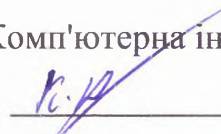


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

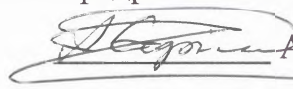
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект високонадійного захищеного
мультипровайдерного Інтернет-підключення
кампусної мережі організації»

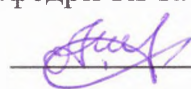
Виконав: студент 4-го курсу групи КІ-20-1
спеціальності 123 «Комп'ютерна інженерія»

 Дмитро КОЛЕСНИК

Керівник: завідувач кафедри КІ та КБ, к.т.н., доцент,

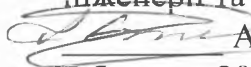
 Андрій ЄФІМЕНКО

Рецензент: доцент кафедри КІ та КБ, к.т.н.

 Олексій ШЕЛУХА

Житомир – 2024

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
 Андрій Єфіменко
5 березня 2024 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Колесник Дмитро Валерійович

Тема роботи: «Проект високонадійного захищеного мультипровайдерного Інтернет-підключення кампусної мережі організації»

затверджена Наказом університету від 5 березня 2024 р. №97/с для КІ

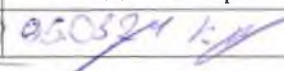
Термін здачі студентом закінченої роботи 9 червня 2024 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
Високонадійні та захищені комп'ютерні мережі на основі мультипровайдерного підключення, з можливостями високої доступності з глобальних мереж

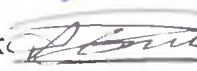
Обладнання та програмне забезпечення:

1. Лабораторія кібербезпеки, ауд. 107;
2. Робочі станції під управління Windows 10 Education x64;
3. Маршрутизатори Cisco 2811 (2 шт.), Cisco 2921/K9 (1 шт.);
4. Комутатори Cisco WS-C2960-24S (2 шт.), Cisco WS-C2960-48TC-L (1 шт.),
Cisco WS-C3560G-24PS-E (1 шт.);
5. Міжмережевий екран Cisco ASA 5512X (2 шт.);
6. Термінальний програмний додаток PuTTY 0.81;
7. Дріт консольного підключення Cisco RJ45 CAB-CONSOLE-USB-RJ45;
8. Програмний аналізатор трафіку Wireshark 4.2.5;
9. Ліцензія для використання Cisco ASA Failover Active/Active.

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

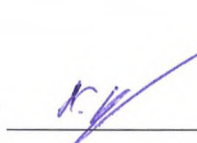
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
I	Єфіменко А.А.	5.03.24 	05.03.24 

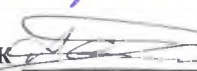
Студент  Колесник Дмитро

Керівник  Єфіменко Андрій

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Огляд та аналіз технологій забезпечення надійності, безпеки та відмовостійкості.	06.03.2024 - 13.03.2024	
2	Розробка фізичної топології проекту з урахуванням технологій до впровадження.	14.03.2024 - 25.03.2024	
3	Відлагодження роботи технологій та протоків. Побудова конфігураційних сценаріїв.	26.03.2024 - 03.04.2024	
4	Підготовка тестового стенду та налагодження проекту.	04.04.2024 - 11.04.2024	
5	Тестування проекту	12.04.2024 - 19.04.2024	
6	Підготовка пояснювальної записки та документів для проведення захисту роботи.	20.04.2024 - 29.04.2024	

Студент  Колесник Дмитро

Керівник  Єфіменко Андрій

АНОТАЦІЯ

Пояснювальна записка містить 161 сторінки текстової частини, серед яких 135 рисунків, 28 таблиць та 16 джерел.

Метою роботи є побудова проєкту високонадійного захищеного мультипровайдерного Інтернет-підключення кампусної мережі організації та виконання його дослідження.

В межах даної роботи, виконується демонстрація використання різних технологій, таких як Cisco ASA Failover у режимі Active/Standby, засобів фільтрації мережевого трафіку на основі FQDN, технологія NAT у режимі Overload, мультипровайдерні підключення, списки контролю доступу, переадресація портів, протокол динамічної маршрутизації OSPF, віртуальні локальні мережі та маршрутизація трафіку між ними, система DNS, технологія IP SLA, що в комбінації забезпечують високий рівень надійності та відмовостійкості роботи комп'ютерної мережі, а також надають засоби безпеки для коректного та безпеченого функціонування. У роботі також виконується демонстрація рівня доступності та відмовостійкості мережі на основі мережевого обладнання компанії Cisco та її рішень.

Ключові слова: ВИСОКА НАДІЙНІСТЬ, ВИСОКИЙ РІВЕНЬ ВІДМОВОСТІЙКОСТІ, CISCO ASA FAILOVER, МУЛЬТИПРОВАЙДЕРНІ ПІДКЛЮЧЕННЯ, БЕЗПЕКА, ВІРТУАЛЬНІ ЛОКАЛЬНІ МЕРЕЖІ, ПЕРЕАДРЕСАЦІЯ ПОРТІВ, ДИНАМІЧНА МАРШРУТИЗАЦІЯ OSPF, РЕЗЕРВУВАННЯ КАНАЛІВ ЗВ'ЯЗКУ.

КІ.КР.Б – 123 – 11– ПЗ

Змн.	Арк.	№ докум.	Підпис	Дата	Проект високонадійного захищеного мультипровайдерного Інтернет-підключення кампусної мережі організації			
Розроб.		Колесник Д.В.		25.06.24				
Керівник		Ефіменко А.А.		25.06.24				
Реценз.		Шелцха О.О.		25.06.24				
Н. контр.		Ефіменко А.А.		25.06.24				
Затверд.		Ефіменко А.А.		25.06.24				
					Літ.	Арк.	Аркушів	
							4	162
					ФІКТ Гр. КІ-20-1			

ANNOTATION

The explanatory note contains 161 pages of the text part, including 135 figures, 28 tables and 16 sources.

The purpose of the work is to build a project of a highly reliable secure multi-provider Internet connection of the campus network of the organization and to carry out its research.

This work demonstrates the use of various technologies, such as Cisco ASA Failover in Active/Standby mode, FQDN-based network traffic filtering, NAT technology in Overload mode, multi-provider connections, access control lists, port forwarding, OSPF, VLANs and traffic routing between them, DNS system, IP SLA technology, that in combination provide a high level of reliability and fault tolerance of the computer network, as well as provide security tools for correct and safe operation. The work also demonstrates the level of availability and fault tolerance of the network based on Cisco network equipment and its solutions.

Keywords: HIGH RELIABILITY, HIGH LEVEL OF FAULT TOLERANCE, CISCO ASA FAILOVER, MULTIPROVIDER CONNECTIONS, SECURITY, VIRTUAL LOCAL NETWORKS, PORT FORWARDING, DYNAMIC ROUTING OSPF, PROTECTION OF COMMUNICATION CHANNELS.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП.....	9
РОЗДІЛ 1. ТЕОРИТИЧНІ АСПЕКТИ ПОБУДОВИ НАДІЙНИХ МЕРЕЖЕВИХ З'ЄДНАНЬ. ТЕХНОЛОГІЇ СУЧАСНИХ КОМП'ЮТЕРНИХ МЕРЕЖ.....	11
1.1. Огляд та аналіз технологій забезпечення надійності та відмовостійкості.	11
1.2. Рішення високої надійності, безпеки та відмовостійкості. Їх призначення та роль у проекті.....	13
1.2.1. Міжмережвий екран Cisco ASA.....	13
1.2.2. Технологія Failover на базі мережевого екрану Cisco ASA.....	14
1.2.3. Фільтрація мережевого трафіку на основі Cisco ASA. Стандартні та розширені списки контролю доступу.	20
1.2.4. Протоколи динамічної маршрутизації. Протокол OSPF (Open Shortest Path First).	23
1.2.5. Технологія віртуальних локальних мереж VLAN. Маршрутизація між VLAN підмережами.....	28
1.2.6. Технологія Network Address Translation, або NAT. NAT у режимі Overload, або Port Address Translation.....	32
1.2.7. Технологія Service-level Agreement, або SLA.....	34
1.2.8. Мультипровайдерні підключення. Переваги та недоліки.	35
1.2.9. Переадресація портів, або Port Forwarding.....	36
1.3. Підготовка технічних рішень.....	38
РОЗДІЛ 2. РОЗРОБКА ФІЗИЧНОЇ ТОПОЛОГІЇ ПРОЕКТУ. ЇЇ НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ.....	41
2.1. Проблеми побудови фізичної топології та впровадження і поєднання технологій.	41
2.2. Розробка фізичної та логічної топології мережі.	54
2.3. Розробка параметрів IP-адресації.	58
2.4. Підготовка тестового стенду.....	68
2.5. Налаштування мережевого обладнання.....	73
2.5.1. Налаштування міжмережвих екранів Cisco ASA.....	78

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

2.5.2. Налаштування мережевих комутаторів.	93
2.5.3. Налаштування маршрутизаторів.	97
2.5.4. Налаштування імітації глобальної мережі інтернет.	106
2.6. Тестування проекту.	109
ВИСНОВКИ.	158
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	159
ДОДАТКИ.	161

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IP – Internet Protocol;
IPv4 – Internet Protocol version 4;
IPv6 – Internet Protocol version 6;
ASA – Adaptive Security Appliance;
ISP – Internet Service Provider;
SLA – Service Level Aggriment;
IPS – Intrusion Prevention System;
DNS – Domain Name Server;
NAT – Network Address Translation;
PAT – Port Address Translation;
DHCP – Dynamic Host Configure Protocol;
VLAN – Virtual Local Area Network;
PVST – Per-VLAN Spanning Tree;
STP – Spanning Tree Protocol ;
RIP – Routing Information Protocol;
OSPF – Open Shortest Path First;
EIGRP – Enhanced Interior Gateway Routing Protocol;
VPN – Virtual Privat Network;
VoIP – Voice over Internet Protocol;
TCP – Transmission Control Protocol;
ACL – Access Control List;
MDI – Medium Dependent Interface;
MDIX – Medium Dependent Interface with Crossover;
HTTP – Hyper Text Transport Protocol ;
FTP – File Transport Protocol;
RDP – Remote Desktop Protocol;
ISL – Inter-Switch Link;
DMZ – Demilitarized Zone.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		8

ВСТУП

Актуальність теми. В умовах сучасної України, яка переживає складний період трансформацій та викликів, забезпечення стабільного та безпечного інтернет-підключення є критично важливим для діяльності підприємств та установ. Пандемія COVID-19 підкреслила значення інформаційних технологій, технологій віддаленого доступу, хмарних рішень, тощо, а військовий конфлікт створив додаткові загрози для інформаційної безпеки. В Україні, де інфраструктура часто стикається з різними технічними та безпековими викликами, впровадження високонадійного мультипровайдерного Інтернет-підключення стає все більш актуальним. Це дозволяє зменшити залежність від одного провайдера і забезпечити резервування каналів зв'язку, що є важливим в умовах нестабільної роботи інфраструктури або цілеспрямованих атак. Мультипровайдерний підхід до Інтернет-підключення забезпечує не тільки вищу надійність мережевих з'єднань, але й покращує загальну продуктивність мережі, мовостями, щодо впровадження розподілення навантаження між кількома каналами. Окрім цього, впровадження сучасних засобів кібербезпеки є необхідним для захисту даних від зловмисних дій, що особливо актуально в умовах підвищеної кіберактивності.

Метою даної кваліфікаційної роботи є розробка проекту високонадійного та захищеного мультипровайдерного Інтернет-підключення для кампусної мережі деякої організації. Цей проект враховуватиме особливості сучасного стану інфраструктури в Україні, а також необхідність забезпечення високого рівня безпеки та відмовостійкості. Реалізація такого проекту сприятиме підвищенню стійкості та безпеки інформаційних систем різних підприємств, де воно може бути впровадженим, що, в свою чергу, позитивно вплине на якість робочого процесу та загальну ефективність діяльності установи.

Визначена мета обумовлює наступні завдання:

- Аналіз сучасних засобів та технологій забезпечення високого рівня надійності, безпеки та відмовостійкості;
- Проектування оптимальної топології комп'ютерної мережі;

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

- Проектування адресаного простору;
- Впровадження технологій та налаштування тестового стенду;
- Моделювання та тестування роботи проекту;
- Створення висновків на основі результатів тестування.

Об’єктом дослідження є проєкт проектування та побудови кампусної мережі підприємства, що включає всі її технічні та програмні компоненти і потреби, які забезпечують внутрішню і зовнішню комунікацію. Кампусна мережа охоплює різноманітні інформаційні системи, підключені до Інтернету через кілька провайдерів, а також різні пристрої користувачів, сервери, маршрутизатори, комутатори та інші мережеві пристрої, які забезпечують її функціонування.

Предметом дослідження є методи, засоби та технології забезпечення високонадійного захищеного мультипровайдерного Інтернет-підключення для кампусної мережі організації. Особлива увага зосереджена на використанні резервування каналів зв’язку, засобів керування вибором каналів зв’язку, а також забезпечення високого рівня доступності для вузлів глобальної мережі. У процесі виконання кваліфікаційної роботи було розроблено проєкт мультипровайдерного Інтернет-підключення для кампусної мережі, який забезпечує високу надійність, безпеку та ефективне використання ресурсів завдяки інтеграції сучасних технологій резервування та фільтрації мережевого трафіку.

У процесі виконання кваліфікаційної роботи було розроблено проєкт високонадійної захищеної комп’ютерної мережі з мультипровайдерним Інтернет підключення для кампусної мережі на основі використання сучасних технологій та апаратного забезпечення для його налагодження, відгалодження та тестування.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ТЕОРИТИЧНІ АСПЕКТИ ПОБУДОВИ НАДІЙНИХ МЕРЕЖЕВИХ З'ЄДНАНЬ. ТЕХНОЛОГІЇ СУЧАСНИХ КОМП'ЮТЕРНИХ МЕРЕЖ.

1.1. Огляд та аналіз технологій забезпечення надійності та відмовостійкості.

Розпочнемо виконання огляду та аналізу технічних рішень для забезпечення високого рівня надійності та відмовостійкості для комп'ютерних мереж. В пошуках рішень для забезпечення таких потреб, у комп'ютерних мережах зустрічаються різні технології та засоби рішення таких задач. До прикладу, створення агрегованих каналів зв'язку, забезпечення оптимальної топології фізичного з'єднання типу кожен-з-кожним, або так звана повнозв'язна топологія, топологія типу зірка, або гібридні топології, що включають в себе різні види топологій в межах однієї комп'ютерної мережі. Забезпечення оптимальної топології дійсно являється одним зі способів підвищення рівня надійності, але далеко не єдиним.

Агрегація каналів зв'язку, також відома як агрегація ліній або агрегація інтерфейсів, є технологією, яка об'єднує кілька фізичних каналів зв'язку в один логічний канал. Це дозволяє збільшити пропускну здатність, забезпечити більш високу надійність і оптимізувати використання мережевих ресурсів. Агрегація каналів широко використовується в мережевих технологіях для підвищення ефективності передачі даних. Використання даної технології може збільшити рівень відмовостійкості комп'ютерної мережі при правильному використанні за рахунок додавання декількох фізичних з'єднань.

У проекті фігурують питання забезпечення захищеності комп'ютерної мережі, а саме тому варто звернути нашу увагу на використання спеціалізованого міжмережевого екрану, так званих апаратних Firewall-ів. Апаратний firewall (міжмережевий екран) є спеціалізованим пристроєм, призначеним для захисту комп'ютерних мереж від несанкціонованого доступу та кіберзагроз. Він виконує функції фільтрації трафіку, перевірки пакетів даних та блокування потенційно небезпечних запитів, відповідно до правил фільтрації, що можуть бути налагоджені системним та мережним адміністратором. Вони мають ряд переваг над іншими, програмними засобами забезпечення фільтрації мережевого трафіку, що підвищує ефективність та

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

надійність використання комп'ютерних мереж. Апаратні firewall зазвичай мають вищу продуктивність порівняно з програмними рішеннями, оскільки вони використовують спеціалізоване обладнання для обробки трафіку. Оскільки апаратний firewall працює незалежно від комп'ютерів в мережі, його налаштування та робота не впливають на продуктивність окремих пристроїв. Використовуючи міжмережевий екран забезпечується централізоване управління безпекою мережі, що спрощує адміністрування та моніторинг. Firewall-и мають різних функцій та призначень для яких вони можуть використовуватися. Серед таких можна відзначити системи виявлення та запобігання вторгнень (IDS/IPS), VPN (Virtual Privat Netowork), контроль додатків, фільтрація контенту та інші. У порівнянні з програмними рішеннями фільтрації та забезпечення безпеки мережі, апаратні firewall зазвичай пропонують більш високий рівень захисту. Популярні бренди апаратних firewall включають Cisco, Fortinet, Palo Alto Networks, Check Point та SonicWall. Вибір конкретного апаратного рішення буде залежати від задач, котрі плануються до виконання на його основі.

Ще одним способом підвищення рівня надійності експлуатації комп'ютерних мереж є технології динамічної маршрутизації. Зазвичай, вони надають кілька можливих маршрутів для забезпечення маршрутизації мережевого трафіку в межах комп'ютерних мереж, що значно підвищує рівень доступності мереж та відмовостійкість мережі в цілому.

Варто відзначити, що особливої універсальної технології побудови надійних та безпечних мереж на даному етапі неіснує. Усі технічні рішення, що впроваджуються у таких мережах зазвичай є не дуже складними технологіями, робота яких у комбінації з іншими технологіями, що направлені для рішення тієї ж задачі, і призводять до появи високонадійних та захищених комп'ютерних мереж. Тому, проводячи огляд та аналіз існуючих технічних рішень побудови високопродуктивних, надійних та захищених комп'ютерних мереж, було виявлено ряд технологій та технічних засобів на основі роботи яких і будуть забезпечуватися усі технічні потреби у роботі розроблюваного проекту комп'ютерної мережі.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		12

1.2. Рішення високої надійності, безпеки та відмовостійкості. Їх призначення та роль у проекті.

1.2.1. Міжмережевий екран Cisco ASA.

Міжмережеві екрани, так звані апаратні брандмауери чи firewall-и, Cisco серії ASA (Adaptive Security Appliance) — це апаратний пристрій забезпечення безпеки мережі, який здійснює моніторинг вхідного та вихідного мережного трафіку та на підставі встановлених наборів правил безпеки приймає рішення, пропустити або блокувати конкретний трафік. Ці мережеві екрани здатні проводити детальний контроль та моніторинг роботи комп'ютерної мережі, а також надають надійний багаторівневий захист, системи запобігання вторгнення IPS (Intrusion Prevention System), комплексні методи захисту від шкідливого програмного забезпечення та підтримують роботу з засобами віддаленого підключення та керування «Cisco AnyConnect», та інше. Міжмережеві екрани з сервісами FirePower також являють собою адаптивно-орієнтовані рішення загроз, які дозволяють забезпечити багаторівневий захист і реалізують ще ширші можливості використання міжмережевих екранів в межах комп'ютерних мереж. Вони здатні працювати з системою управління додатками у поєднанні з системою запобігання вторгнення нового покоління, котра була розроблена компанією Sourcefire, що дозволяє їм забезпечувати посилений захист від шкідливого коду, шкідливого програмного забезпечення, під назвою AMP (Advanced Malware Protection). Як можемо помітити, міжмережеві екрани компанії Cisco ASA це дуже потужний інструмент для забезпечення високого рівня надійності та контролю, роботи з засобами аналізу та моніторингу мережевого трафіку, а також засобів контролю програмного забезпечення, що об'єднуються у межах одного пристрою. Такий потужний інструмент може стати ключевим пристроєм для забезпечення цілого ряду безпекових рішень у різних проектах комп'ютерних мереж.

Лінійка міжмережевих екранів Cisco ASA включає різні моделі: для малого та середнього бізнесу, пристрої підвищеної міцності, для роботи в екстремальних умовах, високопродуктивні екрани для великих мереж і дата-центрів, а також віртуальні додатки для захисту приватних і загальнодоступних корпоративних хмар.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		13

Конкретний вибір моделі Cisco ASA залежить лише від конкретних потреб до даного міжмережевого екрану, що визначаються на основі проведеного аналізу потреб та обсягу мережевого трафіку, котрий необхідно обслуговувати, що в свою чергу це встановлює різні потреби в плані апаратної продуктивності міжмережевого екрану Cisco ASA.

1.2.2. Технологія Failover на базі мережевого екрану Cisco ASA.

В результаті проведеного огляду та аналізу безпекових та високонадійних рішень на базі мережевого обладнання компанії Cisco, а саме Cisco ASA, було виявлено деяку технологію під назвою Cisco ASA Failover, котра являється однією з технологій підвищення рівня відмовостійкості комп'ютерних мережі, що в межах даної роботи являється актуальним. Тому, розглянемо дану технологію, її переваги та потенційні недоліки, а також оглянемо основні принципи та суть її роботи.

Cisco ASA (Adaptive Security Appliance) Failover – це механізм, що забезпечує високу доступність і безперервність роботи мережевих екранів Cisco ASA. Цей механізм дозволяє одному пристрою автоматично перейняти функції іншого в разі збою в його роботі. Існують два типи конфігурацій Failover під назвами Active/Standby Failover та Active/Active Failover. Поглянемо на них.

У режимі відмови Active/Standby один пристрій функціонує як активний блок і пропускає трафік. Другий пристрій, позначений як резервний блок. Він не пропускає трафік, а лише являється резервним. Коли відбувається відмова, блок Active переходить у режим очікування Standby, в той час як інший міжмережевий екран, котрий був в режимі очікування, переходить в активний режим та починає пропускати трафік, в залежності він конфігурації. Для кращого розуміння, на рисунку 1.2.2.1 наведено приклади функціонування даного режиму Cisco ASA Failover.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		14

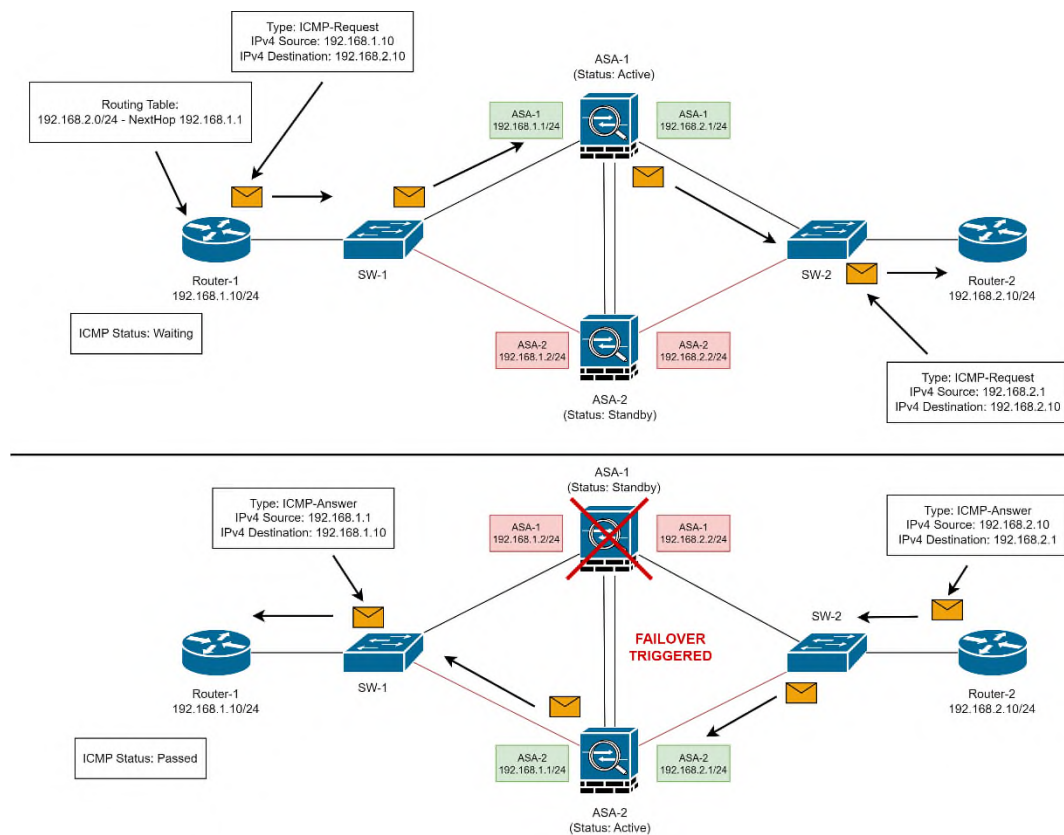


Рисунок 1.2.2.1 – Приклад роботи Cisco ASA Failover у режимі Active/Standby

У конфігурації відмови Active/Active обидва ASA можуть пропускати мережевий трафік. Active/Active Failover доступний лише для ASA в мультиконтекстному режимі роботи (mode multiple). В Active/Active failover, по суті, виконується розподіл контекстів безпеки на 2 групи Failover. Група відмов – це просто логічна група одного або декількох контекстів безпеки. Одна група призначена бути активною на первинному ASA, а інша група призначена бути активною на вторинному ASA. Коли відбувається невдача, вона виникає на рівні групи невдач, а згод інший міжмережевий екран переймає на себе усі обов'язки фільтрування та аналізу трафіку іншого міжмережевого екрану ASA, що був виведений з ладу. Приклад роботи даного режиму роботи наведено на рисунку 1.2.2.2 нижче.

		Колесник Д.В.		
		Ефіменко А.А		
Змн.	Арк.	№ докум.	Підпис	Дата

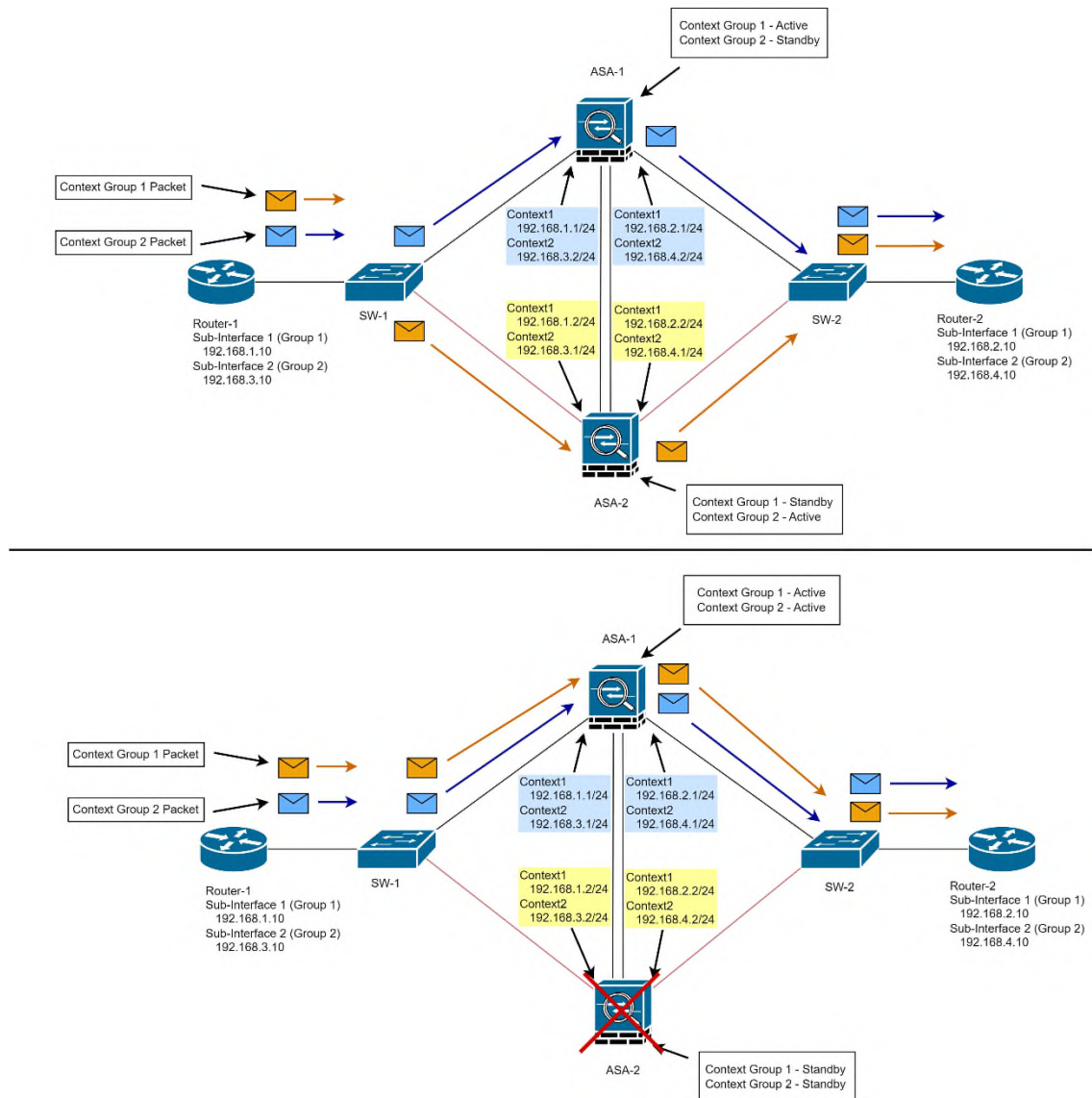


Рисунок 1.2.2.2 – Приклад роботи Cisco ASA Failover у режимі Active/Active

Робота технології Failover, хоч і являється простою для розуміння та дійсно надійним та високоефективним рішенням для тих чи інших випадків, але її реалізація потребує відповідних технічних, програмних та ліцензійних особливостей, котрі необхідно дотримуватися.

Вимоги до ліцензії. Обидві Cisco ASA, в конфігурації Failover, не обов'язково повинні мати однакові ліцензії. Вони об'єднуються, щоб зробити відмовостійку ліцензію кластера. Тобто, за умови, якщо один з міжмережевих екранів підтримує Cisco ASA Failover, то інший може бути автоматично доданий як резервний, або додатковий контролер, без необхідності наявності ліцензії на ньому.

Вимоги до програмного забезпечення. Два пристрої в конфігурації Failover після відмови повинні:

- Перебувати в одному режимі контексту (одиначний або мульти режим).
- Для одиначного режиму необхідно перебувати в тому самому режимі брандмауера (маршрутизованого або прозорого).
- У багатоконтекстному (мульти) режимі роботи брандмауер встановлюється на контекстному рівні, а також можливо використовувати змішані режими.
- Мати однакову основну (перший номер) і другорядну (другий номер) версії програмного забезпечення. Однак можливо тимчасово використовувати різні версії програмного забезпечення під час процесу оновлення. Наприклад, можна оновити один пристрій з версії 8.3(1), а інший до версії 8.3(2), а перемикання після збою залишити активним. У такому випадку використання компанія Cisco рекомендуємо оновити обидва пристрої до однієї версії, щоб забезпечити довготривалу сумісність.
- Мати однакові образи Secure Client. Якщо пара Failover після відмови має невідповідні образи після оновлення, тоді безклієнтське з'єднання SSL VPN припиняється на останньому етапі перезавантаження та оновлення процесу. В той час як база даних показує втрату сеансу, а IP-пул показує, що IP-адреса, призначена для клієнтів і використовується.
- Бути в однаковому режимі FIPS (Federal Information Processing Standards). Це сертифікаційний стандарт, який забезпечує відповідність пристроїв Cisco вимогам безпеки, встановленим урядом США. FIPS стандарти, зокрема FIPS 140-2, визначають вимоги до криптографічних модулів, які використовуються для захисту інформаційних систем та чутливих даних.
- Режимы Firepower 4100/9300 повинні мати однаковий режим розвантаження потоку. Обидва ввімкнені або вимкнені.

Перейдемо до наступної важливої частини реалізації технології Cisco ASA Failover, а саме до апаратних потреб Cisco ASA. Найголовніше це те, що вони повинні бути тієї ж моделі. Крім того, для контейнерних екземплярів вони повинні

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

використовувати однакові атрибути профілю ресурсу, а також мати однакову кількість оперативної пам'яті, кількість інтерфейсів та однакові модулі, що в них встановлені. Такі рішення необхідно забезпечити з метою усунення будь-яких апаратних несумісностей під час конфігурації роботи технології Failover. Якщо використовується пристрій з різними розмірами флеш-пам'яті в конфігурації Failover, важливо переконайтися, що пристрій з меншим об'ємом флеш-пам'яті має достатньо місця для розміщення файлів образів програмного забезпечення та файлів конфігурації. Якщо це не так, синхронізація конфігурації між Cisco ASA з більшою флеш-пам'ятю до блоку з меншою флеш-пам'ятю зазнає невдачі.

Як бачимо, хоча технологія і являється простою для розуміння та впровадження, з рештою вона має досить конкретні вимоги, котрі є обґрунтованими з метою забезпечення найкращого рівня сумісності в результаті роботи технології Cisco ASA Failover. Так як дана технологія займається реплікацією певних налаштувань, то такі рішення необхідні виключно для уникнення потенційних збоїв в роботі ПЗ, збоїв в роботі модулів через несумісність, тощо.

Для роботи технології Cisco ASA Failover використовуються виділені канали зв'язку між міжмережевими екранами, котрі являються Failover Link та Statful Link. Failover Link – це канал зв'язку на основі якого обидві Cisco ASA в режимі відмовостійкої пари постійно спілкуються, щоб визначити робочий стан кожного блоку. У цьому каналі передається інформація про стан блоку (активний або резервний), «привіт» повідомлення (keep-alives), стан мережевого устаткування, виконується обмін MAC-адресою та виконується процес реплікації конфігурації та синхронізація. Інтерфейс Failover Link не налаштований як звичайний мережевий інтерфейс. Він існує тільки для відмовостійкої комунікації. Цей інтерфейс можна використовувати лише для Failover (а також для посилання state). ASA підтримує Auto-MDI/MDIX на своїх портах Ethernet, тому можна використовувати кросоверний або прямий кабель. Якщо використовується прямий кабель, інтерфейс автоматично визначає кабель і змінює одну з пар передачі/прийому на MDIX.

Statful Link. Щоб використовувати Stateful Failover, необхідно налаштувати інтерфейс Stateful Failover (також відоме як інтерфейс стану) для передачі

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

інформації про стани з'єднання та виконання синхронізації наявних підключень в реальному часі. Таке рішення являється дуже корисним, коли необхідно забезпечити безшовний перехід між активним вузлом Cisco ASA та ASA-ою в режимі очікування без втрати наявних з'єднань, таких як TCP/IP, VPN тунелів, VoIP тунелів, тощо. Розглядання наявності такого інтерфейсу також повинен бути, якщо наявна велика конфігурація і високий рівень мережевого трафіку.

Важливим параметром, котрий забезпечує високий рівень надійності під час застосування технології Cisco ASA Failover, є параметри часових затримок, котрі неминуче виникаються під час роботи технології Failover. Така особливість викликана необхідністю активації реплікованих налаштувань та застосування параметрів роботи інтерфейсів, політик інспектування трафіку, інших додаткових параметрів безпеки, переактивація наявних сесій підключень, тощо. Тому компанія Cisco інформує користувачів технології Cisco ASA Failover про потенційні часи затримок під час спрацьовування Failover. Їх наведено у таблиці 1.2.2.1.

Таблиця 1.2.2.1 – Часові затримки спрацьовування Failover.

Стан Failover	Затримка мінімальна	За замовчування	Затримка максимальна
Активний пристрій втрачає живлення, апаратне забезпечення вимикається або програмне забезпечення перезавантажується чи аварійно завершує роботу. При виникненні будь-чого з переліку, контрольовані інтерфейси або посилання відмовостійкості не отримують жодного привітального повідомлення.	800 мілісекунд (msec)	15 секунд (sec)	45 секунд (sec)
Активний блок основний інтерфейс плати переходить у неактивний стан, down.	500 мілісекунд (msec)	5 секунд (sec)	15 секунд (sec)
Активний блок 4GE модуля підключення інтерфейсу переходить у неактивний стан, down.	2 секунд (sec)	5 секунд (sec)	15 секунд (sec)
Активний інтерфейс блоку підіймається, але проблема з підключенням викликає тестування інтерфейсу.	5 секунд (sec)	25 секунд (sec)	75 секунд (sec)

В результаті проведеного огляду та аналізу роботи технології Cisco ASA Failover, було виявлено, що дана технологія являється дуже потужним інструментом забезпечення найвищого рівня відмовостійкості, безпеки та надійності комп'ютерних мереж за рахунок реалізації тих чи інших програмних та апаратних

особливостей під час роботи з декількома міжмережевими екранами Cisco Adaptive Security Appliance у режимі відмовостійкості «Failover».

1.2.3. Фільтрація мережевого трафіку на основі Cisco ASA. Стандартні та розширені списки контролю доступу.

Фільтрація мережевого трафіку та забезпечення безпеки експлуатації комп'ютерної мережі, під час її використання, є однією з головних задач під час використання Cisco ASA. Так, її використання надає кілька методів та функцій, щодо фільтрації мережевого трафіку, а саме: Списки контролю доступу, stateful перевірка пакетів, MPF (Modular Policy Framework), фільтрація URL, фільтрація на рівні додатків (Application Layer Filtering, ALF), системи запобігання вторгненням (Intrusion Prevention System, IPS), контроль доступу на основі ідентичності (Identity-Based Access Control). Ці механізми забезпечують комплексний підхід до фільтрації трафіку, що допомагає захищати мережу від різних типів загроз і забезпечувати дотримання політик безпеки. Коротко оглянемо їх.

Cisco ASA використовує аналізатор мережевого трафіку, перевірку пакетів, що дозволяє контролювати трафік на основі стану з'єднання. Це означає, що пристрій відстежує стан кожного з'єднання, яке проходить через нього, і автоматично дозволяє зворотний трафік для встановлених з'єднань. Що стосується системи MPF (Modular Policy Framework), то вона дозволяє створювати політики для фільтрації трафіку на основі класів трафіку. Це забезпечує гнучке налаштування фільтрації та застосування політик безпеки. До її компонентів відносять класові мапи трафіку (Class Maps), де відбувається визначення типів трафіку для обробки, мапи політики (Policy Maps), що мають в собі правилання поведінки, які виконуються над класифікованим трафіком, а також сервісні політики (Service Policies), що являють собою правила застосування політик до інтерфейсів або глобально. ASA також може інтегруватися з веб-фільтраційними службами для блокування або дозволу доступу до певних веб-сайтів на основі їх URL-адрес. Це дозволяє контролювати веб-трафік та забезпечувати захист від шкідливих сайтів. Фільтрація на рівні додатків дозволяє контролювати трафік на основі специфічних протоколів і додатків, таких як HTTP,

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				20
Змн.	Арк.	№ докум.	Підпис	Дата		

FTP, DNS, та інші. Таке рішення дозволяє більш детально контролювати і обмежувати доступ до певних додатків або служб. Cisco ASA може мати вбудовану систему запобігання вторгненням (IPS), яка аналізує трафік для виявлення та блокування відомих атак і вразливостей. IPS дозволяє захищати мережу від широкого спектру загроз в режимі реального часу. Що стосується контролю доступу на основі ідентичності, то таке рішення дозволяє застосовувати політики безпеки на основі автентифікації користувачів. Це означає, що доступ до ресурсів може бути обмежений залежно від ідентичності користувача, групи або ролі в організації.

Як відзначалося раніше, контроль та фільтрація мережевого трафіку на Cisco ASA, та й на інших мережевих вузлах, може виконуватися на основі списків контролю доступу, котрі також являються простим але досить надійним інструментом керування та фільтрації мережевого трафіку, хоча й в обмеженому вигляді. Списки доступу для комп'ютерних мереж є інструментом для контролю доступу до різних ресурсів і послуг в мережевому середовищі. Вони використовуються для управління трафіком, фільтрації пакетів, забезпечення безпеки і захисту мережевих ресурсів. Списки контролю доступу (ACL), це один з найбільш поширених типів контролю. Вони визначають правила, що вказують які типи трафіку дозволяються або заборонені для передачі через мережеві пристрої, такі як маршрутизатори, комутатори, міжмережеві екрани, тощо. Вони можуть фільтрувати трафік на основі джерела IP-адреси, призначення, портів, протоколів і інших параметрів в залежності від їх типу. ACL використовуються для захисту мережі від несанкціонованого доступу, атак та витоку інформації. На рівні додатків, файрволи або веб-сервери, можуть мати власні списки доступу. Вони використовуються для контролю доступу до конкретних послуг або додатків, наприклад, до веб-сторінок, FTP-серверів або електронної пошти. Ці списки доступу визначають права доступу для окремих користувачів або груп користувачів до функцій і ресурсів додатків.

Деякі мережеві пристрої, такі як файрволи, інтранет-перехоплювачі, системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS), використовують списки доступу для контролю трафіку в мережі. Ці списки доступу дозволяють або блокують пакети на основі різних параметрів, таких як IP-адреса, порт,

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

протокол, заголовки пакетів і т. д. Вони використовуються для фільтрації небажаного трафіку, виявлення та запобігання атакам. Списки доступу на рівні мережевих служб, такі як DHCP (протокол динамічної налаштування хостів) або DNS (система доменних імен), можуть мати списки доступу, які визначають, хто має право отримувати або надавати послуги в мережі.

Списки доступу дозволяють адміністраторам налаштовувати права доступу для користувачів, контролювати трафік і управляти ризиками безпеки. У комп'ютерних мережах існують два типи списків доступу - стандартні списки доступу (Standard Access Control Lists - ACL) і розширені списки доступу (Extended Access Control Lists - ACL). Стандартні ACL дозволяють або блокують трафік на основі джерела пакета. Зазвичай застосовуються на роутерах та інших мережевих пристроях на рівні мережі, ближче до джерела пакетів. Розширені ACL дають можливість контролювати трафік на основі різних параметрів, таких як джерело, призначення, порт, протокол, заголовки пакетів тощо. Вони надають більш гнучкий контроль над трафіком в порівнянні зі стандартними ACL. Розширені списки доступу застосовуються на роутерах, міжмережевих екранах та інших мережевих пристроях на рівні мережі. Зазвичай, списки контролю доступу використовуються у парі з іншими технологіями та протоколами для забезпечення найкращого рівня контролю. До таких прикладів можна відзначити використання списків контролю доступу в парі з засобами фільтрації вхідного чи вихідного трафіку на інтерфейсі, опис правил роботи технології NAT, опис правил редистрибуції маршрутів в картах маршрутизації, під час визначення критеріїв попадання в клас трафіку для подальшої його обробки (MPF), опис параметрів трафіку для шифрування, використання списків контролю доступу в криптографічних картах, створення прав для реалізації підключень через IPSec чи SSL VPN, тощо. Це лише кілька прикладів застосування списків контролю доступів, котрі можуть бути використані як додатковий інструмент опису мережевого трафіку, роботу з яким необхідно виконувати.

Як можемо побачити, міжмережевий екран Cisco ASA має достатню кількість засобів та інструментів для забезпечення фільтрацій мережевого трафіку та його керуванням, щоб забезпечити високий рівень надійності та безпеки експлуатації

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

комп'ютерних систем та мереж. Усі вище перелічені інструменти мають специфічні області застосування, а також мають різні призначення для рішення тих чи інших задач адміністрування та управління мережевим трафіком. Тому, вибір конкретного рішення для фільтрування та обмеження мережевого трафіку буде залежати від тих чи інших потреб, котрі повинні відзначатися у технічному завданні для реалізації різних проектів комп'ютерних мереж.

1.2.4. Протоколи динамічної маршрутизації. Протокол OSPF (Open Shortest Path First).

Протоколи динамічної маршрутизації являються основою побудови сучасних комп'ютерних мереж, в котрих необхідно залишити гнучний набір інструментів для подальшого її масштабування. Так протоколи динамічної маршрутизації, на відміну від статичних засобів маршрутизації, дозволяють забезпечувати побудову комп'ютерних мереж у автоматичному режимі, коли маршрутизатори самостійно обмінюються інформацією про свої наявні підмережі та додають записи про інші підмережі сусідніх маршрутизаторів до своїх таблиць маршрутизації. Ці типи протоколів також надсилають оновлення топології щоразу, коли мережа змінює топологічну структуру. Такі рішення є високонадійними, так як навіть у виході з ладу одного каналу зв'язку між маршрутизаторами, потенційний доступ до тієї чи іншої мережі може бути виконаний на основі іншого маршруту, котрий визначається динамічно в залежності від протоколу та параметрів його роботи. Важливо одразу зазначити недоліки такого способу у тому, що такі рішення зазвичай потребують додаткових ресурсів процесору чи його оперативної пам'яті для своєї коректної роботи, що в цілому збільшує навантаження на систему.

Протоколи динамічної маршрутизації є різні за своїми принципами роботи для визначення найкращих, оптимальних та найкоротших маршрутів до підмереж призначення. Так, у межах реалізації даної роботи проведено огляд протоколу динамічної маршрутизації OSPF, але спочатку визначимо – «Чому саме OSPF?».

Існує кілька протоколів динамічної маршрутизації, але в межах реалізації даного проекту поговоримо лише про декількох з них, а саме про RIP (Routing

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Information Protocol), OSPF (Open Shortest Path First) та EIGRP (Enhanced Interior Gateway Routing Protocol).

RIP (Routing Information Protocol) є простим протоколом маршрутизації, який підходить для невеликих мереж. Він використовує алгоритм відстані-вектора і надсилає оновлення таблиць маршрутизації кожні 30 секунд, що може створювати навантаження на мережу. Основною перевагою RIP є його простота налаштування і низькі вимоги до апаратного забезпечення. Однак, RIP має обмежену масштабованість (до 15 переходів) і не являється ефективним у великих мережах. Через це, він найкраще підходить для малих мереж з обмеженими ресурсами та простими потребами у маршрутизації.

OSPF (Open Shortest Path First) – це протокол маршрутизації, який використовує алгоритм стану каналу (алгоритм Дейкстри) і є дуже ефективним у великих і складних мережах. OSPF обмінюється інформацією про стан каналів між маршрутизаторами, дозволяючи кожному з них мати повну карту топології мережі. Це забезпечує швидку конвергенцію і гнучке маршрутизаційне рішення. OSPF потребує високих обчислювальних ресурсів і більш складної конфігурації, що вимагає більш глибокого рівня розуміння параметрів, що впливатимуть на вибір шляхів маршрутизації. Цей протокол ідеально підходить для великих мереж, де важлива масштабованість і гнучкість маршрутизації, але потребує значних ресурсів і складного налаштування.

EIGRP (Enhanced Interior Gateway Routing Protocol) – це пропрієтарний протокол Cisco, який поєднує переваги протоколів відстані-вектора і стану каналу. EIGRP використовує алгоритм DUAL (Diffusing Update Algorithm) для забезпечення швидкої конвергенції і ефективного використання ресурсів. Він може забезпечувати динамічне балансування навантаження, якщо наявно декілька каналів зв'язку з підмережою призначення, і має гнучку та ефективну маршрутизацію. EIGRP легше налаштовувати, ніж OSPF, але складніше, ніж RIP. Він вимагає помірних апаратних ресурсів і добре підходить для середніх та великих мереж, особливо у корпоративних середовищах. Оскільки EIGRP є власним протоколом Cisco, це може обмежувати його використання в мережах з обладнанням інших

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		24

виробників. Хоча Cisco і намагалися зробити даний стандарт відкритим до використання, але через закритий вихідний код значної популярності даний протокол у мережеских рішеннях інших компаній, окрім Cisco, не зміг набути.

Таким чином, хоча протокол динамічної маршрутизації компанії Cisco під назвою EIGRP дійсно є кращим рішенням, ніж протокол динамічної маршрутизації OSPF, так як він має значно ширший спектр параметрів, що впливають на обрахунок найкоротшого шляху до мережі призначення, а також меншу кількість службового трафіку, що надсилається каналами зв'язку між мережевими пристроями, а також потребує меншої кількості апаратних ресурсів для своєї роботи за рахунок особливостей його роботи. Все ж таки даний протокол є пропрієтарним, тому у разі його використання проект комп'ютерної мережі буде прив'язаним до обладнання компанії Cisco, що значно звужує області його застосування. Тому, з метою забезпечення більшого охоплення ситуацій використання та впровадження даного проекту було прийнято однозначне рішення до використання протоколу динамічної маршрутизації OSPF (Open Shortest Path First). Тому, приступаємо до його огляду та аналізу.

У мережах OSPF, маршрутизатори або системи з однієї області підтримують ту саму базу даних виявлених маршрутів, що описує топологію області. Кожен маршрутизатор або система в області створює свою базу даних інформації про стан каналів, яка складається з оголошень маршрутів (LSAs), отриманих від усіх маршрутизаторів або систем в області, а також LSA, що генеруються самостійно. LSA – це пакет, що містить відомості про сусідів та оцінку шляху. Використовуючи бази даних із виявленням маршрутів за станом зв'язку, кожен маршрутизатор чи сервер з допомогою алгоритму пошуку найкоротшого шляху (SPF) будує дерево шляхів, у якому коренем є сам маршрутизатор чи сервер. За допомогою протоколу OSPF можна розділити автономну систему на окремі області та обробляти їх топології окремо, щоб знизити потік службової інформації маршрутизації OSPF та зменшити розмір бази даних маршрутів кожної області. OSPF забезпечує рівноцінну маршрутизацію з обхідними шляхами. За допомогою різних транзитних вузлів можна

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		25

додавати додаткові маршрути у таблицю маршрутизації тим самим підвищуючи відмовостійкість та ефективність роботи комп'ютерної мережі.

У мережах OSPF з паралельним доступом, тобто у тих мережах де обмін між вузлами виконується постійно в один і той самий момент часу, в яких є не менше двох приєднаних маршрутизаторів, відзначений основний маршрутизатор і резервний маршрутизатор обираються за допомогою протоколу привітання «Hello», а також параметрів, що були встановленими мережевим адміністратором, за необхідністю. Зазначений основний маршрутизатор створює LSA для всієї мережі з паралельним доступом, передає їх іншим маршрутизаторам мережі та визначає суміжні маршрутизатори. Решта маршрутизаторів мережі є суміжними для зазначеного маршрутизатора. Основний маршрутизатор зменшує мережний потік та розмір бази даних маршрутів мережі. Цей процес виконується на основі кількох етапів, котрі відзначено нижче:

- Етап EXSTART. Це перший етап обміну базами даних виявленням маршрутів за станом зв'язку. Серед двох систем визначаються головна та підлегла.
- Етап EXCHANGE. Дві системи обмінюються пакетами опису баз даних для пошуку пакетів LSA, які відсутні у базі даних кожної системи. Знайдені нові системи LSA додаються до списку повторної передачі.
- Етап LOADING. Кожен сервер відправляє сусідові пакет із виявленням маршрутів за станом зв'язку із запитом переслати всі LSA, які були додані зі списку повторної передачі на етапі EXCHANGE. У відповідь на запит сусід надсилає LSA у пакеті оновлення маршрутів.
- Етап FULL. Після того, як системи завершують обмін LSA та синхронізують свої бази даних, між ними встановлюється відповідність.

Наочне представлення процесу привітання та обміну базами даних маршрутів по стану мережі наведено на загальнодоступному рисунку 1.2.4.1.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		26

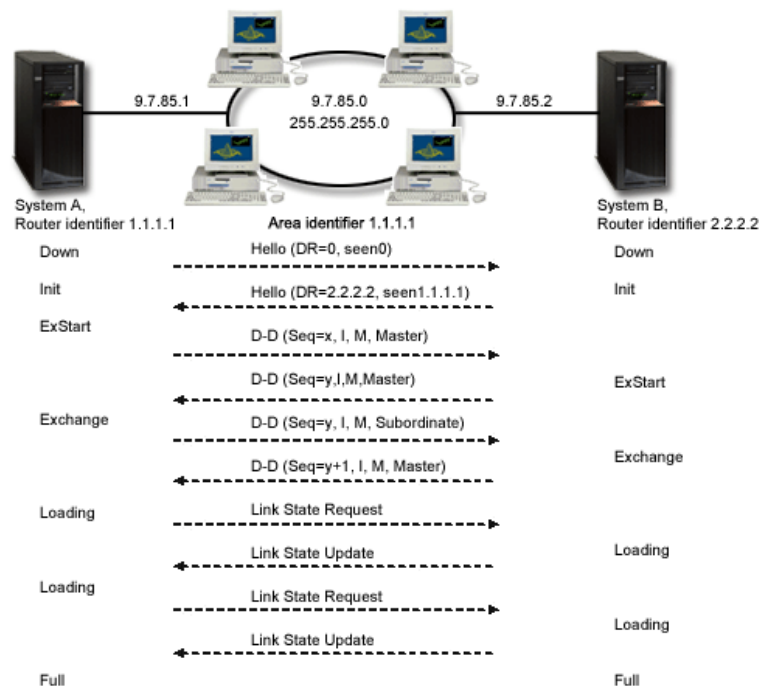


Рисунок 1.2.4.1 – Процес встановлення сусіда OSPF. Привітання та обмін базами даних маршрутів за станом мережі.

Протокол динамічної маршрутизації OSPF працює на основі метрик маршрутів, обрахунок яких він виконує за відповідною формулою для визначення найкращого та найкоротшого шляху до кінцевої підмережі. Дану формулу наведено нижче.

$$M = \sum_{i=1}^n \left[\frac{RefBW}{BW} \right]$$

де M – метрика певного маршруту;

n – кількість ділянок маршруту;

$RefBW$ (Reference BandWidth) – еталонна пропускна здатність, максимальне значення пропускної здатності для розрахунку метрик у протоколі OSPF, біт/с. За замовчуванням на момент прийняття стандарту встановлена як 108 біт/с. $RefBW$ може змінюватися адміністративно;

BW_i (BandWidth_i) – значення пропускної здатності i -тої ділянки (канального сегменту) маршруту, біт/с. За замовчуванням дорівнює фізичній пропускній здатності інтерфейсу. BW_i може змінюватися адміністративно.

Необхідно також зазначити, що метрика маршруту протоколу OSPF є величиною безрозмірною. Слід також звернути увагу на те, що у разі використання стандартного значення $RefBW$ у мережі, у якій застосовуються з'єднання Gigabit

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Ethernet (1000 Мбіт/с), АТМ (155 Мбіт/с) та деякі інші високошвидкісні з'єднання, для цих з'єднань значення BW задається таким, як і для FastEthernet, тобто 100 Мбіт/с. Якщо виникає потреба більш точно розраховувати метрики маршрутів, то необхідно встановити на кожному з маршрутизаторів мережі значення RefBW такими, що є більшим або, як мінімум, дорівнює пропускній здатності технології з найбільшою фізичною пропускну здатністю.

OSPF може працювати всередині ієрархії. Найбільшою сутністю ієрархії є автономна система. Автономна система – це група мереж із загальним адмініструванням та стратегією маршрутизації. Вона може бути поділена на області, з'єднані між собою за допомогою маршрутизаторів. Область складається з групи суміжних мереж та приєднаних хостів. Топологія області є невидимою для сутностей за межами області. Маршрутизатори в області мають однакові бази даних з інформацією про стан каналів. Топологія окремих областей дозволяє скоротити потоки маршрутизації та зменшити базу даних інформації про стан каналів для кожної окремої області. Маршрутизатор, розташований на межі областей OSPF і який з'єднує ці області з мережевою магістраллю, називається граничним маршрутизатором. Граничний маршрутизатор має кілька інтерфейсів для кількох областей і підтримує окремі бази даних про стан каналів кожної області.

1.2.5. Технологія віртуальних локальних мереж VLAN. Маршрутизація між VLAN підмережами.

Технологія віртуальних локальних мереж, або так званий VLAN (Virtual Local Area Network) являється однією з найбільш корисних та поширених технологій під час побудови сучасних локальних мереж, так як дає змогу гнучкої роботи з адресним простором, керуванням мережевого трафіку та надає можливості, щодо реалізації надійної та захищеної комп'ютерної мережі за рахунок особливостей її роботи під час впровадження в мережі.

Технологія VLAN дозволяє виконати розбиття на окремі сегменти комп'ютерної мережі, там сами надаючи можливість зменшення широкомовного шторму в мережі, як результат в мережі збільшується продуктивність за рахунок зменшення

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		28

обсягу службового трафіку. Іншими словами, трафік широкомовного типу, який належить одному домену, не буде проходити через інший. По своїй суті VLAN являє собою мітку в кадрі, передану мережею. У неї є ID, унікальний ідентифікатор, що ссилається на окерму віртуальну мережу. Під унікальний ID в кадрі відводиться 12 біт, тобто мітка може мати нумерацію від 0 до 4095, або 4096 значень. Дана технологія має відповідні типи, які мають свої особливості роботи. Таким чином розглянемо класифікацію технології VLAN:

- VLAN на основі портів чи інтерфейсів. Дозволяє адміністраторам мережі вручну призначати VLAN для кожного порту комутатора. Підходить для невеликої мережі без необхідності часткої зміни інфраструктури мережі;
- VLAN на основі MAC-адрес. Застосування цієї технології може значно збільшити гнучкість мережі. Навіть якщо користувачі часто змінюють своє фізичне розташування, адміністратору мережі не потрібно переналаштовувати мережу;
- VLAN на основі IP-підмережі. Це ефективне рішення для загальнодоступної мережі з більш високими вимогами до мобільності та спрощеного управління, а також із меншими вимогами до безпеки. За допомогою цієї технології користувачі можуть автоматично приєднуватися до нового ідентифікатора VLAN після зміни IP-адреси;
- VLAN на основі протоколу. Для мережі з кількома протоколами цей тип VLAN розробляється відповідно до застосовуваних типів протоколів та форматів інкапсуляції кадрів;
- VLAN на основі політик чи комбінований. Цей просунутий тип можна описати як комбінацію всього перерахованого вище, такий гібридний підхід може значно підвищити безпеку і гнучкість мережі.

Під час побудови комп'ютерних мережей з використанням технології VLAN, системному адміністратору важливо визначити типи каналів зв'язку для обміну інформації між вузлами в мережі. Так, під час роботи з технологією VLAN розрізняють два типи каналів зв'язку – access та trunk. Головною відмінністю між ними являється

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

те, що канали типу access використовуються для підключень кінцевих вузлів, хости, сервери, контролери, принтери, тощо, мітки VLAN підмереж яких являються заздалегіть визначиними. Натомість, канали зв'язку типу trunk являються магістральними каналами, у межах яких можуть передаватися пакети інформації різних підмереж VLAN, котрі можуть бути визначиними системним адміністраторами для забезпечення обміну інформацією. До прикладу, такі канали застосовуються під час реалізації засобів InterVLAN Routing, або так званої маршрутизації між віртуальними підмережами. Так, утворюється магістральний канал для кількох підмереж VLAN, до прикладу, на один фізичний інтерфейс маршрутизатора, де виконується налагодження підінтерфейсів та засобів інкапсуляції трафіку. Ідентифікатор VLAN, його тег, являється інкапсульованим разом з даними в пакет. У якості протоколів інкапсуляції використовуються ISL або 802.1Q. Це два типи інкапсуляції, які використовуються для передачі даних з кількох VLAN через магістральні канали. Коротко відзначимо ці стандарти.

802.1Q – це стандарт IEEE для тегування кадрів у магістралі та підтримує до 4096 VLAN. У 802.1Q транкінговий пристрій вставляє 4-байтовий тег у вихідний кадр і повторно обчислює послідовність перевірки кадрів (FCS) перед тим, як пристрій надішле кадр через магістраль. На приймальному кінці тег видаляється, а кадр пересилається до призначеної VLAN. 802.1Q не позначає кадри у native VLAN, але позначає тегамі всі інші кадри, які передаються та приймаються по магістралі. Коли ви налаштовуєте магістраль 802.1Q, ви повинні переконатися, що ви налаштовуєте ту саму native VLAN з обох сторін магістралі. IEEE 802.1Q визначає єдиний екземпляр spanning tree, який працює у native VLAN для всіх VLAN у мережі. Це називається Mono Spanning Tree (MST). Стандарту 802.1q не вистачає гнучкості та можливості балансування навантаження PVST, які доступні під час використання протоколу ISL.

ISL – це власний протокол Cisco для з'єднання кількох комутаторів і підтримки інформації про VLAN, коли трафік проходить між комутаторами. Використовувався для з'єднання типу точка-точка. На даний момент часу протокол являється застарілим. ISL надає можливості транкінгу VLAN, зберігаючи повну

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

швидкість з'єднання Ethernet у повнодуплексному або напівдуплексному режимі. ISL працює в середовищі точка-точка і може підтримувати до 1000 VLAN. У ISL вихідний кадр інкапсулюється та додається додатковий заголовок перед тим, як кадр передається по магістральному каналу. На приймальному кінці заголовок видаляється, а кадр пересилається до призначеної VLAN. ISL використовує протокол Spanning Tree (PVST), який запускає один екземпляр протоколу Spanning Tree Protocol (STP) для кожної VLAN. PVST дозволяє оптимізувати розташування кореневого комутатора для кожної VLAN і підтримує балансування навантаження VLAN через кілька магістральних каналів.

Маршрутизація між VLAN-ами являється класичною маршрутизацією підмереж. Кожен новоутворений сегмент мережі на основі VLAN-ів являється повноцінною локальною мережею, яка являється відокремленою від інших VLAN мереж, так як має свій унікальний ідентифікатор. Як відомо маршрутизація між підмережами неможлива на 2 рівні моделі OSI, а отже для реалізації обміну інформацією між різними підмережами необхідно застосування інтелектуального комутатора або маршрутизатора, які вже працюються на 3 рівні моделі OSI і дозволяються виконувати маршрутизацію між підмережами. Таким чином кожна підмережа VLAN, для реалізації маршрутизації, повинна володіти своїми параметрами IP-адресації. Під час забезпечення маршрутизації між VLAN-ами використовується метод інкапсуляції, у тому випадку, коли через один фізичний магістральний канал зв'язку проходять пакети декількох підмереж VLAN. Процес інкапсуляції це свого роду процес загортання одного кадру в інший. На мережевому обладнанні компанії Cisco існує два типи інкапсуляції стандарт *dot1q*, який реалізовано на основі стандарту IEEE 802.1q та пропрієтарний протокол компанії Cisco – *ISL*. Таким чином інкапсулюючи відповідні кадри на маршрутизаторі ми виконуємо їх передачу, де згодом інкапсуляція прибирається і відповідний отриманий пакет передається далі до кінцевого отримувача.

Для виконання маршрутизації між VLAN підмережами використовуватиметься тип інкапсуляції *dot1q*. Так як інкапсуляція *dot1q* основана на стандарті зв'язку 802.1q, то всередину кадру розміщується відповідний тег, який вказує на

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

відповідну належність трафіка до певного VLAN, таким самим забезпечуючи маршрутизацію між різними VLAN-підмережами.

1.2.6. Технологія Network Address Translation, або NAT. NAT у режимі Overload, або Port Address Translation.

NAT (Network Address Translation) – це механізм у мережах TCP/IP, котрий дозволяє змінювати IP-адресу у заголовку пакету, що проходить через пристрій маршрутизації трафіку. Отримуючи пакет інформації маршрутизатор комп'ютерної мережі займається обробкою та маршрутизацією цього пакету інформації, в залежності від налагоджених правил фільтрації та маршрутизації трафіку у мережі. У випадках, коли трафік необхідно надсилати у зовнішні зони комп'ютерної мережі, для прикладу глобальну мережу інтернет, маршрутизатор, в результаті переходу від внутрішньої частини мережі для NAT у зовнішню, виконує перетворення деякої внутрішньої IP-адреси у деяку зовнішню адресу, котра обирається на основі правил функціонування технології NAT.

У сучасних комп'ютерних мережах технологія NAT покликана для вирішення актуального питання у постійному зростанні користувачів комп'ютерних мереж, а також недостатній кількості для забезпечення усіх кінцевих користувачів параметрами IP-адресації версії 4. У 80-х роках XX століття заклали основу для протоколу IP (Internet Protocol) версії 4, що дозволяє створювати приблизно 4,3 мільярдів адрес, але ніхто не припускав, що цей запас так швидко вичерпається. З кожним роком з'являлося все більше користувачів, але ліміт параметрів IPv4 адресації уже давно є вичерпаним. Таким чином, технологія NAT дозволяє тимчасово відтермінувати неминуче, а саме відмову від протоколу IPv4, котрий з часом буде витіснено наступником даного протоколу, а саме IP версії 6. Так, основною функцією NAT є збереження публічних адрес, проте додатково він здатний забезпечувати конфіденційність мережі шляхом приховування внутрішніх IPv4 адрес від зовнішньої, тим самим створюючи умови для реалізації одностороннього зв'язку, де у якості ініціаторів такого підключення є лише користувачі локальної мережі. За потреби, мережеві адміністратори мають можливість забезпечити реалізацію

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		32

локальних серверів, доступ до яких може бути отриманий з глобальної мережі на основі технології переадресації портів (Port Forwarding), про яку згодом буде відзначено у роботі.

Технологія NAT може бути реалізована на основі кількох методів, а саме: статичний NAT (Static NAT), динамічний NAT (Dynamic NAT), перевантажений NAT (NAT Overload). Також є досить специфічні методи реалізації технології NAT, так як «Постійна трансляція» та «Трансляція між парою». Усі ці методи мають власні переваги та недоліки, про які зазначимо далі.

Статичний NAT (Static NAT). Метод статичної трансляції IPv4 адреси застосовують для відображення незареєстрованої IP-адреси (внутрішню) на зареєстровану IP-адресу (зовнішню) на основі співвідношення один до одного. Найчастіше використовується в корпоративних мережах, коли необхідно, щоб будь-яка IP-адреса завжди була доступна з глобальної мережі. Найчастіше статичним IP наділяють сервери і поміщають їх в DMZ (Demilitarized Zone).

Динамічний NAT (Dynamic NAT). Метод динамічної трансляції IPv4 адреси відображає незареєстровану IP-адресу (внутрішню) на зареєстровану адресу (зовнішню) з групи зареєстрованих IP-адрес. Динамічний NAT також встановлює безпосереднє відображення між незареєстрованими та зареєстрованими адресами, але відображення може змінюватись залежно від зареєстрованої адреси, що є доступна в деякому пулі (pool – діапазон) адрес під час комунікації.

Перевантажений NAT (NAT Overload). Це найбільш поширений метод реалізації технології NAT у комп'ютерних мережах. Цей тип NAT має велику кількість назв, таких як: NAT Overload, Many-to-One, PAT (Port Address Translation) та IP Masquerading. Однак у більшості джерел вказується як NAT Overload або PAT. Перевантажений NAT представляє собою форму динамічного NAT, який відображає кілька незареєстрованих адрес (внутрішніх) в одну єдину зареєстровану IP-адресу (зовнішню), використовуючи різні порти під час трансляції. При перевантаженні кожен комп'ютер у приватній мережі транлюється на ту саму адресу, але з різним номером порту, тим самим забезпечуючи можливість, щодо комунікації у зовнішніх мережах інтернет.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

Що стосується методів «Постійна трансляція» та «Трансляція між парою», то можна коротко відзначити про них наступне. Постійна трансляція між парою «внутрішня адреса: внутрішній порт» і «публічна адреса: публічний порт» означає, що кожне з'єднання, ініційоване з внутрішньої адреси, дозволяє надалі отримувати йому пакети з будь-якого порту того публічного хоста, до якого він відправляв пакети раніше. Трансляція між парою створює канал трансляції між деякими «внутрішня адреса: внутрішній порт» і «публічна адреса: публічний порт», при якій пакети що надходять до внутрішнього хосту тільки з одного порту публічного хоста, тобто з того, на котрий внутрішній хост вже здійснював обмін.

1.2.7. Технологія Service-level Agremance, або SLA.

SLA (Service-level Agremance) – це технологія, що дозволяє забезпечити перевірку рівня комунікації між тими чи іншими вузлами комп'ютерних мереж. Вона дозволяє виконувати погодження рівнів обслуговування між клієнтом та сервером, або між різними вузлами комп'ютерних мереж, а також дозволяє забезпечити моніторинг та збір інформації про продуктивність мережі. До прикладу, використання IP SLA надає можливості збору інформації про час відповіді, затримки, втрату пакетів інформації, оцінку якості підключення (MOS), перевірку відповідей від серверів, тощо. Уся ця зібрана інформація дозволяє якісно та оперативно приймати рішення, щодо роботи комп'ютерної мережі. Використовуючи IP SLA у комбінації з іншими технологіями, можна досягти високого рівня відмовостійкості, швидкості та надійності будь-яких комп'ютерних мереж.

Для кращого розуміння, розглянемо приклади використання технології SLA. Використовуючи технологію SLA для стеку протоколів TCP/IP можна створити правила перевірки на доступність використовуючи протокол ICMP та на основі отриманого результату приймати відповідні дії в комп'ютерні мережі. Таке рішення може бути застосованим для створення динамічних таблиць маршрутизації, коли вихід в глобальну мережу інтернет може виконуватися на основі кількох підключень до мереж провайдерів. Використання протоклу SLA дозволяє забезпечувати відслідковування доступності шлюзу за замовчування, для одного з каналі

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

зв'язку, та у випадку виходу з ладу одного з них виконувати автоматичне переключення засобів маршрутизації на інший канал зв'язку, що у цей час повинен являється доступним. Таке рішення може застосовуватися не лише у випадках мультипровайдерного підключення, а також для забезпечення коректної роботи внутрішньої локальної мережі. До прикладу, на основі SLA можна реалізувати різні маршрути до однієї і тієї ж локальної мережі без використання засобів динамічної маршрутизації, а також забезпечувати автоматичне переключення між цими маршрутами на основі результатів перевірки на доступність, а також правил метрики маршрутів, що можуть бути налагоджені мережевими адміністраторами власноруч. Це не єдиний приклад застосування технології SLA, але один з найбільш поришених варіантів.

Використання технології SLA надає мережевому адміністратору гнучкість, щодо налагодження та перевірки на доступність тих чи інших сервісів, як у глобальних так і в локальних мережах. В поєднанні з розширеними списками доступу, що були розглянуті нами раніше, у системного адміністратора з'являється більш розширений набір інструментів для забезпечення тих чи інших потреб, щодо маршрутизації, перенаправлення та блокування того чи іншого трафіку, що передається у комп'ютерних мережах, а також створення правил, щодо його передачі.

1.2.8. Мультипровайдерні підключення. Переваги та недоліки.

Мультипровайдерні підключення це один з високоефективних способів підвищення рівня відмовостійкості та надійності експлуатації комп'ютерних мереж. Такі рішення дозволяють мережевим адміністраторам налагоджувати правила проходження трафіку з глобальної мережі в локальну, і навпаки, на основі двох або більше каналів підключення до мережі інтернет провайдерів, або так званого IPS (Internet Service Provider). Кількість каналів зв'язку залежить від конкретних потреб, а також рівня відмовостійкості та надійності, котрий необхідно забезпечити. Важливо відзначити, що у ролі підключень до IPS можна розглядати не лише підключення до окремих провайдерів, але й підключення до однакового інтернет провайдера на основі кількох виділених каналів зв'язку для обробки мережевого трафіку

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		35

та отримання доступів до глобальної мережі інтернет. Таке рішення дозволяє забезпечити балансування трафіку між різними каналами підключення до ISP, забезпечити аварійне перемикання у разі виходу одного з каналів зв'язку для виходу в глобальну мережу інтернет, а також вищий рівень доступності локальних сервісів з глобальної мережі інтернет за рахунок наявності кількох публічних IP-адрес, котрі можуть бути використаними для забезпечення інформаційного обміну.

Мультипровайдерні рішення у рамках реалізації проектів комп'ютерних мереж мають високий рівень попиту, а також високий рівень потреби до компетенцій мережевого адміністратора у питаннях налаштування та підтримки мультипровайдерних підключень. Також, таке рішення може потребувати додаткових ресурсів. При цьому вони також мають ряд особливостей, котрі варто враховувати під час реалізації мультипровайдерного підключення та активного використання усіх можливостей, що надають такі рішення. Так, однією з проблем може постати питання вибору глобальної IP-адреси для забезпечення підключення, або проблема переадресації портів до внутрішніх сервісів. Вони здатні забезпечити вищий рівень загальної пропускної здатності інтернет з'єднання, що позитивно впливає на швидкість та стабільність з'єднання, дозволяють забезпечити розподіл трафіку між провайдерами, що може забезпечити більш ефективне використання мережевих ресурсів і зниження затримок. Наявність декількох з'єднань може покращити мережеву безпеку, оскільки атака на одного провайдера не призведе до повного відключення за рахунок наявності інших.

Мультипровайдерні підключення є доцільними для великих компаній або організацій, що потребують високої надійності та швидкості інтернет-з'єднання. Вони забезпечують значні переваги у плані стабільності та гнучкості, але можуть бути занадто дорогими та складними для малих підприємств чи окремих користувачів.

1.2.9. Переадресація портів, або Port Forwarding.

Переадресація портів, або Port Forwarding – це технологія, що дозволяє забезпечувати безпеку в комп'ютерних мережах захищаючи їх від небажаного зовнішнього трафіку, при цьому забезпечуючи наявність тунелю для обміну інформацією

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

з чітко визначеними внутрішніми серверами на основі їх IP-адрес та портів призначення. За своєю суттю, переадресація портів необхідна для коректної роботи технології NAT у глобальних комп'ютерних мережах. Ця технологія дозволяє захоплювати трафік, до прикладу, що надходить на деякий зовнішній інтерфейс та перенаправляти його до внутрішніх служ та сервісів, тим самим забезпечуючи коректний обмін інформацією у глобальних мережах, та за необхідності у локальних мережах. Для кращого розуміння роботи даної технології, розглянемо деякий приклад її роботи.

Уявімо комп'ютерну мережу, що підключена до глобальної мережі інтернет через мережу деякого інтернет провайдера, котрий надає клієнту статичну IP-адресу, або так звану зовнішню IP-адресу, котра являється реальною адресою та доступна усім користувачам зовнішнього світу. Системний адміністратор локальної мережі має намір створити загальнодоступний ресурс у локальній мережі та надати доступ для його використання користувачам глобальної мережі, або створити ресурс для власних потреб з можливістю його використання з будь-якої точки світу з підключенням до глобальної мережі інтернет. У межах даного прикладу у якості сервісу можна розглядати протокол RDP (Remote Desktop Services), доступ до якого системний адміністратор має намір відкрити для отримання доступу. Так, деякий локальний сервер з IP-адресою 192.168.1.100 та локальним портом 3389 для роботи протоколу RDP буде доступний у межах локальної мережі, в той час як в глобальній мережі, вихід до якої виконується на основі технології NAT Overload через реальну IP-адресу 109.251.146.251, доступ до локального сервера, за звичайних умов, буде відсутній за рахунок особливостей роботи технології NAT Overload, про яку відзначалося раніше. У такому випадку, на допомогу системному адміністратору може бути покликана технологія Port Forwarding, котра дозволить створити деяке правило переадресації трафіку з глобальної мережі, що надходить на IP-адресу 109.251.146.251 з портом призначення 3389, до локальної мережі на IP-адресу призначення 192.168.1.100 на порт призначення 3389. Таким чином, системний адміністратор матиме змогу реалізувати та забезпечити роботу тих чи інших потреб у межах локальної мережі. Важливо відзначити, що переадресація не

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

обов'язково повинна відбуватися за ідентичним портом локальної служби на зовнішній IP-адресі. Простими словами, переадресація порту може бути виконана з зовнішньої мережі, до прикладу з адреси 109.251.146.251 на порт 10, до внутрішнього серверу за адресою 192.168.1.100 на порт 3389. Таким чином виконується робота технології переадресації портів.

1.3. Підготовка технічних рішень.

Переходимо до етапу підготовки технічних рішень у відповідності до технічного завдання. У межах даного етапу буде описано застосування тих чи інших протоколів чи технологій з метою забезпечення конкретних технічних потреб, що повинні бути дотриманими в проекті.

Розпочнімо з основи нашого проекту. Провівши аналіз питань забезпечення високого рівня надійності та безпеки комп'ютерних мереж було прийнято рішення використовувати технологію Failover з використанням міжмережевого екрану компанії Cisco під назвою ASA (Adaptive Security Appliance). Таке технічне рішення дозволяє забезпечити основні потреби у питаннях високої надійності, доступності та безпеки на етапі побудови проекту, а згодом може запропонувати інструменти для більш глибоких налаштувань для забезпечення тих чи інших безпекових потреб для деякої кампусної мережі організації. Використання технології Cisco ASA Failover за дотримання певних умов, також дозволяє забезпечити безшовний перехід під час перепідключення до іншого інтернет провайдеру чи у разі виходу з ладу активного міжмережевого екрану та реактивації його функцій на резервному. Безшовний перехід відбуватиметься за рахунок впровадження додаткового каналу обміну інформацією між міжмережевими екранами ASA під назвою Stateful Link. Таке рішення дозволяє автоматично відновлювати усі наявні сесії підключення до глобальної мережі провайдеру, а також дозволить виконувати автоматичне перепідключення для VPN з'єднань, передачі потокового відео, аудіо, сесій TCP, тощо, що також є значним плюсом використання даної технології.

У якості додаткового засобу підвищення рівня надійності комп'ютерної мережі, було прийнято рішення застосовувати протокол динамічної маршрутизації

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		38

OSPF, використання якого дозволяє побудувати декілька маршрутів для досягнення кінцевої підмережі в питаннях маршрутизації мережевого трафіку. Таким чином, забезпечивши більш ніж один канал зв'язку можна значно підвищити рівень надійності та відмовостійкості комп'ютерної мережі. Це не єдина мета застосування даного протоколу. Його наявність в проекті комп'ютерної мережі дозволять значно спростити процес масштабування комп'ютерної мережі для подальшого розширення її можливостей у питаннях обслуговування клієнтів чи розміщення серверів, сервісів, служб, тощо. Для зменшення рівня навантаження на мережеве обладнання комп'ютерної мережі, протокол динамічної маршрутизації OSPF згодом може бути налагоджений з використання мультizonальних рішень, що дозволить уникати перебудови та переобрахунків метрик маршрутів на усьому мережевому обладнанні, а виконувати це лише для тих, хто належить конкретній зоні OSPF чи є граничним маршрутизатором, що пов'язаний з даною мережевою зоною. Так як проект комп'ютерної мережі, що розроблюється по своїй суті являється основою для впровадження більш серйозніших рішень в плані маршрутизації трафіку до клієнтів різних підмереж, то використання такого рішення на даному етапі не внесе значного підвищення продуктивності. Тому, в проекті, на початковому етапі, планується розробка лише одного зонального рішення, котре згодом може бути розподілене на необхідну кількість зон OSPF.

Для рішень задач маршрутизації трафіку до глобальних мережей буде використовуватися технологія IP SLA (Service-Level Agrimence), на основі якої можна реалізувати правила моніторингів станів каналі зв'язку з підмережами провайдерів, а також на основі результатів їх роботи, забезпечити динамічні оновлення статичних параметрів маршрутизації до шлюзів за замовчування у мережі провайдерів. Використовуючи протокол ICMP, котрий являється основою для діагностування роботи комп'ютерних мережей, а також відомий як утиліта «ping», дозволить виконувати постійний моніторинг та швидке прийняття рішень. Також, даний протокол може бути використаний як зручний інструмент для моніторингу станів каналі зв'язку, що також буде корисним під час наявності декількох можливих маршрутів до глобальної мережі.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		39

Важливо також відзначити проблему підключення міжмережевих екранів до мережі провайдерів, котра полягає у необхідності реалізації комутації між одним каналом зв'язку, до умовного маршрутизатора провайдера, та двом міжмережевим екранам. Загалом, рішення даної проблеми може бути представленим у використанні звичайного комутатора, котрий виконує лише об'єднання. Важливо відзначити, що у разі наявності високого рівня мережевого трафіку, необхідно задуматися про реалізації агрегованих каналів зв'язку між міжмережевими екранами та даним комутатором, щоб уникнути проблеми вузької ділянки пропускнуої здатності комп'ютерної мережі.

В межах проекту для реалізації підключення до підмережі провайдера на основі параметрів IPv4-адресації варто використовувати технологію NAT в режимі Overload, або так званий PAT. Як зазначалося раніше, використання даної технології привносить підвищений рівень безпеки під час експлуатації комп'ютерних мережей за рахунок приховування фізичних вузлів локальної мережі в глобальній мережі інтернет, але при цьому створює проблему у необхідності забезпечувати доступ до внутрішніх серверів з глобальних мереж. Так, у проекті буде реалізовано функцію Port Forwarding для забезпечення засобів трансляції деякого глобального траку до внутрішніх серверів, сервісів чи служб.

Що стосується інших технологій, таких як VLAN, InterVLAN Routing, DHCP, DNS, то їх впровадження виконується з метою забезпечення наочного прикладу роботи проекту комп'ютерної мережі під час демонстрації роботи тих чи інших функцій та засобів, що будуть реалізованими в межах даного проекту. Варто відзначити лише те, що технологія VLAN також виступає у ролі додаткового механізму забезпечення безпеки експлуатації комп'ютерних мереж за рахунок розподілення мережевого трафіку та можливостей налагодження правил маршрутизації трафіку для конкретних VLAN підмереж на основі стандартних чи розширених списків контролю доступів, що також дозволить застосовувати засоби фільтрації мережевого трафіку для конкретних підмереж та усім користувачам, що їм належать.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		40

РОЗДІЛ 2. РОЗРОБКА ФІЗИЧНОЇ ТОПОЛОГІЇ ПРОЕКТУ. ІІ НА- ЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ.

2.1. Проблеми побудови фізичної топології та впровадження і поєднання техноло- гій.

Розпочнімо виконання пратичної частини з проблемних питань, що були ви-
явлені в ході виконання кропітливої роботи, щодо пошуку оптимального рішення
побудови проекту та забезпечення найвищого рівня надійності його експлуатації та
відмовостійкості.

Виконуючи процес побудови проекту комп'ютерної мережі, було виконанно
спроби побудови та тестування декількох проекті комп'ютерної мережі, результати
тестування яких не були успішними. В ході виконання дослідження одного з них,
топология якого відзначена на рисунку 2.1.1, було виявлено проблему у роботі за-
собів маршрутизації мережевого трафіку, а саме проблему у додаванні не оптима-
льних маршрутів для досягнення тих чи інших кінцевих підмереж. Про це і пого-
воримо далі.

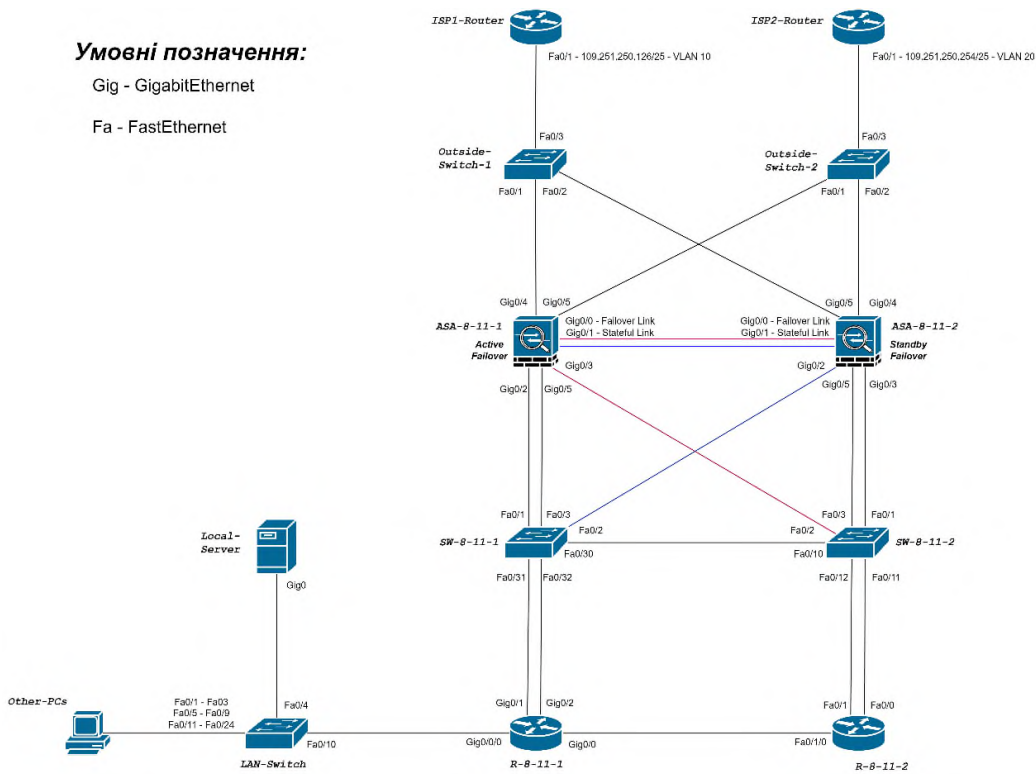


Рисунок 2.1.1 – Фізична топологія варіанту реалізації проекту комп'ютенної
мережі.

Основна суть реалізації проекту на основі таких топологій є виконання спроби забезпечення альтернативних каналів зв'язку з міжмережевими екранами Cisco ASA, для підвищення рівня відмовостійкості експлуатації проекту комп'ютерної мережі. Основна проблем використання такої топологій – це проблеми роботи протоколу OSPF. Дослідження даної топологій виконувалися як на основі реального тестового стенду, про який буде відзначено згодом, так і на основі засобів віртуалізації роботи мережевого обладнання EVE-NG, результати роботи яких було повністю ідентичними в питаннях спроб оптимізації роботи вище зазначеного проекту та рішення проблеми, що була виявлена в ході виконання досліджень.

Коротко відзначимо, що робота інших функцій та технологій на основі вище описаних способів організацій фізичних топологій проекту була успішною та перевіреною на основі реального обладнання та багаторазово проведених тестувань. Ось деякі з прикладів.

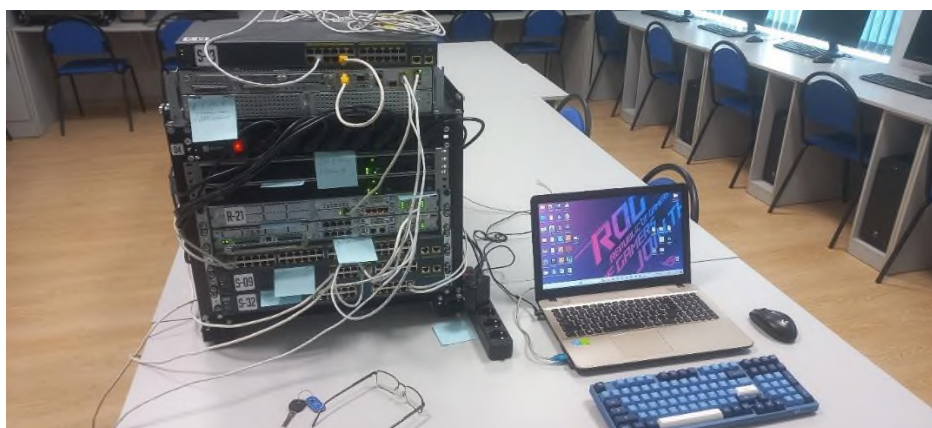


Рисунок 2.1.2. – Тестовий стенд на якому виконувалися тестування.

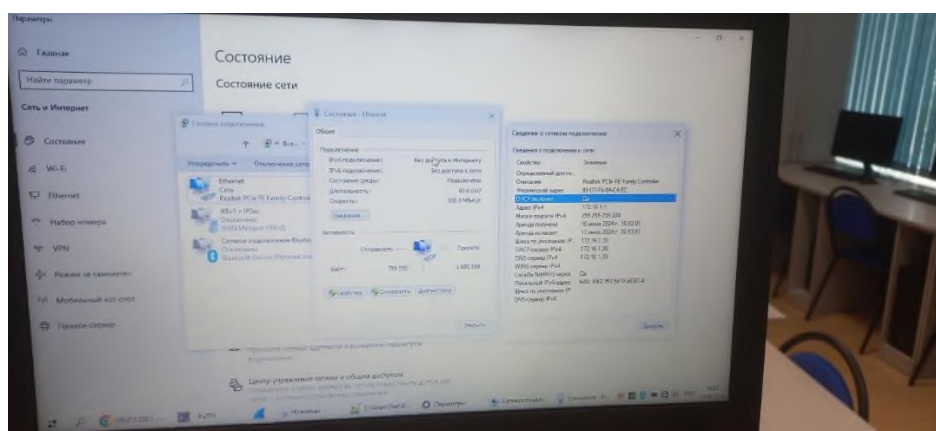


Рисунок 2.1.3. – Перевірка роботи DHCP-сервера на базі мережевого маршрутизатора R-8-11-1 для VLAN12.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефименко А.А				42
Змн.	Арк.	№ докум.	Підпис	Дата		

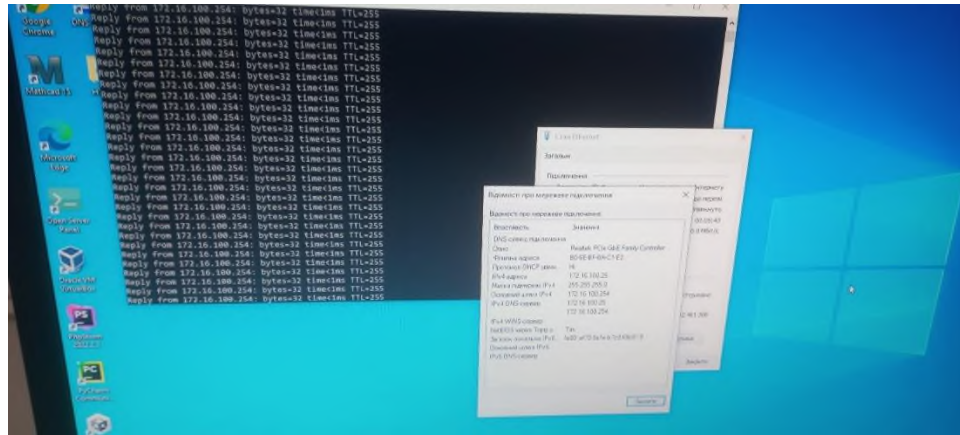


Рисунок 2.1.4. – Результат успішної роботи інформаційного обміну зі шлюзом за замовчуванням для підмережеві локальних серверів.

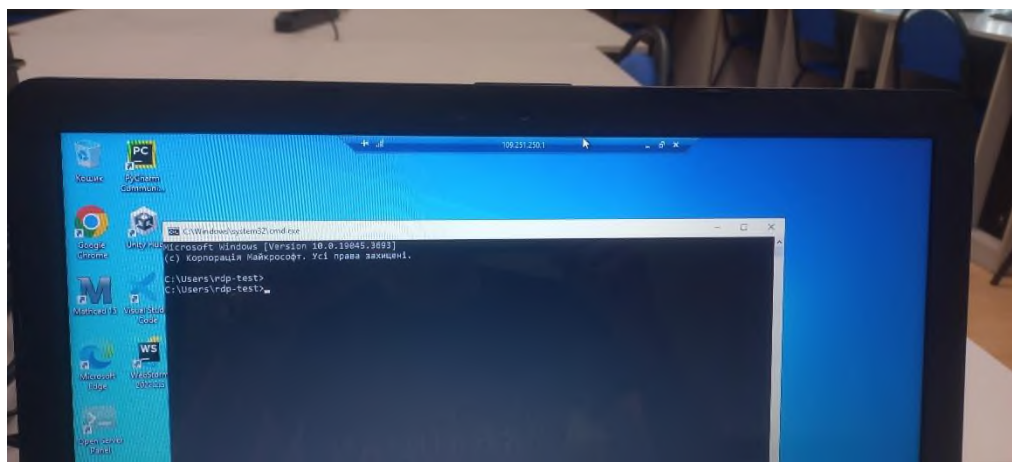


Рисунок 2.1.5 – Результат успішного тестування роботи переадресації портів з глобальних мереж до локальних служб та сервісів у проекті. Приклад роботи протоколу RDP до локального сервера з глобальної мережі.

Саме на етапі перевірки роботи альтернативних каналів зв'язків та перевірки рівня відмовостійкості проекту, було виявлено проблему у роботі засобів маршрутизації мережевого трафіку. В ході тестування роботи вище наведеної топології побудови каналів зв'язку між маршрутизаторами та міжмережевим екраном (рис. 2.1.1), виникає проблема у доступності підмереж, при чому результати відсутності зв'язку з підмережами є не стабільними. Іноді зв'язок втрачається з підмережею 10.0.1.0/29, іноді з підмережею 10.0.2.0/29, іноді через канал зв'язку між маршрутизаторами R-8-11-1 та R-8-11-2. Дану проблему вдалося зафіксувати для підмережі 10.0.2.0/29, котру продемонстровано на рисунках 2.1.6 та 2.1.7 нижче.

		Колесник Д.В.			Арк.
		Ефіменко А.А.			43
Змн.	Арк.	№ докум.	Підпис	Дата	

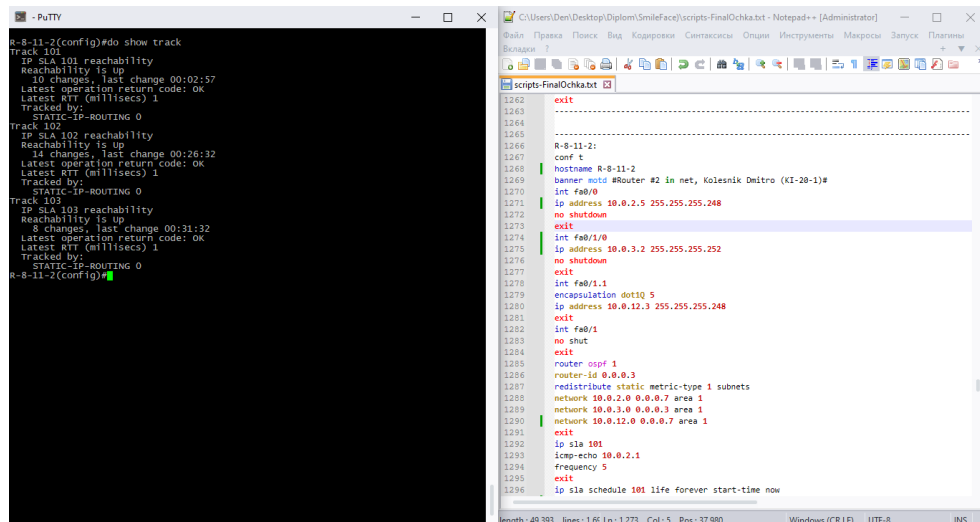


Рисунок 2.1.6. – Перевірка статусів доступності каналів зв'язку між маршрутизатором R-8-11-2 та міжмережовим екраном Cisco ASA-8-11-1, котра на момент тестування є Failover Active.

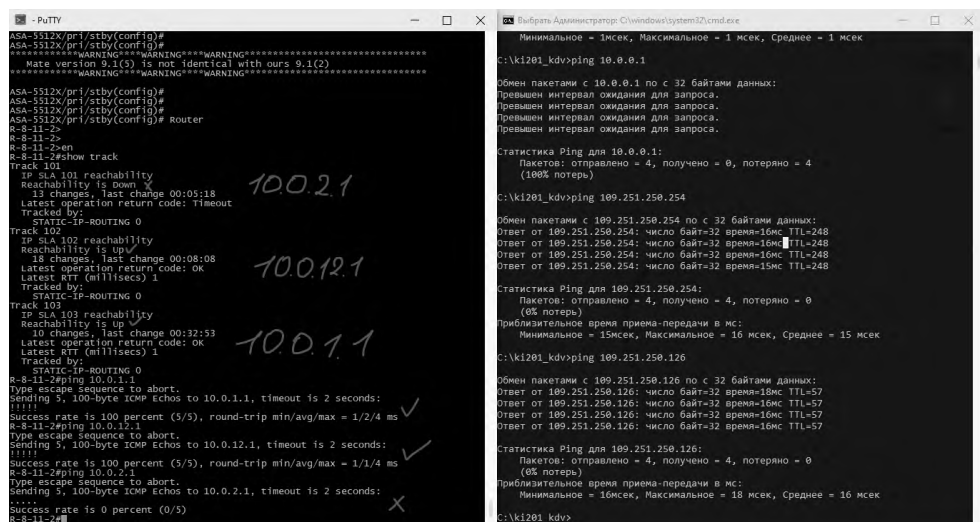


Рисунок 2.1.7. – Відсутність прямого зв'язку між маршрутизатором R-8-11-2 та міжмережовим екраном Cisco ASA, що перебуває у активному стані Failover.

Як відзначено на рисунках вище, дана проблема є плаваючою. Її ігнорування веде до некоректної роботи комп'ютерної мережі, навіть у випадках коли існує працюючих резервний канал обміну мережевого трафіку. Іноді усі тестування каналів зв'язку вдавалося пройти лише одному з маршрутизаторів, в той час як інший не міг пройти тестування на етапі перевірки наявності зв'язку за маршрутом, котрий проходить крізь підмережу 10.0.3.0/30, що являється каналом обміну мережевим трафіком між маршрутизаторами R-8-11-1 та R-8-11-2, що також використовується

		Колесник Д.В.			Арк.
		Ефіменко А.А.			
Змн.	Арк.	№ докум.	Підпис	Дата	44

як один з резервних маршрутів для виходу в глобальну мережу крізь міжмережевий екран Cisco ASA. Потенційна проблема могла бути викликана списками контролю доступу за замовчуванням, що використовується на міжмережевому екрані Cisco ASA, але в ході виконання тестувань дане припущення було спростоване за рахунок створення дозволу на будь-який вхідний трафік у мережі, що був застосований як глобальний список контролю доступу. Додатково, на етапі тестування, канал зв'язку між мережевими маршрутизатора не є сильно завантаженим, але при роботі з великим рівнем навантаження у даному каналі зв'язку виникатимуть проблеми з рівнем затримок у комп'ютерній мережі. До прикладу, так як канал зв'язку між маршрутизаторами R-8-11-1 та R-8-11-2 покликаний забезпечити коректну роботу локальної мережі підприємства, а також слугувати у ролі останнього можливого каналу зв'язку між Cisco ASA, то використання даного каналу має обиратися в останню чергу. Це одна з особливостей, котру необхідно враховувати.

Провівши дослідження даної особливості, було встановлено причину такої поведінки комп'ютерної мережі. Вона полягала у тому, що різні мережеві вузли застосовували різні маршрути до кінцевих підмереж, тим самим створюючи проблеми у засобах роботи маршрутизації. Це вдалося встановити на основі діагностичної команди «*show ip route*» та «*show route*». Приклади наведено на рисунках 2.1.8 та 2.1.9 нижче.

```

- PuTTY
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is 109.251.250.126 to network 0.0.0.0

O 172.16.1.128/24 [110/2] via 10.0.1.5, 1:39:56, Link-to--R-8-11-1
O 172.16.1.32/24 [110/2] via 10.0.1.5, 1:39:56, Link-to--R-8-11-1
O 172.16.1.0/24 [110/2] via 10.0.1.5, 1:39:56, Link-to--R-8-11-1
O 172.16.100.0/24 [110/2] via 10.0.1.5, 1:39:56, Link-to--R-8-11-1
O 172.16.1.96/24 [110/2] via 10.0.1.5, 1:39:56, Link-to--R-8-11-1
O 172.16.1.64/24 [110/2] via 10.0.1.5, 1:39:56, Link-to--R-8-11-1
C 10.0.12.0/24 [110/2] via 10.0.1.5, 1:39:56, Link-to--R-8-11-1
C 10.0.2.0/24 [110/2] via 10.0.1.5, 1:39:56, Link-to--R-8-11-1
C 10.0.3.0/24 [110/2] via 10.0.1.5, 1:39:56, Link-to--R-8-11-1
C 10.0.1.0/24 [110/2] via 10.0.1.5, 1:39:56, Link-to--R-8-11-1
C 109.251.250.0/24 [110/2] via 109.251.250.126, 1:39:56, Link-to--ISP-1
C 109.251.250.128/24 [110/2] via 109.251.250.126, 1:39:56, Link-to--ISP-2
C 192.168.1.0/24 [110/2] via 192.168.1.1, 1:39:56, Link-to--ISP-1
C 192.168.2.0/24 [110/2] via 192.168.2.1, 1:39:56, Link-to--ISP-2
S* 0.0.0.0/0 [110/0] via 109.251.250.126, 1:39:56, Link-to--ISP-1
ASA-5512X/pr1/act(config)#
  
```

Рисунок 2.1.8. – Маршрути до локальних підмереж маршрутизатора R-8-11-1 на міжмережевому екрані Cisco ASA. Маршрут пролягає крізь інтерфейс з ім'ям «Link-to--R-8-11-1»

```
R-8-11-1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 10.0.12.1 to network 0.0.0.0

oE2 0.0.0.0/0 [110/1] via 10.0.12.1, 00:00:34, GigabitEthernet0/2.1
O 10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
O 10.0.1.0/29 [110/3] via 10.0.12.1, 00:00:02, GigabitEthernet0/2.1
O 10.0.2.0/29 [110/3] via 10.0.12.1, 00:00:34, GigabitEthernet0/2.1
C 10.0.3.0/30 is directly connected, GigabitEthernet0/0
L 10.0.3.1/32 is directly connected, GigabitEthernet0/0
C 10.0.12.0/29 is directly connected, GigabitEthernet0/2.1
L 10.0.12.5/32 is directly connected, GigabitEthernet0/2.1
L 172.16.0.0/16 is variably subnetted, 12 subnets, 3 masks
C 172.16.1.0/27 is directly connected, GigabitEthernet0/0/0.12
C 172.16.1.30/32 is directly connected, GigabitEthernet0/0/0.12
C 172.16.1.32/27 is directly connected, GigabitEthernet0/0/0.13
L 172.16.1.62/32 is directly connected, GigabitEthernet0/0/0.13
C 172.16.1.64/27 is directly connected, GigabitEthernet0/0/0.14
C 172.16.1.66/27 is directly connected, GigabitEthernet0/0/0.14
C 172.16.1.96/27 is directly connected, GigabitEthernet0/0/0.15
L 172.16.1.126/32 is directly connected, GigabitEthernet0/0/0.15
C 172.16.1.128/27 is directly connected, GigabitEthernet0/0/0.16
C 172.16.1.158/32 is directly connected, GigabitEthernet0/0/0.16
C 172.16.100.0/24 is directly connected, GigabitEthernet0/0/0.100
L 172.16.100.254/32 is directly connected, GigabitEthernet0/0/0.100
R-8-11-1#
```

Рисунок 2.1.9. – Маршрут до міжмережевого екрану, котрий виконується на основі підмережі 10.0.12.0/29, що відповідає інтерфейсу «Link-for--All» міжмережевого екрану Cisco ASA

Такі невідповідності у побудові маршрутів і призвели до відсутності зв’язків між різними підмережами, так як маршрути для їх досягнення є різними. Такі умови, під час обміну інформацією означають, що маршрутизатори просто не здатні забезпечити коректний обмін. Тому, щоб уникнути вище описаної проблеми проведемо дослідження, щодо побудови оптимальних маршрутів та налагодження їх метрик для врахування в роботі протоколу динамічної маршрутизації OSPF. Побудуємо невелику модель мережі для подальших демонстрацій (рис. 2.1.10.).

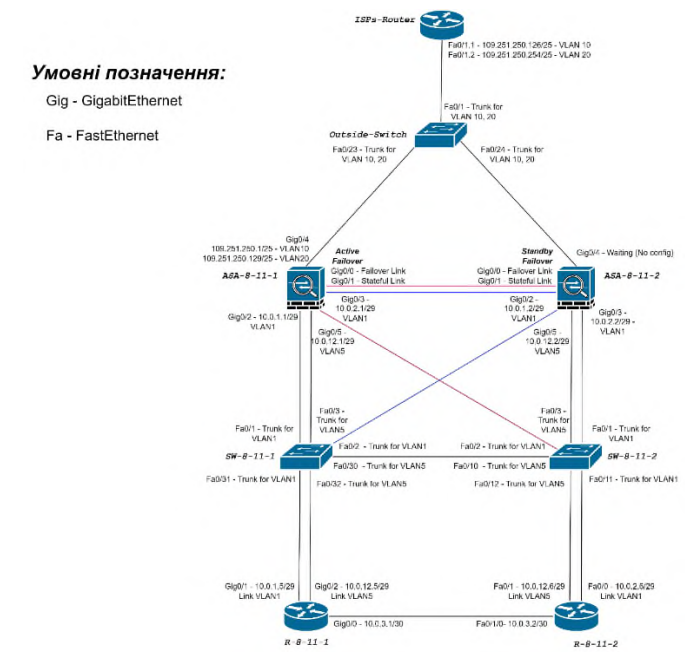


Рисунок 2.1.10 – Тестова модель фізичної топології, що досліджується

Використовуючи рисунок 2.1.10, проведемо дослідження потенційних шляхів проходження мережевого трафіку. Загалом, для кожного з маршрутизаторів було виявлено кілька шляхів проходження для досягнення одного з інтерфейсів активного міжмережевого екрану Cisco ASA. Ці маршрути наведено у таблиці 2.1.1 нижче. Важливо відзначити, що метрики маршрутів у даному випадку обраховуються на основі значень за замовчування, що важливо враховувати для розуміння суті проблеми.

Таблиця 2.1.1 – Таблиця маршрутизації протоколу OSPF

Вузол	Маршрут	Метрика OSPF
<u>Якщо ASA-8-11-1 Failover Active</u>		
R-8-11-1	R-8-11-1(GigabitEthernet0/1) – SW-8-11-1(FastEthernet0/31, FastEthernet0/1) – ASA-8-11-1(GigabitEthernet0/2)	1+1 = 2
	R-8-11-1(GigabitEthernet0/2) – SW-8-11-1(FastEthernet0/32, FastEthernet0/3) – ASA-8-11-1(GigabitEthernet0/5)	1+1 = 2
	R-8-11-1(GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0, FastEthernet0/0) – SW-8-11-2(FastEthernet0/11, FastEthernet0/2) – ASA-8-11-1(GigabitEthernet0/3)	1+1+1 = 3
	R-8-11-1(GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0, FastEthernet0/1) – SW-8-11-2(FastEthernet0/12, FastEthernet0/10) – SW-8-11-1(FastEthernet0/30, FastEthernet0/3) – ASA-8-11-1(GigabitEthernet0/5)	1+1+1+1 = 4
R-8-11-2	R-8-11-2(FastEthernet0/0) – SW-8-11-2(FastEthernet0/11, FastEthernet0/2) – ASA-8-11-1(GigabitEthernet0/3)	1+1 = 2
	R-8-11-2(FastEthernet0/1) – SW-8-11-2(FastEthernet0/12, FastEthernet0/10) – SW-8-11-1(FastEthernet0/30, FastEthernet0/3) – ASA-8-11-1(GigabitEthernet0/5)	1+1+1 = 3
	R-8-11-2(FastEthernet0/1/0) – R-8-11-1(GigabitEthernet0/0, GigabitEthernet0/1) – SW-8-11-1(FastEthernet0/31, FastEthernet0/1) – ASA-8-11-1(GigabitEthernet0/2)	1+1+1 = 3
	R-8-11-2(FastEthernet0/1/0) – R-8-11-1(GigabitEthernet0/0, GigabitEthernet0/2) – SW-8-11-1(FastEthernet0/32, FastEthernet0/3) – ASA-8-11-1(GigabitEthernet0/5)	1+1+1 = 3

<u>Якщо ASA-8-11-2 Failover Active</u>		
R-8-11-1	R-8-11-1(GigabitEthernet0/1) – SW-8-11-1(FastEthernet0/31, FastEthernet0/2) – ASA-8-11-2(GigabitEthernet0/2)	1+1 = 2
	R-8-11-1(GigabitEthernet0/2) – SW-8-11-1(FastEthernet0/32, FastEthernet0/30) – SW-8-11-2(FastEthernet0/10, FastEthernet0/3) – ASA-8-11-2(GigabitEthernet0/5)	1+1+1 = 3
	R-8-11-1(GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0, FastEthernet0/0) – SW-8-11-2(FastEthernet0/11, FastEthernet0/1) – ASA-8-11-2(GigabitEthernet0/3)	1+1+1 = 3
	R-8-11-1(GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0, FastEthernet0/1) – SW-8-11-2(FastEthernet0/12, FastEthernet0/3) – ASA-8-11-2(GigabitEthernet0/5)	1+1+1 = 3
R-8-11-2	R-8-11-2(FastEthernet0/0) – SW-8-11-2(FastEthernet0/11, FastEthernet0/1) – ASA-8-11-2(GigabitEthernet0/3)	1+1 = 2
	R-8-11-2(FastEthernet0/1) – SW-8-11-2(FastEthernet0/12, FastEthernet0/3) – ASA-8-11-2(GigabitEthernet0/5)	1+1 = 2
	R-8-11-2(FastEthernet0/1/0) – R-8-11-1(GigabitEthernet0/0, GigabitEthernet0/1) – SW-8-11-1(FastEthernet0/31, FastEthernet0/2) – ASA-8-11-2(GigabitEthernet0/2)	1+1+1 = 3
	R-8-11-2(GigabitEthernet0/0) – R-8-11-1(GigabitEthernet0/0, GigabitEthernet0/2) – SW-8-11-1(FastEthernet0/32, FastEthernet0/30) – SW-8-11-2(FastEthernet0/10, FastEthernet0/3) – ASA-8-11-2(GigabitEthernet0/5)	1+1+1+1 = 4

Як можемо побачити, така фізична топологія здатна забезпечити до 4-ьох каналів зв'язку між мережевими маршрутизаторами та міжмережевими екранами. Аналізуючи наведені результати у таблиці 2.1.1, в особливості метрики маршрутів, що були отримані в результаті ручного обрахунку, можна помітити, що деякі з маршрутів мають однакові вартості маршрутів, що і призводить до проблем з маршрутизацією до тих чи інших підмереж, та їх невідповідностей на різному мережевому обладнанні. Навіть під час зміни топології комп'ютерних мережей, маршрути можуть залишатися незмінними, так як їх метрики є найменшими з доступних,

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

що створює відповідні проблеми, тому з точки зору засобів маршрутизації вони не підлягають змін, так як ця діє є найпростішою.

Вище зазначена проблема є досить поширеною під час побудови комп'ютерних мереж з кількома каналами зв'язку між мережевим обладнанням, тому протокол OSPF має засоби ручного налагодження метрик маршрутів для створення конкретної та чіткої послідовності вибору каналів зв'язку для забезпечення обміну інформацією у межах комп'ютерної мережі за послідовністю вибору, що є визначеною адміністратором мережі. Тому, для рішення вище описаної проблеми, переходимо до етапу вибору метрик маршрутів для каналів зв'язку з метою забезпечення коректної послідовності їх вибору.

Провівши усі необхідні тестування, щодо підбору метрик маршрутів для тих чи інших каналів зв'язку у комп'ютерній мережі, було визначено параметри для тих чи інших мережевих інтерфейсів. Результати проведеного підбору наведено у таблиці 2.1.2.

Таблиця 2.1.2 – Таблиця метрик інтерфейсів для протоколу OSPF.

Вузол	Інтерфейс	Метрика OSPF
R-8-11-1	GigabitEthernet0/1	1
	GigabitEthernet0/2	10
	GigabitEthernet0/0	20
R-8-11-2	FastEthernet0/0	1
	FastEthernet0/1	10
	FastEthernet0/1/0	20
ASA-8-11-1 та ASA-8-11-2	GigabitEthernet0/2	1
	GigabitEthernet0/3	1
	GigabitEthernet0/5	4

За таких умов, метрики тих чи інших маршрутів чітко наведено у таблиці 2.1.3, що зображена нижче.

Таблиця 2.1.3 – Переобрахована таблиця маршрутизації OSPF

Вузол	Маршрут	Метрика OSPF
<u>Якщо ASA-8-11-1 Failover Active</u>		
R-8-11-1	R-8-11-1(GigabitEthernet0/1) – SW-8-11-1(FastEthernet0/31, FastEthernet0/1) – ASA-8-11-1(GigabitEthernet0/2)	1+1 = 2

R-8-11-1	R-8-11-1(GigabitEthernet0/2) – SW-8-11-1(FastEthernet0/32, FastEthernet0/3) – ASA-8-11-1(GigabitEthernet0/5)	10+1 = 11
	R-8-11-1(GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0, FastEthernet0/0) – SW-8-11-2(FastEthernet0/11, FastEthernet0/2) – ASA-8-11-1(GigabitEthernet0/3)	20+1+1 = 22
	R-8-11-1(GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0, FastEthernet0/1) – SW-8-11-2(FastEthernet0/12, FastEthernet0/10) – SW-8-11-1(FastEthernet0/30, FastEthernet0/3) – ASA-8-11-1(GigabitEthernet0/5)	20+10+1+1 = 32
R-8-11-2	R-8-11-2(FastEthernet0/0) – SW-8-11-2(FastEthernet0/11, FastEthernet0/2) – ASA-8-11-1(GigabitEthernet0/3)	1+1 = 2
	R-8-11-2(FastEthernet0/1) – SW-8-11-2(FastEthernet0/12, FastEthernet0/10) – SW-8-11-1(FastEthernet0/30, FastEthernet0/3) – ASA-8-11-1(GigabitEthernet0/5)	10+1+1 = 12
	R-8-11-2(FastEthernet0/1/0) – R-8-11-1(GigabitEthernet0/0, GigabitEthernet0/1) – SW-8-11-1(FastEthernet0/31, FastEthernet0/1) – ASA-8-11-1(GigabitEthernet0/2)	20+1+1 = 22
	R-8-11-2(FastEthernet0/1/0) – R-8-11-1(GigabitEthernet0/0, GigabitEthernet0/2) – SW-8-11-1(FastEthernet0/32, FastEthernet0/3) – ASA-8-11-1(GigabitEthernet0/5)	20+10+1 = 31
<u>Якщо ASA-8-11-2 Failover Active</u>		
R-8-11-1	R-8-11-1(GigabitEthernet0/1) – SW-8-11-1(FastEthernet0/31, FastEthernet0/2) – ASA-8-11-2(GigabitEthernet0/2)	1+1 = 2
	R-8-11-1(GigabitEthernet0/2) – SW-8-11-1(FastEthernet0/32, FastEthernet0/30) – SW-8-11-2(FastEthernet0/10, FastEthernet0/3) – ASA-8-11-2(GigabitEthernet0/5)	10+1+1 = 12
	R-8-11-1(GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0, FastEthernet0/0) – SW-8-11-2(FastEthernet0/11, FastEthernet0/1) – ASA-8-11-2(GigabitEthernet0/3)	20+1+1 = 22
	R-8-11-1(GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0, FastEthernet0/1) – SW-8-11-2(FastEthernet0/12, FastEthernet0/3) – ASA-8-11-2(GigabitEthernet0/5)	20+10+1 = 31

R-8-11-2	R-8-11-2(FastEthernet0/0) – SW-8-11-2(FastEthernet0/11, FastEthernet0/1) – ASA-8-11-2(GigabitEthernet0/3)	1+1 = 2
	R-8-11-2(FastEthernet0/1) – SW-8-11-2(FastEthernet0/12, FastEthernet0/3) – ASA-8-11-2(GigabitEthernet0/5)	10+1 = 11
	R-8-11-2(FastEthernet0/1/0) – R-8-11-1(GigabitEthernet0/0, GigabitEthernet0/1) – SW-8-11-1(FastEthernet0/31, FastEthernet0/2) – ASA-8-11-2(GigabitEthernet0/2)	20+1+1 = 22
	R-8-11-2(GigabitEthernet0/0) – R-8-11-1(GigabitEthernet0/0, GigabitEthernet0/2) – SW-8-11-1(FastEthernet0/32, FastEthernet0/30) – SW-8-11-2(FastEthernet0/10, FastEthernet0/3) – ASA-8-11-2(GigabitEthernet0/5)	20+10+1+1 = 32

Аналогічним чином, відобразимо метрики маршрутів для міжмережевого екрану Cisco ASA. Їх наведено в таблиці 2.1.4.

Таблиця 2.1.4 – Таблиця маршрутизації OSPF для міжмережевих екранів Cisco ASA

Джерело	Призначення	Маршрут	Метрика OSPF
<u>Якщо ASA-8-11-1 Failover Active</u>			
ASA-8-11-1	R-8-11-1	ASA-8-11-1(GigabitEthernet0/2) – SW-8-11-1(FastEthernet0/1, FastEthernet0/31) – R-8-11-1(GigabitEthernet0/1)	1+1=2
		ASA-8-11-1(GigabitEthernet0/5) – SW-8-11-1(FastEthernet0/3, FastEthernet0/32) – R-8-11-1(GigabitEthernet0/2)	5+1=6
		ASA-8-11-1(GigabitEthernet0/3) — SW-8-11-2(FastEthernet0/2, FastEthernet0/11) – R-8-11-2(FastEthernet0/0, FastEthernet0/1/0) – R-8-11-1 (GigabitEthernet0/0)	1+1+20=22
		ASA-8-11-1(GigabitEthernet0/5) – SW-8-11-1(FastEthernet0/3, FastEthernet0/30) – SW-8-11-2(FastEthernet0/10, FastEthernet0/12) – R-8-11-2(FastEthernet0/1, FastEthernet0/1/0) – R-8-11-1 (GigabitEthernet0/0)	1+1+1+20=23

Джерело	Призначення	Маршрут	Метрика OSPF
<u>Якщо ASA-8-11-1 Failover Active</u>			
ASA-8-11-1	R-8-11-2	ASA-8-11-1(GigabitEthernet0/3) — SW-8-11-2(FastEthernet0/2, FastEthernet0/11) – R-8-11-2(FastEthernet0/0)	1+1=2
		ASA-8-11-1(GigabitEthernet0/5) — SW-8-11-1(FastEthernet0/3, FastEthernet0/30) – SW-8-11-2(FastEthernet0/10, FastEthernet0/12) – R-8-11-2(FastEthernet0/1)	1+1+1=3
		ASA-8-11-1(GigabitEthernet0/2) — SW-8-11-1(0/1, FastEthernet0/31) – R-8-11-1(GigabitEthernet0/1, GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0)	1+1+20=22
		ASA-8-11-1(GigabitEthernet0/5) — SW-8-11-1(0/3, FastEthernet0/32) – R-8-11-1(GigabitEthernet0/2, GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0)	4+1+20=25
<u>Якщо ASA-8-11-2 Failover Active</u>			
ASA-8-11-2	R-8-11-1	ASA-8-11-2(GigabitEthernet0/2) — SW-8-11-1(FastEthernet0/2, FastEthernet0/31) – R-8-11-1(GigabitEthernet0/1)	1+1=2
		ASA-8-11-2(GigabitEthernet0/5) — SW-8-11-2(FastEthernet0/3, FastEthernet0/10) – SW-8-11-1(FastEthernet0/30, FastEthernet0/32) – R-8-11-1(GigabitEthernet0/2)	1+1+1=3
		ASA-8-11-2(GigabitEthernet0/3) — SW-8-11-2(FastEthernet0/1, FastEthernet0/11) – R-8-11-2(FastEthernet0/0, FastEthernet0/1/0) – R-8-11-1(GigabitEthernet0/0)	1+1+20=22
		ASA-8-11-2(GigabitEthernet0/5) — SW-8-11-2(FastEthernet0/3, FastEthernet0/12) – R-8-11-2(FastEthernet0/1, FastEthernet0/1/0) – R-8-11-1(GigabitEthernet0/0)	4+1+20=25

Джерело	Призначення	Маршрут	Метрика OSPF
<u>Якщо ASA-8-11-2 Failover Active</u>			
ASA-8-11-2	R-8-11-2	ASA-8-11-2(GigabitEthernet0/3) – SW-8-11-2(FastEthernet0/1, FastEthernet0/11) – R-8-11-2(FastEthernet0/0)	1+1=2
		ASA-8-11-2(GigabitEthernet0/5) – SW-8-11-2(FastEthernet0/3, FastEthernet0/12) – R-8-11-2(FastEthernet0/1)	5+1=6
		ASA-8-11-2(GigabitEthernet0/2) — SW-8-11-1(FastEthernet0/2, FastEthernet0/31) – R-8-11-1(GigabitEthernet0/1, GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0)	1+1+20=22
		ASA-8-11-2(GigabitEthernet0/5) – SW-8-11-2(FastEthernet0/3, FastEthernet0/10) – SW-8-11-1(FastEthernet0/30, FastEthernet0/32) – R-8-11-1(GigabitEthernet0/2, GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0)	1+1+1+20=23

Використовуючи такий спосіб маніпулюванням вибору маршрутів для протоколу динамічної маршрутизації OSPF, в результаті проведених тестувань, було виявлено повну працеспроможність. А тому, проведена нами розробка метри маршрутів для роботи протоколу OSPF є чітко визначаною та продемонстрованою у таблиці 2.1.2.



Рисунок 2.1.11 – Результат успішного тестування роботи ручного налагодження метрик маршрутів протоколу OSPF на фізичному стенді.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

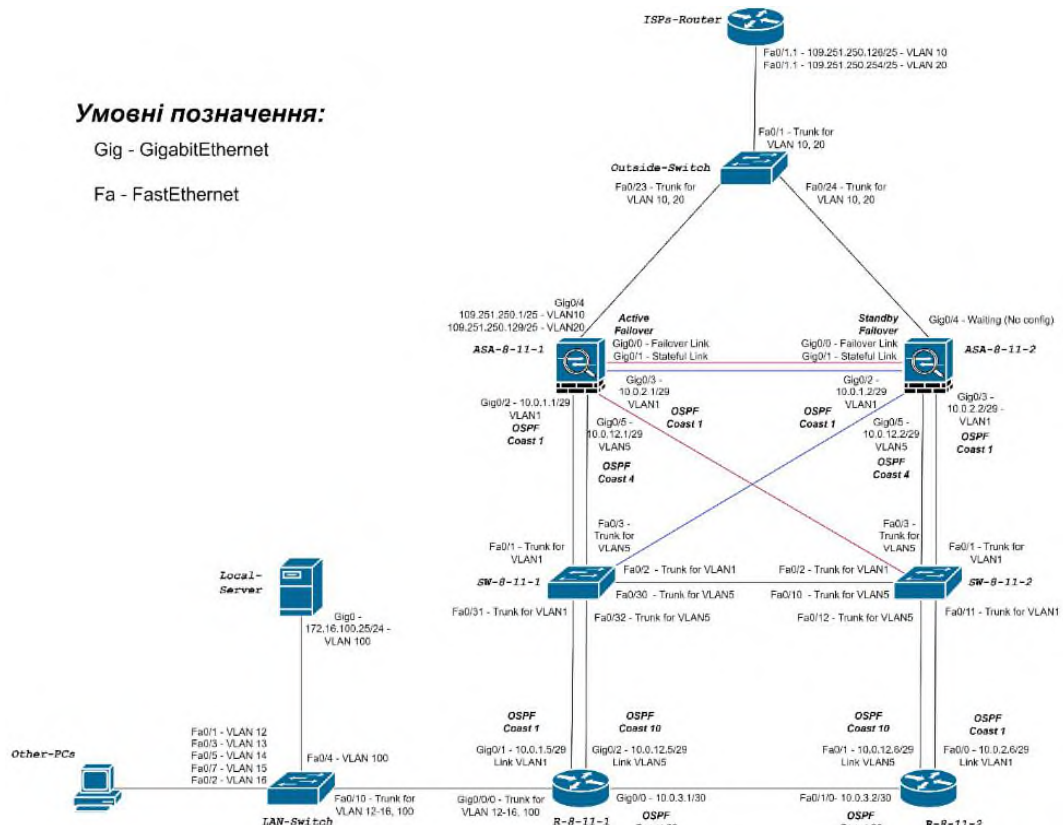


Рисунок 2.1.12 – Фізична топологія стенду з результатами проведеного підбору метрик маршрутів крізь інтерфейси для OSPF

Таким чином, було проведено рішення однієї з проблем використання протоколу динамічної маршрутизації OSPF у межах вище зазначеної топології проекту комп'ютерної мережі. На даному етапі, такого рішення для реалізації проекту є цілком достатньо, тому переходимо до наступних етапів реалізації проекту комп'ютерної мережі.

2.2. Розробка фізичної та логічної топології мережі.

Перейдемо до процесу розробки фізичної топології комп'ютерної мережі проекту. Враховуючи прийняті нами раніше технічні рішення, а також проведені тестування та дослідження однієї зі спроб реалізації проекту комп'ютерної мережі, на даному етапі бачення цього проекту є сформованими. До прикладу, необхідно забезпечити два канали зв'язку між Cisco ASA для роботи технології Failover, реалізувати транкові канали зв'язку для підключення VLAN підмереж на маршрутизаторі, реалізувати роботу протоколу OSPF у мережі для забезпечення роботи

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				54
Змн.	Арк.	№ докум.	Підпис	Дата		

засобів динамічної маршрутизації, котра повинна виконувати між двома маршрутизаторами мережі та Cisco ASA, а також необхідно забезпечити можливість мультитипровайдерного підключення для двох Cisco ASA з врахуванням наявності лише двох каналів зв'язку з підмережами інтернет провайдерів. Таким чином, основа фізичної топології проекту є реалізованою.

Враховуючи потреби та особливості роботи тих чи інших протоколів комп'ютерної мережі, що розроблюється та впроваджуються у даному проекті, можемо провести створення фізичної топології проекту високонадійної, захищеної та відмовостійкої комп'ютерної мережі. В результаті проведеної розробки, фізичну топологію можна побачити на рисунку 2.2.1, що наведено нижче.

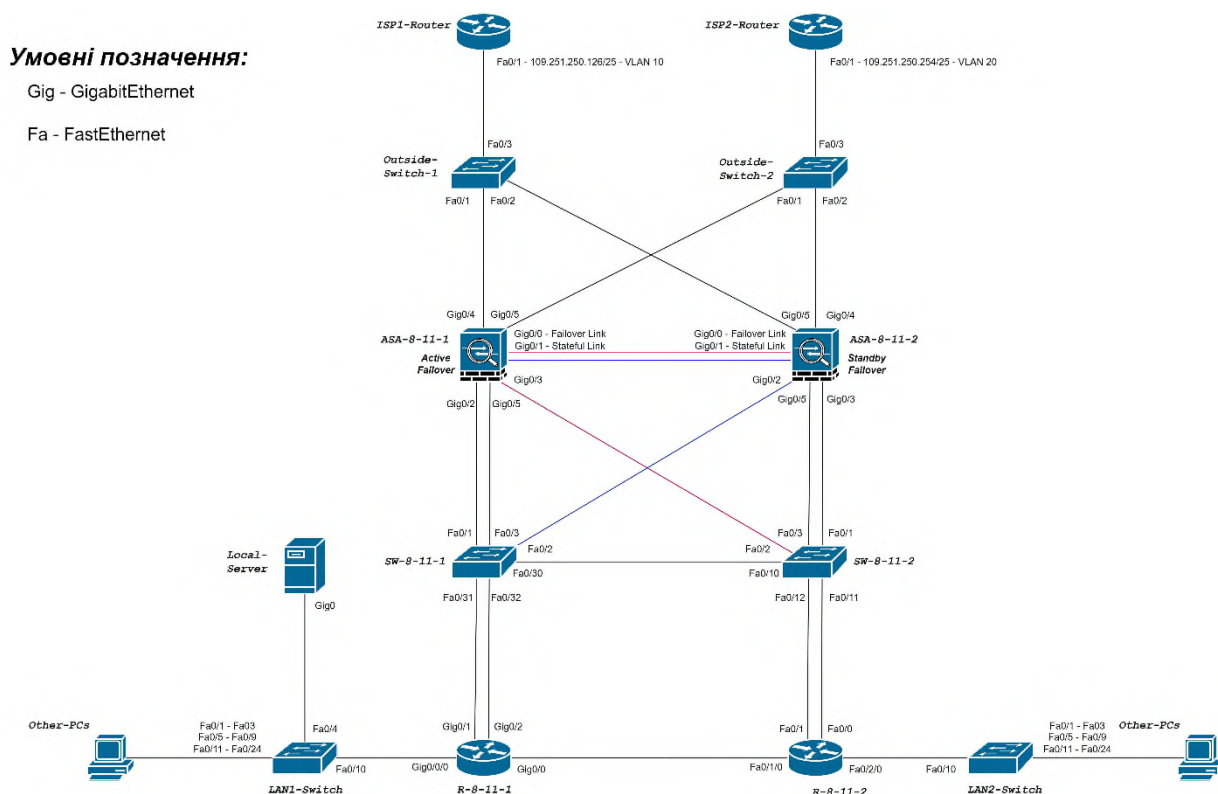


Рисунок 2.2.1 – Фізична топологія проекту високонадійної, захищеної та відмовостійкої комп'ютерної мережі з мультитипровайдерним підключенням

Наступним етапом розробки проекту є побудова таблиці комутації між мережевим обладнанням, для полегшення подальшого процесу проектування та тестувань роботи створеного проекту. Для цього, побудуємо таблицю 2.2.1, у рамках

яких буде відображено усі наявні фізичні з'єднання між тими чи іншими вузлами проекту комп'ютерної мережі. Відповідну таблицю комутації представлено у вигляді таблиці 2.2.1.

Таблиця 2.1.1 – Таблиця комутації проекту

ДЛЯ ПОВНОЦІННОЇ ФІЗИЧНОЇ ТОПОЛОГІЇ			
<i>Пристрій</i>	<i>Інтерфейс</i>	<i>Підключення до пристрою</i>	<i>Підключення до інтерфейсу</i>
Мережевий екран ASA-8-11-1	GigabitEthernet0/0	ASA-8-11-2	GigabitEthernet0/0
	GigabitEthernet0/1		GigabitEthernet0/1
	GigabitEthernet0/2	SW-8-11-1	FastEthernet0/1
	GigabitEthernet0/5		FastEthernet0/3
	GigabitEthernet0/3	SW-8-11-2	FastEthernet0/3
	GigabitEthernet0/4	Outside-Switch-1	GigabitEthernet0/1
	GigabitEthernet0/6	Outside-Switch-2	GigabitEthernet0/1
Мережевий екран ASA-8-11-2	GigabitEthernet0/0	ASA-8-11-1	GigabitEthernet0/0
	GigabitEthernet0/1		GigabitEthernet0/1
	GigabitEthernet0/2	SW-8-11-1	FastEthernet0/2
	GigabitEthernet0/3	SW-8-11-2	FastEthernet0/1
	GigabitEthernet0/5		FastEthernet0/3
	GigabitEthernet0/4	Outside-Switch-1	GigabitEthernet0/2
	GigabitEthernet0/6	Outside-Switch-2	GigabitEthernet0/2
Маршрутизатор R-8-11-1	GigabitEthernet0/1	SW-8-11-1	FastEthernet0/31
	GigabitEthernet0/2		FastEthernet0/32
	GigabitEthernet0/0	R-8-11-2	FastEthernet0/1/0
	GigabitEthernet0/0/0	LANs1-Switch	FastEthernet0/10
Маршрутизатор R-8-11-2	FastEthernet0/0	SW-8-11-2	FastEthernet0/11
	FastEthernet0/1		FastEthernet0/12
	FastEthernet0/1/0	R-8-11-1	GigabitEthernet0/0
	FastEthernet0/2/0	LANs2-Switch	FastEthernet0/10
Комутатор SW-8-11-1	FastEthernet0/1	ASA-8-11-1	GigabitEthernet0/2
	FastEthernet0/3		GigabitEthernet0/5
	FastEthernet0/31	R-8-11-1	GigabitEthernet0/1
	FastEthernet0/32		GigabitEthernet0/2
	FastEthernet0/30	SW-8-11-2	FastEthernet0/10

Комутатор SW-8-11-2	FastEthernet0/1	ASA-8-11-2	GigabitEthernet0/3
	FastEthernet0/3		GigabitEthernet0/5
	FastEthernet0/11	R-8-11-2	FastEthernet0/0
	FastEthernet0/12		FastEthernet0/1
	FastEthernet0/10	SW-8-11-1	FastEthernet0/30
Комутатор LANS1-Switch	FastEthernet0/10	R-8-11-1	GigabitEthernet0/0/0
Комутатор LANS2-Switch	FastEthernet0/10	R-8-11-2	FastEthernet0/2/0
Комутатор Out-side-Switch-1	GigabitEthernet0/1	ASA-8-11-1	GigabitEthernet0/4
	GigabitEthernet0/2	ASA-8-11-2	GigabitEthernet0/4
	GigabitEthernet0/0	ISP1-Router	---
Комутатор Out-side-Switch-2	GigabitEthernet0/1	ASA-8-11-1	GigabitEthernet0/6
	GigabitEthernet0/2	ASA-8-11-2	GigabitEthernet0/6
	GigabitEthernet0/0	ISP2-Router	---

На даному етапі підготовки топологій проекту, необхідно провести розробку логічної топології, котра покликана продемонструвати те, як мережевий трафік буде передаватися в межах проекту комп'ютерної мережі. Це спростить процес сприйняття для подальшого проведення налаштувань мережевого обладнання, а також дозволить наочно поглянути на розподіл комп'ютерних мереж проекту. Таким чином, виходячи з фізичної топології, що була наведена на рисунку 2.2.1, було побудовано логічну топологію проекту, котру наведено на рисунку 2.2.2.

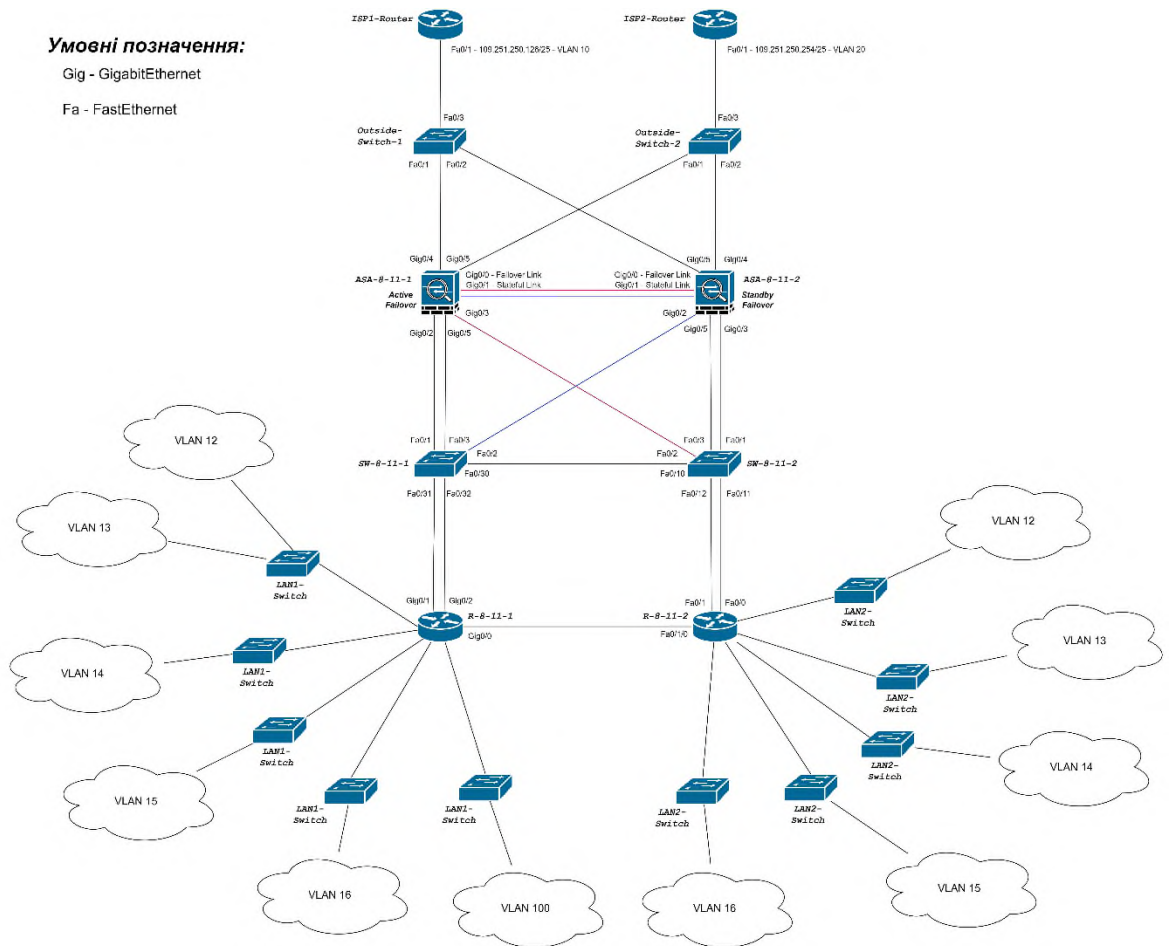


Рисунок 2.2.2 – Логічна топологія проекту високонадійної, захищеної та відмовостійкої комп'ютерної мережі з мультипровайдерним підключенням

На цьому процес проектування логічної та фізичної топології проекту, є закінченими, тому переходимо до процесу розробки параметрів IP-адресації для забезпечення взаємодії між різними вузлами комп'ютерної мережі.

2.3. Розробка параметрів IP-адресації.

Розпочнімо виконання процесу проектування параметрів IP-адресації для забезпечення взаємодії між вузлами в проекті комп'ютерної мережі. Для цього, в першу чергу, необхідно визначитися з кількістю підмереж, для яких буде виконано розробку параметрів IPv4 адресації.

Оглянувши проект комп'ютерної мережі, було виявлено необхідність у побудові 6-ми підмереж для забезпечення зв'язків між мережевим обладнанням, а також необхідність у 10-ти підмережах для підключення локальних вузлів до кожної окремої підмережі VLAN та одну підмережу для розміщення локальних серверів.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				58
Змн.	Арк.	№ докум.	Підпис	Дата		

Загалом, кількість локальних підмереж для вузлів комп'ютерної мережі, може бути необмеженою, але при цьому залежати від потужностей мережевого обладнання та відповідних кількісних потреб. Таким чином, маючи уявлення про кількість підмереж, а також приблизну уяву про кількість вузлів у даних підмережах, можемо приступати до процесу розрахунків параметрів IPv4-адресації, котрі будуть формуватися на основі масок змінної довжини, або так званих VLSM (Variable-Length Subnet Mask). Для зручності виконання подальшого процесу проектування побудуємо таблицю кількості вузлів, котрі повинні бути розміщеними у тій чи іншій підмережі. Її наведено у таблиці 2.3.1.

Таблиця 2.3.1 – Таблиця кількості вузлів у підмережах проекту

Назва підмережі	Кількість вузлів	Призначення
Підмережа А	2	Канал зв'язку між ASA-8-11-1 та ASA-8-11-2 (Failove link)
Підмережа В	2	Канал зв'язку між ASA-8-11-1 та ASA-8-11-2 (State link)
Підмережа С	5	Канал зв'язку між R-8-11-1, ASA-8-11-1 та ASA-8-11-2, VLAN інтерфейси для SW-8-11-1 та SW-8-11-2
Підмережа D	5	Канал зв'язку між R-8-11-2, ASA-8-11-1 та ASA-8-11-2, VLAN інтерфейси для SW-8-11-1 та SW-8-11-2
Підмережа Е	6	Канал зв'язку між R-8-11-1, R-8-11-2, ASA-8-11-1 та ASA-8-11-2, VLAN інтерфейси для SW-8-11-1 та SW-8-11-2
Підмережа F	2	Канал зв'язку між R-8-11-1 та R-8-11-2
Підмережа VLAN12-1	30	Підмережа VLAN 12 для користувачів локальної підмережі (маршрутизатор R-8-11-1)
Підмережа VLAN13-1	30	Підмережа VLAN 13 для користувачів локальної підмережі (маршрутизатор R-8-11-1)
Підмережа VLAN14-1	30	Підмережа VLAN 14 для користувачів локальної підмережі (маршрутизатор R-8-11-1)
Підмережа VLAN15-1	30	Підмережа VLAN 15 для користувачів локальної підмережі (маршрутизатор R-8-11-1)
Підмережа VLAN16-1	30	Підмережа VLAN 16 для користувачів локальної підмережі (маршрутизатор R-8-11-1)
Підмережа VLAN12-2	30	Підмережа VLAN 12 для користувачів локальної підмережі (маршрутизатор R-8-11-2)
Підмережа VLAN13-2	30	Підмережа VLAN 13 для користувачів локальної підмережі (маршрутизатор R-8-11-2)
Підмережа VLAN14-2	30	Підмережа VLAN 14 для користувачів локальної підмережі (маршрутизатор R-8-11-2)
Підмережа VLAN15-2	30	Підмережа VLAN 15 для користувачів локальної підмережі (маршрутизатор R-8-11-2)
Підмережа VLAN16-2	30	Підмережа VLAN 16 для користувачів локальної підмережі (маршрутизатор R-8-11-2)
Підмережа серверів VLAN100	254	Підмережа VLAN 100 для розміщення серверів в локальній мережі

Таким чином, маючи відповідні уявлення про структуру підмереж, їх призначення та кількість вузлів, що повинні їм належати, може приступати до процесів обрахунків параметрів IP-адресації для тих чи інших підмереж.

Розпочнімо виконання обрахунків з огляду одного з прикладів виконання даного процесу. Для цього обремо одну з підмережей та детально оглянемо процес підбору тих чи інших параметрів. До прикладу, розглянемо розрахунок параметрів IP-адресації для підмережі з ім'ям «Підмережа VLAN12-1». Для початку необхідні правильно розрахувати маску. У зв'язку з тим, що необхідно розмістити що найменш 30 адрес в межах однієї мережі розглянемо маску з префіксом /26. Маска з префіксом 26, представлення в десятковому коді, як 255.255.255.192. В двійковому, як 11111111.11111111.11111111.11000000, де 26 бітів відносяться до маски, а інші 6 бітів залишаються для адрес вузлів. Таким чином можемо помітити, що дана маска дозволяє розмістити в мережі $2^6 - 2 = 64 - 2 = 62$ адреси вузлів. Таким чином, дана маска може бути використана в межах нашого проекту, але кількість її параметрів IP-адресації може бути надлишковою за деяких умов. Тому розглянемо іншу маску з префіксом /27. Маска за префіксом 27, представлення в десятковому коді, як 255.255.255.224. В двійковому, як 11111111.11111111.11111111.11100000, де 27 бітів відносяться до маски, а інші 5 бітів залишаються для адрес вузлів. Виконуючи відповідні обрахунки, можна відзначити, що данна маска дозволяє розмістити в мережі $2^5 - 2 = 32 - 2 = 30$ адреси вузлів. Як можемо помітити, маска з префіксом /27, являється більш збалансованою у рамках використання адресного простору, тому можемо використовувати її як основу для використання у підмережі з ім'ям «Підмережа VLAN12-1», та подібним їй підмережам.

Таким чином, спираючись на вище описаний приклад, було проведено обрахунки параметрів IP-адресації для різних підмереж. Їх результати наведено в таблицях 2.3.2 – 2.3.18.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

Таблиця 2.3.2 – Параметри IP-адресації для підмережі А

Параметри IP-адреси мережі А		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.00000000	255.255.255.0
Інвертована маска	00000000.00000000.00000000.11111111	0.0.0.255
IP-адреса мережі	11000000.10101000.00000001.00000000	192.168.1.0
Мінімальна IP-адреса вузла	11000000.10101000.00000001.00000001	192.168.1.0
Максимальна IP-адреса вузла	11000000.10101000.00000001.11111110	192.168.1.254
Широкомовна IP-адреса	11000000.10101000.00000001.11111111	192.168.1.255
Кількість вузлів в мережі	11111110	254

Таблиця 2.3.3 – Параметри IP-адресації для підмережі В

Параметри IP-адреси мережі В		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.00000000	255.255.255.0
Інвертована маска	00000000.00000000.00000000.11111111	0.0.0.255
IP-адреса мережі	11000000.10101000.00000010.00000000	192.168.2.0
Мінімальна IP-адреса вузла	11000000.10101000.00000010.00000001	192.168.2.0
Максимальна IP-адреса вузла	11000000.10101000.00000010.11111110	192.168.2.254
Широкомовна IP-адреса	11000000.10101000.00000010.11111111	192.168.2.255
Кількість вузлів в мережі	11111110	254

Таблиця 2.3.4 – Параметри IP-адресації для підмережі С

Параметри IP-адреси мережі С		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11111000	255.255.255.248
Інвертована маска	00000000.00000000.00000000.00000111	0.0.0.7
IP-адреса мережі	00001010.00000000.00000001.00000000	10.0.1.0
Мінімальна IP-адреса вузла	00001010.00000000.00000001.00000001	10.0.1.1
Максимальна IP-адреса вузла	00001010.00000000.00000001.00000110	10.0.1.6
Широкомовна IP-адреса	00001010.00000000.00000001.00000111	10.0.1.7
Кількість вузлів в мережі	110	6

Таблиця 2.3.5 – Параметри IP-адресації для підмережі D

Параметри IP-адреси мережі D		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11111000	255.255.255.248
Інвертована маска	00000000.00000000.00000000.00000111	0.0.0.7
IP-адреса мережі	00001010.00000000.00000010.00000000	10.0.2.0
Мінімальна IP-адреса вузла	00001010.00000000.00000010.00000001	10.0.2.1
Максимальна IP-адреса вузла	00001010.00000000.00000010.00000110	10.0.2.6
Широкомовна IP-адреса	00001010.00000000.00000010.00000111	10.0.2.7
Кількість вузлів в мережі	110	6

Таблиця 2.3.6 – Параметри IP-адресації для підмережі E

Параметри IP-адреси мережі E		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11111000	255.255.255.248
Інвертована маска	00000000.00000000.00000000.00000111	0.0.0.7
IP-адреса мережі	00001010.00000000.00001100.00000000	10.0.12.0
Мінімальна IP-адреса вузла	00001010.00000000.00001100.00000001	10.0.12.1
Максимальна IP-адреса вузла	00001010.00000000.00001100.00000110	10.0.12.6
Широкомовна IP-адреса	00001010.00000000.00001100.00000111	10.0.12.7
Кількість вузлів в мережі	110	6

Таблиця 2.3.7 – Параметри IP-адресації для підмережі F

Параметри IP-адреси мережі F		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11111100	255.255.255.252
Інвертована маска	00000000.00000000.00000000.00000011	0.0.0.3
IP-адреса мережі	00001010.00000000.00000011.00000000	10.0.3.0
Мінімальна IP-адреса вузла	00001010.00000000.00000011.00000001	10.0.3.1
Максимальна IP-адреса вузла	00001010.00000000.00000011.00000010	10.0.3.2
Широкомовна IP-адреса	00001010.00000000.00000011.00000011	10.0.3.3
Кількість вузлів в мережі	10	2

Таблиця 2.3.8 – Параметри IP-адресації для підмережі VLAN12-1

Параметри IP-адреси мережі VLAN12-1		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000001.00000000	172.16.1.0
Мінімальна IP-адреса вузла	10101100.00010000.00000001.00000001	172.16.1.1
Максимальна IP-адреса вузла	10101100.00010000.00000001.00011110	172.16.1.30
Широкомовна IP-адреса	10101100.00010000.00000001.00011111	172.16.1.31
Кількість вузлів в мережі	11110	30

Таблиця 2.3.9 – Параметри IP-адресації для підмережі VLAN13-1

Параметри IP-адреси мережі VLAN13-1		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000001.00100000	172.16.1.32
Мінімальна IP-адреса вузла	10101100.00010000.00000001.00100001	172.16.1.33
Максимальна IP-адреса вузла	10101100.00010000.00000001.00111110	172.16.1.62
Широкомовна IP-адреса	10101100.00010000.00000001.00111111	172.16.1.63
Кількість вузлів в мережі	11110	30

Таблиця 2.3.10 – Параметри IP-адресації для підмережі VLAN14-1

Параметри IP-адреси мережі VLAN14-1		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000001.01000000	172.16.1.64
Мінімальна IP-адреса вузла	10101100.00010000.00000001.01000001	172.16.1.65
Максимальна IP-адреса вузла	10101100.00010000.00000001.01011110	172.16.1.94
Широкомовна IP-адреса	10101100.00010000.00000001.01011111	172.16.1.95
Кількість вузлів в мережі	11110	30

Таблиця 2.3.11 – Параметри IP-адресації для підмережі VLAN15-1

Параметри IP-адреси мережі VLAN15-1		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000001.01100000	172.16.1.96
Мінімальна IP-адреса вузла	10101100.00010000.00000001.01100001	172.16.1.97
Максимальна IP-адреса вузла	10101100.00010000.00000001.01111110	172.16.1.126
Широкомовна IP-адреса	10101100.00010000.00000001.01111111	172.16.1.127
Кількість вузлів в мережі	11110	30

Таблиця 2.3.12 – Параметри IP-адресації для підмережі VLAN16-1

Параметри IP-адреси мережі VLAN16-1		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000001.10000000	172.16.1.128
Мінімальна IP-адреса вузла	10101100.00010000.00000001.10000001	172.16.1.129
Максимальна IP-адреса вузла	10101100.00010000.00000001.10011110	172.16.1.158
Широкомовна IP-адреса	10101100.00010000.00000001.10011111	172.16.1.159
Кількість вузлів в мережі	11110	30

Таблиця 2.3.13 – Параметри IP-адресації для підмережі VLAN12-2

Параметри IP-адреси мережі VLAN12-2		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000010.00000000	172.16.2.0
Мінімальна IP-адреса вузла	10101100.00010000.00000010.00000001	172.16.2.1
Максимальна IP-адреса вузла	10101100.00010000.00000010.00011110	172.16.2.30
Широкомовна IP-адреса	10101100.00010000.00000010.00011111	172.16.2.31
Кількість вузлів в мережі	11110	30

Таблиця 2.3.14 – Параметри IP-адресації для підмережі VLAN13-2

Параметри IP-адреси мережі VLAN13-2		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000010.00100000	172.16.2.32
Мінімальна IP-адреса вузла	10101100.00010000.00000010.00100001	172.16.2.33
Максимальна IP-адреса вузла	10101100.00010000.00000010.00111110	172.16.2.62
Широкомовна IP-адреса	10101100.00010000.00000010.00111111	172.16.2.63
Кількість вузлів в мережі	11110	30

Таблиця 2.3.15 – Параметри IP-адресації для підмережі VLAN14-2

Параметри IP-адреси мережі VLAN14-2		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000010.01000000	172.16.2.64
Мінімальна IP-адреса вузла	10101100.00010000.00000010.01000001	172.16.2.65
Максимальна IP-адреса вузла	10101100.00010000.00000010.01011110	172.16.2.94
Широкомовна IP-адреса	10101100.00010000.00000010.01011111	172.16.2.95
Кількість вузлів в мережі	11110	30

Таблиця 2.3.16 – Параметри IP-адресації для підмережі VLAN15-2

Параметри IP-адреси мережі VLAN15-2		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000010.01100000	172.16.2.96
Мінімальна IP-адреса вузла	10101100.00010000.00000010.01100001	172.16.2.97
Максимальна IP-адреса вузла	10101100.00010000.00000010.01111110	172.16.2.126
Широкомовна IP-адреса	10101100.00010000.00000010.01111111	172.16.2.127
Кількість вузлів в мережі	11110	30

Таблиця 2.3.17 – Параметри IP-адресації для підмережі VLAN16-2

Параметри IP-адреси мережі VLAN16-2		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000010.10000000	172.16.2.128
Мінімальна IP-адреса вузла	10101100.00010000.00000010.10000001	172.16.2.129
Максимальна IP-адреса вузла	10101100.00010000.00000010.10011110	172.16.2.158
Широкомовна IP-адреса	10101100.00010000.00000010.10011111	172.16.2.159
Кількість вузлів в мережі	11110	30

Таблиця 2.3.18 – Параметри IP-адресації для підмережі VLAN100

Параметри IP-адреси мережі VLAN100		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.00000000	255.255.255.0
Інвертована маска	00000000.00000000.00000000.11111111	0.0.0.255
IP-адреса мережі	10101100.00010000.01100100.00000000	172.16.100.0
Мінімальна IP-адреса вузла	10101100.00010000.01100100.00000001	172.16.100.1
Максимальна IP-адреса вузла	10101100.00010000.01100100.11111110	172.16.100.254
Широкомовна IP-адреса	10101100.00010000.01100100.11111111	172.16.100.255
Кількість вузлів в мережі	11111110	254

На цьому етап розрахунків параметрів IP-адресації є закінченим, тому переходимо до етапу розподілу параметрів IP-адресації між вузлами. Для цього було побудовано таблицю на основі якої відображено усі розподілені параметри IP-адресації для вузлів тих чи інших підмереж. Результати даного розподілу наведено у таблиці 2.3.19.

Таблиця 2.3.19 – Таблиця розподілу адресного простору

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підме- режі	Пре фікс
Мережа А	-	192.168.1.0	255.255.255.0	/24
ASA-8-11-1	GigabitEthernet0/0	192.168.1.100	255.255.255.0	/24
ASA-8-11-2	GigabitEthernet0/0	192.168.1.101	255.255.255.0	/24
Мережа В	-	192.168.2.0	255.255.255.0	/24
ASA-8-11-1	GigabitEthernet0/1	192.168.2.100	255.255.255.0	/24
ASA-8-11-2	GigabitEthernet0/1	192.168.2.101	255.255.255.0	/24
Мережа С	-	10.0.1.0	255.255.255.248	/29
ASA-8-11-1	GigabitEthernet0/2	10.0.1.1	255.255.255.248	/29
ASA-8-11-2	GigabitEthernet0/2	10.0.1.2	255.255.255.248	/29
SW-8-11-1	VLAN1	10.0.1.3	255.255.255.248	/29
R-8-11-1	GigabitEthernet0/1	10.0.1.5	255.255.255.248	/29
Мережа D	-	10.0.2.0	255.255.255.248	/29
ASA-8-11-1	GigabitEthernet0/3	10.0.2.1	255.255.255.248	/29
ASA-8-11-2	GigabitEthernet0/3	10.0.2.2	255.255.255.248	/29
SW-8-11-2	VLAN1	10.0.2.4	255.255.255.248	/29
R-8-11-2	FastEthernet0/0	10.0.2.6	255.255.255.248	/29
Мережа Е	-	10.0.2.0	255.255.255.248	/29
ASA-8-11-1	GigabitEthernet0/5	10.0.12.1	255.255.255.248	/29
ASA-8-11-2	GigabitEthernet0/5	10.0.12.2	255.255.255.248	/29
SW-8-11-1	VLAN5	10.0.12.3	255.255.255.248	/29
SW-8-11-2	VLAN5	10.0.12.4	255.255.255.248	/29
R-8-11-1	GigabitEthernet0/2.1	10.0.12.5	255.255.255.248	/29
R-8-11-2	FastEthernet0/1.1	10.0.12.6	255.255.255.248	/29
Мережа F	-	10.0.3.0	255.255.255.252	/30
R-8-11-1	GigabitEthernet0/0	10.0.3.1	255.255.255.252	/30
R-8-11-2	Fast Ethernet0/1/0	10.0.3.2	255.255.255.252	/30

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	ІР-адреса	Маска підме- режі	Пре фікс
Мережа VLAN12-1	-	172.16.1.0	255.255.255.224	/27
R-8-11-1	GigabitEthernet0/0/0.12	172.16.1.30	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN13-1	-	172.16.1.32	255.255.255.224	/27
R-8-11-1	GigabitEthernet0/0/0.13	172.16.1.62	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN14-1	-	172.16.1.64	255.255.255.224	/27
R-8-11-1	GigabitEthernet0/0/0.14	172.16.1.94	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN15-1	-	172.16.1.96	255.255.255.224	/27
R-8-11-1	GigabitEthernet0/0/0.15	172.16.1.126	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN16-1	-	172.16.1.128	255.255.255.224	/27
R-8-11-1	GigabitEthernet0/0/0.16	172.16.1.158	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN12-2	-	172.16.2.0	255.255.255.224	/27
R-8-11-2	GigabitEthernet0/2/0.12	172.16.2.30	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN13-2	-	172.16.2.32	255.255.255.224	/27
R-8-11-2	GigabitEthernet0/2/0.1	172.16.2.62	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN14-2	-	172.16.2.64	255.255.255.224	/27
R-8-11-2	GigabitEthernet0/2/0.1	172.16.2.94	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN15-2	-	172.16.2.96	255.255.255.224	/27
R-8-11-2	GigabitEthernet0/2/0.1	172.16.2.126	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN16-2	-	172.16.2.128	255.255.255.224	/27
R-8-11-2	GigabitEthernet0/2/0.1	172.16.2.158	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN100-1	-	172.16.100.254	255.255.255.224	/27
R-8-11-1	GigabitEthernet0/0/0.100	172.16.100.254	255.255.255.0	/24
Srv-8-11-1	GigabitEthernet	172.16.100.25	255.255.255.0	/24

Таким чином, нами було проведено процес підготовки параметрів IP-адресації для вузлів нашого проекту комп'ютерної мережі. Так як у межах проекту планується використання технології DHCP, то наступним кроком, проведемо розробку параметрів IP-адресації для роботи даної технології. Усі необхідні параметри для її роботи наведені у таблиці 2.3.20, що відображено нижче.

Таблиця 2.3.20 – Параметри роботи протоколу DHCP

Вид адрес	Кількість	Діапазон IP-адрес/ Ок-ремі IP-адреси	Адреси DHCP-сервером
Мережа для VLAN12-1			
Динамічні IP-адреси	29	172.16.1.1 – 172.16.1.29	Так, пизначаються
Статичні IP-адреси	1	172.16.1.30	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN13-1			
Динамічні IP-адреси	29	172.16.1.33 – 172.16.1.61	Так, пизначаються
Статичні IP-адреси	1	172.16.1.62	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN14-1			
Динамічні IP-адреси	29	172.16.1.65 – 172.16.1.93	Так, пизначаються
Статичні IP-адреси	1	172.16.1.94	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN15-1			
Динамічні IP-адреси	29	172.16.1.97 – 172.16.1.125	Так, пизначаються
Статичні IP-адреси	1	172.16.1.126	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN16-1			
Динамічні IP-адреси	29	172.16.1.129. – 172.16.1.157	Так, пизначаються
Статичні IP-адреси	1	172.16.1.158	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN12-2			
Динамічні IP-адреси	29	172.16.2.1 – 172.16.2.29	Так, пизначаються
Статичні IP-адреси	1	172.16.2.30	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN13-2			
Динамічні IP-адреси	29	172.16.2.33 – 172.16.2.61	Так, пизначаються
Статичні IP-адреси	1	172.16.2.62	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN14-2			
Динамічні IP-адреси	29	172.16.2.65 – 172.16.2.93	Так, пизначаються
Статичні IP-адреси	1	172.16.2.94	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN15-2			
Динамічні IP-адреси	29	172.16.2.97 – 172.16.2.125	Так, пизначаються
Статичні IP-адреси	1	172.16.2.126	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються

Вид адрес	Кількість	Діапазон IP-адрес/ Ок- ремі IP-адреси	Адреси DHCP- сервером
Мережа для VLAN16-2			
Динамічні IP-адреси	29	172.16.2.129 – 172.16.2.157	Так, пизначаються
Статичні IP-адреси	1	172.16.2.158	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються

На цьому, розробка параметрів IP-адресації є закінченою. Переходимо до наступного етапу впровадження та тестування проекту.

2.4. Підготовка тестового стенду.

Розпочнімо підготовку тестового стенду на основі якого будемо проводити процес налагодження та тестування роботи побудованого проекту комп'ютерної мережі. Відповідно до фізичної топології, для реалізації проекту необхідна наявність хоча б 6-ьох керованих комутаторів, 2-ох міжмережевих екранів Cisco ASA, наявність 2-ох маршрутизаторів, а також робочі станції, котрі можуть бути використаними для проведення подальших тестувань. Загалом, релізація проекту можлива і за дещо спрощеним варіантом з метою зменшення обсягів налаштувань, а також кількості мережевого обладнання, при цьому без значної втрати ефективності та надійності роботи проекту. За своєю суттю, спрощена реалізація проекту нічим не поступається повноцінній фізичній топології, але з точки зору необхідної кількості проведених налаштувань та мережевого обладнання таке рішення є простішим. Спрощений варіант побудови проекту, що буде використано під час подальших налаштувань наведено на рисунку 2.4.1.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		68

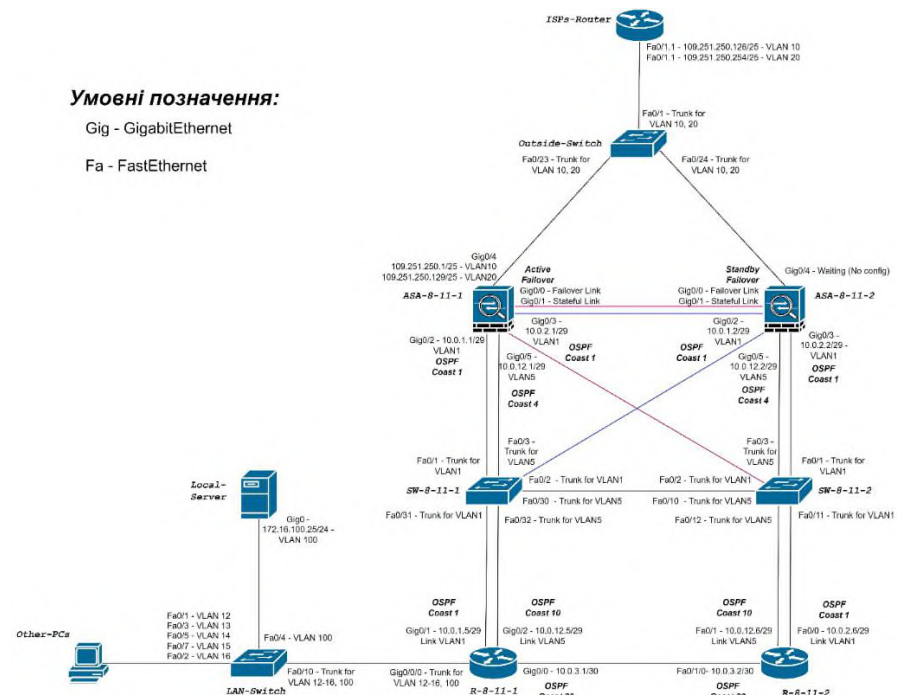


Рисунок 2.4.1 – Спрощена фізична топологія для реалізації на основі тестового стенду.

Такої кількості мережевого обладнання, що наведено на рисунку 2.4.1, буде цілком достатньо для впровадження усіх необхідних функцій та технологій у межах виконання побудови та тестування роботи проекту. Таким чином, використовуючи лабораторію кібербезпеки, що наявна в університеті, було погоджено з керівником проекту та лаборантом можливість отримання доступу до мережевого обладнання для побудови проекту за фізичною топологією, що наведена на рисунку 2.4.1. Тестовий стенд відображено на рисунку 2.4.3.



Рисунок 2.4.2 – Одна з лабораторій кібербезпеки ДУ «Житомирська політехніка»

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				69
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 2.4.3. – Тестовий стенд проекту високонадійного захищеного мультитипровайдерного Інтернет-підключення кампусної мережі організації

Коротко ознайомимося з тестовою стійкою, з якою буде виконуватися подальша робота по впровадженню та тестування побудованого проекту комп'ютерної мережі. На рисунку 2.4.4 нижче наведено умовні позначення мережевого обладнання на схемі спрощеної фізичної топології проекту. Це важливо, щоб у подальшому мати розуміння процесів, що відбуватимуться під час тестування.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				70
Змн.	Арк.	№ докум.	Підпис	Дата		

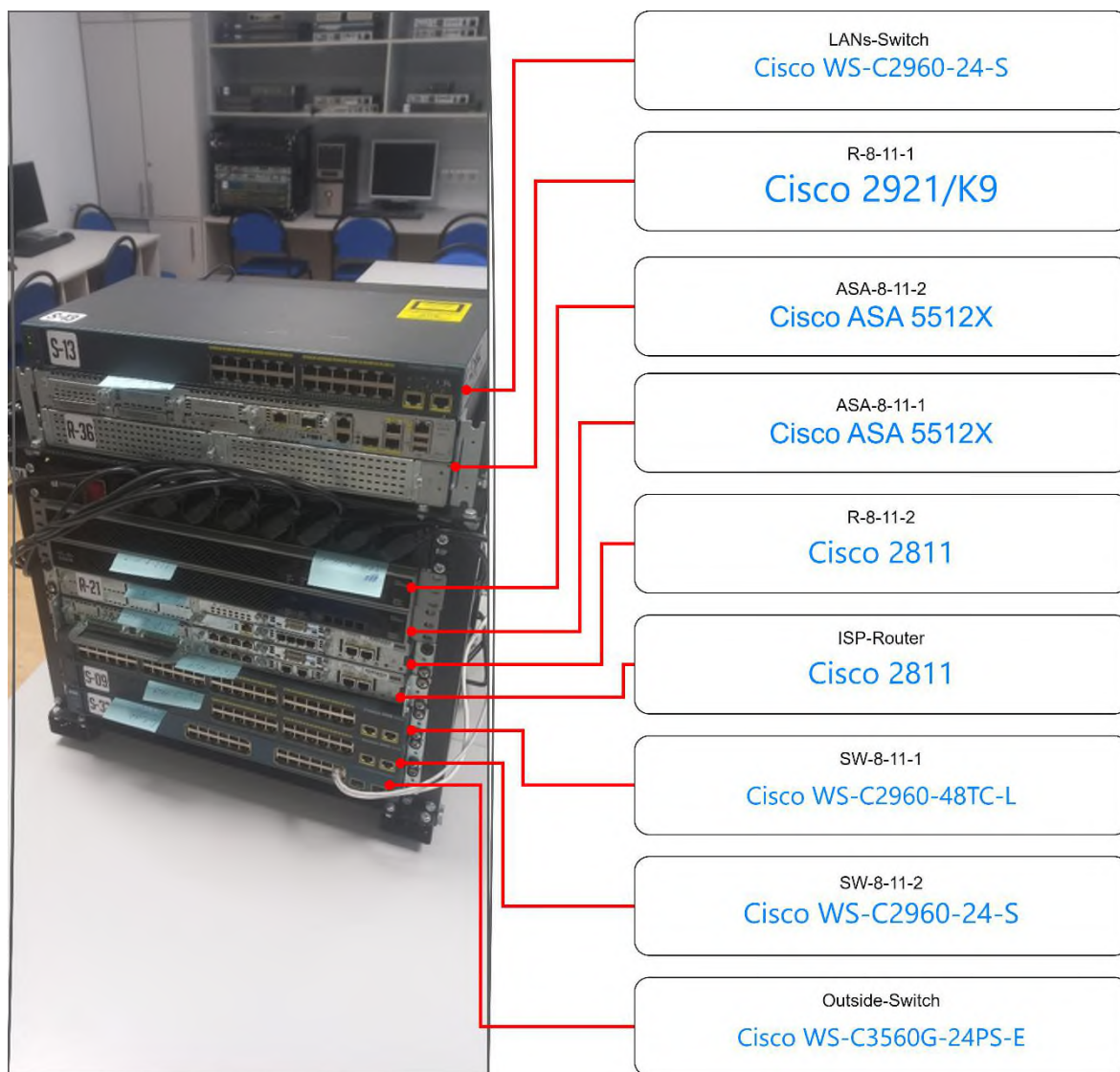


Рисунок 2.4.4. – Моделі та найменування мережевого обладнання у тестовій стійці для реалізації та тестування проекту

У зв'язку з тим, що реалізація проекту планується на основі дещо спрощеної фізичної топології, то схема підключення для спрощеної фізичної топології також буде побудованою та наведена у таблиці 2.4.1.

Таблиця 2.4.1 – Таблиця комутації тестового стенду

ДЛЯ СПРОЩЕНОЇ ФІЗИЧНОЇ ТОПОЛОГІЇ			
Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерфейсу
Мережевий екран ASA-8-11-1	GigabitEthernet0/0	ASA-8-11-2	GigabitEthernet0/0
	GigabitEthernet0/1		GigabitEthernet0/1
	GigabitEthernet0/2	SW-8-11-1	FastEthernet0/1
	GigabitEthernet0/5		FastEthernet0/3

ДЛЯ СПРОЩЕНОЇ ФІЗИЧНОЇ ТОПОЛОГІЇ			
<i>Пристрій</i>	<i>Інтерфейс</i>	<i>Підключення до пристрою</i>	<i>Підключення до інтерфейсу</i>
Мережевий екран ASA-8-11-1	GigabitEthernet0/3	SW-8-11-2	FastEthernet0/3
	GigabitEthernet0/4	Outside-Switch	GigabitEthernet0/1
Мережевий екран ASA-8-11-2	GigabitEthernet0/0	ASA-8-11-1	GigabitEthernet0/0
	GigabitEthernet0/1		GigabitEthernet0/1
	GigabitEthernet0/2	SW-8-11-1	FastEthernet0/2
	GigabitEthernet0/3	SW-8-11-2	FastEthernet0/1
	GigabitEthernet0/5		FastEthernet0/3
	GigabitEthernet0/4	Outside-Switch	GigabitEthernet0/2
Маршрутизатор R-8-11-1	GigabitEthernet0/1	SW-8-11-1	FastEthernet0/31
	GigabitEthernet0/2		FastEthernet0/32
	GigabitEthernet0/0	R-8-11-2	FastEthernet0/1/0
	GigabitEthernet0/0/0	LANs1-Switch	FastEthernet0/10
Маршрутизатор R-8-11-2	FastEthernet0/0	SW-8-11-2	FastEthernet0/11
	FastEthernet0/1		FastEthernet0/12
	FastEthernet0/1/0	R-8-11-1	GigabitEthernet0/0
Комутатор SW-8-11-1	FastEthernet0/1	ASA-8-11-1	GigabitEthernet0/2
	FastEthernet0/3		GigabitEthernet0/5
	FastEthernet0/31	R-8-11-1	GigabitEthernet0/1
	FastEthernet0/32		GigabitEthernet0/2
	FastEthernet0/30	SW-8-11-2	FastEthernet0/10
Комутатор SW-8-11-2	FastEthernet0/1	ASA-8-11-2	GigabitEthernet0/3
	FastEthernet0/3		GigabitEthernet0/5
	FastEthernet0/11	R-8-11-2	FastEthernet0/0
	FastEthernet0/12		FastEthernet0/1
	FastEthernet0/10	SW-8-11-1	FastEthernet0/30
Комутатор LANs1-Switch	FastEthernet0/10	R-8-11-1	GigabitEthernet0/0/0
Комутатор Outside-Switch-1	GigabitEthernet0/1	ASA-8-11-1	GigabitEthernet0/4
	GigabitEthernet0/2	ASA-8-11-2	GigabitEthernet0/4
	GigabitEthernet0/0	ISPs-Router	---

Використовуючи спрощену схему реалізації фізичної топології проекту, що наведено у таблиці 2.4.1, було виконано пробудову проекту комп'ютерної мережі на основі реального мережевого обладнання. Його наведено на рисунку 2.4.5.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		72

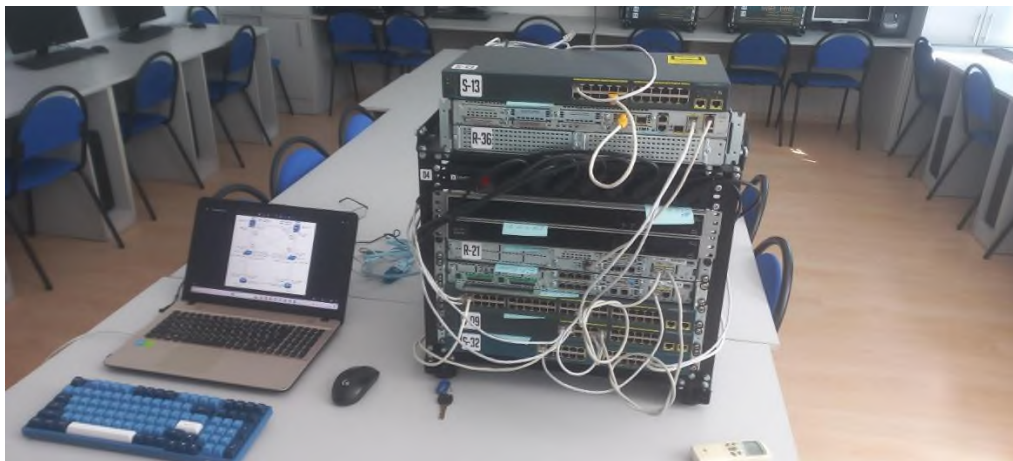


Рисунок 2.4.5. – Результат підготовки та впровадження фізичної топології спрощеного варіанту реалізації проекту на основі тестового стенду

Таким чином, на даному етапі, підготовка тестового стенду є закінченою. Можемо приступати до процесу налагодження мережевого обладнання.

2.5. Налаштування мережевого обладнання.

Перейдемо до процесу налагодження мережевого обладнання. Даний етап виконання роботи є важливим, так як від правильності проведених налаштувань та конфігураційних параметрів тих чи інших технологій залежить функціональні здатності даного проекту. Перед початком виконання налаштувань мережевого обладнання проведемо встановлення термінального додатку PuTTY на основі якого і виконуватимуться консольні підключення до мережевого обладнання. Даний процес покроково продемонстровано нижче:

- Крок 1. Переходимо на офіційний сайт додатку PuTTY та виконуємо його завантаження. Посилання наведено у списках використаних джерел під номером 13.

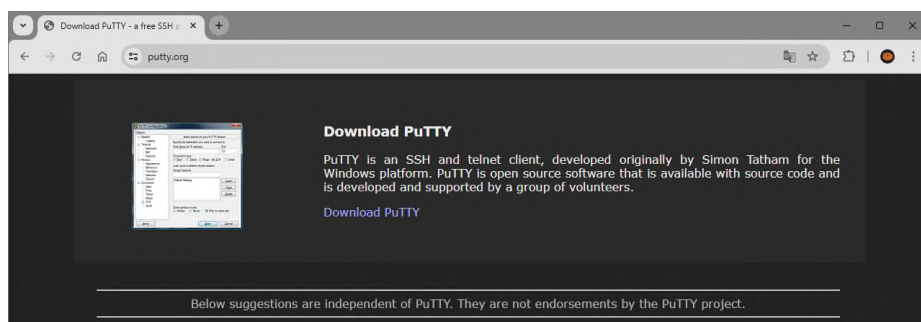


Рисунок 2.5.1 – Офіційний сайт програмного додатку PuTTY

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		73

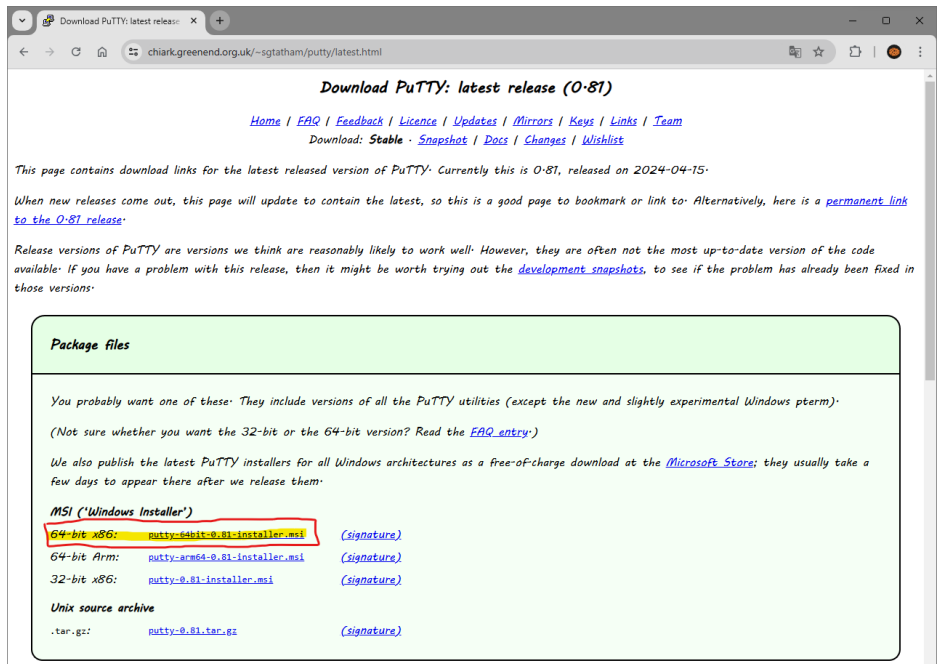


Рисунок 2.5.2 – Сторінка завантаження додатку з посилання на версію для 64-ох розрядної операційної системи Windows

- Крок 2. Відчиняємо встановлювальний пакет програмного додатку та виконуємо його встановлення.

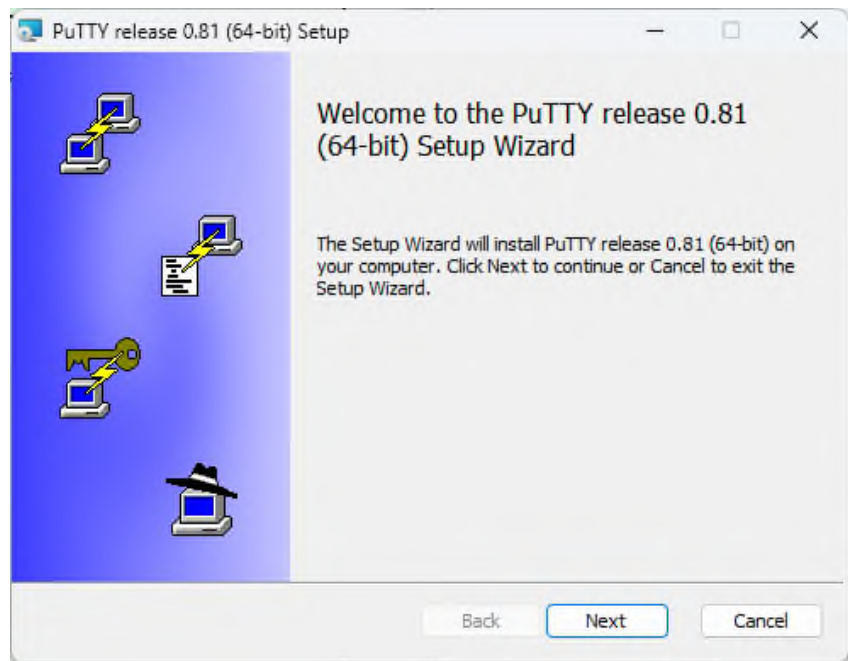


Рисунок 2.5.3 – Вікно інсталяції програмного застосунку PuTTY

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				74
Змн.	Арк.	№ докум.	Підпис	Дата		

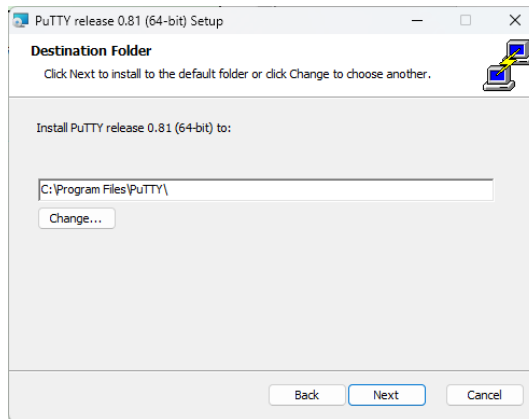


Рисунок 2.5.4 – Вибір місця розташування на диску для програмного застосунку PuTTY під час виконання інсталяції

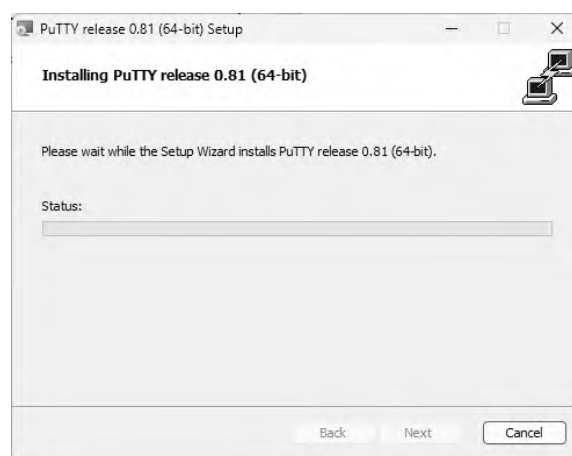


Рисунок 2.5.5 – Процес встановлення термінального програмного додатку PuTTY

- Крок 3. Перевіряємо доступність програмного додатку.

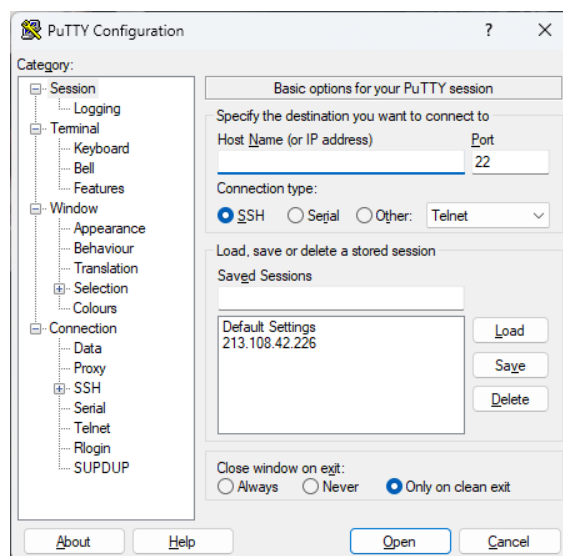


Рисунок 2.5.6 – Вікно термінального програмного додатку PuTTY

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				75
Змн.	Арк.	№ докум.	Підпис	Дата		

- Крок 4. Виконуємо встановлення допоміжного драйвера для консольного підключення на основі послідовного порту. Для цього розпаковуємо архів та виконуємо встановлення через файл «*setup.exe*» (рис. 2.5.7).

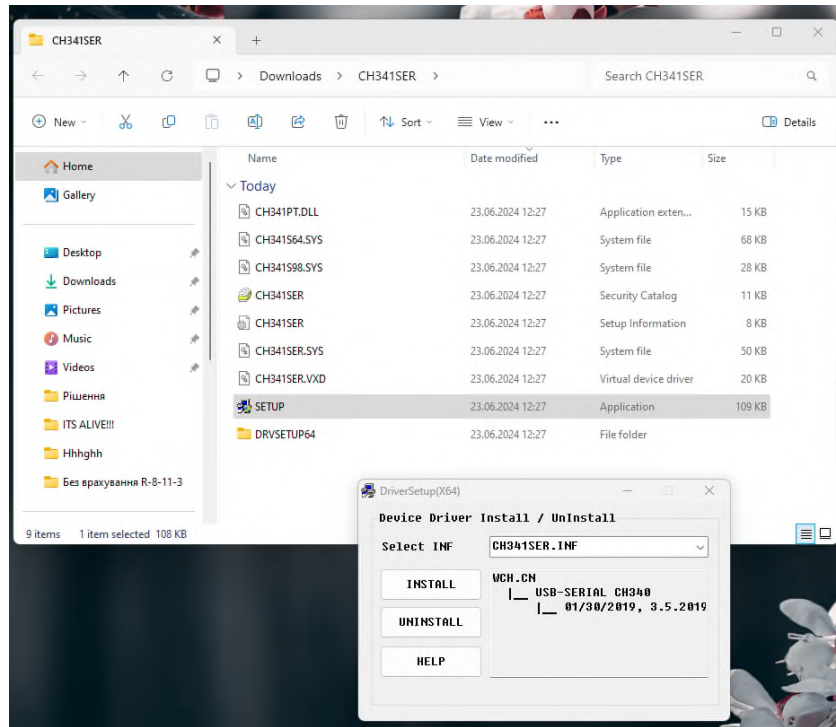


Рисунок 2.5.7 – Встановлений та розархівований каталог допоміжного драйверного застосунку для роботи з послідовним портом. Вікно інсталяційного застосунку

У відповідному контекстному меню настикаємо на кнопку «INSTALL». Приклад наведено нижче (рис. 2.5.8).

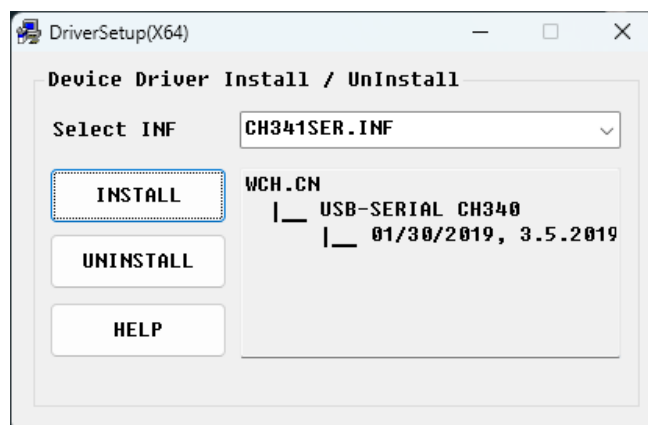


Рисунок 2.5.8 – Вікно інсталяційного застосунку. Активний елемент – кнопка «INSTALL», що виконує автоматичне встановлення допоміжного драйвера

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				76
Змн.	Арк.	№ докум.	Підпис	Дата		

В результаті, драйвер було успішно встановлено. Про це свідчить інформаційне вікно встановлення драйвера (рис. 2.5.9).

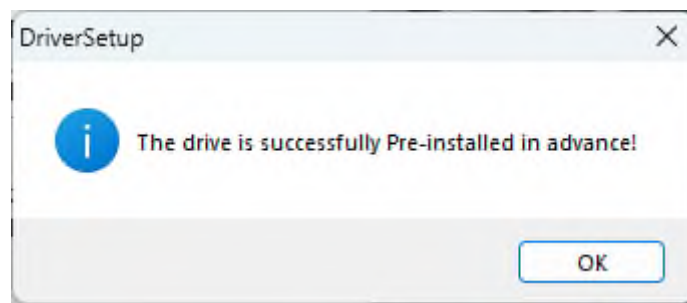


Рисунок 2.5.9 – Вікно успішного виконання встановлення допоміжного драйвера для роботи з послідовним портом

На цьому підготовка термінального додатку для підключення через консольний дріт є завершеною. Переходимо до налагодження обладнання. Виконуємо підключення на основі послідовного COM порту за номером COM3, що відповідає порту USB на портативному ПК з якого виконуватимуться налаштування (рис. 2.5.10). В результаті, з'єднання з мережевим вузлом було успішно встановлено.

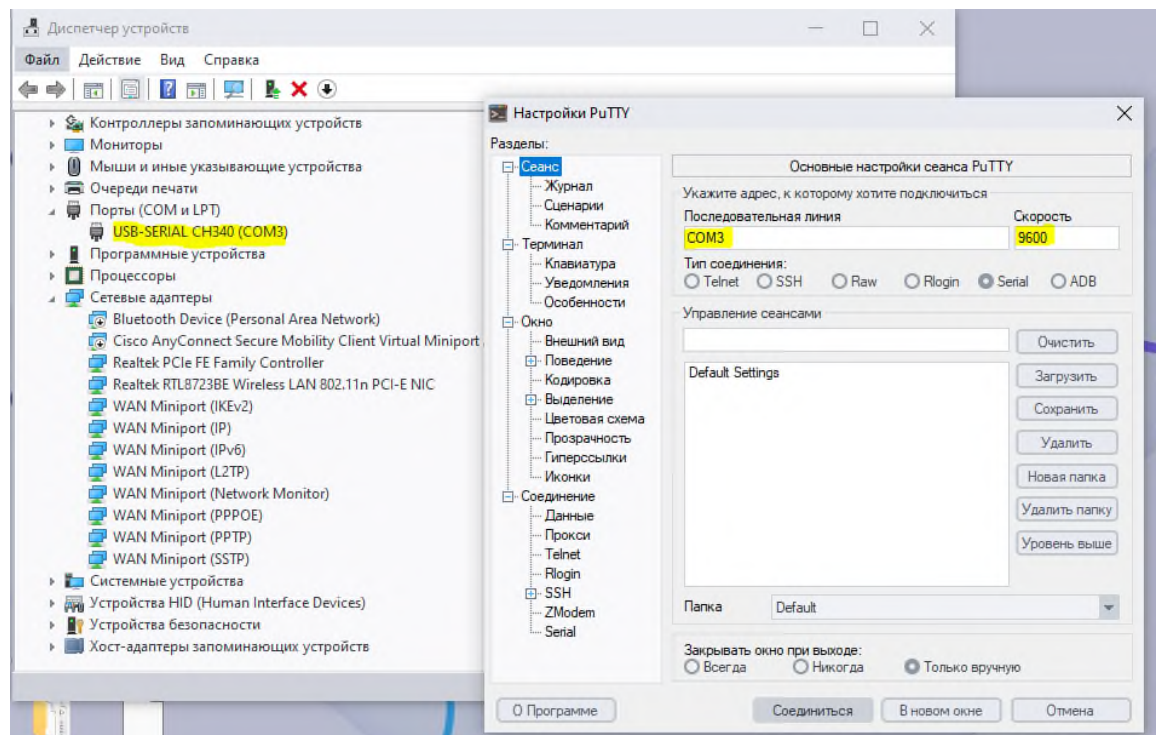


Рисунок 2.5.10 – Вибір послідовного порту для термінального підключення через консольний дріт, що під'єднано до портативного ПК на порт «СОМ3»

Тепер, використовуючи особливості роботи програмного додатку PuTTY, у якості команд налаштування можна застосовувати цілі сценарії виконання коду, що буде нам на користь під час виконання процесу налагодження мережевого обладнання. Тому, розпочинаємо процес налагодження мережевого обладнання. Для цього, виконуючи налаштування за тими чи іншими сценаріями, будемо впроваджувати відповідні налаштування та технології, на основі яких і базуватиметься робота нашого проекту комп'ютерної мережі.

2.5.1. Налаштування міжмережевих екранів Cisco ASA.

Перейдемо до виконання налагоджень міжмережевих екранів Cisco ASA. В першу чергу, проведемо налагодження функціонування технології Failover у режимі Active/Standby. Для цього, виконуємо набір команд в ході виконання яких вказуються ролі для мережевого обладнання, створюють інтерфейси «*Failover Link*» та «*Stateful Link*», а також виконується налагодження їх параметрів IP-адресації для забезпечення інформаційного обміну між ними. Команда «*failover*», що наявна у сценарії налагодження нижче відповідає за початок процесу пошуку сусіда Failover.

Для ASA-8-11-1:

```
conf t
hostname ASA-5512X
failover lan unit primary
int gig0/0
no shutdown
int gig0/1
no shutdown
exit
failover lan interface FAILOVER gig0/0
failover interface ip FAILOVER 192.168.1.100 255.255.255.0 standby
192.168.1.101
failover link STATE gig0/1
failover interface ip STATE 192.168.2.100 255.255.255.0 standby 192.168.2.101
failover
```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		78

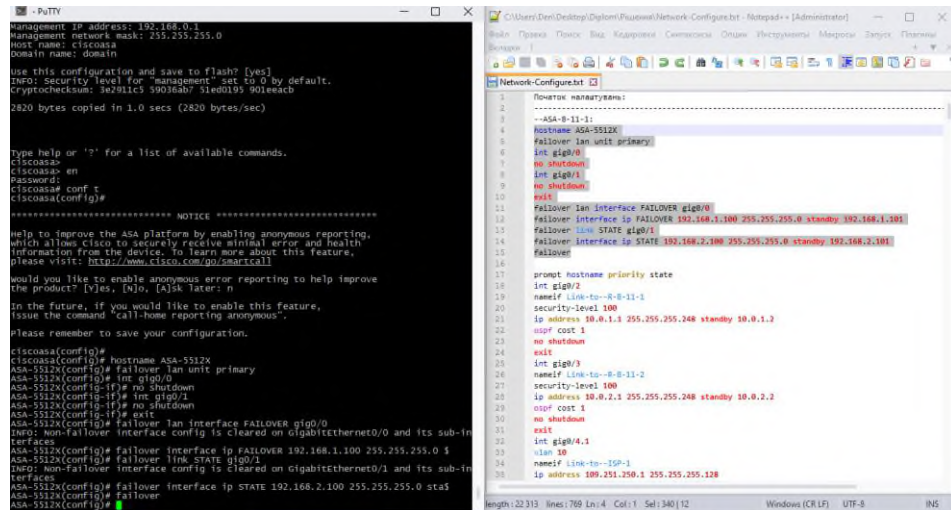


Рисунок 2.5.1.1. – Виконання налаштування роботи технології Failover для міжмережевого екрану ASA-8-11-1. ASA-8-11-1 – Failover Active

Для ASA-8-11-2:

```
conf t
hostname ASA-5512X
failover lan unit secondary
int gig0/0
no shutdown
int gig0/1
no shutdown
exit
failover lan interface FAILOVER gig0/0
failover interface ip FAILOVER 192.168.1.100 255.255.255.0 standby
192.168.1.101
failover link STATE gig0/1
failover interface ip STATE 192.168.2.100 255.255.255.0 standby 192.168.2.101
failover
```

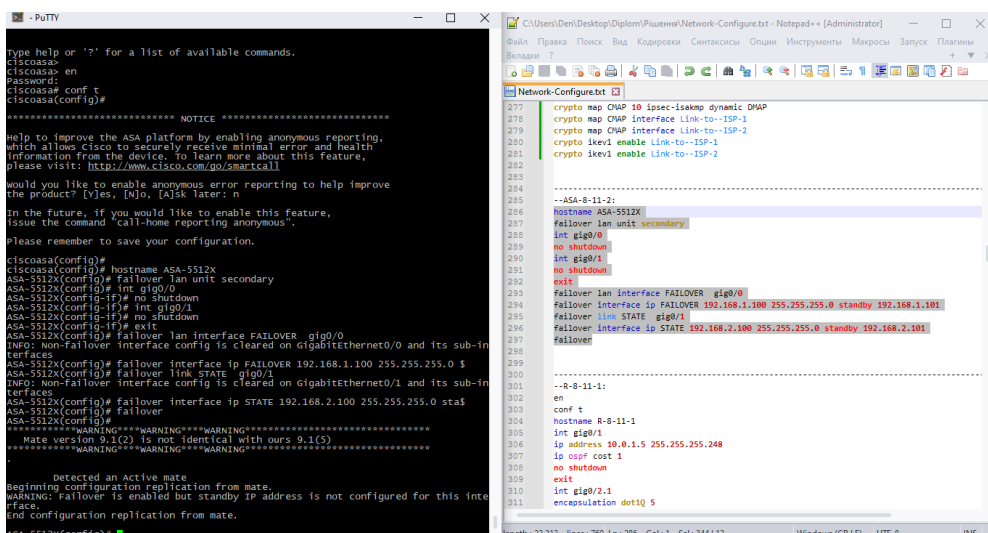


Рисунок 2.5.1.2. – Виконання налаштування роботи технології Failover для міжмережевого екрану ASA-8-11-2. ASA-8-11-2 – Failover Standby

		Колесник Д.В.			Арк.
		Ефименко А.А.			79
Змн.	Арк.	№ докум.	Підпис	Дата	

В результаті такого налаштування, було виконано успішний пошук сусіда Failover, що означає успішне створення пари між вузлами ASA-8-11-1 та ASA-8-11-2. Приклад наведено нижче.

```

Type help or '?' for a list of available commands.
ciscoasa>
ciscoasa> en
Password:
ciscoasa# conf t
ciscoasa(config)#

***** NOTICE *****
help to improve the ASA platform by enabling anonymous reporting,
which allows cisco to securely receive minimal error and health
information from the device. To learn more about this feature,
please visit: http://www.cisco.com/go/smartcall
would you like to enable anonymous error reporting to help improve
the product? [Y]es, [N]o, [A]sk later: n
In the future, if you would like to enable this feature,
issue the command "call-home reporting anonymous".
Please remember to save your configuration.

ciscoasa(config)#
ciscoasa(config)# hostname ASA-5512X
ASA-5512X(config)# failover lan unit secondary
ASA-5512X(config)# int gig0/0
ASA-5512X(config-if)# no shutdown
ASA-5512X(config-if)# int gig0/1
ASA-5512X(config-if)# no shutdown
ASA-5512X(config-if)# exit
ASA-5512X(config)# failover lan interface FAILOVER gig0/0
INFO: Non-failover interface config is cleared on GigabitEthernet0/0 and its sub-in
terfaces
ASA-5512X(config)# failover interface ip FAILOVER 192.168.1.100 255.255.255.0 $
ASA-5512X(config)# failover link STATE gig0/1
INFO: Non-failover interface config is cleared on GigabitEthernet0/1 and its sub-in
terfaces
ASA-5512X(config)# failover interface ip STATE 192.168.2.100 255.255.255.0 sta$
ASA-5512X(config)# failover
ASA-5512X(config)#
*****WARNING*****WARNING*****WARNING*****
Mate version 9.1(2) is not identical with ours 9.1(5)
*****WARNING*****WARNING*****WARNING*****
Detected an Active mate
Beginning configuration replication from mate.
WARNING: Failover is enabled but standby IP address is not configured for this inte
rface.
End configuration replication from mate.
ASA-5512X(config)#
  
```

```

277 crypto map CHAP 10 ipsec-isakmp dynamic DMAP
278 crypto map CHAP interface Link-to--ISP-1
279 crypto map CHAP interface Link-to--ISP-2
280 crypto ikev1 enable Link-to--ISP-1
281 crypto ikev1 enable Link-to--ISP-2
282
283
284 -----
285 --ASA-8-11-2:
286 hostname ASA-5512X
287 failover lan unit secondary
288 int gig0/0
289 no shutdown
290 int gig0/1
291 no shutdown
292 exit
293 failover lan interface FAILOVER gig0/0
294 failover interface ip FAILOVER 192.168.1.100 255.255.255.0 standby 192.168.1.101
295 failover link STATE gig0/1
296 failover interface ip STATE 192.168.2.100 255.255.255.0 standby 192.168.2.101
297 failover
298
299 -----
300 --R-8-11-1:
301 en
302 conf t
303 hostname R-8-11-1
304 int gig0/1
305 ip address 10.0.1.5 255.255.255.248
306 ip ospf cost 1
307 no shutdown
308 exit
309 int gig0/2.1
310 encapsulation dot1q 5
311
  
```

Рисунок 2.5.1.3. – Результат успішного знаходження сусіда Failover. Повідомлення у терміналі «*Detected an Active mate*»

Далі, за рахунок особливостей роботи даної технології, виконання подальших налаштувань буде виконуватися лише для вузла, що на момент налаштувань є активним Failover. Згодом, усі виконані нами налаштування активного вузла будуть репліковані до резервного. У якості активного вузла, під час проведення налаштувань виступав вузол ASA-8-11-1.

Наступним кроком налагодження роботи міжмережевих екранів є налаштування параметрів найменування інтерфейсів, їх параметрів IP-адресації, метрик протоколу OSPF, а також рівні безпеки тих чи інших інтерфейсів. Для зручності роботи з міжмережевими екранами, у якості додаткового налаштування буде виконано налаштування найменування вузла з відображенням поточних характеристики роботи технології Failover, а саме статусу вузла та його пріоритету. Це виконується за рахунок команди – «*prompt hostname priority state*». Інші налаштування

відповідно до сценарію наведені у інформаційному вікні нижче, а також на рисунку 2.5.1.4.

Для ASA-8-11-1:

```
prompt hostname priority state
int gig0/2
nameif Link-to--R-8-11-1
security-level 100
ip address 10.0.1.1 255.255.255.248 standby 10.0.1.2
no shutdown
exit
int gig0/3
nameif Link-to--R-8-11-2
security-level 100
ip address 10.0.2.1 255.255.255.248 standby 10.0.2.2
no shutdown
exit
int gig0/4.1
vlan 10
nameif Link-to--ISP-1
ip address 109.251.250.1 255.255.255.128
int gig0/4.2
vlan 20
nameif Link-to--ISP-2
ip address 109.251.250.129 255.255.255.128
int gig0/4
no shut
exit
int gig0/5.1
vlan 5
nameif Link-for--All
security-level 100
ip address 10.0.12.1 255.255.255.248 standby 10.0.12.2
int gig0/5
no shut
exit
```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		81

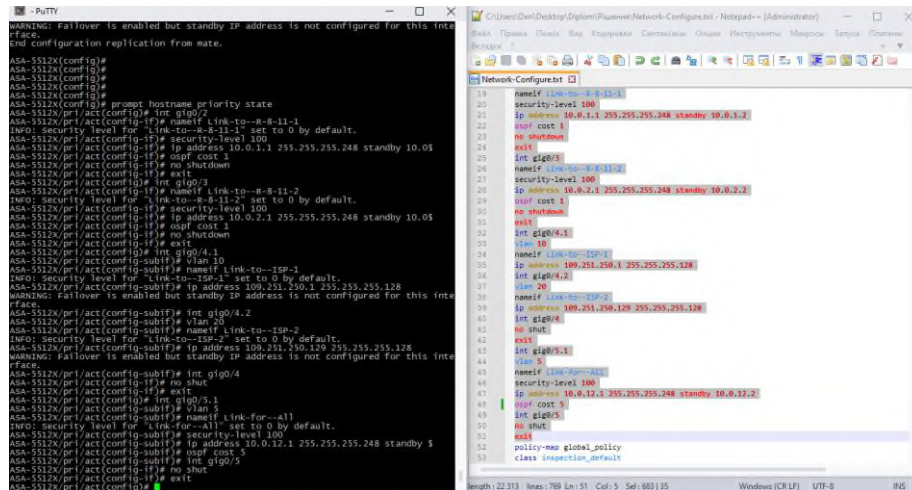


Рисунок 2.5.1.4. – Налаштування мережевих інтерфейсів ASA-8-11-1. Встановлення найменувань, параметрів IP-адресації, метрик інтерфейсів для OSPF, а також рівнів безпеки інтерфейсу

Далі, виконуємо налаштування дозволу для інспектування трафіку протоколу ICMP, щоб у подальшому мати можливість використання діагностичних інструментів для перевірок наявності зв'язку між різними вузлами глобальної мережі (рис. 2.5.1.5). Для цього виконуємо наступний командний сценарій.

Для ASA-8-11-1:

```
policy-map global_policy
class inspection_default
inspect icmp
exit
exit
```

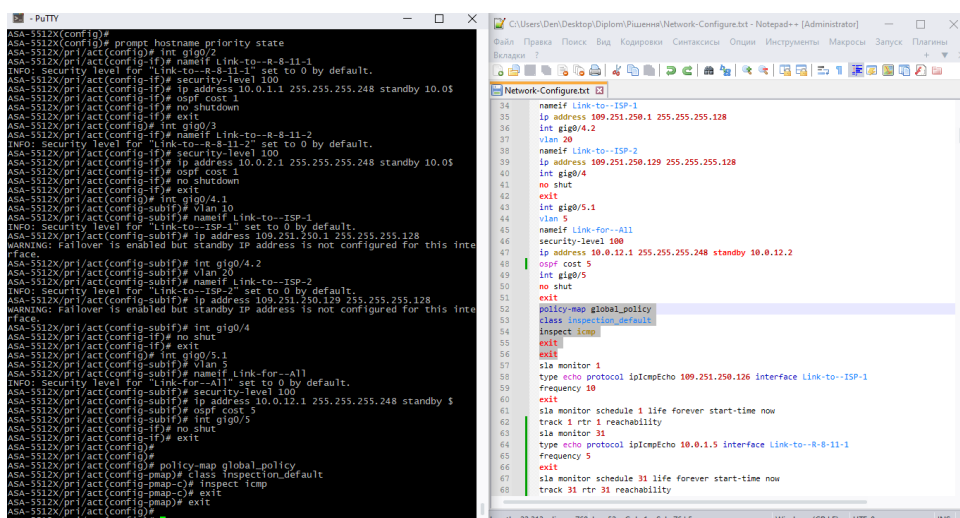


Рисунок 2.5.1.5. – Створення правила інспектування протоколу ICMP на основі глобальної політики «global_policy» та класу «inspection_default»

		Колесник Д.В.			Арк.
		Ефіменко А.А.			82
Змн.	Арк.	№ докум.	Підпис	Дата	

Наступним кроком, виконаємо налагодження роботи технології IP SLA та засобів моніторингу стану вузлів, з метою реалізації засобів вибору шлюзу до мережі одного з мережевих провайдерів, а також інструменту моніторингу стану доступності локальних вузлів. Для цього виконуємо конфігураційні команди, що наведено у інформаційному вікні нижче. Приклад їх виконання також продемонстровано на рисунку 2.5.1.6.

Для ASA-8-11-1:

```
sla monitor 1
type echo protocol ipIcmpEcho 109.251.250.126 interface Link-to--ISP-1
frequency 10
exit
sla monitor schedule 1 life forever start-time now
track 1 rtr 1 reachability
sla monitor 31
type echo protocol ipIcmpEcho 10.0.1.5 interface Link-to--R-8-11-1
frequency 5
exit
sla monitor schedule 31 life forever start-time now
track 31 rtr 31 reachability
sla monitor 32
type echo protocol ipIcmpEcho 10.0.2.6 interface Link-to--R-8-11-2
frequency 5
exit
sla monitor schedule 32 life forever start-time now
track 32 rtr 32 reachability
sla monitor 33
type echo protocol ipIcmpEcho 10.0.12.5 interface Link-for--All
frequency 5
exit
sla monitor schedule 33 life forever start-time now
track 33 rtr 33 reachability
sla monitor 34
type echo protocol ipIcmpEcho 10.0.12.6 interface Link-for--All
frequency 5
exit
sla monitor schedule 34 life forever start-time now
track 34 rtr 34 reachability
```

На основі створеного раніше засобу моніторингу «*track 1*», виконуємо налаштування шлюзів за замовчування до підмережі провайдерів, де перший провайдер буде обиратися за умови, що «*track 1*» є доступним. У протилежному випадку, у якості альтернативного шлюзу буде застосовано підмережу провайдера №2. Для цього виконуємо налаштування, що наведено нижче. Приклад зображено на рисунку 2.5.1.6.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		83

Для ASA-8-11-1:

```
route Link-to--ISP-1 0.0.0.0 0.0.0.0 109.251.250.126 1 track 1
route Link-to--ISP-2 0.0.0.0 0.0.0.0 109.251.250.254 2
```

```
ASA-5512X/pr1/act(config-subif)# nameif Link-for--All
INFO: Security level for "Link-for--All" set to 0 by default.
ASA-5512X/pr1/act(config-subif)# security-level 100
ASA-5512X/pr1/act(config-subif)# ip address 10.0.12.1 255.255.255.248 standby $
ASA-5512X/pr1/act(config-subif)# ospf cost 5
ASA-5512X/pr1/act(config-if)# no shut
ASA-5512X/pr1/act(config-if)# exit
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)# policy-map global_policy
ASA-5512X/pr1/act(config-pmap)# class inspection_default
ASA-5512X/pr1/act(config-pmap-c)# inspect icmp
ASA-5512X/pr1/act(config-pmap-c)# exit
ASA-5512X/pr1/act(config-pmap)# exit
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)# sla monitor 1
ASA-5512X/pr1/act(config-sla-monitor)# type echo protocol ipIcmpEcho 109.251.250.126
ASA-5512X/pr1/act(config-sla-monitor-echo)# frequency 10
ASA-5512X/pr1/act(config-sla-monitor-echo)# exit
ASA-5512X/pr1/act(config-sla-monitor)# sla monitor schedule 1 life forever start-time now
ASA-5512X/pr1/act(config)# track 1 rtr 1 reachability
ASA-5512X/pr1/act(config)# sla monitor 31
ASA-5512X/pr1/act(config-sla-monitor)# type echo protocol ipIcmpEcho 10.0.1.5 $
ASA-5512X/pr1/act(config-sla-monitor-echo)# frequency 5
ASA-5512X/pr1/act(config-sla-monitor-echo)# exit
ASA-5512X/pr1/act(config-sla-monitor)# sla monitor schedule 31 life forever start-time now
ASA-5512X/pr1/act(config)# track 31 rtr 31 reachability
ASA-5512X/pr1/act(config)# sla monitor 32
ASA-5512X/pr1/act(config-sla-monitor)# type echo protocol ipIcmpEcho 10.0.2.5 $
ASA-5512X/pr1/act(config-sla-monitor-echo)# frequency 5
ASA-5512X/pr1/act(config-sla-monitor-echo)# exit
ASA-5512X/pr1/act(config-sla-monitor)# sla monitor schedule 32 life forever start-time now
ASA-5512X/pr1/act(config)# track 32 rtr 32 reachability
ASA-5512X/pr1/act(config)# sla monitor 33
ASA-5512X/pr1/act(config-sla-monitor)# type echo protocol ipIcmpEcho 10.0.12.5 $
ASA-5512X/pr1/act(config-sla-monitor-echo)# frequency 5
ASA-5512X/pr1/act(config-sla-monitor-echo)# exit
ASA-5512X/pr1/act(config-sla-monitor)# sla monitor schedule 33 life forever start-time now
ASA-5512X/pr1/act(config)# track 33 rtr 33 reachability
ASA-5512X/pr1/act(config)# sla monitor 34
ASA-5512X/pr1/act(config-sla-monitor)# type echo protocol ipIcmpEcho 10.0.12.6 $
ASA-5512X/pr1/act(config-sla-monitor-echo)# frequency 5
ASA-5512X/pr1/act(config-sla-monitor-echo)# exit
ASA-5512X/pr1/act(config-sla-monitor)# sla monitor schedule 34 life forever start-time now
ASA-5512X/pr1/act(config)# track 34 rtr 34 reachability
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)# route Link-to--ISP-1 0.0.0.0 0.0.0.0 109.251.250.126 1
ASA-5512X/pr1/act(config)# route Link-to--ISP-2 0.0.0.0 0.0.0.0 109.251.250.254 2
ASA-5512X/pr1/act(config)#
```

```
64 type echo protocol ipIcmpEcho 10.0.1.5 interface Link-to--R-8-11-1
65 frequency 5
66 exit
67 sla monitor schedule 31 life forever start-time now
68 track 31 rtr 31 reachability
69 sla monitor 32
70 type echo protocol ipIcmpEcho 10.0.2.5 interface Link-to--R-8-11-2
71 frequency 5
72 exit
73 sla monitor schedule 32 life forever start-time now
74 track 32 rtr 32 reachability
75 sla monitor 33
76 type echo protocol ipIcmpEcho 10.0.12.5 interface Link-for--All
77 frequency 5
78 exit
79 sla monitor schedule 33 life forever start-time now
80 track 33 rtr 33 reachability
81 sla monitor 34
82 type echo protocol ipIcmpEcho 10.0.12.6 interface Link-for--All
83 frequency 5
84 exit
85 sla monitor schedule 34 life forever start-time now
86 track 34 rtr 34 reachability
87 route Link-to--ISP-1 0.0.0.0 0.0.0.0 109.251.250.126 1 track 1
88 route Link-to--ISP-2 0.0.0.0 0.0.0.0 109.251.250.254 2
89 object network INSIDE-NET1-ISP1
90 range 0.0.0.0 255.255.255.255
91 nat (Link-to--R-8-11-1,Link-to--ISP-1) dynamic interface
92 exit
93 object network INSIDE-NET1-ISP2
94 range 0.0.0.0 255.255.255.255
95 nat (Link-to--R-8-11-1,Link-to--ISP-2) dynamic interface
96 exit
97 object network INSIDE-NET2-ISP1
98 range 0.0.0.0 255.255.255.255
```

Рисунок 2.5.1.6. – Налаштування інструментів моніторингу стану вузлів комп'ютерної мережі, а також впровадження засобів вибору маршруту до підмережі провайдера на основі стану провайдера №1.

Наступним важливим кроком виконання налаштувань є створення правил мережевої трансляції трафіку NAT у режимі Overload. Для виконання цього налаштування, на міжмережевому екрані Cisco ASA буде створено декілька об'єктів мережі, що визначатимуть необхідність трансляції для діапазону тих чи інших локальних IP-адрес, що надходить на відповідний локальний інтерфейс, та мають бути перенаправленими на зовнішній інтерфейс до однієї з підмереж провайдерів. Таким чином, було створено шість об'єктів трансляції NAT для усіх можливих локальних IP-адрес, що визначаються у вигляді діапазону від 0.0.0.0 до 255.255.255.255. Відповідний сценарій налагодження наведено нижче, а також продемонстровано на рисунку 2.5.1.7.

Для ASA-8-11-1:

```
object network INSIDE-NET1-ISP1
range 0.0.0.0 255.255.255.255
nat (Link-to--R-8-11-1,Link-to--ISP-1) dynamic interface
exit
object network INSIDE-NET1-ISP2
range 0.0.0.0 255.255.255.255
nat (Link-to--R-8-11-1,Link-to--ISP-2) dynamic interface
exit
object network INSIDE-NET2-ISP1
range 0.0.0.0 255.255.255.255
nat (Link-to--R-8-11-2,Link-to--ISP-1) dynamic interface
exit
object network INSIDE-NET2-ISP2
range 0.0.0.0 255.255.255.255
nat (Link-to--R-8-11-2,Link-to--ISP-2) dynamic interface
exit
object network INSIDE-NET3-ISP1
range 0.0.0.0 255.255.255.255
nat (Link-for--All,Link-to--ISP-1) dynamic interface
exit
object network INSIDE-NET3-ISP2
range 0.0.0.0 255.255.255.255
nat (Link-for--All,Link-to--ISP-2) dynamic interface
exit
```

```
ASA-5512X/pr# act(config)# track 31 rtr 31 reachability
ASA-5512X/pr# act(config)# sla monitor 32
ASA-5512X/pr# act(config-sla-monitor)# type echo protocol icmpEcho 10.0.2.5 $
ASA-5512X/pr# act(config-sla-monitor-echo)# frequency 5
ASA-5512X/pr# act(config)# sla monitor schedule 32 life forever start-time now
ASA-5512X/pr# act(config)# track 32 rtr 32 reachability
ASA-5512X/pr# act(config)# sla monitor 33
ASA-5512X/pr# act(config-sla-monitor)# type echo protocol icmpEcho 10.0.12.5 $
ASA-5512X/pr# act(config-sla-monitor-echo)# frequency 5
ASA-5512X/pr# act(config-sla-monitor-echo)# exit
ASA-5512X/pr# act(config)# sla monitor schedule 33 life forever start-time now
ASA-5512X/pr# act(config)# track 33 rtr 33 reachability
ASA-5512X/pr# act(config)# sla monitor 34
ASA-5512X/pr# act(config-sla-monitor)# type echo protocol icmpEcho 10.0.12.6 $
ASA-5512X/pr# act(config-sla-monitor-echo)# frequency 5
ASA-5512X/pr# act(config-sla-monitor-echo)# exit
ASA-5512X/pr# act(config)# sla monitor schedule 34 life forever start-time now
ASA-5512X/pr# act(config)# track 34 rtr 34 reachability
ASA-5512X/pr# act(config)#
ASA-5512X/pr# act(config)# route Link-to--ISP-1 0.0.0.0 0.0.0.0 109.251.250.126
ASA-5512X/pr# act(config)# route Link-to--ISP-2 0.0.0.0 0.0.0.0 109.251.250.253
ASA-5512X/pr# act(config)#
ASA-5512X/pr# act(config)#
ASA-5512X/pr# act(config)#
ASA-5512X/pr# act(config)# object network INSIDE-NET1-ISP1
ASA-5512X/pr# act(config-network-object)# range 0.0.0.0 255.255.255.255
ASA-5512X/pr# act(config-network-object)# nat (Link-to--R-8-11-1,Link-to--ISP-$
ASA-5512X/pr# act(config-network-object)# exit
ASA-5512X/pr# act(config)# object network INSIDE-NET1-ISP2
ASA-5512X/pr# act(config-network-object)# range 0.0.0.0 255.255.255.255
ASA-5512X/pr# act(config-network-object)# nat (Link-to--R-8-11-2,Link-to--ISP-$
ASA-5512X/pr# act(config-network-object)# exit
ASA-5512X/pr# act(config)# object network INSIDE-NET2-ISP1
ASA-5512X/pr# act(config-network-object)# range 0.0.0.0 255.255.255.255
ASA-5512X/pr# act(config-network-object)# nat (Link-to--R-8-11-2,Link-to--ISP-$
ASA-5512X/pr# act(config-network-object)# exit
ASA-5512X/pr# act(config)# object network INSIDE-NET2-ISP2
ASA-5512X/pr# act(config-network-object)# range 0.0.0.0 255.255.255.255
ASA-5512X/pr# act(config-network-object)# nat (Link-to--R-8-11-2,Link-to--ISP-$
ASA-5512X/pr# act(config-network-object)# exit
ASA-5512X/pr# act(config)# object network INSIDE-NET3-ISP1
ASA-5512X/pr# act(config-network-object)# range 0.0.0.0 255.255.255.255
ASA-5512X/pr# act(config-network-object)# nat (Link-for--All,Link-to--ISP-1) d$
ASA-5512X/pr# act(config-network-object)# exit
ASA-5512X/pr# act(config)# object network INSIDE-NET3-ISP2
ASA-5512X/pr# act(config-network-object)# range 0.0.0.0 255.255.255.255
ASA-5512X/pr# act(config-network-object)# nat (Link-for--All,Link-to--ISP-2) d$
ASA-5512X/pr# act(config-network-object)# exit
ASA-5512X/pr# act(config)#
```

Рисунок 2.5.1.7. – Налаштування об'єктів трансляції NAT у режимі Overload для 3-х локальних інтерфейсів Cisco ASA та двох глобальних інтерфейсів

Далі, виконуємо налагодження засобів роботи протоколу динамічної маршрутизації OSPF. У межах його налаштування вказуємо ідентифікатор маршрутизатора, відомі йому підмережі, а також вказуємо необхідність поширення власного шлюзу за замовчування до підмереж провайдерів, щоб забезпечити коректний обмін маршрутами з різними учасниками протоколу OSPF. Сценарій даного налаштування наведено нижче, а також продемонстровано на рисунку 2.5.1.8.

Для ASA-8-11-1:

```
router ospf 1
router-id 0.0.0.10
network 10.0.1.0 255.255.255.248 area 1
network 10.0.12.0 255.255.255.248 area 1
network 10.0.2.0 255.255.255.248 area 1
default-information originate
exit
```

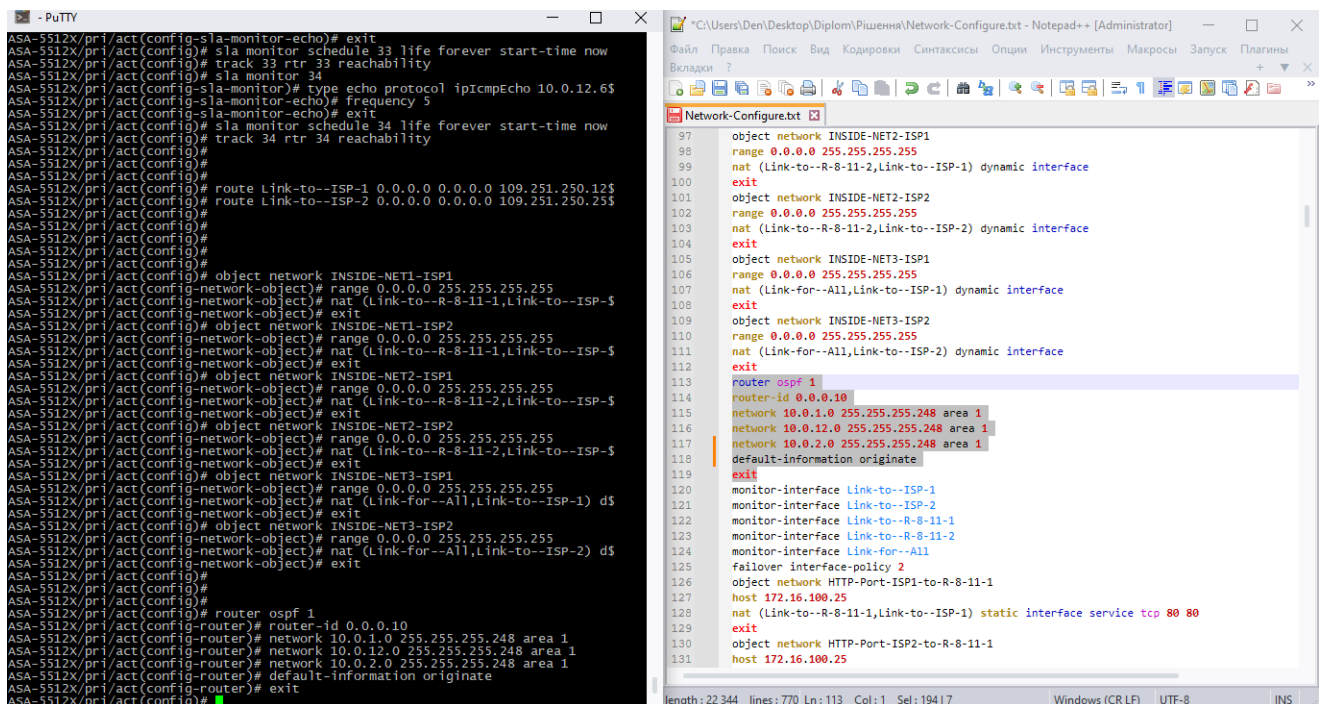


Рисунок 2.5.1.8. – Налаштування процесу OSPF для міжмережевого екрану ASA-8-11-1. Налаштування ідентифікатора маршрутизатора, вказання відомих йому підмереж, а також створення правила поширення власних шлюзів до підмережі провайдерів.

Наступним кроком, виконуємо налаштування правил спрацьовування Failover за статусами інтерфейсів міжмережевого екрану. Для цього, вказуємо інтерфейс, котрий необхідно моніторити, а також правило спрацьовування Failover у

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		86

вигляді виходу з ладу як мінімум двох інтерфейсів. Даний сценарій налаштування наведено нижче, а також відображено на рисунку 2.5.1.9.

Для ASA-8-11-1:

```
monitor-interface Link-to--ISP-1
monitor-interface Link-to--ISP-2
monitor-interface Link-to--R-8-11-1
monitor-interface Link-to--R-8-11-2
monitor-interface Link-for--All
failover interface-policy 2
```

The image shows two windows side-by-side. The left window is a PuTTY terminal session with a Cisco ASA configuration. The right window is a Notepad++ editor showing the configuration file 'Network-Configure.txt'.

PuTTY Terminal Output:

```
ASA-5512X/pr# act(config)#
ASA-5512X/pr# act(config)#
ASA-5512X/pr# act(config)# route Link-to--ISP-1 0.0.0.0 0.0.0.0 109.251.250.12$
ASA-5512X/pr# act(config)# route Link-to--ISP-2 0.0.0.0 0.0.0.0 109.251.250.25$
ASA-5512X/pr# act(config)#
ASA-5512X/pr# act(config)#
ASA-5512X/pr# act(config)#
ASA-5512X/pr# act(config)#
ASA-5512X/pr# act(config)# object network INSIDE-NET1-ISP1
ASA-5512X/pr# act(config-network-object)# range 0.0.0.0 255.255.255.255
ASA-5512X/pr# act(config-network-object)# nat (Link-to--R-8-11-1,Link-to--ISP-$
ASA-5512X/pr# act(config-network-object)# exit
ASA-5512X/pr# act(config-network-object)# range 0.0.0.0 255.255.255.255
ASA-5512X/pr# act(config-network-object)# nat (Link-to--R-8-11-1,Link-to--ISP-$
ASA-5512X/pr# act(config-network-object)# exit
ASA-5512X/pr# act(config-network-object)# object network INSIDE-NET2-ISP1
ASA-5512X/pr# act(config-network-object)# range 0.0.0.0 255.255.255.255
ASA-5512X/pr# act(config-network-object)# nat (Link-to--R-8-11-2,Link-to--ISP-$
ASA-5512X/pr# act(config-network-object)# exit
ASA-5512X/pr# act(config-network-object)# object network INSIDE-NET3-ISP1
ASA-5512X/pr# act(config-network-object)# range 0.0.0.0 255.255.255.255
ASA-5512X/pr# act(config-network-object)# nat (Link-for--All,Link-to--ISP-1) d$
ASA-5512X/pr# act(config-network-object)# exit
ASA-5512X/pr# act(config-network-object)# object network INSIDE-NET3-ISP2
ASA-5512X/pr# act(config-network-object)# range 0.0.0.0 255.255.255.255
ASA-5512X/pr# act(config-network-object)# nat (Link-for--All,Link-to--ISP-2) d$
ASA-5512X/pr# act(config-network-object)# exit
ASA-5512X/pr# act(config)#
ASA-5512X/pr# act(config)#
ASA-5512X/pr# act(config)# router ospf 1
ASA-5512X/pr# act(config-router)# router-id 0.0.0.10
ASA-5512X/pr# act(config-router)# network 10.0.1.0 255.255.255.248 area 1
ASA-5512X/pr# act(config-router)# network 10.0.12.0 255.255.255.248 area 1
ASA-5512X/pr# act(config-router)# network 10.0.2.0 255.255.255.248 area 1
ASA-5512X/pr# act(config-router)# default-information originate
ASA-5512X/pr# act(config-router)# exit
ASA-5512X/pr# act(config)#
ASA-5512X/pr# act(config)#
ASA-5512X/pr# act(config)# monitor-interface Link-to--ISP-1
ASA-5512X/pr# act(config)# monitor-interface Link-to--ISP-2
ASA-5512X/pr# act(config)# monitor-interface Link-to--R-8-11-1
ASA-5512X/pr# act(config)# monitor-interface Link-to--R-8-11-2
ASA-5512X/pr# act(config)# monitor-interface Link-for--All
ASA-5512X/pr# act(config)# failover interface-policy 2
ASA-5512X/pr# act(config)#
```

Notepad++ Content:

```
103 nat (Link-to--R-8-11-2,Link-to--ISP-2) dynamic interface
104 exit
105 object network INSIDE-NET3-ISP1
106 range 0.0.0.0 255.255.255.255
107 nat (Link-for--All,Link-to--ISP-1) dynamic interface
108 exit
109 object network INSIDE-NET3-ISP2
110 range 0.0.0.0 255.255.255.255
111 nat (Link-for--All,Link-to--ISP-2) dynamic interface
112 exit
113 router ospf 1
114 router-id 0.0.0.10
115 network 10.0.1.0 255.255.255.248 area 1
116 network 10.0.12.0 255.255.255.248 area 1
117 network 10.0.2.0 255.255.255.248 area 1
118 default-information originate
119 exit
120 monitor-interface Link-to--ISP-1
121 monitor-interface Link-to--ISP-2
122 monitor-interface Link-to--R-8-11-1
123 monitor-interface Link-to--R-8-11-2
124 monitor-interface Link-for--All
125 failover interface-policy 2
126 object network HTTP-Port-ISP1-to-R-8-11-1
127 host 172.16.100.25
128 nat (Link-to--R-8-11-1,Link-to--ISP-1) static interface service tcp 80 80
129 exit
130 object network HTTP-Port-ISP2-to-R-8-11-1
131 host 172.16.100.25
132 nat (Link-to--R-8-11-1,Link-to--ISP-2) static interface service tcp 80 80
133 exit
134 object network HTTP-Port-ISP1-to-R-8-11-2
135 host 172.16.100.25
136 nat (Link-to--R-8-11-2,Link-to--ISP-1) static interface service tcp 80 81
137 exit
```

Рисунок 2.5.1.9. – Налаштування правил виклику Failover на основі стану інтерфейсів. Активація Failover виконується за умови, що мінімум 2 інтерфейси виходять з ладу.

У якості наступного етапу налаштування, буде виконано налагодження правил переадресації мережевого трафіку, що надходить на один з глобальних інтерфейсів міжмережевого екрану Cisco ASA, тобто тих інтерфейсів, що підключені до глобальної мережі інтернет, за відповідним номером порту для виконання переадресації такого трафіку до внутрішньої підмережі серверів, а саме до внутрішнього сервера, на якому може бути розміщено деякі сервісні служби. Відповідно до нище наведеного сценарію налаштування, буде виконано створення правил переадресації зовнішніх портів 80 – 82, до внутрішнього сервера 172.16.100.25 на порт 80, що

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефименко А.А.				87
Змн.	Арк.	№ докум.	Підпис	Дата		

відповідає порту протокола HTTP. Правила переадресації портів 3389 – 3391 виконуються з метою забезпечення доступу до локального сервера 172.16.100.25 на порт 3389 для роботи протоколу RDP, або протоколу віддаленого робочого столу, через один з доступних каналів зв'язку до кінцевої підмережі.

Для ASA-8-11-1:

```
object network HTTP-Port-ISP1-to-R-8-11-1
host 172.16.100.25
nat (Link-to--R-8-11-1,Link-to--ISP-1) static interface service tcp 80 80
exit
object network HTTP-Port-ISP2-to-R-8-11-1
host 172.16.100.25
nat (Link-to--R-8-11-1,Link-to--ISP-2) static interface service tcp 80 80
exit
object network HTTP-Port-ISP1-to-R-8-11-2
host 172.16.100.25
nat (Link-to--R-8-11-2,Link-to--ISP-1) static interface service tcp 80 81
exit
object network HTTP-Port-ISP2-to-R-8-11-2
host 172.16.100.25
nat (Link-to--R-8-11-2,Link-to--ISP-2) static interface service tcp 80 81
exit
object network HTTP-Port-ISP1-to-All
host 172.16.100.25
nat (Link-for--All,Link-to--ISP-1) static interface service tcp 80 82
exit
object network HTTP-Port-ISP2-to-All
host 172.16.100.25
nat (Link-for--All,Link-to--ISP-2) static interface service tcp 80 82
exit
object network RDP-Port-ISP1-to-R-8-11-1
host 172.16.100.25
nat (Link-to--R-8-11-1,Link-to--ISP-1) static interface service tcp 3389 3389
exit
object network RDP-Port-ISP2-to-R-8-11-1
host 172.16.100.25
nat (Link-to--R-8-11-1,Link-to--ISP-2) static interface service tcp 3389 3389
exit
object network RDP-Port-ISP1-to-R-8-11-2
host 172.16.100.25
nat (Link-to--R-8-11-2,Link-to--ISP-1) static interface service tcp 3389 3390
exit
object network RDP-Port-ISP2-to-R-8-11-2
host 172.16.100.25
nat (Link-to--R-8-11-2,Link-to--ISP-2) static interface service tcp 3389 3390
exit
object network RDP-Port-ISP1-to-All
host 172.16.100.25
nat (Link-for--All,Link-to--ISP-1) static interface service tcp 3389 3391
exit
object network RDP-Port-ISP2-to-All
host 172.16.100.25
nat (Link-for--All,Link-to--ISP-2) static interface service tcp 3389 3391
exit
```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		88

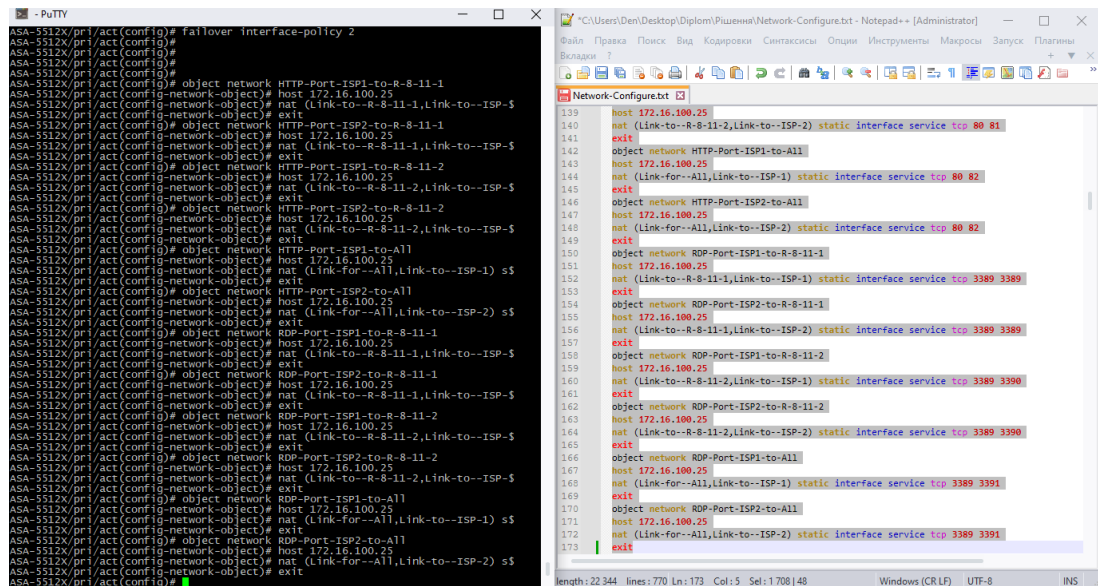


Рисунок 2.5.1.10. – Налаштування правил статичної переадресації NAT для доступу до локального сервера 172.16.100.25 з глобальної мережі Інтернет

У зв'язку з тим, що відповідно до правил роботи міжмережевого екрану у разі передачі трафіку від інтерфейса з меншим рівень безпеки, у нашому випадку від рівня безпеки 0, до інтерфейса з більшим рівнем безпеки, у нашому випадку це рівень 100, виконується застосування правила «ір deny any any», тобто заборона усього трафіку, то наступним кроком налаштування є створення списку доступу на дозвіл передачу трафіку за тим чи іншим портом до локальної підмережі серверів. Для цього, було виконано команди, що наведені у сценарії нижче. Відповідні списки доступу було застосовано до того чи іншого інтерфейсу, що забезпечує інформаційний обмін між вузлами глобальної мережі (рис. 2.5.1.11).

Для ASA-8-11-1:

```
access-list Ports-Forwarding-ISP1 extended permit tcp any object HTTP-Port-ISP1-to-R-8-11-1 eq 80
access-list Ports-Forwarding-ISP1 extended permit tcp any object HTTP-Port-ISP1-to-R-8-11-2 eq 81
access-list Ports-Forwarding-ISP1 extended permit tcp any object HTTP-Port-ISP1-to-A11 eq 82
access-list Ports-Forwarding-ISP1 extended permit tcp any object RDP-Port-ISP1-to-R-8-11-1 eq 3389
access-list Ports-Forwarding-ISP1 extended permit tcp any object RDP-Port-ISP1-to-R-8-11-2 eq 3390
access-list Ports-Forwarding-ISP1 extended permit tcp any object RDP-Port-ISP1-to-A11 eq 3391
```

```

access-list Ports-Forwarding-ISP2 extended permit tcp any object HTTP-Port-ISP2-to-R-8-11-1 eq 80
access-list Ports-Forwarding-ISP2 extended permit tcp any object HTTP-Port-ISP2-to-R-8-11-2 eq 81
access-list Ports-Forwarding-ISP2 extended permit tcp any object HTTP-Port-ISP2-to-All eq 82
access-list Ports-Forwarding-ISP2 extended permit tcp any object RDP-Port-ISP2-to-R-8-11-1 eq 3389
access-list Ports-Forwarding-ISP2 extended permit tcp any object RDP-Port-ISP2-to-R-8-11-2 eq 3390
access-list Ports-Forwarding-ISP2 extended permit tcp any object RDP-Port-ISP2-to-All eq 3391
access-group Ports-Forwarding-ISP1 in interface Link-to--ISP-1
access-group Ports-Forwarding-ISP2 in interface Link-to--ISP-2

```

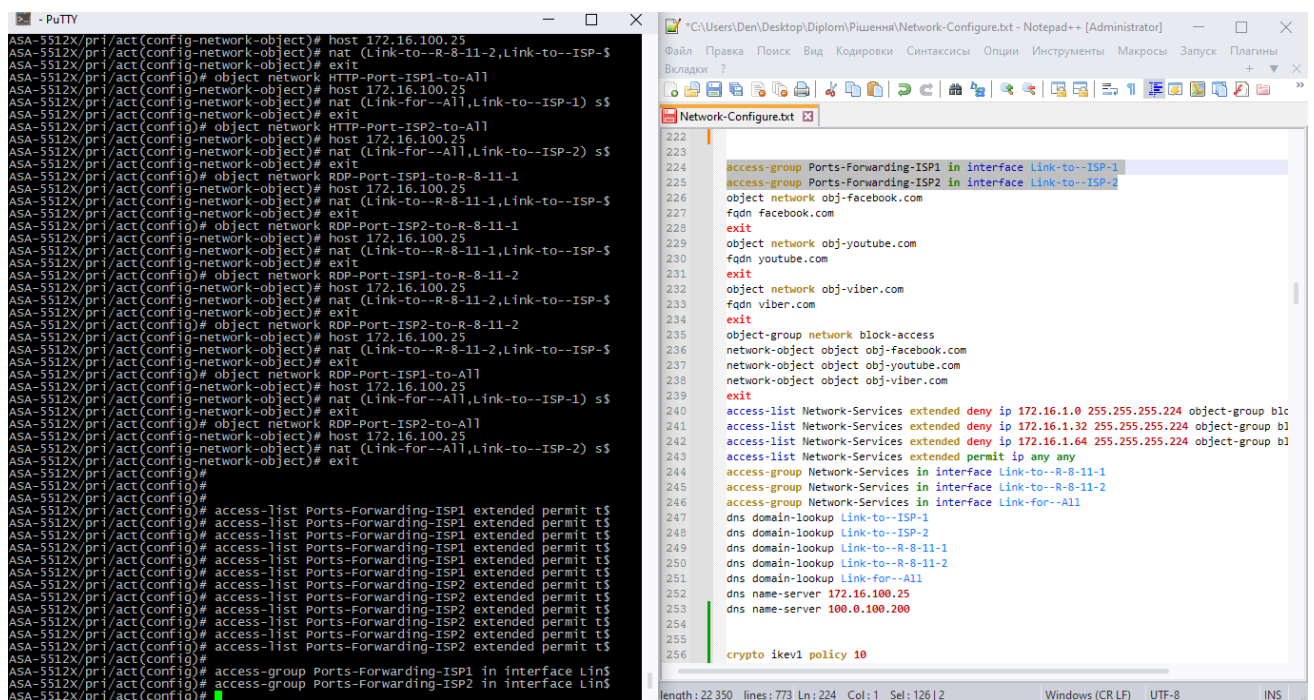


Рисунок 2.5.1.11. – Створення дозволів на проходження зовнішнього мережевого трафіку до внутрішньої підмережі серверів на основі чітко визначених портів доступу

Наступним кроком, виконаємо налагодження засобів фільтрації мережевого трафіку на основі FQDN для створення інструменту блокування доступу до тих чи інших інтернет ресурсів за їх доменними іменами. Відповідно до проведених налаштувань, що відзначені у сценарії нижче, виконується створення декількох об'єктів мережі, що визначають доменні імена ресурсів доступ до яких необхідно заблокувати. Далі, ці ресурси об'єднують у групу об'єктів, котра далі буде використана у списках контролю доступу, для забезпечення динамічного додавання заборон у список контролю доступу на основі усіх об'єктів, що входять у групу об'єктів

		Колесник Д.В.				КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефименко А.А.					90
Змн.	Арк.	№ докум.	Підпис	Дата			

блокування. Після чого створюється розширений список контролю доступу на основі роботи якого виконується блокування усього можливого трафіку, для тієї чи іншої локальної підмережі, до чітко визначених глобальних ресурсів. Отримані списки доступу застосовуються на вхід інтерфейсів підключення до локальної мережі. Приклад виконання налаштувань наведено на рисунку 2.5.1.12.

Для ASA-8-11-1:

```
object network obj-facebook.com
fqdn facebook.com
exit
object network obj-youtube.com
fqdn youtube.com
exit
object network obj-viber.com
fqdn viber.com
exit
object-group network block-access
network-object object obj-facebook.com
network-object object obj-youtube.com
network-object object obj-viber.com
exit
access-list Network-Services extended deny ip 172.16.1.0 255.255.255.224 object-group
block-access log
access-list Network-Services extended deny ip 172.16.1.32 255.255.255.224 object-group
block-access log
access-list Network-Services extended deny ip 172.16.1.64 255.255.255.224 object-group
block-access log
access-list Network-Services extended permit ip any any
access-group Network-Services in interface Link-to--R-8-11-1
access-group Network-Services in interface Link-to--R-8-11-2
access-group Network-Services in interface Link-for--All
```

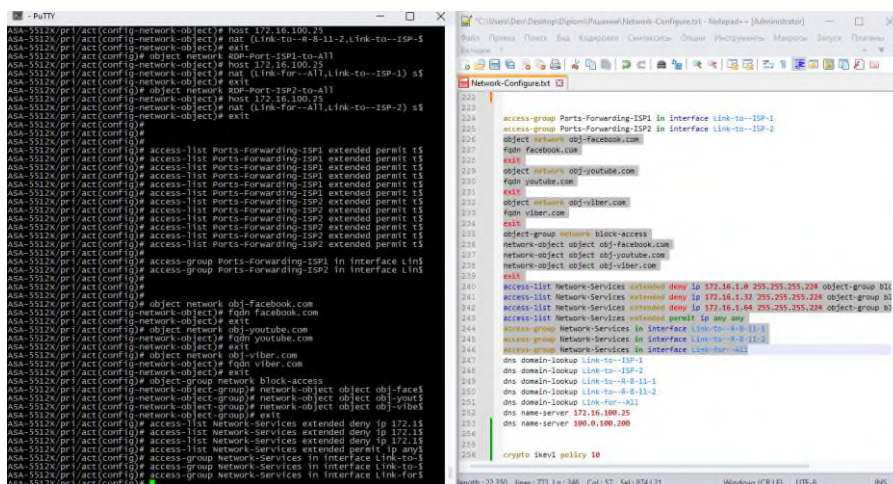


Рисунок 2.5.1.12. – Створення засобів фільтрації доступу до мережевих ресурсів на основі FQDN. Створення розширеного списку контролю доступу на основі об’єктів блокування. Застосування правил у списках контролю доступу до локальних інтерфейсів на вхід

		Колесник Д.В.			Арк.
		Ефіменко А.А.			91
Змн.	Арк.	№ докум.	Підпис	Дата	

Для роботи вище наведених засобів блокування мережевого трафіку на основі списків контролю доступу та об'єктів FQDN, виконуємо налаштування роботи засобів DNS міжмережевому екрані. Для цього вказуємо інтерфейси, на яких необхідно виконувати пошуку домених серверів, а також їх IP-адреси, що у межах роботи представлені у вигляді локального DNS сервера (172.16.100.25), а також деякого глобального DNS сервера (100.0.100.200). Відповідний сценарій налагодження наведено нижче, а також відображено на рисунку 2.5.1.13.

Для ASA-8-11-1:

```
dns domain-lookup Link-to--ISP-1
dns domain-lookup Link-to--ISP-2
dns domain-lookup Link-to--R-8-11-1
dns domain-lookup Link-to--R-8-11-2
dns domain-lookup Link-for--All
dns name-server 172.16.100.25
dns name-server 100.0.100.200
```

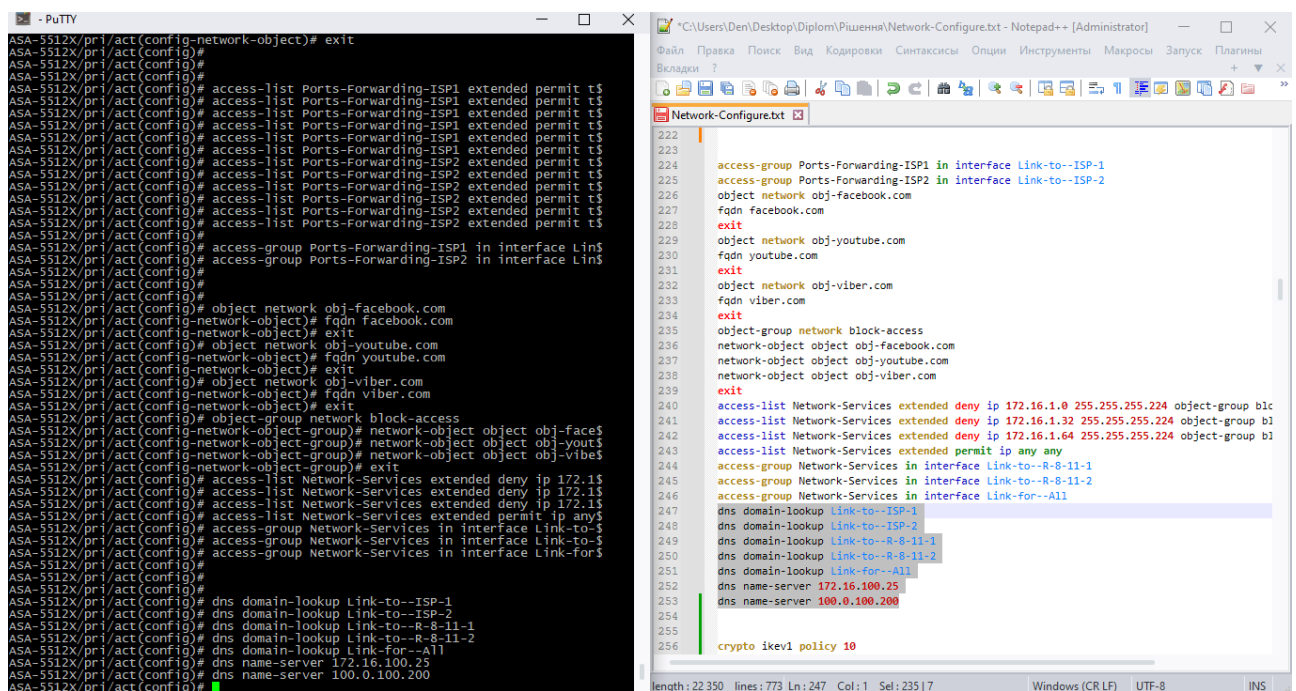


Рисунок 2.5.1.13. – Налаштування інтерфейсів пошуку DNS-серверів. Встановлення параметрів IP-адресації локального та глобального DNS-серверів.

На цьому виконання налаштувань міжмережевих екранів є завершеним, тому рухаємося далі.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефименко А.А.				92
Змн.	Арк.	№ докум.	Підпис	Дата		

2.5.2. Налаштування мережевих комутаторів.

Виконуємо налагодження мережевих комутаторів. В цілому, особливостей їх налаштування в даному проекті немає. Виконуємо лише розподіл деяких інтерфейсів для реалізації роботи інтерфейсів VLAN5, що піключені до інтерфейсів FastEthernet0/3, FastEthernet0/30 та FastEthernet0/32 комутатора SW-8-11-1 та інтерфейсів FastEthernet0/3, FastEthernet0/10 та FastEthernet0/12 комутатора SW-8-11-2. У якості режиму роботи інтерфейса важливо встановити «trunk». У протилежному варіанті, робота цих каналів зв'язку не відбуватиметься через використання засобів енкапсуляції «Dot1Q» на маршрутизаторах та міжмережевих екранах Cisco ASA. Сценарії налагодження комутаторів комп'ютерної мережі наведено у сценаріях, що відображені нижче. Також, сценарії налаштувань наведені на рисунках 2.5.2.1 та 2.5.2.2.

Для SW-8-11-1:

```
en
conf t
hostname SW-8-11-1
vlan 5
name VLAN-5-LAN
exit
int fa0/32
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit
int fa0/30
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit
int fa0/3
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit
```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		93

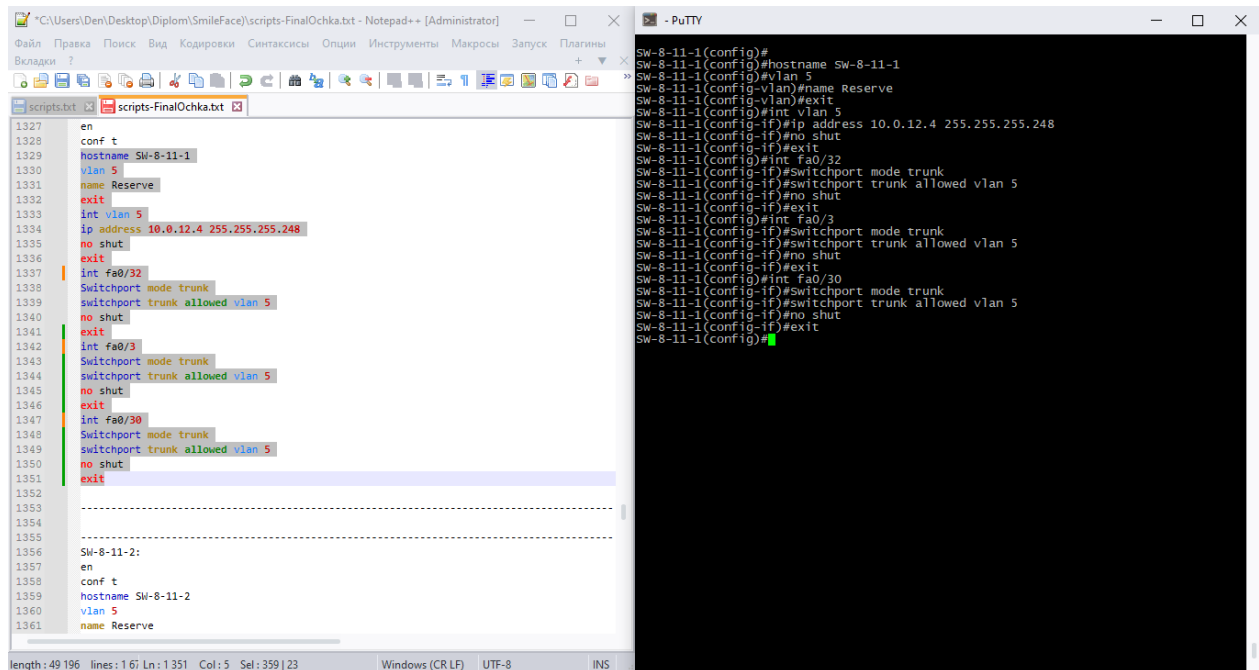


Рисунок 2.5.2.1. – Налаштування комутатора SW-8-11-1

Для SW-8-11-2:

```

en
conf t
hostname SW-8-11-2
no vlan 2
name VLAN-2-LAN
exit
vlan 5
name VLAN-5-LAN
exit
int fa0/12
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit
int fa0/10
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit
int fa0/3
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				94
Змн.	Арк.	№ докум.	Підпис	Дата		

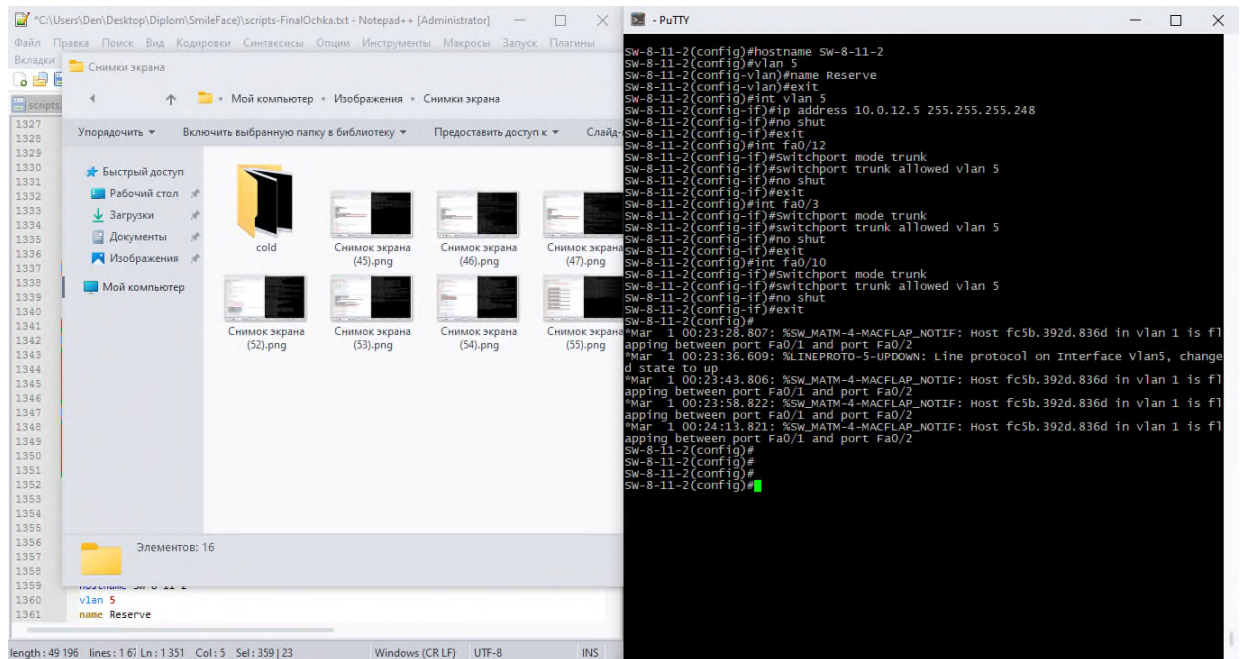


Рисунок 2.5.2.2. – Налаштування комутатора SW-8-11-2

Наступним кроком, проведемо також налагодження локального маршрутизатора, що підключений за схемою тестового стенду до маршрутизатора R-8-11-1 та виконує комутацію для забезпечення роботи локальних вузлів нашого проекту. Відповідно, необхідно провести налагодження транкового каналу зв'язку між маршрутизатором для забезпечення роботи різних підмереж VLAN, а також присвоєння різних міток VLAN тим чи іншим інтерфейсам даного комутатора. Це виконується шляхом встановлення режиму роботи порту «access», а також привласнювання йому мітки деякого VLAN. Сценарій налагодження даного комутатора наведено нижче. Приклад відображено на рисунку 2.5.2.3.

Для LAN-Switch:

```

en
conf t
hostname LAN-Switch
vlan 12
name VLAN-12-LAN
exit
vlan 13
name VLAN-13-LAN
exit
vlan 14
name VLAN-14-LAN
exit

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				95
Змн.	Арк.	№ докум.	Підпис	Дата		

```

vlan 15
name VLAN-15-LAN
exit
vlan 16
name VLAN-16-LAN
exit
vlan 100
name VLAN-100-Serv&Service
exit
int fa0/10
switchport mode trunk
switchport trunk allowed vlan 12,13,14,15,16,100
exit
int fa0/1
switchport mode access
switchport access vlan 12
exit
int fa0/3
switchport mode access
switchport access vlan 13
exit
int fa0/5
switchport mode access
switchport access vlan 14
exit
int fa0/7
switchport mode access
switchport access vlan 15
exit
int fa0/2
switchport mode access
switchport access vlan 16
exit
int fa0/4
switchport mode access
switchport access vlan 100
exit

```

Рисунок 2.5.2.3. – Налаштування локального комутатора LAN-Switch

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				96
Змн.	Арк.	№ докум.	Підпис	Дата		

На цьому, виконання налагодження для локальних комутаторів є закінченим. Переходимо до налаштувань мережесих маршрутизаторів.

2.5.3. Налаштування маршрутизаторів.

Перейдемо до етапу налаштування маршрутизаторі комп'ютерної мережі. В першу чергу, проведемо виконання процесу налаштування параметрів їх найменування, а також параметрів IP-адресації. Також, створимо під-інтерфейси для роботи VLAN підмереж і аналогічно встановимо для них параметри IP-адресації. Таким чином, такі налаштування для мережесих маршрутизаторів наведені у сценаріях нижче. Також, приклади виконання таких налаштувань наведені на рисунках 2.5.3.1 та 2.5.3.2.

Для R-8-11-1:

```
en
conf t
hostname R-8-11-1
int gig0/1
ip address 10.0.1.5 255.255.255.248
ip ospf cost 1
no shutdown
exit
int gig0/2.1
encapsulation dot1Q 5
ip address 10.0.12.5 255.255.255.248
ip ospf cost 10
int gig0/2
no shutdown
exit
int gig0/0
ip address 10.0.3.1 255.255.255.252
ip ospf cost 20
no shutdown
exit
int gig0/0/0.12
description For-VLAN2
encapsulation dot1Q 12
ip address 172.16.1.30 255.255.255.224
exit
int gig0/0/0.13
description For-VLAN3
encapsulation dot1Q 13
ip address 172.16.1.62 255.255.255.224
exit
int gig0/0/0.14
description For-VLAN4
encapsulation dot1Q 14
ip address 172.16.1.94 255.255.255.224
exit
```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				97
Змн.	Арк.	№ докум.	Підпис	Дата		

```

int gig0/0/0.15
description For-VLAN5
encapsulation dot1Q 15
ip address 172.16.1.126 255.255.255.224
exit
int gig0/0/0.16
description For-VLAN6
encapsulation dot1Q 16
ip address 172.16.1.158 255.255.255.224
exit
int gig0/0/0.100
description VLAN100-Server&Services
encapsulation dot1Q 100
ip address 172.16.100.254 255.255.255.0
exit
int gig0/0/0
no shut
exit

```

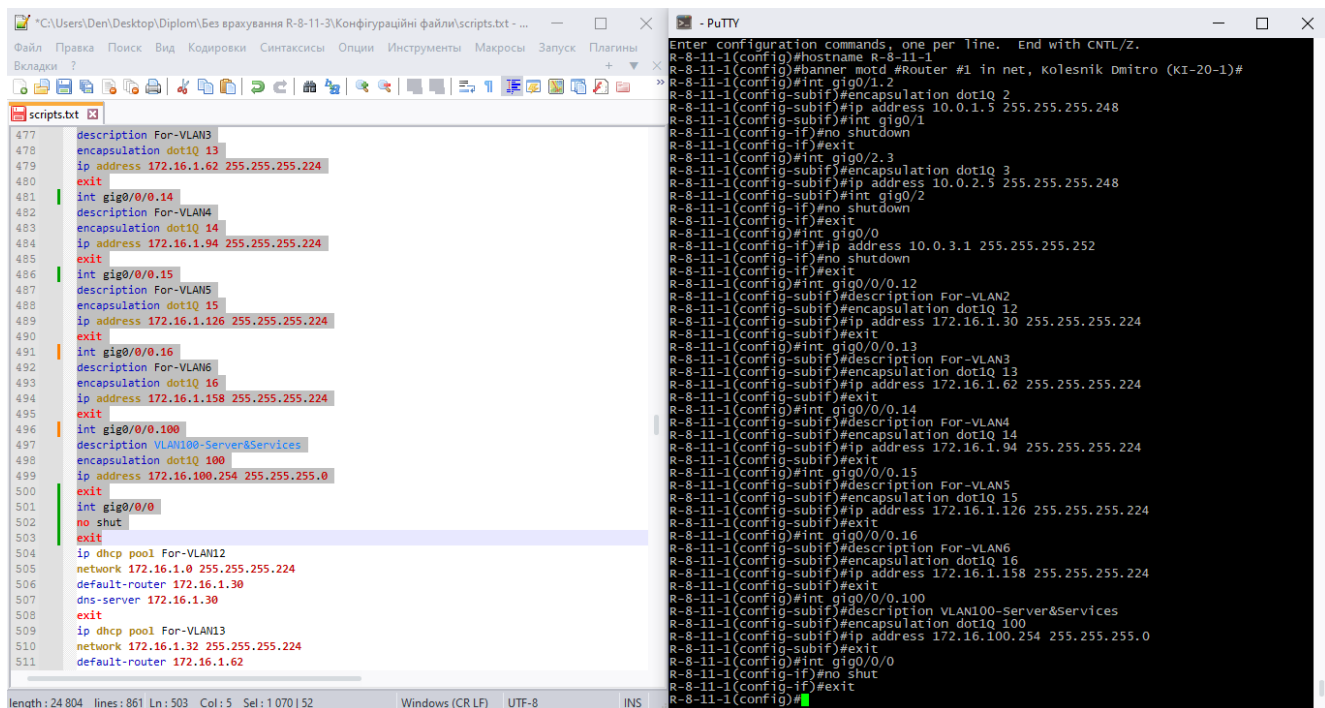


Рисунок 2.5.3.1. – Налаштування інтерфейсів та під-інтерфейсів маршрутизатора R-8-11-1. Налаштування метрик інтерфейсу для протоколу OSPF

Для R-8-11-2:

```

en
conf t
hostname R-8-11-2
int fa0/0
description Link-for-VLAN2
ip address 10.0.2.6 255.255.255.248
ip ospf cost 1
no shutdown
exit

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				98
Змн.	Арк.	№ докум.	Підпис	Дата		

```

int fa0/1.1
description Link-for-VLAN3
encapsulation dot1Q 5
ip address 10.0.12.6 255.255.255.248
ip ospf cost 10
int fa0/1
no shutdown
exit
int fa0/1/0
description Link-to--R-8-11-1
ip address 10.0.3.2 255.255.255.252
ip ospf cost 20
no shutdown
exit

```

Рисунок 2.5.3.2. – Налаштування інтерфейсів та під-інтерфейсів маршрутизатора R-8-11-2. Налаштування метрик інтерфейсу для протоколу OSPF

Наступним кроком, виконуємо налаштування IP DHCP пулів для роботи технології DHCP у різних підмережах VLAN. Для цього було виконано наступний сценарій налаштувань, де було вказано підмережу, DNS-сервери для підмережі та шлюз за замовчуванням. Також, додаємо виключення IP-адрес з пулів динамічного присвоювання, щоб уникнути проблем у дублюванні параметрів IP-адресації (рис. 2.5.3.3).

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефименко А.А.				99
Змн.	Арк.	№ докум.	Підпис	Дата		

Для R-8-11-1:

```
ip dhcp pool For-VLAN12
network 172.16.1.0 255.255.255.224
default-router 172.16.1.30
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN13
network 172.16.1.32 255.255.255.224
default-router 172.16.1.62
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN14
network 172.16.1.64 255.255.255.224
default-router 172.16.1.94
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN15
network 172.16.1.96 255.255.255.224
default-router 172.16.1.126
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN16
network 172.16.1.128 255.255.255.224
default-router 172.16.1.158
dns-server 100.0.100.200
exit
ip dhcp excluded-address 172.16.1.30
ip dhcp excluded-address 172.16.1.62
ip dhcp excluded-address 172.16.1.94
ip dhcp excluded-address 172.16.1.126
ip dhcp excluded-address 172.16.1.158
```

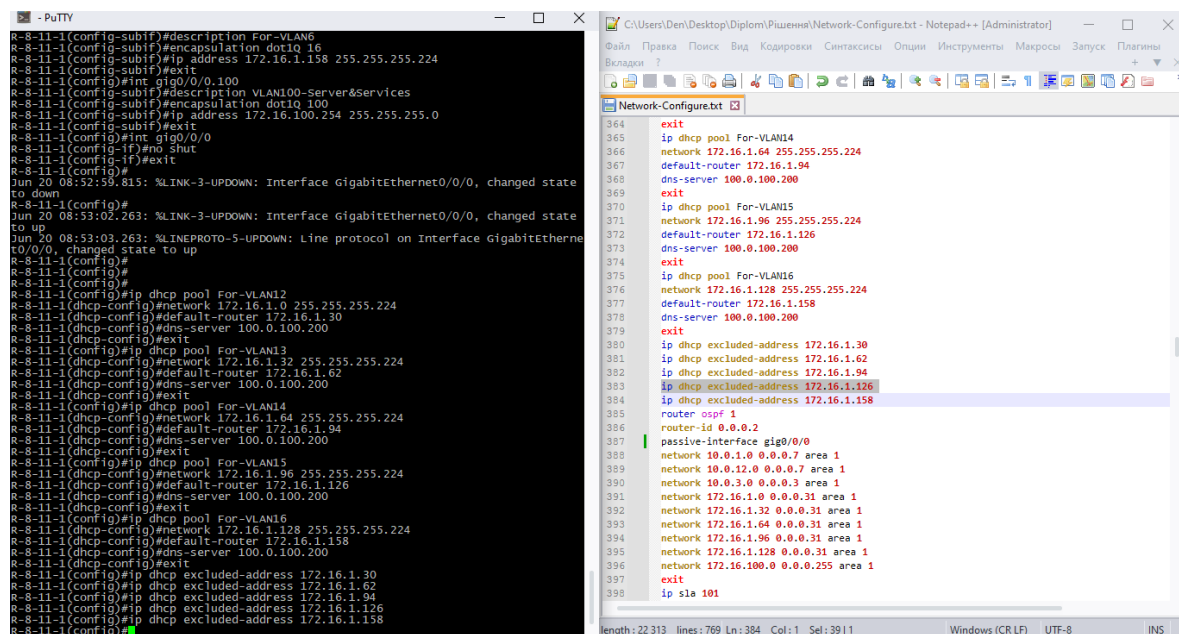


Рисунок 2.5.3.3. – Налаштування IP DHCP пулів IPv4 адресації для маршрутизатора R-8-11-1 та його локальних підмереж. Виключення деяких IP з пулу IP-адресації

Наступним кроком, виконаємо налаштування роботи протоколу динамічної маршрутизації OSPF шляхом створення процесу OSPF, додаванням ідентифікатора маршрутизатора, а також вказуванням відомих підмереж маршрутизатору. Також, було додано виключення з інтерфейсів широкомовної розсилки привітальних пакетів OSPF для інтерфейсів, що підключені до кінцевих локальних підмереж. Відповідний сценарій налаштування наведено нижче. Також, його наведено на рисунках 2.5.3.4 та 2.5.3.5.

Для R-8-11-1:

```
router ospf 1
router-id 0.0.0.2
passive-interface gig0/0/0
network 10.0.1.0 0.0.0.7 area 1
network 10.0.12.0 0.0.0.7 area 1
network 10.0.3.0 0.0.0.3 area 1
network 172.16.1.0 0.0.0.31 area 1
network 172.16.1.32 0.0.0.31 area 1
network 172.16.1.64 0.0.0.31 area 1
network 172.16.1.96 0.0.0.31 area 1
network 172.16.1.128 0.0.0.31 area 1
network 172.16.100.0 0.0.0.255 area 1
exit
```

```
to up
Jun 20 08:53:03.263: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet
to 0/0/0, changed state to up
R-8-11-1(config)#
R-8-11-1(config)#
R-8-11-1(config)#
R-8-11-1(config)#ip dhcp pool For-VLAN12
R-8-11-1(dhcp-config)#network 172.16.1.0 255.255.255.224
R-8-11-1(dhcp-config)#default-router 172.16.1.30
R-8-11-1(dhcp-config)#dns-server 100.0.100.200
R-8-11-1(dhcp-config)#exit
R-8-11-1(config)#ip dhcp pool For-VLAN13
R-8-11-1(dhcp-config)#network 172.16.1.32 255.255.255.224
R-8-11-1(dhcp-config)#default-router 172.16.1.62
R-8-11-1(dhcp-config)#dns-server 100.0.100.200
R-8-11-1(dhcp-config)#exit
R-8-11-1(config)#ip dhcp pool For-VLAN14
R-8-11-1(dhcp-config)#network 172.16.1.64 255.255.255.224
R-8-11-1(dhcp-config)#default-router 172.16.1.94
R-8-11-1(dhcp-config)#dns-server 100.0.100.200
R-8-11-1(dhcp-config)#exit
R-8-11-1(config)#ip dhcp pool For-VLAN15
R-8-11-1(dhcp-config)#network 172.16.1.96 255.255.255.224
R-8-11-1(dhcp-config)#default-router 172.16.1.126
R-8-11-1(dhcp-config)#dns-server 100.0.100.200
R-8-11-1(dhcp-config)#exit
R-8-11-1(config)#ip dhcp pool For-VLAN16
R-8-11-1(dhcp-config)#network 172.16.1.128 255.255.255.224
R-8-11-1(dhcp-config)#default-router 172.16.1.158
R-8-11-1(dhcp-config)#dns-server 100.0.100.200
R-8-11-1(dhcp-config)#exit
R-8-11-1(config)#ip dhcp excluded-address 172.16.1.30
R-8-11-1(config)#ip dhcp excluded-address 172.16.1.62
R-8-11-1(config)#ip dhcp excluded-address 172.16.1.94
R-8-11-1(config)#ip dhcp excluded-address 172.16.1.126
R-8-11-1(config)#ip dhcp excluded-address 172.16.1.158
R-8-11-1(config)#
R-8-11-1(config)#
R-8-11-1(config)#
R-8-11-1(config)#router ospf 1
R-8-11-1(config-router)#router-id 0.0.0.2
R-8-11-1(config-router)#passive-interface gig0/0/0
R-8-11-1(config-router)#network 10.0.1.0 0.0.0.7 area 1
R-8-11-1(config-router)#network 10.0.12.0 0.0.0.7 area 1
R-8-11-1(config-router)#network 10.0.3.0 0.0.0.3 area 1
R-8-11-1(config-router)#network 172.16.1.0 0.0.0.31 area 1
R-8-11-1(config-router)#network 172.16.1.32 0.0.0.31 area 1
R-8-11-1(config-router)#network 172.16.1.64 0.0.0.31 area 1
R-8-11-1(config-router)#network 172.16.1.96 0.0.0.31 area 1
R-8-11-1(config-router)#network 172.16.1.128 0.0.0.31 area 1
R-8-11-1(config-router)#network 172.16.100.0 0.0.0.255 area 1
R-8-11-1(config-router)#exit
R-8-11-1(config)#
```

```
ip dhcp pool For-VLAN15
network 172.16.1.96 255.255.255.224
default-router 172.16.1.126
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN16
network 172.16.1.128 255.255.255.224
default-router 172.16.1.158
dns-server 100.0.100.200
exit
ip dhcp excluded-address 172.16.1.30
ip dhcp excluded-address 172.16.1.62
ip dhcp excluded-address 172.16.1.94
ip dhcp excluded-address 172.16.1.126
ip dhcp excluded-address 172.16.1.158
Router ospf 1
router-id 0.0.0.2
passive-interface gig0/0/0
network 10.0.1.0 0.0.0.7 area 1
network 10.0.12.0 0.0.0.7 area 1
network 10.0.3.0 0.0.0.3 area 1
network 172.16.1.0 0.0.0.31 area 1
network 172.16.1.32 0.0.0.31 area 1
network 172.16.1.64 0.0.0.31 area 1
network 172.16.1.96 0.0.0.31 area 1
network 172.16.1.128 0.0.0.31 area 1
network 172.16.100.0 0.0.0.255 area 1
exit
ip sla 101
icmp-echo 10.0.1.1
frequency 5
exit
ip sla schedule 101 life forever start-time now
track 101 ip sla 101 reachability
exit
```

Рисунок 2.5.3.4. – Налагодження функціонування процесу OSPF для маршрутизатора R-8-11-1

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				101
Змн.	Арк.	№ докум.	Підпис	Дата		

Для R-8-11-2:

```
router ospf 1
router-id 0.0.0.3
network 10.0.2.0 0.0.0.7 area 1
network 10.0.12.0 0.0.0.7 area 1
network 10.0.3.0 0.0.0.3 area 1
network 172.16.2.0 0.0.0.31 area 1
network 172.16.2.32 0.0.0.31 area 1
network 172.16.2.64 0.0.0.31 area 1
network 172.16.2.96 0.0.0.31 area 1
network 172.16.2.128 0.0.0.31 area 1
exit
```

```
Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R-8-11-2
R-8-11-2(config)#int fa0/0
R-8-11-2(config-if)#description Link-for-VLAN2
R-8-11-2(config-if)#ip address 10.0.2.6 255.255.255.248
R-8-11-2(config-if)#ip ospf cost 1
R-8-11-2(config-if)#no shutdown
R-8-11-2(config-if)#exit
R-8-11-2(config)#int fa0/1
R-8-11-2(config-subif)#description Link-for-VLAN3
R-8-11-2(config-subif)#encapsulation dot1q 5
R-8-11-2(config-subif)#ip address 10.0.12.6 255.255.255.248
R-8-11-2(config-subif)#ip ospf cost 2
R-8-11-2(config-subif)#int fa0/1
R-8-11-2(config-if)#no shutdown
R-8-11-2(config-if)#exit
R-8-11-2(config)#int fa0/1/0
R-8-11-2(config-if)#description Link-to--R-8-11-1
R-8-11-2(config-if)#ip address 10.0.3.2 255.255.255.252
R-8-11-2(config-if)#ip ospf cost 4
R-8-11-2(config-if)#no shutdown
R-8-11-2(config-if)#exit
R-8-11-2(config)#
*Jun 20 13:50:50.939: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Jun 20 13:50:51.079: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Jun 20 13:50:51.183: %LINK-3-UPDOWN: Interface FastEthernet0/1/0, changed state to up
*Jun 20 13:50:51.939: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
*Jun 20 13:50:52.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
*Jun 20 13:50:52.183: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1/0, changed state to up
R-8-11-2(config)#
R-8-11-2(config)#
R-8-11-2(config)#router ospf 1
R-8-11-2(config-router)#router-id 0.0.0.3
R-8-11-2(config-router)#network 10.0.2.0 0.0.0.7 area 1
R-8-11-2(config-router)#network 10.0.12.0 0.0.0.7 area 1
R-8-11-2(config-router)#network 10.0.3.0 0.0.0.3 area 1
R-8-11-2(config-router)#network 172.16.2.0 0.0.0.31 area 1
R-8-11-2(config-router)#network 172.16.2.32 0.0.0.31 area 1
R-8-11-2(config-router)#network 172.16.2.64 0.0.0.31 area 1
R-8-11-2(config-router)#network 172.16.2.96 0.0.0.31 area 1
R-8-11-2(config-router)#network 172.16.2.128 0.0.0.31 area 1
R-8-11-2(config-router)#exit
R-8-11-2(config)#
```

```
436 description Link-for-VLAN3
437 encapsulation dot1q 5
438 ip address 10.0.12.6 255.255.255.248
439 int ospf cost 2
440 int fa0/1
441 no shutdown
442 exit
443 int fa0/1/0
444 description Link-to--R-8-11-1
445 ip address 10.0.3.2 255.255.255.252
446 ip ospf cost 4
447 no shutdown
448 exit
449
450 router ospf 1
451 router-id 0.0.0.3
452 network 10.0.2.0 0.0.0.7 area 1
453 network 10.0.12.0 0.0.0.7 area 1
454 network 10.0.3.0 0.0.0.3 area 1
455 network 172.16.2.0 0.0.0.31 area 1
456 network 172.16.2.32 0.0.0.31 area 1
457 network 172.16.2.64 0.0.0.31 area 1
458 network 172.16.2.96 0.0.0.31 area 1
459 network 172.16.2.128 0.0.0.31 area 1
460 exit
461 ip sla 101
462 icmp-echo 10.0.2.1
463 frequency 5
464 exit
465 ip sla schedule 101 life forever start-time now
466 track 101 ip sla 101 reachability
467 exit
468 ip sla 102
469 icmp-echo 10.0.12.1
470 frequency 5
471 exit
```

Рисунок 2.5.3.5. – Налагодження функціонування процесу OSPF для маршрутизатора R-8-11-2

Наступним етапом виконання налаштувань мережевих маршрутизаторів є додавання інструментів моніторингу станів каналів зв'язку з міжмережевими екранами Cisco ASA. Для цього використовуючи технологію IP SLA було додано відповідні процеси моніторингу станів. Приклади їх налаштувань наведені у сценаріях нижче. Також, процес налаштування відображено на рисунках 2.5.3.6 та 2.5.3.7.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				102
Змн.	Арк.	№ докум.	Підпис	Дата		

Для R-8-11-1:

```
ip sla 101
icmp-echo 10.0.1.1
frequency 5
exit
ip sla schedule 101 life forever start-time now
track 101 ip sla 101 reachability
exit
ip sla 102
icmp-echo 10.0.12.1
frequency 5
exit
ip sla schedule 102 life forever start-time now
track 102 ip sla 102 reachability
exit
ip sla 103
icmp-echo 10.0.2.1
frequency 5
exit
ip sla schedule 103 life forever start-time now
track 103 ip sla 103 reachability
exit
```

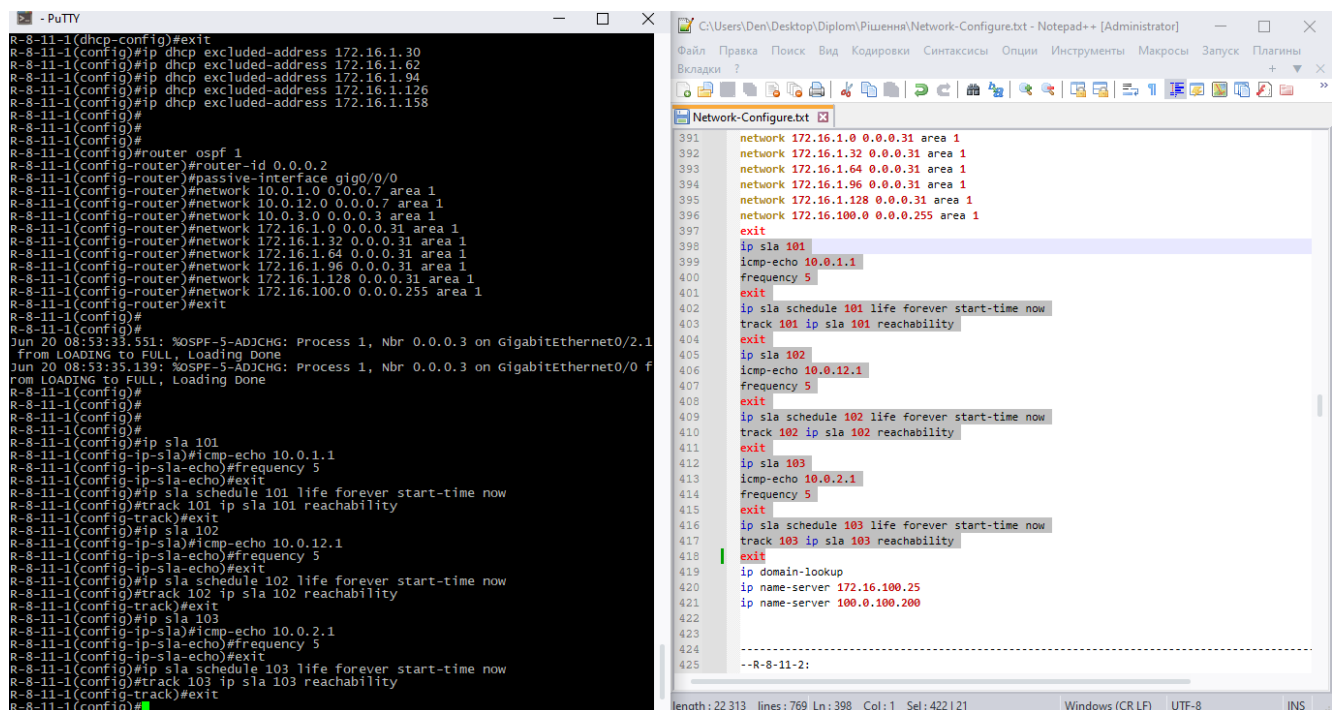


Рисунок 2.5.3.6. – Налаштування інструментів моніторингу стану доступності вузлів для маршрутизатора R-8-11-1

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефименко А.А.				103
Змн.	Арк.	№ докум.	Підпис	Дата		

Для R-8-11-2:

```
ip sla 101
icmp-echo 10.0.2.1
frequency 5
exit
ip sla schedule 101 life forever start-time now
track 101 ip sla 101 reachability
exit
ip sla 102
icmp-echo 10.0.12.1
frequency 5
exit
ip sla schedule 102 life forever start-time now
track 102 ip sla 102 reachability
exit
ip sla 103
icmp-echo 10.0.1.1
frequency 5
exit
ip sla schedule 103 life forever start-time now
track 103 ip sla 103 reachability
exit
```

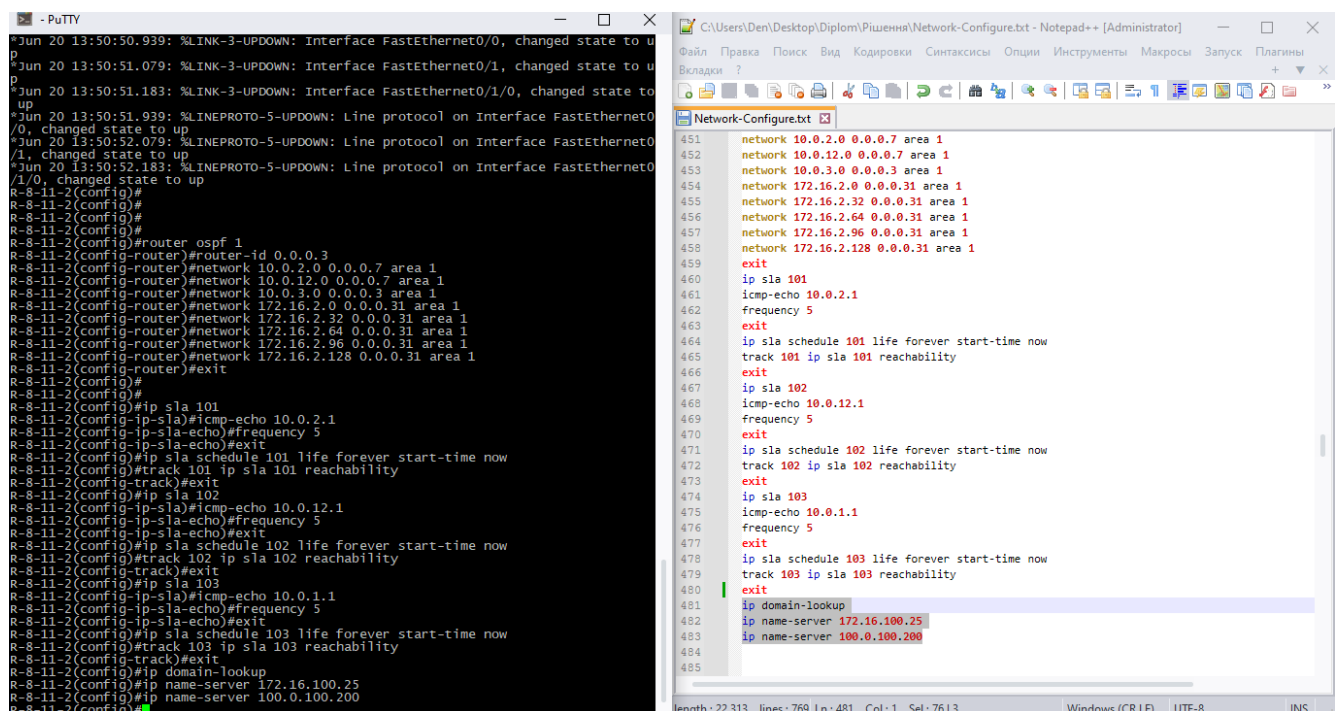


Рисунок 2.5.3.7. – Налаштування інструментів моніторингу стану доступності вузлів для маршрутизатора R-8-11-2

Наступним кроком, виконуємо налагодження засобів роботи DNS протоколу, а саме, активуємо пошук домених імен та вказуємо DNS-сервери, до яких будуть виконуватися звернення DNS-Request. Для цього виконуємо команди, що наведені

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефименко А.А.				104
Змн.	Арк.	№ докум.	Підпис	Дата		

у сценаріях налаштування. Приклади виконання даних налаштувань наведені на рисунках 2.5.3.8 та 2.5.3.9.

Для R-8-11-1:

```
ip domain-lookup
ip name-server 172.16.100.25
ip name-server 100.0.100.200
```

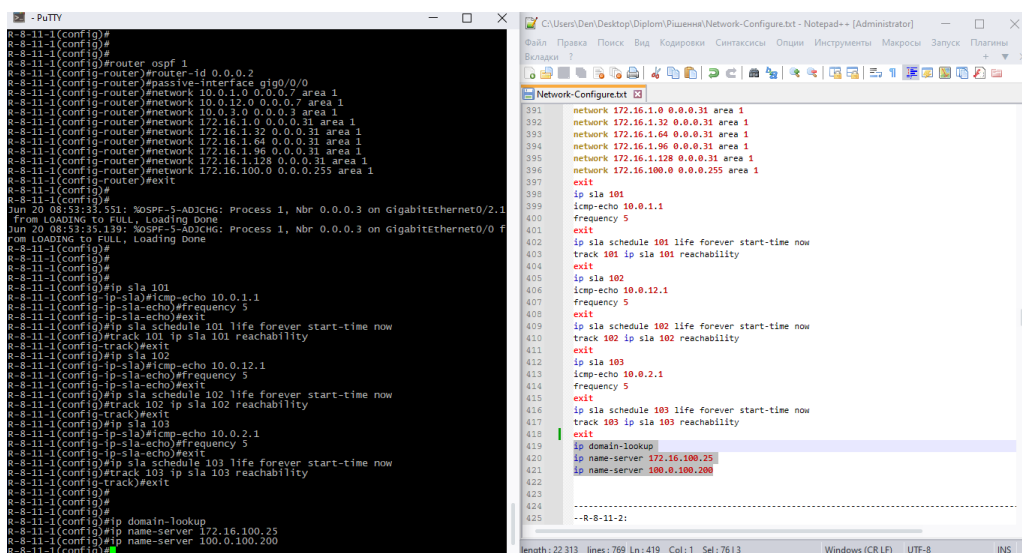


Рисунок 2.5.3.8. – Налаштування роботи DNS на маршрутизатора R-8-11-1

Для R-8-11-2:

```
ip domain-lookup
ip name-server 172.16.100.25
ip name-server 100.0.100.200
```

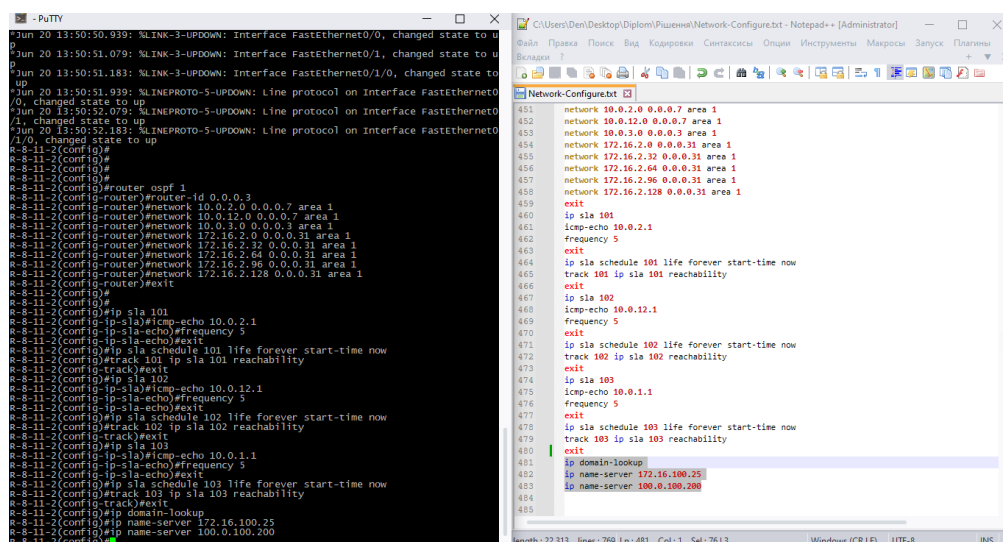


Рисунок 2.5.3.9. – Налаштування роботи DNS на маршрутизатора R-8-11-2

На цьому, виконання процесу налагодження мережевих маршрутизаторів є закінченим. Приступаємо до налагодження зовнішнього комутатора та

		Колесник Д.В.			Арк.
		Ефименко А.А.			
Змн.	Арк.	№ докум.	Підпис	Дата	105

маршрутизатора ISP-Router, що у межах реалізації даного проекту виступає у ролі імітації зовнішньої глобальної мережі інтернет провайдера.

2.5.4. Налаштування імітації глобальної мережі інтернет.

Виконуємо налаштування зовнішнього комутатора. Загалом, у зв'язку з тим, що реалізація проекту виконується на основі дещо спрощеного варіанту побудови фізичної топології, то такий крок налаштування є необхідним, щоб створити імітацію наявності двох підмереж провайдера, що підключаються до міжмережевого екрану Cisco ASA. За звичайних умов, даний комутатор не потребує налаштувань, так як забезпечує лише комутацію двох Cisco ASA до підмережі провайдера. Відповідно до наших потреб, було виконано створення двох підмереж VLAN, а саме VLAN 10 та VLAN 20, для імітації роботи двох підмереж провайдера, створено та налагоджено відповідні транкові підключення між мережевими екранами Cisco ASA та маршрутизатором ISP-Router, відповідно до топології, а також для зручності виконання подальшої діагностики та тестування, створено та присвоєно параметри IPv4 адресації для VLAN інтерфейсів комутатора та додано два інтерфейси для VLAN 10 та VLAN 20, що призначені для подальшої можливості підключення деякого вузла, що імітуватиме підключення з глобальної мережі. Усі ці налаштування виконуються на основі нижче наведеного сценарію налаштування. Приклад виконання такого налаштування наведено на рисунку 2.5.4.1.

Для Outside-Switch:

```
en
conf t
hostname Outside-Switch
vlan 10
name Net-ISP1
exit
vlan 20
name Net-ISP2
exit
vlan 100
name Global-Net
exit
```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		106

```

int fa0/1
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20
no shut
exit
int range fa0/23-24
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 10,20
no shut
exit
int fa0/2
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk allowed vlan 100
no shut
exit
int fa0/3
switchport mode access
switchport access vlan 10
no shut
exit
int fa0/4
switchport mode access
switchport access vlan 20
no shut
exit
int vlan 10
ip address 109.251.250.64 255.255.255.128
no shut
exit
int vlan 20
ip address 109.251.250.200 255.255.255.128
no shut
exit

```

Рисунок 2.5.4.1. – Налаштування комутатора Outside-Switch

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				107
Змн.	Арк.	№ докум.	Підпис	Дата		

Наступним кроком, виконуємо налаштування імітації роботи маршрутизатора інтернет провайдера. Загалом, за звичайних умов, виконання даної частини налаштувань не потребується. Відповідно до наведених у сценарії нижче налаштувань, було виконано створення двох підінтерфейсів, що імітуватимуть роботу двох підмереж провайдерів, виконано налаштування параметрів IP-адресації на основі протоколу DHCP для деякого мережевого інтерфейсу маршрутизатора, що підключається до локальної мережі університету, а також виконано налаштування засобів роботи NAT у режимі Overload, з метою інформаційного обміну у локальній підмережі університету. Приклад виконання відповідного налаштування також наведено на рисунку 2.5.4.2.

Для ISP-Router:

```

en
conf t
hostname ISP-Router
int f0/1.2
encapsulation dot1Q 10
ip address 109.251.250.126 255.255.255.128
exit
int f0/1.3
encapsulation dot1Q 20
ip address 109.251.250.254 255.255.255.128
exit
int fa0/1
no shut
exit
int fa0/0
ip address dhcp
no shut
exit
ip domain-lookup
int f0/1.2
ip nat inside
exit
int f0/1.3
ip nat inside
exit
int fa0/1
ip nat inside
exit
int fa0/0
ip nat outside
exit
access-list 10 permit any
ip nat inside source list 10 interface FastEthernet0/0 overload

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		108

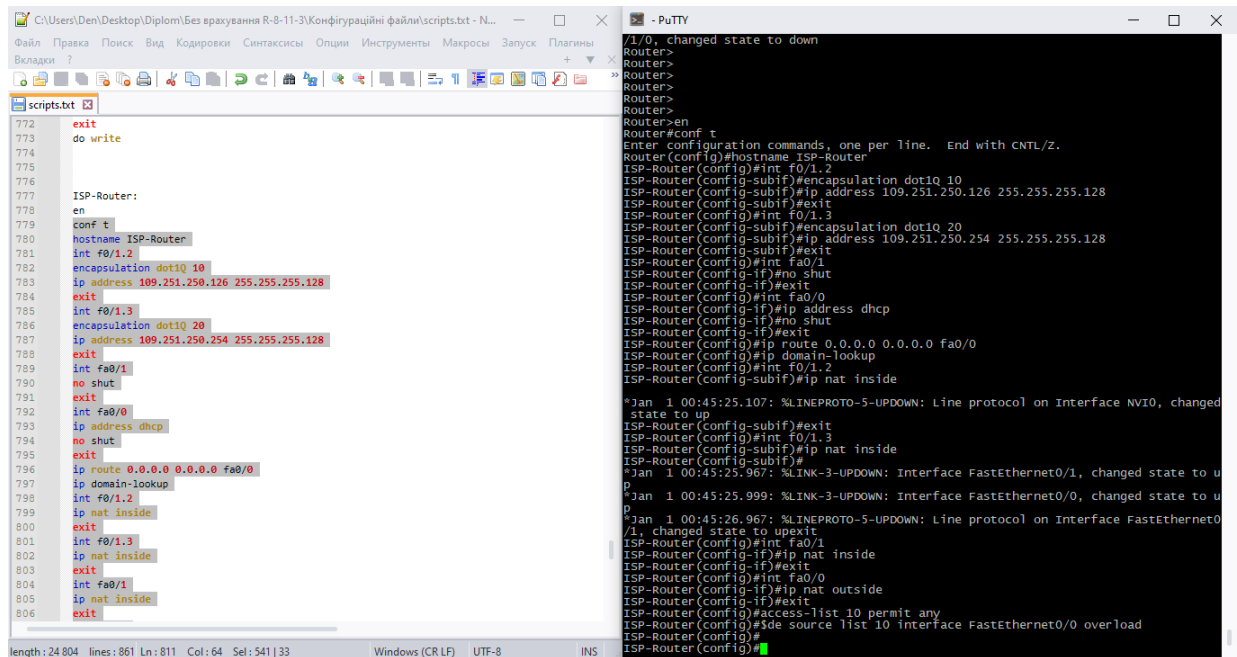


Рисунок 2.5.4.2. – Налаштування маршрутизатора ISP-Router

Таким чином, виконання налаштувань мережевого обладнання, що покликане забезпечити імітацію інтернет підключення є закінченим.

На цьому, виконання процес налаштування тестового стенду є закінченим, тому переходимо до етапу детального тестування проекту високонадійного захищеного мультипровайдерного Інтернет-підключення кампусної мережі організації.

2.6. Тестування проекту.

Переходимо до етапу тестування пробудованого проекту комп'ютерної мережі. В межах виконання даної частини роботи, проведемо перевірку працездатності усіх спроектованих нами функцій, налагоджений протоколів та засобів маршрутизації мережевого трафіку, а також проведемо перевірку роботи засобів фільтрації мережевого трафіку.

В першу чергу, виконання тестувань роботи проекту комп'ютерної мережі базувалися на основі застосування діагностичних команд роботи мережевого обладнання, що базувалося на основі мережної операційної системи Cisco IOS. Перейдемо до огляду саме тих команд, які активно використовувалися під час виконання діагностики роботи мережевого обладнання, а також саме тих команд, що

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефименко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		109

неодноразово застосувалися для діагностування роботи мережі та оперативного внесення змін у її роботу та параметри налаштувань.

Основною діагностичною командою, що неоднократно використовувалася під час тестування роботи комп'ютерної мережі є діагностична команда – «show failover». Ця команда відображає поточний стан роботи технології Cisco Failover на одному з вузлів, де її застосовано. Вона також відображає відомості про стани інтерфейсів, на яких було налагоджено моніторинг для відпрацьовування роботи даної технології у разі виходу з ладу деяких каналів зв'язу, параметри IP-адресації, найменування інтерфейсів та їх стан моніторингу, як для основного, так і для резервного вузлів, надає інформацію про стан сесій і з'єднань, що синхронізуються між активним та резервним пристроєм, а також іншу діагностичну інформацію. Приклад роботи даної діагностичної команди на активному вузлі Cisco ASA Failover наведено на рисунку 2.6.1, що наведено нижче.

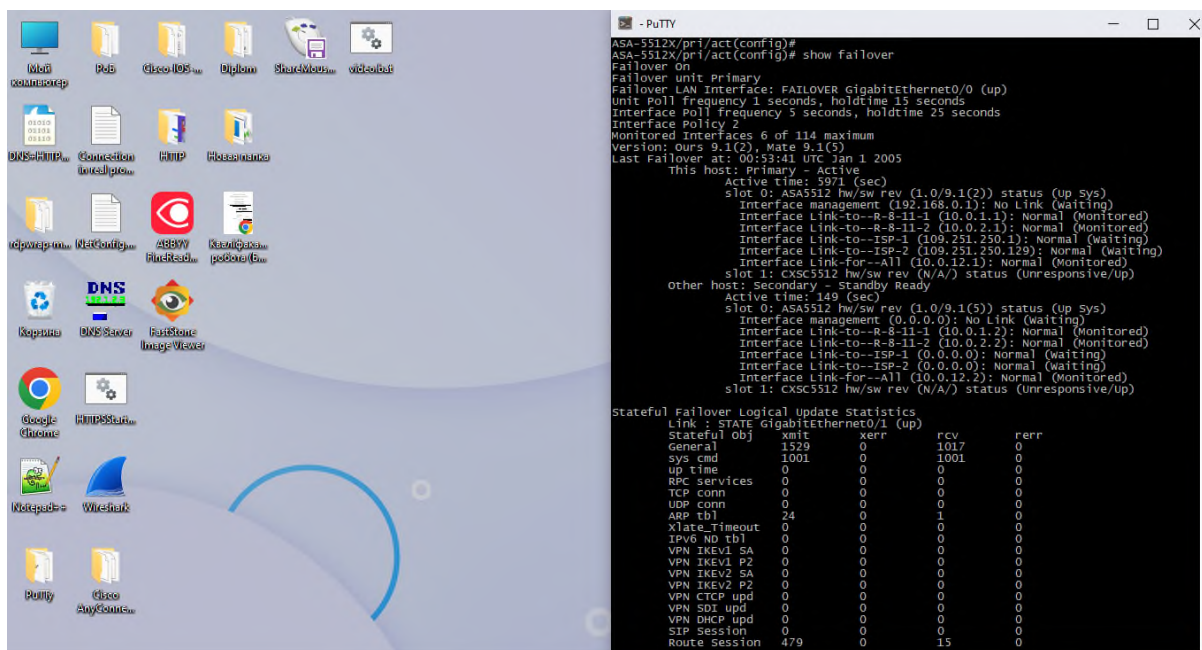


Рисунок 2.6.1. – Приклад виводу діагностичної команди «show failover»

Важливо відзначити, що використовуючи активний вузол Cisco ASA Failover з застосування діагностичної команди «failover exec mate show failover» можна також вивести діагностичні відомості про роботу Failover на резервному вузлі. Приклад наведено на рисунку нижче.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		110

Для зручності виконання діагностики роботи комп'ютерної мережі також було реалізовано зручний інструмент моніторингу станів мережевих вузлів, котрий використовується не лише як діагностичний інструмент, але й як інструмент керування шлюзом за замовчування до однієї з підмереж інтернет провайдерів. Так використовуючи діагностичну команду *«show track»* можна отримати відомості про події відслідковування станів мережевих вузлів, робота яких виконується на основі технології IP SLA. Використовуючи дану команду можна отримати відомості про події відслідковування, у яких зазначається тип відслідковування, у нашому випадку це доступність (reachability), стан події відслідковування (активна, або up, та неактивна, down), час фіксування останньої зміни, а також затримка каналу зв'язку. Приклад використання даної діагностичної команди наведено на рисунку 2.6.2 нижче.

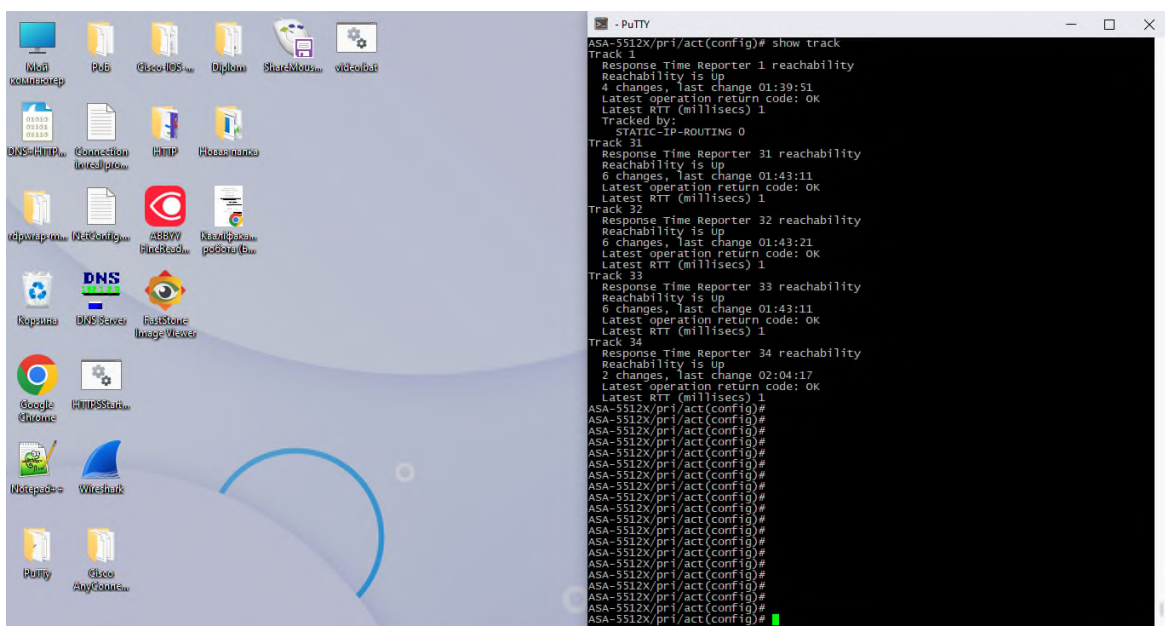


Рисунок 2.6.2. – Приклад виводу діагностичної команди *«show track»*

Наступною важливою діагностичною командою, про яку однозначно варто відзначити є команда *«show ip route»*, або *«show route»*. Ця команда відіграє важливу роль у виконання коректних відлагоджувальних робіт, що проводилися під час проектування роботи комп'ютерної мережі. Діагностична команда *«show ip route»*, або *«show route»* відображає поточні таблиці маршрутизації на мережевому обладнанні, що у роботі представлені у вигляді двох маршрутизаторів та

міжмережевого екрану, що у нашому випадку працює у режимі маршрутизатора мережевого трафіку. Як зазначалося вище, команда відображає інформацію про таблицю маршрутизації, у якій відзначаються усі наявні маршрути для маршрутизації мережевого трафіку до тих чи інших підмереж. Інформація про маршрут надається у вигляді: Тип запису, IP-адреса мережі та маска підмережі, назва інтерфейсу маршрутизації трафіку, а також IP-адреса наступного переходу. Додатково наявна інформація про метрику до підмережі, якщо це протоколи динамічної маршрутизації, для яких метрика є важливим параметром формування маршрутів, а також час останньої зміни маршруту. Приклад роботи даної діагностичної команди наведено на рисунку 2.6.3, що зображено нижче.

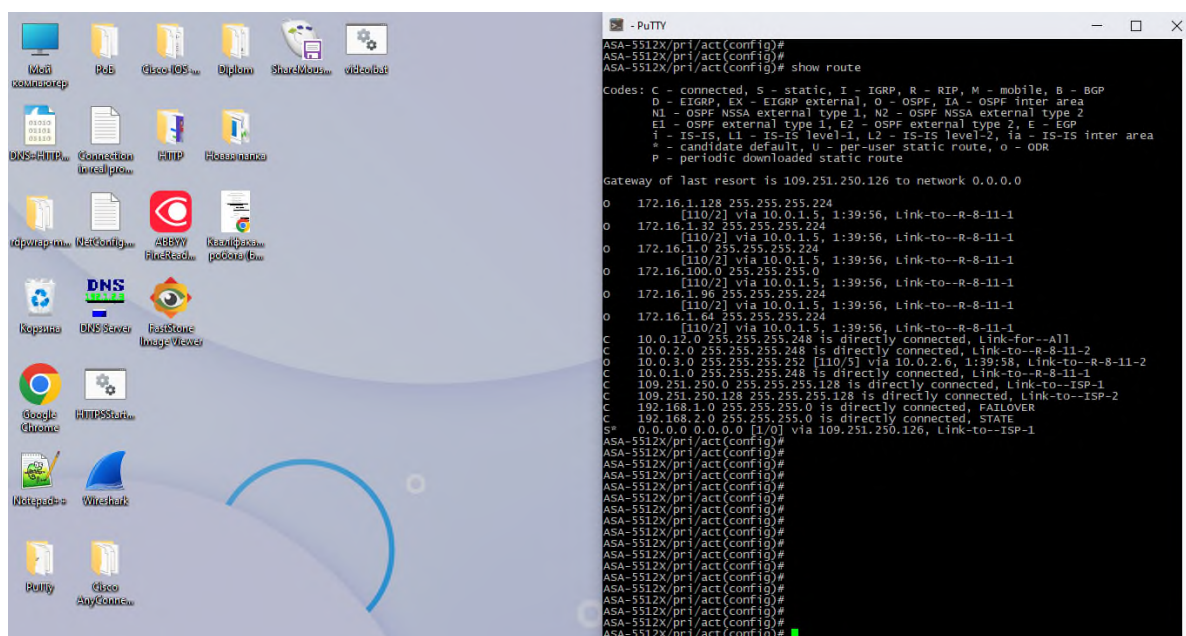


Рисунок 2.6.3. – Приклад виводу діагностичної команди «show route»

В ході виконання розробки проекту комп'ютерної мережі, дана діагностична команда допомогла виявити велику кількість проблем під час виконання спроб реалізації роботи протоколу OSPF різними способами та на основі різних топологій комп'ютерної мережі, у межах реалізації даного проекту. Деякі з прикладів наведені на рисунках 2.6.4 та 2.6.5 нижче.

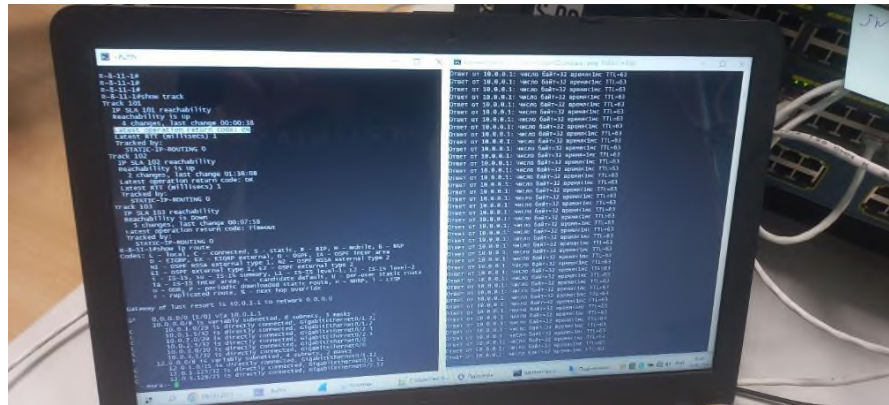


Рисунок 2.6.4. – Приклад діагностичного застосування команди «show route» та «show track» під час діагностики роботи комп'ютерної мережі та правил маршрутизації мережевого трафіку

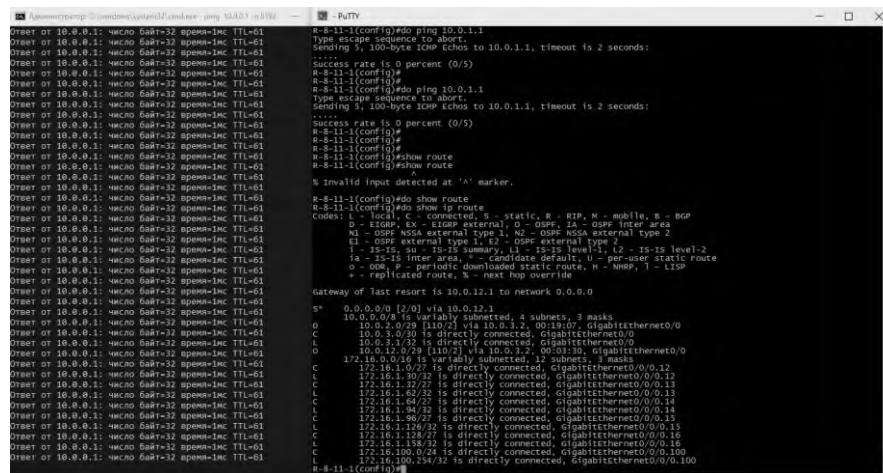


Рисунок 2.6.5. – Приклад застосування команди «show route» під час тестування відмовостійкості

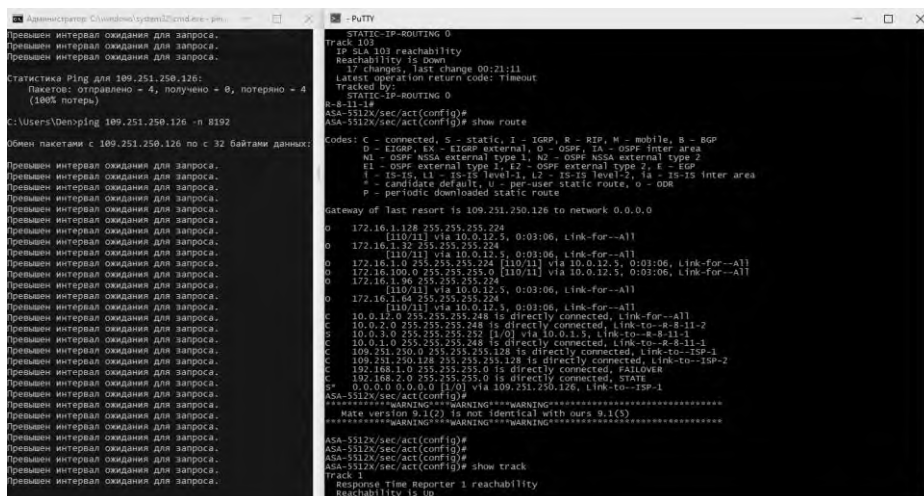


Рисунок 2.6.6. – Приклад застосування команди «show route» під час спроб виявлення причини відсутності зв'язку

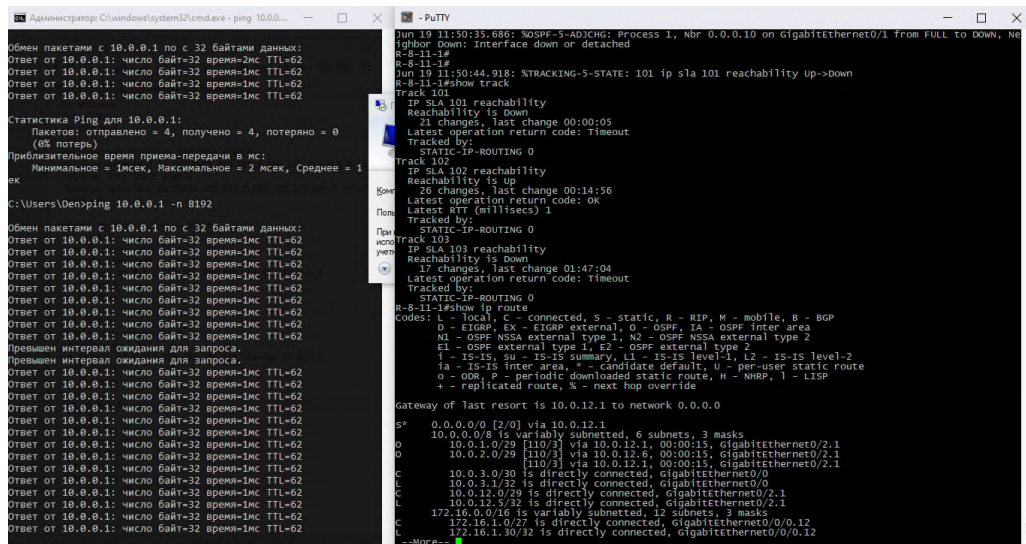


Рисунок 2.6.7. – Приклад застосування команди «*show route*» під час тестування відмовостійкості з глобальною мережею інтернет

Наступною важливою діагностичною командою є команда моніторингу сусідів протоколу OSPF, котрий у межах даної роботи є одним з важливіших протоколів та технологій, що покликані забезпечити високий рівень надійності та відмовостійкості проекту комп'ютерної мережі. Цією командою є «*show ip ospf neighbor*», або «*show ospf neighbor*». Ця команда покликана надати інформацію про наявні сусідства з іними маршрутизаторами, що також є учасниками роботи протоколу OSPF. Дана команда надає відомості про ідентифікатор маршрутизатора, так званий Router ID, пріоритет маршрутизатора, статус маршрутизатора у протоколі OSPF, час виконання повторної спроби перевірки на доступність OSPF, надсилання пакетів «*Hello*» даного протоколу після чого виконання поновлення сусідства чи видалення, IP-адресу інтерфейса на якому було виявлено даного сусіда, а також назву інтерфесу. Відображення цієї інформації дозволяє відобразити які сусідства були виявлені тим чи іншим мережевим вузлом, а так за якими адресами та інтерфейсами, що стає важливим під час побудови високонадійних проектів комп'ютерних мереж, так як на основі цієї інформації можливо виконати діагностування та моделювання потенційних записів маршрутизації, що можуть бути сформованими та доданими в таблиці маршрутизації. Приклад роботи даної команди наведено на рисунку 2.6.8 нижче.

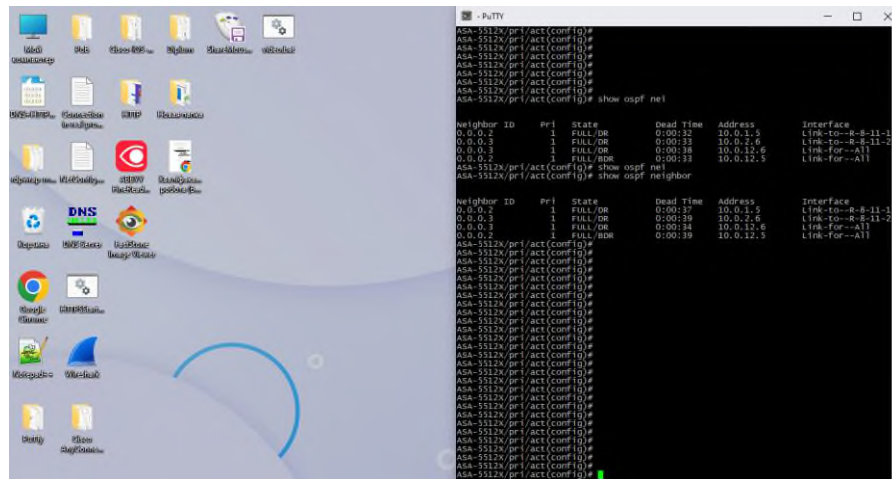


Рисунок 2.6.8. – Приклад застосування команди «*show ospf neighbor*»

Наступна діагностична команда, інформація в результаті якої є дуже корисною під час виконання діагностики роботи комп'ютерної мережі є команда відображення трансляцій NAT. В межах даної роботи, та й взагалі в будь-якій сучасній комп'ютерній мережі, технологія NAT використовується для трансляції внутрішньої, тобто локальної IP-адрес, в деяку глобальну мережу, що використовується для маршрутизації мережевого трафіку в середині глобальної мережі Інтернет. Так команда «*show nat translation interface <назва інтерфейсу> detail*» відображає інформацію про наявні записи трансляції NAT з тих чи інших інтерфейсів в інтерфейси доступу до глобальної мережі, а також відображає кількість мережевого трафіку, що був таким чином трансльований, або трафік, що було відкинуто. Приклад роботи даної команди для двох зовнішніх інтерфейсів наведено на рисунках 2.6.9 та 2.6.10 нижче.

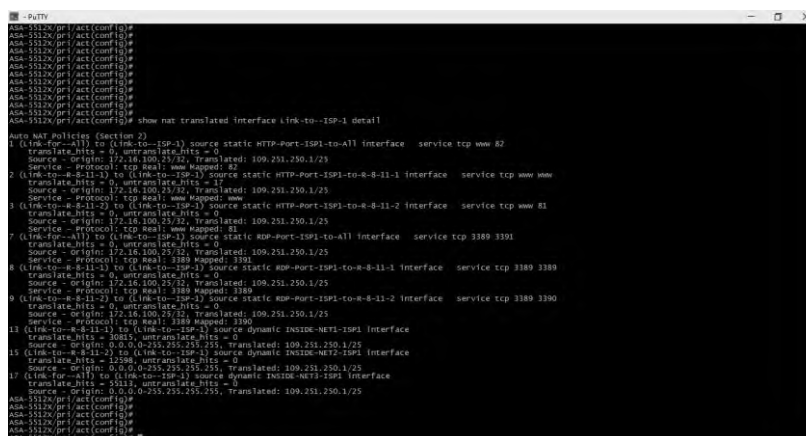


Рисунок 2.6.9. – Приклад застосування діагностичної команди «*show nat translation interface Link-to--ISP-1 detail*»

		Колесник Д.В.			Арк.
		Ефіменко А.А.			115
Змн.	Арк.	№ докум.	Підпис	Дата	

```
- PuTTY
translate_hits = 30815, untranslate_hits = 0
source - Origin: 0.0.0.0-255.255.255.255, Translated: 109.251.250.1/25
19 (Link-to--R-8-11-2) to (Link-to--ISP-1) source dynamic INSIDE-NET2-ISP1 interface
translate_hits = 12598, untranslate_hits = 0
source - Origin: 0.0.0.0-255.255.255.255, Translated: 109.251.250.1/25
17 (Link-For--All) to (Link-to--ISP-1) source dynamic INSIDE-NET3-ISP1 interface
translate_hits = 55113, untranslate_hits = 0
source - Origin: 0.0.0.0-255.255.255.255, Translated: 109.251.250.1/25
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)# show nat translated interface Link-to--ISP-2 detail
Auto NAT Policies (Section 2)
4 (Link-For--All) to (Link-to--ISP-2) source static HTTP-Port-ISP2-to-All interface service tcp www 82
translate_hits = 0, untranslate_hits = 0
source - Origin: 172.16.100.25/32, Translated: 109.251.250.129/25
service - Protocol: tcp Real: www Mapped: 82
5 (Link-to--R-8-11-1) to (Link-to--ISP-2) source static HTTP-Port-ISP2-to-R-8-11-1 interface service tcp www www
translate_hits = 0, untranslate_hits = 5
source - Origin: 172.16.100.25/32, Translated: 109.251.250.129/25
service - Protocol: tcp Real: www Mapped: www
6 (Link-to--R-8-11-2) to (Link-to--ISP-2) source static HTTP-Port-ISP2-to-R-8-11-2 interface service tcp www 81
translate_hits = 0, untranslate_hits = 0
source - Origin: 172.16.100.25/32, Translated: 109.251.250.129/25
service - Protocol: tcp Real: www Mapped: 81
10 (Link-For--All) to (Link-to--ISP-2) source static RDP-Port-ISP2-to-All interface service tcp 3389 3391
translate_hits = 0, untranslate_hits = 0
source - Origin: 172.16.100.25/32, Translated: 109.251.250.129/25
service - Protocol: tcp Real: 3389 Mapped: 3391
11 (Link-to--R-8-11-1) to (Link-to--ISP-2) source static RDP-Port-ISP2-to-R-8-11-1 interface service tcp 3389 3389
translate_hits = 0, untranslate_hits = 0
source - Origin: 172.16.100.25/32, Translated: 109.251.250.129/25
service - Protocol: tcp Real: 3389 Mapped: 3389
12 (Link-to--R-8-11-2) to (Link-to--ISP-2) source static RDP-Port-ISP2-to-R-8-11-2 interface service tcp 3389 3390
translate_hits = 0, untranslate_hits = 0
source - Origin: 172.16.100.25/32, Translated: 109.251.250.129/25
service - Protocol: tcp Real: 3389 Mapped: 3390
14 (Link-to--R-8-11-3) to (Link-to--ISP-2) source dynamic INSIDE-NET1-ISP2 interface
translate_hits = 0, untranslate_hits = 0
source - Origin: 0.0.0.0-255.255.255.255, Translated: 109.251.250.129/25
16 (Link-to--R-8-11-2) to (Link-to--ISP-2) source dynamic INSIDE-NET2-ISP2 interface
translate_hits = 0, untranslate_hits = 0
source - Origin: 0.0.0.0-255.255.255.255, Translated: 109.251.250.129/25
18 (Link-For--All) to (Link-to--ISP-2) source dynamic INSIDE-NET3-ISP2 interface
translate_hits = 0, untranslate_hits = 0
source - Origin: 0.0.0.0-255.255.255.255, Translated: 109.251.250.129/25
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
```

Рисунок 2.6.10. – Приклад застосування діагностичної команди «*show nat translation interface Link-to--ISP-2 detail*»

Дана команда використовувалася для перевірки роботи засобів трансляції під час спроб обміну даними у глобальній мережі інтернет, так і для трафіку, що мав бути переадресований з глобальної мережі до локального сервера, котрий має бути доступним у глобальній мережі інтернет.

Наступною важливою діагностичною командою є команда «*show access-list <ім'я>*». Ця команда покликана надати інформацію про списки контролю доступу, що можуть бути відлагодженими для додавання або віднімання тих чи інших записів, що впливають на роботу комп'ютерної мережі в цілому. Дана команда неодноразово використовувалася під час роботи зі списками контролю доступу, що були покликаними заблокувати доступ до тих чи інших глобальних ресурсів на основі їх FQDN. Приклад роботи даної команди наведено на рисунках нижче.

```
- PuTTY
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)# show acc
ASA-5512X/pr1/act(config)# show access-list Network-Services
access-list Network-Services: 10 elements; name hash: 0xd3af255f
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224 object-group block-access log informational interval 300 (hitcnt=0) 0x8630e503
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224 fqdn facebook.com (unresolved) log informational interval 300 (inactive) 0x46dd79bb
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224 fqdn youtube.com (unresolved) log informational interval 300 (inactive) 0xb3f857c1
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224 fqdn viber.com (unresolved) log informational interval 300 (inactive) 0x17fc9735
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224 object-group block-access log informational interval 300 (hitcnt=0) 0x36120d10
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224 fqdn facebook.com (unresolved) log informational interval 300 (inactive) 0xd4b0090b
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224 fqdn youtube.com (unresolved) log informational interval 300 (inactive) 0x9b344508
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224 fqdn viber.com (unresolved) log informational interval 300 (inactive) 0x62871c3f
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224 object-group block-access log informational interval 300 (hitcnt=0) 0xd06a18ef
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224 fqdn facebook.com (unresolved) log informational interval 300 (inactive) 0x211d6b86
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224 fqdn youtube.com (unresolved) log informational interval 300 (inactive) 0x01d36d0e
access-list Network-Services line 4 extended permit ip any any (hitcnt=98326) 0xad98f099
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
ASA-5512X/pr1/act(config)#
```

Рисунок 2.6.11. – Приклад застосування діагностичної команди «*show access-list Network-Services*»

```

access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224
fgdn facebook.com (resolved) log informational interval 300 0xd4b009b
<--- More --->
*****WARNING*****WARNING*****WARNING*****
*****WARNING*****WARNING*****WARNING*****
*****WARNING*****WARNING*****WARNING*****
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224
fgdn youtube.com (unresolved) log informational interval 300 (inactive) 0x9b344508
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224
host 100.0.100.98 (facebook.com) log informational interval 300 (hitcnt=0) 0xa6e2c7c7
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224
host 100.0.100.65 (viber.com) log informational interval 300 (hitcnt=0) 0xc82c1dcc
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224
fgdn facebook.com (resolved) log informational interval 300 0x21d6b86
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224
fgdn youtube.com (unresolved) log informational interval 300 (inactive) 0x01d36d0e
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224
fgdn viber.com (resolved) log informational interval 300 0xc9dadd0
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224
host 100.0.100.98 (facebook.com) log informational interval 300 (hitcnt=0) 0xbe715221
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224
host 100.0.100.65 (viber.com) log informational interval 300 (hitcnt=0) 0x53a4a63e
access-list Network-Services line 4 extended permit ip any any (hitcnt=1059) 0xada940d9
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)# show access-list Network-Services
access-list Network-Services: 16 elements; name hash: 0xd3af255f
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224
object-group block-access log informational interval 300 (hitcnt=0) 0x8630e503
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224
fgdn facebook.com (resolved) log informational interval 300 0x46dd79bb
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224
fgdn youtube.com (unresolved) log informational interval 300 (inactive) 0xb5f857c1
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224
fgdn viber.com (resolved) log informational interval 300 0xd7f9735
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224
host 100.0.100.98 (facebook.com) log informational interval 300 (hitcnt=0) 0x583ed7b0
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224
host 100.0.100.65 (viber.com) log informational interval 300 (hitcnt=0) 0xb389b7de
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224
object-group block-access log informational interval 300 (hitcnt=0) 0x36120d10
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224
fgdn facebook.com (resolved) log informational interval 300 0xd06a18ef
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224
fgdn youtube.com (unresolved) log informational interval 300 (inactive) 0x9b344508
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224
fgdn viber.com (resolved) log informational interval 300 0x62871c3f
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224
host 100.0.100.98 (facebook.com) log informational interval 300 (hitcnt=0) 0xa6e2c7c7
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224
host 100.0.100.65 (viber.com) log informational interval 300 (hitcnt=0) 0xc82c1dcc
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224
fgdn facebook.com (resolved) log informational interval 300 0x21d6b86
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224
fgdn youtube.com (unresolved) log informational interval 300 (inactive) 0x01d36d0e
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224
fgdn viber.com (resolved) log informational interval 300 0xc9dadd0
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224
host 100.0.100.98 (facebook.com) log informational interval 300 (hitcnt=0) 0xbe715221
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224
host 100.0.100.65 (viber.com) log informational interval 300 (hitcnt=0) 0x53a4a63e
access-list Network-Services line 4 extended permit ip any any (hitcnt=1059) 0xada940d9
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#

```

Рисунок 2.6.12. – Приклад застосування діагностичної команди «show access-list Network-Services» з наявним DNS сервером у комп’ютерній мережі тестового стенду

На рисунках 2.6.11 та 2.6.12 продемонстровано розширений список контролю доступу під назвою «Network-Services», що покликаний забезпечити фільтрацію та контролю доступу до ресурсів глобальної мережі інтернет для користувачів деяких локальних підмереж. Список побудований на основі додавання заборон на відвідування тих чи інших ресурсів, де визначено лише заборони. Усі інші ресурси у даному списку контролю доступу є дозволеними. Список працює у динамічному режимі роботи, тобто автоматично додає IP-адреси тих чи інших доменів, що були отримані у результаті запиту DNS-Request.

Мережева операційна система міжмережевого екрану оснащена дуже потужним програмним засобом, що покликаний проводити глибоке тестування роботи міжмережевого екрану та його правил фільтрації мережевого трафіку. Даною утилітою є «Packet Tracer», про який буде відзначено далі. Вона дозволяє симулювати проходження пакета через Cisco ASA і аналізувати, як різні налаштування та правила впливають на обробку пакета. Це корисно для розуміння того, чому певний трафік блокується або дозволяється. В ході виконання даної роботи, дана команда неодноразово дозволяла зрозуміти правила, що забороняють проходження

мережевого трафіку у комп'ютерній мережі, наприклад під час роботи засобів NAT трансляції у глобальну мережу. Приклад наведено нижче (рис. 2.6.13).

```

ASA-5512X/pri/act(config)# $--ISP-1 icmp 109.251.250.1 8 0 172.16.1.1 de
ASA-5512X/pri/act(config)# packet-tracer input Link-to--ISP-1 icmp 109.251.2505

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
  in id=0x7fff9fbd7d0, priority=1, domain=permit, deny=False
  hits=251046, user_data=0x0, cs_id=0x0, l3_type=0x8
  src mac=0000.0000.0000, mask=0000.0000.0000
  dst mac=0000.0000.0000, mask=0100.0000.0000
  input_ifc=Link-to--ISP-1, output_ifc=any

Phase: 2
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
  in 172.16.1.0 255.255.255.224 Link-For-VLAN3

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
  in id=0x7fff9fbf6750, priority=500, domain=permit, deny=true
  hits=0, user_data=0x6, cs_id=0x0, reverse, flags=0x0, protocol=0
  src ip/id=109.251.250.1, mask=255.255.255.255, port=0, tag=0
  dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
  input_ifc=Link-to--ISP-1, output_ifc=any

Result:
input-interface: Link-to--ISP-1
input-status: up
input-line-status: up
output-interface: Link-For-VLAN3
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule

ASA-5512X/pri/act(config)#
*****WARNING*****WARNING*****WARNING*****
Mate version 9.1(3) is not identical with ours 9.1(2)
*****WARNING*****WARNING*****WARNING*****

```

Рисунок 2.6.13. – Приклад застосування діагностичної команди «*packet-tracer*» з метою виявлення причини блокування мережевого трафіку у глобальну мережу інтернет для деякого вузла

Використання даної утиліти також дозволило провести відлагоджувальні роботи під час тестування засобів трансляції деякого зовнішнього мережевого трафіку до підмережі локальних серверів, в особливості до мережевого сервера, який, як зазначалося раніше, має бути доступним у глобальній мережі для роботи тих чи інших сервісів. Так, до прикладу, дана команда дозволила провести відлагодження роботи правил трансляції NAT, а також запевнитися у їх коректному налаштуванні та роботі з точки зору правил фільтрації мережевого трафіку. Далі, наведено приклад роботи команди «*packet-tracer input Link-to--ISP-1 tcp 10.54.68.12 3389 109.251.250.1 3389 detail*», результати роботи якої демонструє спробу отримання доступу за протоколом RDP для деякого віддаленого вузла 10.54.68.12, що розташований у глобальній мережі інтернет, до інтерфейсу Cisco ASA, що має IP адресу 109.251.250.1 на основі порту доступу 3389, що є стандартним для даного протоколу. Формування результату виконується на основі кількох етапів перевірки

правил, що наведені у виводі у вигляді «Фаз/Етапів» з тим чи іншим порядковим номером. Відповідні приклади додано у вигляді рисунків 2.6.14 – 2.6.17.

```

ASA-5512X/pr1/act(config)# $89 109.251.250.1 3389 detailed
ASA-5512X/pr1/act(config)# $89 109.251.250.1 3389 detailed
ASA-5512X/pr1/act(config)# $89 109.251.250.1 3389 detailed
ASA-5512X/pr1/act(config)# packet-tracer input Link-to--ISP-1 tcp 10.54.68.12 $

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
  in id=0x7fff9b9de0, priority=1, domain=permit, deny=false
    hits=100055, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0100.0000.0000
    input_ifc=Link-to--ISP-1, output_ifc=any

Phase: 2
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network RDP-Port-ISP1-to-R-8-11-1
 nat (Link-to--R-8-11-1,Link-to--ISP-1) static interface service tcp 3389 3389
Additional Information:
NAT divert to egress interface Link-to--R-8-11-1
untranslate 109.251.250.1/3389 to 172.16.100.25/3389

Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group Ports-Forwarding-ISP1 in interface Link-to--ISP-1
access-list Ports-Forwarding-ISP1 extended permit tcp any object RDP-Port-ISP1-to-R-8-11-1 eq 3389
Additional Information:
Forward Flow based lookup yields rule:
  in id=0x7fff9fea7b10, priority=13, domain=permit, deny=false
    hits=0, user_data=0x7fff9b9e1400, cs_id=0x0, use_real_addr, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
    dst ip/id=172.16.100.25, mask=255.255.255.255, port=3389, tag=0, dscp=0x0
    input_ifc=Link-to--ISP-1, output_ifc=any

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
  in id=0x7fff9f72c330, priority=1, domain=nat-per-session, deny=true
  <--- More --->

```

Рисунок 2.6.14. – Приклад застосування діагностичної команди «*packet-tracer input Link-to--ISP-1 tcp 10.54.68.12 3389 109.251.250.1 3389 detail*». Етапи аналізу та фільтрування мережевого трафіку №1 – 3.

```

Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
  in id=0x7fff972c330, priority=1, domain=nat-per-session, deny=true
    hits=142, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
    input_ifc=any, output_ifc=any

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
  in id=0x7fff9b9d9e0, priority=0, domain=inspect-ip-options, deny=true
    hits=100089, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
    input_ifc=Link-to--ISP-1, output_ifc=any

Phase: 6
Type: FOVER
Subtype: standby-update
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
  in id=0x7fff9f9bcd7e0, priority=20, domain=1u, deny=false
    hits=1, user_data=0x0, cs_id=0x0, flags=0x0, protocol=6
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
    input_ifc=Link-to--ISP-1, output_ifc=any

Phase: 7
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
  in id=0x7fff9fb8f050, priority=13, domain=ipsec-tunnel-flow, deny=true
    hits=124, user_data=0x0, cs_id=0x0, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
    input_ifc=Link-to--ISP-1, output_ifc=any

Phase: 8
Type: NAT
Subtype: rpf-check
Result: ALLOW
  <--- More --->

```

Рисунок 2.6.15. – Приклад застосування діагностичної команди «*packet-tracer input Link-to--ISP-1 tcp 10.54.68.12 3389 109.251.250.1 3389 detail*». Етапи аналізу та фільтрування мережевого трафіку №4 – 7.

```

Phase: 8
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
object network RDP-Port-ISP1-to-R-8-11-1
nat (Link-to--R-8-11-1,Link-to--ISP-1) static interface service tcp 3389 3389
Additional Information:
Forward Flow based lookup yields rule:
out id=0x7fff9f9e90b30, priority=6, domain=nat-reverse, deny=false
  hits=1, user_data=0x7fff9f9e90060, cs_id=0x0, use_real_addr, flags=0x0, protocol=6
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
  dst ip/id=172.16.100.25, mask=255.255.255.255, port=3389, tag=0, dscp=0x0
  input_ifc=Link-to--ISP-1, output_ifc=Link-to--R-8-11-1

Phase: 9
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in id=0x7fff9f972c330, priority=1, domain=nat-per-session, deny=true
  hits=144, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
  dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
  input_ifc=any, output_ifc=any

Phase: 10
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in id=0x7fff9fb0fef0, priority=0, domain=inspect-ip-options, deny=true
  hits=34262, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
  dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
  input_ifc=Link-to--R-8-11-1, output_ifc=any

Phase: 11
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 112796, packet dispatched to next module
Module information for forward flow ...
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat
Module information for reverse flow ...
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat
Result:
input-interface: Link-to--ISP-1
input-status: up
input-line-status: up
output-interface: Link-to--R-8-11-1
output-status: up
output-line-status: up
Action: allow
ASA-5512X/pri/act(config)#

```

Рисунок 2.6.16. – Приклад застосування діагностичної команди «*packet-tracer input Link-to--ISP-1 tcp 10.54.68.12 3389 109.251.250.1 3389 detail*». Етапи аналізу та фільтрування мережевого трафіку №8 – 10.

```

in id=0x7fff9f972c330, priority=1, domain=nat-per-session, deny=true
  hits=144, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
  dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
  input_ifc=any, output_ifc=any

Phase: 10
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in id=0x7fff9fb0fef0, priority=0, domain=inspect-ip-options, deny=true
  hits=34262, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
  src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
  dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
  input_ifc=Link-to--R-8-11-1, output_ifc=any

Phase: 11
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 112796, packet dispatched to next module
Module information for forward flow ...
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat
Module information for reverse flow ...
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat
Result:
input-interface: Link-to--ISP-1
input-status: up
input-line-status: up
output-interface: Link-to--R-8-11-1
output-status: up
output-line-status: up
Action: allow
ASA-5512X/pri/act(config)#

```

Рисунок 2.6.17. – Приклад застосування діагностичної команди «*packet-tracer input Link-to--ISP-1 tcp 10.54.68.12 3389 109.251.250.1 3389 detail*». Етапи аналізу та фільтрування мережевого трафіку №10 – 11. Результат роботи діагностичної команди – «Трафік дозволено».

У якості ще одного прикладу, виконаємо команду *«packet-tracer input Link-to--ISP-1 tcp 10.54.97.12 34895 109.251.250.1 8000 detail»* у якій буде виконано спробу отримання доступу за портом 34895 для деякого віддаленого вузла 10.54.97.12, що розташований у глобальній мережі інтернет, до інтерфейсу Cisco ASA, що має IP адресу 109.251.250.1 на основі порту доступу 8000. Нагадаємо, що відповідно до правил трансляції NAT, даний порт не використовується, тому теоритично, міжмережевий екран має заблокувати спробу отримання доступом. Перевіriamo це. Результат наведено у вигляді рисунку 2.6.18.

```

ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)# packet-tracer input Link-to--ISP-1 tcp 10.54.97.12 34895 109.251.250.1 8000 detail
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 109.251.250.1 255.255.255.255 identity
Phase: 2
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7fff9f72c330, priority=1, domain=nat-per-session, deny=true
hits=145, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 3
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7fff9f7bdf10, priority=0, domain=permit, deny=true
hits=39, user_data=0x9, cs_id=0x0, use_real_addr, flags=0x1000, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0, dscp=0x0
input_ifc=Link-to--ISP-1, output_ifc=any
Result:
input-interface: Link-to--ISP-1
input-status: up
input-line-status: up
output-interface: NP Identity ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
ASA-5512X/pri/act(config)#

```

Рисунок 2.6.18. – Приклад застосування діагностичної команди *«packet-tracer input Link-to--ISP-1 tcp 10.54.97.12 34895 109.251.250.1 8000 detail»*. Етапи аналізу та фільтрування мережевого трафіку №1 – 3. Результат роботи діагностичної команди – «Трафік відхилено. Відхилено на основі списку контролю доступу».

Як можемо побачити, трафік було заблоковано. Це відбулося на основі списку контролю доступу, що чітко видно на рисунку вище. За замовчування глобальний інтерфейс Link-to--ISP-1 має рівень безпеки 0, що був встановлений командою *«security-level 0»* під час налаштувань інтерфейсу. Локальні інтерфейси комп’ютерної мережі, так як *«Link-to--R-8-11-1»*, *«Link-to--R-8-11-2»* та *«Link-for--All»* мають рівні безпеки 100, що були встановлені аналогічною командою з параметром 100 – *«security-level 100»*. За логікою роботи Cisco ASA, трафік між

інтерфейсами від меншого рівня до вищого автоматично блокується, в протилежному випадку – ні. Тому, вище відзначений результат є цілком очікуваним, так як у вище наведеному сценарії до інтерфейсу «Link-to--ISP-1», у спробі переходу до локального інтерфейсу, застосовується правило «*ip deny any any*». Воно використовується не завжди. Існують правила передачі трафіку, що мають вищі рівні пріоритету та виконуються раніше, тим самим надаючи доступ. Серед таких правил є використання об'єктів мережі, у яких були сформованими правила переадресації трафіку NAT до локального серверу.

Іншою діагностичною командою під час виконання відлагоджувальних робіт та процесів тестування була діагностична команда, що активує відлагоджувальний режим для протоколу ICMP – «*debug icmp trace*». Роботу даної команди наведено на рисунку 2.6.19 нижче.

```

exec mode commands/options:
<1-255> Specify an optional debug level (default is 1)
KCP>
ASA-5512X/pri/act(config)# debug icmp trace 255
debug icmp trace enabled at level 255
ASA-5512X/pri/act(config)# ICMP echo request from 109.251.250.1 to 109.251.250.126 ID=17473 seq=14666 len=36
ICMP echo request from 10.0.2.6 to 10.0.2.1 ID=4430 seq=1 len=36
ICMP echo reply from 10.0.2.1 to 10.0.2.6 ID=4430 seq=1 len=36
ICMP echo request from 10.0.12.6 to 10.0.12.1 ID=4431 seq=1 len=36
ICMP echo reply from 10.0.12.1 to 10.0.12.6 ID=4431 seq=1 len=36
ICMP echo request from 10.0.1.1 to 10.0.1.5 ID=3674 seq=3905 len=36
ICMP echo reply from 10.0.1.5 to 10.0.1.1 ID=3674 seq=3905 len=36
ICMP echo request from 10.0.12.1 to 10.0.12.5 ID=23896 seq=48512 len=36
ICMP echo reply from 10.0.12.5 to 10.0.12.1 ID=23896 seq=48512 len=36
ICMP echo request from 10.0.12.1 to 10.0.12.6 ID=29346 seq=15874 len=36
ICMP echo reply from 10.0.12.6 to 10.0.12.1 ID=29346 seq=15874 len=36
ICMP echo request from 10.0.2.1 to 10.0.2.6 ID=31111 seq=31181 len=36
ICMP echo reply from 10.0.2.6 to 10.0.2.1 ID=31111 seq=31181 len=36
ICMP echo request from 10.0.1.5 to 10.0.1.1 ID=4273 seq=1 len=36
ICMP echo reply from 10.0.1.1 to 10.0.1.5 ID=4273 seq=1 len=36
ICMP echo request from 10.0.12.5 to 10.0.12.1 ID=4274 seq=1 len=36
ICMP echo reply from 10.0.12.1 to 10.0.12.5 ID=4274 seq=1 len=36
ICMP echo request from 10.0.2.6 to 10.0.2.1 ID=4433 seq=1 len=36
ICMP echo reply from 10.0.2.1 to 10.0.2.6 ID=4433 seq=1 len=36
ICMP echo request from 10.0.12.1 to 10.0.12.6 ID=4434 seq=1 len=36
ICMP echo reply from 10.0.12.6 to 10.0.12.1 ID=4434 seq=1 len=36
ICMP echo request from 10.0.1.1 to 10.0.1.5 ID=15559 seq=11270 len=36
ICMP echo reply from 10.0.1.5 to 10.0.1.1 ID=15559 seq=11270 len=36
ICMP echo request from 10.0.12.1 to 10.0.12.5 ID=56238 seq=14191 len=36
ICMP echo reply from 10.0.12.5 to 10.0.12.1 ID=56238 seq=14191 len=36
ICMP echo request from 10.0.12.1 to 10.0.12.6 ID=29272 seq=14694 len=36
ICMP echo reply from 10.0.12.6 to 10.0.12.1 ID=29272 seq=14694 len=36
ICMP echo request from 10.0.2.1 to 10.0.2.6 ID=30236 seq=53090 len=36
ICMP echo reply from 10.0.2.6 to 10.0.2.1 ID=30236 seq=53090 len=36
ICMP echo request from 10.0.1.5 to 10.0.1.1 ID=4276 seq=1 len=36
ICMP echo reply from 10.0.1.1 to 10.0.1.5 ID=4276 seq=1 len=36
ICMP echo request from 10.0.12.5 to 10.0.12.1 ID=4277 seq=1 len=36
ICMP echo reply from 10.0.12.1 to 10.0.12.5 ID=4277 seq=1 len=36
ICMP echo request from 109.251.250.1 to 109.251.250.126 ID=15415 seq=7210 len=36
ICMP echo reply from 109.251.250.126 to 109.251.250.1 ID=15415 seq=7210 len=36
ICMP echo request from 10.0.2.6 to 10.0.2.1 ID=4435 seq=1 len=36
ICMP echo reply from 10.0.2.1 to 10.0.2.6 ID=4435 seq=1 len=36
ICMP echo request from 10.0.12.6 to 10.0.12.1 ID=4436 seq=1 len=36
ICMP echo reply from 10.0.12.1 to 10.0.12.6 ID=4436 seq=1 len=36
ICMP echo request from 10.0.1.1 to 10.0.1.5 ID=8254 seq=842 len=36
ICMP echo reply from 10.0.1.5 to 10.0.1.1 ID=8254 seq=842 len=36
ICMP echo request from 10.0.12.1 to 10.0.12.5 ID=23933 seq=245 len=36
ICMP echo reply from 10.0.12.5 to 10.0.12.1 ID=23933 seq=245 len=36
ICMP echo request from 10.0.12.1 to 10.0.12.6 ID=5673 seq=4998 len=36
ICMP echo reply from 10.0.12.6 to 10.0.12.1 ID=5673 seq=4998 len=36
ICMP echo request from 10.0.2.1 to 10.0.2.6 ID=13986 seq=4799 len=36
ICMP echo reply from 10.0.2.6 to 10.0.2.1 ID=13986 seq=4799 len=36

```

Рисунок 2.6.19. – Приклад роботи діагностичної команди «*debug icmp trace*»

Ця команда дозволяє відстежувати ICMP запити та відповіді, що проходять крізь мережевий пристрій, і виявляти можливі проблеми з підключенням або конфігурацією мережі. В ході виконання проектування та відлагоджувальних робіт, дана команда використовувалася неодноразова, та допомагала виявити проблемні рішення у питаннях маршрутизації мережевого трафіку, а також вдалі рішення. Одни з прикладів її застосування наведено на рисунку 2.6.20 нижче.

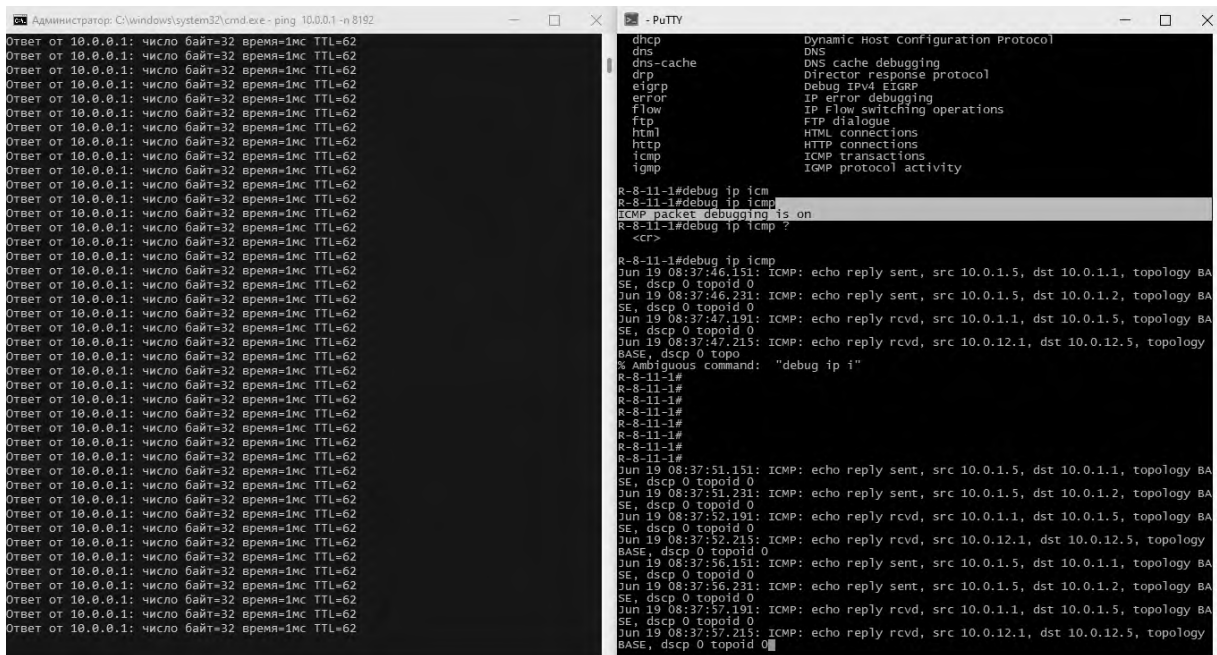


Рисунок 2.6.20. – Приклад застосування діагностичної команди «*debug icmp trace*» під час перевірки роботи засобів маршрутизації мережевого трафіку

На цьому демонстрація основних діагностичних засобів на мережевому обладанні, що були використаними під час відлагоджувальних робіт в ході виконання налагодження роботи проекту комп'ютерної мережі є закінченою. Рухаємося далі.

Розпочнімо виконання тестувань з перевірки відмовостійкості побудованого проекту комп'ютерної мережі. Для цього, підготуємо ряд сценаріїв на основі яких буде проведено дослідження. Перейдемо до їх відтворення, збору інформації та перевірки отриманих результатів.

Сценарій №1. У межах даного сценарію виконується імітація виходу з ладу одного з каналів зв'язку між маршрутизатором R-8-11-1 та комутатором SW-8-11-1. Така відмова потенційно можлива, тому важливо запевнитися у коректно налагоджених правилах маршрутизації трафіку у межах даного проекту, робота яких на пряму впливає на рівень відмовостійкості проекту. Наочне представлення для даного сценарію наведено на рисунку 2.6.21.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				123
Змн.	Арк.	№ докум.	Підпис	Дата		

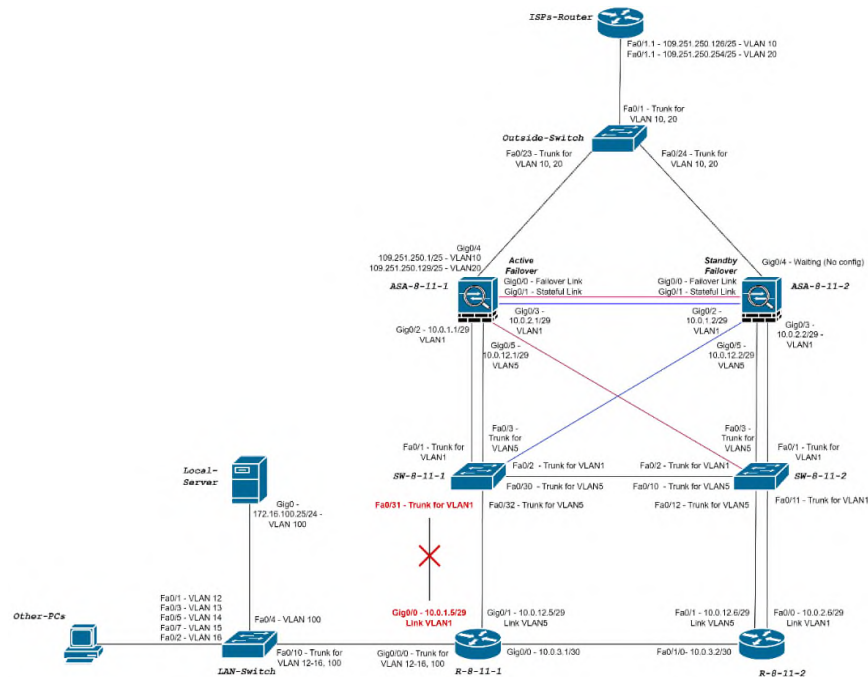


Рисунок 2.6.21 – Сценарій №1. Тестування відмовостійкості за умови виходу з ладу каналу зв'язку між комутатором SW-8-11-1 та маршрутизатором R-8-11-1.

Розпочинаємо підготовку. Для цього спершу активуємо роботу діагностичної команди «*ping*» на час виконання тестування. Перевірку наявності зв'язку будемо виконувати з сервером DNS у підмережі університету, котра виступає у ролі імітації глобальної мережі інтернет. Початково, доступ між вузлом локальної мережі та сервером 10.0.0.1 наявний. Це продемонстровано на рисунку 2.6.23 нижче.

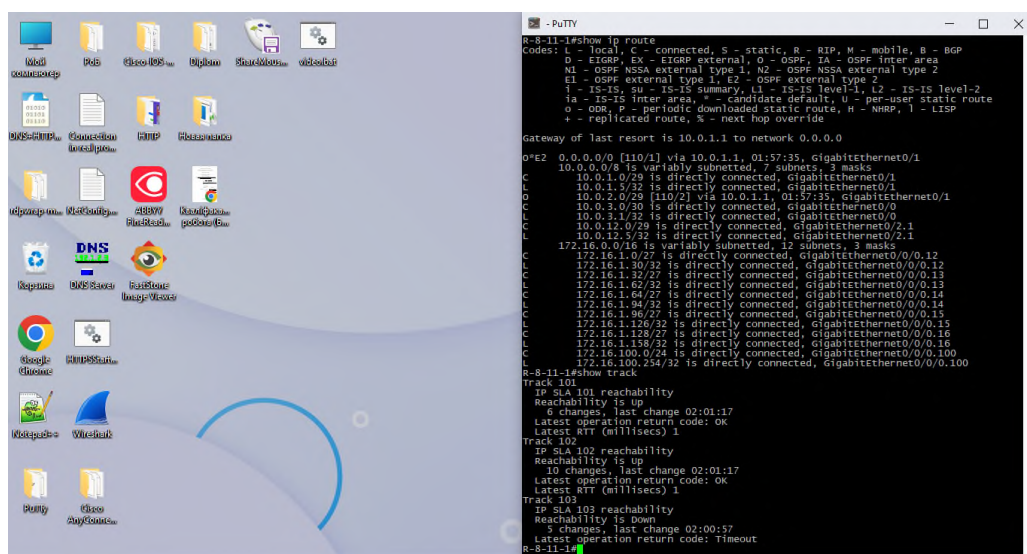


Рисунок 2.6.22 – Початкова таблиця маршрутизації для R-8-11-1. Стан каналів зв'язку на момент тестування є прийнятним

		Колесник Д.В.			Арк.
		Ефіменко А.А.			
Змн.	Арк.	№ докум.	Підпис	Дата	124

Рисунок 2.6.23 – Перевірка наявності зв’язку з глобальним вузлом 10.0.0.1.
Наявність зв’язку є підтвердженою

Далі, виконуємо імітацію виходу з ладу. Для цього достатньо просто розірвати фізичне з’єднання між вузлами, для прикладу, вимкнувши кабель з’єднання між вузлами. В результаті такої маніпуляції отримуємо наступний результат.

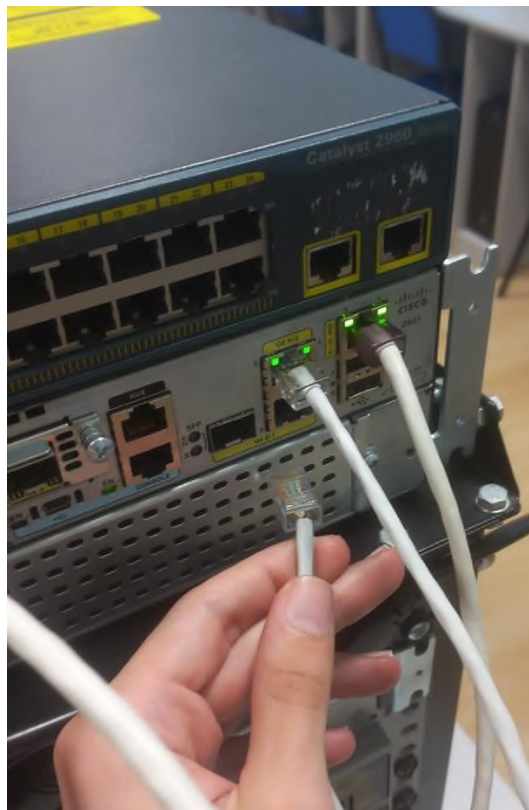


Рисунок 2.6.24 – Відключення фізичного каналу зв’язку між маршрутизатором R-8-11-1 та комутатором SW-8-11-1

У якості додаткового тестування, виконуємо спробу віддаленого підключення до локального сервера мережі через протокол RDP, порт для якого ми відчинили раніше за рахунок Port Forwarding. Для цього буде застосовуватися деяка робоча станція, що імітує підключення з глобальної мережі. Результат даного тестування наведено на рисунку 2.6.27.

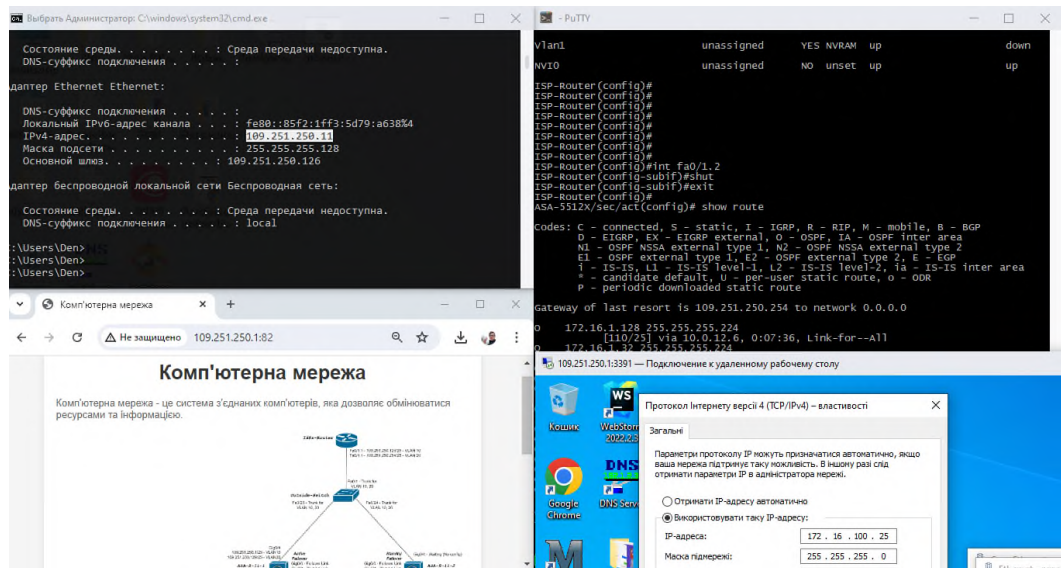


Рисунок 2.6.27 – Результат успішного підключення по протоколу RDP до локального сервера в результаті відтворення сценарію №1. Порт доступу 3391

Також, перевіряємо можливість отримання веб-сторінки від сервера. Відповідно до проведеного вище тестування, очікуємо подібний результат (рис 2.6.28).

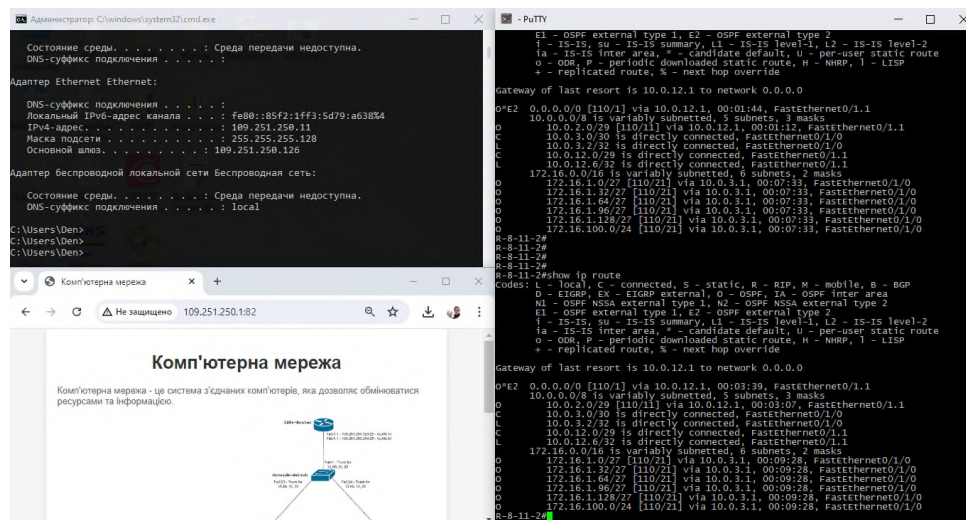


Рисунок 2.6.28 – Результат успішного отримання веб-сторінки по протоколу HTTP до локального сервера в результаті відтворення сценарію №1. Порт доступу

		Колесник Д.В.			Арк.
		Ефіменко А.А.			
Змн.	Арк.	№ докум.	Підпис	Дата	127

Висновки за сценарієм №1. Мережа застосувала резервні шляхи маршрутизації для відновлення передачі мережевого трафіку. Зв'язок між вузлами мережі не зник. Доступ до локального сервера з глобальної мережі за таких умов для роботи з протоколом RDP чи HTTP було підтверджено, але за рахунок використання інших портів для зовнішньої переадресації до внутрішніх сервісів. Мережа працює коректно, відповідно до проведених налаштувань.

Сценарій №2. У межах даного сценарію виконується імітація виходу з ладу одразу двох каналів зв'язку між маршрутизатором R-8-11-1 та комутатором SW-8-11-1. Такий сценарій є можливим, тому запевнимосся у коректно налагоджених правилах маршрутизації трафіку у межах даного проекту, робота яких напряду впливає на рівень відмовостійкості проекту. Нагадаємо, що такий сценарій було передбачено, за рахунок використання останнього можливого каналу зв'язку для досягнення шлюзу у вигляді Cisco ASA на основі каналу зв'язку між R-8-11-1 та R-8-11-2, роботу якого і буде перевірено нами зараз. Наочне представлення для даного сценарію наведено на рисунку 2.6.29.

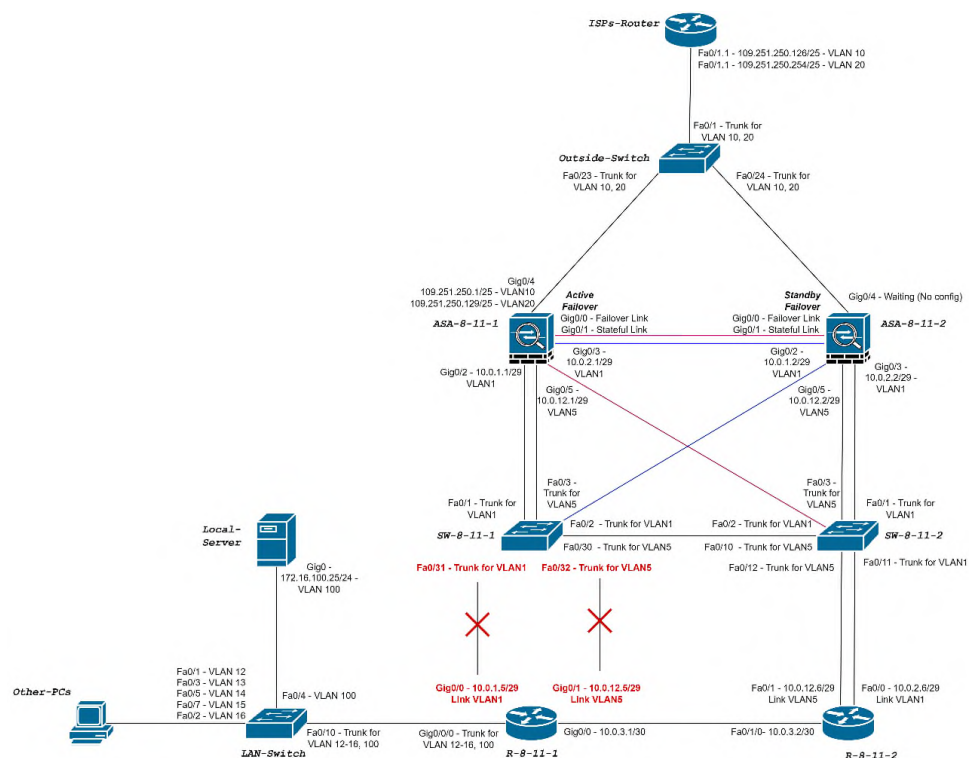


Рисунок 2.6.29 – Сценарій №2. Тестування відмовостійкості за умови виходу з ладу усіх каналів зв'язку між комутатором SW-8-11-1 та маршрутизатором R-8-11-1.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				128
Змн.	Арк.	№ докум.	Підпис	Дата		

Розпочинаємо підготовку. Активуємо роботу діагностичної команди Ping на час виконання тестування. Перевірку наявності зв'язку будемо виконувати з сервером DNS у підмережі університету, котра виступає у ролі імітації глобальної мережі інтернет. Початково, доступ між вузлом локальної мережі та сервером 10.0.0.1 наявний. Це продемонстровано на рисунку 2.6.30 нижче.

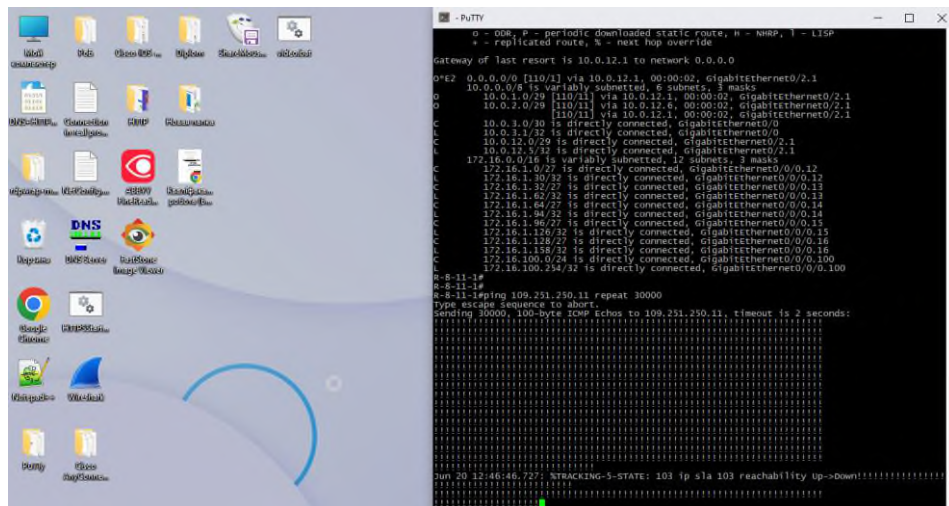


Рисунок 2.6.30 – Перевірка наявності зв'язку перед початком виконання сценарію відмови №2

Далі, виконуємо імітацію виходу з ладу. Для цього достатньо просто розірвати фізичні з'єднання між вузлами, для прикладу, вимкнувши кабелі з'єднання між вузлами. В результаті такої маніпуляції отримуємо наступний результат.



Рисунок 2.6.31 – Розрив фізичних з'єднань між маршрутизатором R-8-11-1 та комутатором SW-8-11-1

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				129
Змн.	Арк.	№ докум.	Підпис	Дата		

Рисунок 2.6.32 – Результат успішного застосування останнього можливого маршруту до міжмережевого екрану Cisco ASA маршрутизатором R-8-11-1

Як можемо побачити на рисунку 2.6.32, зв'язок не зник, що говорить про коректність проведенням нами раніше налаштувань роботи засобів маршрутизації мережевого трафіку. Це відбулося тому, що маршрутизатор R-8-11-1 задіяв останній можливий резервний маршрут до мережі призначення на основі засобів динамічної маршрутизації та роботи IP SLA, котрі, як можна помітити на рисунку вище, відпрацювати та сповістити, що процес відслідковування 101 та 102, було переведено у неактивний режим, а вихід з ладу інтерфейсів спровокував зміни у таблиці маршрутизації.

У якості додаткового тестування, виконуємо спробу віддаленого підключення до локального сервера мережі через протокол RDP, порт для якого ми відчиняли раніше за рахунок Port Forwarding. Так як канал зв'язку крізь інтерфейс «Link-to--R-8-11-1» та «Link-for--All» є недоступними, то порти доступу 3389 та 3391 є недоступними, тому спробу підключення виконуватимемо на основі порту 3390. Для цього буде застосовуватися деяка робоча станція, що імітує підключення з глобальної мережі (рис. 2.6.33).

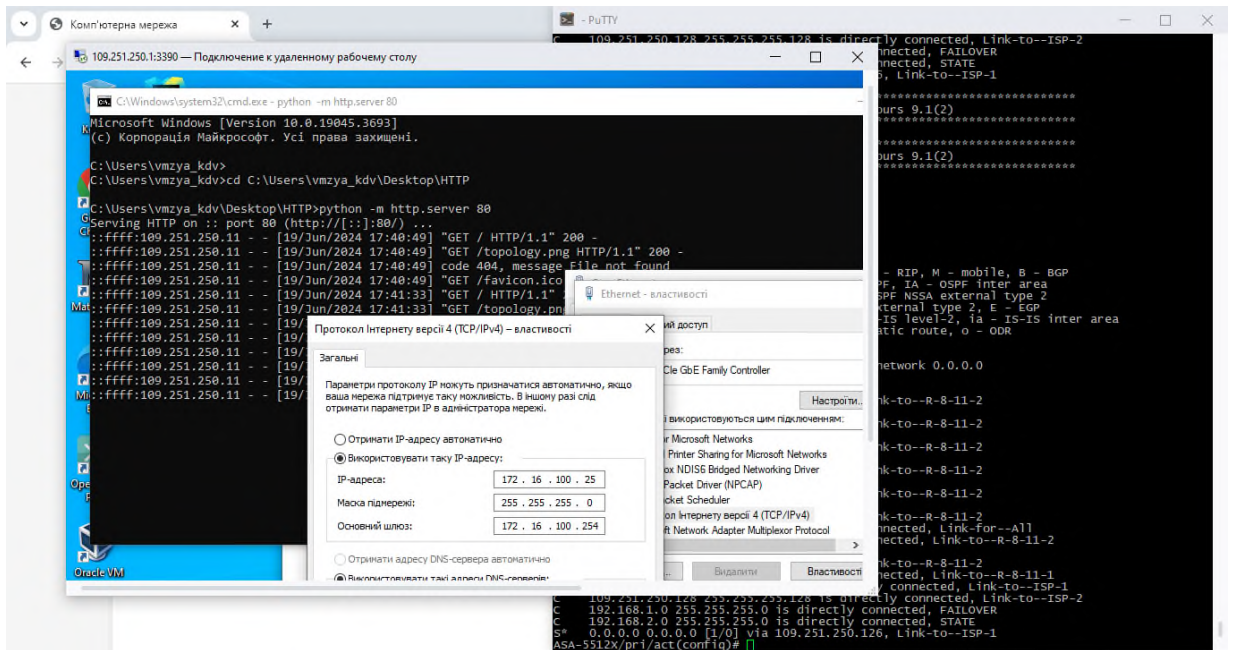


Рисунок 2.6.33 – Результат успішного підключення на основі протоколу RDP за портом доступу 3390 для вузла глобальної мережі інтернет.

Також, перевіряємо можливість отримання веб-сторінки від сервера. Аналогічним чином, порти 80 та 82 є недоступними за такого сценарію, тому використовуємо порт підключення 81. Відповідно до проведеного вище тестування, очікуємо подібний результат (рис. 2.6.34).

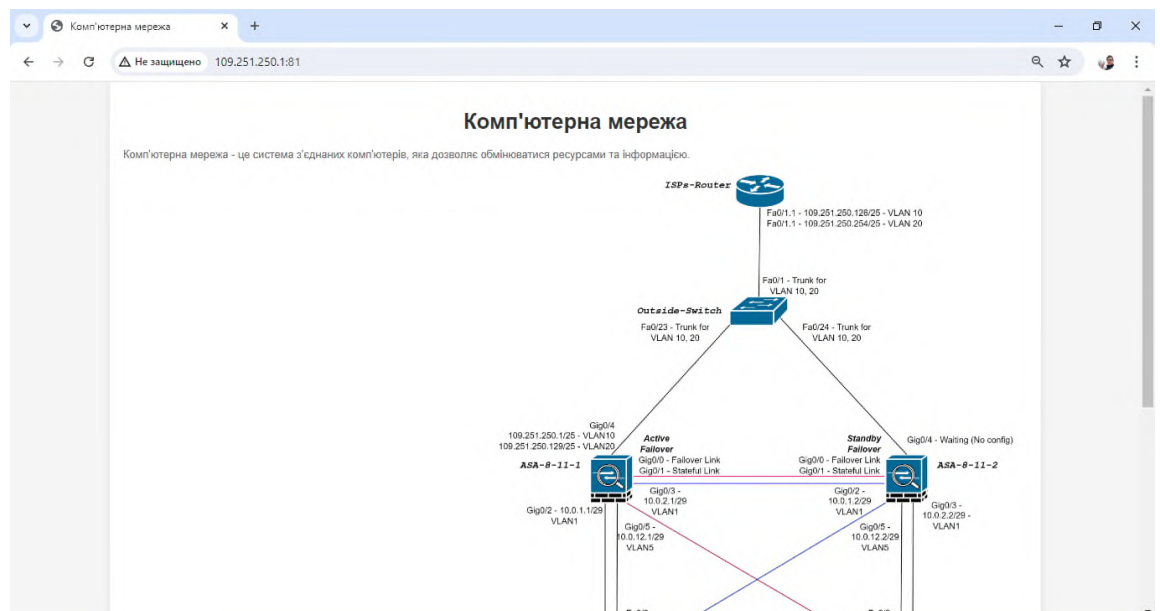


Рисунок 2.6.34 – Результат успішної спроби отримання HTTP сторінки від локального сервера за портом 81

Висновки за сценарієм №2. Мережа застосувала резервні шляхи маршрутизації для відновлення передачі мережевого трафіку. Зв'язок між вузлами мережі не зник. Доступ до локального сервера з глобальної мережі за таких умов для роботи з протоколом RDP чи HTTP було підтверджено, але за рахунок використання інших портів для зовнішньої переадресації до внутрішніх сервісів. Мережа працює коректно, відповідно до проведених налаштувань.

Сценарій №3. У межах даного сценарію виконується спроба виклику Failover у роботі Cisco ASA за результатами роботи якої пошкоджені канали будуть відновлені за рахунок використання іншого, резервного міжмережевого екрану. Наочне представлення для даного сценарію наведено на рисунку 2.6.35.

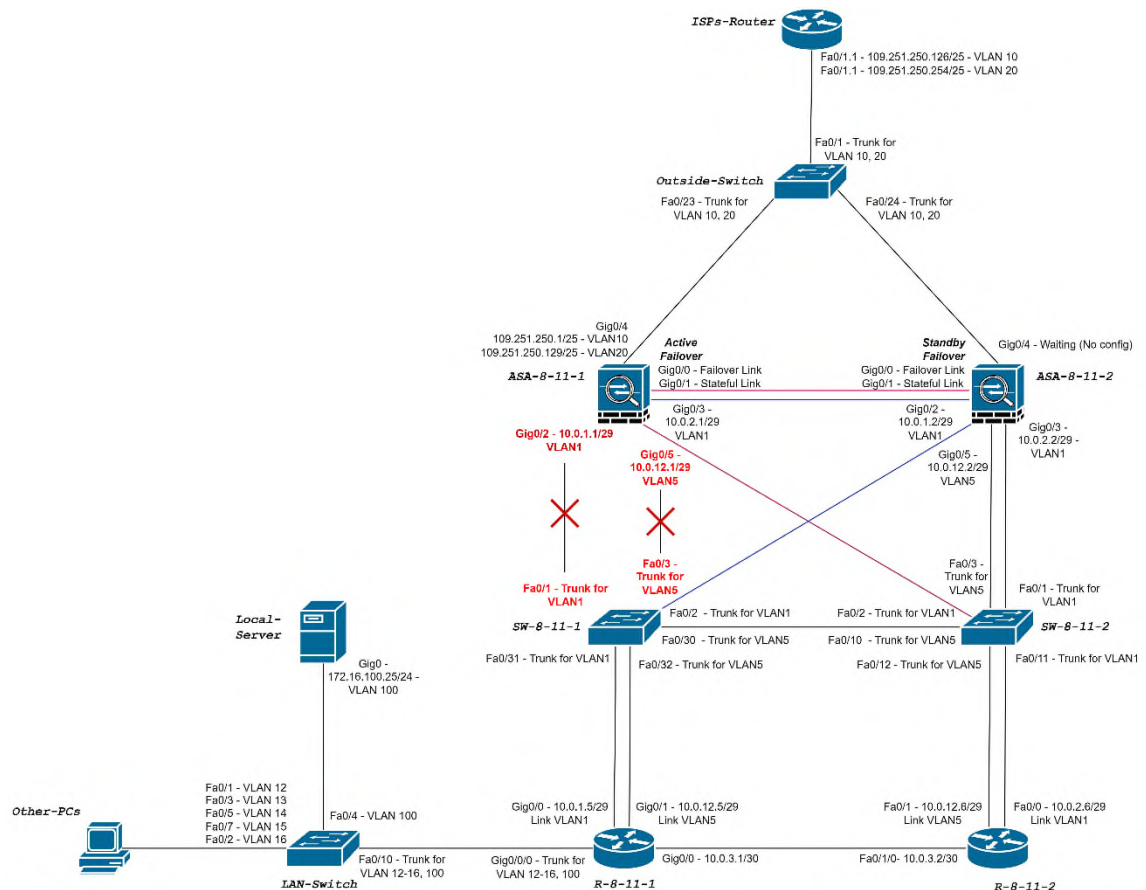


Рисунок 2.6.35 – Сценарій №3. Тестування відмовостійкості за умови виходу з ладу усіх каналів зв'язку між комутатором SW-8-11-1 та міжмережевим екраном Cisco ASA. Спроба провокування Failover.

Розпочинаємо підготовку. Активуємо роботу діагностичної команди «ping» на час виконання тестування. Перевірку наявності зв'язку будемо виконувати з

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		132

сервером DNS у підмережі університету, котра виступає у ролі імітації глобальної мережі інтернет. Початково, доступ між вузлом локальної мережі та сервером 10.0.0.1 наявний. Це продемонстровано на рисунку 2.6.36 нижче.

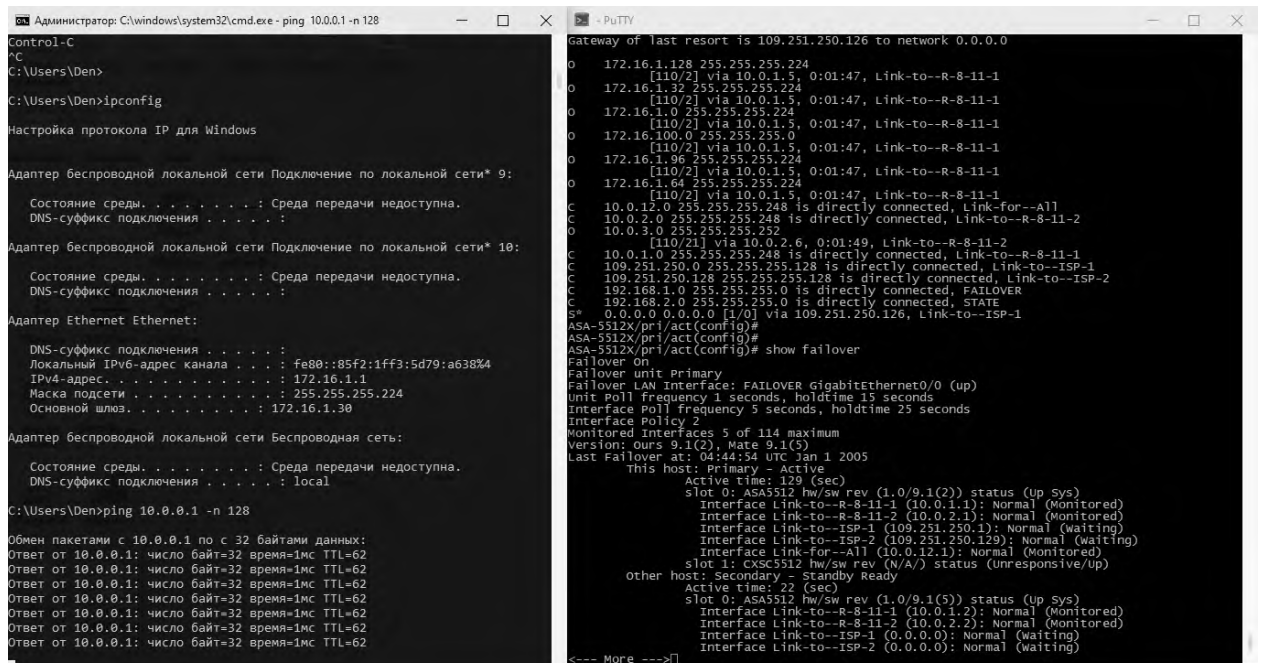


Рисунок 2.6.36 – Результат успішного початкового тестування наявності зв'язку для подальшого виконання досліджень сценарію №3

Далі, виконуємо імітацію виходу з ладу. Для цього достатньо просто розірвати фізичні з'єднання між вузлами, для прикладу, вимкнувши кабелі з'єднання між вузлами. В результаті такої маніпуляції отримуємо наступний результат.



Рисунок 2.6.37 – Тестовий стенд до впровадження сценарію №3

		Колесник Д.В.			Арк.
		Ефіменко А.А.			
Змн.	Арк.	№ докум.	Підпис	Дата	КІ.КР.Б – 123 – 11– ПЗ
					133

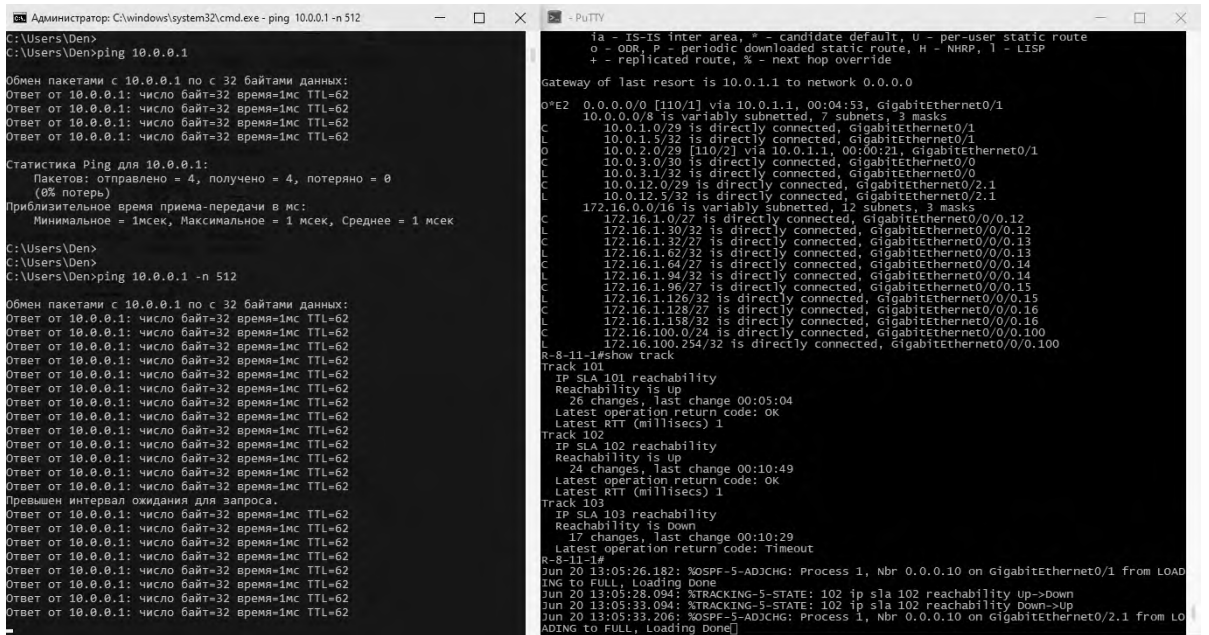


Рисунок 2.6.40 – Демонстрація затримки у перемикання між мережевими екранами ASA на основі технології Failover. Змін у таблиці маршрутизації не відбулося

Як можемо побачити, зв'язок не зник, що говорить про успішну роботу технології Failover на основі режиму роботи Active/Standby, налаштування якого проводилися нами раніше. Це можна чітко помітити на рисунках 2.6.41 та 2.6.42 нижче.



Рисунок 2.6.41 – Стан міжмережеви екранів до спрацювання Failover. Активний вузол – ASA-8-11-1

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				135
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 2.6.42 – Стан міжмережеви екранів після спрацювання Failover.

Активний вузол – ASA-8-11-2

Важливо також запевнитися у можливостях автоматичної віднови наявних сесій у реальному часі. Робота такої функції була передбачена нами під час виконання розробки проекту за рахунок додавання каналу *Stateful Link* між міжмережевими екранами Cisco ASA. В результаті провокування переключення між мережевими екранами, усі наявні сесії були автоматично та успішно збережені. Про це свідчать результати тестування роботи протоколу RDP. За результатами тестувань, було виявлено невеличке підвисання, котре відбулося лише на долі секунди, а згодом і зовсім зникло. Для зручності проведеного тестування, на фоні відтворювалося відео з аудіопотоком. Значних затримок виявлено не було. Перемикання відбулося швидко.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				136
Змн.	Арк.	№ докум.	Підпис	Дата		

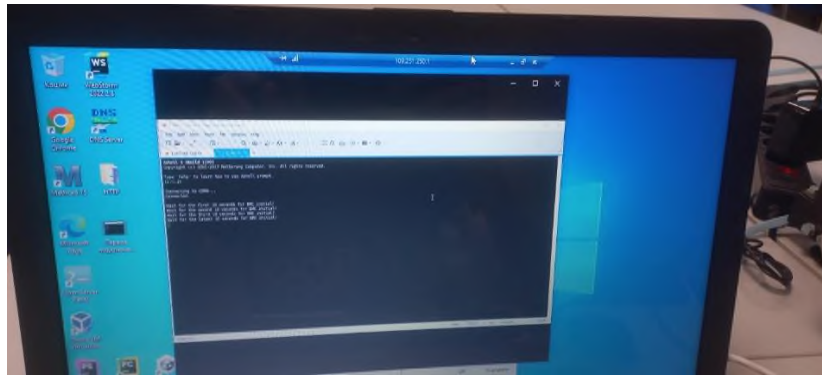


Рисунок 2.6.43 – Робота протоколу RDP до провокування Failover. Порт доступу 3389.

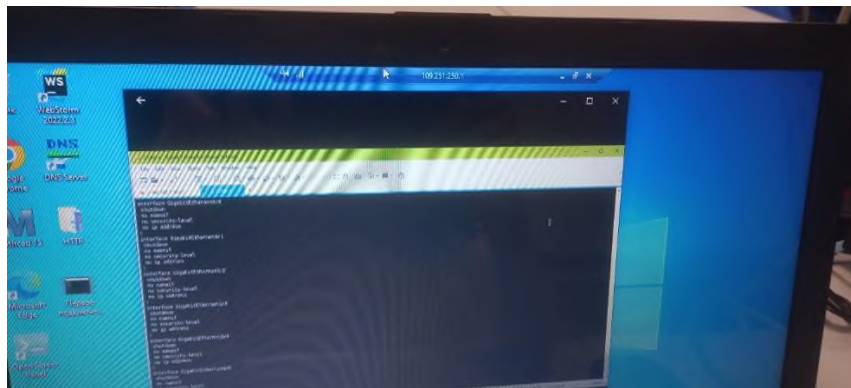


Рисунок 2.6.44 – Робота протоколу RDP після провокування Failover. Порт доступу 3389.

У якості наступного етапу тестування, виконуємо спробу віддаленого підключення до локального сервера мережі через протокол RDP, порт для якого ми відчиняли раніше за рахунок Port Forwarding. Для цього буде застосовуватися деяка робоча станція, що імітує підключення з глобальної мережі (рис. 2.6.45).

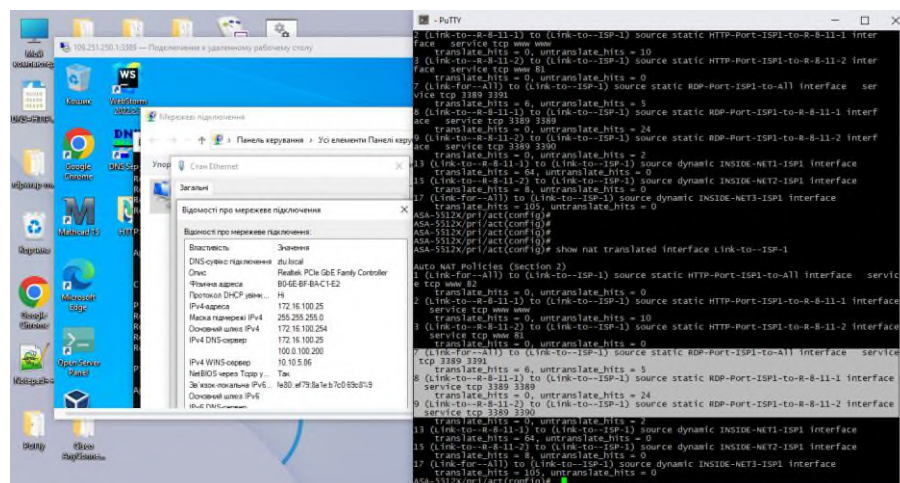


Рисунок 2.6.45 – Успішне тестування роботи протоколу RDP у сценарії №3

		Колесник Д.В.			Арк.
		Ефіменко А.А.			137
Змн.	Арк.	№ докум.	Підпис	Дата	

Також, перевіряємо можливість отримання веб-сторінки від сервера. Відповідно до проведеного вище тестування, очікуємо подібний результат (рис. 2.6.46).

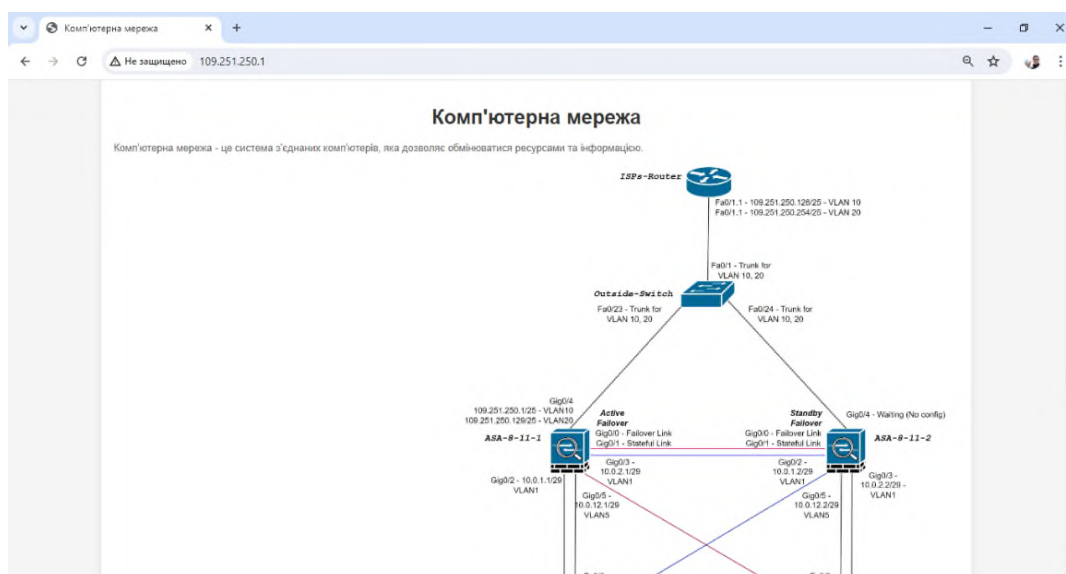


Рисунок 2.6.46 – Успішне тестування спроби отримання веб-сторінки за протоколом HTTP у сценарії №3

Висновки за сценарієм №3. Робота технології Cisco ASA Failover у режимі Active/Standby була успішно продемонстрована та підтверджена. Зв'язок між вузлами мережі не зник. Доступ до локального сервера з глобальної мережі за таких умов для роботи з протоколом RDP чи HTTP було підтверджено. Мережа працює коректно, відповідно до проведених налаштувань. Змін у таблицях маршрутизації виявлено не було. Перехід відбувся непомітно.

Сценарій №4. У межах даного сценарію демонструється вихід з ладу значної частини комп'ютерної мережі, а також можливості проекту, щодо відмовостійкості. У межах цього сценарію демонструється вихід з ладу одразу усіх каналів зв'язку між комутатором SW-8-11-1 та маршрутизатором R-8-11-1 і міжмережним екраном ASA-8-11-1. За своєю суттю, даний сценарій демонструє майже повний вихід з ладу комутатора SW-8-11-1. Наочне представлення для даного сценарію наведено на рисунку 2.6.47.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		138

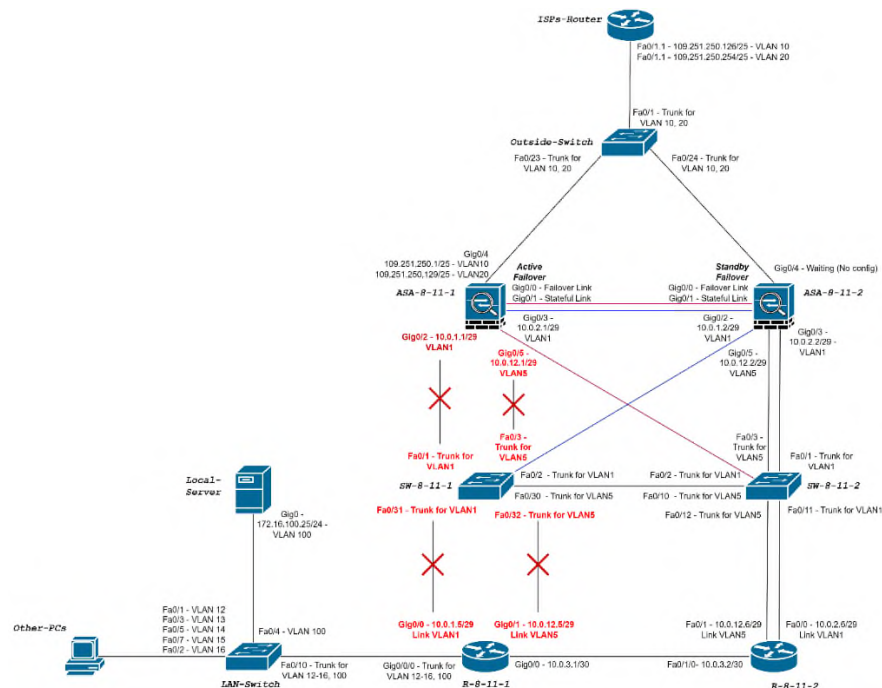


Рисунок 2.6.47 – Сценарій №4. Тестування відмовостійкості за умови виходу з ладу усіх каналів зв'язку між комутатором SW-8-11-1 та міжмережним екраном ASA-8-11-1 і маршрутизатором R-8-11-1.

Розпочинаємо підготовку. Активуємо роботу діагностичної команди «ping» на час виконання тестування. Перевірку наявності зв'язку будемо виконувати з сервером DNS у підмережі університету, котра виступає у ролі імітації глобальної мережі інтернет. Початково, доступ між вузлом локальної мережі та сервером 10.0.0.1 наявний. Це продемонстровано на рисунку 2.6.48 нижче.

```

Администратор: C:\windows\system32\cmd.exe - ping 10.0.0.1 -n 128

Control-C
C:\Users\Den>
C:\Users\Den>ipconfig

Настройка протокола IP для Windows

Адаптер Беспроводной локальной сети Подключение по локальной сети* 9:
    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Адаптер Беспроводной локальной сети Подключение по локальной сети* 10:
    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Адаптер Ethernet Ethernet:
    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::85f2:1ff3:5d79:a638%4
    IPv4-адрес. . . . . : 172.16.1.1
    Маска подсети . . . . . : 255.255.255.224
    Основной шлюз. . . . . : 172.16.1.30

Адаптер Беспроводной локальной сети Беспроводная сеть:
    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . : local

C:\Users\Den>ping 10.0.0.1 -n 128

Обмен пакетами с 10.0.0.1 по 32 байтами данных:
Ответ от 10.0.0.1: число байт=32 время=1мс TTL=62
Ответ от 10.0.0.1: число байт=32 время=1мс TTL=62
Ответ от 10.0.0.1: число байт=32 время=1мс TTL=62
Ответ от 10.0.0.1: число байт=32 время=1мс TTL=62
Ответ от 10.0.0.1: число байт=32 время=1мс TTL=62

```

```

Gateway of last resort is 109.251.250.126 to network 0.0.0.0
0 172.16.1.128 255.255.255.224
   [110/2] via 10.0.1.5, 0:01:47, Link-to--R-8-11-1
0 172.16.1.30 255.255.255.224
   [110/2] via 10.0.1.5, 0:01:47, Link-to--R-8-11-1
0 172.16.1.0 255.255.255.224
   [110/2] via 10.0.1.5, 0:01:47, Link-to--R-8-11-1
0 172.16.100.0 255.255.255.0
   [110/2] via 10.0.1.5, 0:01:47, Link-to--R-8-11-1
0 172.16.1.96 255.255.255.224
   [110/2] via 10.0.1.5, 0:01:47, Link-to--R-8-11-1
0 172.16.1.64 255.255.255.224
   [110/2] via 10.0.1.5, 0:01:47, Link-to--R-8-11-1
0 10.0.12.0 255.255.255.248 is directly connected, Link-to--R-8-11-2
0 10.0.2.0 255.255.255.248 is directly connected, Link-to--R-8-11-2
0 10.0.3.0 255.255.255.252
   [110/2] via 10.0.2.6, 0:01:49, Link-to--R-8-11-2
0 10.0.1.0 255.255.255.248 is directly connected, Link-to--R-8-11-1
0 109.251.250.0 255.255.255.128 is directly connected, Link-to--ISP-1
0 109.251.250.128 255.255.255.128 is directly connected, Link-to--ISP-2
0 192.168.1.0 255.255.255.0 is directly connected, FAILOVER
0 192.168.2.0 255.255.255.0 is directly connected, STATE
0 0.0.0.0 0.0.0.0 [1/0] via 109.251.250.126, Link-to--ISP-1
C# ASA5512X/pr1/act(config)# show failover
Failover unit primary
Failover LAN interface: FAILOVER GigabitEthernet0/0 (up)
Unit Poll Frequency 1 seconds, holdtime 15 seconds
Interface Poll Frequency 5 seconds, holdtime 25 seconds
Interface policy 2
Monitored interfaces 5 of 114 maximum
Version: Ours 9.1(2), Mate 9.1(2)
Last Failover at: 04:44:54 UTC Jan 1 2005
This host: Primary - Active
Active time: 129 (Sec)
slot 0: ASA5512 hw/sw rev (1.0/9.1(2)) status (Up Sys)
Interface Link-to--R-8-11-1 (10.0.1.1): Normal (monitored)
Interface Link-to--R-8-11-2 (10.0.2.1): Normal (monitored)
Interface Link-to--ISP-1 (109.251.250.1): Normal (waiting)
Interface Link-to--ISP-2 (109.251.250.129): Normal (waiting)
Interface Link-for--All (10.0.12.1): Normal (monitored)
slot 1: CSC5512 hw/sw rev (N/A) status (Unresponsive/Up)
other host: Secondary - Standby Ready
Active time: (Sec)
slot 0: ASA5512 hw/sw rev (1.0/9.1(3)) status (Up Sys)
Interface Link-to--R-8-11-1 (10.0.1.2): Normal (monitored)
Interface Link-to--R-8-11-2 (10.0.2.2): Normal (monitored)
Interface Link-to--ISP-1 (0.0.0.0): Normal (waiting)
Interface Link-to--ISP-2 (0.0.0.0): Normal (waiting)

```

Рисунок 2.6.48 – Перевірка наявності зв'язку перед початком виконання сценарію №4

Далі, виконуємо імітацію виходу з ладу. Для цього виконуємо вимкнення живлення для комутатора SW-8-11-1. В результаті такої маніпуляції отримуємо наступний результат.

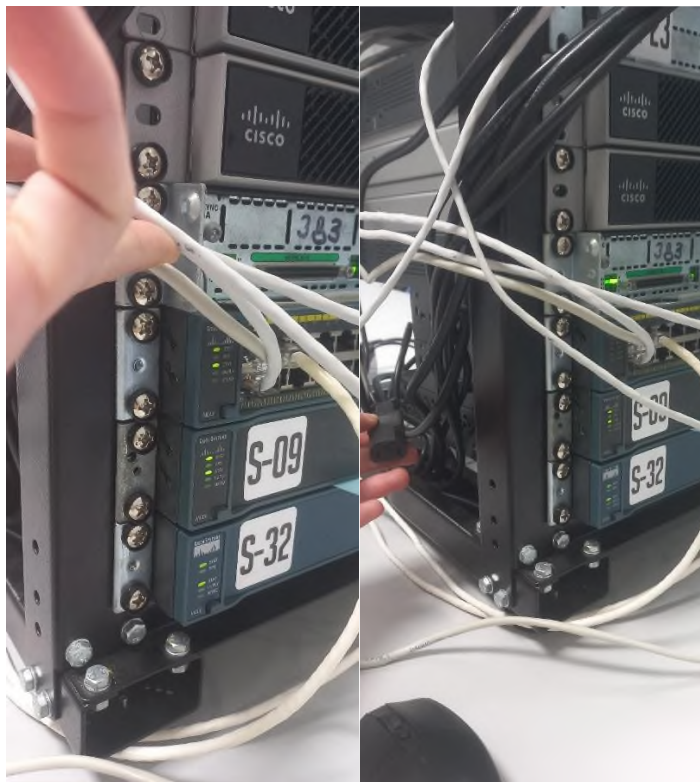


Рисунок 2.6.49 – Приклад вимкнення живлення для комутатора SW-8-11-1 під час відтворення роботи мережі у сценарії №4

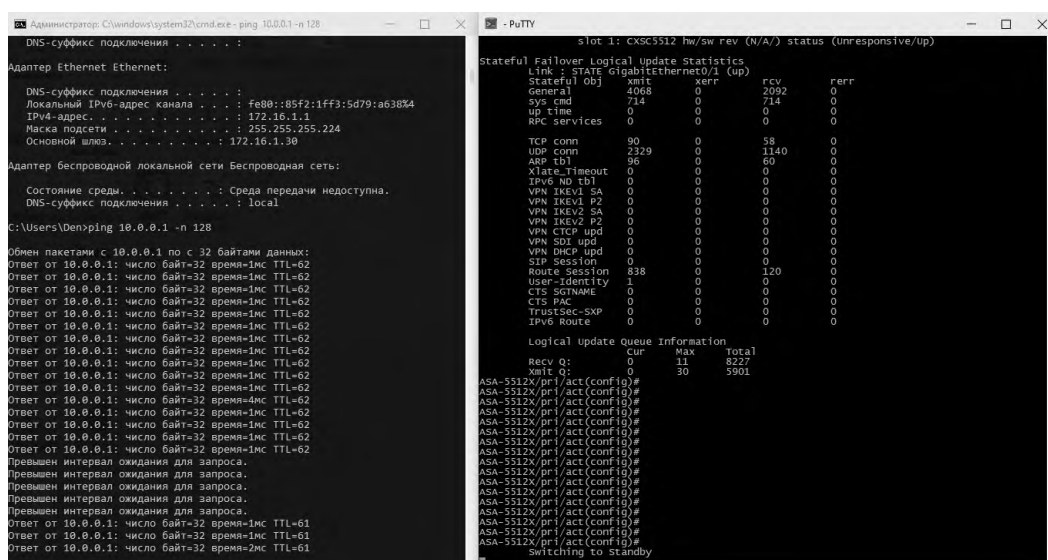


Рисунок 2.6.50 – Результат успішного перемикування каналів зв'язку та спрацьовування технології Cisco ASA Failover. Інформаційний обмін – наявний

		Колесник Д.В.			Арк.
		Ефіменко А.А.			
Змн.	Арк.	№ докум.	Підпис	Дата	140

Як можемо побачити, зв'язок не зник, що говорить про успішну роботу технології Failover на основі режиму роботи Active/Standby, налаштування якого проводилися нами раніше, а також засобів маршрутизації мережевого трафіку, успішна робота яких допомогла зберегти працеспроможність проекту комп'ютерної мережі. Це можна чітко помітити на рисунках 2.6.51 та 2.6.52 нижче.

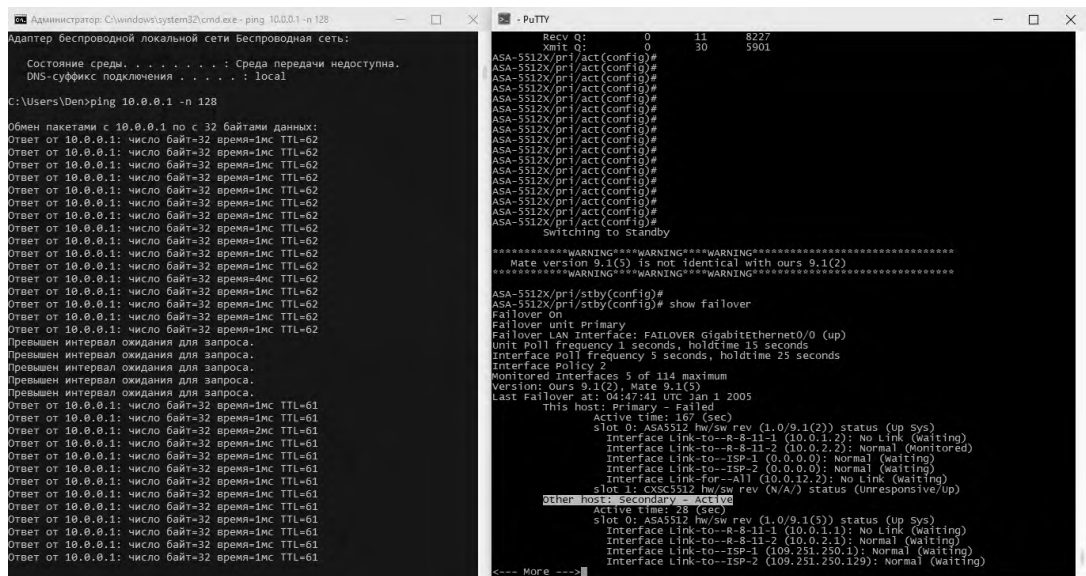


Рисунок 2.6.51 – Робота технології Failover після відтворення сценарію №4

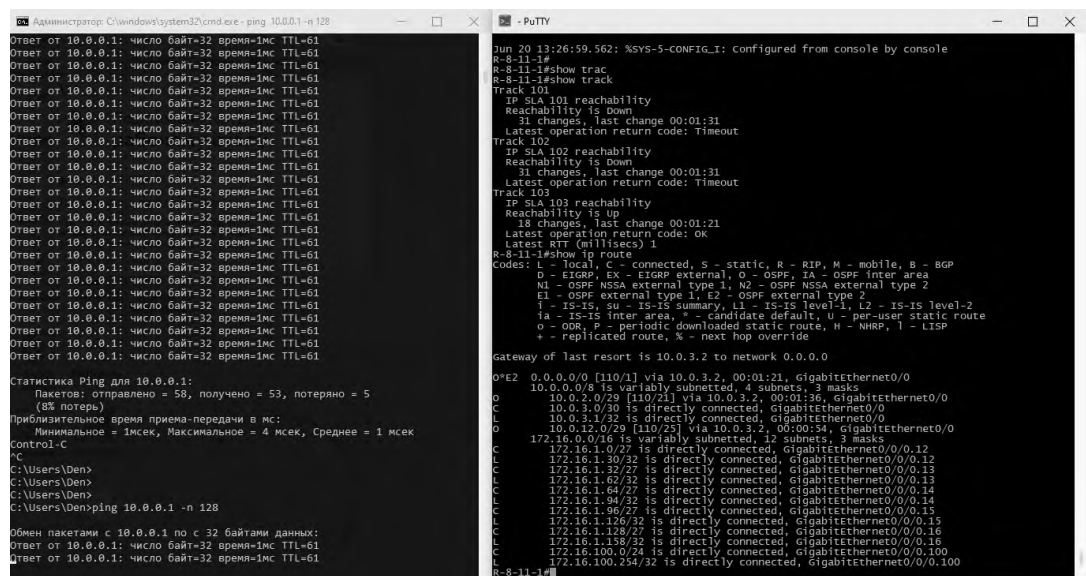


Рисунок 2.6.52 – Таблиця маршрутизації для R-8-11-1 після впровадження сценарію №4

У якості наступного етапу тестування, виконуємо спробу віддаленого підключення до локального сервера мережі через протокол RDP, порт для якого ми

		Колесник Д.В.			Арк.
		Ефименко А.А.			
Змн.	Арк.	№ докум.	Підпис	Дата	
КІ.КР.Б – 123 – 11– ПЗ					141

відчиняли раніше за рахунок Port Forwarding. Для цього буде застосовуватися деяка робоча станція, що імітує підключення з глобальної мережі (рис. 2.6.53).

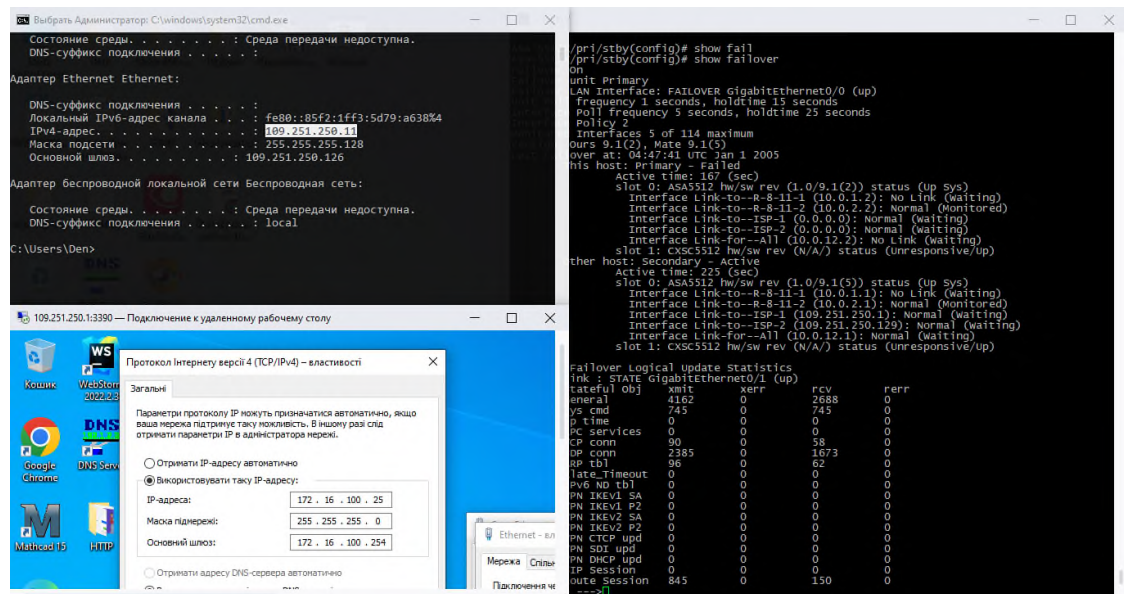


Рисунок 2.6.53 – Виконання успішної спроби отримання віддаленого доступу RDP на основі порту доступу 3390

Також, перевіряємо можливість отримання веб-сторінки від сервера. Відповідно до проведеного вище тестування, очікуємо подібний результат (рис. 2.6.54).

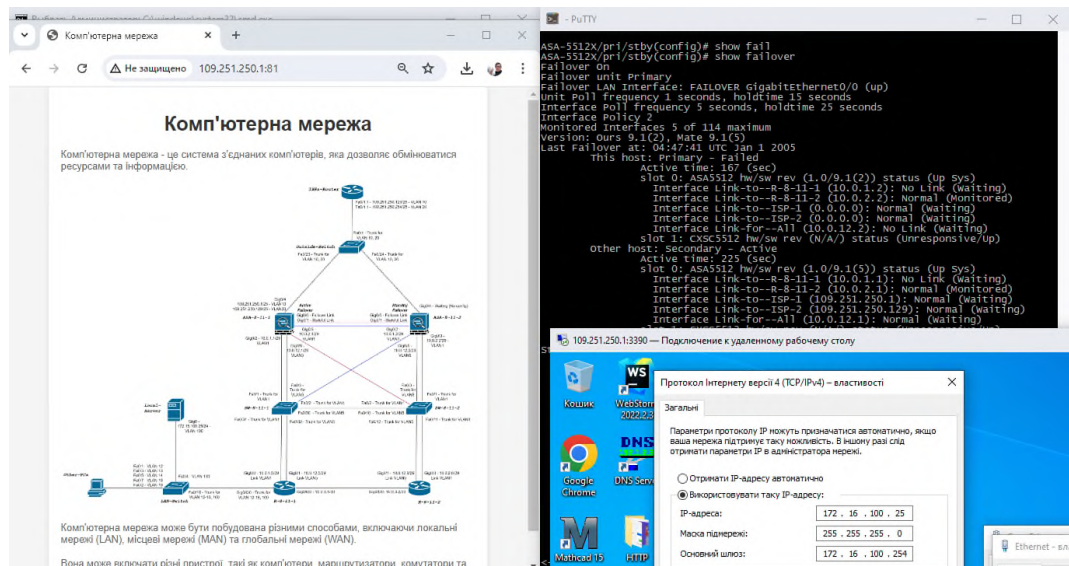


Рисунок 2.6.54 – Результат виконання успішної спроби отримання веб-сторінки на основі протоколу HTTP за портом 81

Висновки за сценарієм №4. Хоча значна частина комп'ютерної мережі, за обставин виходу з ладу (імітація вимкнення живлення) мережевого комутатора SW-

		Колесник Д.В.			Арк.
		Ефименко А.А.			
Змн.	Арк.	№ докум.	Підпис	Дата	142

8-11-1, відмовила в обслуговуванні, за рахунок наявності резервних каналів зв'язку для обміну даними, а також роботи технології Cisco ASA Failover у режимі Active/Standby, робота проекту комп'ютерної мережі не була зупинена. Таким чином, проект демонструє дійсно високий рівень відмовостійкості каналів зв'язку, що підтверджується не лише теоритичними, але й практичними та фактично виявленими результатами поведінки за таких умов. Відмова в обслуговуванні засобів локальних серверів також не була виявлена. Проект працює коректно та надійно, відповідно до проведених налаштувань.

Сценарій №5. У сценарії №5 буде продемонстровано роботу у одному з найгірших сценаріїв роботи проекту комп'ютерної мережі. За рахунок особливостей роботи проекту комп'ютерної мережі її відмова за таких умов ще не є гарантовано, тому перевіримо це. Наочне представлення для даного сценарію наведено на рисунку 2.6.55.

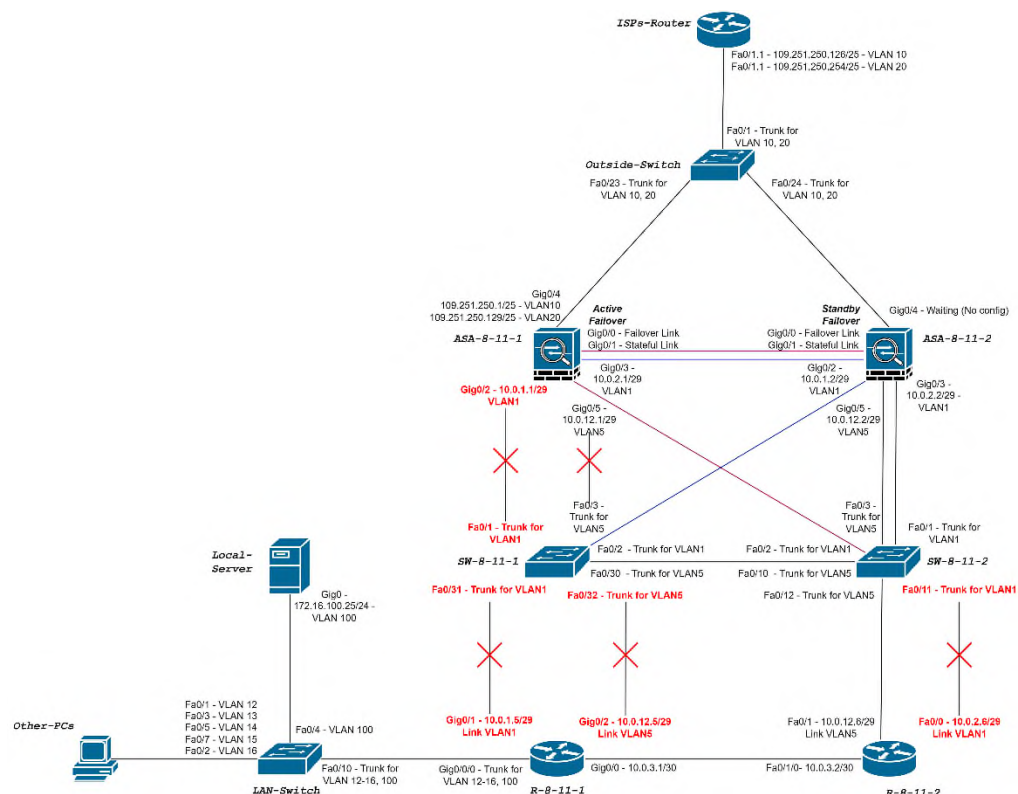


Рисунок 2.6.55 – Сценарій №5. Вихід з ладу мережевого комутатора SW-8-11-1, а також каналу зв'язку між R-8-11-2 та комутатором SW-8-11-2.

Розпочинаємо підготовку. Активуємо роботу діагностичної команди «ping» на час виконання тестування. Перевірку наявності зв'язку будемо виконувати з сервером DNS у підмережі університету, котра виступає у ролі імітації глобальної мережі інтернет. Початково, доступ між вузлом локальної мережі та сервером 10.0.0.1 наявний. Далі, виконуємо імітацію виходів з ладу. Для цього виконуємо вимкнення живлення для комутатора SW-8-11-1, а також роз'єднання фізичного каналу зв'язку між комутатором SW-8-11-2 та маршрутизатором R-8-11-2. В результаті такої маніпуляції отримуємо наступний результат.



Рисунок 2.6.56 – Роз'єднання фізичного з'єднання між маршрутизатором R-8-11-2 та комутатором SW-8-11-2.

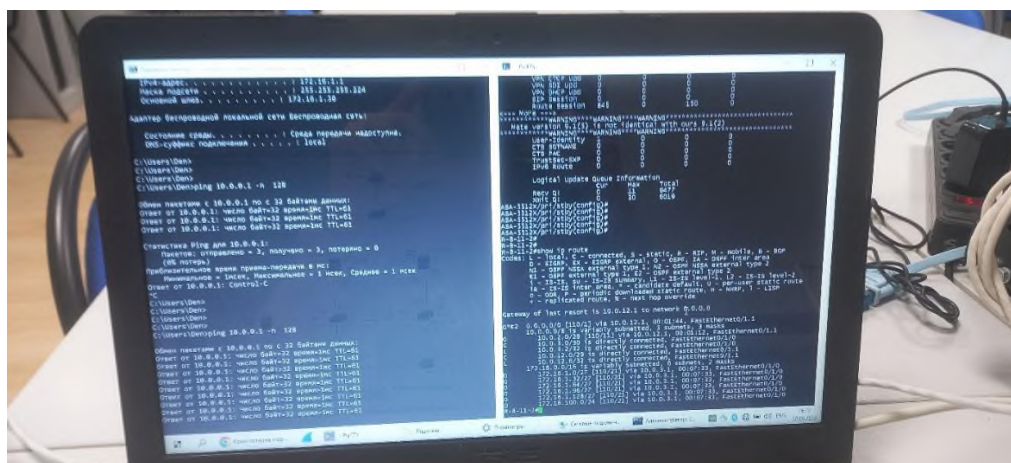


Рисунок 2.6.57 – Успішне тестування відмовостійкості для сценарію №5

		Колесник Д.В.			Арк.
		Ефіменко А.А.			
Змн.	Арк.	№ докум.	Підпис	Дата	144

Як можемо побачити, за такого сценарію проект все ще здатний забезпечувати відмовостійкість. Такий результат є цілком очікуваним. У якості наступного етапу тестування, виконуємо спробу віддаленого підключення до локального сервера мережі через протокол RDP, порт для якого ми відчиняли раніше за рахунок Port Forwarding. Також, перевіряємо можливість отримання веб-сторінки від сервера. Для цього буде застосовуватися деяка робоча станція, що імітує підключення з глобальної мережі (рис. 2.6.58).

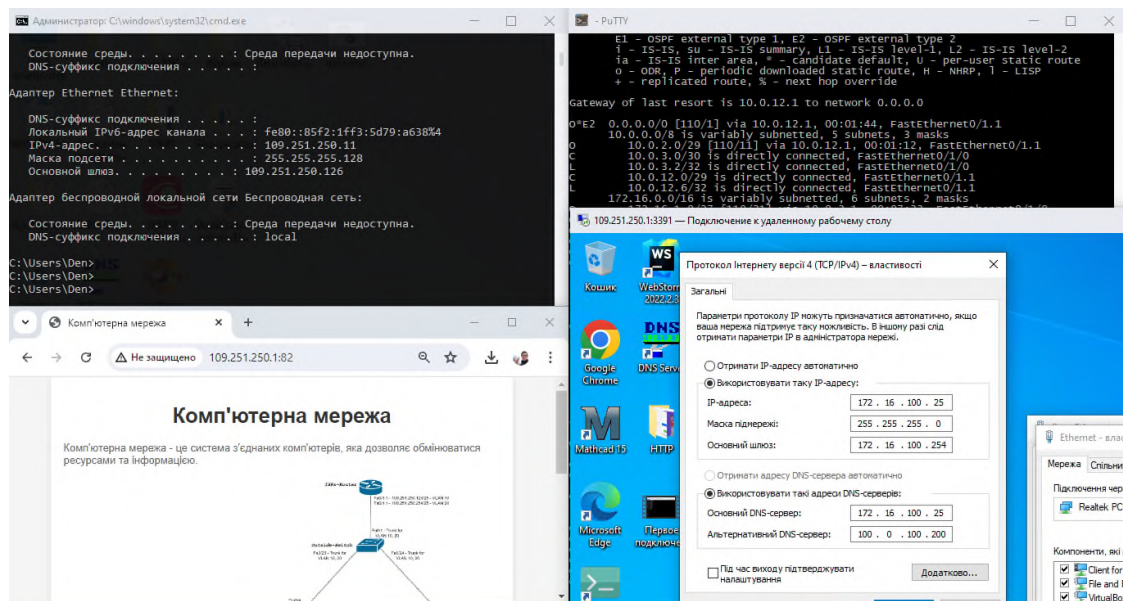


Рисунок 2.6.58 – Результат успішної доступності сервісів локального сервера для вузлів глобальної мережі

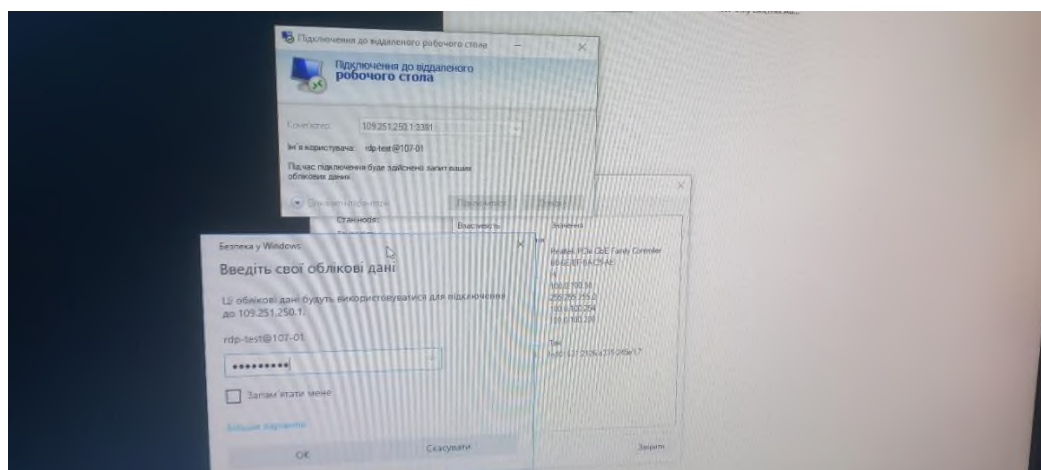


Рисунок 2.6.59 – Успішна спроба отримання доступу до локального сервера на основі протоколу RDP та порту доступу 3391 для деякого вузла глобальної мережі інтернет

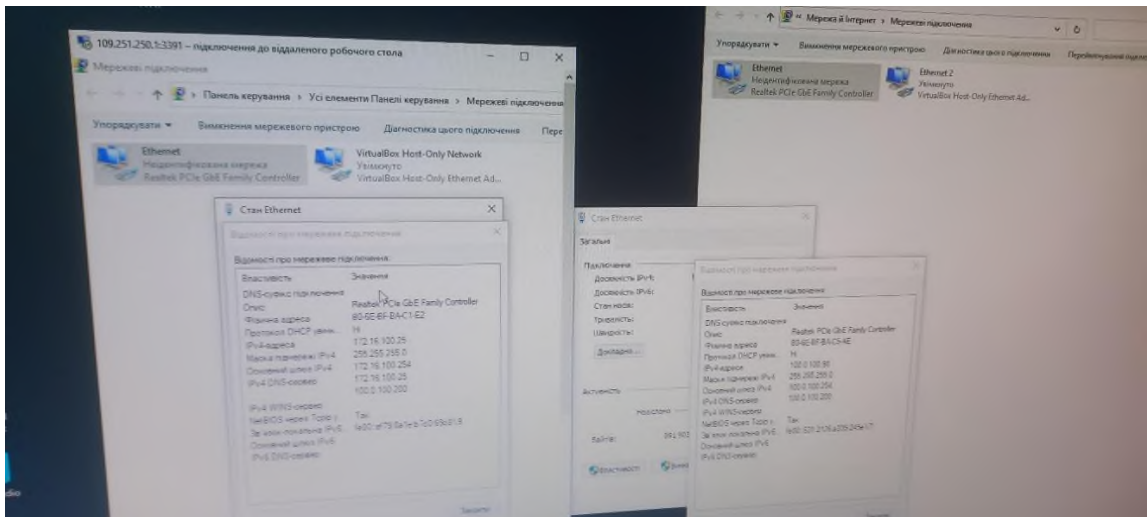


Рисунок 2.6.60 – Успішна спроба підключення до локального сервера на основі протоколу RDP та порту доступу 3391 для деякого вузла глобальної мережі інтернет

Висновки за сценарієм №5. Сценарій №5 демонструє дуже високий рівень пропрацьованості та відмовостійкості комп'ютерної мережі. У випадку, коли більша частина мережі перебуває у неактивному стані, з'являється останній можливий, четвертий канал обміну трафіку для усіх локальних вузлів комп'ютерної мережі. Робота комп'ютерної мережі за такого сценарію є можливою, але варто недопускати таких серйозних проблем у роботі проекту, так як інших альтернативних каналів зв'язку з глобальною мережею немає.

Сценарій №6. Сценарій №6 є повною ідентичністю до сценарію №5, але з врахуванням виходу з ладу одного з інтернет провайдерів. Наочне представлення для даного сценарію наведено на рисунку 2.6.61.

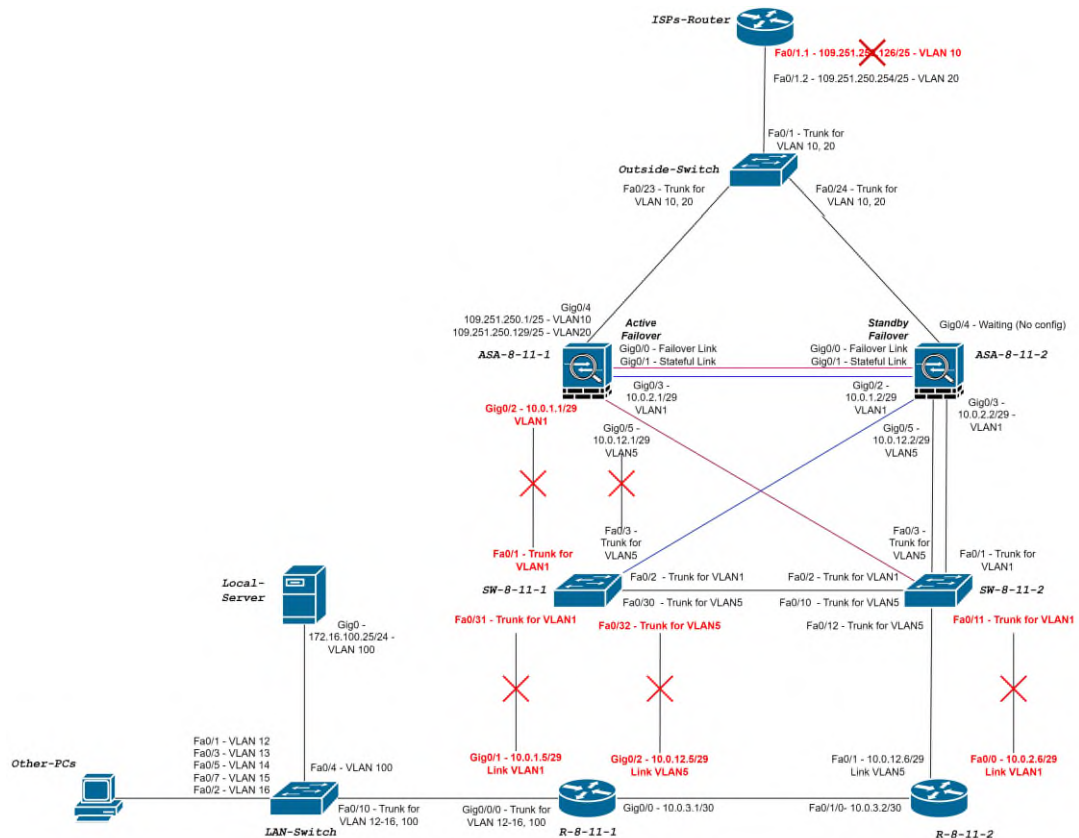


Рисунок 2.6.61 – Сценарій №6. Тестування відмовостійкості за умови виходу з ладу комутатора SW-8-11-1, каналу зв'язку між маршрутизатором R-8-11-2 та комутатором SW-8-11-2, а також при умові виходу з ладу каналу зв'язку з першим інтернет провайдером.

Розпочинаємо підготовку. Активуємо роботу діагностичної команди Ping на час виконання тестування. Перевірку наявності зв'язку будемо виконувати з сервером DNS у підмережі університету, котра виступає у ролі імітації глобальної мережі інтернет. Початково, доступ між вузлом локальної мережі та сервером 10.0.0.1 наявний. Далі, виконуємо імітацію виходу з ладу. Для виконуємо вимкнення живлення для комутатора SW-8-11-1, а також деактивацію каналу зв'язку першого інтернет провайдера. В результаті такої маніпуляції отримуємо наступний результат (рис. 2.6.62).

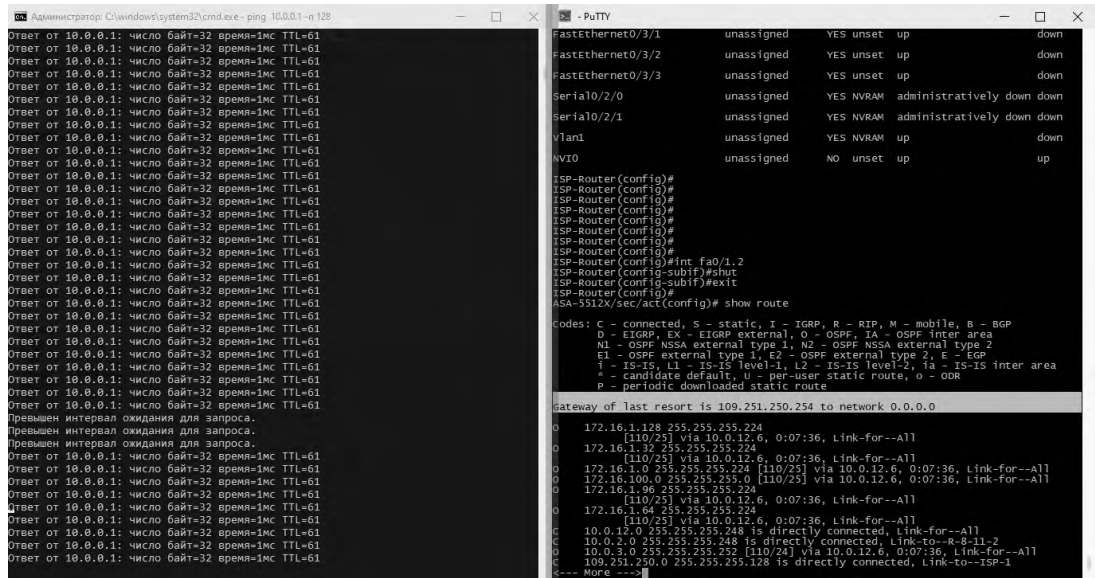


Рисунок 2.6.62 – Результат успішного тестування наявності зв’язку з вузлом глобальної мережі за сценарію №6

Як можемо побачити, відповідно до налагоджених правил мережевої маршрутизації трафіку, було задіяно альтернативний канал зв’язку з другим інтернет провайдером, робота якого все ще дозволяє отримати доступ до глобальної мережі інтернет. Це можна чітко помітити на рисунках 2.6.63 та 2.6.64 нижче.

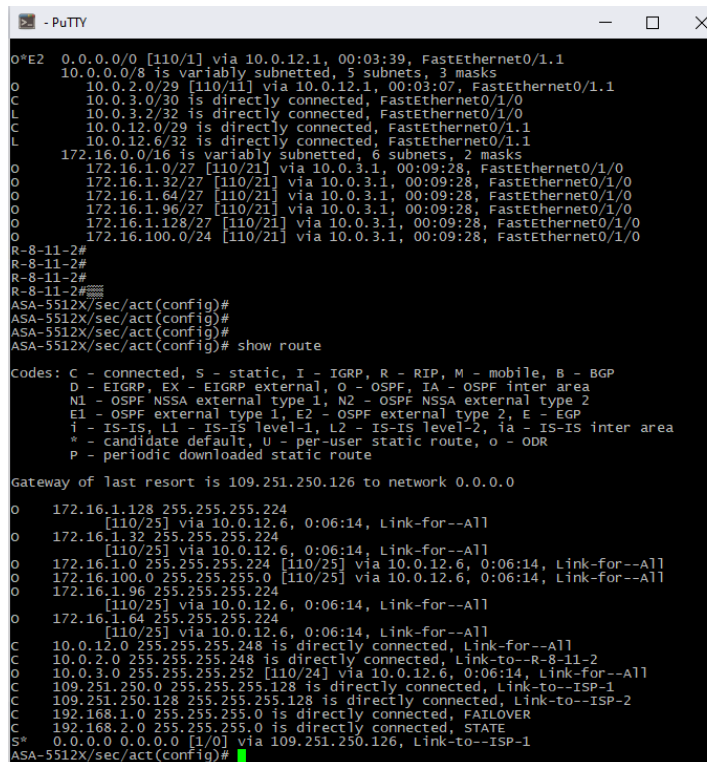


Рисунок 2.6.63 – Таблиця маршрутизації активного міжмережевого екрану до впровадження сценарію №6

		Колесник Д.В.			Арк.
		Ефіменко А.А.			
Змн.	Арк.	№ докум.	Підпис	Дата	148

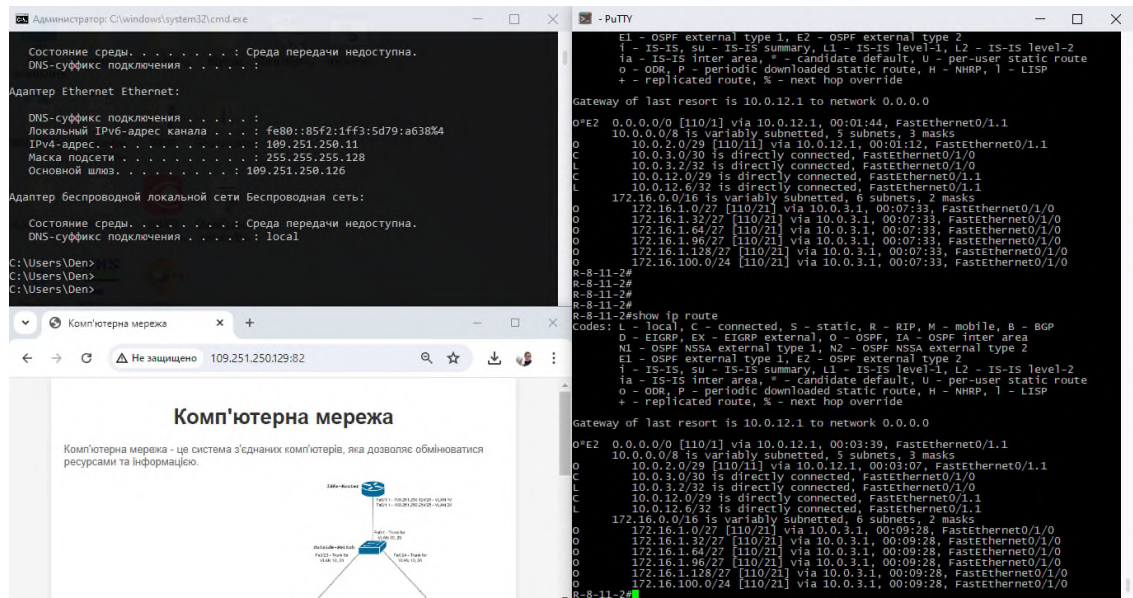


Рисунок 2.6.66 – Результат успішної спроби отримання веб-сторінки на основі IP-адреси 109.251.250.129, що являється IP-адресою у другій підмережі інтернет провайдера, та порту доступу 82

Висновки за сценарієм №6. Робота альтернативних каналів зв'язку з підмережами інтернет провайдерів є підтвердженою. У разі відмови в обслуговуванні зі сторони одного з інтернет провайдерів, наявна підтверджена робота альтернативного каналу зв'язку, що надає доступ до глобальної мережі інтернет. Інші результати тестування є ідентичними результатам, що були отримані під час тестування роботи сценарію №5.

Таким чином, на основі вище проведених досліджень роботи проекту комп'ютерної мережі, було підтверджено її рівень високої відмовостійкості та достатнього рівня надійності для коректного функціонування за тих чи інших досліджених та описаних сценаріїв вище.

Перейдемо до етапу тестування роботи засобів фільтрації мережевого трафіку на основі повністю визначених доменних імен мережевих ресурсів. Для цього, було проведено модифікацію тестового стенду, де буде додано імітацію зовнішнього DNS-сервера, який покликаний займатися обробкою запитів доменних імен. Для демонстрації роботи було модифіковано проект комп'ютерної мережі, у рамках якої було проведено додавання трьох додаткових робочих станцій, котрі

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				150
Змн.	Арк.	№ докум.	Підпис	Дата		

імітуватимуть роботу DNS-сервера, а також трьох HTTP-серверів. Приклад наведено на рисунку 2.6.67 нижче.



Рисунок 2.6.67 – Тестовий стенд з підключеними імітація глобальних ресурсів у вигляді трьох робочих станцій

Виконуємо підключення у ролі користувача VLAN12. Відповідно до проведених нами раніше налаштувань, користувачі даної підмережі VLAN мають заблокований доступ до інтернет ресурсів «viber.com», «facebook.com» та «youtube.com». У якості демонстрації, було створено 3 записи про деякі доменні ім'я на сервері, що імітує роботу DNS-сервера у мережі провайдера. Їх наведено на рисунку нижче.

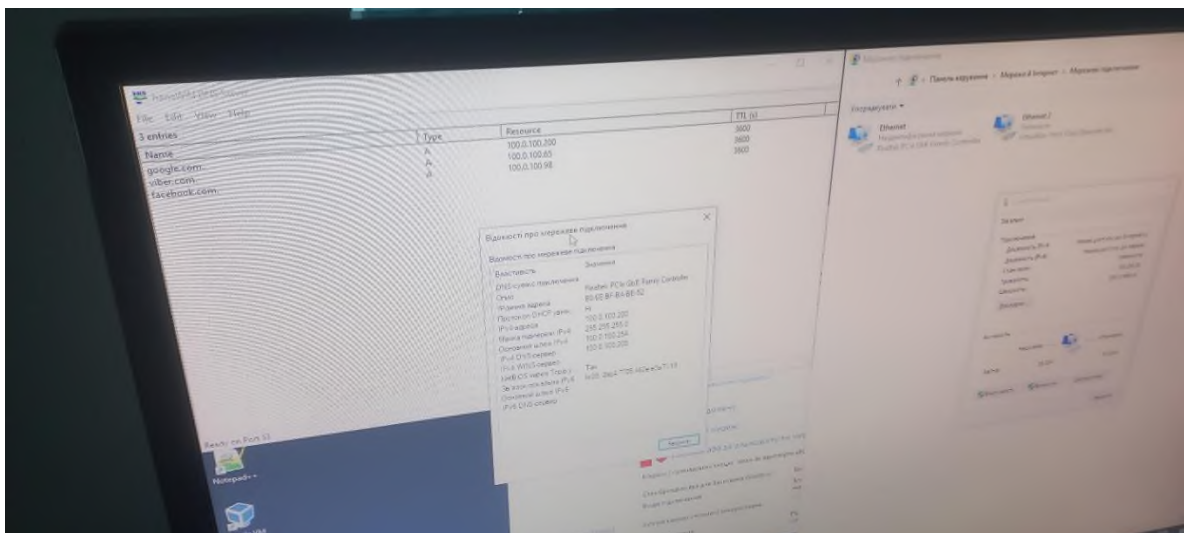


Рисунок 2.6.68 – Приклад створеного DNS-сервера на базі одного з глобальних вузлів у тестовому стенді. Створі 3 записи типу «А» про деякі доменні імена вузлів

На даному етапі, оглянемо роботу засобів фільтрації мережевого трафіку, а саме списків контролю доступу, що працюють на основі FQDN. Саме на основі їх роботи і забезпечується блокування мережевого трафіку шляхом опитування відданого DNS-сервера та створення динамічних правил блокування мережевого трафіку. Результати перевірки наведено на рисунку 2.6.69 нижче.

```

- PuTTY
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224
fqdn facebook.com (resolved) log informational interval 300 0xd4b000b
<--- More --->
*****WARNING*****WARNING*****WARNING*****
Mate version 9.1(5) is not identical with ours 9.1(2)
*****WARNING*****WARNING*****WARNING*****
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224 fqdn youtube.com (unresolved) log informational interval 300 (inactive) 0x9b344508
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224 fqdn viber.com (resolved) log informational interval 300 0x62871c3f
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224 host 100.0.100.98 (facebook.com) log informational interval 300 (hitcnt=0) 0xa6e2c7c7
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224 host 100.0.100.65 (viber.com) log informational interval 300 (hitcnt=0) 0xc82c1dcc
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224 object-group block-access log informational interval 300 (hitcnt=0) 0xd06a18ef
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224 fqdn facebook.com (resolved) log informational interval 300 0x211d6b86
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224 fqdn youtube.com (unresolved) log informational interval 300 (inactive) 0x01d36d0e
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224 fqdn viber.com (resolved) log informational interval 300 0x8c9dadd0
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224 host 100.0.100.98 (facebook.com) log informational interval 300 (hitcnt=0) 0xb7e715221
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224 host 100.0.100.65 (viber.com) log informational interval 300 (hitcnt=0) 0x53a4a63e
access-list Network-Services line 4 extended permit ip any any (hitcnt=1059) 0xada940d9
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)# show access-list Network-Services
access-list Network-Services; 16 elements; name hash: 0xd3af255f
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224 object-group block-access log informational interval 300 (hitcnt=0) 0x8630e503
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224 fqdn facebook.com (resolved) log informational interval 300 0x46dd79bb
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224 fqdn youtube.com (unresolved) log informational interval 300 (inactive) 0xb5f857c1
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224 fqdn viber.com (resolved) log informational interval 300 0x17fc9735
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224 host 100.0.100.98 (facebook.com) log informational interval 300 (hitcnt=0) 0x583ed7b0
access-list Network-Services line 1 extended deny ip 172.16.1.0 255.255.255.224 host 100.0.100.65 (viber.com) log informational interval 300 (hitcnt=0) 0xb389b7de
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224 object-group block-access log informational interval 300 (hitcnt=0) 0x36120d10
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224 fqdn facebook.com (resolved) log informational interval 300 0xd4b000b
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224 fqdn youtube.com (unresolved) log informational interval 300 (inactive) 0x9b344508
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224 fqdn viber.com (resolved) log informational interval 300 0x62871c3f
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224 host 100.0.100.98 (facebook.com) log informational interval 300 (hitcnt=0) 0xa6e2c7c7
access-list Network-Services line 2 extended deny ip 172.16.1.32 255.255.255.224 host 100.0.100.65 (viber.com) log informational interval 300 (hitcnt=0) 0xc82c1dcc
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224 object-group block-access log informational interval 300 (hitcnt=0) 0xd06a18ef
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224 fqdn facebook.com (resolved) log informational interval 300 0x211d6b86
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224 fqdn youtube.com (unresolved) log informational interval 300 (inactive) 0x01d36d0e
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224 fqdn viber.com (resolved) log informational interval 300 0x8c9dadd0
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224 host 100.0.100.98 (facebook.com) log informational interval 300 (hitcnt=0) 0xb7e715221
access-list Network-Services line 3 extended deny ip 172.16.1.64 255.255.255.224 host 100.0.100.65 (viber.com) log informational interval 300 (hitcnt=0) 0x53a4a63e
access-list Network-Services line 4 extended permit ip any any (hitcnt=1059) 0xada940d9
ASA-5512X/pri/act(config)#
ASA-5512X/pri/act(config)#

```

Рисунок 2.6.69 – Списки контролю доступу, що були автоматично сконфігурованими на основі інформації про IP-адреси глобальних вузлів за запитами DNS-Request

Як можемо побачити, було отримано IP-адреси ресурсів, що мають попадати під заборону, на основі яких і було створено правила у списках контролю доступу для користувачів тих чи інших локальних підмереж. Ці IP-адреси представлені у вигляді *100.0.100.98*, що відповідає ресурсу «*facebook.com*», а також *100.0.100.65*, що відповідає ресурсу «*viber.com*». Для демонстрації роботи засобів фільтрації цього буде цілком достатньо.

Виконуємо фактичне тестування. Під'єднуємося у ролі користувача деякої VLAN підмережі, що наведені нижче, та починаємо виконувати спроби отримання доступу до даних мережевих ресурсів, котрі були заздалегіть налагодженими та протестованими на доступність з іншого мережевого вузла. Таким чином, отримані результати для користувачів різних VLAN підмереж наведено на рисунках нижче.

Для користувачів VLAN 12:

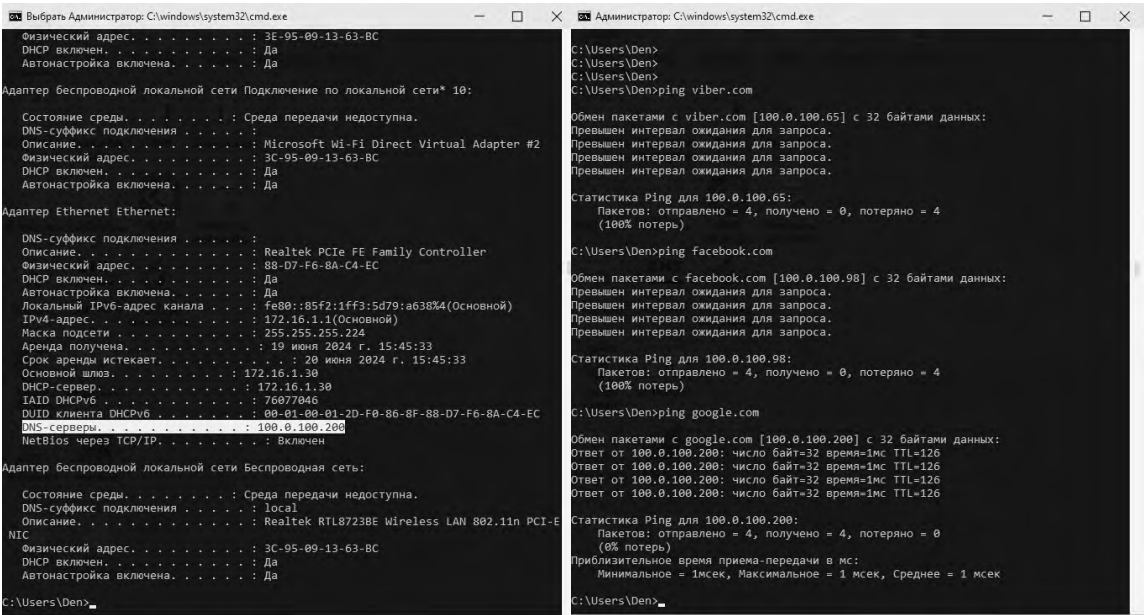


Рисунок 2.6.70 – Результат успішного тестування засобів фільтрації мережевого трафіку для вузла підмереж VLAN 12. Підмережа 172.16.1.0/27

Для користувачів VLAN 13:

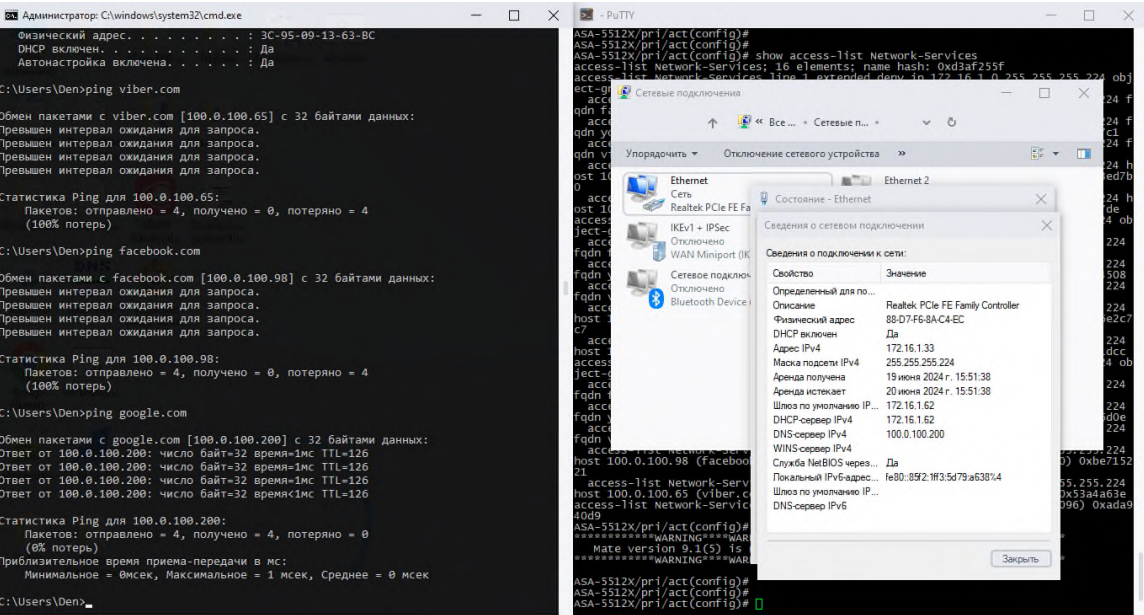


Рисунок 2.6.71 – Результат успішного тестування засобів фільтрації мережевого трафіку для вузла підмереж VLAN 13. Підмережа 172.16.1.32/27

Для користувачів VLAN 14:

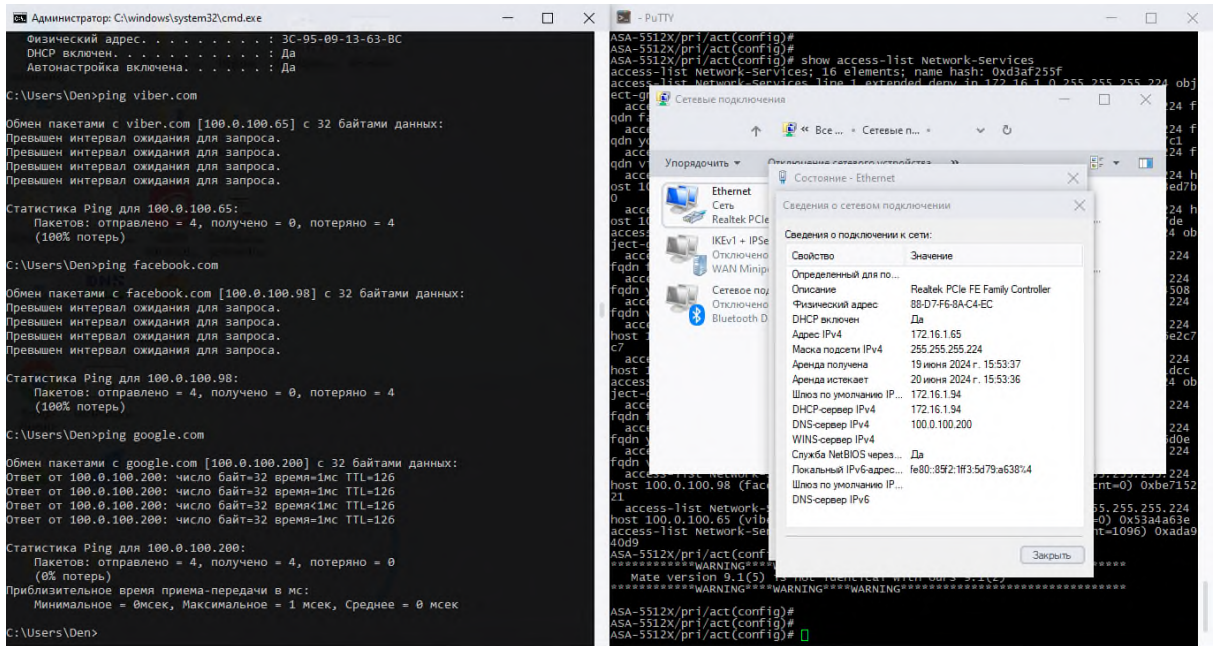


Рисунок 2.6.72 – Результат успішного тестування засобів фільтрації мереже-
вого трафіку для вузла підмереж VLAN 14. Підмережа 172.16.1.64/27

Для користувачів VLAN 15:

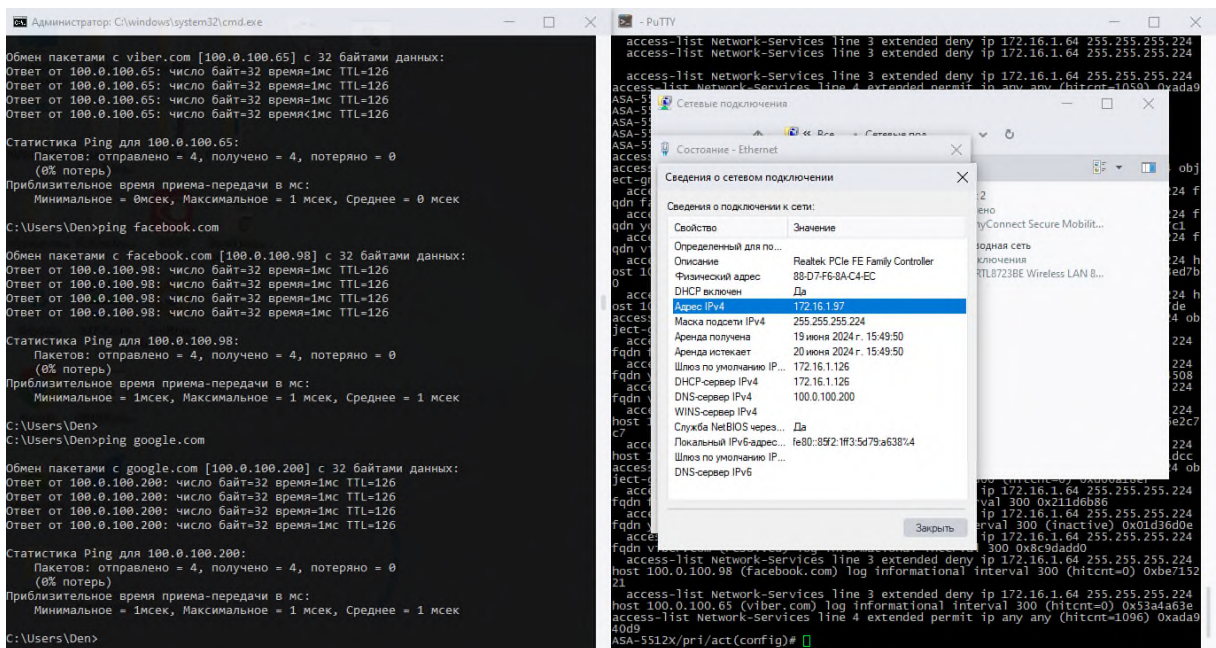


Рисунок 2.6.73 – Результат успішного тестування засобів фільтрації мереже-
вого трафіку для вузла підмереж VLAN 15. Підмережа 172.16.1.96/27

Для користувачів VLAN 16:

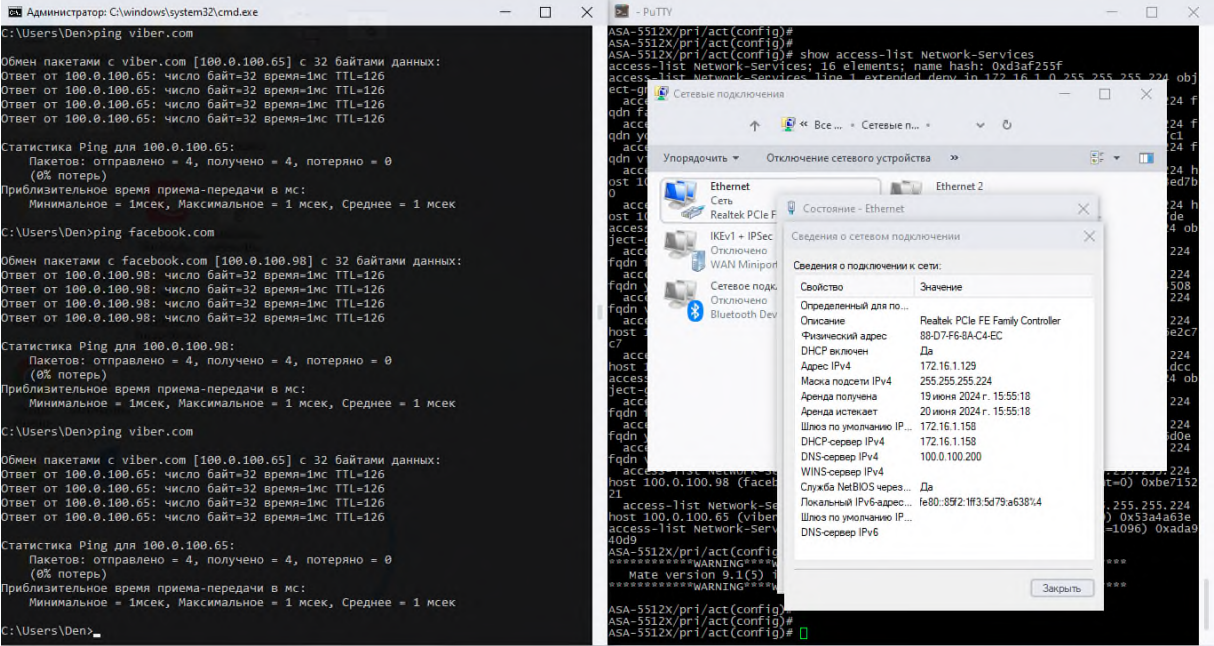


Рисунок 2.6.74 – Результат успішного тестування засобів фільтрації мережевого трафіку для вузла підмереж VLAN 16. Підмережа 172.16.1.128/27

Для кращого розуміння, за результатами тестувань було побудовано таблицю 2.6.1 наявних доступів за доменними ім'ями для наведених вище підмереж VLAN.

Таблиця 2.6.1 – Зведені результати тестування засобів фільтрації доступу

Назва\ Домен	Google.com	Facebook.com	Viber.com
VLAN 12	✓	✗	✗
VLAN 13	✓	✗	✗
VLAN 14	✓	✗	✗
VLAN 15	✓	✓	✓
VLAN 16	✓	✓	✓

В ході виконання вище відзначеного тестування, успішна робота засобів фільтрації мережевого трафіку до ресурсів глобальної мережі на основі FQDN була підтверджена. В результаті проведеного налаштування, було забезпечено роботу зручного інструменту керування доступу до інтернет ресурсів з повним блокування можливостей інформаційного обміну з цими ресурсами, котра працюють у динамічному режимі. За необхідності, проводячи модифікації об'єкту мережі, у якому було виконанно визначення доменних імен, що підпадають під блокування, додаючи

до нього нові об'єкти FQDN, їх буде автоматично додано до списку контролю доступу, що їх блокує.

Далі, було виконано налагодження та тестування роботи локального сервера DNS для забезпечення зручної роботи з ресурсами локальної мережі. Приклади побудови та тестування наведені на рисунках 2.6.75 та 2.6.76 нижче.

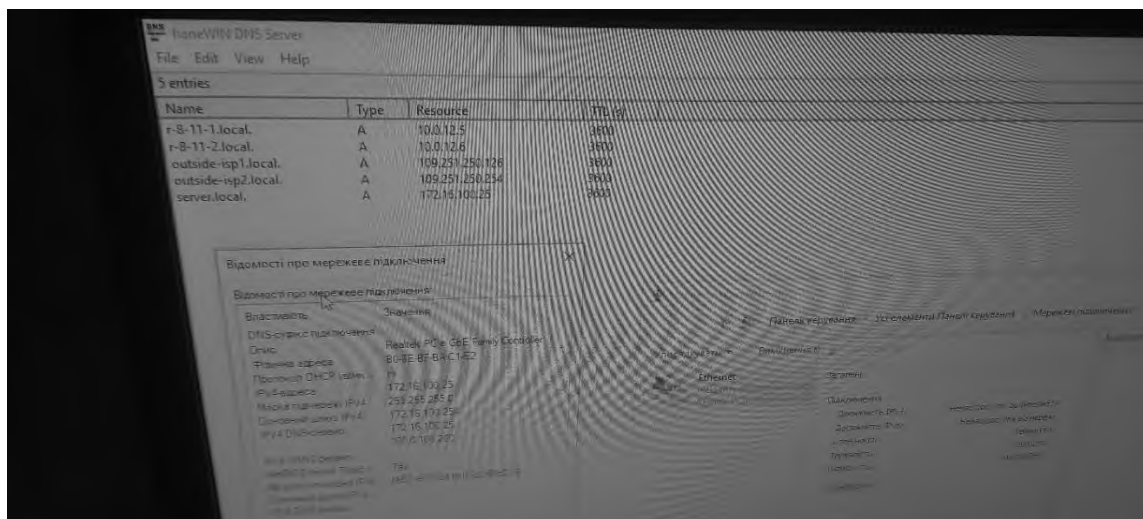


Рисунок 2.6.75 – Локальний DNS сервера на базі сервера 172.16.100.25. Кілька записів типу «А» відповідаю локальним вузлам для зручності взаємодії з ними

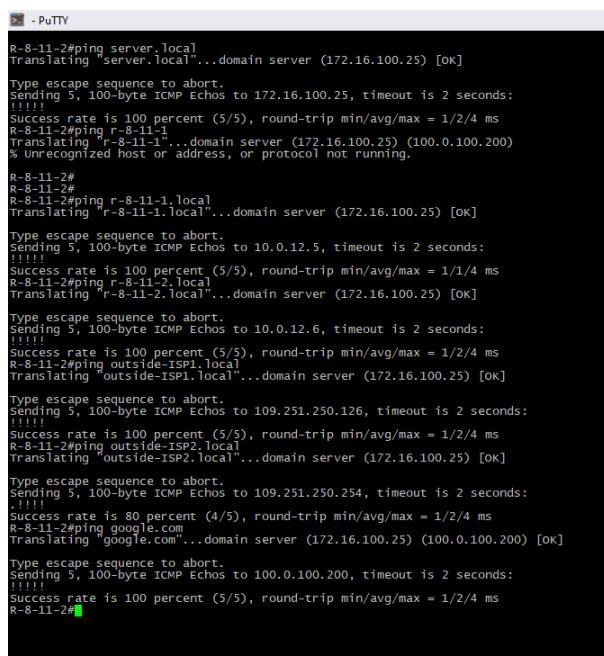


Рисунок 2.6.76 – Результат успішного тестування роботи локального DNS сервера у вигляді вузла 172.16.100.25. Інформаційний обмін на основі домених імен є можливим та перевіреним

За результатами проведеного тестування, робота локального DNS-сервера була успішно підтвердженою.

На цьому виконання тестувань працеспроможності проекту, котрий покликаний забезпечувати ті чи інші раніше відзначені та описані потреби у технічному завданні, є виконаними. За результатами проведеного тестування, було підтверджено високу надійність та ефективність роботи проекту комп'ютерної мережі. Він здатний забезпечувати покладені на нього потреби та є основою для подальшого розширення та введення додаткових функцій, сервісів чи засобів безпеки експлуатації комп'ютерних систем та мереж.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				157
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи бакалавра, було проведено покращення та посилення власних навичок та вмінь, щодо роботи з комп'ютерними мережами, а також засобами забезпечення їх високої доступності, надійності та безпеки. Виконуючи проектування, було продемонстровано теоритичний та практичний матеріал, що був набути за результатами навчання, а також власних зусиль щодо вивчення теоритичного та практичного матеріалу.

За результатами роботи, було побудовано проект високонадійного захищеного мультипровайдерного Інтернет-підключення кампусної мережі організації, що базується на основі ряду технологій, котрі в комібнації своєї роботи і створюють по справжньому надійну та відмовостійку роботу комп'ютерної мережі.

Проводячи процес проектування, було проведено дослідження різних технологій, що були тим чи іншим чином висвітлені у теоритичній частині виконання проект. Це дозволило отримати уявлення про роботу тих чи інших технологій комп'ютерних мережей, котрі згодом були успішно впровадженими та протестованими в ході виконання практичної частини. За результатами великого обсягу тестувань, що було проведено на основі реального тестового стенду, котрий відображає роботи проекту комп'ютерної мережі після його побудови та налаштування, за дещо спрощеною моделю, котра ніяк не впливає на роботу основних технологій та протоколів, було проведено, як відлагодження роботи тих чи інших технологій, так і підтверджено та продемонстровано високий рівень пропрацьованості для даного проетку.

За результатами проведеного процесу проектування високонадійної захищеної комп'ютерної мережі з застосуванням мультипровайдерного Інтернет-підключення кампусної мережі організації було отримано закінчений проект комп'ютерної мережі, котрий здатний успішно виконувати завдання, що були чітко сформованими та поставленими у технічному завданні, а також може бути використаний як основа для подальшого допрацьовування та впровадження більш спеціалізованих та необхідних програмних та технічних рішень, щодо використання технологій, протоколів чи різних сервісів.

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		158

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. CLI Book 1: Cisco Secure Firewall ASA Series General Operations CLI Configuration Guide, 9.19. Failover for High Availability. [Електронний ресурс]. – 2024 – Режим доступу: <https://www.cisco.com/c/en/us/td/docs/security/asa/asa919/configuration/general/asa-919-general-config/ha-failover.html>
2. IP Application Services Configuration Guide, Cisco IOS Release 15M&T. Configuring Enhanced Object Tracking [Електронний ресурс]. – 2024 – Режим доступу: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp/configuration/15-mt/iap-15-mt-book/iap-eot.html>
3. The Cisco Learning Network. IP SLA Fundamentals. [Електронний ресурс]. – 2024 – Режим доступу: <https://learningnetwork.cisco.com/s/blogs/a0D3i000002SKN0EAO/ip-sla-fundamentals>
4. Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6. Configuring OSPF. [Електронний ресурс]. – 2024 – Режим доступу: https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/route_ospf.html
5. Cisco Security Appliance Command Line Configuration Guide, Version 7.2. Configuring Failover. [Електронний ресурс]. – 2024 – Режим доступу: https://www.cisco.com/c/en/us/td/docs/security/asa/asa72/configuration/guide/conf_gd/failover.html#wp1075905
6. Networking Engineering. Dual ASA5510 with dual ISP failover. [Електронний ресурс]. – 2024 – Режим доступу: <https://networkengineering.stackexchange.com/questions/10560/dual-asa5510-with-dual-isp-failover>
7. Cisco Community. Active/standby asa with dual ISP connections. [Електронний ресурс]. – 2024 – Режим доступу: <https://community.cisco.com/t5/network-security/active-standby-asa-with-dual-isp-connections/td-p/3048960>

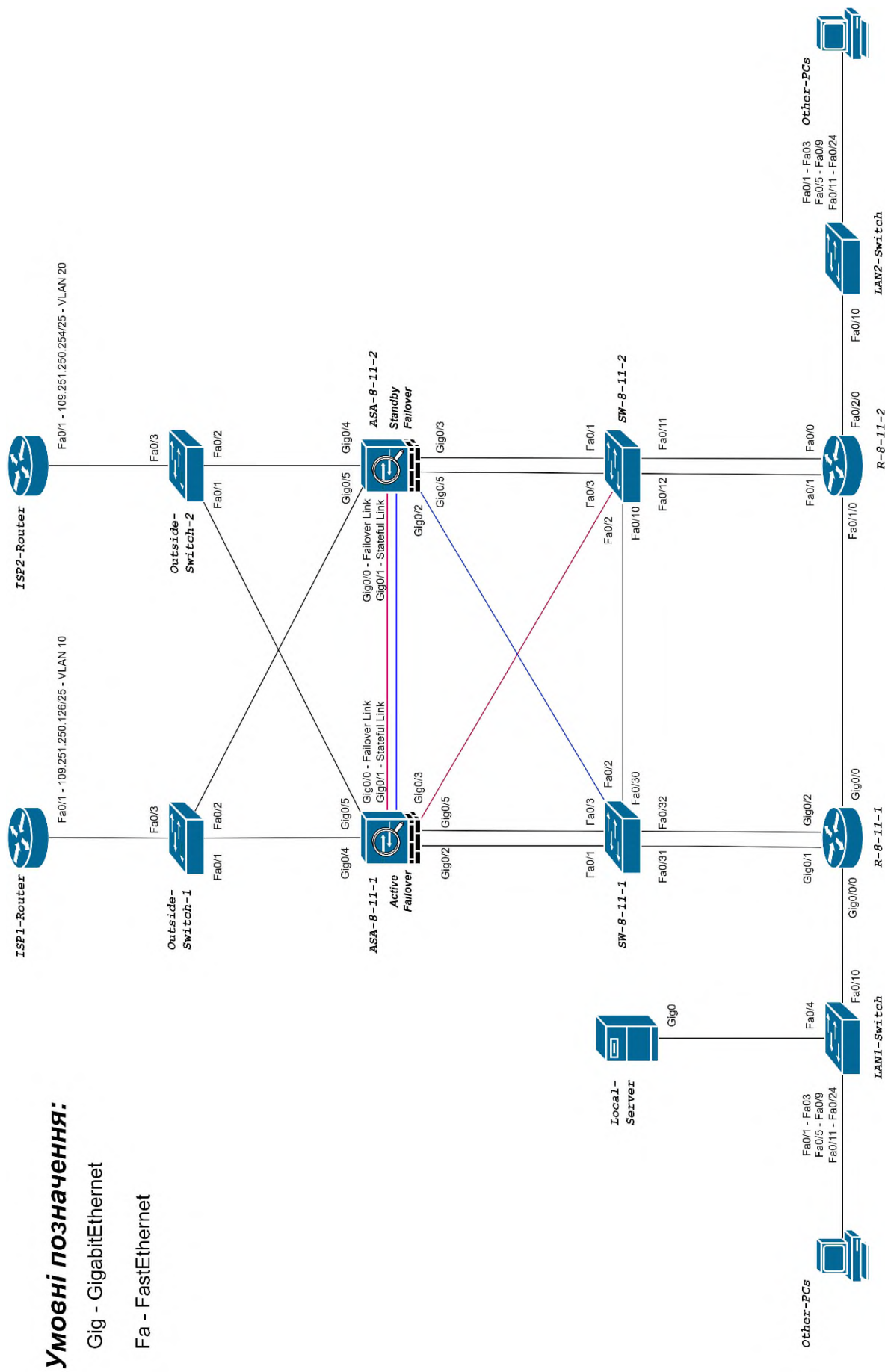
		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		159

8. Cisco Community. Dual ISP, Active/Standby ASA, and RA VPN. [Електроний ресурс]. – 2024 – Режим доступу: <https://community.cisco.com/t5/vpn/dual-isp-active-standby-asa-and-ra-vpn/td-p/2649822>
9. Traffic redirection and failover of ASA with multiple ISPs. [Електроний ресурс]. – 2024 – Режим доступу: <https://networkengineering.stackexchange.com/questions/64885/traffic-redirection-and-failover-of-asa-with-multiple-isps>
10. Experts exchange. Full redundant WAN design, Multiple ISP with failover in asa [Електроний ресурс]. – 2024 – Режим доступу: <https://www.experts-exchange.com/questions/27386694/full-redundant-wan-design-Multiple-ISP-with-fail-over-in-asa.html>
11. Configure OSPF with Multi-Area Adjacency. [Електроний ресурс]. – 2024 – Режим доступу: <https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/118879-configure-ospf-00.html>
12. Автор: Doctor Networks. ASA Active/Standby Failover - Detailed Lab. [Електроний ресурс]. – 2024 – Режим доступу: <https://www.youtube.com/watch?v=fcdeYdtJ2Ck&t=3232s>
13. Термінальний програмний додаток PuTTY. [Електроний ресурс]. – 2024 – Режим доступу: <https://putty.org/>
14. Конфігураційний посібник для Cisco ASA. [Електроний ресурс]. – 2024 – Режим доступу: <https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/products-installation-and-configuration-guides-list.html>
15. Chapter: Configuring Network Object NAT. [Електроний ресурс]. – 2024 – Режим доступу: https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/nat_objects.html
16. Configure ASA Version 9 Port Forwarding with NAT. [Електроний ресурс]. – 2024 – Режим доступу: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/118996-config-asa-00.html>

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				160
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				161
Змн.	Арк.	№ докум.	Підпис	Дата		



Умовні позначення:
Gig - GigabitEthernet
Fa - FastEthernet

Додаток Б – Параметри IP-адресації проекту

Таблиця 1 – Таблиця кількості вузлів у підмережах проекту

Назва підмережі	Кількість вузлів	Призначення
Підмережа А	2	Канал зв'язку між ASA-8-11-1 та ASA-8-11-2 (Failove link)
Підмережа В	2	Канал зв'язку між ASA-8-11-1 та ASA-8-11-2 (State link)
Підмережа С	5	Канал зв'язку між R-8-11-1, ASA-8-11-1 та ASA-8-11-2, VLAN інтерфейси для SW-8-11-1 та SW-8-11-2
Підмережа D	5	Канал зв'язку між R-8-11-2, ASA-8-11-1 та ASA-8-11-2, VLAN інтерфейси для SW-8-11-1 та SW-8-11-2
Підмережа Е	6	Канал зв'язку між R-8-11-1, R-8-11-2, ASA-8-11-1 та ASA-8-11-2, VLAN інтерфейси для SW-8-11-1 та SW-8-11-2
Підмережа F	2	Канал зв'язку між R-8-11-1 та R-8-11-2
Підмережа VLAN12-1	30	Підмережа VLAN 12 для користувачів локальної підмережі (маршрутизатор R-8-11-1)
Підмережа VLAN13-1	30	Підмережа VLAN 13 для користувачів локальної підмережі (маршрутизатор R-8-11-1)
Підмережа VLAN14-1	30	Підмережа VLAN 14 для користувачів локальної підмережі (маршрутизатор R-8-11-1)
Підмережа VLAN15-1	30	Підмережа VLAN 15 для користувачів локальної підмережі (маршрутизатор R-8-11-1)
Підмережа VLAN16-1	30	Підмережа VLAN 16 для користувачів локальної підмережі (маршрутизатор R-8-11-1)
Підмережа VLAN12-2	30	Підмережа VLAN 12 для користувачів локальної підмережі (маршрутизатор R-8-11-2)
Підмережа VLAN13-2	30	Підмережа VLAN 13 для користувачів локальної підмережі (маршрутизатор R-8-11-2)
Підмережа VLAN14-2	30	Підмережа VLAN 14 для користувачів локальної підмережі (маршрутизатор R-8-11-2)
Підмережа VLAN15-2	30	Підмережа VLAN 15 для користувачів локальної підмережі (маршрутизатор R-8-11-2)
Підмережа VLAN16-2	30	Підмережа VLAN 16 для користувачів локальної підмережі (маршрутизатор R-8-11-2)
Підмережа серверів VLAN100	254	Підмережа VLAN 100 для розміщення серверів в локальній мережі

Таблиця 2 – Параметри IP-адресації для підмережі А

Параметри IP-адреси мережі А		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.00000000	255.255.255.0
Інвертована маска	00000000.00000000.00000000.11111111	0.0.0.255
IP-адреса мережі	11000000.10101000.00000001.00000000	192.168.1.0
Мінімальна IP-адреса вузла	11000000.10101000.00000001.00000001	192.168.1.0
Максимальна IP-адреса вузла	11000000.10101000.00000001.11111110	192.168.1.254

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		163

Широкомовна IP-адреса	11000000.10101000.00000001.11111111	192.168.1.255
Кількість вузлів в мережі	11111110	254

Таблиця 3 – Параметри IP-адресації для підмережі В

Параметри IP-адреси мережі В		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.00000000	255.255.255.0
Інвертована маска	00000000.00000000.00000000.11111111	0.0.0.255
IP-адреса мережі	11000000.10101000.00000010.00000000	192.168.2.0
Мінімальна IP-адреса вузла	11000000.10101000.00000010.00000001	192.168.2.0
Максимальна IP-адреса вузла	11000000.10101000.00000010.11111110	192.168.2.254
Широкомовна IP-адреса	11000000.10101000.00000010.11111111	192.168.2.255
Кількість вузлів в мережі	11111110	254

Таблиця 4 – Параметри IP-адресації для підмережі С

Параметри IP-адреси мережі С		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11111000	255.255.255.248
Інвертована маска	00000000.00000000.00000000.00000111	0.0.0.7
IP-адреса мережі	00001010.00000000.00000001.00000000	10.0.1.0
Мінімальна IP-адреса вузла	00001010.00000000.00000001.00000001	10.0.1.1
Максимальна IP-адреса вузла	00001010.00000000.00000001.00000110	10.0.1.6
Широкомовна IP-адреса	00001010.00000000.00000001.00000111	10.0.1.7
Кількість вузлів в мережі	110	6

Таблиця 5 – Параметри IP-адресації для підмережі D

Параметри IP-адреси мережі D		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11111000	255.255.255.248
Інвертована маска	00000000.00000000.00000000.00000111	0.0.0.7
IP-адреса мережі	00001010.00000000.00000010.00000000	10.0.2.0
Мінімальна IP-адреса вузла	00001010.00000000.00000010.00000001	10.0.2.1
Максимальна IP-адреса вузла	00001010.00000000.00000010.00000110	10.0.2.6
Широкомовна IP-адреса	00001010.00000000.00000010.00000111	10.0.2.7
Кількість вузлів в мережі	110	6

Таблиця 6 – Параметри IP-адресації для підмережі E

Параметри IP-адреси мережі E		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11111000	255.255.255.248
Інвертована маска	00000000.00000000.00000000.00000111	0.0.0.7
IP-адреса мережі	00001010.00000000.00001100.00000000	10.0.12.0
Мінімальна IP-адреса вузла	00001010.00000000.00001100.00000001	10.0.12.1

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				164
Змн.	Арк.	№ докум.	Підпис	Дата		

Максимальна IP-адреса вузла	00001010.00000000.00001100.00000110	10.0.12.6
Широкомовна IP-адреса	00001010.00000000.00001100.00000111	10.0.12.7
Кількість вузлів в мережі	110	6

Таблиця 7 – Параметри IP-адресації для підмережі F

Параметри IP-адреси мережі F		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11111100	255.255.255.252
Інвертована маска	00000000.00000000.00000000.00000011	0.0.0.3
IP-адреса мережі	00001010.00000000.00000011.00000000	10.0.3.0
Мінімальна IP-адреса вузла	00001010.00000000.00000011.00000001	10.0.3.1
Максимальна IP-адреса вузла	00001010.00000000.00000011.00000010	10.0.3.2
Широкомовна IP-адреса	00001010.00000000.00000011.00000011	10.0.3.3
Кількість вузлів в мережі	10	2

Таблиця 8 – Параметри IP-адресації для підмережі VLAN12-1

Параметри IP-адреси мережі VLAN12-1		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000001.00000000	172.16.1.0
Мінімальна IP-адреса вузла	10101100.00010000.00000001.00000001	172.16.1.1
Максимальна IP-адреса вузла	10101100.00010000.00000001.00011110	172.16.1.30
Широкомовна IP-адреса	10101100.00010000.00000001.00011111	172.16.1.31
Кількість вузлів в мережі	11110	30

Таблиця 9 – Параметри IP-адресації для підмережі VLAN13-1

Параметри IP-адреси мережі VLAN13-1		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000001.00100000	172.16.1.32
Мінімальна IP-адреса вузла	10101100.00010000.00000001.00100001	172.16.1.33
Максимальна IP-адреса вузла	10101100.00010000.00000001.00111110	172.16.1.62
Широкомовна IP-адреса	10101100.00010000.00000001.00111111	172.16.1.63
Кількість вузлів в мережі	11110	30

Таблиця 10 – Параметри IP-адресації для підмережі VLAN14-1

Параметри IP-адреси мережі VLAN14-1		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000001.01000000	172.16.1.64

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				165
Змн.	Арк.	№ докум.	Підпис	Дата		

Мінімальна IP-адреса вузла	10101100.00010000.00000001.01000001	172.16.1.65
Максимальна IP-адреса вузла	10101100.00010000.00000001.01011110	172.16.1.94
Широкомовна IP-адреса	10101100.00010000.00000001.01011111	172.16.1.95
Кількість вузлів в мережі	11110	30

Таблиця 11 – Параметри IP-адресації для підмережі VLAN15-1

Параметри IP-адреси мережі VLAN15-1		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000001.01100000	172.16.1.96
Мінімальна IP-адреса вузла	10101100.00010000.00000001.01100001	172.16.1.97
Максимальна IP-адреса вузла	10101100.00010000.00000001.01111110	172.16.1.126
Широкомовна IP-адреса	10101100.00010000.00000001.01111111	172.16.1.127
Кількість вузлів в мережі	11110	30

Таблиця 12 – Параметри IP-адресації для підмережі VLAN16-1

Параметри IP-адреси мережі VLAN16-1		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000001.10000000	172.16.1.128
Мінімальна IP-адреса вузла	10101100.00010000.00000001.10000001	172.16.1.129
Максимальна IP-адреса вузла	10101100.00010000.00000001.10011110	172.16.1.158
Широкомовна IP-адреса	10101100.00010000.00000001.10011111	172.16.1.159
Кількість вузлів в мережі	11110	30

Таблиця 13 – Параметри IP-адресації для підмережі VLAN12-2

Параметри IP-адреси мережі VLAN12-2		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000010.00000000	172.16.2.0
Мінімальна IP-адреса вузла	10101100.00010000.00000010.00000001	172.16.2.1
Максимальна IP-адреса вузла	10101100.00010000.00000010.00011110	172.16.2.30
Широкомовна IP-адреса	10101100.00010000.00000010.00011111	172.16.2.31
Кількість вузлів в мережі	11110	30

Таблиця 14 – Параметри IP-адресації для підмережі VLAN13-2

Параметри IP-адреси мережі VLAN13-2		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.00011111	0.0.0.31

IP-адреса мережі	10101100.00010000.00000010.00100000	172.16.2.32
Мінімальна IP-адреса вузла	10101100.00010000.00000010.001 00001	172.16.2.33
Максимальна IP-адреса вузла	10101100.00010000.00000010.001 11110	172.16.2.62
Широкомовна IP-адреса	10101100.00010000.00000010.001 11111	172.16.2.63
Кількість вузлів в мережі	11110	30

Таблиця 15 – Параметри IP-адресації для підмережі VLAN14-2

Параметри IP-адреси мережі VLAN14-2		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.000 11111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000010.01000000	172.16.2.64
Мінімальна IP-адреса вузла	10101100.00010000.00000010.01 000001	172.16.2.65
Максимальна IP-адреса вузла	10101100.00010000.00000010.01 011110	172.16.2.94
Широкомовна IP-адреса	10101100.00010000.00000010.01 011111	172.16.2.95
Кількість вузлів в мережі	11110	30

Таблиця 16 – Параметри IP-адресації для підмережі VLAN15-2

Параметри IP-адреси мережі VLAN15-2		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.000 11111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000010.01100000	172.16.2.96
Мінімальна IP-адреса вузла	10101100.00010000.00000010.01 100001	172.16.2.97
Максимальна IP-адреса вузла	10101100.00010000.00000010.01 111110	172.16.2.126
Широкомовна IP-адреса	10101100.00010000.00000010.01 111111	172.16.2.127
Кількість вузлів в мережі	11110	30

Таблиця 17 – Параметри IP-адресації для підмережі VLAN16-2

Параметри IP-адреси мережі VLAN16-2		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.11100000	255.255.255.224
Інвертована маска	00000000.00000000.00000000.000 11111	0.0.0.31
IP-адреса мережі	10101100.00010000.00000010.10000000	172.16.2.128
Мінімальна IP-адреса вузла	10101100.00010000.00000010.10 000001	172.16.2.129
Максимальна IP-адреса вузла	10101100.00010000.00000010.10 011110	172.16.2.158
Широкомовна IP-адреса	10101100.00010000.00000010.10 011111	172.16.2.159
Кількість вузлів в мережі	11110	30

Таблиця 18 – Параметри IP-адресації для підмережі VLAN100

Параметри IP-адреси мережі VLAN100		
	Двійкове представлення	Десяткове представлення
Маска мережі	11111111.11111111.11111111.00000000	255.255.255.0

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		167

Інвертована маска	00000000.00000000.00000000. 11111111	0.0.0.255
IP-адреса мережі	10101100.00010000.01100100.00000000	172.16.100.0
Мінімальна IP-адреса вузла	10101100.00010000.01100100. 00000001	172.16.100.1
Максимальна IP-адреса вузла	10101100.00010000.01100100. 11111110	172.16.100.254
Широкомовна IP-адреса	10101100.00010000.01100100. 11111111	172.16.100.255
Кількість вузлів в мережі	11111110	254

Таблиця 19 – Таблиця розподілу адресного простору

Підмережа/ Пристрій	Інтерфейс/Мережний адаптер/Шлюз	IP-адреса	Маска підме- режі	Пре фікс
Мережа А	-	192.168.1.0	255.255.255.0	/24
ASA-8-11-1	GigabitEthernet0/0	192.168.1.100	255.255.255.0	/24
ASA-8-11-2	GigabitEthernet0/0	192.168.1.101	255.255.255.0	/24
Мережа В	-	192.168.2.0	255.255.255.0	/24
ASA-8-11-1	GigabitEthernet0/1	192.168.2.100	255.255.255.0	/24
ASA-8-11-2	GigabitEthernet0/1	192.168.2.101	255.255.255.0	/24
Мережа С	-	10.0.1.0	255.255.255.248	/29
ASA-8-11-1	GigabitEthernet0/2	10.0.1.1	255.255.255.248	/29
ASA-8-11-2	GigabitEthernet0/2	10.0.1.2	255.255.255.248	/29
SW-8-11-1	VLAN1	10.0.1.3	255.255.255.248	/29
R-8-11-1	GigabitEthernet0/1	10.0.1.5	255.255.255.248	/29
Мережа D	-	10.0.2.0	255.255.255.248	/29
ASA-8-11-1	GigabitEthernet0/3	10.0.2.1	255.255.255.248	/29
ASA-8-11-2	GigabitEthernet0/3	10.0.2.2	255.255.255.248	/29
SW-8-11-2	VLAN1	10.0.2.4	255.255.255.248	/29
R-8-11-2	FastEthernet0/0	10.0.2.6	255.255.255.248	/29
Мережа Е	-	10.0.2.0	255.255.255.248	/29
ASA-8-11-1	GigabitEthernet0/5	10.0.12.1	255.255.255.248	/29
ASA-8-11-2	GigabitEthernet0/5	10.0.12.2	255.255.255.248	/29
SW-8-11-1	VLAN5	10.0.12.3	255.255.255.248	/29
SW-8-11-2	VLAN5	10.0.12.4	255.255.255.248	/29
R-8-11-1	GigabitEthernet0/2.1	10.0.12.5	255.255.255.248	/29
R-8-11-2	FastEthernet0/1.1	10.0.12.6	255.255.255.248	/29
Мережа F	-	10.0.3.0	255.255.255.252	/30
R-8-11-1	GigabitEthernet0/0	10.0.3.1	255.255.255.252	/30
R-8-11-2	Fast Ethernet0/1/0	10.0.3.2	255.255.255.252	/30
Мережа VLAN12-1	-	172.16.1.0	255.255.255.224	/27
R-8-11-1	GigabitEthernet0/0/0.12	172.16.1.30	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN13-1	-	172.16.1.32	255.255.255.224	/27
R-8-11-1	GigabitEthernet0/0/0.13	172.16.1.62	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN14-1	-	172.16.1.64	255.255.255.224	/27
R-8-11-1	GigabitEthernet0/0/0.14	172.16.1.94	255.255.255.224	/27

Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN15-1	-	172.16.1.96	255.255.255.224	/27
R-8-11-1	GigabitEthernet0/0/0.15	172.16.1.126	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN16-1	-	172.16.1.128	255.255.255.224	/27
R-8-11-1	GigabitEthernet0/0/0.16	172.16.1.158	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27

Продовження таблиці №19

Мережа VLAN12-2	-	172.16.2.0	255.255.255.224	/27
R-8-11-2	GigabitEthernet0/2/0.12	172.16.2.30	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN13-2	-	172.16.2.32	255.255.255.224	/27
R-8-11-2	GigabitEthernet0/2/0.1	172.16.2.62	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN14-2	-	172.16.2.64	255.255.255.224	/27
R-8-11-2	GigabitEthernet0/2/0.1	172.16.2.94	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN15-2	-	172.16.2.96	255.255.255.224	/27
R-8-11-2	GigabitEthernet0/2/0.1	172.16.2.126	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN16-2	-	172.16.2.128	255.255.255.224	/27
R-8-11-2	GigabitEthernet0/2/0.1	172.16.2.158	255.255.255.224	/27
Other-Hosts	DHCP		255.255.255.224	/27
Мережа VLAN100-1	-	172.16.100.254	255.255.255.224	/27
R-8-11-1	GigabitEthernet0/0/0.100	172.16.100.254	255.255.255.0	/24
Srv-8-11-1	GigabitEthernet	172.16.100.25	255.255.255.0	/24

Таблиця 20 – Параметри роботи протоколу DHCP

Вид адрес	Кількість	Діапазон IP-адрес/ Ок-ремі IP-адреси	Адреси DHCP-сервером
Мережа для VLAN12-1			
Динамічні IP-адреси	29	172.16.1.1 – 172.16.1.29	Так, пизначаються
Статичні IP-адреси	1	172.16.1.30	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN13-1			
Динамічні IP-адреси	29	172.16.1.33 – 172.16.1.61	Так, пизначаються
Статичні IP-адреси	1	172.16.1.62	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN14-1			
Динамічні IP-адреси	29	172.16.1.65 – 172.16.1.93	Так, пизначаються

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		169

Статичні IP-адреси	1	172.16.1.94	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN15-1			
Динамічні IP-адреси	29	172.16.1.97 – 172.16.1.125	Так, призначаються
Статичні IP-адреси	1	172.16.1.126	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються

Продовження таблиці №20

Мережа для VLAN16-1			
Динамічні IP-адреси	29	172.16.129. – 172.16.1.157	Так, призначаються
Статичні IP-адреси	1	172.16.1.158	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN12-2			
Динамічні IP-адреси	29	172.16.2.1 – 172.16.2.29	Так, призначаються
Статичні IP-адреси	1	172.16.2.30	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN13-2			
Динамічні IP-адреси	29	172.16.2.33 – 172.16.2.61	Так, призначаються
Статичні IP-адреси	1	172.16.2.62	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN14-2			
Динамічні IP-адреси	29	172.16.2.65 – 172.16.2.93	Так, призначаються
Статичні IP-адреси	1	172.16.2.94	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN15-2			
Динамічні IP-адреси	29	172.16.2.97 – 172.16.2.125	Так, призначаються
Статичні IP-адреси	1	172.16.2.126	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються
Мережа для VLAN16-2			
Динамічні IP-адреси	29	172.16.2.129 – 172.16.2.157	Так, призначаються
Статичні IP-адреси	1	172.16.2.158	Ні, не призначаються
Резервні IP-адреси	0	---	Ні, не призначаються

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		170

Додаток Г – Робота протоколу OSPF

Таблиця 1 – Таблиця метрик інтрефейсів для протоколу OSPF

Вузол	Інтерфейс	Метрика OSPF
R-8-11-1	GigabitEthernet0/1	1
	GigabitEthernet0/2	10
	GigabitEthernet0/0	20
R-8-11-2	FastEthernet0/0	1
	FastEthernet0/1	10
	FastEthernet0/1/0	20
ASA-8-11-1 та ASA-8-11-2	GigabitEthernet0/2	1
	GigabitEthernet0/3	1
	GigabitEthernet0/5	4

Таблиця 2 - Таблиця маршрутизації OSPF

Вузол	Маршрут	Метрика OSPF
<u>Якщо ASA-8-11-1 Failover Active</u>		
R-8-11-1	R-8-11-1(GigabitEthernet0/1) – SW-8-11-1(FastEthernet0/31, FastEthernet0/1) – ASA-8-11-1(GigabitEthernet0/2)	1+1 = 2
R-8-11-1	R-8-11-1(GigabitEthernet0/2) – SW-8-11-1(FastEthernet0/32, FastEthernet0/3) – ASA-8-11-1(GigabitEthernet0/5)	10+1 = 11
	R-8-11-1(GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0, FastEthernet0/0) – SW-8-11-2(FastEthernet0/11, FastEthernet0/2) – ASA-8-11-1(GigabitEthernet0/3)	20+1+1 = 22
	R-8-11-1(GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0, FastEthernet0/1) – SW-8-11-2(FastEthernet0/12, FastEthernet0/10) – SW-8-11-1(FastEthernet0/30, FastEthernet0/3) – ASA-8-11-1(GigabitEthernet0/5)	20+10+1+1 = 32
R-8-11-2	R-8-11-2(FastEthernet0/0) – SW-8-11-2(FastEthernet0/11, FastEthernet0/2) – ASA-8-11-1(GigabitEthernet0/3)	1+1 = 2
	R-8-11-2(FastEthernet0/1) – SW-8-11-2(FastEthernet0/12, FastEthernet0/10) – SW-8-11-1(FastEthernet0/30, FastEthernet0/3) – ASA-8-11-1(GigabitEthernet0/5)	10+1+1 = 12

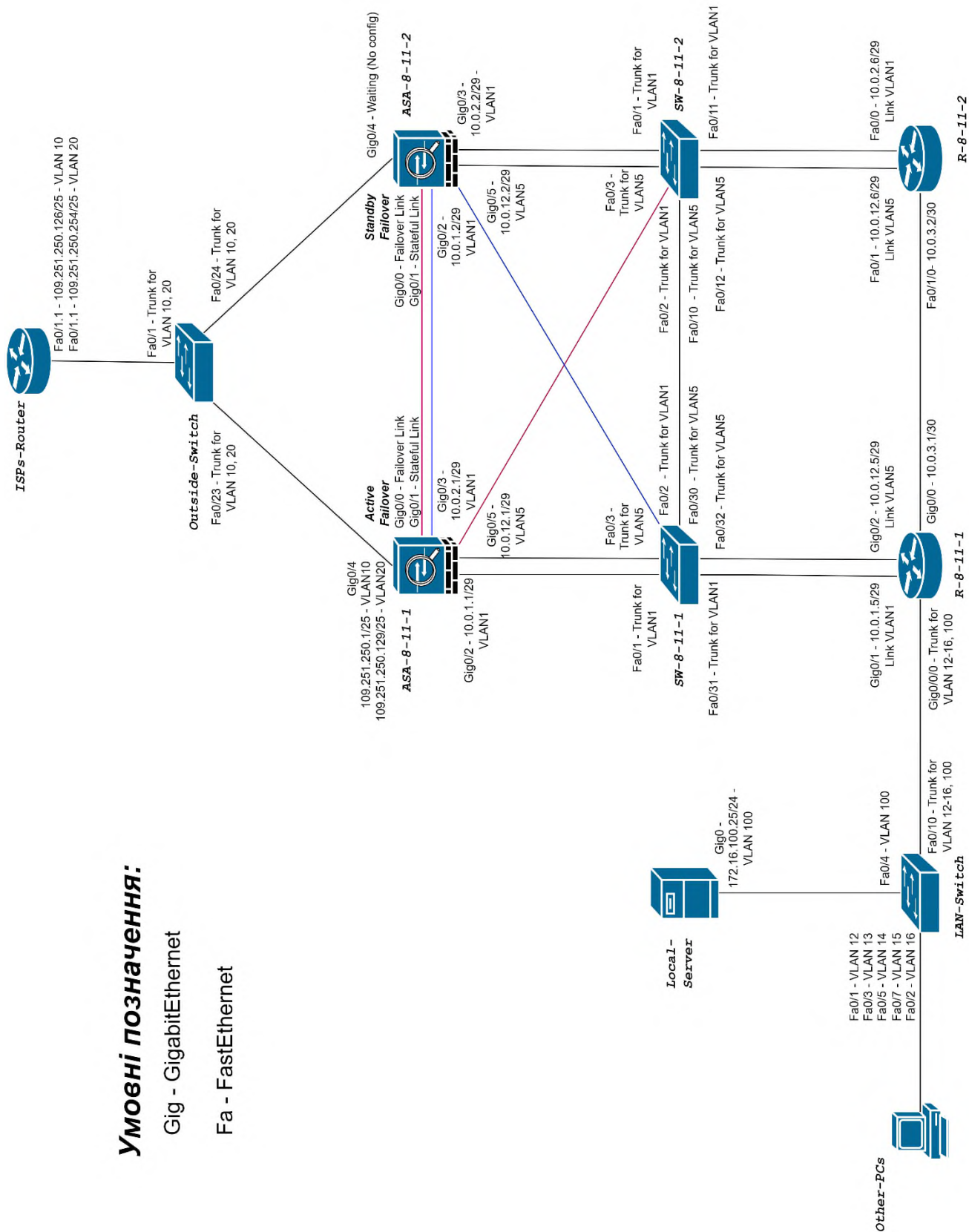
Вузол	Маршрут	Метрика OSPF
<u>Якщо ASA-8-11-1 Failover Active</u>		
R-8-11-2	R-8-11-2(FastEthernet0/1/0) – R-8-11-1(GigabitEthernet0/0, GigabitEthernet0/1) – SW-8-11-1(FastEthernet0/31, FastEthernet0/1) – ASA-8-11-1(GigabitEthernet0/2)	20+1+1 = 22
	R-8-11-2(FastEthernet0/1/0) – R-8-11-1(GigabitEthernet0/0, GigabitEthernet0/2) – SW-8-11-1(FastEthernet0/32, FastEthernet0/3) – ASA-8-11-1(GigabitEthernet0/5)	20+10+1 = 31
<u>Якщо ASA-8-11-2 Failover Active</u>		
R-8-11-1	R-8-11-1(GigabitEthernet0/1) – SW-8-11-1(FastEthernet0/31, FastEthernet0/2) – ASA-8-11-2(GigabitEthernet0/2)	1+1 = 2
	R-8-11-1(GigabitEthernet0/2) – SW-8-11-1(FastEthernet0/32, FastEthernet0/30) – SW-8-11-2(FastEthernet0/10, FastEthernet0/3) – ASA-8-11-2(GigabitEthernet0/5)	10+1+1 = 12
	R-8-11-1(GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0, FastEthernet0/0) – SW-8-11-2(FastEthernet0/11, FastEthernet0/1) – ASA-8-11-2(GigabitEthernet0/3)	20+1+1 = 22
	R-8-11-1(GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0, FastEthernet0/1) – SW-8-11-2(FastEthernet0/12, FastEthernet0/3) – ASA-8-11-2(GigabitEthernet0/5)	20+10+1 = 31
R-8-11-2	R-8-11-2(FastEthernet0/0) – SW-8-11-2(FastEthernet0/11, FastEthernet0/1) – ASA-8-11-2(GigabitEthernet0/3)	1+1 = 2
	R-8-11-2(FastEthernet0/1) – SW-8-11-2(FastEthernet0/12, FastEthernet0/3) – ASA-8-11-2(GigabitEthernet0/5)	10+1 = 11
	R-8-11-2(FastEthernet0/1/0) – R-8-11-1(GigabitEthernet0/0, GigabitEthernet0/1) – SW-8-11-1(FastEthernet0/31, FastEthernet0/2) – ASA-8-11-2(GigabitEthernet0/2)	20+1+1 = 22
	R-8-11-2(GigabitEthernet0/0) – R-8-11-1(GigabitEthernet0/0, GigabitEthernet0/2) – SW-8-11-1(FastEthernet0/32, FastEthernet0/30) – SW-8-11-2(FastEthernet0/10, FastEthernet0/3) – ASA-8-11-2(GigabitEthernet0/5)	20+10+1+1 = 32

Таблиця 3 – Таблиця маршрутизації OSPF для міжмережевих екранів Cisco ASA

Джерело	Призначення	Маршрут	Метрика OSPF
Якщо ASA-8-11-1 Failover Active			
ASA-8-11-1	R-8-11-1	ASA-8-11-1(GigabitEthernet0/2) – SW-8-11-1(FastEthernet0/1, FastEthernet0/31) – R-8-11-1(GigabitEthernet0/1)	1+1=2
		ASA-8-11-1(GigabitEthernet0/5) – SW-8-11-1(FastEthernet0/3, FastEthernet0/32) – R-8-11-1(GigabitEthernet0/2)	5+1=6
		ASA-8-11-1(GigabitEthernet0/3) — SW-8-11-2(FastEthernet0/2, FastEthernet0/11) – R-8-11-2(FastEthernet0/0, FastEthernet0/1/0) – R-8-11-1 (GigabitEthernet0/0)	1+1+20=22
		ASA-8-11-1(GigabitEthernet0/5) – SW-8-11-1(FastEthernet0/3, FastEthernet0/30) – SW-8-11-2(FastEthernet0/10, FastEthernet0/12) – R-8-11-2(FastEthernet0/1, FastEthernet0/1/0) – R-8-11-1 (GigabitEthernet0/0)	1+1+1+20=23
Якщо ASA-8-11-1 Failover Active			
ASA-8-11-1	R-8-11-2	ASA-8-11-1(GigabitEthernet0/3) — SW-8-11-2(FastEthernet0/2, FastEthernet0/11) – R-8-11-2(FastEthernet0/0)	1+1=2
		ASA-8-11-1(GigabitEthernet0/5) — SW-8-11-1(FastEthernet0/3, FastEthernet0/30) – SW-8-11-2(FastEthernet0/10, FastEthernet0/12) – R-8-11-2(FastEthernet0/1)	1+1+1=3
		ASA-8-11-1(GigabitEthernet0/2) — SW-8-11-1(0/1, FastEthernet0/31) – R-8-11-1(GigabitEthernet0/1, GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0)	1+1+20=22
		ASA-8-11-1(GigabitEthernet0/5) — SW-8-11-1(0/3, FastEthernet0/32) – R-8-11-1(GigabitEthernet0/2, GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0)	4+1+20=25

<u>Якщо ASA-8-11-2 Failover Active</u>			
ASA-8-11-2	R-8-11-1	ASA-8-11-2(GigabitEthernet0/2) — SW-8-11-1(FastEthernet0/2, FastEthernet0/31) – R-8-11-1(GigabitEthernet0/1)	1+1=2
		ASA-8-11-2(GigabitEthernet0/5) — SW-8-11-2(FastEthernet0/3, FastEthernet0/10) – SW-8-11-1(FastEthernet0/30, FastEthernet0/32) – R-8-11-1(GigabitEthernet0/2)	1+1+1=3
		ASA-8-11-2(GigabitEthernet0/3) — SW-8-11-2(FastEthernet0/1, FastEthernet0/11) – R-8-11-2(FastEthernet0/0, FastEthernet0/1/0) – R-8-11-1(GigabitEthernet0/0)	1+1+20=22
		ASA-8-11-2(GigabitEthernet0/5) — SW-8-11-2(FastEthernet0/3, FastEthernet0/12) – R-8-11-2(FastEthernet0/1, FastEthernet0/1/0) – R-8-11-1(GigabitEthernet0/0)	4+1+20=25
	R-8-11-2	ASA-8-11-2(GigabitEthernet0/3) – SW-8-11-2(FastEthernet0/1, FastEthernet0/11) – R-8-11-2(FastEthernet0/0)	1+1=2
		ASA-8-11-2(GigabitEthernet0/5) – SW-8-11-2(FastEthernet0/3, FastEthernet0/12) – R-8-11-2(FastEthernet0/1)	5+1=6
		ASA-8-11-2(GigabitEthernet0/2) — SW-8-11-1(FastEthernet0/2, FastEthernet0/31) – R-8-11-1(GigabitEthernet0/1, GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0)	1+1+20=22
		ASA-8-11-2(GigabitEthernet0/5) – SW-8-11-2(FastEthernet0/3, FastEthernet0/10) – SW-8-11-1(FastEthernet0/30, FastEthernet0/32) – R-8-11-1(GigabitEthernet0/2, GigabitEthernet0/0) – R-8-11-2(FastEthernet0/1/0)	1+1+1+20=23

Додаток Д – Спрощена топологія комп’ютерної мережі тестового стенду



Умовні позначення:
Gig - GigabitEthernet
Fa - FastEthernet

--ASA-8-11-1:

```
hostname ASA-5512X
failover lan unit primary
int gig0/0
no shutdown
int gig0/1
no shutdown
exit
failover lan interface FAILOVER gig0/0
failover interface ip FAILOVER 192.168.1.100 255.255.255.0 standby
192.168.1.101
failover link STATE gig0/1
failover interface ip STATE 192.168.2.100 255.255.255.0 standby
192.168.2.101
failover
prompt hostname priority state
int gig0/2
nameif Link-to--R-8-11-1
security-level 100
ip address 10.0.1.1 255.255.255.248 standby 10.0.1.2
ospf cost 1
no shutdown
exit
int gig0/3
nameif Link-to--R-8-11-2
security-level 100
ip address 10.0.2.1 255.255.255.248 standby 10.0.2.2
ospf cost 1
no shutdown
exit
int gig0/4.1
vlan 10
nameif Link-to--ISP-1
ip address 109.251.250.1 255.255.255.128
int gig0/4.2
vlan 20
nameif Link-to--ISP-2
ip address 109.251.250.129 255.255.255.128
int gig0/4
no shut
exit
int gig0/5.1
vlan 5
nameif Link-for--All
security-level 100
ip address 10.0.12.1 255.255.255.248 standby 10.0.12.2
ospf cost 4
```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				176
Змн.	Арк.	№ докум.	Підпис	Дата		

```

int gig0/5
no shut
exit
policy-map global_policy
class inspection_default
inspect icmp
exit
exit
sla monitor 1
type echo protocol ipIcmpEcho 109.251.250.126 interface Link-to--ISP-1
frequency 10
exit
sla monitor schedule 1 life forever start-time now
track 1 rtr 1 reachability
sla monitor 31
type echo protocol ipIcmpEcho 10.0.1.5 interface Link-to--R-8-11-1
frequency 5
exit
sla monitor schedule 31 life forever start-time now
track 31 rtr 31 reachability
sla monitor 32
type echo protocol ipIcmpEcho 10.0.2.6 interface Link-to--R-8-11-2
frequency 5
exit
sla monitor schedule 32 life forever start-time now
track 32 rtr 32 reachability
sla monitor 33
type echo protocol ipIcmpEcho 10.0.12.5 interface Link-for--All
frequency 5
exit
sla monitor schedule 33 life forever start-time now
track 33 rtr 33 reachability
sla monitor 34
type echo protocol ipIcmpEcho 10.0.12.6 interface Link-for--All
frequency 5
exit
sla monitor schedule 34 life forever start-time now
track 34 rtr 34 reachability
route Link-to--ISP-1 0.0.0.0 0.0.0.0 109.251.250.126 1 track 1
route Link-to--ISP-2 0.0.0.0 0.0.0.0 109.251.250.254 2
object network INSIDE-NET1-ISP1
range 0.0.0.0 255.255.255.255
nat (Link-to--R-8-11-1,Link-to--ISP-1) dynamic interface
exit
object network INSIDE-NET1-ISP2
range 0.0.0.0 255.255.255.255
nat (Link-to--R-8-11-1,Link-to--ISP-2) dynamic interface
exit
object network INSIDE-NET2-ISP1
range 0.0.0.0 255.255.255.255
nat (Link-to--R-8-11-2,Link-to--ISP-1) dynamic interface

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				177
Змн.	Арк.	№ докум.	Підпис	Дата		

```

exit
object network INSIDE-NET2-ISP2
range 0.0.0.0 255.255.255.255
nat (Link-to--R-8-11-2,Link-to--ISP-2) dynamic interface
exit
object network INSIDE-NET3-ISP1
range 0.0.0.0 255.255.255.255
nat (Link-for--All,Link-to--ISP-1) dynamic interface
exit
object network INSIDE-NET3-ISP2
range 0.0.0.0 255.255.255.255
nat (Link-for--All,Link-to--ISP-2) dynamic interface
exit
router ospf 1
router-id 0.0.0.10
network 10.0.1.0 255.255.255.248 area 1
network 10.0.12.0 255.255.255.248 area 1
network 10.0.2.0 255.255.255.248 area 1
default-information originate
exit
monitor-interface Link-to--ISP-1
monitor-interface Link-to--ISP-2
monitor-interface Link-to--R-8-11-1
monitor-interface Link-to--R-8-11-2
monitor-interface Link-for--All
failover interface-policy 2
object network HTTP-Port-ISP1-to-R-8-11-1
host 172.16.100.25
nat (Link-to--R-8-11-1,Link-to--ISP-1) static interface service tcp 80 80
exit
object network HTTP-Port-ISP2-to-R-8-11-1
host 172.16.100.25
nat (Link-to--R-8-11-1,Link-to--ISP-2) static interface service tcp 80 80
exit
object network HTTP-Port-ISP1-to-R-8-11-2
host 172.16.100.25
nat (Link-to--R-8-11-2,Link-to--ISP-1) static interface service tcp 80 81
exit
object network HTTP-Port-ISP2-to-R-8-11-2
host 172.16.100.25
nat (Link-to--R-8-11-2,Link-to--ISP-2) static interface service tcp 80 81
exit
object network HTTP-Port-ISP1-to-All
host 172.16.100.25
nat (Link-for--All,Link-to--ISP-1) static interface service tcp 80 82
exit
object network HTTP-Port-ISP2-to-All
host 172.16.100.25
nat (Link-for--All,Link-to--ISP-2) static interface service tcp 80 82
exit
object network RDP-Port-ISP1-to-R-8-11-1

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		178

```

host 172.16.100.25
nat (Link-to--R-8-11-1,Link-to--ISP-1) static interface service tcp 3389
3389
exit
object network RDP-Port-ISP2-to-R-8-11-1
host 172.16.100.25
nat (Link-to--R-8-11-1,Link-to--ISP-2) static interface service tcp 3389
3389
exit
object network RDP-Port-ISP1-to-R-8-11-2
host 172.16.100.25
nat (Link-to--R-8-11-2,Link-to--ISP-1) static interface service tcp 3389
3390
exit
object network RDP-Port-ISP2-to-R-8-11-2
host 172.16.100.25
nat (Link-to--R-8-11-2,Link-to--ISP-2) static interface service tcp 3389
3390
exit
object network RDP-Port-ISP1-to-All
host 172.16.100.25
nat (Link-for--All,Link-to--ISP-1) static interface service tcp 3389 3391
exit
object network RDP-Port-ISP2-to-All
host 172.16.100.25
nat (Link-for--All,Link-to--ISP-2) static interface service tcp 3389 3391
exit
access-list Ports-Forwarding-ISP1 extended permit tcp any object HTTP-Port-
ISP1-to-R-8-11-1 eq 80
access-list Ports-Forwarding-ISP1 extended permit tcp any object HTTP-Port-
ISP1-to-R-8-11-2 eq 81
access-list Ports-Forwarding-ISP1 extended permit tcp any object HTTP-Port-
ISP1-to-All eq 82
access-list Ports-Forwarding-ISP1 extended permit tcp any object RDP-Port-
ISP1-to-R-8-11-1 eq 3389
access-list Ports-Forwarding-ISP1 extended permit tcp any object RDP-Port-
ISP1-to-R-8-11-2 eq 3390
access-list Ports-Forwarding-ISP1 extended permit tcp any object RDP-Port-
ISP1-to-All eq 3391
access-list Ports-Forwarding-ISP2 extended permit tcp any object HTTP-Port-
ISP2-to-R-8-11-1 eq 80
access-list Ports-Forwarding-ISP2 extended permit tcp any object HTTP-Port-
ISP2-to-R-8-11-2 eq 81
access-list Ports-Forwarding-ISP2 extended permit tcp any object HTTP-Port-
ISP2-to-All eq 82
access-list Ports-Forwarding-ISP2 extended permit tcp any object RDP-Port-
ISP2-to-R-8-11-1 eq 3389
access-list Ports-Forwarding-ISP2 extended permit tcp any object RDP-Port-
ISP2-to-R-8-11-2 eq 3390
access-list Ports-Forwarding-ISP2 extended permit tcp any object RDP-Port-
ISP2-to-All eq 3391

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		179

```

access-group Ports-Forwarding-ISP1 in interface Link-to--ISP-1
access-group Ports-Forwarding-ISP2 in interface Link-to--ISP-2
object network obj-facebook.com
fqdn facebook.com
exit
object network obj-youtube.com
fqdn youtube.com
exit
object network obj-viber.com
fqdn viber.com
exit
object-group network block-access
network-object object obj-facebook.com
network-object object obj-youtube.com
network-object object obj-viber.com
exit
access-list Network-Services extended deny ip 172.16.1.0 255.255.255.224
object-group block-access log
access-list Network-Services extended deny ip 172.16.1.32 255.255.255.224
object-group block-access log
access-list Network-Services extended deny ip 172.16.1.64 255.255.255.224
object-group block-access log
access-list Network-Services extended deny ip 172.16.2.0 255.255.255.224
object-group block-access log
access-list Network-Services extended deny ip 172.16.2.32 255.255.255.224
object-group block-access log
access-list Network-Services extended deny ip 172.16.2.64 255.255.255.224
object-group block-access log
access-list Network-Services extended permit ip any any
access-group Network-Services in interface Link-to--R-8-11-1
access-group Network-Services in interface Link-to--R-8-11-2
access-group Network-Services in interface Link-for--All
dns domain-lookup Link-to--ISP-1
dns domain-lookup Link-to--ISP-2
dns domain-lookup Link-to--R-8-11-1
dns domain-lookup Link-to--R-8-11-2
dns domain-lookup Link-for--All
dns name-server 172.16.100.25
dns name-server 100.0.100.200

```

--ASA-8-11-2:

```

hostname ASA-5512X
failover lan unit secondary
int gig0/0
no shutdown
int gig0/1
no shutdown
exit
failover lan interface FAILOVER gig0/0

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				180
Змн.	Арк.	№ докум.	Підпис	Дата		

```

failover interface ip FAILOVER 192.168.1.100 255.255.255.0 standby
192.168.1.101
failover link STATE gig0/1
failover interface ip STATE 192.168.2.100 255.255.255.0 standby
192.168.2.101
failover

```

--R-8-11-1:

```

en
conf t
hostname R-8-11-1
int gig0/1
ip address 10.0.1.5 255.255.255.248
ip ospf cost 1
no shutdown
exit
int gig0/2.1
encapsulation dot1Q 5
ip address 10.0.12.5 255.255.255.248
ip ospf cost 10
int gig0/2
no shutdown
exit
int gig0/0
ip address 10.0.3.1 255.255.255.252
ip ospf cost 20
no shutdown
exit
int gig0/0/0.12
description For-VLAN2
encapsulation dot1Q 12
ip address 172.16.1.30 255.255.255.224
exit
int gig0/0/0.13
description For-VLAN3
encapsulation dot1Q 13
ip address 172.16.1.62 255.255.255.224
exit
int gig0/0/0.14
description For-VLAN4
encapsulation dot1Q 14
ip address 172.16.1.94 255.255.255.224
exit
int gig0/0/0.15
description For-VLAN5
encapsulation dot1Q 15
ip address 172.16.1.126 255.255.255.224
exit
int gig0/0/0.16
description For-VLAN6

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				181
Змн.	Арк.	№ докум.	Підпис	Дата		

```

encapsulation dot1Q 16
ip address 172.16.1.158 255.255.255.224
exit
int gig0/0/0.100
description VLAN100-Server&Services
encapsulation dot1Q 100
ip address 172.16.100.254 255.255.255.0
exit
int gig0/0/0
no shut
exit
ip dhcp pool For-VLAN12
network 172.16.1.0 255.255.255.224
default-router 172.16.1.30
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN13
network 172.16.1.32 255.255.255.224
default-router 172.16.1.62
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN14
network 172.16.1.64 255.255.255.224
default-router 172.16.1.94
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN15
network 172.16.1.96 255.255.255.224
default-router 172.16.1.126
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN16
network 172.16.1.128 255.255.255.224
default-router 172.16.1.158
dns-server 100.0.100.200
exit
ip dhcp excluded-address 172.16.1.30
ip dhcp excluded-address 172.16.1.62
ip dhcp excluded-address 172.16.1.94
ip dhcp excluded-address 172.16.1.126
ip dhcp excluded-address 172.16.1.158
router ospf 1
router-id 0.0.0.2
passive-interface gig0/0/0
network 10.0.1.0 0.0.0.7 area 1
network 10.0.12.0 0.0.0.7 area 1
network 10.0.3.0 0.0.0.3 area 1
network 172.16.1.0 0.0.0.31 area 1
network 172.16.1.32 0.0.0.31 area 1
network 172.16.1.64 0.0.0.31 area 1
network 172.16.1.96 0.0.0.31 area 1

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				182
Змн.	Арк.	№ докум.	Підпис	Дата		

```

network 172.16.1.128 0.0.0.31 area 1
network 172.16.100.0 0.0.0.255 area 1
exit
ip sla 101
icmp-echo 10.0.1.1
frequency 5
exit
ip sla schedule 101 life forever start-time now
track 101 ip sla 101 reachability
exit
ip sla 102
icmp-echo 10.0.12.1
frequency 5
exit
ip sla schedule 102 life forever start-time now
track 102 ip sla 102 reachability
exit
ip sla 103
icmp-echo 10.0.2.1
frequency 5
exit
ip sla schedule 103 life forever start-time now
track 103 ip sla 103 reachability
exit
ip domain-lookup
ip name-server 172.16.100.25
ip name-server 100.0.100.200

```

--R-8-11-2:

```

en
conf t
hostname R-8-11-2
int fa0/0
description Link-for-VLAN2
ip address 10.0.2.6 255.255.255.248
ip ospf cost 1
no shutdown
exit
int fa0/1.1
description Link-for-VLAN3
encapsulation dot1Q 5
ip address 10.0.12.6 255.255.255.248
ip ospf cost 10
int fa0/1
no shutdown
exit
int fa0/1/0
description Link-to--R-8-11-1
ip address 10.0.3.2 255.255.255.252
ip ospf cost 20

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				183
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no shutdown
exit
int fa0/2/0.12
description For-VLAN2
encapsulation dot1Q 12
ip address 172.16.2.30 255.255.255.224
exit
int fa0/2/0.13
description For-VLAN3
encapsulation dot1Q 13
ip address 172.16.2.62 255.255.255.224
exit
int fa0/2/0.14
description For-VLAN4
encapsulation dot1Q 14
ip address 172.16.2.94 255.255.255.224
exit
int fa0/2/0.15
description For-VLAN5
encapsulation dot1Q 15
ip address 172.16.2.126 255.255.255.224
exit
int fa0/2/0.16
description For-VLAN6
encapsulation dot1Q 16
ip address 172.16.2.158 255.255.255.224
exit
ip dhcp pool For-VLAN12
network 172.16.2.0 255.255.255.224
default-router 172.16.2.30
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN13
network 172.16.2.32 255.255.255.224
default-router 172.16.2.62
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN14
network 172.16.2.64 255.255.255.224
default-router 172.16.2.94
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN15
network 172.16.2.96 255.255.255.224
default-router 172.16.2.126
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN16
network 172.16.2.128 255.255.255.224
default-router 172.16.2.158
dns-server 100.0.100.200

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				184
Змн.	Арк.	№ докум.	Підпис	Дата		

```

exit
ip dhcp excluded-address 172.16.2.30
ip dhcp excluded-address 172.16.2.62
ip dhcp excluded-address 172.16.2.94
ip dhcp excluded-address 172.16.2.126
ip dhcp excluded-address 172.16.2.158
router ospf 1
router-id 0.0.0.3
network 10.0.2.0 0.0.0.7 area 1
network 10.0.12.0 0.0.0.7 area 1
network 10.0.3.0 0.0.0.3 area 1
network 172.16.2.0 0.0.0.31 area 1
network 172.16.2.32 0.0.0.31 area 1
network 172.16.2.64 0.0.0.31 area 1
network 172.16.2.96 0.0.0.31 area 1
network 172.16.2.128 0.0.0.31 area 1
exit
ip sla 101
icmp-echo 10.0.2.1
frequency 5
exit
ip sla schedule 101 life forever start-time now
track 101 ip sla 101 reachability
exit
ip sla 102
icmp-echo 10.0.12.1
frequency 5
exit
ip sla schedule 102 life forever start-time now
track 102 ip sla 102 reachability
exit
ip sla 103
icmp-echo 10.0.1.1
frequency 5
exit
ip sla schedule 103 life forever start-time now
track 103 ip sla 103 reachability
exit
ip domain-lookup
ip name-server 172.16.100.25
ip name-server 100.0.100.200

```

--SW-8-11-1:

```

en
conf t
hostname SW-8-11-1
vlan 5
name VLAN-5-LAN
exit
int fa0/32

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				185
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit
int fa0/30
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit
int fa0/3
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit

```

--SW-8-11-2:

```

en
conf t
hostname SW-8-11-2
no vlan 2
name VLAN-2-LAN
exit
vlan 5
name VLAN-5-LAN
exit
int fa0/12
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit
int fa0/10
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit
int fa0/3
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit

```

--LAN1-Switch:

```

en
conf t
hostname LAN1-Switch

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				186
Змн.	Арк.	№ докум.	Підпис	Дата		

```

vlan 12
name VLAN-12-LAN
exit
vlan 13
name VLAN-13-LAN
exit
vlan 14
name VLAN-14-LAN
exit
vlan 15
name VLAN-15-LAN
exit
vlan 16
name VLAN-16-LAN
exit
vlan 100
name VLAN-100-Serv&Service
exit
int fa0/10
switchport mode trunk
switchport trunk allowed vlan 12,13,14,15,16,100
exit
int fa0/1
switchport mode access
switchport access vlan 12
exit
int fa0/3
switchport mode access
switchport access vlan 13
exit
int fa0/5
switchport mode access
switchport access vlan 14
exit
int fa0/7
switchport mode access
switchport access vlan 15
exit
int fa0/2
switchport mode access
switchport access vlan 16
exit
int fa0/4
switchport mode access
switchport access vlan 100
exit

```

--LAN2-Switch:

```

en
conf t
hostname LAN2-Switch

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				187
Змн.	Арк.	№ докум.	Підпис	Дата		

```

vlan 12
name VLAN-12-LAN
exit
vlan 13
name VLAN-13-LAN
exit
vlan 14
name VLAN-14-LAN
exit
vlan 15
name VLAN-15-LAN
exit
vlan 16
name VLAN-16-LAN
exit
vlan 100
name VLAN-100-Serv&Service
exit
int fa0/10
switchport mode trunk
switchport trunk allowed vlan 12,13,14,15,16
exit
int fa0/1
switchport mode access
switchport access vlan 12
exit
int fa0/3
switchport mode access
switchport access vlan 13
exit
int fa0/5
switchport mode access
switchport access vlan 14
exit
int fa0/7
switchport mode access
switchport access vlan 15
exit
int fa0/2
switchport mode access
switchport access vlan 16
exit

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				188
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток Є – Лістинг команд налаштування для тестового стенду

--ASA-8-11-1:

```
hostname ASA-5512X
failover lan unit primary
int gig0/0
no shutdown
int gig0/1
no shutdown
exit
failover lan interface FAILOVER gig0/0
failover interface ip FAILOVER 192.168.1.100 255.255.255.0 standby
192.168.1.101
failover link STATE gig0/1
failover interface ip STATE 192.168.2.100 255.255.255.0 standby
192.168.2.101
failover
prompt hostname priority state
int gig0/2
nameif Link-to--R-8-11-1
security-level 100
ip address 10.0.1.1 255.255.255.248 standby 10.0.1.2
ospf cost 1
no shutdown
exit
int gig0/3
nameif Link-to--R-8-11-2
security-level 100
ip address 10.0.2.1 255.255.255.248 standby 10.0.2.2
ospf cost 1
no shutdown
exit
int gig0/4.1
vlan 10
nameif Link-to--ISP-1
ip address 109.251.250.1 255.255.255.128
int gig0/4.2
vlan 20
nameif Link-to--ISP-2
ip address 109.251.250.129 255.255.255.128
int gig0/4
no shut
exit
int gig0/5.1
vlan 5
nameif Link-for--All
security-level 100
ip address 10.0.12.1 255.255.255.248 standby 10.0.12.2
ospf cost 4
```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				189
Змн.	Арк.	№ докум.	Підпис	Дата		

```

int gig0/5
no shut
exit
policy-map global_policy
class inspection_default
inspect icmp
exit
exit
sla monitor 1
type echo protocol ipIcmpEcho 109.251.250.126 interface Link-to--ISP-1
frequency 10
exit
sla monitor schedule 1 life forever start-time now
track 1 rtr 1 reachability
sla monitor 31
type echo protocol ipIcmpEcho 10.0.1.5 interface Link-to--R-8-11-1
frequency 5
exit
sla monitor schedule 31 life forever start-time now
track 31 rtr 31 reachability
sla monitor 32
type echo protocol ipIcmpEcho 10.0.2.6 interface Link-to--R-8-11-2
frequency 5
exit
sla monitor schedule 32 life forever start-time now
track 32 rtr 32 reachability
sla monitor 33
type echo protocol ipIcmpEcho 10.0.12.5 interface Link-for--All
frequency 5
exit
sla monitor schedule 33 life forever start-time now
track 33 rtr 33 reachability
sla monitor 34
type echo protocol ipIcmpEcho 10.0.12.6 interface Link-for--All
frequency 5
exit
sla monitor schedule 34 life forever start-time now
track 34 rtr 34 reachability
route Link-to--ISP-1 0.0.0.0 0.0.0.0 109.251.250.126 1 track 1
route Link-to--ISP-2 0.0.0.0 0.0.0.0 109.251.250.254 2
object network INSIDE-NET1-ISP1
range 0.0.0.0 255.255.255.255
nat (Link-to--R-8-11-1,Link-to--ISP-1) dynamic interface
exit
object network INSIDE-NET1-ISP2
range 0.0.0.0 255.255.255.255
nat (Link-to--R-8-11-1,Link-to--ISP-2) dynamic interface
exit
object network INSIDE-NET2-ISP1
range 0.0.0.0 255.255.255.255
nat (Link-to--R-8-11-2,Link-to--ISP-1) dynamic interface

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				190
Змн.	Арк.	№ докум.	Підпис	Дата		

```

exit
object network INSIDE-NET2-ISP2
range 0.0.0.0 255.255.255.255
nat (Link-to--R-8-11-2,Link-to--ISP-2) dynamic interface
exit
object network INSIDE-NET3-ISP1
range 0.0.0.0 255.255.255.255
nat (Link-for--All,Link-to--ISP-1) dynamic interface
exit
object network INSIDE-NET3-ISP2
range 0.0.0.0 255.255.255.255
nat (Link-for--All,Link-to--ISP-2) dynamic interface
exit
router ospf 1
router-id 0.0.0.10
network 10.0.1.0 255.255.255.248 area 1
network 10.0.12.0 255.255.255.248 area 1
network 10.0.2.0 255.255.255.248 area 1
default-information originate
exit
monitor-interface Link-to--ISP-1
monitor-interface Link-to--ISP-2
monitor-interface Link-to--R-8-11-1
monitor-interface Link-to--R-8-11-2
monitor-interface Link-for--All
failover interface-policy 2
object network HTTP-Port-ISP1-to-R-8-11-1
host 172.16.100.25
nat (Link-to--R-8-11-1,Link-to--ISP-1) static interface service tcp 80 80
exit
object network HTTP-Port-ISP2-to-R-8-11-1
host 172.16.100.25
nat (Link-to--R-8-11-1,Link-to--ISP-2) static interface service tcp 80 80
exit
object network HTTP-Port-ISP1-to-R-8-11-2
host 172.16.100.25
nat (Link-to--R-8-11-2,Link-to--ISP-1) static interface service tcp 80 81
exit
object network HTTP-Port-ISP2-to-R-8-11-2
host 172.16.100.25
nat (Link-to--R-8-11-2,Link-to--ISP-2) static interface service tcp 80 81
exit
object network HTTP-Port-ISP1-to-All
host 172.16.100.25
nat (Link-for--All,Link-to--ISP-1) static interface service tcp 80 82
exit
object network HTTP-Port-ISP2-to-All
host 172.16.100.25
nat (Link-for--All,Link-to--ISP-2) static interface service tcp 80 82
exit
object network RDP-Port-ISP1-to-R-8-11-1

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		191

```

host 172.16.100.25
nat (Link-to--R-8-11-1,Link-to--ISP-1) static interface service tcp 3389
3389
exit
object network RDP-Port-ISP2-to-R-8-11-1
host 172.16.100.25
nat (Link-to--R-8-11-1,Link-to--ISP-2) static interface service tcp 3389
3389
exit
object network RDP-Port-ISP1-to-R-8-11-2
host 172.16.100.25
nat (Link-to--R-8-11-2,Link-to--ISP-1) static interface service tcp 3389
3390
exit
object network RDP-Port-ISP2-to-R-8-11-2
host 172.16.100.25
nat (Link-to--R-8-11-2,Link-to--ISP-2) static interface service tcp 3389
3390
exit
object network RDP-Port-ISP1-to-All
host 172.16.100.25
nat (Link-for--All,Link-to--ISP-1) static interface service tcp 3389 3391
exit
object network RDP-Port-ISP2-to-All
host 172.16.100.25
nat (Link-for--All,Link-to--ISP-2) static interface service tcp 3389 3391
exit
access-list Ports-Forwarding-ISP1 extended permit tcp any object HTTP-Port-
ISP1-to-R-8-11-1 eq 80
access-list Ports-Forwarding-ISP1 extended permit tcp any object HTTP-Port-
ISP1-to-R-8-11-2 eq 81
access-list Ports-Forwarding-ISP1 extended permit tcp any object HTTP-Port-
ISP1-to-All eq 82
access-list Ports-Forwarding-ISP1 extended permit tcp any object RDP-Port-
ISP1-to-R-8-11-1 eq 3389
access-list Ports-Forwarding-ISP1 extended permit tcp any object RDP-Port-
ISP1-to-R-8-11-2 eq 3390
access-list Ports-Forwarding-ISP1 extended permit tcp any object RDP-Port-
ISP1-to-All eq 3391
access-list Ports-Forwarding-ISP2 extended permit tcp any object HTTP-Port-
ISP2-to-R-8-11-1 eq 80
access-list Ports-Forwarding-ISP2 extended permit tcp any object HTTP-Port-
ISP2-to-R-8-11-2 eq 81
access-list Ports-Forwarding-ISP2 extended permit tcp any object HTTP-Port-
ISP2-to-All eq 82
access-list Ports-Forwarding-ISP2 extended permit tcp any object RDP-Port-
ISP2-to-R-8-11-1 eq 3389
access-list Ports-Forwarding-ISP2 extended permit tcp any object RDP-Port-
ISP2-to-R-8-11-2 eq 3390
access-list Ports-Forwarding-ISP2 extended permit tcp any object RDP-Port-
ISP2-to-All eq 3391

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		192

```

access-group Ports-Forwarding-ISP1 in interface Link-to--ISP-1
access-group Ports-Forwarding-ISP2 in interface Link-to--ISP-2
object network obj-facebook.com
fqdn facebook.com
exit
object network obj-youtube.com
fqdn youtube.com
exit
object network obj-viber.com
fqdn viber.com
exit
object-group network block-access
network-object object obj-facebook.com
network-object object obj-youtube.com
network-object object obj-viber.com
exit
access-list Network-Services extended deny ip 172.16.1.0 255.255.255.224
object-group block-access log
access-list Network-Services extended deny ip 172.16.1.32 255.255.255.224
object-group block-access log
access-list Network-Services extended deny ip 172.16.1.64 255.255.255.224
object-group block-access log
access-list Network-Services extended permit ip any any
access-group Network-Services in interface Link-to--R-8-11-1
access-group Network-Services in interface Link-to--R-8-11-2
access-group Network-Services in interface Link-for--All
dns domain-lookup Link-to--ISP-1
dns domain-lookup Link-to--ISP-2
dns domain-lookup Link-to--R-8-11-1
dns domain-lookup Link-to--R-8-11-2
dns domain-lookup Link-for--All
dns name-server 172.16.100.25
dns name-server 100.0.100.200

```

--ASA-8-11-2:

```

hostname ASA-5512X
failover lan unit secondary
int gig0/0
no shutdown
int gig0/1
no shutdown
exit
failover lan interface FAILOVER gig0/0
failover interface ip FAILOVER 192.168.1.100 255.255.255.0 standby
192.168.1.101
failover link STATE gig0/1
failover interface ip STATE 192.168.2.100 255.255.255.0 standby
192.168.2.101
failover

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				193
Змн.	Арк.	№ докум.	Підпис	Дата		

--R-8-11-1:

```
en
conf t
hostname R-8-11-1
int gig0/1
ip address 10.0.1.5 255.255.255.248
ip ospf cost 1
no shutdown
exit
int gig0/2.1
encapsulation dot1Q 5
ip address 10.0.12.5 255.255.255.248
ip ospf cost 10
int gig0/2
no shutdown
exit
int gig0/0
ip address 10.0.3.1 255.255.255.252
ip ospf cost 20
no shutdown
exit
int gig0/0/0.12
description For-VLAN2
encapsulation dot1Q 12
ip address 172.16.1.30 255.255.255.224
exit
int gig0/0/0.13
description For-VLAN3
encapsulation dot1Q 13
ip address 172.16.1.62 255.255.255.224
exit
int gig0/0/0.14
description For-VLAN4
encapsulation dot1Q 14
ip address 172.16.1.94 255.255.255.224
exit
int gig0/0/0.15
description For-VLAN5
encapsulation dot1Q 15
ip address 172.16.1.126 255.255.255.224
exit
int gig0/0/0.16
description For-VLAN6
encapsulation dot1Q 16
ip address 172.16.1.158 255.255.255.224
exit
int gig0/0/0.100
description VLAN100-Server&Services
encapsulation dot1Q 100
ip address 172.16.100.254 255.255.255.0
```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				194
Змн.	Арк.	№ докум.	Підпис	Дата		

```

exit
int gig0/0/0
no shut
exit
ip dhcp pool For-VLAN12
network 172.16.1.0 255.255.255.224
default-router 172.16.1.30
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN13
network 172.16.1.32 255.255.255.224
default-router 172.16.1.62
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN14
network 172.16.1.64 255.255.255.224
default-router 172.16.1.94
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN15
network 172.16.1.96 255.255.255.224
default-router 172.16.1.126
dns-server 100.0.100.200
exit
ip dhcp pool For-VLAN16
network 172.16.1.128 255.255.255.224
default-router 172.16.1.158
dns-server 100.0.100.200
exit
ip dhcp excluded-address 172.16.1.30
ip dhcp excluded-address 172.16.1.62
ip dhcp excluded-address 172.16.1.94
ip dhcp excluded-address 172.16.1.126
ip dhcp excluded-address 172.16.1.158
router ospf 1
router-id 0.0.0.2
passive-interface gig0/0/0
network 10.0.1.0 0.0.0.7 area 1
network 10.0.12.0 0.0.0.7 area 1
network 10.0.3.0 0.0.0.3 area 1
network 172.16.1.0 0.0.0.31 area 1
network 172.16.1.32 0.0.0.31 area 1
network 172.16.1.64 0.0.0.31 area 1
network 172.16.1.96 0.0.0.31 area 1
network 172.16.1.128 0.0.0.31 area 1
network 172.16.100.0 0.0.0.255 area 1
exit
ip sla 101
icmp-echo 10.0.1.1
frequency 5
exit

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				
Змн.	Арк.	№ докум.	Підпис	Дата		195

```

ip sla schedule 101 life forever start-time now
track 101 ip sla 101 reachability
exit
ip sla 102
icmp-echo 10.0.12.1
frequency 5
exit
ip sla schedule 102 life forever start-time now
track 102 ip sla 102 reachability
exit
ip sla 103
icmp-echo 10.0.2.1
frequency 5
exit
ip sla schedule 103 life forever start-time now
track 103 ip sla 103 reachability
exit
ip domain-lookup
ip name-server 172.16.100.25
ip name-server 100.0.100.200

```

--R-8-11-2:

```

en
conf t
hostname R-8-11-2
int fa0/0
description Link-for-VLAN2
ip address 10.0.2.6 255.255.255.248
ip ospf cost 1
no shutdown
exit
int fa0/1.1
description Link-for-VLAN3
encapsulation dot1Q 5
ip address 10.0.12.6 255.255.255.248
ip ospf cost 10
int fa0/1
no shutdown
exit
int fa0/1/0
description Link-to--R-8-11-1
ip address 10.0.3.2 255.255.255.252
ip ospf cost 20
no shutdown
exit
router ospf 1
router-id 0.0.0.3
network 10.0.2.0 0.0.0.7 area 1
network 10.0.12.0 0.0.0.7 area 1
network 10.0.3.0 0.0.0.3 area 1

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				196
Змн.	Арк.	№ докум.	Підпис	Дата		

```

network 172.16.2.0 0.0.0.31 area 1
network 172.16.2.32 0.0.0.31 area 1
network 172.16.2.64 0.0.0.31 area 1
network 172.16.2.96 0.0.0.31 area 1
network 172.16.2.128 0.0.0.31 area 1
exit
ip sla 101
icmp-echo 10.0.2.1
frequency 5
exit
ip sla schedule 101 life forever start-time now
track 101 ip sla 101 reachability
exit
ip sla 102
icmp-echo 10.0.12.1
frequency 5
exit
ip sla schedule 102 life forever start-time now
track 102 ip sla 102 reachability
exit
ip sla 103
icmp-echo 10.0.1.1
frequency 5
exit
ip sla schedule 103 life forever start-time now
track 103 ip sla 103 reachability
exit
ip domain-lookup
ip name-server 172.16.100.25
ip name-server 100.0.100.200

```

--SW-8-11-1:

```

en
conf t
hostname SW-8-11-1
vlan 5
name VLAN-5-LAN
exit
int fa0/32
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit
int fa0/30
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit
int fa0/3
switchport mode trunk

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				197
Змн.	Арк.	№ докум.	Підпис	Дата		

```

switchport trunk allowed vlan 5
no shut
exit

```

--SW-8-11-2:

```

en
conf t
hostname SW-8-11-2
no vlan 2
name VLAN-2-LAN
exit
vlan 5
name VLAN-5-LAN
exit
int fa0/12
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit
int fa0/10
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit
int fa0/3
switchport mode trunk
switchport trunk allowed vlan 5
no shut
exit

```

--LANs-Switch:

```

en
conf t
hostname LAN-Switch
vlan 12
name VLAN-12-LAN
exit
vlan 13
name VLAN-13-LAN
exit
vlan 14
name VLAN-14-LAN
exit
vlan 15
name VLAN-15-LAN
exit
vlan 16
name VLAN-16-LAN

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				198
Змн.	Арк.	№ докум.	Підпис	Дата		

```

exit
vlan 100
name VLAN-100-Serv&Service
exit
int fa0/10
switchport mode trunk
switchport trunk allowed vlan 12,13,14,15,16,100
exit
int fa0/1
switchport mode access
switchport access vlan 12
exit
int fa0/3
switchport mode access
switchport access vlan 13
exit
int fa0/5
switchport mode access
switchport access vlan 14
exit
int fa0/7
switchport mode access
switchport access vlan 15
exit
int fa0/2
switchport mode access
switchport access vlan 16
exit
int fa0/4
switchport mode access
switchport access vlan 100
exit

```

--ISP-Router:

```

en
conf t
hostname ISP-Router
int f0/1.2
encapsulation dot1Q 10
ip address 109.251.250.126 255.255.255.128
exit
int f0/1.3
encapsulation dot1Q 20
ip address 109.251.250.254 255.255.255.128
exit
int fa0/1
no shut
exit
int fa0/0
ip address dhcp

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				199
Змн.	Арк.	№ докум.	Підпис	Дата		

```

no shut
exit
ip domain-lookup
ip name-server 100.0.100.200
int f0/1.2
ip nat inside
exit
int f0/1.3
ip nat inside
exit
int fa0/1
ip nat inside
exit
int fa0/0
ip nat outside
exit
access-list 10 permit any
ip nat inside source list 10 interface FastEthernet0/0 overload

```

--Outside-Switch:

```

en
conf t
hostname Outside-Switch
vlan 10
name Net-ISP1
exit
vlan 20
name Net-ISP2
exit
vlan 100
name Global-Net
exit
int fa0/1
switchport trunk encapsulation dot1Q
switchport mode trunk
switchport trunk allowed vlan 10,20
no shut
exit
int range fa0/23-24
switchport trunk encapsulation dot1Q
switchport mode trunk
switchport trunk allowed vlan 10,20
no shut
exit
int fa0/2
switchport trunk encapsulation dot1Q
switchport mode trunk
switchport trunk allowed vlan 100
no shut

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				200
Змн.	Арк.	№ докум.	Підпис	Дата		

```

exit
int fa0/5
switchport mode access
switchport access vlan 100
no shut
exit
int fa0/6
switchport mode access
switchport access vlan 100
no shut
exit
int fa0/7
switchport mode access
switchport access vlan 100
no shut
exit
int fa0/8
switchport mode access
switchport access vlan 100
no shut
exit
int vlan 10
ip address 109.251.250.64 255.255.255.128
no shut
exit
int vlan 20
ip address 109.251.250.200 255.255.255.128
no shut
exit

```

		Колесник Д.В.			КІ.КР.Б – 123 – 11– ПЗ	Арк.
		Ефіменко А.А				201
Змн.	Арк.	№ докум.	Підпис	Дата		

Додаток І – Таблиця сценаріїв тестування відмовостійкості

Таблиця 1 – Варіант тестування відмовостійкості №1

Канали зв'язку	ASA-8-11-1	ASA-8-11-2	SW-8-11-1	SW-8-11-2	R-8-11-1	R-8-11-2	ISP1	ISP2
ASA-8-11-1	---	---	✓ ✓	✓	---	---	✓	✓
ASA-8-11-2	---	---	✓	✓ ✓	---	---	✓	✓
SW-8-11-1	✓ ✓	✓	---	✓	✗ ✓	✓ ✓	---	---
SW-8-11-2	✓	✓ ✓	✓	---	✓ ✓	✓ ✓	---	---
R-8-11-1	---	---	✗ ✓	---	---	✓	---	---
R-8-11-2	---	---	---	✓ ✓	✓	---	---	✓---
ISP1	---	---	---	---	---	---	---	---
ISP2	---	---	---	---	---	---	---	---
Відмовостійкість	Відмовостійкість підтверджена за результатами тестування							

Таблиця 2 – Варіант тестування відмовостійкості №2

Канали зв'язку	ASA-8-11-1	ASA-8-11-2	SW-8-11-1	SW-8-11-2	R-8-11-1	R-8-11-2	ISP1	ISP2
ASA-8-11-1	---	---	✓ ✓	✓	---	---	✓	✓
ASA-8-11-2	---	---	✓	✓ ✓	---	---	✓	✓
SW-8-11-1	✓ ✓	✓	---	✓	✗ ✗	✓ ✓	---	---
SW-8-11-2	✓	✓ ✓	✓	---	✓ ✓	✓ ✓	---	---
R-8-11-1	---	---	✗ ✗	---	---	✓	---	---
R-8-11-2	---	---	---	✓ ✓	✓	---	---	✓---
ISP1	---	---	---	---	---	---	---	---
ISP2	---	---	---	---	---	---	---	---
Відмовостійкість	Відмовостійкість підтверджена за результатами тестування							

Таблиця 3 – Варіант тестування відмовостійкості №3

Канали зв'язку	ASA-8-11-1	ASA-8-11-2	SW-8-11-1	SW-8-11-2	R-8-11-1	R-8-11-2	ISP1	ISP2
ASA-8-11-1	---	---	✗ ✓	✓	---	---	✓	✓
ASA-8-11-2	---	---	✓	✓ ✓	---	---	✓	✓
SW-8-11-1	✗ ✓	✓	---	✓	✓ ✓	✓ ✓	---	---
SW-8-11-2	✓	✓ ✓	✓	---	✓ ✓	✓ ✓	---	---
R-8-11-1	---	---	✓ ✓	---	---	✓	---	---
R-8-11-2	---	---	---	✓ ✓	✓	---	---	✓---
ISP1	---	---	---	---	---	---	---	---
ISP2	---	---	---	---	---	---	---	---
Відмовостійкість	Відмовостійкість підтверджена за результатами тестування							

Таблиця 4 – Варіант тестування відмовостійкості №4

Канали зв'язку	ASA-8-11-1	ASA-8-11-2	SW-8-11-1		SW-8-11-2		R-8-11-1		R-8-11-2		ISP1	ISP2		
ASA-8-11-1	---	---	✗	✗	✓		---		---		✓	✓		
ASA-8-11-2	---	---	✓		✓	✓	---		---		✓	✓		
SW-8-11-1	✗	✗	✓		---		✓	✓	✓	✓	---	---		
SW-8-11-2	✓		✓	✓	✓		---		✓	✓	✓	✓	---	---
R-8-11-1	---	---	✓	✓	---		---		✓		---	---		
R-8-11-2	---	---	---		✓	✓	✓		---		---	✓---		
ISP1	---	---	---		---		---		---		---	---		
ISP2	---	---	---		---		---		---		---	---		
Відмовостій- кість	Відмовостійкість підтверджена за результатами тестування													

Таблиця 5 – Варіант тестування відмовостійкості №5

Канали зв'язку	ASA-8-11-1	ASA-8-11-2	SW-8-11-1		SW-8-11-2		R-8-11-1		R-8-11-2		ISP1	ISP2		
ASA-8-11-1	---	---	✗	✗	✗		---		---		✓	✓		
ASA-8-11-2	---	---	✓		✓	✓	---		---		✓	✓		
SW-8-11-1	✗	✗	✓		---		✓	✓	✓	✓	---	---		
SW-8-11-2	✗		✓	✓	✓		---		✓	✓	✓	✓	---	---
R-8-11-1	---	---	✓	✓	---		---		✓		---	---		
R-8-11-2	---	---	---		✓	✓	✓		---		---	✓---		
ISP1	---	---	---		---		---		---		---	---		
ISP2	---	---	---		---		---		---		---	---		
Відмовостій- кість	Відмовостійкість підтверджена за результатами тестування													

Таблиця 6 – Варіант тестування відмовостійкості №6

Канали зв'язку	ASA-8-11-1		ASA-8-11-2		SW-8-11-1		SW-8-11-2		R-8-11-1		R-8-11-2		ISP1	ISP2
ASA-8-11-1	---		---		✗	✗	✗		---		---		✓	✓
ASA-8-11-2	---		---		✗		✓	✓	---		---		✓	✓
SW-8-11-1	✗	✗	✗		---		✓		✓	✓	✓	✓	---	---
SW-8-11-2	✗		✓	✓	✓		---		✓	✓	✓	✓	---	---
R-8-11-1	---		---		✓	✓	---		---		✓		---	---
R-8-11-2	---		---		---		✓	✓	✓		---		---	✓---
ISP1	---		---		---		---		---		---		---	---
ISP2	---		---		---		---		---		---		---	---
Відмовостій- кість	Відмовостійкість підтверджена за результатами тестування													

Таблиця 7 – Варіант тестування відмовостійкості №7

Канали зв'язку	ASA-8-11-1	ASA-8-11-2	SW-8-11-1		SW-8-11-2		R-8-11-1		R-8-11-2		ISP1	ISP2		
ASA-8-11-1	---	---	✗	✗	✗		---		---		✓	✓		
ASA-8-11-2	---	---	✗		✗	✓	---		---		✓	✓		
SW-8-11-1	✗	✗	✗		✓		✓	✓	✓	✓	---	---		
SW-8-11-2	✗		✗	✓	✓		---		✓	✓	✓	✓	---	---
R-8-11-1	---		---		✓	✓	---		---		✓	---	---	---
R-8-11-2	---		---		---		✓	✓	✓		---		---	✓---
ISP1	---		---		---		---		---		---		---	---
ISP2	---		---		---		---		---		---		---	---
Відмовостій- кість	Відмовостійкість підтверджена за результатами тестування													

Таблиця 8 – Варіант тестування відмовостійкості №8

Таблиця 8. Варіант тестування відмовостійкості														
Канали зв'язку	ASA-8-11-1		ASA-8-11-2		SW-8-11-1		SW-8-11-2		R-8-11-1		R-8-11-2		ISP1	ISP2
ASA-8-11-1	---		---		✓	✓	✓		---		---		✓	✓
ASA-8-11-2	---		---		✓		✓	✓	---		---		✓	✓
SW-8-11-1	✓	✓	✓		---		✓		✓	✓	✓	✓	---	---
SW-8-11-2	✓		✓	✓	✓		---		✓	✓	✗	✓	---	---
R-8-11-1	---		---		✓	✓	---		---		✓		---	---
R-8-11-2	---		---		---		✗	✓	✓		---		---	✓---
ISP1	---		---		---		---		---		---		---	---
ISP2	---		---		---		---		---		---		---	---
Відмовостій- кість	Відмовостійкість підтверджена за результатами тестування													

Таблиця 9 – Варіант тестування відмовостійкості №9

Канали зв'язку	ASA-8-11-1	ASA-8-11-2	SW-8-11-1	SW-8-11-2	R-8-11-1	R-8-11-2	ISP1	ISP2		
ASA-8-11-1	---	---	✓	✓	✓	---	---	✓	✓	
ASA-8-11-2	---	---	✓	✓	✓	---	---	✓	✓	
SW-8-11-1	✓	✓	✓	✓	✓	✓	✓	✓	---	---
SW-8-11-2	✓	✓	✓	---	✓	✓	✗	✗	---	---
R-8-11-1	---	---	✓	✓	---	---	✓	---	---	---
R-8-11-2	---	---	---	✗	✗	✓	---	---	---	✓---
ISP1	---	---	---	---	---	---	---	---	---	---
ISP2	---	---	---	---	---	---	---	---	---	---
Відмовостій- кість	Відмовостійкість підтверджена за результатами тестування									

Таблиця 10 – Варіант тестування відмовостійкості №10

Канали зв'язку	ASA-8-11-1	ASA-8-11-2	SW-8-11-1	SW-8-11-2	R-8-11-1	R-8-11-2	ISP1	ISP2
ASA-8-11-1	---	---	✓ ✓	✓	---	---	✓	✓
ASA-8-11-2	---	---	✓	✗ ✗	---	---	✓	✓
SW-8-11-1	✓ ✓	✗	---	✓	✓ ✓	✓ ✓	---	---
SW-8-11-2	✗	✗ ✗	✓	---	✓ ✓	✗ ✗	---	---
R-8-11-1	---	---	✓ ✓	---	---	✓	---	---
R-8-11-2	---	---	---	✗ ✗	✓	---	---	✓---
ISP1	---	---	---	---	---	---	---	---
ISP2	---	---	---	---	---	---	---	---
Відмовостійкість	Відмовостійкість підтверджена за результатами тестування							

Таблиця 11 – Варіант тестування відмовостійкості №11

Канали зв'язку	ASA-8-11-1	ASA-8-11-2	SW-8-11-1	SW-8-11-2	R-8-11-1	R-8-11-2	ISP1	ISP2
ASA-8-11-1	---	---	✗ ✗	✓	---	---	✓	✓
ASA-8-11-2	---	---	✓	✓ ✓	---	---	✓	✓
SW-8-11-1	✗ ✗	✓	---	✓	✗ ✗	✓ ✓	---	---
SW-8-11-2	✓	✓ ✓	✓	---	✓ ✓	✓ ✗	---	---
R-8-11-1	---	---	✗ ✗	---	---	✓	---	---
R-8-11-2	---	---	---	✓ ✗	✓	---	---	✓---
ISP1	---	---	---	---	---	---	---	---
ISP2	---	---	---	---	---	---	---	---
Відмовостійкість	Відмовостійкість підтверджена за результатами тестування							

Таблиця 12 – Варіант тестування відмовостійкості №12

Канали зв'язку	ASA-8-11-1	ASA-8-11-2	SW-8-11-1	SW-8-11-2	R-8-11-1	R-8-11-2	ISP1	ISP2
ASA-8-11-1	---	---	✓ ✓	✓	---	---	✗	✓
ASA-8-11-2	---	---	✓	✓ ✓	---	---	✗	✓
SW-8-11-1	✓ ✓	✓	---	✓	✓ ✓	✓ ✓	---	---
SW-8-11-2	✓	✓ ✓	✓	---	✓ ✓	✓ ✓	---	---
R-8-11-1	---	---	✓ ✓	---	---	✓	---	---
R-8-11-2	---	---	---	✓ ✓	✓	---	---	✓---
ISP1	---	---	---	---	---	---	---	---
ISP2	---	---	---	---	---	---	---	---
Відмовостійкість	Відмовостійкість підтверджена за результатами тестування							

