Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Кібербезпеки
(повна назва)

Кафедра Інформаційно-мережної інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)
(позначення документа)

Розробка гібридної мережевої інфраструктури для студії розробки цифрового контенту з використанням SD-WAN та хмарних сервісів
(тема)

Виконав:
здобувач 4 року навчання,
групи ТРІМІ-22-2
Максим Нищий
(власне ім'я, прізвище)

Спеціальність 172 – Телекомунікації та радіотехніка
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційно-мережна інженерія
(повна назва освітньої програми)

Керівник доц. Андрій Костромицький
(посада, власне ім'я, прізвище)

Допускається до захисту

В.о. зав. кафедри _____ Дарія Чеботрарьова
(підпис) (власне ім'я, прізвище)

Харків - 2026 р.

Не містить відомостей, заборонених до відкритого публікування

Студент _____ / Максим Нищий /
(підпис) (власне ім'я прізвище)

Керівник _____ / Андрій Костромицький /
(підпис) (власне ім'я прізвище)

Харківський національний університет радіоелектроніки

Факультет_____Кібербезпеки_____

Кафедра_____Інформаційно-мережної інженерії _____

Рівень вищої освіти_____перший (бакалаврський)_____

Спеціальність___172 – Телекомунікації та радіотехніка_____

(код і повна назва)

Тип програми _____освітньо-професійна_____

Освітня програма_____"Інформаційно-мережна інженерія" _____

(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____

(підпис)

«____»_____ 20 ___ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві_____Нищому Максиму Віталійовичу_____

(прізвище, ім'я, по батькові)

1. Тема роботи __Розробка гібридної мережевої інфраструктури для студії розробки цифрового контенту з використанням SD-WAN та хмарних сервісів._____

_____

_____

затверджена наказом університету від _02___ __червня_____2026 р. № _466Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії _16___ __липня___ 2026 р.

3. Вихідні дані до роботи __Об'єкт проєктування: студія розробки цифрового контенту «Nebula Forge». Кількість робочих місць: до 60 дротових та до 40 бездротових підключень. Організаційна структура: Art-департамент, Dev-відділ, Administration/HR, Server Farm. Вимоги до швидкості: 1 Gigabit Ethernet для рівня доступу, 10 Gigabit Ethernet для магістральних каналів та серверного вузла. Вимоги до гібридної інфраструктури: резервне копіювання та розміщення тестових середовищ в Amazon Web Services (AWS) через Site-to-Site VPN._____

4. Перелік питань, що потрібно опрацювати в роботі _____

Вступ_____

1. Аналіз предметної області та формування технічних вимог_____

2. Розрахунок та логічне проєктування мережі_____

3. Обґрунтування технологій та вибір обладнання_____

Висновок_____

_____

_____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) Слайди у форматі PowerPoint (завдання роботи, мета, структура Nebula Forge, технічні вимоги, логічна топологія мережі, розрахунок портів і резерв, пропускна здатність, політики доступу, вибір обладнання, висновки)

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
1	Отримання завдання, підбір та аналіз літератури, збір вихідних даних.	28.04.2026 - 10.05.2026	
2	Аналіз бізнес-процесів, існуючих рішень та формування технічного завдання.	11.05.2026 - 25.05.2026	
3	Розрахунок портів, пропускної здатності, створення IPv4-плану та VLAN-сегментації.	26.05.2026 - 10.06.2026	
4	Обґрунтування політик доступу, QoS та розрахунок гібридного підключення до AWS.	11.06.2026 - 25.06.2026	
5	Вибір мережевого обладнання, формування специфікації та оцінка ризиків/витрат.	26.06.2026 - 02.07.2026	
6	Оформлення вступу, висновків, реферату та списку джерел за стандартом ДСТУ.	03.07.2026 - 08.07.2026	
7	Подання роботи на перевірку на плагіат та проходження нормоконтролю.	09.07.2026	
8	Усунення зауважень (за наявності), підписання роботи у керівника.	10.07.2026 - 12.07.2026	
9	Підготовка до захисту ДЕК.	13.07.2026 - 15.07.2026	

Дата видачі завдання 28 квітня 2026 р.

Здобувач _____
(підпис)

Керівник роботи _____ доцент Андрій Костромицький
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 64 с., 4 рис., 29 таблиць, 18 джерел

Об'єкт роботи – корпоративна гібридна мережа студії цифрового контенту.

Мета роботи – розрахунок і обґрунтування гібридної мережевої інфраструктури для студії «Nebula Forge» з використанням VLAN-сегментації, 10 Gigabit Ethernet, NGFW, IPsec VPN, елементів SD-WAN-підходу та хмарної інтеграції з AWS.

У роботі розглянуто організаційну структуру підприємства, визначено вимоги до продуктивності, безпеки, відмовостійкості та гібридного підключення до хмарних сервісів AWS.

Ключові слова: VLAN, 10 GIGABIT ETHERNET, CISCO CATALYST, NGFW, IPSEC VPN, AWS, SD-WAN, QOS, ACL, BYOD, ГІБРИДНА МЕРЕЖА.

ABSTRACT

Explanatory note: 64 p., 4 fig., 29 tab., 18 sources.

Object of the work – corporate hybrid network of a digital content studio.

Purpose of the work – calculation and justification of the hybrid network infrastructure for the «Nebula Forge» studio using VLAN segmentation, 10 Gigabit Ethernet, NGFW, IPsec VPN, elements of the SD-WAN approach, and cloud integration with AWS.

The paper considers the organizational structure of the enterprise, defines the requirements for performance, security, fault tolerance, and hybrid connection to AWS cloud services.

Keywords: VLAN, 10 GIGABIT ETHERNET, CISCO CATALYST, NGFW, IPSEC VPN, AWS, SD-WAN, QOS, ACL, BYOD, HYBRID NETWORK.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 9
ВСТУП 10
1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ФОРМУВАННЯ ТЕХНІЧНИХ ВИМОГ 11
1.1 Аналіз бізнес-процесів та організаційної структури IT-студії 11
1.2 Аналіз існуючих рішень та вимог до пропускної здатності мережі 12
1.3 Формування технічного завдання на проєктування 13
2 РОЗРАХУНОК ТА ЛОГІЧНЕ ПРОЄКТУВАННЯ МЕРЕЖІ 15
2.1 Розрахунок портів та резерву масштабування 15
2.2 VLAN-сегментація та IPv4-план адресації 16
2.3 Розрахунок пропускної здатності та магістральних каналів 18
2.4 Політики маршрутизації, ACL та QoS 19
2.5 Розрахунок гібридного підключення до AWS 22
3 ОБҐРУНТУВАННЯ ТЕХНОЛОГІЙ ТА ВИБІР ОБЛАДНАННЯ 24
3.1 Обґрунтування ключових мережевих технологій 24
3.2 Вибір комутаційного обладнання 25
3.3 Вибір NGFW, VPN та SD-WAN/WAN Edge 26
3.4 Специфікація обладнання та перевірка відповідності вимогам 27
3.5 Подальше моделювання як необов’язковий етап 29
3.6 Деталізований розрахунок масштабування та експлуатаційного запасу 30
3.7 Деталізація IPv4-плану, шлюзів і резерву адресації 33
3.8 Розрахунок магістральних каналів, oversubscription та LACP 35
3.9 Розрахунок політик доступу, NGFW і QoS 38
3.10 Розрахунок бездротового сегмента BYOD та Guest WLAN 40
3.11 Розрахунок хмарної інтеграції, резервного копіювання та VPN-навантаження 42
3.12 Порівняльне обґрунтування вибору обладнання 45

3.13 Експлуатаційні ризики та перевірка прийнятих рішень 46
3.14 Економічний розрахунок CAPEX та OPEX 47
ВИСНОВКИ 52
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ 54
ДОДАТОК А СЛАЙДИ ПРЕЗЕНТАЦІЇ 56

ПЕРЕЛІК СКОРОЧЕНЬ

ACL - Access Control List - список контролю доступу.

AP - Access Point - точка бездротового доступу.

AWS - Amazon Web Services - платформа хмарних сервісів Amazon.

BYOD - Bring Your Own Device - використання особистих пристроїв у корпоративній мережі.

CI/CD - Continuous Integration / Continuous Delivery - безперервна інтеграція та доставка.

DHCP - Dynamic Host Configuration Protocol - протокол динамічної конфігурації вузлів.

FHRP - First Hop Redundancy Protocol - протоколи резервування першого шлюзу.

HSRP - Hot Standby Router Protocol - протокол гарячого резервування маршрутизатора.

IPsec - Internet Protocol Security - набір протоколів захисту IP-трафіку.

LACP - Link Aggregation Control Protocol - протокол агрегації каналів.

LAN - Local Area Network - локальна комп’ютерна мережа.

MFA - Multi-Factor Authentication - багатофакторна автентифікація.

NAS - Network Attached Storage - мережеве сховище даних.

NGFW - Next-Generation Firewall - міжмережевий екран нового покоління.

QoS - Quality of Service - якість обслуговування трафіку.

SD-WAN - Software-Defined Wide Area Network - програмно визначена глобальна мережа.

SFP+ - Small Form-factor Pluggable Plus - оптичний модуль для 10 Gigabit Ethernet.

SVI - Switched Virtual Interface - віртуальний інтерфейс комутатора рівня 3.

VLAN - Virtual Local Area Network - віртуальна локальна мережа.

VPN - Virtual Private Network - віртуальна приватна мережа.

ВСТУП

Сучасні студії розробки цифрового контенту поєднують класичні офісні інформаційні системи, високопродуктивні робочі станції, серверні вузли, хмарні сервіси, віддалені підключення та системи захисту інтелектуальної власності. Для такої організації комп'ютерна мережа не є допоміжним сервісом: вона забезпечує доступ до вихідного коду, 3D-ресурсів, систем контролю версій, рендер-нодів, тестових середовищ і резервних копій [2, 11].

Актуальність роботи обумовлена тим, що студія цифрового контенту працює з великими файлами, чутливими до затримок сервісами та комерційно цінними даними. У таких умовах проєктування мережі повинно включати не лише побудову логічної топології, а й кількісний розрахунок портів, пропускної здатності, адресного простору, резерву масштабування, політик доступу та параметрів гібридного підключення до хмари [2, 3].

Метою бакалаврської роботи є розрахунок і обґрунтування гібридної мережевої інфраструктури для студії «Nebula Forge» з використанням VLAN-сегментації, 10 Gigabit Ethernet, NGFW, IPsec VPN, елементів SD-WAN-підходу та хмарної інтеграції з AWS [8, 11].

Для досягнення мети необхідно вирішити такі завдання: проаналізувати предметну область і технічні вимоги; розрахувати кількість портів та резерв масштабування; розробити VLAN-сегментацію та IPv4-план; визначити пропускну здатність магістральних каналів; обґрунтувати політики ACL та QoS; вибрати технології та обладнання; сформувати специфікацію обладнання з перевіркою відповідності проєктним вимогам [13, 14].

Об'єктом роботи є корпоративна гібридна мережа студії цифрового контенту. Предметом роботи є методи розрахунку, логічного проєктування та вибору мережевих технологій і обладнання для середовища з високими вимогами до пропускної здатності, безпеки та хмарної інтеграції [2, 3].

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ФОРМУВАННЯ ТЕХНІЧНИХ ВИМОГ

1.1 Аналіз бізнес-процесів та організаційної структури IT-студії

Проєктування корпоративної мережі доцільно починати з аналізу бізнес-процесів та прикладних сервісів, а не з вибору конкретних моделей обладнання. Такий підхід відповідає загальній логіці проєктування комп'ютерних мереж, у якій вимоги додатків, користувачів і даних визначають параметри канального, мережевого та транспортного рівнів [1-3].

Студія «Nebula Forge» складається з кількох функціональних зон. Art-департамент створює 3D-моделі, текстури, сцени та інші важкі мультимедійні об'єкти. Dev-відділ працює з вихідним кодом, Git-репозиторіями, CI/CD та тестовими середовищами. Адміністративний підрозділ використовує офісні сервіси, бухгалтерські системи, IP-телефонію та корпоративний документообіг. Серверний вузол зосереджує NAS, Git, build-сервери та локальні render nodes. Окремо виділяються бездротові клієнти, BYOD-пристрої, гості та віддалені працівники [15, 16].

Ключовою особливістю такої структури є різнорідність трафіку. Частина потоків є об'ємною, але не критичною до мілісекундних затримок, наприклад копіювання графічних ресурсів. Інша частина, зокрема голосовий зв'язок або інтерактивний доступ до віддалених ресурсів, є чутливою до затримки та втрат пакетів. Тому мережа має бути не пласкою, а сегментованою, керованою та здатною застосовувати різні політики до різних класів трафіку [2, 3]. Основні функціональні зони та їхні мережеві вимоги зведено у таблиці 1.1.

Таблиця 1.1 - Функціональні зони та мережеві вимоги

Зона	Кількість	Основні сервіси	Ключова вимога
Art-департамент	20	NAS, 3D-assets, текстури, render-файли	висока пропускна здатність uplink
Dev-відділ	15	Git, CI/CD, тестові середовища, VPN	захист коду та контроль доступу
Адміністрація / HR	15	ERP, документообіг, IP-телефонія	стабільність і QoS для голосу
Server Farm	10	NAS, Git, render nodes, build servers	10G-підключення та резервування
Wi-Fi / BYOD	до 40	корпоративний доступ, гостьовий інтернет	ізоляція й автентифікація
Remote users	10-15	VPN-доступ до Dev/Art ресурсів	MFA, ACL, шифрування

1.2 Аналіз існуючих рішень та вимог до пропускної здатності мережі

З погляду продуктивності проєктована мережа повинна забезпечувати 1 Gigabit Ethernet для робочих станцій користувачів, 10 Gigabit Ethernet для серверного сегмента та uplink-каналів до ядра мережі. Для цього в офісній мережі застосовуються комутатори доступу з 1G-портами та 10G SFP+ uplink, а також ядро/розподіл з достатньою кількістю 10G/25G портів для серверів і магістралей [14, 2].

З погляду безпеки основною вимогою є ізоляція потоків за ролями. Guest WLAN не повинен мати маршруту до внутрішніх серверів. BYOD-пристрої повинні проходити автентифікацію та отримувати доступ лише до дозволених сервісів. Dev-відділ має доступ до Git, CI/CD та тестових середовищ, але не повинен отримувати неконтрольований доступ до адміністративних систем. Art-департамент отримує доступ до NAS та ресурсів рендерингу, але його трафік має бути відокремлений від Guest і Management сегментів [15, 16].

Гібридна складова передбачає підключення до AWS для резервного копіювання, тестових середовищ і зберігання артефактів білдів. Базовим варіантом для студії такого масштабу є AWS Site-to-Site VPN, оскільки кожне таке з'єднання в AWS має два VPN-тунелі для підвищення доступності [11, 12]. Для подальшого розвитку проєкту можна передбачити AWS Direct Connect, але як базова бакалаврська реалізація достатнім є IPsec VPN з резервуванням тунелів.

1.3 Формування технічного завдання на проєктування

Технічне завдання на проєктування формулюється у вигляді набору вимірюваних вимог. По-перше, мережа повинна підтримувати не менше 60 дротових і 40 бездротових підключень. Резерв масштабування у 20% приймається як плановий експлуатаційний запас для коротко- та середньострокового росту студії: для 60 дротових підключень це ще 12 портів, для 40 бездротових клієнтів - ще 8 клієнтів, а для серверного вузла - щонайменше 2 додаткові 10G-підключення. Такий резерв не є довільним збільшенням сторінок або обладнання, а використовується як мінімальний запас, що дозволяє підключити нових співробітників, додаткові точки доступу, тестові вузли та службове обладнання без негайної перебудови ядра мережі [1-3].

Враховуючи рекомендацію керівника щодо пріоритетів бакалаврської роботи, основний результат зосереджено на розрахунку мережі, обґрунтуванні технологій та виборі обладнання. Підсумкові технічні вимоги до проектованої мережі наведено у таблиці 1.2.

Таблиця 1.2 - Підсумкові технічні вимоги

Група вимог	Вимога	Критерій виконання
Порти	60 дротових + 4 AP + резерв	не менше 77 портів доступу з урахуванням 20% резерву
Сервери	10 серверних вузлів	не менше 10 портів 10G, рекомендовано 12+

Продовження таблиці 1.2

VLAN	логічна сегментація	окремі VLAN для Management, Art, Dev, Admin, Server, Guest
WAN/Cloud	AWS Site-to-Site VPN	два IPsec-тунелі та статична/динамічна маршрутизація
VPN users	10-15 одночасних користувачів	продуктивність NGFW/VPN із запасом не менше 5x
Безпека	NGFW + ACL + deny by default	дозволені лише необхідні потоки між VLAN

Узагальнена логічна топологія проектованої мережі представлена на рисунку 1.1.

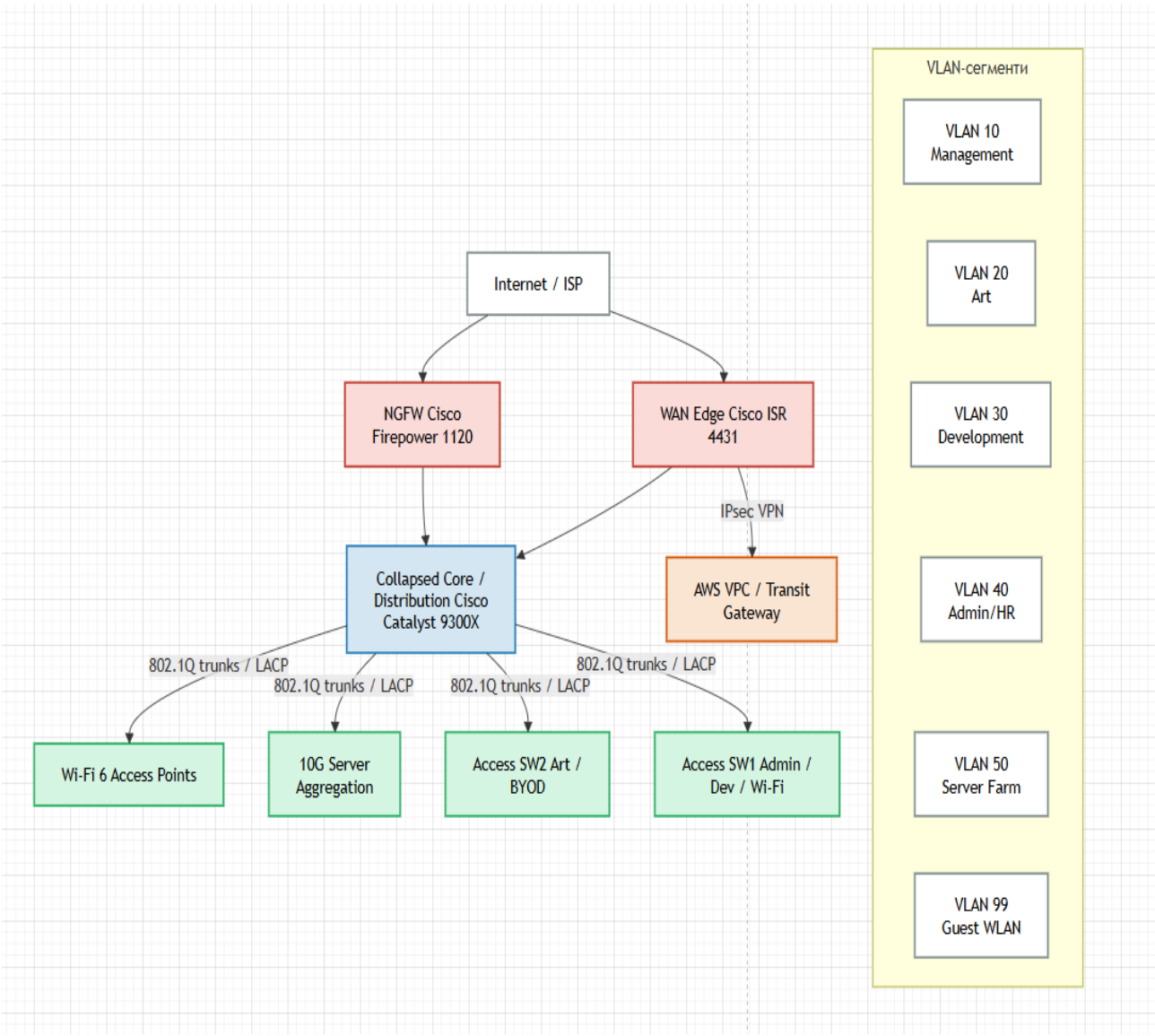


Рисунок 1.1 - Узагальнена логічна топологія проєктованої мережі

2 РОЗРАХУНОК ТА ЛОГІЧНЕ ПРОЄКТУВАННЯ МЕРЕЖІ

2.1 Розрахунок портів та резерву масштабування

Першим кількісним етапом є розрахунок портової ємності. Вихідними даними є 60 дротових робочих місць, 4 точки доступу Wi-Fi, 10 серверних портів 10G, службові порти керування та uplink-канали. Для мережевого проєктування прийнято два сценарії: базовий сценарій з резервом 20% і сценарій значного масштабування +100%. У першому сценарії достатньо двох 48-портових access-комутаторів. У другому сценарії кількість дротових робочих місць зростає до 120, а кількість Wi-Fi-клієнтів - до 80, тому потрібно додати ще щонайменше два access-комутатори, розширити PoE-бюджет для точок доступу, збільшити кількість uplink-каналів і переглянути політики QoS [10; 14].

Для розрахунку використовується формула:

$$P_{\text{заг}} = [(P_{\text{корист}} + P_{AP} + P_{\text{служб}}) \cdot K_{\text{рез}}]$$

де $P_{\text{корист}}$ - кількість користувацьких портів, P_{AP} - кількість портів для точок доступу, $P_{\text{служб}}$ - службові підключення, $K_{\text{рез}}$ - коефіцієнт резерву. Для даної роботи приймається $K_{\text{рез}} = 1{,}2$, тобто 20% резерву. Для користувацького рівня: $P_{\text{заг}} = ceil\big((60 + 4) \cdot 1{,}2\big) = 77$ портів. Отже, двох 48-портових комутаторів доступу достатньо, оскільки вони сумарно надають 96 портів [15, 10].

Серверний сегмент розраховується окремо, тому що він потребує 10G-підключень. Мінімальна кількість серверних портів становить 10. З урахуванням 20% резерву потрібно $ceil(10 \cdot 1{,}2) = 12$ портів 10G. Тому ядро або серверний aggregation-рівень повинен мати не менше 12 портів 10G, а краще 24 порти для резервних uplink-каналів, майбутніх NAS і додаткових render nodes [14, 6]. Детальний розрахунок портової ємності представлено у таблиці 2.1.

Таблиця 2.1 - Розрахунок портової ємності

Категорія	Базова кількість	Коефіцієнт резерву	Розрахунок	Потрібно портів
Користувачі + AP	$60 + 4$	1,2	$ceil(64 \cdot 1{,}2)$	77
Серверний 10G-сегмент	10	1,2	$ceil(10 \cdot 1{,}2)$	12
WAN/NGFW/Core links	4	1,5	$ceil(4 \cdot 1{,}5)$	6
Підсумок 1G access	77	-	$2 \cdot 48$ портів	96 доступно
Підсумок 10G core/server	12 + uplinks	-	24 порти 10G/25G	достатньо

Висновок з розрахунку портів: для рівня доступу доцільно використати два 48-портові PoE+ комутатори з 10G uplink, а для ядра/серверного сегмента - комутатор з не менше ніж 24 високошвидкісними портами SFP+/SFP28. Така конфігурація забезпечує поточні потреби та резерв для розвитку [7; 14].

2.2 VLAN-сегментація та IPv4-план адресації

VLAN-сегментація використовується для розмежування широкомовних доменів, спрощення адміністрування та підвищення безпеки. IEEE 802.1Q визначає механізми мостів і VLAN у локальних мережах [13, 2]. У проєкті VLAN виділяються відповідно до ролі підрозділів, а маршрутизація між VLAN здійснюється через SVI на рівні ядра/розподілу.

Для адресації обрано приватний діапазон 10.20.0.0/16 відповідно до RFC 1918 [13, 17]. Адресний план побудовано так, щоб номер VLAN відображався у третьому октеті. Це спрощує експлуатацію: VLAN 20 відповідає підмережі 10.20.20.0/26, VLAN 30 - 10.20.30.0/26 тощо. Gateway кожної VLAN приймається як перша адреса підмережі, тобто 10.20.X.1. Розподіл VLAN-сегментації та IP-план наведено у таблиці 2.2.

Таблиця 2.2 - VLAN-сегментація та IP-план

VLAN	Назва	Підмережа	Шлюз SVI	Кількість адрес	Призначення
10	Management	10.20.10.0/27	10.20.10.1	30	керування комутаторами, NGFW, ISR
20	Art_Department	10.20.20.0/26	10.20.20.1	62	робочі станції дизайнерів, доступ до NAS
30	Development	10.20.30.0/26	10.20.30.1	62	програмісти, DevOps, VPN-доступ
40	Administration_HR	10.20.40.0/27	10.20.40.1	30	адміністрація, бухгалтерія, IP-телефонія
50	Server_Farm	10.20.50.0/27	10.20.50.1	30	NAS, Git, CI/CD, render nodes
60	VPN_Remote	10.20.60.0/27	10.20.60.1	30	адресний пул віддалених працівників
99	Guest_WLAN	10.20.99.0/26	10.20.99.1	62	гостьовий Wi-Fi тільки в Internet

Для AWS використовується окремий адресний простір 0/16, щоб уникнути перекриття з локальними підмережами. Наприклад, 0/24 може бути використано для приватної підмережі CI/CD, 0/24 - для резервних копій, 0/24 - для тестових середовищ. Відсутність перекриття адрес є обов’язковою умовою стабільної роботи Site-to-Site VPN [11; 12]. Адресний план для сегментів AWS наведено у таблиці 2.3.

Таблиця 2.3 - Адресний план AWS-сегментів

Сегмент AWS	Підмережа	Призначення	Маршрут з офісу
VPC Nebula Forge	10.60.0.0/16	загальний адресний простір AWS	через IPsec VPN
Private CI/CD	10.60.10.0/24	сервери збірки та тестування	дозволено з VLAN 30

Продовження таблиці 2.3

Backup subnet	10.60.20.0/24	резервні копії NAS/Git	дозволено з VLAN 50
Artifacts subnet	10.60.30.0/24	артефакти білдів	дозволено з VLAN 30/50
Management subnet	10.60.99.0/24	адміністрування хмарних ресурсів	дозволено з VLAN 10

2.3 Розрахунок пропускної здатності та магістральних каналів

Пропускна здатність розраховується окремо для рівня доступу, uplink-каналів і серверного сегмента. Для кожного підрозділу визначається потенційна сумарна швидкість портів доступу та пропускна здатність uplink. Співвідношення цих величин утворює коефіцієнт перевантаження: Koversub = Baccess / Buplink. Чим менше значення коефіцієнта, тим менша ймовірність заторів під час пікових обмінів [14, 3].

Для Art-департаменту прийнято найсуворіший режим, оскільки він працює з великими 3D-ресурсами. 20 робочих станцій по 1G дають 20G потенційного доступу. При uplink $2 \cdot 10$G LACP сумарна швидкість становить 20G, тому Koversub = $20G/20G$ = 1:1. Це відповідає вимозі мінімізувати затори під час копіювання текстур і проєктних файлів на NAS [14, 6].

Для Dev-відділу сумарний доступ становить 15G. Якщо використати $2 \cdot 10G$ uplink, коефіцієнт буде $15G/20G$ = 0,75:1, тобто uplink не стане вузьким місцем. У мінімальному варіанті можна було б використати $2 \cdot 1G$ LACP, однак для сучасної гібридної інфраструктури з CI/CD доцільніше одразу закласти 10G uplink, оскільки build-артефакти й синхронізація репозиторіїв можуть створювати пікові потоки [14, 6].

Для адміністративного сегмента 15G потенційного доступу не означають постійного 15G навантаження. Офісний трафік і VoIP зазвичай мають значно меншу інтенсивність, тому 1G або 2G uplink достатній за умови QoS. Однак з

уніфікації обладнання доцільно використовувати ті самі 10G uplink-модулі, що і для інших комутаторів доступу [14, 3]. Розрахунок пропускної здатності за сегментами зведено у таблиці 2.4.

Таблиця 2.4 - Розрахунок пропускної здатності за сегментами

Сегмент	Порти доступу	Потенційний доступ	Рекомендований uplink	Коефіцієнт	Висновок
Art	20 × 1G	20G	2 × 10G LACP	1:1	оптимально для великих файлів
Development	15 × 1G	15G	2 × 10G LACP	0,75:1	є запас для CI/CD
Admin/HR	15 × 1G	15G	1-2 × 10G	≤1,5:1	достатньо з QoS
Guest/BYOD Wi-Fi	4 × 1G AP	4G wired backhaul	1 × 10G uplink	0,4:1	достатньо, обмеження через політики
Server Farm	10 × 10G	100G	4 × 10G LACP	2,5:1	рекомендовано 40G до core
WAN/AWS	VPN + Internet	до 100-200 Mbps базово	1G Internet edge	≤0,2:1	достатньо для VPN/backup

Порівняння показує, що головним критичним сегментом є Server Farm, тому для нього бажано мати не 20G, а 40G aggregate-uplink до ядра. Якщо в лабораторному або бюджетному варіанті використовується 20G, це можна вказати як мінімально допустиме рішення, але у фінальному обґрунтуванні доцільно закласти $4 \cdot 10G$ LACP [14, 6].

2.4 Політики маршрутизації, ACL та QoS

Маршрутизація між VLAN виконується на рівні L3-комутатора ядра/розподілу. Для кожної VLAN створюється SVI з адресою шлюзу. Такий підхід зменшує навантаження на edge-router, дозволяє застосовувати ACL ближче до джерела трафіку та забезпечує високу швидкість міжсегментної маршрутизації всередині офісу [13, 3].

Політики доступу будуються за принципом мінімально необхідних прав. Guest_WLAN отримує лише вихід в Internet через NGFW і не має маршрутів до

VLAN 10, 20, 30, 40, 50. VPN-користувачі після автентифікації потрапляють у VLAN 60 або відповідний VPN pool, після чого ACL дозволяють їм доступ лише до сервісів, необхідних для ролі. Art має доступ до NAS і render nodes, Dev - до Git, CI/CD і тестових середовищ, Administration/HR - лише до офісних сервісів і IP-телефонії [8, 13]. Матрицю політик доступу між VLAN наведено у таблиці 2.5.

Таблиця 2.5 - Матриця політик доступу між VLAN

Джерело	Дозволені напрями	Заборонені напрями	Пояснення
VLAN 10 Management	усі мережеві пристрої, NGFW, ISR	користувацький трафік без потреби	адміністрування обладнання
VLAN 20 Art	VLAN 50 NAS/render, Internet через NGFW	VLAN 40, VLAN 10	доступ до мультимедійних ресурсів
VLAN 30 Dev	VLAN 50 Git/CI/CD, AWS CI/CD, Internet	VLAN 40, VLAN 10	захист коду та сервісів
VLAN 40 Admin/HR	офісні сервіси, VoIP, Internet	VLAN 20, 30, 50 крім дозволених сервісів	ізоляція бухгалтерії/HR
VLAN 60 VPN	доступ за роллю до VLAN 20 або 30/50	Guest, Management без прав	віддалена робота з MFA
VLAN 99 Guest	Internet only	усі внутрішні VLAN	ізольований гостьовий доступ

QoS застосовується для пріоритезації трафіку. Найвищий пріоритет отримує мережеве керування та голосовий трафік. Високий пріоритет отримує трафік Server Farm, Git/CI/CD та критичні backup-процеси. Art-трафік має середньо-високий пріоритет, оскільки він об’ємний, але не завжди потребує мінімальної затримки. Guest_WLAN працює в режимі best-effort з обмеженням швидкості [15, 2]. Класи обслуговування (QoS) для різних типів трафіку описано у таблиці 2.6.

Таблиця 2.6 - Класи QoS для мережі Nebula Forge

Клас	Приклади трафіку	Пріоритет	Політика
Network Control	SSH/SNMP/NTP/syslog	найвищий	дозволити тільки з VLAN 10
Voice	IP-телефонія адміністрації	високий	низька затримка, пріоритетна черга
Server Critical	Git, CI/CD, NAS metadata	високий	гарантована смуга в core
Art Bulk	3D-assets, текстури, рендер-файли	середньо-високий	10G uplink, контроль черг
Backup	резервні копії до AWS	середній	нічне вікно, rate-limit за потреби
Guest	гостьовий інтернет	низький	best-effort, обмеження швидкості

Зонування доступу та базова логіка списків контролю доступу (ACL) зображені на рисунку 2.1.

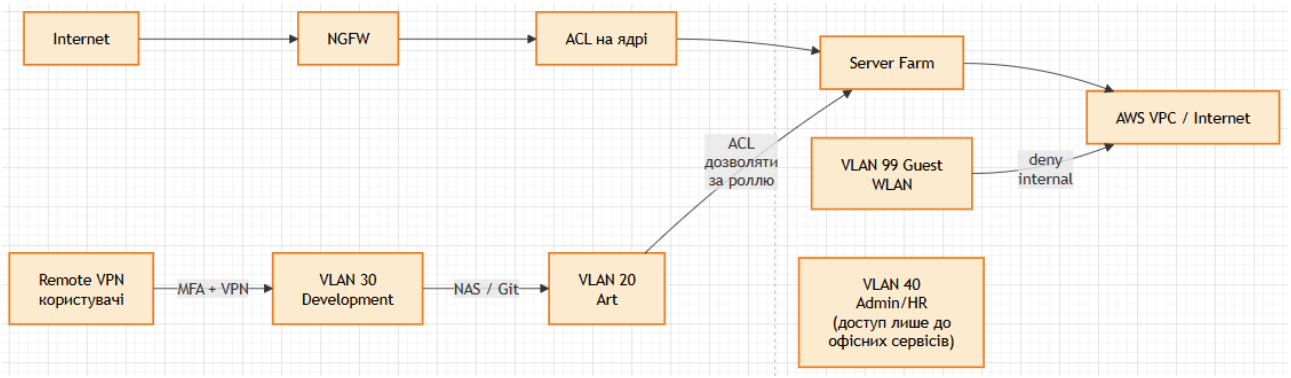


Рисунок 2.1 - Зонування доступу та базова логіка ACL

2.5 Розрахунок гібридного підключення до AWS

Для розрахунку каналу до AWS приймається, що хмара використовується не для постійного рендерингу всіх робочих задач, а для резервних копій, тестових середовищ CI/CD та зберігання артефактів білдів. Тому базовим рішенням є Site-to-Site VPN поверх Internet-каналу з перспективою переходу на Direct Connect у разі зростання трафіку [11, 12].

Розрахунок нічного резервного копіювання виконується за формулою $B = V \cdot 8/T$, де V - обсяг змінених даних за добу в бітах, T - доступне вікно передачі в секундах. Якщо прийняти добовий обсяг змінених даних 100 GB і нічне вікно 8 годин, отримаємо: $B = 100 \cdot 8 \cdot 1024 \frac{\text{MB}}{28800\ \text{s}} \approx 28{,}4\ \text{MB/s}$. Для мережевих розрахунків у бітах це приблизно 222 Mbps. З урахуванням стискання, дедуплікації та нерівномірності потоку практичний мінімум становить 100-200 Mbps, а рекомендований Internet edge - 1 Gbps із можливістю обмеження backup-трафіку [2, 11].

Для VPN-користувачів приймається 15 одночасних підключень і середня потреба 5 Mbps на користувача під час роботи з репозиторіями, документацією та віддаленими сервісами. Базова потреба становить $15 \cdot 5 = 75$ Mbps. З урахуванням службових накладних витрат IPsec і резерву 25% отримаємо приблизно 94 Mbps. Тому NGFW або VPN-шлюз із IPsec-продуктивністю понад 1 Gbps має значний запас [8, 5]. Розрахунок WAN/VPN-навантаження для різних сценаріїв наведено у таблиці 2.7.

Таблиця 2.7 - Розрахунок WAN/VPN-навантаження

Сценарій	Вихідні припущення	Розрахунок	Рекомендація
Remote VPN	15 користувачів × 5 Mbps	75 Mbps + 25% ≈ 94 Mbps	NGFW/VPN ≥ 1 Gbps IPsec
Backup to AWS	до 100 GB змін за добу	100-200 Mbps практично	1G Internet edge, нічне вікно
CI/CD artifacts	пікові завантаження білдів	20-100 Mbps	QoS/rate-limit за потреби

Продовження таблиці 2.7

Site-to-Site VPN	2 IPsec-тунелі AWS	active/failover	маршрутизація через TGW/VPC
Майбутній розвиток	зростання cloud rendering	>1 Gbps stable	Direct Connect + VPN backup

AWS у документації зазначає, що Site-to-Site VPN має два тунелі, які можна використовувати для високої доступності [11]. У разі відмови одного тунелю або технічного обслуговування другий тунель забезпечує резервний шлях. Для підвищення надійності на стороні офісу доцільно мати резервування customer gateway або принаймні резервне живлення й дублювання edge-компонентів. Схема гібридного підключення локальної мережі до AWS через Site-to-Site VPN наведена на рисунку 2.2.

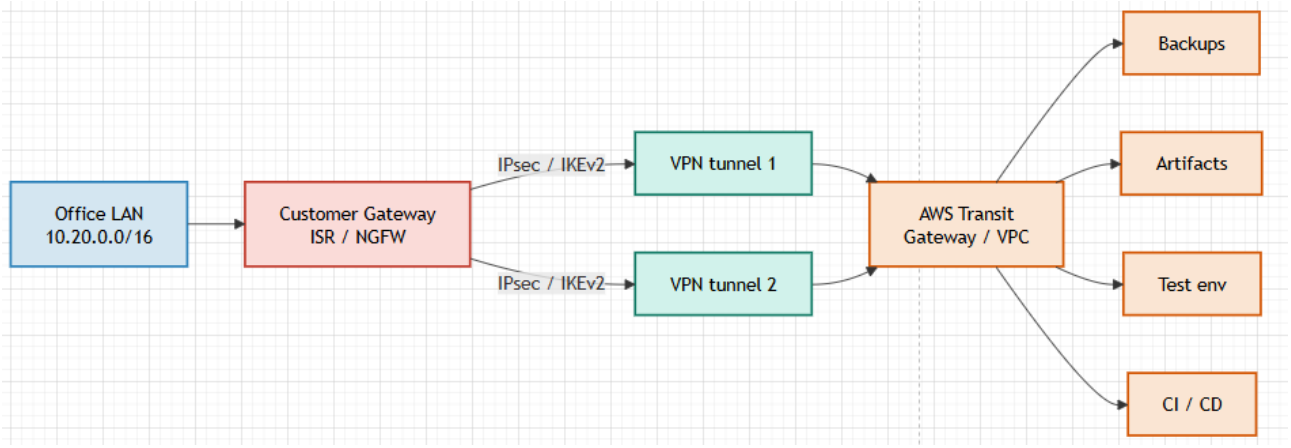


Рисунок 2.2 - Гібридне підключення до AWS через Site-to-Site VPN

3 ОБҐРУНТУВАННЯ ТЕХНОЛОГІЙ ТА ВИБІР ОБЛАДНАННЯ

3.1 Обґрунтування ключових мережевих технологій

Вибір технологій виконується на основі розрахованих вимог. VLAN IEEE 802.1Q потрібні для логічного поділу мережі на ізольовані широкомовні домени. 10 Gigabit Ethernet потрібен для серверного сегмента та uplink-каналів Art-департаменту. LACP застосовується для об’єднання кількох фізичних каналів в один логічний, що одночасно підвищує пропускну здатність і забезпечує відмовостійкість [13; 14].

NGFW необхідний на межі мережі, оскільки студія працює з вихідним кодом і цифровими активами. На відміну від простого firewall, NGFW забезпечує stateful inspection, контроль додатків, IPS/IDS, VPN та централізовані політики безпеки. IPsec VPN потрібен для захищеного підключення віддалених працівників і AWS. BYOD і Guest WLAN мають бути ізольовані через окремі VLAN і політики доступу [8; 11].

SD-WAN-підхід у межах бакалаврської роботи використовується як архітектурний принцип для WAN Edge: централізоване керування політиками, контроль каналів і можливість майбутнього підключення другого провайдера або Direct Connect. Повноцінне розгортання SD-WAN-контролерів може бути предметом окремого етапу, однак вибір WAN Edge обладнання повинен підтримувати такий розвиток [9; 5]. Обґрунтування ключових технологій для мережі студії зведено у таблиці 3.1.

Таблиця 3.1 - Обґрунтування технологій

Технологія	Для чого використовується	Чому потрібна в проекті	Джерело
IEEE 802.1Q VLAN	логічна сегментація	ізоляція Art, Dev, Admin, Server, Guest	[13]

Продовження таблиці 3.1

10 Gigabit Ethernet	сервери та uplink	робота з 3D-assets, NAS, render nodes	[14]
LACP / EtherChannel	агрегація каналів	підвищення пропускної здатності та резервування	[4]
SVI / L3 switching	маршрутизація між VLAN	швидке inter-VLAN routing у core	[4; 6]
NGFW	периметровий захист	IPS, VPN, контроль додатків, захист коду	[8]
IPsec VPN	remote та AWS connectivity	шифрування трафіку через Internet	[9; 11]
Wi-Fi 6 / 802.11ax	бездротовий доступ	підтримка щільного офісного Wi-Fi	[10; 15]

3.2 Вибір комутаційного обладнання

Для ядра/розподілу потрібен комутатор із високошвидкісними портами SFP+/SFP28, підтримкою L3-функцій, ACL, QoS і резервування. Актуальною платформою Cisco для enterprise access/core у малих і середніх кампусних мережах є сімейство Catalyst 9300. Cisco описує Catalyst 9300 як провідну stackable enterprise switching platform для гібридного середовища, де кінцеві точки та додатки можуть бути розміщені будь-де [6; 14].

Для рівня доступу потрібні 48-портові комутатори з PoE+ для живлення точок доступу та IP-телефонів, а також 10G uplink до ядра. Cisco Catalyst 9200 позиціонується як cost-effective access-рішення з повним PoE+, Layer 3 support, резервуванням живлення/вентиляторів і stacking bandwidth до 160 Gbps [7; 14]. Для проєкту достатньо двох 48-портових Catalyst 9200L/9200 з uplink-модулями 10G.

Попередні моделі Catalyst 3650/2960 можуть бути використані як навчальні аналоги в Packet Tracer або для пояснення лабораторної логіки, але у фінальному обґрунтуванні реального обладнання доцільно використовувати Catalyst 9000,

оскільки тема роботи акцентує сучасні стандарти, cloud і enterprise-підхід [1; 3]. Порівняльний аналіз та вибір комутаційного обладнання наведено у таблиці 3.2.

Таблиця 3.2 - Вибір комутаторів

Рівень	Рекомендована модель	Кількість	Ключові характеристики	Обґрунтування
Core / Distribution	Cisco Catalyst 9300X-24Y або близький Catalyst 9300 з 10G/25G uplinks	1-2	24 високошвидкісні SFP+/SFP28 порти, L3, ACL, QoS, stacking	покриває 10G server farm та uplink-и доступу
Access 1	Cisco Catalyst 9200L-48P-4X / 9200-48P	1	48 × 1G PoE+, 4 × 10G uplink	користувачі, AP, IP-телефонія
Access 2	Cisco Catalyst 9200L-48P-4X / 9200-48P	1	48 × 1G PoE+, 4 × 10G uplink	Art, Dev або резервний розподіл портів
Server connectivity	порти core Catalyst 9300X	12+	10G підключення серверів і NAS	потрібен резерв для render nodes

За розрахунком у розділі 2 рівень доступу потребує 77 портів з резервом, а два 48-портові комутатори дають 96 портів. Для серверного сегмента потрібно щонайменше 12 портів 10G, тому ядро з 24 високошвидкісними портами має достатній запас для серверів, uplink-каналів і майбутнього розширення [14; 6].

3.3 Вибір NGFW, VPN та SD-WAN/WAN Edge

Для периметрового захисту та VPN обрано Cisco Firepower 1120 або близьку модель Cisco Secure Firewall/Firepower 1000. За даними Cisco, Firepower 1120 має IPsec VPN throughput близько 1,2 Gbps і підтримує до 150 VPN peers [8]. Для проєктної потреби 10-15 одночасних VPN-підключень цього більш ніж достатньо, оскільки розрахункова потреба віддалених користувачів становить близько 94 Mbps.

Для WAN Edge та SD-WAN-перспективи можна використати Cisco ISR 4331 або Cisco ISR 4431. Cisco 4000 Family ISR підтримує Catalyst SD-WAN

software features і призначена для branch-office WAN-рішень [9; 11]. У цьому проєкті ISR використовується як edge-router для підключення до провайдера, маршрутизації до AWS VPN та майбутнього переходу на SD-WAN-політики.

Для бездротового доступу рекомендовано чотири точки доступу Cisco Catalyst 9105 або 9115 Wi-Fi 6. Cisco описує Catalyst 9105 як Wi-Fi 6 access point з вбудованими можливостями безпеки, надійності та операційної гнучкості [10; 15]. За кількості 40 бездротових клієнтів чотири AP дають орієнтовно 10 клієнтів на точку доступу, що є помірним навантаженням для офісного сценарію. Вибір обладнання безпеки, WAN та Wi-Fi сегментів зведено у таблиці 3.3.

Таблиця 3.3 - Вибір обладнання безпеки, WAN і Wi-Fi

Функція	Рекомендована модель	Ключові параметри	Відповідність вимогам
NGFW / VPN	Cisco Firepower 1120	IPsec VPN throughput ≈ 1,2 Gbps, до 150 VPN peers	запас для 15 VPN-користувачів і AWS VPN
WAN Edge / SD-WAN	Cisco ISR 4331 або ISR 4431	підтримка Cisco Catalyst SD-WAN features	можливість розвитку до SD-WAN
Wi-Fi AP	Cisco Catalyst 9105 / 9115	Wi-Fi 6, enterprise security, PoE	4 AP для 40 клієнтів
Cloud VPN endpoint	AWS Site-to-Site VPN + TGW/VGW	2 IPsec тунелі	відмовостійке підключення до AWS

3.4 Специфікація обладнання та перевірка відповідності вимогам

Специфікація обладнання формується не як список випадкових пристроїв, а як результат розрахунків. Кожна позиція повинна закривати конкретну вимогу: порти доступу, 10G server farm, PoE для AP, IPsec VPN, NGFW, AWS connectivity, резервування uplink і масштабування [8; 11].

Для базового впровадження пропонується мінімальний комплект: один core/distribution комутатор Catalyst 9300X, два access-комутатори Catalyst 9200 PoE+, один NGFW Cisco Firepower 1120, один WAN Edge Cisco ISR 4331/4431,

чотири Wi-Fi 6 AP, SFP+ модулі, оптичні патчкорди та джерела безперебійного живлення. Для підвищення відмовостійкості core і NGFW можуть дублюватися, але мінімальний бакалаврський проєкт може обґрунтовувати один комплект із резервом портів та каналів [6; 7]. Підсумкова специфікація обладнання з обґрунтуванням кожної позиції наведена у таблиці 3.4.

Таблиця 3.4 - Підсумкова специфікація обладнання

№	Позиція	Кількість	Призначення	Обґрунтування
1	Cisco Catalyst 9300X-24Y / Catalyst 9300	1	core/distribution, 10G server/uplink	24 високошвидкісні порти покривають 12+ серверних/ uplink потреб
2	Cisco Catalyst 9200L-48P-4X / 9200-48P	2	рівень доступу	96 портів замість розрахованих 77, PoE+ для AP
3	Cisco Firepower 1120	1	NGFW, IPS, remote access VPN	1,2G IPsec і 150 peers з великим запасом
4	Cisco ISR 4331/4431	1	WAN Edge, SD-WAN-ready, ISP/AWS	підтримка Cisco Catalyst SD-WAN features
5	Cisco Catalyst 9105/9115 AP	4	Wi-Fi 6 для BYOD/Guest	приблизно 10 клієнтів на AP
6	SFP+ 10G modules + fiber patch cords	12-16	uplink Art, Dev, Server, Core	забезпечення 10G магістралей
7	UPS для core/NGFW/server	1-2	резерв живлення	зменшення ризику простою

Перевірка відповідності обраного обладнання технічним вимогам проекту наведена у таблиці 3.5.

Таблиця 3.5 - Перевірка відповідності обладнання вимогам

Вимога	Розраховане значення	Обране рішення	Висновок
Access-порти	77 з резервом	2 × 48 = 96 портів	виконано
Server 10G-порти	12 з резервом	24 порти core/aggregation	виконано
Art uplink	20G для 1:1	2 × 10G LACP	виконано
Server uplink	20G мінімум, 40G рекомендовано	4 × 10G LACP	виконано

Продовження таблиці 3.5

VPN users	15 користувачів ≈ 94 Mbps	Firepower 1120 1,2G IPsec, 150 peers	виконано
Wi-Fi clients	40 клієнтів	4 AP Wi-Fi 6	виконано
AWS VPN	резервний тунель	AWS Site-to-Site VPN 2 тунелі	виконано
Security	VLAN + ACL + NGFW	Catalyst L3 ACL + Firepower NGFW	виконано

Отже, вибране обладнання відповідає розрахованим вимогам із запасом. Найбільший запас створюється в access-рівні, де доступні 96 портів замість 77 потрібних, і в VPN-рівні, де продуктивність NGFW значно перевищує розраховану потребу. Це дає змогу масштабувати студію без негайної заміни базового обладнання [8; 5].

3.5 Подальше моделювання як необов’язковий етап

Після завершення розрахунку та вибору обладнання можливе моделювання основних функцій у Cisco Packet Tracer або іншому лабораторному середовищі. Оскільки не всі актуальні моделі Catalyst 9000, Firepower або AWS-сервіси повноцінно доступні в Packet Tracer, моделювання не повинно розглядатися як єдиний доказ правильності проєкту. Його доцільно використовувати для перевірки логіки VLAN, trunk, SVI, DHCP, ACL і маршрутизації [8; 11].

Для навчального моделювання можна замінити реальні моделі обладнання на доступні аналоги: L3-switch для Catalyst 9300, access switch для Catalyst 9200, router для ISR, generic server для NAS/Git/CI. Така модель дозволяє продемонструвати працездатність адресного плану й ACL, але основне обґрунтування бакалаврської роботи вже виконане через розрахунки та вибір обладнання [6; 7].

3.6 Деталізований розрахунок масштабування та експлуатаційного запасу

Після уточнення вимог до бакалаврської роботи основний акцент переноситься з моделювання на інженерний розрахунок мережі. Тому необхідно показати не тільки кінцеву кількість портів або перелік обладнання, а й логіку, за якою ці показники отримано. Для студії «Nebula Forge» розрахунок виконується для трьох груп ресурсів: користувацький рівень доступу, серверний сегмент і периметр гібридного підключення. Такий поділ дозволяє уникнути помилки, коли всі пристрої розглядаються однаково, хоча їхній трафік і критичність суттєво відрізняються [2; 1].

Базова кількість дротових підключень становить 60, однак фактична кількість фізичних портів повинна бути більшою. У розрахунок потрібно включити точки доступу Wi-Fi, службові підключення для керування, резервні порти для швидкої заміни робочих місць, а також порти під тимчасові лабораторні або тестові стенди. У практичному проєктуванні резерв портів не є надмірністю, оскільки відсутність вільних портів змушує виконувати незаплановані закупівлі, переробляти комутаційні шафи і порушувати прийняту логіку сегментації [10; 15].

Для даної роботи прийнято коефіцієнт резерву 20 %. Він є достатнім для малого або середнього офісу, де чисельність користувачів може зростати поступово, але немає вимоги одразу проєктувати мережу на сотні робочих місць. Розрахунок має вигляд:

$$N_{\text{портів}} = ceil((N_{\text{дротових}} + N_{\text{точок доступу}} + N_{\text{службових}}) \cdot 1{,}2.$$

Якщо взяти 60 дротових підключень, 4 точки доступу та мінімум 0-2 службові підключення, отримуємо потребу приблизно 77 портів. Саме тому два 48-портові комутатори доступу є логічним вибором: вони дають 96 фізичних портів і залишають резерв після підключення всіх поточних користувачів [10; 2].

Окремо потрібно врахувати серверний вузол. У Server Farm передбачено 10 підключень для NAS, Git, CI/CD, build-сервера та render nodes. На відміну від користувацького рівня, серверні вузли не можна підключати за залишковим

принципом через звичайні 1G-порти, тому що саме вони формують центральну точку доступу до великих файлів і сервісів. Для серверного сегмента прийнято мінімум 10G на вузол, а також резерв 20 %, що дає 12 високошвидкісних портів. Вибір core/aggregation-рішення з 24 портами 10G/25G дозволяє не лише підключити наявні сервери, а й додати нові вузли рендерингу або окремий backup-сервер без зміни ядра мережі [14; 2].

Суттєвим є також розрахунок не тільки кількості портів, а й можливості керування мережею. Management-сегмент не повинен бути змішаний із користувацьким трафіком, оскільки через нього адміністратори отримують доступ до комутаторів, NGFW, WAN Edge та точок доступу. Для цього в адресному плані виділяється окрема VLAN 10 і окрема підмережа /27. Навіть якщо фактично керованих пристроїв менше, така підмережа дає місце для подальшого розширення без зміни базової логіки адресації [8; 9]. Узагальнену модель розрахунку пропускної здатності та резерву масштабування наведено на рисунку 3.4.

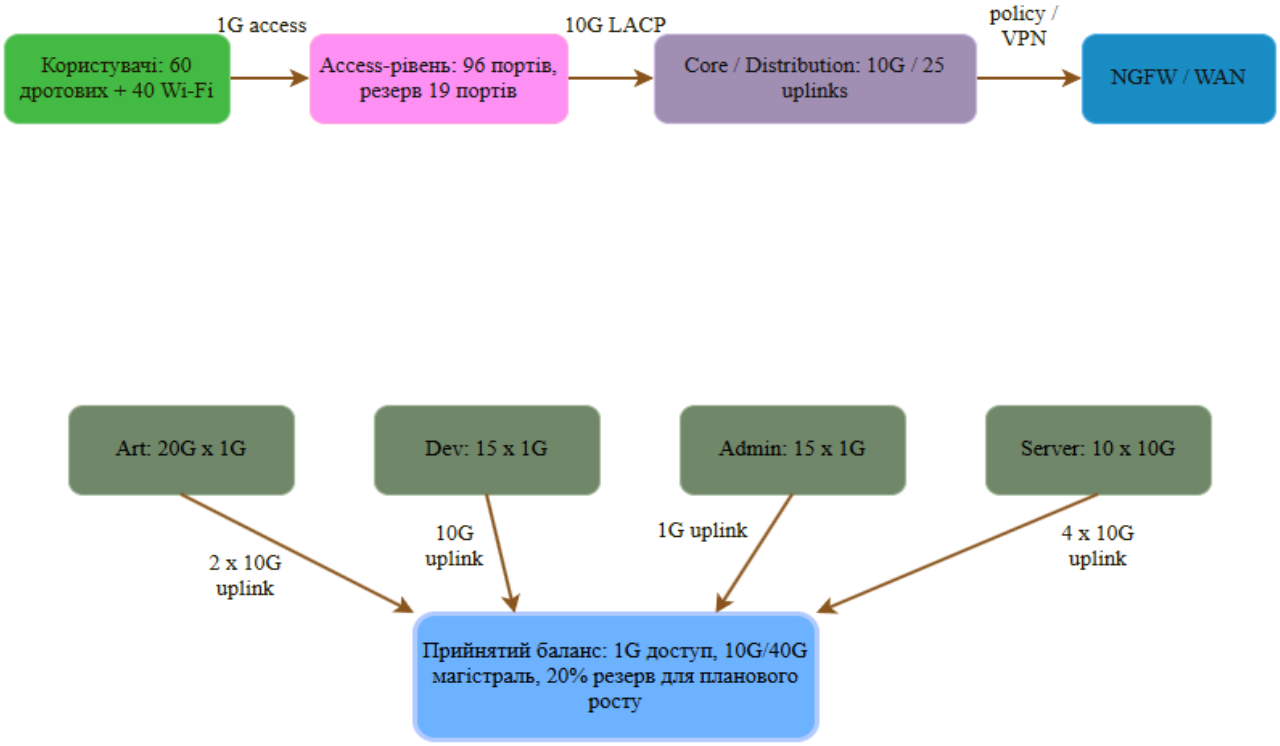


Рисунок 3.4 - Узагальнена модель розрахунку пропускної здатності та резерву масштабування

Розширений розрахунок портової ємності з урахуванням резерву наведено у таблиці 3.6.

Таблиця 3.6 - Розширений розрахунок портової ємності

Категорія	Поточна потреба	Резерв	Проєктна потреба	Рішення
Art-департамент	20 × 1G	20 %	24 порти	1 access-комутатор, окрема VLAN 20
Dev-відділ	15 × 1G	20 %	18 портів	спільний access-рівень з ACL
Admin/HR	15 × 1G	20 %	18 портів	окрема VLAN 40, пріоритет VoIP
Wi-Fi AP	4 × PoE+	1-2 AP	6 портів	PoE+ на Catalyst 9200
Management	8-12 пристроїв	до 30 адрес	/27	окремий керуючий сегмент
Server Farm	10 × 10G	20 %	12 портів	10G/25G core/aggregation
Загальний access-рівень	64 підключення	20 %	77 портів	2 × 48 портів = 96

Отриманий запас не означає, що мережа проєктується завеликою. У мережевих проєктах резерв забезпечує експлуатаційну стійкість: наявність вільних портів спрощує заміну робочих місць, підключення тимчасових пристроїв, розгортання додаткових точок доступу або створення тестового стенда. Для студії, яка працює з цифровим контентом, це особливо важливо, оскільки нові робочі станції можуть з’являтися не поступово, а під конкретний проєкт або реліз гри [2; 1].

Таким чином, за результатом розрахунку обґрунтовано використання двох 48-портових комутаторів доступу та окремого високошвидкісного вузла для серверних підключень. Це рішення відповідає поточному навантаженню, має достатній резерв і не створює надмірно складної топології для бакалаврського проєкту [3; 1].

3.7 Деталізація IPv4-плану, шлюзів і резерву адресації

Адресний план є одним із ключових результатів розрахунку мережі, оскільки він визначає не лише IP-адреси пристроїв, а й майбутню логіку маршрутизації, політик доступу та моніторингу. Для проєкту прийнято приватний адресний простір 10.20.0.0/16, що відповідає практиці використання приватних IPv4-адрес у корпоративних мережах. Перевага такого підходу полягає в тому, що кожна VLAN отримує окрему підмережу, а третій октет адреси відповідає номеру VLAN. Наприклад, VLAN 20 використовує підмережу 10.20.20.0/24, VLAN 30 - 10.20.30.0/24, VLAN 50 - 10.20.50.0/24 [13; 17].

Логічний зв’язок між номером VLAN і підмережею спрощує експлуатацію. Адміністратор одразу бачить, до якого сегмента належить IP-адреса, а це зменшує кількість помилок під час діагностики. Якщо користувач має адресу 10.20.30.45, то зрозуміло, що це Development-сегмент. Якщо пристрій має адресу 10.20.99.18, то він належить до Guest WLAN. Така схема не є випадковою, вона спеціально обрана для зрозумілості та масштабування [13; 15].

Для більшості користувацьких VLAN використовується маска /24. На перший погляд це більше, ніж потрібно для 15 або 20 робочих місць, однак у бакалаврському проєкті важливо зберегти простоту та однорідність. Використання /24 дозволяє без зміни маршрутизації додавати пристрої, створювати резервні робочі місця, підключати тестові стенди й уникати складної фрагментації адресного простору. Для Management і Guest WLAN можна використовувати компактніші підмережі /27 або /26, оскільки їхня очікувана ємність менша та краще піддається оцінці [13; 15].

Шлюзом кожної VLAN виступає SVI на L3-комутаторі ядра/розподілу. Для уніфікації прийнято адресу.1 у кожній підмережі: 10.20.20.1 для Art, 10.20.30.1 для Development, 10.20.50.1 для Server Farm. Такий підхід є зручним для налаштування DHCP, ACL, моніторингу та документації. Для критичних VLAN доцільно передбачити резервування першого шлюзу за допомогою FHRP,

якщо в реальній реалізації використовується пара комутаторів ядра [13; 17]. Деталізований IPv4-план адресації для мережі студії наведено у таблиці 3.7.

Таблиця 3.7 - Деталізований IPv4-план адресації

VLAN	Назва	Підмережа	Шлюз	DHCP/Static	Резерв адрес
10	Management	10.20.10.0/27	10.20.10.1	Static	до 30 пристроїв керування
20	Art_Department	10.20.20.0/24	10.20.20.1	DHCP + reservations	до 254 адрес
30	Development	10.20.30.0/24	10.20.30.1	DHCP + reservations	до 254 адрес
40	Administration_HR	10.20.40.0/24	10.20.40.1	DHCP	до 254 адрес
50	Server_Farm	10.20.50.0/24	10.20.50.1	Static	сервери, NAS, Git, CI/CD
60	VPN_Remote	10.20.60.0/24	10.20.60.1	pool VPN	віддалені користувачі
99	Guest_WLAN	10.20.99.0/26	10.20.99.1	DHCP	до 62 клієнтів
AWS	Cloud VPC	10.60.0.0/16	TGW/VPN	cloud managed	окремий від on-prem простір

Окремим рішенням є виділення VLAN 60 для VPN-користувачів. Такий сегмент дозволяє не змішувати віддалені підключення з внутрішніми робочими станціями Dev або Art. Навіть якщо фрілансер фактично працює з ресурсами Art-департаменту, його початкова IP-адреса належить до VPN_Remote. Далі доступ до потрібних ресурсів відкривається через ACL залежно від ролі. Це спрощує аудит, тому що трафік віддалених користувачів можна відокремити від локального трафіку [13; 5].

Для AWS використовується адресний простір 10.60.0.0/16, який не перетинається з офісними підмережами. Це важливо для Site-to-Site VPN, оскільки перетин адресного простору між локальною мережею і VPC призводить до неоднозначної маршрутизації. У рамках бакалаврського проєкту достатньо показати, що локальна адресація 10.20.0.0/16 і хмарна 10.60.0.0/16 не конфліктують, а маршрути між ними можуть передаватися через IPsec VPN або Transit Gateway [11; 12].

Для DHCP доцільно резервувати нижню частину кожної підмережі під інфраструктурні адреси, а динамічні адреси видавати з середини діапазону. Наприклад, для VLAN 20 шлюз має адресу 10.20.20.1, мережеві принтери або службові вузли можуть отримувати 10.20.20.10-10.20.20.30, а DHCP-пул для робочих станцій може починатися з 10.20.20.100. Така дрібна дисципліна адресації сильно спрощує подальшу підтримку [13; 17]. Рекомендовані DHCP-діапазони та статичні резерви адрес зведено у таблиці 3.8.

Таблиця 3.8 - Рекомендовані DHCP-діапазони та статичні резерви

VLAN	Статичний діапазон	DHCP-пул	Примітка
20 Art	10.20.20.1-10.20.20.99	10.20.20.100-10.20.20.220	резерв для NAS mapping, printers, workstations
30 Dev	10.20.30.1-10.20.30.99	10.20.30.100-10.20.30.220	резерви для build-agents і dev tools
40 Admin	10.20.40.1-10.20.40.99	10.20.40.100-10.20.40.220	офісні ПК та IP-телефонія
60 VPN	10.20.60.1-10.20.60.49	10.20.60.50-10.20.60.150	пул віддалених користувачів
99 Guest	10.20.99.1-10.20.99.9	10.20.99.10-10.20.99.60	короткий lease time

3.8 Розрахунок магістральних каналів, oversubscription та LACP

Розрахунок пропускної здатності не повинен зводитися до простого додавання швидкостей усіх портів. У реальній мережі не всі робочі станції одночасно передають дані на повній швидкості, тому застосовується поняття oversubscription - співвідношення між сумарною швидкістю портів доступу та пропускною здатністю uplink. Для звичайного офісного трафіку це співвідношення може бути високим, але для мультимедійного середовища його потрібно зменшувати [14; 2].

Art-департамент є найбільш вимогливим користувацьким сегментом. Якщо 20 робочих станцій мають по 1G, теоретична сумарна швидкість доступу становить 20 Gbps. Прийняття uplink 2 × 10G через LACP дає 20 Gbps агрегованої

пропускної здатності і співвідношення 1:1. Для студії цифрового контенту це обґрунтовано, оскільки передача текстур, сцен, кешів і графічних пакетів може створювати пікове навантаження в моменти збірки або підготовки релізу [14; 3].

Dev-відділ має 15 робочих місць по 1G, але його трафік зазвичай менш масивний, ніж у Art-департаменті. Основні потоки пов’язані з Git, CI/CD, контейнерними образами, тестовими артефактами та підключенням до хмарних сервісів. Для цього сегмента достатнім є uplink 10G або 2 × 10G у разі об’єднання з іншими access-комутаторами. Якщо в таблиці розрахунків для Dev раніше зазначалася агрегація 2 Gbps, її доцільно розглядати як мінімальний навчальний варіант; для сучасної enterprise-версії краще закладати 10G uplink, оскільки обране обладнання Catalyst 9200/9300 це підтримує [7; 14].

Серверний вузол має 10 портів по 10G, тобто теоретично 100 Gbps на рівні підключення серверів. Однак одночасне повне використання всіх серверних портів не є типовим для даного підприємства. Для Server Farm приймається агрегований uplink 4 × 10G, тобто 40 Gbps. Співвідношення 100:40 або 2,5:1 є допустимим для середовища, де найбільші потоки йдуть між Art, NAS і render nodes, а не всі сервери одночасно передають дані на максимальній швидкості [14; 6].

Використання LACP має дві функції. Перша - збільшення сумарної пропускної здатності. Друга - підвищення відмовостійкості, оскільки в разі відмови одного фізичного каналу логічний канал продовжує працювати з меншою швидкістю. Для бакалаврського проєкту це важливо показати в розрахунках: 2 × 10G дає 20G у нормальному режимі та 10G у режимі відмови одного лінка; 4 × 10G дає 40G у нормальному режимі та 30G/20G залежно від кількості відмов [14; 3]. Розрахунок коефіцієнтів oversubscription для основних сегментів наведено у таблиці 3.9.

Таблиця 3.9 - Розрахунок oversubscription для основних сегментів

Сегмент	Access-порти	Сумарний access	Uplink	Співвідношення	Оцінка
Art	20 × 1G	20 Gbps	2 × 10G LACP	1:1	оптимально для важких assets
Dev	15 × 1G	15 Gbps	1 × 10G або 2 × 10G	1,5:1 або 0,75:1	достатньо для Git/CI/CD
Admin/HR	15 × 1G	15 Gbps	1 × 10G	1,5:1	достатньо для офісного трафіку
Wi-Fi	4 AP, до 40 клієнтів	залежить від WLAN	4 × 1G/2.5G	контрольовано	обмежується радіосередовищем
Server Farm	10 × 10G	100 Gbps	4 × 10G LACP	2,5:1	прийнятно з QoS та локалізацією потоків

У розрахунках також потрібно врахувати напрям трафіку. Якщо Art-департамент активно працює з NAS, то основний потік проходить між VLAN 20 і VLAN 50 через ядро мережі. Тому саме перетин Art-uplink і Server-uplink є критичним. Якщо ж Dev-відділ працює з Git або CI/CD, його навантаження зазвичай менше за обсягом, але має більшу вимогу до стабільності й доступності. Для Admin/HR важливішою є не максимальна швидкість, а пріоритетність голосового трафіку та стабільність доступу до офісних сервісів [13; 14].

Результатом розрахунку є ієрархія пріоритетів: Server Farm і Art отримують найбільшу магістральну пропускну здатність; Dev отримує захищений доступ до Git, CI/CD та AWS; Admin/HR отримує QoS для голосових сервісів; Guest WLAN отримує best-effort і не має доступу до внутрішньої мережі. Такий баланс відповідає реальній структурі студії та не перевантажує проєкт зайвими технологіями [11; 14]. Аналіз поведінки LACP-каналів при виході з ладу ліній зв'язку наведено у таблиці 3.10.

Таблиця 3.10 - Поведінка LACP-каналів при відмовах

Канал	Нормальний режим	Відмова 1 лінка	Залишкова пропускна здатність	Висновок
Art uplink	2 × 10G = 20G	1 × 10G	50 %	робота продовжується, але можливе обмеження великих копіювань
Server uplink	4 × 10G = 40G	3 × 10G	75 %	критичні сервіси залишаються доступними
Core to NGFW	1/2 × 10G	залежить від резерву	до 50-100 %	бажано дублювати шлях
Access Admin	1 × 10G	0	0 %	для некритичного сегмента допустимо або додається резерв

3.9 Розрахунок політик доступу, NGFW і QoS

Безпека проєктованої мережі базується на принципі мінімально необхідного доступу. Це означає, що сам факт перебування користувача у внутрішній мережі не повинен автоматично відкривати йому всі сервери. Сегментація VLAN створює технічну межу між підрозділами, але сама по собі вона не є повною політикою безпеки. Реальний контроль формується через ACL на рівні L3-комутатора та NGFW на периметрі [8; 13].

ACL доцільно розміщувати максимально близько до джерела небажаного трафіку. Наприклад, Guest_WLAN повинен блокуватися вже при спробі звернення до приватних підмереж 10.20.0.0/16. Для Dev-відділу потрібно дозволити доступ до Git, CI/CD і тестових середовищ, але не відкривати прямий доступ до HR або бухгалтерських сервісів. Для Art-департаменту дозволяється доступ до NAS і render nodes, однак Management VLAN повинна залишатися недоступною [13; 15].

NGFW на межі мережі виконує функції фільтрації зовнішнього трафіку, VPN-концентратора, NAT, контролю додатків і виявлення загроз. Для студії цифрового контенту це особливо важливо, оскільки витік вихідного коду або 3D-ресурсів може мати прямі фінансові наслідки. На відміну від звичайного

маршрутизатора, NGFW дозволяє будувати політики не тільки за IP-адресою, але й за типом додатку, користувачем, категорією трафіку та сигнатурами атак [8; 2].

QoS необхідний для того, щоб великі копіювання файлів не витісняли чутливі до затримок сервіси. У проєкті прийнято чотири класи: критичний керуючий трафік, голосовий трафік, продуктивний трафік Art/Server/Dev та best-effort для загального доступу і гостей. Така модель достатньо проста для впровадження, але дозволяє пояснити, чому не всі пакети в мережі мають однаковий пріоритет [2; 3]. Матриця політик доступу та маршрутизації між VLAN наведена у таблиці 3.11.

Таблиця 3.11 - Матриця доступу між VLAN

Джерело	Management	Art	Dev	Admin/HR	Server Farm	Internet/AWS
Management	allow	admin only	admin only	admin only	admin only	allow
Art	deny	local	deny direct	deny	allow NAS/render	allow limited
Dev	deny	deny direct	local	deny	allow Git/CI/CD	allow AWS
Admin/HR	deny	deny	deny	local	deny except services	allow
VPN Remote	deny	role-based	role-based	deny	role-based	allow limited
Guest WLAN	deny	deny	deny	deny	deny	allow Internet only

Класифікація та пріоритезація трафіку (QoS) для мережі Nebula Forge наведена у таблиці 3.12.

Таблиця 3.12 - Класифікація трафіку QoS

Клас	Приклад трафіку	Пріоритет	Причина
Network Control	OSPF/HSRP/management	найвищий	підтримка роботи інфраструктури
Voice	IP-телефонія Admin/HR	високий	чутливість до затримки та jitter

Продовження таблиці 3.12

Business Critical	Git, CI/CD, NAS, render	середньо-високий	продуктивні процеси студії
Standard Data	web, документообіг	звичайний	типовий офісний трафік
Guest / BYOD	гостьовий інтернет	низький	не повинен заважати корпоративним сервісам

Розрахунок продуктивності NGFW виконується відносно очікуваного інтернет- і VPN-навантаження. Для 10-15 віддалених користувачів прийнято середнє навантаження 5 Mbps на активне підключення і коефіцієнт піку 1,25. Отже, розрахункова потреба становить приблизно 94 Mbps. Cisco Firepower 1120 має значно більший IPsec VPN throughput і підтримує до 150 VPN peers, тому обраний пристрій покриває не тільки поточні, а й майбутні потреби [8; 3].

Окремо варто підкреслити, що NGFW не замінює внутрішню сегментацію. Якщо зловмисник або заражений пристрій опиниться всередині мережі, лише периметровий firewall не зможе повністю обмежити горизонтальний рух. Саме тому у проєкті поєднуються VLAN, ACL, NGFW, VPN-політики та окремий Management-сегмент. Така багаторівнева схема є більш стійкою, ніж один централізований бар’єр [8; 13].

3.10 Розрахунок бездротового сегмента BYOD та Guest WLAN

Бездротова частина мережі має два різні призначення: корпоративний BYOD-доступ і гостьовий доступ до Інтернету. Їх не можна об’єднувати в одну логічну мережу, тому що BYOD-пристрої можуть належати співробітникам і використовуватися для робочих задач, а гостьові пристрої не повинні мати жодного доступу до внутрішніх ресурсів. Для цього використовується окремий SSID для корпоративного доступу і окремий SSID для Guest WLAN з прив’язкою до різних VLAN [13; 15].

Для кількості до 40 бездротових клієнтів прийнято 4 точки доступу. Середнє навантаження становить 10 клієнтів на одну точку доступу, що є

помірним значенням для офісного середовища. Насправді пропускна здатність Wi-Fi залежить не лише від стандарту, а й від радіоефіру, перешкод, кількості активних клієнтів, типу пристроїв і розташування точок доступу. Тому проєкт не повинен обіцяти кожному Wi-Fi-клієнту гарантований 1G, але повинен забезпечити стабільний доступ до сервісів і контроль ізоляції [10; 15].

Для живлення точок доступу обирається PoE+ на комутаторах Catalyst 9200. Це спрощує монтаж, оскільки не потрібно окреме живлення біля кожної точки доступу. Крім того, PoE-порти полегшують централізоване резервування живлення через UPS у телекомунікаційній шафі. Якщо точка доступу живиться від комутатора, то при короткочасному зникненні електроживлення UPS підтримує не лише комутаційне обладнання, а й Wi-Fi-сегмент [7; 10].

Guest WLAN повинен мати коротший DHCP lease time і вихід тільки в Internet через NAT на NGFW. Корпоративний BYOD може мати доступ до обмежених сервісів після автентифікації, наприклад до системи завдань, корпоративної пошти або документації, але не до Server Farm за замовчуванням. Такий підхід відповідає принципу розділення довіри: особистий ноутбук співробітника не прирівнюється до керованої корпоративної робочої станції [8; 15]. Розрахунок бездротового сегмента та вимоги до точок доступу наведено у таблиці 3.13.

Таблиця 3.13 - Розрахунок Wi-Fi-сегмента

Показник	Значення	Обґрунтування
Кількість клієнтів	до 40	поточна потреба BYOD і гостьових пристроїв
Кількість AP	4	середнє навантаження 10 клієнтів/AP
Підключення AP	PoE+ access port	живлення і дані через один кабель
Guest VLAN	VLAN 99, /26	до 62 адрес, ізоляція від LAN
BYOD-політика	окремий SSID/VLAN або role-based access	доступ тільки до дозволених сервісів
QoS	best-effort для Guest, standard/business для BYOD	захист критичного дротового трафіку

Для бакалаврської роботи достатньо показати логічне зонування бездротової мережі, розрахунок кількості точок доступу та вимоги до портів PoE+. Детальне радіопланування з тепловими картами, вимірюванням RSSI та аналізом перешкод може бути виконане окремо в межах подальшого проєктування, але воно не є обов’язковим для основної мети цієї роботи [7; 15].

Таким чином, Wi-Fi-сегмент проєктується як керований додаток до дротової мережі, а не як неконтрольований «зручний доступ». Основними критеріями є ізоляція, автентифікація, живлення PoE+, достатня кількість точок доступу та обмеження впливу гостьового трафіку на продуктивні сегменти [7; 15].

3.11 Розрахунок хмарної інтеграції, резервного копіювання та VPN-навантаження

AWS у проєкті використовується як основна хмарна платформа для резервних копій, тестових середовищ і зберігання артефактів білдів. Для студії такого масштабу гібридне підключення доцільно починати з AWS Site-to-Site VPN, оскільки кожне VPN-з’єднання має два IPsec-тунелі, які можна використовувати одночасно для підвищення доступності [11; 12]. Якщо навантаження зростає до сценарію +100% і передача великих asset-файлів до хмари стає постійною, доцільно перейти до Direct Connect або комбінованої моделі Direct Connect + VPN backup, оскільки Direct Connect тарифікується окремо за port-hour і data transfer [11; 12].

AWS Site-to-Site VPN створює два тунелі, кожен із власною публічною IP-адресою, і AWS рекомендує налаштовувати обидва тунелі для резервування [11; 12]. Це добре вписується в бакалаврський проєкт, тому що дозволяє показати відмовостійкість без надмірного ускладнення. Якщо один тунель недоступний, трафік може бути спрямований через інший тунель. Для ще більшої стійкості в майбутньому можна створити два customer gateway або підключити Direct Connect як основний канал, а VPN залишити як резерв.

Розрахунок хмарного трафіку залежить від режиму резервного копіювання. Якщо студія щодня передає повний обсяг великих assets, інтернет-канал швидко стане вузьким місцем. Тому для базового проєкту доцільно застосувати інкрементальне резервне копіювання: у хмару передаються тільки змінені блоки або нові артефакти. Це зменшує вимоги до пропускної здатності та робить VPN-підключення практично придатним для середньої студії [3; 11].

Для оцінки можна прийняти три типи хмарного трафіку: щоденні резервні копії Git/CI/CD, передача артефактів білдів і синхронізація тестових середовищ. Якщо середній обсяг змін становить 50-100 GB на добу, то при нічному вікні 8 годин потрібна середня швидкість приблизно 14-28 Mbps без урахування накладних витрат. Навіть з коефіцієнтом запасу 2 це залишається в межах можливостей звичайного корпоративного інтернет-каналу та NGFW/VPN-рішення [8; 11].

Для важких 3D-assets доцільно не передавати повні копії щодня, а використовувати політику рівнів: критичні дані і вихідний код копіюються частіше, великі архіви проєктів - за розкладом, а завершені релізні assets - після контрольних точок проєкту. Така політика краще відповідає реальним обмеженням WAN і дозволяє не завищувати вимоги до інтернет-каналу [1; 2]. Оцінка обсягів хмарного трафіку для резервного копіювання зведена у таблиці 3.14.

Таблиця 3.14 - Оцінка хмарного трафіку для резервного копіювання

Сценарій	Обсяг змін за добу	Вікно передачі	Середня швидкість	Рішення
Git/CI metadata	10 GB	8 год	≈ 3 Mbps	щодня
Build artifacts	50 GB	8 год	≈ 14 Mbps	щодня/за релізом
Test environments	100 GB	8 год	≈ 28 Mbps	за розкладом
Large 3D archives	500 GB	вихідні/нічне вікно	≈ 140 Mbps для 8 год	інкрементально або поетапно
Critical backup set	до 100 GB	8 год	≈ 28 Mbps + reserve	VPN достатньо

Порівняльний аналіз варіантів підключення до AWS наведено у таблиці 3.15.

Таблиця 3.15 - Варіанти підключення до AWS

Варіант	Переваги	Обмеження	Доцільність для Nebula Forge
AWS Site-to-Site VPN	шифрування, швидкий старт, два тунелі	залежність від Internet	основний варіант для БКР
AWS Direct Connect	передбачувана пропускна здатність, менша залежність від Internet	вартість і складність підключення	перспектива розвитку
VPN + Direct Connect backup	висока доступність	найдорожчий і складніший варіант	для майбутнього масштабування
Public Internet only	простота	недостатній захист і контроль	не підходить для вихідного коду та assets

З урахуванням обсягу студії оптимальним є сценарій Site-to-Site VPN як базового хмарного каналу. Він забезпечує захищене з’єднання з AWS, дозволяє пояснити маршрутизацію між локальними VLAN і VPC, а також не потребує економічного обґрунтування виділеного каналу. Direct Connect можна згадати як рекомендацію для майбутнього, якщо студія збільшить обсяги рендерингу або почне активно переносити обчислення в хмару [11; 12].

У маршрутизації до AWS не потрібно анонсувати всі локальні сегменти без винятку. Достатньо надати доступ тим VLAN, які реально працюють із хмарою: Dev, Server Farm і, за потреби, Art для артефактів або assets. Guest і Admin/HR не повинні отримувати прямий маршрут до AWS VPC, якщо для цього немає службової потреби. Такий підхід зменшує площу атаки та робить політики доступу зрозумілішими [11; 13].

3.12 Порівняльне обґрунтування вибору обладнання

Вибір обладнання у роботі повинен бути не списком бажаних моделей, а наслідком попередніх розрахунків. Для ядра потрібні 10G/25G порти, L3-функції, підтримка ACL, QoS, агрегації каналів і резервування. Для access-рівня потрібні 1G-порти, PoE+ для точок доступу, 10G uplink і можливість базового L2/L3-керування. Для периметра потрібні NGFW-функції, IPsec VPN, NAT, контроль додатків і достатня кількість VPN peers [7; 8].

Cisco Catalyst 9300/9300X обрано для core/aggregation-рівня, оскільки ця серія позиціонується Cisco як enterprise switching platform для гібридного середовища, де робочі місця та додатки можуть бути розміщені будь-де [6; 7]. Для роботи це важливо, тому що тема прямо пов’язана з хмарними сервісами та сучасними стандартами. Catalyst 9200 обрано для access-рівня через наявність PoE+, stacking bandwidth до 160 Gbps, modular uplinks і підтримку Layer 3 функцій [6; 7].

Cisco Firepower 1120 обрано як NGFW/VPN-рішення. За даними Cisco Firepower 1000 Series, модель 1120 має IPsec VPN throughput на рівні 1,2 Gbps і підтримує до 150 VPN peers [8; 11]. Порівняно з розрахованими 10-15 одночасними VPN-підключеннями це створює великий запас. Такий запас корисний не лише для майбутнього зростання кількості фрілансерів, а й для підтримки site-to-site VPN до AWS [8; 11].

Cisco ISR 4000 використовується як WAN Edge/SD-WAN-ready платформа. У роботі не обов’язково будувати повноцінну production SD-WAN-інфраструктуру, однак важливо обґрунтувати, що обране WAN-обладнання не обмежує подальший розвиток. Якщо студія матиме кілька офісів, другий провайдер або активні хмарні маршрути, SD-WAN-підхід дозволить централізовано керувати політиками WAN, пріоритетами додатків і резервуванням каналів [5; 9]. Специфікація обладнання з поясненням ролі кожного елемента наведена у таблиці 3.16.

Таблиця 3.16 - Специфікація з поясненням ролі кожного елемента

Елемент	Кількість	Роль у проекті	Чому саме так
Catalyst 9300X/9300	1-2	Core/Distribution, Server aggregation	потрібні 10G/25G, SVI, ACL, QoS, LACP
Catalyst 9200 48-port PoE+	2	Access для користувачів і AP	96 портів покривають розраховані 77
Firepower 1120	1	NGFW, VPN, NAT, IPS	1,2G IPsec і 150 peers > потреба
ISR 4331/4431	1	WAN Edge, SD-WAN-ready	резерв розвитку WAN
Catalyst 9105/9115 AP	4	Wi-Fi 6 BYOD/Guest	10 клієнтів/AP у середньому
SFP+ модулі 10G	12-16	uplink і серверні з’єднання	підтримка 10G магістралей

3.13 Експлуатаційні ризики та перевірка прийнятих рішень

Після вибору технологій та обладнання потрібно оцінити, які ризики залишаються в проєкті. Це не замінює моделювання, але дозволяє показати, що рішення перевірено логічно. Основними ризиками для Nebula Forge є перевантаження серверного uplink, несанкціонований доступ із BYOD або Guest WLAN, компрометація VPN-облікового запису, помилки ACL, відмова NGFW або провайдера, а також неконтрольоване зростання обсягу хмарних резервних копій [8; 14].

Для кожного ризику в проєкті має бути визначений технічний або організаційний захід. Перевантаження uplink зменшується через LACP і QoS. Доступ гостей блокується ACL і NGFW. VPN захищається MFA, обмеженням доступу за ролями та окремою VLAN 60. Помилки ACL зменшуються через документацію матриці доступу. Відмова одного VPN-тунелю до AWS компенсується другим тунелем. Зростання backup-трафіку контролюється інкрементальною політикою резервного копіювання [8; 11].

Матриця експлуатаційних ризиків та заходів з їх зменшення наведена у таблиці 3.17.

Таблиця 3.17 - Матриця ризиків і заходів зменшення

Ризик	Ймовірність	Вплив	Заходи
Перевантаження Art/Server uplink	середня	високий	2 × 10G / 4 × 10G LACP, QoS, моніторинг
Доступ Guest до LAN	низька за умови ACL	високий	deny 10.20.0.0/16, NAT only
Компрометація VPN	середня	високий	MFA, role-based ACL, журналювання
Відмова одного AWS VPN tunnel	середня	середній	налаштувати обидва тунелі
Відмова access switch	низька	середній	резерв портів, документація підключень
Нестача портів при рості	середня	середній	20 % reserve, 96 access ports
Неконтрольований backup-трафік	середня	середній	інкрементальні копії, нічні вікна
Помилка ACL	середня	високий	матриця доступу, staged rollout, backup config

За результатами ризик-аналізу можна зробити висновок, що обрані технології покривають основні проблеми проєкту. Найбільш критичними залишаються правильне налаштування ACL, контроль VPN-доступу та дисципліна резервного копіювання.

3.14 Економічний розрахунок CAPEX та OPEX

Економічна частина у цій роботі подається як попередня інженерна оцінка вартості проєкту. Вона не є комерційною пропозицією постачальника, оскільки реальна ціна Cisco-обладнання залежить від партнера, гарантії, ліцензійного пакета, курсу валюти та умов закупівлі. Для бакалаврської роботи достатньо розділити витрати на CAPEX і OPEX: CAPEX - одноразові витрати на придбання обладнання та пасивної інфраструктури, OPEX - регулярні витрати на хмарні

сервіси, підтримку, ліцензії, електроживлення та інтернет-канали. Розрахунок AWS-складової прив'язано до відкритих тарифних принципів AWS: Site-to-Site VPN має погодинну оплату, Transit Gateway attachment також має погодинну оплату, Direct Connect тарифікується за port-hour і data transfer, а S3 Standard - за обсяг збережених даних [11; 12]. Орієнтовна оцінка капітальних витрат (CAPEX) на проєкт наведена у таблиці 3.18.

Таблиця 3.18 - Орієнтовний CAPEX проєкту

Стаття CAPEX	Кількість	Орієнтовна ціна за одиницю, $	Сума, $	Призначення
Cisco Catalyst 9300X / 9300 для core/distribution	2	8500	17000	L3-ядро, 10G/25G uplink, резервування StackWise
Cisco Catalyst 9200L 48-port PoE+ access switch	2	3000	6000	96 access-портів для робочих місць, AP і резерву
Cisco Firepower 1120 NGFW	1	2500	2500	Межовий захист, IPS/AVC, VPN remote access
Cisco ISR 4431 / 4331 WAN Edge	1	6000	6000	WAN Edge, IPsec до AWS, майбутній SD-WAN
Cisco Catalyst 9105 Wi-Fi 6 AP	4	600	2400	BYOD і Guest WLAN
SFP+/оптика/патч-корди/кросове обладнання	1 комплект	2500	2500	10G uplink-и, server aggregation, резервні лінії
UPS, rack, PDU, монтажні роботи	1 комплект	3000	3000	Фізична інфраструктура серверної
Разом CAPEX			39400	Орієнтовна одноразова вартість проєкту

Для сценарію +100% CAPEX не можна вважати покритим початковим 20% резервом. У такому разі треба додати щонайменше два 48-портові access-

комутатори, 4 додаткові Wi-Fi 6 AP, SFP+/оптичні модулі для нових uplink-ів і, за потреби, другий NGFW або старшу модель firewall. Орієнтовний додатковий CAPEX для такого сценарію становить 10000-18000 USD без урахування будівельних робіт і комерційної знижки постачальника [8; 14]. Орієнтовна оцінка експлуатаційних витрат (OPEX) на місяць наведена у таблиці 3.19.

Таблиця 3.19 - Орієнтовний OPEX проєкту

Стаття OPEX	Метод розрахунку	Орієнтовна сума на місяць, USD	Коментар
AWS Site-to-Site VPN	0,05 USD/год × 24 × 30	36	Базове VPN-з'єднання до AWS [11; 12]
AWS Transit Gateway attachment	0,05 USD/год × 24 × 30	36	Підключення VPN до TGW [11]
AWS S3 Standard для backup 5 TB	5120 GB × 0,023 USD/GB-month	118	Оцінка для резервних копій [11]
Data transfer out з AWS	400 GB × 0,09 USD/GB після 100 GB free tier	36	Залежить від реального egress-трафіку [11]
Cisco support/licensing	оцінка за договором підтримки	300	Підтримка, оновлення, security-підписки
Інтернет-канал/ISP	бізнес-тариф	100	Залежить від провайдера і SLA
Електроживлення та охолодження	оцінка експлуатаційних витрат	80	Серверна, комутатори, AP, NGFW
Разом OPEX		706	Орієнтовна регулярна вартість на місяць

Якщо компанія зростає на +100%, OPEX збільшується не тільки через нові пристрої. Основними драйверами стають: більший обсяг backup-даних у S3, збільшення egress-трафіку з AWS, необхідність розширених security-ліцензій, вищий клас інтернет-каналу та підтримка додаткового обладнання. Для постійної передачі великих обсягів даних до AWS доцільно розглянути AWS Direct Connect, оскільки ця послуга має окрему модель оплати за port-hour і передачу даних, а також дозволяє винести критичний трафік із публічного Internet [11]. Порівняння параметрів базового та масштабованого сценаріїв наведено у таблиці 3.20.

Таблиця 3.20 - Порівняння базового і масштабованого сценаріїв

Параметр	Базовий сценарій	Резерв 20%	Сценарій +100%	Необхідні зміни
Дротові робочі місця	60	72	120	Додати 2 access-комутатори 48p
Wi-Fi-клієнти	40	48	80	Додати 4 AP, перевірити PoE-бюджет
Серверні 10G-порти	10	12	20	Розширити server aggregation до 4×10G або 25G
Uplink Art	2×10G LACP	достатньо	4×10G або 2×25G	Замінити/додати SFP+ модулі
WAN/VPN	до 15 VPN-користувачів	до 18	30+	Розглянути SD-WAN/Direct Connect/старшу NGFW
Адресний простір	10.20.0.0/16	достатньо	достатньо	IP-план не є обмеженням, потрібна деталізація ACL

Таким чином, 20% резерв обґрунтовано як плановий запас для органічного росту студії без зміни архітектури. Сценарій +100% не покривається резервом і

повинен розглядатися як окремий етап масштабування з додатковим CAPEX/OPEX, переглядом uplink-каналів, збільшенням кількості access-комутаторів та оновленням політик маршрутизації і безпеки [14; 6].

ВИСНОВКИ

У бакалаврській роботі виконано розрахунок і обґрунтування гібридної мережевої інфраструктури для студії гейм-дизайну «Nebula Forge».

У ході роботи визначено вихідні параметри: до 60 дротових підключень, до 40 бездротових клієнтів, 20 робочих місць Art-департаменту, 15 місць Dev-відділу, 15 адміністративних робочих місць, 10 серверних вузлів та 10-15 одночасних VPN-підключень. Розрахунок портів показав, що для рівня доступу потрібно 77 портів з резервом, тому два 48-портові комутатори забезпечують необхідний запас. Для серверного сегмента потрібно щонайменше 12 портів 10G, тому обрано core/aggregation-рішення з 24 високошвидкісними портами.

Розроблено VLAN-сегментацію для Management, Art, Development, Administration/HR, Server Farm, VPN Remote та Guest WLAN. Для адресації використано приватний простір 10.20.0.0/16 з логічним зв’язком між номером VLAN і третього октетом IP-адреси. Для AWS визначено окремий простір 10.60.0.0/16, що виключає конфлікти маршрутизації між локальною та хмарною інфраструктурою.

Розрахунок пропускної здатності показав потребу у 2 × 10G LACP для Art-департаменту, 10G uplink для access-рівня та рекомендовано 4 × 10G LACP для Server Farm. Для віддаленого доступу розрахункова потреба становить приблизно 94 Mbps, тому Cisco Firepower 1120 із IPsec-продуктивністю близько 1,2 Gbps має достатній запас.

Обґрунтовано використання технологій IEEE 802.1Q VLAN, 10 Gigabit Ethernet, LACP, SVI, ACL, QoS, NGFW, IPsec VPN, Wi-Fi 6 та AWS Site-to-Site VPN. Для обладнання обрано Cisco Catalyst 9300X/Catalyst 9200L, Cisco Firepower 1120, Cisco ISR 4431/4331 та Cisco Catalyst 9105 AP. Окремо виконано економічну оцінку CAPEX/OPEX і показано, що 20% резерв покриває планове зростання, але сценарій +100% потребує додаткового етапу масштабування.

Таким чином всі вимоги завдання на бакалаврську роботу виконані в повному обсязі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Kurose J., Ross K. Computer Networking: A Top-Down Approach, Global Edition. 8-ме вид. Harlow : Pearson Higher Ed, 2021. 797 с. ISBN 9781292405513.

2. Tanenbaum A., Feamster N., Wetherall D. J. Computer Networks, Global Edition. 6-те вид. Harlow : Pearson Higher Ed, 2021. 922 с. ISBN 9781292374017.

3. Stallings W. Data and Computer Communications, International Edition. 10-те вид. Pearson Education Limited, 2013. 917 с. ISBN 9780133506487.

4. Cisco. Campus LAN and Wireless LAN Solution Design Guide. URL: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.html

5. Cisco. Cisco Catalyst SD-WAN Design Guide. URL: https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html

6. Cisco. Cisco Catalyst 9300 Series Switches Data Sheet. URL: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html

7. Cisco. Cisco Catalyst 9200 Series Switches Data Sheet. URL: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html

8. Cisco. Cisco Firepower 1000 Series Data Sheet. URL: https://www.cisco.com/c/en/us/products/collateral/security/firepower-1000-series/datasheet-c78-742469.html

9. Cisco. Cisco 4000 Family Integrated Services Router Data Sheet. URL: https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/data_sheet-c78-732542.html

10. Cisco. Cisco Catalyst 9105 Series Access Points Data Sheet. URL: https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/datasheet-c78-744062.html

11. Amazon Web Services. AWS Site-to-Site VPN Documentation. URL: https://docs.aws.amazon.com/vpn/latest/s2svpn/VPC_VPN.html

12. Amazon Web Services. Tunnel options for AWS Site-to-Site VPN. URL: https://docs.aws.amazon.com/vpn/latest/s2svpn/VPNTunnels.html

13. IEEE 802.1Q-2022. IEEE Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks. URL: https://standards.ieee.org/standard/802_1Q-2022.html

14. IEEE 802.3-2022. IEEE Standard for Ethernet. URL: https://standards.ieee.org/ieee/802.3/10422/

15. IEEE 802.11ax-2021. IEEE Standard for Wireless LAN MAC and PHY Enhancements. URL: https://standards.ieee.org/ieee/802.11ax/7180/

16. NIST SP 800-207. Zero Trust Architecture. URL: https://csrc.nist.gov/pubs/sp/800/207/final

17. Rekhter Y. et al. RFC 1918: Address Allocation for Private Internets. IETF, 1996. URL: https://datatracker.ietf.org/doc/html/rfc1918

18. Moy J. RFC 2328: OSPF Version 2. IETF, 1998. URL: https://datatracker.ietf.org/doc/rfc2328/