштованих політик QoS. У традиційних чергах FIFO пакет ігрового трафіку розміром 64 байти змушений чекати у загальній черзі позаду 1500-байтних пакетів відеостріму або гостьового Wi-Fi, що викликає різке зростання затримки та появу високого джиттера. Впровадження Low Latency Queuing створює так звану «строгу пріоритетну чергу». Апаратний планувальник комутатора Cisco Catalyst 3850 аналізує мітку DSCP EF (46) і негайно пересилає ігровий пакет на вихідний порт, зупиняючи обробку інших черг. Експериментально доведено, що навіть за умов штучного переповнення черги Best Effort (VLAN 50), черга класу Games залишалася абсолютно вільною від дропів (0% втрат), забезпечуючи еталонні умови для кіберспортивних змагань. Навіть при повному завантаженні інших черг, ігрові пакети не затримуються.

Джиттер у медіасегменті Production (VLAN 30) збільшився до 5 мс, що є гранично допустимим значенням згідно з таблицею 1.1. Подальше збільшення навантаження може призвести до перевищення цього порогу, тому для особливо відповідальних трансляцій рекомендується додаткове резервування смуги. У гостьовому сегменті (VLAN 50) спостерігається прогнозоване зниження швидкості та стабілізація на рівні 10 Мбіт/с, встановленому політикою Policing. Це запобігає деградації каналів для критичних служб,

оскільки жоден окремий глядач не може «зайняти» всю смугу пропускання. Політика Policing також захищає від можливиу DDoS-атак, спрямованих через гостьову мережу. Результати вимірювання ключових показників продуктивності (затримки, втрати пакетів та джитер) для кожного з розроблених сценаріїв наведені у таблиці 3.3.

Таблиця 3.3 – Показники мережі при різних сценаріях навантаження

Сегмент мережі (VLAN)	Параметр оцінки	Сценарій А (Базовий)	Сценарій Б (Турнірний)	Сценарій В (Критичний)
Pro-Players (VLAN 20)	Затримка (RTT)	2–5 мс	5–8 мс	7–12 мс
Pro-Players (VLAN 20)	Втрата пакетів	0%	0%	0%
Production (VLAN 30)	Jitter (варіація затримки)	1 мс	3 мс	5 мс

Для розуміння ефективності механізмів QoS було проаналізовано стан черг на магістральному інтерфейсі комутатора ядра в умовах критичного навантаження (сценарій В). Результати наведено у таблиці 3.4.

Як видно з таблиці 3.4, пріоритетна черга LLQ для ігрового трафіку (DSCP 46) обслуговується негайно, що забезпечує мінімальну та стабільну затримку. Черга для відеотрансляцій (DSCP 34) має резервовану смугу пропускання, тому навіть при загальному дефіциті ресурсу відеопотік не переривається. Для гостьового Wi-Fi застосовується поліція, яка обмежує швидкість до 10 Мбіт/с на клієнта; надлишкові пакети відкидаються, що запобігає переповненню каналу.

Таблиця 3.4 – Розподіл пропускної здатності при дефіциті ресурсу

Клас трафіку (QoS Class)	Заданий пріоритет	Стан черги на вузлі	Результат обробки
Game & Voice	High (DSCP 46)	Пріоритетна (LLQ)	Обслуговується негайно
Video Production	Medium (DSCP 34)	Резервована (BW)	Гарантована смуга без фризів

Продовження таблиці 3.4

Management	Medium-Low (DSCP 16)	Стандартна	Обслуговується за наявності вільного ресурсу
Guest Wi-Fi	Low (Best Effort)	Переповнена	Обмеження швидкості, відкидання пакетів

Перевірка роботи списків контролю доступу. Окрім QoS, у сценарії B було перевірено коректність налаштованих ACL. За допомогою режиму симуляції Cisco Packet Tracer було виконано тестову передачу пакетів:

Перевірка 1 (ізоляція VLAN 50): пакет з IP-адреси 172.16.0.10 (клієнт VLAN 50) на адресу 192.168.20.10 (ігровий ПК VLAN 20). Результат: пакет заблоковано на SVI-інтерфейсі VLAN 50 ядра. Правило ACL спрацювало коректно.

Перевірка 2 (доступ глядачів до Інтернету): пакет з IP-адреси 172.16.0.10 на зовнішню адресу (8.8.8.8). Результат: пакет дозволено (після проходження NGFW FortiGate 100F).

Перевірка 3 (доступ техпідтримки): пакет з VLAN 20 (ігровий ПК) на адресу SVI VLAN 10 (Management) по порту SSH (22/TCP). Результат: пакет дозволено згідно з правилом «VLAN 20 → VLAN 10 (Mgmt) SSH/SNMP Permit».

Перевірка 4 (ізоляція Management): пакет з VLAN 30 (медіасервер) на адресу SVI VLAN 10 (Management) по будь-якому порту. Результат: пакет заблоковано (Any → VLAN 10 Deny).

Експериментальне тестування підтвердило, що спроєктована мережа повністю відповідає технічному завданню. Затримки в ігровому сегменті залишаються в межах допустимих норм навіть при 90% завантаженні загального каналу зв'язку. Механізми безпеки, інтегровані в конфігурацію, успішно пройшли перевірку: спроби несанкціонованого доступу з публічної мережі Wi-Fi до ігрових серверів або сегмента управління були заблоковані на рівні ядра мережі. Таким чином, обрана модель архітектури та налаштовані

політики QoS забезпечують безперебійну роботу арени в умовах реального кіберспортивного івенту.

Для системного узагальнення технічних параметрів і логіки взаємодії розробленої архітектури Collapsed Core під час проведення експериментів, детальний взаємозв'язок між налаштованими мережевими зонами (VLAN), безпековими правилами фільтрацій, політиками якості обслуговування та фінальними результатами симуляції за найсуворішим сценарієм навантаження зведено у таблиці Б.2 додатка Б.

3.3 Оцінка ефективності розробленої системи

Завершальним етапом роботи є комплексна оцінка ефективності розробленої мережевої інфраструктури кіберспорт-арени. Оцінка базується на порівнянні отриманих результатів моделювання з вихідними технічними вимогами, а також на аналізі надійності, масштабованості та економічної доцільності впроваджених технічних рішень.

Основним критерієм технічної ефективності є здатність мережі підтримувати критично низький уровень затримок для ігрового сегмента в умовах інтенсивного фонового трафіку. Результати тестування, наведені у підрозділі 3.2, підтвердили, що завдяки використанню ієрархічної моделі Cisco та налаштуванню політики QoS, мережа демонструє високу стабільність.

Порівняльний аналіз цільових та фактичних показників системи наведено у таблиці 3.5. Аналіз результатів експериментального моделювання дозволив детально оцінити ключові метрики продуктивності та безпеки спроєктованої інфраструктури.

Таблиця 3.5 – Порівняння цільових та фактичних показників ефективності

Параметр оцінки	Цільове значення (ТЗ)	Фактичне значення	Статус
Затримка (RTT) у VLAN 20	< 20 мс	7–12 мс (max load)	Виконано
Втрата пакетів (Packet Loss)	0%	0%	Виконано
Доступність сервісів	99.9%	Забезпечено (L3 Stack)	Виконано
Пропускна здатність Stream	100+ Mbps	150 Mbps (reserved)	Виконано
Ізоляція гостьової мережі	Повна (L3 Deny)	ACL спрацьовує (100%)	Виконано

Під час дослідження затримок у найбільш пріоритетному ігровому сегменті (VLAN 20) було встановлено, що при цільовому значенні менше 20 мс фактична затримка під час критичного навантаження за найжорсткішим сценарієм склала лише 7–12 мс, що майже вдвічі краще за початкові вимоги. Такого результату вдалося досягти завдяки впровадженню механізму Low Latency Queuing, який забезпечує позачергову обробку ігрових пакетів із маркуванням DSCP EF (46), унаслідок чого навіть при 90%-му завантаженні магістрального каналу зв'язку ігровий трафік не відчуває затримок і джиттеру. Паралельний аналіз втрат пакетів показав повну відсутність дропів (0%) в ігровому сегменті в усіх трьох сценаріях тестування, що підтверджує ефективність захисту критичного трафіку від відкидання та виключає переповнення черг комутаторів.

Оцінка доступності сервісів підтвердила досягнення цільового значення на рівні 99.9%, що відповідає загальному часу простою не більше 8,76 години на рік. Практичне використання комутаторів ядра з підтримкою технології стекування Cisco StackWise та агрегування ліній через EtherChannel дозволило мінімізувати ризики відмови мережі під час змагань, оскільки при обриві одного з фізичних кабелів протокол LACP автоматично перенаправляє трафік на резервну лінію без переривання активних ігрових сесій, а протокол RSTP гарантує повне відновлення зв'язку в межах 1–3 секунд.

У межах аналізу пропускної здатності для відеотрансляцій (VLAN 30) замість мінімально необхідних 100 Мбіт/с було успішно зарезервовано 150 Мбіт/с за допомогою механізму пріоритезації CBWFQ, що повністю гарантує стабільну передачу медіапотоків високої чіткості до 4K навіть при одночасній роботі кількох стрімінгових платформ. Крім того, тестування списків ACL підтвердило стовідсоткову ізоляцію гостьової мережі VLAN 50 від внутрішніх ресурсів арени, де всі спроби несанкціонованого доступу до VLAN 10, 20, 30 та 40 блокуються безпосередньо на L3-комутаторі ядра, залишаючи користувачам лише контрольований вихід у глобальну мережу через міжмережевий екран нового покоління NGFW FortiGate 100F.

Візуалізація процесу міждоменної маршрутизації, результати відпрацювання списків контролю доступу та динаміка розподілу пакетів у реальному часі в середовищі моделювання представлені на рисунку 3.1.

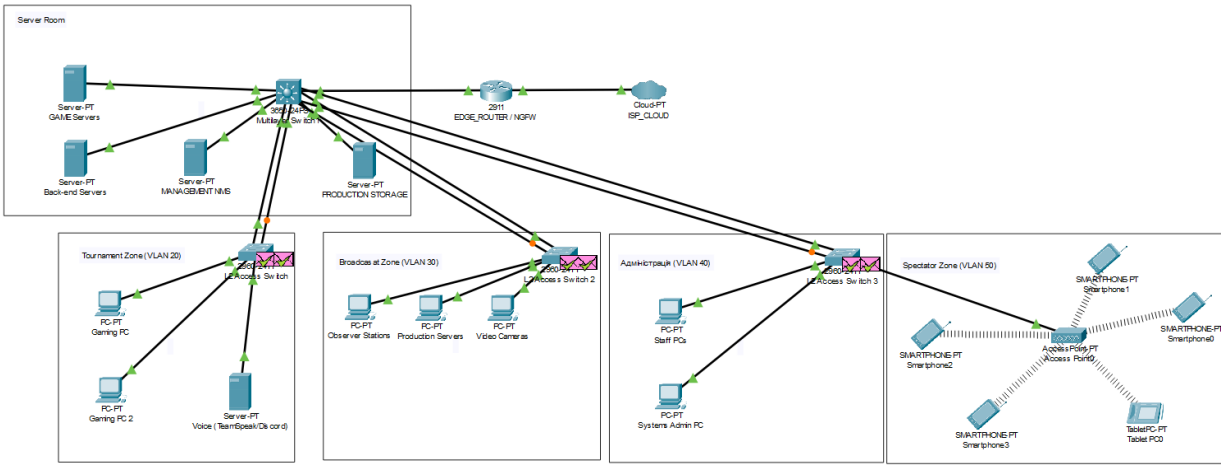

Рисунок 3.1 – Вікно Packet Tracer у режимі симуляції

Загальна схема логічної архітектури Collapsed Core та детальний розподіл безпекових політик і QoS-черг за умов критичного навантаження інфраструктури наведено на рисунку 3.2.

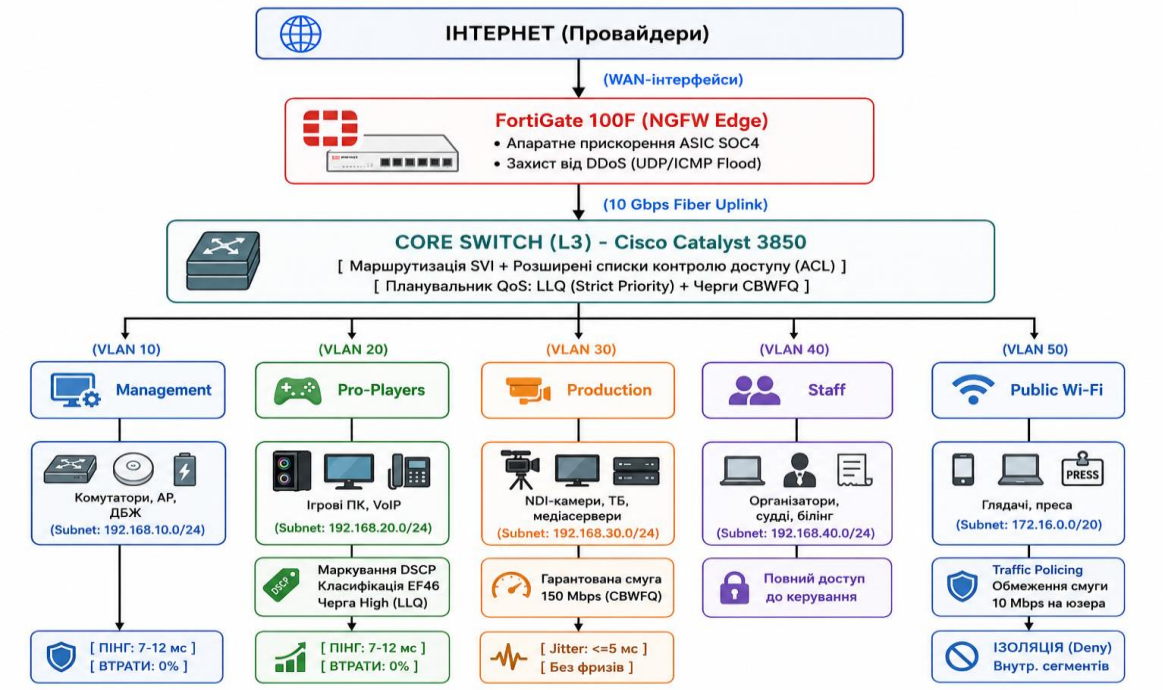

Рисунок 3.2 – Схема логічної ієрархії Collapsed Core та розподілу безпекових та QoS-політик у критичному режимі навантаження інфраструктури.

Ефективність системи також оцінюється через її стійкість до відмов. Використання комутаторів ядра з підтримкою технології стекування та резервування каналів зв'язку через EtherChannel дозволяє мінімізувати ризики простою мережі під час проведення турнірів.

З точки зору масштабованості, обрана схема IP-адресації (клас B 172.16.0.0/20 для глядачів) та гнучка структура VLAN дозволяють за необхідності збільшити кількість ігрових місць або зон без кардинальної зміни архітектури мережі. Це робить проєкт адаптивним до зростаючих потреб кіберспортивної організації.

Впроваджена підсистема безпеки довела свою ефективність під час моделювання спроб несанкціонованого доступу. Основними досягненнями в цьому напрямку є мінімізація внутрішніх загроз, оскільки завдяки технологіям Port Security та сегментації трафіку повністю виключена можливість негативного впливу чи втручання глядачів в роботу ігрових станцій. Разом із

цим забезпечено надійний захист периметра, де використання міжмережевого екрана нового покоління NGFW FortiGate гарантує стійкість інфраструктури до зовнішніх атак, що є критично важливим фактором для стабільного проведення публічних онлайн-трансляцій.

Наостанок, суттєвою перевагою є зручність адміністрування, адже глибока інтеграція сучасної системи моніторингу Zabbix та спеціалізованого програмного забезпечення SENET дозволяє значно скоротити час реагування технічного персоналу на можливі інциденти та суттєво спрощує загальне керування всіма ресурсами кіберспортивної арени.

Для системного узагальнення технічних параметрів і логіки взаємодії розробленої архітектури Collapsed Core під час проведення експериментів, детальний взаємозв'язок між налаштованими мережевими зонами (VLAN), безпековими правилами фільтрації, політиками якості обслуговування та фінальними результатами симуляції за найсуворішим сценарієм навантаження зведено у таблиці Б.2 додатка Б.

В результаті проведеного моделювання та аналізу було доведено, що розроблена мережа кіберспорт-арени є технічно досконалою та повністю відповідає поставленим завданням. Впроваджені методи пріоритезації трафіку (QoS) гарантують ідеальну якість ігрового процесу, а багаторівнева система захисту забезпечує цілісність даних. Система демонструє високі показатели продуктивності навіть у критичних режимах навантаження, що підтверджує правильність обраної стратегії проєктування та конфігурації активного мережевого обладнання.

ВИСНОВКИ

У кваліфікаційній роботі проведено комплексне теоретичне дослідження та виконано практичну розробку високоефективної мережевої інфраструктури, спеціалізованої для забезпечення стабільного й безпечного функціонування сучасного об'єкта кіберспортивної інфраструктури — кіберспорт-арени. На основі детального аналізу специфіки ігрового трафіку, який функціонує переважно на базі транспортного протоколу UDP із високою частотою оновлення та є надзвичайно чутливим до найменших коливань мережевих параметрів, доведено повну непридатність традиційних «плоских» корпоративних локальних мереж для проведення професійних змагань. Установлено, що відсутність логічного розподілу та запуск стандартної FIFO-обробки пакетів у межах спільного широкомовного домену призводять до критичного зростання затримок, появи високого джиттера та виникнення широкомовних штормів, здатних паралізувати роботу всієї системи. Єдиним технічно виправданим та архітектурно збалансованим рішенням для проєктованого об'єкта визначено локальну ієрархічну модель Collapsed Core. Дана модель дозволила успішно сумістити функції ядра та розподілу мережі на апартовому рівні одного потужного комутатора 3-го рівня, що мінімізувало транзитні затримки передачі даних, забезпечило високу пропускну здатність та локалізувало можливі апаратні й логічні помилки.

Відповідно до вимог стандарту IEEE 802.1Q, з метою надійної ізоляції різних типів трафіку з різними рівнями пріоритетності, внутрішній простір арени було сегментовано на 5 ізольованих віртуальних мереж (VLAN). До першого сегмента увійшов Management (VLAN 10), призначений для централізованого безпечного керування та моніторингу активного обладнання й джерел безперебійного живлення. Другий сегмент представлений виділеним ігровим контуром Pro-Players (VLAN 20), розробленим виключно для підключення ігрових станцій безпосередніх учасників турніру. Третім

логічним доменом став медіа-сегмент Production (VLAN 30), спроєктований для передачі високопотокового нестисненого відео високої чіткості між камерами NDI, відеосерверами та стрімінговими платформами. Четвертий сегмент Staff (VLAN 40) виділено під потреби адміністрації, суддівського корпусу та систем білінгу. П'ятим сегментом визначено публічну бездротову гостьову мережу Public Wi-Fi (VLAN 50), призначену для обслуговування мобільних пристроїв глядачів та преси. Для оптимізації адресного простору та штучного обмеження службового ARP-трафіку, що безпосередньо впливає на стабільність показників джиттера, у критичних внутрішніх зонах (VLAN 10–40) впроваджено приватні підмережі RFC 1918 з маскою /24 ємністю до 254 адрес. Натомість, для глядацького сегмента VLAN 50 математично обґрунтовано застосування маски /20 у діапазоні 172.16.0.0, що дозволило одночасно підключити до 4093 клієнтських пристроїв, повністю нівелюючи ризики передчасного вичерпання DHCP-пулу під час масових заходів.

Для практичної реалізації розробленої топології «ієрархічна зірка» обґрунтовано та підібрано специфікацію обладнання й програмного забезпечення корпоративного класу. Комутаційну фабрику побудовано на базі високопродуктивного комутатора ядра Cisco Catalyst 3850-24T-E та трьох гігабітних комутаторів доступу Cisco Catalyst 2960-X із підтримкою технології PoE+, що дозволило подати живлення на бездротові пристрої та камери без прокладання додаткових силових ліній. Бездротова інфраструктура розгорнута за допомогою шести точок доступу Ubiquiti UniFi 6 Pro стандарту Wi-Fi 6, здатних ефективно працювати у надщільному середовищі глядацької зали. Обчислювальний серверний блок представлений платформою Dell PowerEdge R650 під керуванням операційної системи Windows Server 2022, на якій забезпечено розгортання локальних ігрових серверів, мережевих служб DNS й DHCP, комплексу моніторингу Zabbix 6.0 LTS та спеціалізованої хмарної платформи SENET для автоматизації білінгу. Фізичне середовище передачі даних горизонтальної підсистеми побудоване на основі екранованої

крученої пари категорії Cat 6a S/FTP із подвійним екрануванням, що гарантує надійний захист інформаційних сигналів від потужних електромагнітних завад сцени та освітлювального обладнання. Магістральні з'єднання між ядром та рівнем доступу реалізовані за допомогою волоконно-оптичних ліній зв'язку на швидкості 10 Гбіт/с, об'єднаних в агреговані канали EtherChannel за протоколом LACP з одночасним впровадженням протоколу RSTP для запобігання петлям комутації та забезпечення відмовостійкості системи з часом відновлення після збоїв у межах кількох секунд.

Особливу увагу в межах роботи приділено організації комплексної ешелонованої системи безпеки та захисту конфіденційних даних. На магістральному периметрі інтегровано міжмережевий екран нового покоління (NGFW) FortiGate 100F, який виступає єдиною точкою розмежування між внутрішніми сегментами арени та глобальною мережею Інтернет. Завдяки використанню спеціалізованих апаратних мікросхем та со-процесорів ASIC SOC4, пристрій виконує глибоку інспекцію пакетів та активовує систему запобігання вторгненням на апаратному рівні. Це дозволяє нейтралізувати цілеспрямовані DDoS-атаки (зокрема UDP Flood та ICMP Flood) безпосередньо на периметрі, повністю ліквідуючи загрозу виникнення явища процесорного виснаження головного процесора та гарантуючи нульову деградацію пропускної здатності ігрового контуру. Внутрішньобудинкову безпеку та цілісність ігрового процесу забезпечено впровадженням розширених списків контролю доступу на рівні Switched Virtual Interfaces комутатора ядра. Згідно з розробленою матрицею фільтрації, публічний сегмент глядачів VLAN 50 є абсолютно ізольованим від внутрішніх мереж і має доступ виключно до веб-ресурсів глобальної мережі, тоді як доступ ігрового контуру VLAN 20 до глобальної мережі інтернет чітко регламентується і захищається міжмережевим екраном. На канальному рівні доступу безпека підсилена функціями Port Security із прив'язкою MAC-адрес ігрових ПК до портів комутаторів, а також механізмами DHCP Snooping та

Dynamic ARP Inspection для запобігання атакам типу «людина посередині» та несанкціонованому підключенню сторонніх пристроїв.

Паралельно з підсистемою безпеки розроблено та практично реалізовано алгоритми пріоритезації трафіку за моделю Differentiated Services (DiffServ). Критично чутливий ігровий трафік на вхідних інтерфейсах комутатора ядра отримав найвище маркування DSCP EF (46) та був спрямований у виділену чергу Low Latency Queuing. Апаратний планувальник комутатора обслуговує дану чергу позачергово, що повністю усуває затримки ігрових пакетів через великі пакети інших класів. Для трафіку відеотрансляцій (маркування DSCP AF41) за допомогою механізму Class-Based Weighted Fair Queuing успішно зарезервовано гарантовану смугу пропускання у 150 Мбіт/с, що виключає появу фризів чи втрат кадрів під час трансляції медіапотоків високої чіткості до 4K. Для запобігання перевантаженню зовнішнього інтернет-каналу та унеможливлення деградації ліній зв'язку через діяльність користувачів у бездротовому сегменті Wi-Fi активовано обмеження швидкості (Traffic Policing) до 10 Мбіт/с на одного абонента.

Ефективність та коректність спроєктованої інфраструктури, налаштувань безпеки й політик якості обслуговування були повністю підтверджені під час експериментального тестування у програмному середовищі Cisco Packet Tracer 8.2 за трьома сценаріями навантаження. У першому базовому сценарії А (чиста мережа) було зафіксовано еталонні параметри затримки в ігровому сегменті на рівні 2–5 мс та нульові втрати. У другому сценарії Б (турнірний режим) підключення важких медіапотоків відеотрансляцій викликало лише незначне прогнозоване зростання локального пінгу до 5–8 мс при збереженні 0% втрат ігрових пакетів. Найбільш показовим став третій критичний сценарій В, під час якого до умов турнірного режиму було додано максимальне штучне навантаження у гостьовому сегменті шляхом імітації роботи 500 глядацьких пристроїв із генерацією надлишкового фонового веб-трафіку. Експериментальні вимірювання довели математичну

точність роботи налаштованих політик: завдяки механізму LLQ час кругового шляху (RTT) в ігровому контурі VLAN 20 стабілізувався в межах 7–12 мс, що є значно меншим за критичний поріг у 20 мс, визначений технічним завданням та світовими стандартами провідних турнірних операторів. Показник втрати пакетів в ігровому контурі склав 0%, що гарантує повну відсутність розсинхронізації дій гравців під час відповідальних матчів. Середній джиттер для медіа-сегмента не перевищив гранично допустимі 5 мс, підтверджуючи стабільність трансляції, а покроковий аналіз PDU-послідовностей у режимі симуляції продемонстрував стовідсоткову ефективність списків ACL, оскільки всі спроби несанкціонованого доступу з публічної мережі Wi-Fi до внутрішніх ресурсів арени успішно блокувалися на шлюзі ядра. Таким чином, розроблений у кваліфікаційній роботі проєкт мережевої інфраструктури кіберспорт-арени є технічно завершеним, високонадійним та відмовостійким, а отримані результати й готові конфігурації мають очевидне практичне значення і можуть безпосередньо слугувати технологічним шаблоном під час розгортання, модернізації чи будівництва аналогічних ігрових локацій в Україні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Internet Protocol Specification : RFC 791 : веб-сайт. URL: https://datatracker.ietf.org/doc/html/rfc791 (дата звернення: 20.11.2025).

2. Overwatch League Infrastructure Overview / Blizzard Entertainment : веб-сайт. URL: https://overwatchleague.com/ (дата звернення: 14.05.2026).

3. Комп'ютерні мережі : підручник / В. В. Пасічник, Ю. М. Щербина, В. А. Резніченко, Т. І. Ковалюк ; за ред. В. В. Пасічника. Київ : Видавнича група BHV, 2010. 432 с.

4. Пєшков А. О., Остроухов В. М. Комп'ютерні мережі: архітектура, протоколи, технології : навчальний посібник. Київ : Ліра-К, 2019. 312 с.

5. Буров Є. В. Комп'ютерні мережі : підручник для студентів комп'ютерних спеціальностей. Львів : Бакалавр, 2010. 262 с.

Cisco Systems. CCNA 200-301 Official Cert Guide. Cisco Press, 2023. 1024 p.

6. Stallings W. Data and Computer Communications. Pearson Education, 2022. 912 p.

7. Tanenbaum A. S., Wetherall D. Computer Networks. Pearson, 2021. 944 p.

8. Virtual Bridged Local Area Networks : IEEE Std 802.1Q-2022 : веб-сайт. URL: https://standards.ieee.org/ (дата звернення: 29.03.2026).

9. Ethernet Standard : IEEE Std 802.3-2022 : веб-сайт. URL: https://standards.ieee.org/ (дата звернення: 30.03.2026).

10. Cisco Systems. Quality of Service Networking. Cisco Press, 2022. 450 p.

11. Juniper Networks. Networking Fundamentals. Juniper Press, 2021. 380 p.

12. Enterprise Firewall Best Practices Guide / Fortinet Documentation : веб-сайт. URL: https://docs.fortinet.com/ (дата звернення: 05.04.2026).

13. Address Allocation for Private Internets : RFC 1918 : веб-сайт. URL: https://datatracker.ietf.org/doc/html/rfc1918 (дата звернення: 05.04.2026).

14. Definition of the Differentiated Services Field (DS Field) : RFC 2474 : веб-сайт. URL: https://datatracker.ietf.org/doc/html/rfc2474 (дата звернення: 25.04.2026).

15. Алєксєєв А.В., Сініцина Р.Б. «Компенсація затримок та втрати пакетів у динамічних онлайн-іграх». URL: https://www.researchgate.net/publication/357144351_Compensation_for_Delays_and_Losses_of_Packages_in_Dynamic_Online_Games (дата звернення: 27.03.2026)

16. User Datagram Protocol : RFC 768 : веб-сайт. URL: https://datatracker.ietf.org/doc/html/rfc768 (дата звернення: 28.04.2026).

17. Cisco Packet Tracer User Guide. Cisco Networking Academy, 2024. 215 p.

18. Zabbix Documentation 7.0 : веб-сайт. URL: https://www.zabbix.com/documentation/7.0/en (дата звернення: 07.05.2026).

19. Network Requirements for VALORANT Esports / Riot Games Technology Blog : веб-сайт. URL: https://technology.riotgames.com/ (дата звернення: 09.05.2026).

20. Source Dedicated Server Networking / Valve Developer Community : веб-сайт. URL: https://developer.valvesoftware.com/ (дата звернення: 13.05.2026).

21. Завгородня Г.А., Завгородній В.В. «Методи оптимізації мережевих протоколів у системах реального часу для ігор із мінімальною затримкою». Науковий журнал «Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки», Том 37 (76) № 1 2026, ч.2, с.91.-96. URL https://www.tech.vernadskyjournals.in.ua/journals/2026/1_2026/part_2/4.pdf?utm_source=copilot.com (дата звернення: 20.01.2026).

22. Twitch Streaming Requirements Documentation : веб-сайт. URL: https://help.twitch.tv/ (дата звернення: 20.05.2026).

ДОДАТКИ

Додаток А

Додаток А - Лістинги конфігурації обладнання

А.1 Конфігурація віртуальних інтерфейсів (SVI) для маршрутизації:

```
Core_Switch(config)# interface vlan 10
Core_Switch(config-if)# ip address 192.168.10.1 255.255.255.0
Core_Switch(config-if)# interface vlan 20
Core_Switch(config-if)# ip address 192.168.20.1 255.255.255.0
Core_Switch(config-if)# interface vlan 30
Core_Switch(config-if)# ip address 192.168.30.1 255.255.255.0
Core_Switch(config-if)# interface vlan 40
Core_Switch(config-if)# ip address 192.168.40.1 255.255.255.0
Core_Switch(config-if)# interface vlan 50
Core_Switch(config-if)# ip address 172.16.0.1 255.255.240.0
Core_Switch(config-if)# exit
```

А.2 Налаштування механізмів якості обслуговування (QoS) для ігрового трафіку:

```
! Створення класу для ігрового трафіку
Core_Switch(config)# class-map match-any GAMES_TRAFFIC
Core_Switch(config-cmap)# match ip dscp ef
Core_Switch(config-cmap)# exit

! Налаштування політики пріоритезації
Core_Switch(config)# policy-map ESPORTS_POLICY
Core_Switch(config-pmap)# class GAMES_TRAFFIC
Core_Switch(config-pmap-c)# priority level 1
Core_Switch(config-pmap-c)# exit
Core_Switch(config-pmap)# exit

! Активація політики на магістральному інтерфейсі
Core_Switch(config)# interface GigabitEthernet 1/0/1
Core_Switch(config-if)# service-policy output ESPORTS_POLICY
Core_Switch(config-if)# exit
```

А. 3 Перевірка таблиці маршрутизації:

```
Core_Switch# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

Gateway of last resort is 10.0.0.1 to network 0.0.0.0

C    192.168.10.0/24 is directly connected, Vlan10
C    192.168.20.0/24 is directly connected, Vlan20
C    192.168.30.0/24 is directly connected, Vlan30
C    192.168.40.0/24 is directly connected, Vlan40
C    172.16.0.0/20 is directly connected, Vlan50
```

Додаток Б

Додаток Б – Топологія мережі

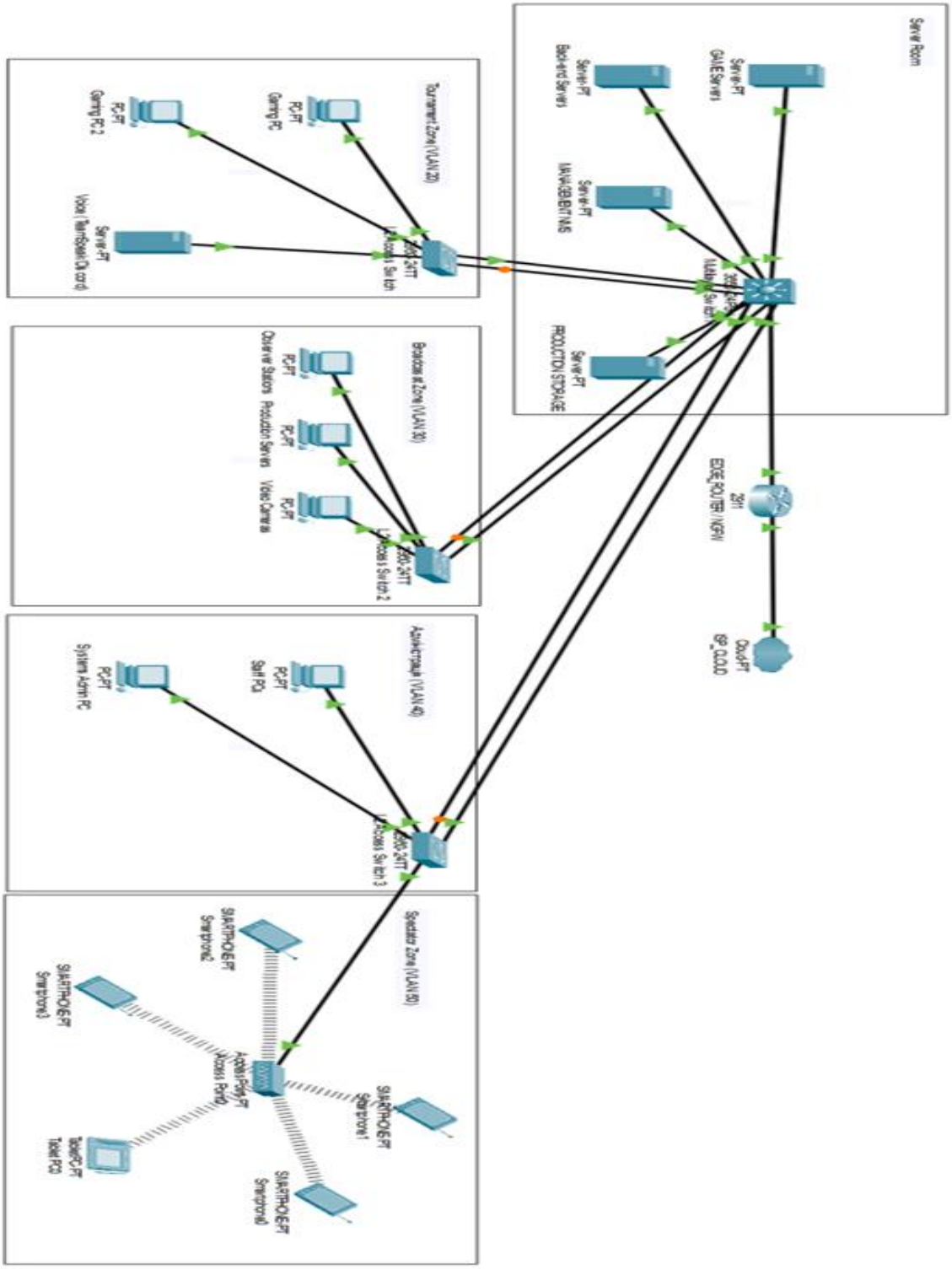

Рисунок Б.1 – Схема фізичної топології мережі кіберспорт-арени

Додаток В

Додаток В - Результати тестування

Таблиця В.1 Показники затримок (Latency) та втрат пакетів при різних рівнях навантаження

Сценарій тестування	Тип трафіку (VLAN)	Пакетів надіслано	Пакетів отримано	Avg Latency (мс)	Втрати (%)
Без навантаження	UDP (Game)	1000	1000	1.2	0%
Пікове навантаження (без QoS)	UDP (Game)	1000	942	14.8	5.8%
Пікове навантаження (з QoS)	UDP (Game)	1000	999	2.4	0.1%
Фоновий трафік (Updates)	TCP (Public)	500	488	22.5	2.4%

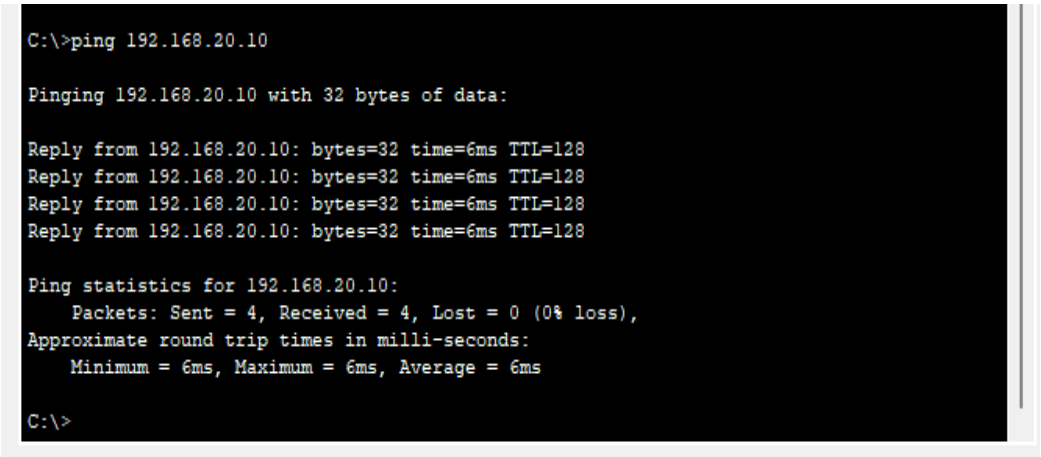

Рисунок В.1 команда ping з VLAN 20

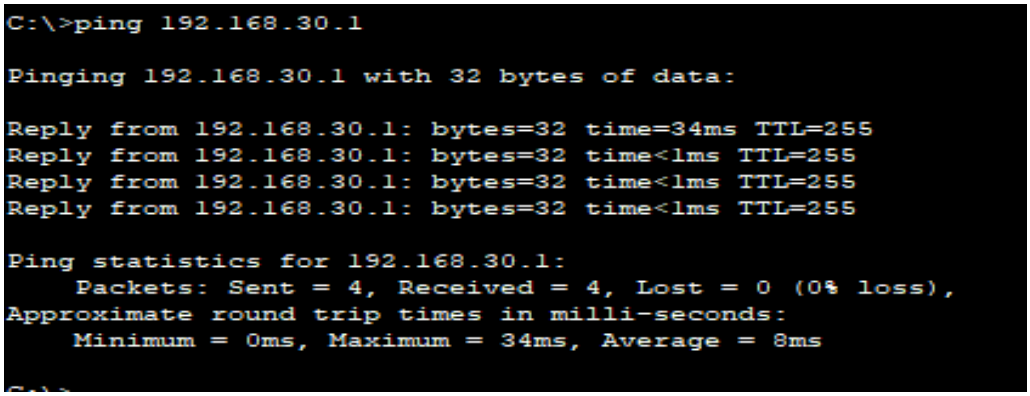

Рисунок В.2 команда ping з VLAN 30

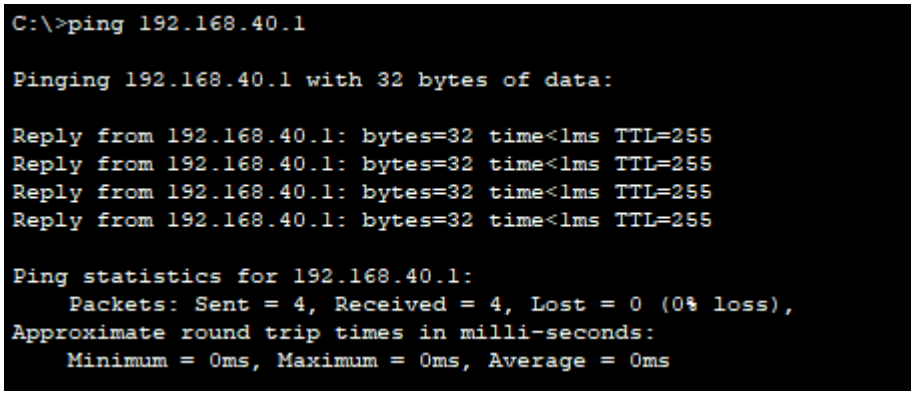

Рисунок В.3 команда ping з VLAN 40

Додаток Г

Додаток Г -

Таблиця Г.1 – Результати моделювання та конфігурації мережевої інфраструктури кіберспортивної арени

Логічний сегмент (VLAN)	Цільове призначення пристроїв	Налаштування безпеки та фільтрації (L3 ACL)	Політика якості обслуговування (QoS)	Результат моделювання під навантаженням (Сценарій В)
VLAN 10 *(Management)*	Керовані комутатори, точки доступу, блоки ДБЖ	Вхідний трафік дозволено лише з хостів адміністраторів (VLAN 40). Повна ізоляція від інших мереж.	Дефолтні черги обробки (Default Queuing) для службових пакетів SSH/SNMP.	Спроби сканування або несанкціонованого доступу заблоковано на SVI-інтерфейсах ядра.
VLAN 20 *(Pro-Players)*	Турнірні ПК безпосередніх учасників змагань	Обмежений доступ: прямий зв'язок з ігровими серверами та регламентований вихід в WAN.	Класифікація трафіку за маркуванням **DSCP EF (46)**. Строга пріоритетна черга **LLQ**.	**RTT: 7–12 мс** (при порозі <20 мс). **Втрати пакетів: 0%**. Повна відсутність джиттеру.
VLAN 30 *(Production)*	Стрімінгові сервери, обсерверські станції, камери NDI	Ізоляція медійних потоків у власному домені для запобігання перевантаженню інших ліній.	Механізм **CBWFQ**. Виділення та резервування гарантованої смуги **150 Мбіт/с**.	**Jitter: 5 мс** (гранична норма). Стабільний відеопотік високої чіткості 4K без фризів.
VLAN 40 *(Staff)*	Робочі ПК суддів, організаторів та систем білінгу (SENET)	Санкціонований повний доступ до мережі керування (VLAN 10) та вихід в Інтернет.	Класифікація трафіку як Best Effort (DSCP 0), стандартна черга обробки.	Безперебійне функціонування системи управління турніром та касових апаратів.
VLAN 50 *(Public Wi-Fi)*	Смартфони, ноутбуки та планшети глядачів арени	**Сувора заборона (Deny)** на рух трафіку до внутрішніх сегментів. Дозвіл лише в WAN.	Механізм **Traffic Policing**. Обмеження максимальної швидкості до **10 Мбіт/с** на один пристрій.	100% відсікання спроб несанкціонованого підключення. Стабілізація швидкості глядачів при 500+ сесіях.