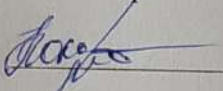


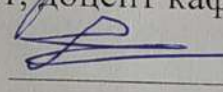
Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

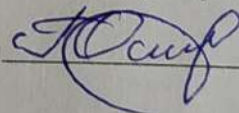
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми дзеркалювання трафіку
комп'ютерної мережі організації»

Виконала студентка 4-го курсу, групи КІ-3
спеціальності 123 «Комп'ютерна інженерія»

 І. А. Кондратюк
Керівник к.т.н., доцент, доцент кафедри КІ та КБ

 Ю.М. Росінський
Рецензент к.пед.н., доцент кафедри КІ та КБ

 О.С. Головня

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

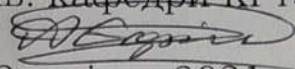
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ

СПЕЦІАЛЬНІСТЬ 123 «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри КІ та КБ

 Єфіменко А. А.
«12» квітня 2021р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента Кондратюк Ірини Андріївни

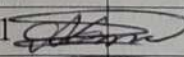
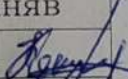
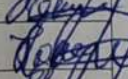
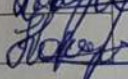
Тема роботи: Проект підсистеми дзеркалювання трафіку комп'ютерної мережі організації

Затверджена Наказом університету від «12» квітня 2021 р. № 133\С

Термін здачі студентом закінченої роботи 24.06.2020

Вихідні дані роботи (зазначається предмет і об'єкт дослідження)
процес проектування, розробки та налагодження підсистеми дзеркалювання трафіку комп'ютерної мережі організації; комутатори Cisco Catalyst як основа підсистеми дзеркалювання трафіку мережі організації;

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	12.04.2021 	12.04.20.21 
2	Єфіменко А.А.	13.05.2021 	13.05.2021 
3	Єфіменко А.А.	15.06.2021 	15.06.2021 

Керівник:  Россієнький Ю. М.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Видача завдання	12.04.2021	
2	Розробка плану роботи	14.04.2021 - 18.04.2021	
3	Розробка розгорнутого плану	19.04.2021 - 20.04.2021	
4	Подача чернетки керівнику для перевірки	21.04.2021	
5	Доопрацювання роботи та перевірка керівником	27.04.2021 - 29.05.2021	
6	Затвердження графічних матеріалів у керівника	01.06.2021 - 04.06.2021	
7	Проведення попереднього захисту	05.06.2021 -	
8	Отримання відгуку керівника	15.06.2021	
9	Допуск завідувача кафедри	16.06.2021	
10	Подання роботи на рецензування	22.06.2021	
11	Захист		

Студент Кондратюк І. А.

Керівник Росі́нський Ю. М.

АНОТАЦІЯ

Випускна кваліфікаційна робота представляє з себе проект підсистеми дзеркалювання трафіку комп'ютерної мережі організації. Пояснювальна записка до випускної дипломної кваліфікаційної роботи містить в собі 61 сторінка, 22 рисунки та 6 таблиць. Список використаних джерел містить 15 найменувань і займає 2 сторінки.

Метою випускної кваліфікаційної роботи є розробка підсистеми дзеркалювання трафіку комп'ютерної мережі організації та забезпечення функціонування даної мережі.

В роботі визначено основні завдання для побудови мережі організації, проаналізовано базові підходи до побудови мережі з використанням продукції компанії Cisco. Наведено розробку, налагодження функціонування підсистеми дзеркалювання комп'ютерної мережі за допомогою комутаторів Cisco Catalyst та тестування її працездатності й виконання поставлених задач.

Ключові слова: МЕРЕЖА ОРГАНІЗАЦІЇ, КОМУТАТОРИ, CISCO, CISCO CATALYST, ПІДСИСТЕМА ДЗЕРКАЛЮВАННЯ, ДЗЕРКАЛЮВАННЯ, ТРАФІК.

KIK.KP.B – 123 – 08 – ПЗ

Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Кондратиюк І. А.		25.06.21	Проект підсистеми дзеркалювання трафіку комп'ютерної мережі Пояснювальна записка		
Керівник		Росієнський Ю.		25.06.21			
Рецензент		Головня О. С.		25.06.21			
Н. контр.							
Зав. каф.		Єфіменко А. А.		25.06.21			
					Літ.	Арк.	Аркушів
						4	61
					ФІКТ, КІ-3		

ANNOTATION

The final qualification work is a project of the traffic mirroring subsystem of the computer network of the organization. The explanatory note to the final thesis qualifier contains 61 pages, 22 figures and 6 tables. The list of used sources contains 15 the name and occupies 2 pages.

The purpose of the final qualification work is to develop a subsystem for mirroring the traffic of the computer network of the organization and ensure the functioning of this network.

The main tasks for building the organization 's network are defined in the work, the basic approaches to building a network with the use of Cisco products are analyzed. The development, debugging of the computer network mirroring subsystem with the help of Cisco Catalyst switches and testing of its operability and performance of the set tasks are given.

Keywords: NETWORK OF ORGANIZATION, SWITCHES, CISCO, CISCO CATALYST, SUBSYSTEM OF MIRRORING, MIRRORING, TRAFFIC.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		5

ЗМІСТ

ВСТУП	7
РОЗДІЛ 1. ПРИНЦИПИ ПОБУДОВИ ТА ТЕХНОЛОГІЇ ДЗЕРКАЛЮВАННЯ ТРАФІКУ	9
1.1 Аналіз принципів дзеркалювання трафіку в комутованих мережах	9
1.2 Засоби та технології дзеркалювання трафіку комутаторів Cisco....	13
1.3 Принципи та засоби захоплення трафіку	16
1.4 Постановка технічного завдання.	18
Висновки до першого розділу.....	Ошибка! Закладка не определена.
РОЗДІЛ 2. ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ПІДСИСТЕМИ ДЗЕРКАЛЮВАННЯ ТРАФІКУ	20
2.1 Проектування топології комп'ютерної мережі організації	20
2.2 Розробка схеми адресації мережі	24
2.3 Розробка підсистеми дзеркалювання трафіку.....	26
Висновки до другого розділу	Ошибка! Закладка не определена.
РОЗДІЛ 3. НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ РОБОТИ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ПІДСИСТЕМИ ДЗЕРКАЛЮВАННЯ ТРАФІКУ	28
3.1 Вибір обладнання та програмного забезпечення для реалізації проекту комп'ютерної мережі та підсистеми дзеркалювання трафіку	28
3.2 Налаштування проміжних та кінцевих вузлів мережі	29
3.3 Налаштування підсистеми дзеркалювання трафіку	31
3.4 Тестування роботи підсистеми дзеркалювання трафіку.....	40
Висновки до третього розділу.....	Ошибка! Закладка не определена.
ВИСНОВКИ.....	47
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	49
ДОДАТКИ.....	50

ВСТУП

На сьогоднішній день комп'ютерні мережі міцно увійшли в сучасне життя. Давно минули часи, коли комп'ютер розумівся виключно як автономний обчислювальний пристрій. Комп'ютери та інші цифрові пристрої практично завжди підключаються в мережу, що дозволяє обмінюватися інформацією, отримувати доступ до цифрових ресурсів, спільно використовувати периферійні пристрої та ін. Комп'ютерні мережі забезпечують і новий рівень обчислень - за рахунок розподілу навантаження між багатьма машинами створюються високопродуктивні обчислювальні мережі.

Ідея об'єднання комп'ютерів в мережу зажадала рішення багатьох завдань - розробки принципів спільного використання мережевих ресурсів, мережевих стандартів і протоколів, технологій захисту даних і ін. Для практичної реалізації комп'ютерних мереж було створено різноманітне апаратне забезпечення, мережеві операційні системи, а також численні мережеві додатки, що використовуються як на серверах, так і на робочих станціях мережі.

Все більше організацій зустрічаються з проблемами несправності мережі. Причиною цих проблем можуть бути віруси, шкідливе та несанкціоноване програмне забезпечення. Також кожна компанія має свої цінні файли, які ні в якому разі не мають потрапити в руки злоумисника. Передбачити усі проблеми в мережі неможливо, але з метою спрощення виявлення використовують засоби аналізу трафіку.

Актуальність теми полягає в потребі контролю пакетів мережі для подальшого швидкого виявлення збоїв системи локальної мережі.

Об'єктом дослідження є комутатори Cisco Catalyst, які є основою підсистеми дзеркалювання трафіку комп'ютерної мережі організації.

Предметом дослідження є підсистема дзеркалювання трафіку комп'ютерної мережі організації.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		7

Метою кваліфікаційної роботи є розробка проекту підсистеми дзеркалювання трафіку комп'ютерної мережі організації.

Для виконання кваліфікаційної роботи були поставлені наступні завдання:

- Провести дослідження і аналіз предметної області;
- Спроектувати логічну схему мережі;
- Спроектувати фізичну схему мережі;
- Вибрати активне і пасивне устаткування;
- Вибрати серверне обладнання і програмне забезпечення.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

РОЗДІЛ 1. ПРИНЦИПИ ПОБУДОВИ ТА ТЕХНОЛОГІЇ ДЗЕРКАЛЮВАННЯ ТРАФІКУ

1.1 Аналіз принципів дзеркалювання трафіку в комутованих мережах

Дзеркалювання трафіку (англ. Port mirroring) - технологія дублювання пакетів одного порту мережевого комутатора (або окремої VLAN) на іншому. Велика кількість керованих мережевих комутаторів дозволяють дублювати трафік від одного або декількох портів і / або VLAN на окремо взятий порт.

Віддзеркалення портів використовується на мережевому комутаторі або маршрутизаторі для відправки копії мережевих пакетів, видимих для вибраних портів (вихідний порт), на інші зазначені порти (порт призначення). При включеному дзеркалюванні портів пакети можна відстежувати і аналізувати. Віддзеркалення портів застосовується широко, наприклад, мережеві інженери можуть використовувати віддзеркалення портів для аналізу та налагодження даних або діагностики помилок в своїх мережах, без впливу на можливості обробки пакетів мережевих пристроїв. А Міністерство культури і громадської безпеки можуть збирати пов'язані дані з віддзеркалення портів для аналізу поведінки мережі, щоб забезпечити здорову мережеву середу.

Локальне та віддалене віддзеркалення портів - це два типи віддзеркалення портів, засновані на різних робочих діапазонах зеркалювання. Вони працюють за різними принципами.

Локальне віддзеркалення портів є найбільш простою формою віддзеркалення. Всі вихідні порти розташовані на тому ж мережевому пристрої як порт призначення. Як показано на рисунку 1.1, віддзеркалення локального порту дозволяє мережного комутатора переслати копію пакета з вихідного порту (Eth 1/1) на порт призначення (Eth 1/2). Потім пристрій моніторингу, підключений до порту призначення, може відстежувати і аналізувати пакет.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

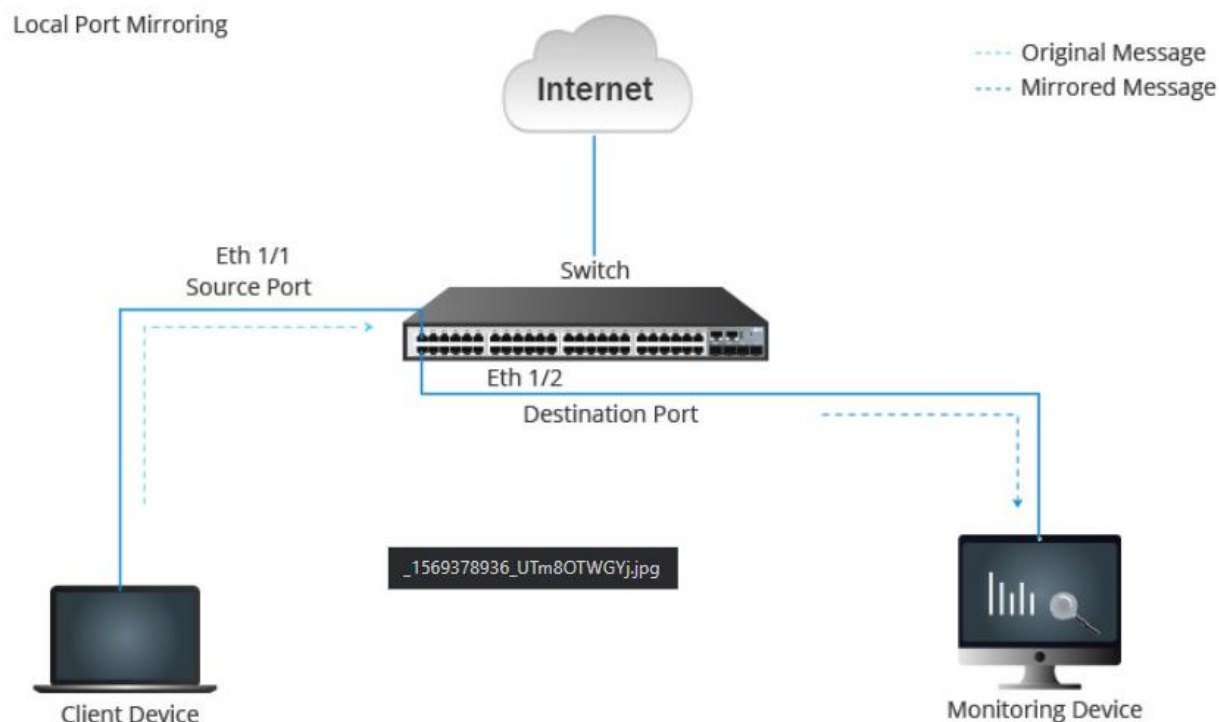


Рисунок 1.1 – Локальне дзеркалювання портів

Що стосується дзеркалювання віддалених портів, вихідні порти і порти призначення не перебувають на одному пристрої. Як показано на рисунку 1.2, вихідні порти (Eth 1/3) знаходиться на одному комутаторі, а порт призначення (Eth 1/3) - на іншому комутаторі. Вихідний порт пересилає копію пакета на порт призначення через з'єднання висхідної лінії зв'язку, досягнуте портом (Eth 1/4) на двох комутаторах. Отже, віддзеркалення локальних портів дозволяє здійснювати моніторинг і аналіз даних на різних пристроях.

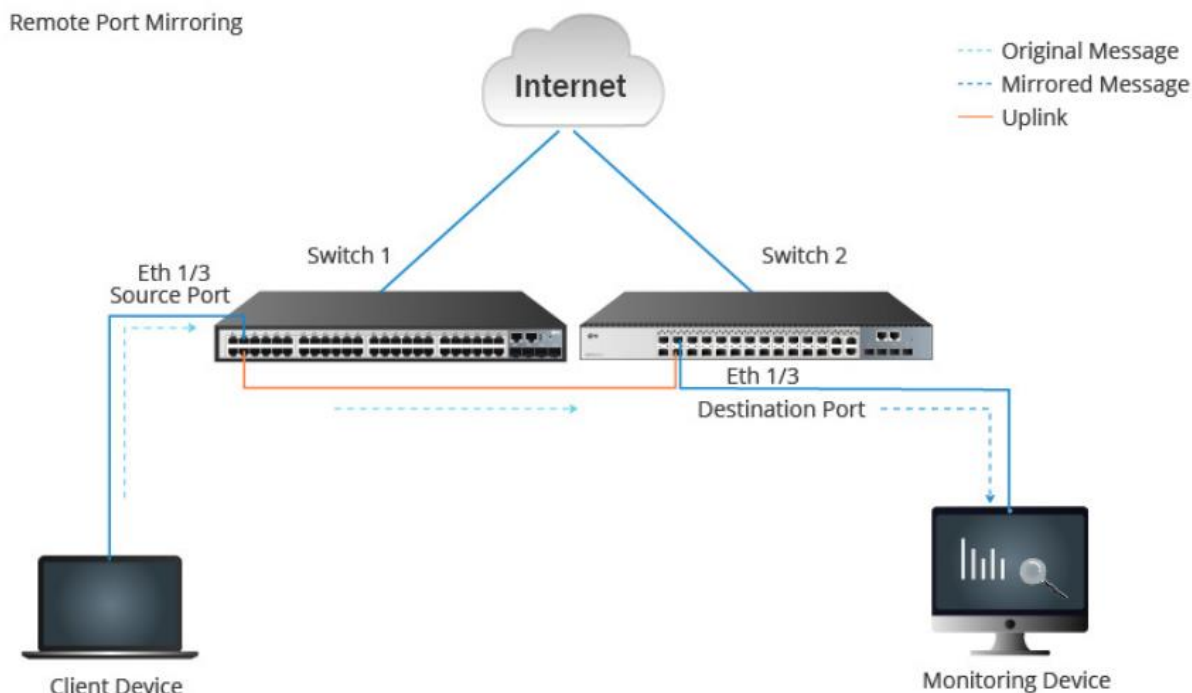


Рисунок 1.2 – Віддалене дзеркалювання портів

Обов'язковою умовою налаштування віддзеркалення портів є забезпечення того, що мережевий пристрій (незалежно від комутатора або маршрутизатора) підтримує віддзеркалення портів. Потім виберіть один з режимів: віддзеркалення локальних портів або налаштування дзеркалювання віддалених портів.

Схема конфігурації дзеркалювання локального порту:

1. Створіть VLAN.
2. Додайте порт джерела і порт призначення в VLAN.
3. Налаштуйте IP-адреси.
4. Налаштуйте віддзеркалення порту на порту призначення і скопіюйте пакет з вихідного порту на порт призначення.

План налаштування дзеркалювання віддалених портів:

1. Створіть вихідний порт в глобальній схемі.
2. Налаштуйте порт висхідного зв'язку на одному комутаторі.
3. Створіть порт призначення в глобальній схемі.
4. Налаштуйте порт висхідної лінії зв'язку на іншому комутаторі.

Звернемо увагу, на:

- Конфігурація вступає в силу після установки одного порту в якості порту джерела і установки іншого порту в якості порту призначення в створення дзеркал локального порту.
- При створенні групи дзеркалювання можна встановити тільки один порт призначення, але в групі може бути один або кілька вихідних портів.
- Якщо один порт був зазначений в якості вихідного порту в одній групі дзеркалювання, він не може бути членом іншої групи дзеркалювання.
- Якщо один порт був вказаний як порт призначення в одній групі дзеркалювання, він не може бути членом іншої групи.
- Рекомендується не застосовувати STP, RSTP або MSTP до порту призначення, в іншому випадку пристрій може не працювати належним чином.

Віддзеркалення порту і Віддзеркалення трафіку відносяться до функції віддзеркалення, тому розглянемо в чому між ними різниця.

Віддзеркалення трафіку - функція комутатора, призначена для перенаправлення трафіку з одного порту комутатора на інший порт цього ж комутатора (локальне віддзеркалення) або на віддалений комутатор (віддалене віддзеркалення). Як показано на малюнку 1.3, вихідний порт копіює потік даних, відповідний правилу від клієнта 2 до порту призначення, який потім відправляє скопійований потік даних на пристрій моніторингу. Відповідний потік даних може бути встановлений ACL (Access Control List) або командами конфігурації. При створення віддзеркалення трафіку на пристрій моніторингу відправляється тільки обраний або узгоджений трафік, а при створення віддзеркалення портів копіюється кожен пакет, який проходить через інтерфейс, на пристрій моніторингу.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

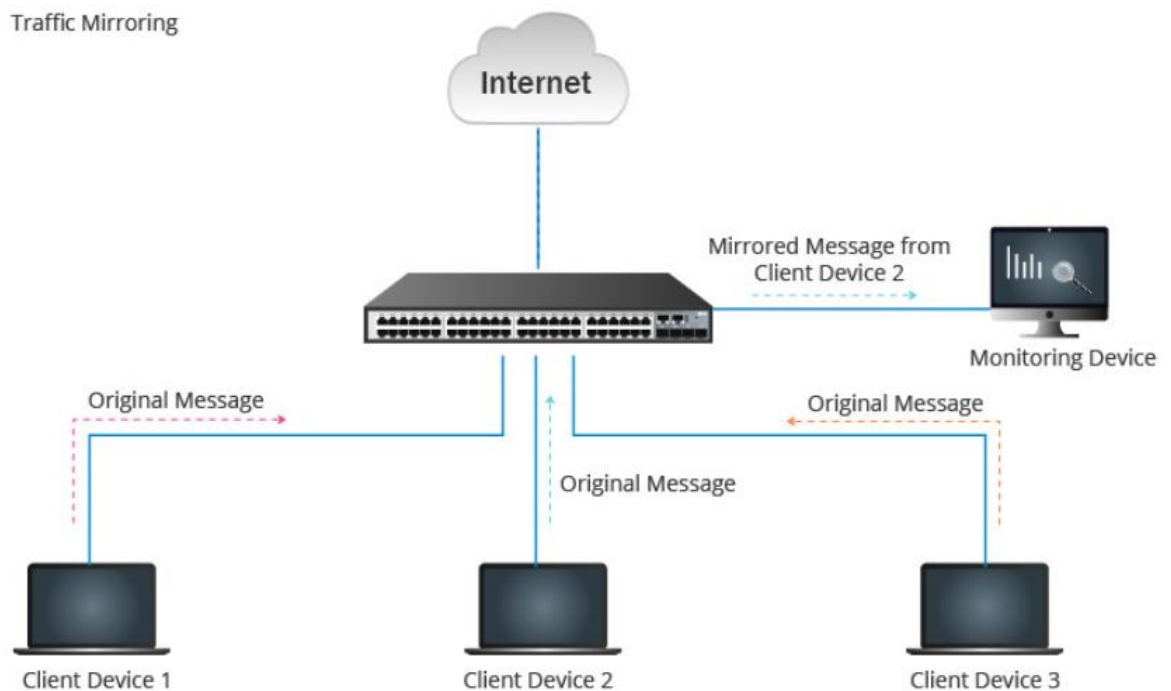


Рисунок 1.3 – Моніторинг трафіку.

Також розглянемо різницю між дзеркальним відображенням портів та зіставлення портів. Port mapping - це переадресація прийнятих даних таким чином, щоб дані, що приймаються на якийсь порт одного комп'ютера автоматично переадресовувалися на якийсь інший порт іншого комп'ютера. Всі передані вами дані без жодних спотворень передаються на інший комп'ютер, який може бути розташований де завгодно. Ця технологія в чомусь аналогічна проксі серверу, проте вона набагато простіше і набагато менш гнучка. Таким чином, port mapping - це процес пересилання даних, а віддзеркалення порту - це процес копіювання даних.

1.2 Засоби та технології дзеркалювання трафіку комутаторів Cisco

Дзеркалювання трафіку на комутаторах Cisco називається SPAN – Switch port Analyzer. SPAN копіює трафік від одного або деяких портів, каналів або віртуальних локальних мереж (VLAN) та надсилає скопійований трафік в один або декілька пунктів призначення для аналізу. SPAN не впливає на переключення трафіку по джерелам але копії трафіку конкурують за ресурси комутатора.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росієнський Ю.М.				13
Змн.	Арк.	№ докум.	Підпис	Дата		

На комутаторах Cisco існує можливість налаштування трьох видів дзеркалювання портів, а саме:

1. Локальний SPAN
2. Віддалений SPAN (Remote SPAN)
3. Інкапсульований віддалений ERSPAN (Encapsulated Remote SPAN)

Локальний сеанс SPAN – це асоціація вихідних портів та вихідних VLAN з одним або декількома пунктами призначення. Локальний SPAN не має окремих сеансів джерела та призначення. Кожен локальний сеанс SPAN може мати в якості джерел або порти або VLAN але не одночасно.

Віддалений сеанс SPAN (RSPAN) – розширення SPAN, яке дозволяє відслідковувати трафік з вихідних портів розподілених по декільком комутаторам, що дозволяє централізувати пристрій мережевого захвату. RSPAN працює шляхом дзеркалювання трафіку з вихідних портів сеансу RSPAN на VLAN, виділену для сеансу RSPAN. Далі ця VLAN з'єднується з іншими комутаторами, що дозволяє передавати трафік сеансу RSPAN через декілька комутаторів. На комутаторі, який містить порт призначення для сеансу, трафік з VLAN сеансу RSPAN просто віддзеркалюється на порт призначення.

Інкапсульований віддалений SPAN (ERSPAN) – сеанс SPAN який забезпечує загальну інкапсуляцію маршрутизації () для усього захопленого трафіку і дозволяє поширити його на домени рівня 3.

ERSPAN – це пропрієтарна функція Cisco, яка на сьогоднішній день доступна лише для платформ Catalyst 6500, 7600, Nexus та ASR 1000. ASR 1000 підтримує джерело (моніторинг) RSPAN лише на інтерфейсах Fast Ethernet, Gigabit Ethernet та порт-канал.

Для усіх видів SPAN використовується спеціальна термінологія:

- Вхідний трафік – це трафік, який поступає на комутатор.
- Вихідний трафік – трафік який залишає комутатор.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

- Порт-джерело – порт, який відстежується за допомогою функції SPAN.
- VLAN-джерело – VLAN, трафік якої відстежується за допомогою функції SPAN.
- Порт призначення – порт, відстежує порти-джерела; зазвичай це саме той порт, до якого підключений мережевий аналізатор.
- Порт-відбивач – це порт, який копіює пакети у VLAN RSPAN.

За замовчуванням локальний SPAN та ERSPAN відслідковують весь трафік, включаючи кадри багатоадресної передачі та блоку даних протоколу мосту (BPDU). RSPAN не підтримує моніторинг BPDU.

Розглянемо загальні правила та обмеження описаних вище видів дзеркалювання портів.

Будь-який з наведених видів дзеркалювання трафіку створює навантаження на ресурси комутатору та мережі. Для того аби уникнути порушення трафіку, варто не перевищувати об'єм підпису ні на одну з точок в топології SPAN.

В випуску IOS 12.2 (33) SXH та більш пізніх випусках локальні обмеження сеансів SPAN, RSPAN, ERSPAN наведені в таблиці 1.1.

Таблиця 1.1 – Обмеження сеансів локального SPAN, RSPAN та ERSPAN

Загальна кількість сенсів	Локальні та вихідні сеанси		Цільові сеанси	
	SPAN, RSPAN Source, ERSPAN Source	Лише локальний вихід SPAN	RSPAN	ERSPAN
80	2	14	64	23

Можна виділити деякі правила та обмеження що застосовуються до локальних SPAN, RSPAN та ERSPAN:

- Якщо налаштовувати більше одного вихідного порту вихідного SPAN, трафік, що надсилається на мережевий аналізатор, також включає наступні типи вхідного трафіку:
 - Будь-який одноадресний трафік, який лавинно розсилається по VLAN.
 - Широкомовний та багатоадресний трафік
- В рамках сеансу SPAN всі призначення SPAN отримують весь трафік від всіх джерел SPAN, за винятком випадків, коли фільтрація вихідної VLAN налаштована на джерелі SPAN.
- Неможна змішувати окремі вихідні порти та вихідні VLAN в рамках одного сеансу.
- Можливе налаштування декількох вихідних портів, які належать різним VLAN.
- Порти та VLAN призначення не можуть бути одночасно джерелами SPAN.
- Якщо ви вказуєте джерела та не вказуєте напрям трафіку (вхідних, вихідний або обидва), за замовчуванням використовуються обидва.
- SPAN копіює кадри Ethernet рівня 2, але SPAN не копіює теги ISL або 802.1Q вихідного магістрального порту. Можливо налаштувати місця призначення як транки для вілправки локально відміченого трафіку на аналізатор трафіку.

1.3 Принципи та засоби захоплення трафіку

Захоплення трафіку – це перший крок при будь якому аналізі трафіку на предмет як продуктивності так і безпеки. Захоплення мережевого трафіку може бути корисним для:

- Дослідження на предмет активності ПЗ (що саме програма робить в мережі, який трафік генерує).
- Траблшутінга проблем зі зв'язністю (не хоче працювати TCP-з'єднання; або працює, але потім раптово обривається).

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		16

- Діагностики поганої продуктивності як інтерактивних «балакучих» з'єднань, так і при передачі об'ємних даних.
- Мережевої безпеки, відновлення порядку подій, які відбулися в мережі.
- Deep Packet Inspection, пошуку відомих індикаторів компрометації (Indicators of Compromise, IOCs).
- Вивчення потоків в мережі і побудови графіків (Metadata, NetFlow).
- Реверс-інжинірингу (дослідження з метою зрозуміти принцип роботи) мережевих протоколів.
- Перезбирання і вилучення файлів які "пролітають" по мережі.
- Розкрадання паролів, облікових даних, токенів і т.д.

Одним з способів захвату трафіку є спеціальні програми, що встановлюються на комп'ютер в мережі. Однією з таких програм є Wireshark.

Wireshark - це передовий і широко використовуваний аналізатор мережевих протоколів. Програмний продукт Wireshark перехоплює вхідні та вихідні TCP-пакети. І завдяки вбудованим функціям моніторить вміст, шукає помилки. Помітно спрощує використання програми система фільтрів, а також простий і логічний графічний інтерфейс на фреймворку GTK + з підтримкою відкритого API (зовні вікна схожі на Windows).

Особливості програми:

1. Кросплатформеність - випускаються версії під Linux, Windows, macOS.
2. Безкоштовність - поширюється під ліцензією GNU GPL v2.
3. Простота - інсталяція полягає в декількох натисканнях кнопки «Next».

Розглянемо основні можливості програми Wireshark. Затребувані функції мережевого аналізатора Wireshark:

- Захоплення пакетів в реальному часі або при читанні з файлу.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росісський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

- Підтримка дротового інтерфейсу Ethernet, бездротових IEEE 802.11, PPP і локальних віртуальних інтерфейсів.
- Відсіювання мережевих пакетів по великій кількості встановлених фільтрів, включаючи розшифрування тільки VoIP-дзвінків, HTTPS-трафіку.
- Підсвічування різних протоколів при змішаному трафіку, виділення TCP, HTTP, FTP, DNS, ICMP і т.д.
- Розшифровка WEP-, WPA-трафіку бездротових мереж при наявності ключа безпеки і Handshake.

Паралельно програма фіксує навантаження на мережу, зберігає статистику, відображає в реальному часі відправку та отримання пакетів, але це вже другорядні функції. Основний залишається перехоплення трафіку. Тут потрібно уточнити, що використання програми має узгоджуватися з власником підмережі, інакше це цілком зійде за «хакерську атаку» з відповідними наслідками для фахівця.

1.4 Постановка технічного завдання.

Метою кваліфікаційної роботи є проектування та побудова підсистеми дзеркалювання трафіку комп'ютерної мережі організації, що передбачає виконання наступних завдань:

1. Розробка загального проекту комп'ютерної мережі організації;
2. Розробка схеми адресації спроектованої мережі;
3. Розробка підсистеми захисту спроектованої мережі організації;
4. Аналіз та розробка структури Windows мережі;
5. Вибір мережевого обладнання;
6. Налаштування необхідних функцій на мережевому обладнанні;
7. Налаштування Windows мережі;
8. Тестування працездатності налагодженої мережі.

При розробці загального проекту мережі організації необхідно спроектувати загальну структуру мережі та поділ на підмережі філій. Також

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

необхідно розробити загальну схему зв'язку центральної мережі з пристроями підмереж.

При розробці схеми адресації необхідно для усіх рівнів мережі обрати IP-адреси та розподілити їх між пристроями.

При розробці підсистеми захисту необхідно врахувати можливість впливу атак на мережеве обладнання та уникнути їх.

При аналізі та розробці структури Windows мережі необхідно врахувати особливості роботи серверів на базі обраної серверної ОС – Windows Server 2019.

Після проектування усіх вищевказаних пунктів потрібно перейти до налаштування функцій дзеркалювання трафіку, а саме SPAN, RSPAN та ERSPAN. Також необхідно налаштувати сервери на базі ОС Windows Server 2019 та усі кінцеві вузли.

Після налагодження усього необхідного обладнання необхідно провести тестування працездатності комп'ютерної мережі організації та перевірити правильність виконання усіх поставлених задач.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

РОЗДІЛ 2. ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ПІДСИСТЕМИ ДЗЕРКАЛЮВАННЯ ТРАФІКУ

2.1 Проектування топології комп'ютерної мережі організації

При проектуванні мережі буде використана трирівнева ієрархічна модель мережі, в якій використовуються три рівні:

- Рівень ядра (Core layer);
- Рівень розподілу (Distribution layer);
- Рівень доступу (Access layer).

Загальна топологія спроектованої мережі представлена на рисунку 2.1

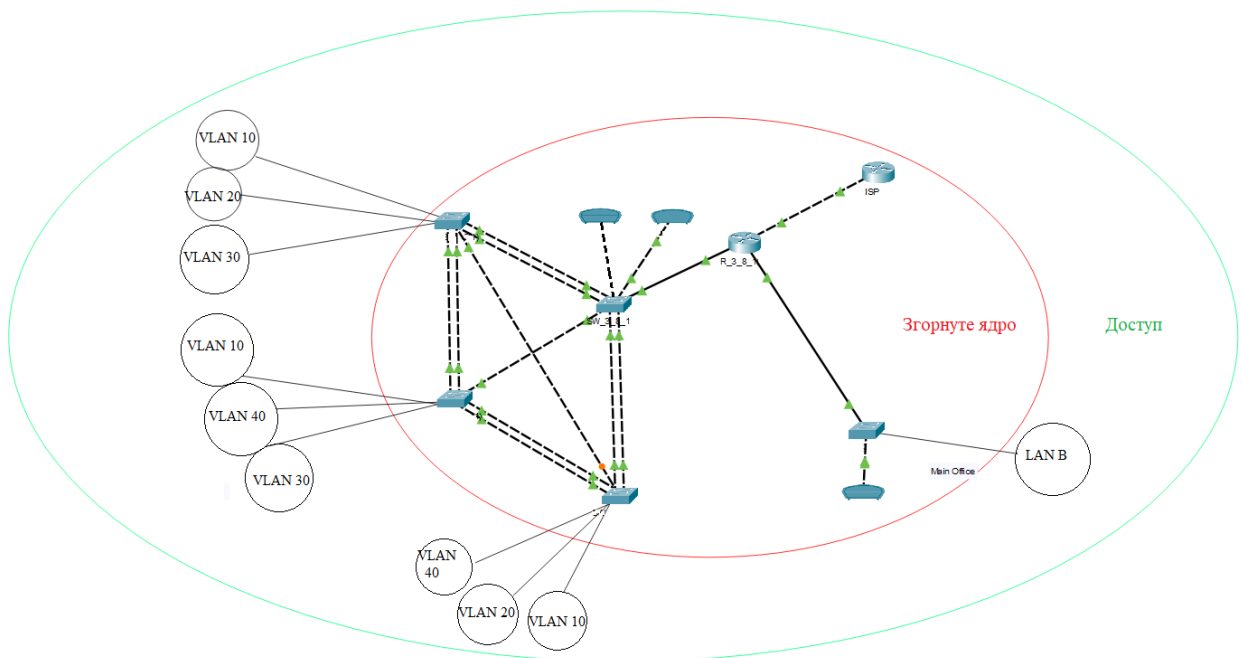


Рисунок 2.1 – Загальна топологія спроектованої мережі

Рівень ядра в даній мережі – згорнуте ядро, що виконує функції ядра та одночасно рівня розподілу. Рівень ядра складається складається зі з'єднаних між собою в одній підмережі чотирма комутаторами, в іншій – одним, за допомогою витої пари для забезпечення високої швидкості на даному рівні.

Рівень доступу представлений кінцями вузлами, які відносяться до різних вланів, саме з'єднання до рівня розподілу забезпечуються витою парою Fast Ethernet.

У загальному в мережі використано два маршрутизатори. Мережа складається з шести підмереж, які розподілені на різні влани.

Розглянемо детальніше спроектовану мережу.

Загальна структура мережі показана в додатку А.

Рівень доступу складається з двох основних підмереж А та В, чотирьох VLAN підключених до маршрутизатору рівня ядра та комутаторів рівня розподілу. Поділ на віртуальні локальні мережі здійснюється з метою об'єднати комп'ютерів в логічні групи по виду зайнятості працівників мережі.

До центрального комутатора SW_3_8_1 підключені три комутатори рівня ядра, які передають увесь трафік з чотирьох Vlan на підключені до нього аналізатори трафіку.

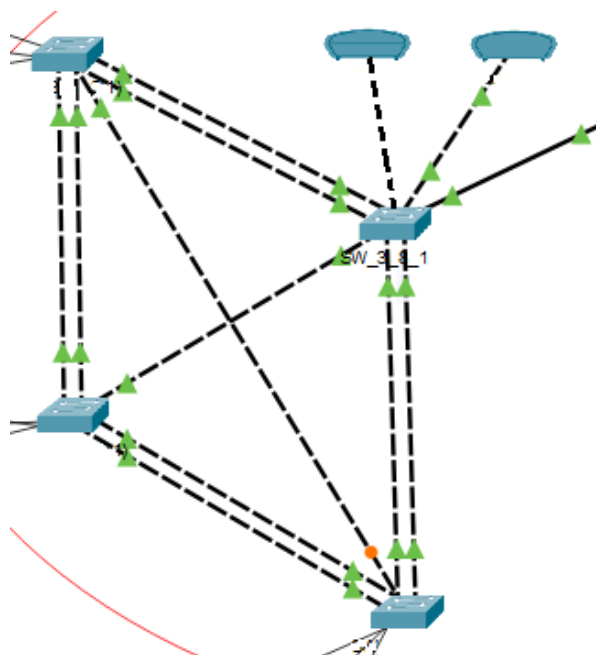


Рисунок 2.2 – Центральний комутатор з'єднаний з трьома комутаторами та аналізатором трафіку

До комутатора SW_3_8_2 підключені три VLAN, які мають по два кінцевих вузли.

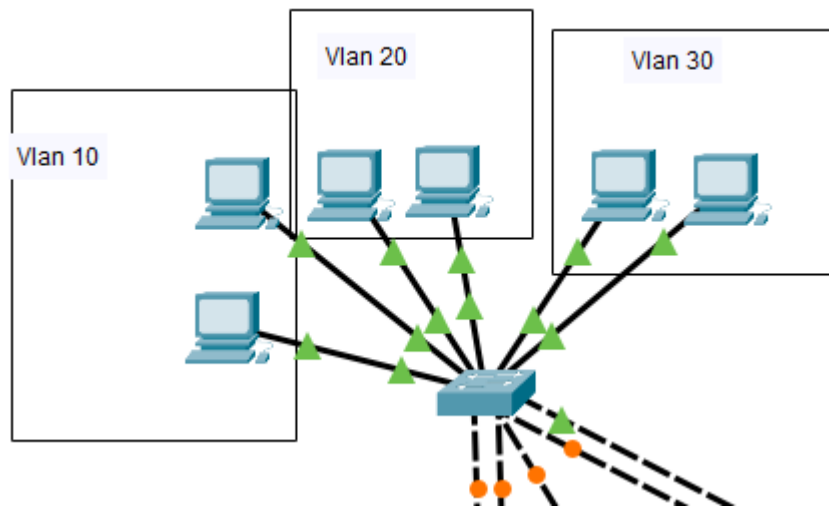


Рисунок 2.3 – Комутатор SW_3_8_2 та підключені до нього три VLAN
До комутатору SW_3_8_3 підключені два VLAN, які мають по два кінцевих вузли.

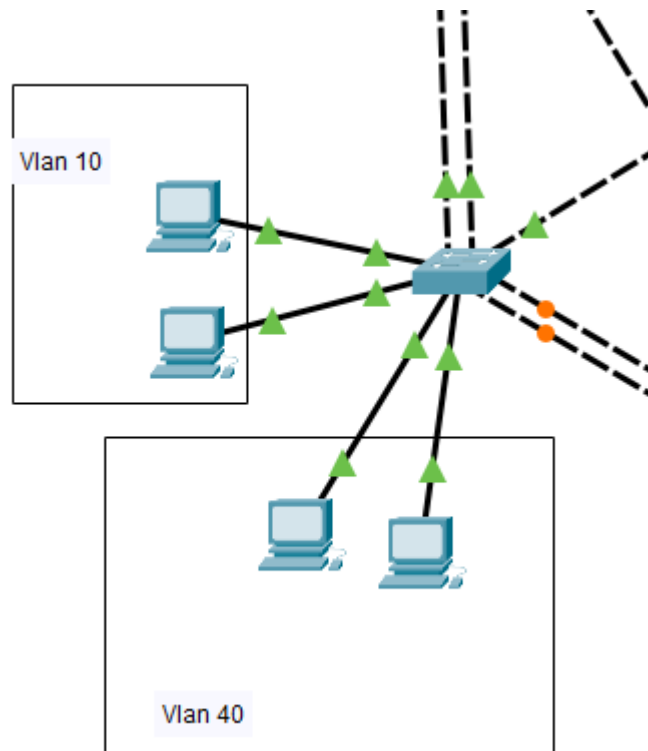


Рисунок 2.4 – Комутатор SW_3_8_3 та підключені до нього два VLAN

До комутатора SW_3_8_4 підключені три VLAN по два комп'ютери:

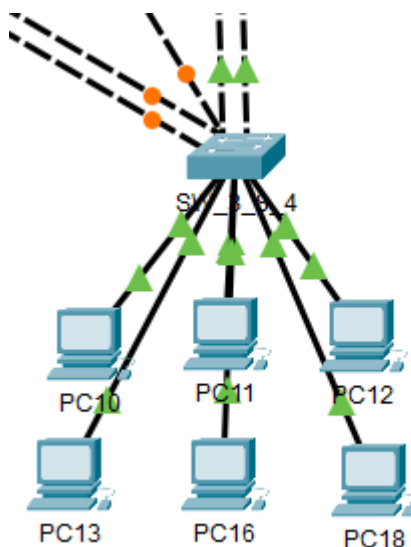


Рисунок 2.5 – Комутатор SW_3_8_4 та підключені до нього сервери

До комутатору SPAN_SW, який знаходиться в головному офісі організації, підключені три кінцевих вузла та Sniffer.

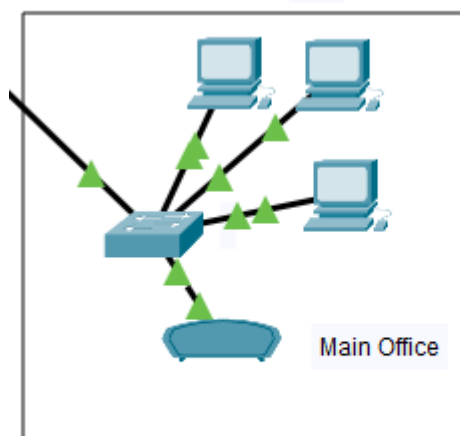


Рисунок 2.6 – Комутатор SPAN_SW та підключені до нього пристрої.

Загалом сумарна кількість кінцевих вузлів кожної VLAN наведено в таблиці 2.1.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Таблиця 2.1 – Загальна кількість кінцевих вузлів кожної VLAN

Номер VLAN	Загальна кількість кінцевих вузлів
10	4
20	2
30	2
40	2
100 (remote)	1

2.2 Розробка схеми адресації мережі

Для усієї мережі обрані IPv4 адреси, які наведено в таблиці 2.2

Для рівня ядра, а саме для трьох маршрутизаторів використано адреси вигляду 32.135.10.0 з префіксом /52, адресація інтерфейсів пристроїв мережі наведено в таблиці 2.3.

Таблиця 2.2 – IPv4 адреси мереж

Ім'я мережі	IPv4-адреса	Маска мережі	Префікс мережі
A	10.3.8.0	255.255.255.240	/28
B	10.3.8.16	255.255.255.240	/28
C	32.135.10.0	255.255.255.252	/30
D	32.135.10.4	255.255.255.252	/30
E	91.146.8.32	255.255.255.248	/29
VLAN 10	192.168.1.0	255.255.255.0	/24
VLAN 20	192.168.2.0	255.255.255.0	/24
VLAN 30	192.168.3.0	255.255.255.0	/24
VLAN 40	192.168.4.0	255.255.255.0	/24

Таблиця 2.3 – Адресація пристроїв мережі на рівні ядра

Пристрій мережі	Інтерфейс	IPv4-адреса	Маска мережі	Префікс мережі
Маршрутизатор R_3_8_1	Gig 2/0	32.135.10.1	255.255.255.252	/30
	Gig 0/0	10.3.8.1	255.255.255.240	/28
	Gig 1/0	10.3.8.17	255.255.255.240	/28
	Gig 0/0.10	192.168.1.1	255.255.255.0	/24
	Gig 0/0.20	192.168.2.1	255.255.255.0	/24
	Gig 0/0.30	192.168.3.1	255.255.255.0	/24
	Gig 0/0.40	192.168.4.1	255.255.255.252	/30
Маршрутизатор ISP	Gig 0/0	32.135.10.2	255.255.255.252	/30
	Gig 1/0	32.135.10.5	255.255.255.252	/30

Для комутаторів рівня розподілу та рівня доступу використовуються дві різні підмережі та чотири Vlan. Адресація вище вказаних пристроїв мережі наведена в таблиці 2.4:

Таблиця 2.4 – Адресація пристроїв мережі на рівні розподілу, рівні доступу

Пристрій мережі	Інтерфейс	IPv4-адреса	Маска мережі	Префікс мережі
Комутатор SW_3_8_1	Vlan 1	10.3.8.2	255.255.255.240	/28
	Vlan 10	192.168.1.2	255.255.255.0	/24
	Vlan 20	192.168.2.2	255.255.255.0	/24
	Vlan 30	192.168.3.2	255.255.255.0	/24
	Vlan 40	192.168.4.2	255.255.255.0	/24
Комутатор SW_3_8_2	Vlan 1	10.3.8.3	255.255.255.240	/28
	Vlan 10	192.168.1.3	255.255.255.0	/24
	Vlan 20	192.168.2.3	255.255.255.0	/24
	Vlan 30	192.168.3.3	255.255.255.0	/24
	Vlan 40	192.168.4.3	255.255.255.0	/24
Комутатор SW_3_8_3	Vlan 1	10.3.8.4	255.255.255.240	/28
	Vlan 10	192.168.1.4	255.255.255.0	/24
	Vlan 20	192.168.2.4	255.255.255.0	/24
	Vlan 30	192.168.3.4	255.255.255.0	/24
Комутатор SW_3_8_3	Vlan 40	192.168.4.4	255.255.255.0	/24
Комутатор SW_3_8_4	Vlan 1	10.3.8.5	255.255.255.240	/28
	Vlan 10	192.168.1.5	255.255.255.0	/24
	Vlan 20	192.168.2.5	255.255.255.0	/24

Таблиця 2.4 – Адресація пристроїв мережі на рівні розподілу, рівні доступу (Продовження)

Комутатор SW_3_8_4	Vlan 30	192.168.3.5	255.255.255.0	/24
	Vlan 40	192.168.4.5	255.255.255.0	/24
Комутатор SPAN_SW	Vlan 1	10.3.8.18	255.255.255.240	/28

Адресація кінцевих вузлів здійснюється за допомогою DHCP.

2.3 Розробка підсистеми дзеркалювання трафіку

Підсистему дзеркалювання трафіку буде реалізовано на базі комутаторів Cisco Catalyst.

Підсистема дзеркалювання трафіку в комутаторах Cisco реалізовується за допомогою функцій SPAN. Як було розглянуто в першому розділі, SPAN існує трьох видів: локальний SPAN, RSPAN та ERSPAN. Кожен з цих видів дзеркалювання буде реалізований в підсистемі дзеркалювання трафіку.

Локальний SPAN буде доцільно використати на комутаторі SPAN_SW, для контролю трафіку комп'ютерів які знаходяться в головному офісі організації.

Так як підмережа А є досить об'ємною, складається з чотирьох комутаторів та містить поділ на VLAN, для централізації та спрощення огляду віддзеркалених пакетів буде правильним використати віддалений SPAN (RSPAN). Для розмежування більш цінного трафіку необхідно розділити дзеркалювання на дві сесії. Перша сесія дзеркалювання трафіку буде охоплювати конкретні порти, а саме порти до яких підключені комп'ютери директорів організації. Друга сесія віддзеркалюватиме трафік усіх VLAN на кожному комутаторі. Віддзеркалений трафік першої сесії буде приходити на Sniffer_1, другої – на Sniffer_2.

Також для контролю всієї мережі централізовано необхідно налаштувати інкапсульований віддалений SPAN (ERSPAN). ERSPAN налаштовується між двома комутаторами рівня L3 моделі OCI. Пакети будуть

дзеркалюватися на центральному комутаторі підмережі А та відправлятися на центральний комутатор підмережі Б комп’ютерної мережі організації.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

РОЗДІЛ 3. НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ РОБОТИ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ПІДСИСТЕМИ ДЗЕРКАЛЮВАННЯ ТРАФІКУ

3.1 Вибір обладнання та програмного забезпечення для реалізації проекту комп'ютерної мережі та підсистеми дзеркалювання трафіку

Для побудови комп'ютерної мережі організації можна використати велику кількість мережевих пристроїв компанії Cisco. Існує декілька серій мережевого обладнання Cisco з підтримкою дзеркалювання трафіку. З усіх серій можна виокремити три – це Catalyst, Nexus та маршрутизатори Cisco ASR 1000.

Для реалізації проекту підсистеми дзеркалювання трафіку було обрано комутатори серії Cisco Catalyst. Підтримка SPAN пристроями компанії Cisco серії Catalyst наведена в додатку Б таблиця Б.1.

З даних наведених в таблиці можна побачити, що єдиними комутаторами з підтримкою ERSPAN є Cisco Catalyst 6000/6500. Тому було б правильним обрати саме ці комутатори для роботи з інкапсульованим віддаленим дзеркалюванням трафіку.

Для рівня розподілу порівняємо три комутатори з підтримкою SPAN та наведемо порівняльну таблицю з основними характеристиками (таблиця 3.1).

Таблиця 3.1 – Порівняння основних характеристик комутаторів Cisco Catalyst

	Catalyst WS-C3750X-48T-L	Catalyst WS-C3550-24-SMI	WS-C2970G-24T-E
Працює на рівні	2	2	2
Кількість мережевих портів	48	24	24
Технологія портів	Gigabit Ethernet	Fast Ethernet	Gigabit Ethernet
Пам'ять	256 Mb	64 Mb	128 Mb
Flash пам'ять	128 Mb	16 Mb	16 Mb

З поданої таблиці можна зробити висновок, що для подальшої роботи комутатор Cisco Catalyst WS-C3550-24-SMI підходить менше всього, бо має досить малий, в порівнянні з іншими, об'єм пам'яті та порти Fast Ethernet, що може значно сповільнити роботу мережі. З огляду на подальше можливе розширення мережі, для її справної роботи було обрано комутатор Cisco Catalyst WS-C3750X-48T-L, як комутатор з достатнім об'ємом пам'яті та кількістю портів Gigabit Ethernet.

Для перехоплення віддаленого віддзеркаленого трафіку будуть використовуватись сніфери – спеціальні пристрої що відображають весь вхідний трафік. Для перехоплення локального SPAN було обрано програму Wireshark. Дана програма є кроплатформеною, що дозволяє в якості комп'ютеру, на якому вона буде встановлена, використовувати ОС як сімейства Windows так і Linux та інші. Також за допомогою цієї програми можна зберігати, для подальшої обробки, увесь перехоплений трафік.

3.2 Налаштування проміжних та кінцевих вузлів мережі

Потрібно налагодити маршрутизатор підмережі, а саме налагодити функціонування транкового протоколу та DHCP.

Сценарій налагодження параметрів на маршрутизаторі R_3_8_1:

```
...
R_3_8_1(config)#hostname R_3_8_1
R_3_8_1(config)#interface gig0/0
R_3_8_1(config-if)#ip address 10.3.8.1 255.255.255.240
R_3_8_1(config-if)#no shutdown
R_3_8_1(config-if)#exit
R_3_8_1(config)#interface gig0/0.10
R_3_8_1(config-subif)#encapsulation dot1q 10
R_3_8_1(config-subif)#ip address 192.168.1.1 255.255.255.0
R_3_8_1(config-subif)#exit
R_3_8_1(config)#interface gig0/0.20
R_3_8_1(config-subif)#encapsulation dot1q 20
R_3_8_1(config-subif)#ip address 192.168.2.1 255.255.255.0
R_3_8_1(config-subif)#exit
R_3_8_1(config)#interface gig0/0.30
R_3_8_1(config-subif)#encapsulation dot1q 30
R_3_8_1(config-subif)#ip address 192.168.3.1 255.255.255.0
R_3_8_1(config-subif)#exit
R_3_8_1(config)#interface gig0/0.40
R_3_8_1(config-subif)#encapsulation dot1q 40
```

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				29
Змн.	Арк.	№ докум.	Підпис	Дата		

```

R_3_8_1(config-subif)#ip address 192.168.4.1 255.255.255.0
R_3_8_1(config-subif)#exit
R_3_8_1(config)#interface gig1/0
R_3_8_1(config-if)#ip address 10.3.8.17 255.255.255.240
R_3_8_1(config-if)#no shutdown
R_3_8_1(config-if)#exit
R_3_8_1(config)#
R_3_8_1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.5
R_3_8_1(config)#ip dhcp excluded-address 192.168.2.1 192.168.2.5
R_3_8_1(config)#ip dhcp excluded-address 192.168.3.1 192.168.3.5
R_3_8_1(config)#ip dhcp excluded-address 192.168.4.1 192.168.4.5
R_3_8_1(config)#ip dhcp excluded-address 10.3.8.17 10.3.8.18
R_3_8_1(config)#
R_3_8_1(config)#ip dhcp pool VLAN10
R_3_8_1(dhcp-config)#network 192.168.1.0 255.255.255.0
R_3_8_1(dhcp-config)#default-router 192.168.1.1
R_3_8_1(dhcp-config)#dns-server 10.3.8.6
R_3_8_1(dhcp-config)#exit
R_3_8_1(config)#ip dhcp pool VLAN20
R_3_8_1(dhcp-config)#network 192.168.2.0 255.255.255.0
R_3_8_1(dhcp-config)#default-router 192.168.2.1
R_3_8_1(dhcp-config)#dns-server 10.3.8.6
R_3_8_1(dhcp-config)#exit
R_3_8_1(config)#ip dhcp pool VLAN30
R_3_8_1(dhcp-config)#network 192.168.3.0 255.255.255.0
R_3_8_1(dhcp-config)#default-router 192.168.3.1
R_3_8_1(dhcp-config)#dns-server 10.3.8.6
R_3_8_1(dhcp-config)#exit
R_3_8_1(config)#ip dhcp pool VLAN40
R_3_8_1(dhcp-config)#network 192.168.4.0 255.255.255.0
R_3_8_1(dhcp-config)#default-router 192.168.4.1
R_3_8_1(dhcp-config)#dns-server 10.3.8.6
R_3_8_1(dhcp-config)#exit
R_3_8_1(config)#ip dhcp pool LAN_B
R_3_8_1(dhcp-config)#network 10.3.8.16 255.255.255.240
R_3_8_1(dhcp-config)#default-router 10.3.8.17
R_3_8_1(dhcp-config)#dns-server 10.3.8.6
R_3_8_1(dhcp-config)#exit
R_3_8_1(config)#
R_3_8_1(config)#interface gig2/0
R_3_8_1(config-if)#ip address 32.135.10.1 255.255.255.252
R_3_8_1(config-if)#no shutdown
R_3_8_1(config-if)#exit
R_3_8_1(config)#
...
```

Також для забезпечення зв'язку з мережею інтернет налаштуємо NAT. Так як кількість вузлів в мережі є досить великою буде доцільно налаштувати Port Address Translation NAT, який дозволить зіставити декілька адрес однією – адресою порту який веде до маршрутизатора ISP.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

Сценарій налагодження параметрів PAT на маршрутизаторі R_3_8_1:

```
...
R_3_8_1(config)#access-list 1 permit 192.168.1.1 0.0.0.255
R_3_8_1(config)#access-list 1 permit 192.168.2.1 0.0.0.255
R_3_8_1(config)#access-list 1 permit 192.168.3.1 0.0.0.255
R_3_8_1(config)#access-list 1 permit 192.168.4.1 0.0.0.255
R_3_8_1(config)#access-list 1 permit 10.3.8.0 0.0.0.15
R_3_8_1(config)#access-list 1 permit 10.3.8.16 0.0.0.15
R_3_8_1(config)#
R_3_8_1(config)#ip nat inside source list 1 interface gig2/0 overload
R_3_8_1(config)#interface gig0/0
R_3_8_1(config-if)#ip nat inside
R_3_8_1(config-if)#exit
R_3_8_1(config)#interface gig0/0.10
R_3_8_1(config-subif)#ip nat inside
R_3_8_1(config-subif)#exit
R_3_8_1(config)#interface gig0/0.20
R_3_8_1(config-subif)#ip nat inside
R_3_8_1(config-subif)#exit
R_3_8_1(config)#interface gig0/0.30
R_3_8_1(config-subif)#ip nat inside
R_3_8_1(config-subif)#exit
R_3_8_1(config)#interface gig0/0.40
R_3_8_1(config-subif)#ip nat inside
R_3_8_1(config-subif)#exit
R_3_8_1(config)#interface gig1/0
R_3_8_1(config-if)#ip nat inside
R_3_8_1(config-if)#exit
R_3_8_1(config)#interface gig2/0
R_3_8_1(config-if)#ip nat outside
R_3_8_1(config-if)#exit
...
```

3.3 Налаштування підсистеми дзеркалювання трафіку

Через відсутність та дороговизну реального обладнання немає змоги налагодити спроектовану мережу на реальному обладнанні, тому для реалізації підсистеми дзеркалювання трафіку буде використано програми GNS3 та Cisco Packet Tracer.

Зважаючи на різницю архітектур комп'ютера та комутаторів Cisco Catalyst емуляція їх в GNS3 неможлива. З огляду на вищевикладене налагодження мережі буде проводитися на комутаторах Cisco Catalyst 2960 в програмному середовищі Packet Tracer та, частково, на маршрутизаторі Cisco c3725, з модулем комутації NM-16ESW, в програмному емуляторі GNS3.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Налагодження функцій SPAN відрізняється в залежності від операційної системи, але для обраних, в пункті 3.1, комутаторів та комутатора Cisco Catalyst 2960 налаштування відбувається однаково тому сценарій налагодження можна застосовувати для реального обладнання.

Загальне налагодження підсистеми дзеркалювання трафіку можна розбити на два етапи: налагодження головних функцій підсистеми комп'ютерної мережі організації та налагодження додаткових функцій.

До налагодження основних функцій можна віднести:

- Налагодження локального дзеркалювання трафіку (Локальний SPAN);
- Налагодження віддаленого дзеркалювання трафіку (Remote SPAN);
- Налагодження інкапсульованого віддаленого дзеркалювання трафіку (ERSPAN).

До налагодження додаткових функцій належить:

- Налаштування статичного агрегування каналів;
- Налаштування RPTVST;
- Налаштування захисту комутаторів від деяких видів атак;
- Налагодження DHCP серверів;
- Налагодження динамічної маршрутизації на маршрутизаторах рівня ядра мережі;

Першим кроком налагодження параметрів підсистеми дзеркалювання трафіку мережі організації буде налагодження базових параметрів IP-адресації та створення VLAN'ів.

Сценарій налагодження базових параметрів на комутаторі SW_3_8_1 наведено нижче:

```
...
Switch(config)#hostname SW_3_8_1
SW_3_8_1(config)#vlan 10
SW_3_8_1(config-vlan)#name VLAN_10
SW_3_8_1(config-vlan)#exit
SW_3_8_1(config)#vlan 20
```

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

```

SW_3_8_1(config-vlan)#name VLAN_20
SW_3_8_1(config-vlan)#exit
SW_3_8_1(config)#vlan 30
SW_3_8_1(config-vlan)#name VLAN_30
SW_3_8_1(config-vlan)#exit
SW_3_8_1(config)#vlan 40
SW_3_8_1(config-vlan)#name VLAN_40
SW_3_8_1(config-vlan)#exit
SW_3_8_1(config)#interface vlan 1
SW_3_8_1(config-if)#ip address 10.3.8.2 255.255.255.240
SW_3_8_1(config-if)#no shutdown
SW_3_8_1(config-if)#exit
SW_3_8_1(config)#interface vlan 10
SW_3_8_1(config-if)#ip address 192.168.1.2 255.255.255.0
SW_3_8_1(config-if)#exit
SW_3_8_1(config)#interface vlan 20
SW_3_8_1(config-if)#ip address 192.168.2.2 255.255.255.0
SW_3_8_1(config-if)#exit
SW_3_8_1(config)#interface vlan 30
SW_3_8_1(config-if)#ip address 192.168.3.2 255.255.255.0
SW_3_8_1(config-if)#exit
SW_3_8_1(config)#interface vlan 40
SW_3_8_1(config-if)#ip address 192.168.4.2 255.255.255.0
SW_3_8_1(config-if)#exit

```

...

Сценарій налагодження базових параметрів на комутаторі SW_3_8_2

наведено нижче:

...

```

Switch(config)#hostname SW_3_8_2
SW_3_8_2(config)#vlan 10
SW_3_8_2(config-vlan)#name VLAN_10
SW_3_8_2(config-vlan)#exit
SW_3_8_2(config)#vlan 20
SW_3_8_2(config-vlan)#name VLAN_20
SW_3_8_2(config-vlan)#exit
SW_3_8_2(config)#vlan 30
SW_3_8_2(config-vlan)#name VLAN_30
SW_3_8_2(config-vlan)#exit
SW_3_8_2(config)#vlan 40
SW_3_8_2(config-vlan)#name VLAN_40
SW_3_8_2(config-vlan)#exit
SW_3_8_2(config)#interface vlan 1
SW_3_8_2(config-if)#ip address 10.3.8.3 255.255.255.240
SW_3_8_2(config-if)#no shutdown
SW_3_8_2(config-if)#exit
SW_3_8_2(config)#interface vlan 10
SW_3_8_2(config-if)#ip address 192.168.1.3 255.255.255.0
SW_3_8_2(config-if)#exit
SW_3_8_2(config)#interface vlan 20
SW_3_8_2(config-if)#ip address 192.168.2.3 255.255.255.0

```

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

```

SW_3_8_2(config-if)#exit
SW_3_8_2(config)#interface vlan 30
SW_3_8_2(config-if)#ip address 192.168.3.3 255.255.255.0
SW_3_8_2(config-if)#exit
SW_3_8_2(config)#interface vlan 40
SW_3_8_2(config-if)#ip address 192.168.4.3 255.255.255.0
SW_3_8_2(config-if)#exit

```

...

Комутатори SW_3_8_3 та SW_3_8_4 налаштуваються аналогічним чином.

Для забезпечення кращої роботи локальної мережі налаштуємо агрегацію каналів що з'єднують комутатори між собою. Агреговані канали налаштуємо на передачу віртуальних локальних мереж (VLAN) за допомогою протоколу 802.1q.

Сценарій налагодження параметрів статичної агрегації на комутаторі SW_3_8_1 наведено нижче:

...

```

SW_3_8_1(config)#interface range fa0/3-4
SW_3_8_1(config-if-range)#shutdown
SW_3_8_1(config-if-range)#channel-group 1 mode on
SW_3_8_1(config-if-range)#no shutdown
SW_3_8_1(config-if-range)#exit
SW_3_8_1(config)#interface range fa0/1-2
SW_3_8_1(config-if-range)#shutdown
SW_3_8_1(config-if-range)#channel-group 2 mode on
SW_3_8_1(config-if-range)#no shutdown
SW_3_8_1(config-if-range)#exit
SW_3_8_1(config)#interface port-channel 1
SW_3_8_1(config-if)#switchport mode trunk
SW_3_8_1(config-if)#switchport nonegotiate
SW_3_8_1(config-if)#switchport trunk allowed vlan add 10
SW_3_8_1(config-if)#switchport trunk allowed vlan add 20
SW_3_8_1(config-if)#switchport trunk allowed vlan add 30
SW_3_8_1(config-if)#switchport trunk allowed vlan add 40
SW_3_8_1(config-if)#exit
SW_3_8_1(config)#interface port-channel 2
SW_3_8_1(config-if)#switchport mode trunk
SW_3_8_1(config-if)#switchport nonegotiate
SW_3_8_1(config-if)#switchport trunk allowed vlan add 10
SW_3_8_1(config-if)#switchport trunk allowed vlan add 20
SW_3_8_1(config-if)#switchport trunk allowed vlan add 30
SW_3_8_1(config-if)#switchport trunk allowed vlan add 40
SW_3_8_1(config-if)#exit
SW_3_8_1(config)#interface gig0/2
SW_3_8_1(config-if)#switchport mode trunk

```

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

```

SW_3_8_1(config-if)#switchport nonegotiate
SW_3_8_1(config-if)#switchport trunk allowed vlan add 10
SW_3_8_1(config-if)#switchport trunk allowed vlan add 20
SW_3_8_1(config-if)#switchport trunk allowed vlan add 30
SW_3_8_1(config-if)#switchport trunk allowed vlan add 40
SW_3_8_1(config-if)#exit
SW_3_8_1(config)#interface gig0/1
SW_3_8_1(config-if)#switchport mode trunk
SW_3_8_1(config-if)#switchport nonegotiate
SW_3_8_1(config-if)#switchport trunk allowed vlan add 10
SW_3_8_1(config-if)#switchport trunk allowed vlan add 20
SW_3_8_1(config-if)#switchport trunk allowed vlan add 30
SW_3_8_1(config-if)#switchport trunk allowed vlan add 40
SW_3_8_1(config-if)#exit

```

...

Сценарій налагодження параметрів статичної агрегації каналів на комутаторі SW_3_8_2 наведено нижче:

...

```

SW_3_8_2(config)#interface range fa0/3-4
SW_3_8_2(config-if-range)#shutdown
SW_3_8_2(config-if-range)#channel-group 1 mode on
SW_3_8_2(config-if-range)#no shutdown
SW_3_8_2(config-if-range)#exit
SW_3_8_2(config)#interface range fa0/1-2
SW_3_8_2(config-if-range)#shutdown
SW_3_8_2(config-if-range)#channel-group 2 mode on
SW_3_8_2(config-if-range)#no shutdown
SW_3_8_2(config-if-range)#exit
SW_3_8_2(config)#interface port-channel 1
SW_3_8_2(config-if)#switchport mode trunk
SW_3_8_2(config-if)#switchport nonegotiate
SW_3_8_2(config-if)#switchport trunk allowed vlan add 10
SW_3_8_2(config-if)#switchport trunk allowed vlan add 20
SW_3_8_2(config-if)#switchport trunk allowed vlan add 30
SW_3_8_2(config-if)#switchport trunk allowed vlan add 40
SW_3_8_2(config-if)#exit
SW_3_8_2(config)#interface port-channel 2
SW_3_8_2(config-if)#switchport mode trunk
SW_3_8_2(config-if)#switchport nonegotiate
SW_3_8_2(config-if)#switchport trunk allowed vlan add 10
SW_3_8_2(config-if)#switchport trunk allowed vlan add 20
SW_3_8_2(config-if)#switchport trunk allowed vlan add 30
SW_3_8_2(config-if)#switchport trunk allowed vlan add 40
SW_3_8_2(config-if)#exit
SW_3_8_2(config)#interface gig0/1
SW_3_8_2(config-if)#switchport mode trunk
SW_3_8_2(config-if)#switchport nonegotiate
SW_3_8_2(config-if)#switchport trunk allowed vlan add 10
SW_3_8_2(config-if)#switchport trunk allowed vlan add 20
SW_3_8_2(config-if)#switchport trunk allowed vlan add 30

```

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		35

```

SW_3_8_2(config-if)#switchport trunk allowed vlan add 40
SW_3_8_2(config-if)#exit
SW_3_8_2(config)#interface range fa0/6-7
SW_3_8_2(config-if-range)#switchport mode access
SW_3_8_2(config-if-range)#switchport access vlan 30
SW_3_8_2(config-if-range)#exit
SW_3_8_2(config)#interface range fa0/8-9
SW_3_8_2(config-if-range)#switchport mode access
SW_3_8_2(config-if-range)#switchport access vlan 20
SW_3_8_2(config-if-range)#exit
SW_3_8_2(config)#interface range fa0/10-11
SW_3_8_2(config-if-range)#switchport mode access
SW_3_8_2(config-if-range)#switchport access vlan 10
SW_3_8_2(config-if-range)#exit
SW_3_8_2(config)#

```

...

Також для покращення ефективності з'єднань налагодимо роботу протоколу RPVST+.

Сценарій налагодження параметрів протоколу RPVST+ на комутаторі SW_3_8_1 наведено нижче:

...

```

SW_3_8_1(config)#spanning-tree mode rapid-pvst
SW_3_8_1(config)#spanning-tree vlan 1 root primary
SW_3_8_1(config)#interface port-channel 1
SW_3_8_1(config-if)#spanning-tree vlan 10 port-priority 16
SW_3_8_1(config-if)#spanning-tree vlan 20 port-priority 16
SW_3_8_1(config-if)#spanning-tree vlan 30 port-priority 16
SW_3_8_1(config-if)#spanning-tree vlan 40 port-priority 16
SW_3_8_1(config-if)#exit
SW_3_8_1(config)#interface port-channel 2
SW_3_8_1(config-if)#spanning-tree vlan 10 port-priority 16
SW_3_8_1(config-if)#spanning-tree vlan 20 port-priority 16
SW_3_8_1(config-if)#spanning-tree vlan 30 port-priority 16
SW_3_8_1(config-if)#spanning-tree vlan 40 port-priority 16
SW_3_8_1(config-if)#exit
SW_3_8_1(config)#interface gig0/2
SW_3_8_1(config-if)#spanning-tree vlan 10 port-priority 16
SW_3_8_1(config-if)#spanning-tree vlan 20 port-priority 16
SW_3_8_1(config-if)#spanning-tree vlan 30 port-priority 16
SW_3_8_1(config-if)#spanning-tree vlan 40 port-priority 16
SW_3_8_1(config-if)#exit

```

...

Сценарій налагодження параметрів та протоколу RPVST+ на комутаторі SW_3_8_2 наведено нижче:

...

```

SW_3_8_2(config)#spanning-tree mode rapid-pvst

```

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

```

SW_3_8_2(config)#spanning-tree vlan 1 root secondary
SW_3_8_2(config)#interface port-channel 1
SW_3_8_2(config-if)#spanning-tree vlan 10 port-priority 32
SW_3_8_2(config-if)#spanning-tree vlan 20 port-priority 32
SW_3_8_2(config-if)#spanning-tree vlan 30 port-priority 32
SW_3_8_2(config-if)#spanning-tree vlan 40 port-priority 32
SW_3_8_2(config-if)#exit
SW_3_8_2(config)#interface port-channel 2
SW_3_8_2(config-if)#spanning-tree vlan 10 port-priority 64
SW_3_8_2(config-if)#spanning-tree vlan 20 port-priority 64
SW_3_8_2(config-if)#spanning-tree vlan 30 port-priority 64
SW_3_8_2(config-if)#spanning-tree vlan 40 port-priority 64
SW_3_8_2(config-if)#exit
SW_3_8_2(config)#interface gig0/2
SW_3_8_2(config-if)#spanning-tree vlan 10 port-priority 48
SW_3_8_2(config-if)#spanning-tree vlan 20 port-priority 48
SW_3_8_2(config-if)#spanning-tree vlan 30 port-priority 48
SW_3_8_2(config-if)#spanning-tree vlan 40 port-priority 48
SW_3_8_2(config-if)#exit

```

...

Усі підготовчі налаштування підмережі А закінчені, тепер можна перейти до налагодження дзеркалювання портів. В даній підмережі буде доцільно використовувати віддалене дзеркалювання портів (RSPAN). Для цього необхідно на кожному комутаторі підмережі створити Remote VLAN, дозволити його передачу засобами транку та налаштувати сесію моніторингу, де джерелом моніторингу першої сесії будуть раніше створені VLAN під номерами 10, 20, 30 та 40, другої – порти до яких підключені важливі комп'ютери. Для зменшення кількості дубльованих пакетів будемо відслідковувати лише вхідні пакети (в налаштуваннях tx). На всіх комутаторах, крім SW_3_8_1, призначенням сесії моніторингу буде налаштована Remote VLAN, та порт відображення – Fast Ethernet 0/24.

Сценарій налагодження параметрів дзеркалювання портів на комутаторі SW_3_8_1 наведено нижче:

...

```

SW_3_8_1(config)#interface port-channel 1
SW_3_8_1(config-if)#switchport trunk allowed vlan add 100
SW_3_8_1(config-if)#switchport trunk allowed vlan add 101
SW_3_8_1(config-if)#exit
SW_3_8_1(config)#interface port-channel 2
SW_3_8_1(config-if)#switchport trunk allowed vlan add 100
SW_3_8_1(config-if)#switchport trunk allowed vlan add 101
SW_3_8_1(config-if)#exit

```

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		37

```

SW_3_8_1(config)#interface gig0/2
SW_3_8_1(config-if)#switchport trunk allowed vlan add 100
SW_3_8_1(config-if)#switchport trunk allowed vlan add 101
SW_3_8_1(config-if)#exit
SW_3_8_1(config)#monitor session 2 source remote vlan 101
SW_3_8_1(config)#monitor session 2 destination interface fa0/5

```

...

Сценарій налагодження параметрів дзеркалювання портів на комутаторі SW_3_8_2 наведено нижче:

...

```

SW_3_8_2(config)#vlan 100
SW_3_8_2(config-vlan)#remote-span
SW_3_8_2(config-vlan)#exit
SW_3_8_2(config)#vlan 101
SW_3_8_2(config-vlan)#remote-span
SW_3_8_2(config-vlan)#exit
SW_3_8_2(config)#interface port-channel 1
SW_3_8_2(config-if)#switchport trunk allowed vlan add 100
SW_3_8_2(config-if)#switchport trunk allowed vlan add 101
SW_3_8_2(config-if)#exit
SW_3_8_2(config)#interface port-channel 2
SW_3_8_2(config-if)#switchport trunk allowed vlan add 100
SW_3_8_2(config-if)#switchport trunk allowed vlan add 101
SW_3_8_2(config-if)#exit
SW_3_8_2(config)#interface gig0/1
SW_3_8_2(config-if)#switchport trunk allowed vlan add 100
SW_3_8_2(config-if)#switchport trunk allowed vlan add 101
SW_3_8_2(config-if)#exit
SW_3_8_2(config)#monitor session 1 source vlan 10 tx
SW_3_8_2(config)#monitor session 1 source vlan 20 tx
SW_3_8_2(config)#monitor session 1 source vlan 30 tx
SW_3_8_2(config)#monitor session 1 source vlan 40 tx
SW_3_8_2(config)#monitor session 1 destination remote vlan 100 reflector-port fa0/24
SW_3_8_2(config)#monitor session 2 source interface fa0/6 tx
SW_3_8_2(config)#monitor session 2 destination remote vlan 101 reflector-port fa0/24

```

...

Налаштування дзеркалювання портів на комутаторах SW_3_8_3 та SW_3_8_4 відбувається аналогічно до налаштувань комутатора SW_3_8_2.

Перейдемо до налаштування підмережі В. В даній підмережі буде доцільним налаштування локального дзеркалювання портів. Налаштувань VLAN в дані підмережі не відбуватиметься через невелику кількість кінцевих вузлів. Наступні налагодження будуть відбуватися в програмному емуляторі GNS3 на маршрутизаторі Cisco c3725, для модуля комутації NM-16ESW.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

Сценарій базового налагодження параметрів комутаторі SPAN_SW

наведено нижче:

```
...  
SPAN_SW(config)#interface vlan 1  
SPAN_SW(config-if)#ip address 10.3.8.18 255.255.255.240  
SPAN_SW(config-if)#no shutdown  
SPAN_SW(config-if)#exit  
...
```

Для налагодження локального SPAN достатнім буде в сесії моніторингу вказати порти джерела та призначення дзеркалювання вхідного трафіку.

Сценарій налагодження параметрів SPAN на комутаторі SPAN_SW

наведено нижче:

```
...  
SPAN_SW(config)#  
SPAN_SW(config)#monitor session 1 source interface fa1/2  
SPAN_SW(config)#monitor session 1 source interface fa1/3  
SPAN_SW(config)#monitor session 1 source interface fa1/4  
SPAN_SW(config)#monitor session 1 source interface fa1/5  
SPAN_SW(config)#monitor session 1 source interface fa1/6  
SPAN_SW(config)#monitor session 1 destination fa1/1  
...
```

На жаль налаштування ERSPAN не є можливим в програмних симуляторах, тому розглянемо теоретично як відбувається налагодження даного виду дзеркалювання портів.

Приклад налагодження сценарію параметрів ERSPAN для комутатора

SW_3_8_1:

```
...  
SW_3_8_1(config)# monitor session 1 type erspan-source  
SW_3_8_1(config-mon-erspan-src)# source vlan 10  
SW_3_8_1(config-mon-erspan-src)# source vlan 20  
SW_3_8_1(config-mon-erspan-src)# source vlan 30  
SW_3_8_1(config-mon-erspan-src)# source vlan 40  
SW_3_8_1(config-mon-erspan-src)# destination  
  
#Назначаємо id для erspan, на усіх комутаторах має бути однаковим  
SW_3_8_1(config-mon-erspan-src-dst)# erspan-id 111  
  
#Вказуємо ip-адресу комутатора призначення  
SW_3_8_1(config-mon-erspan-src-dst)# ip address 10.3.8.18  
#Вказуємо ip-адресу комутатора джерела  
SW_3_8_1(config-mon-erspan-src-dst)# origin ip address 10.3.8.2  
...
```

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

Приклад налагодження сценарію параметрів ERSPAN для комутатора SPAN_SW:

```
...
SPAN_SW(config)# monitor session 1 type erspan-destination
SPAN_SW(config-mon-erspan-dst)# destination interface fa1/1
SPAN_SW (config-mon-erspan-dst)# source
SPAN_SW (config-mon-erspan-dst-src)# erspan-id 111
SPAN_SW (config-mon-erspan-dst-src)# ip address 10.3.8.18
...
```

3.4 Тестування роботи підсистеми дзеркалювання трафіку

Тестування невід’ємна частина налагодження комп’ютерної мережі. Для подальшої перевірки працездатності спершу перевірю роботу протоколу DHCP, а саме отримання кінцевими вузлами налаштувань ір-адресації.

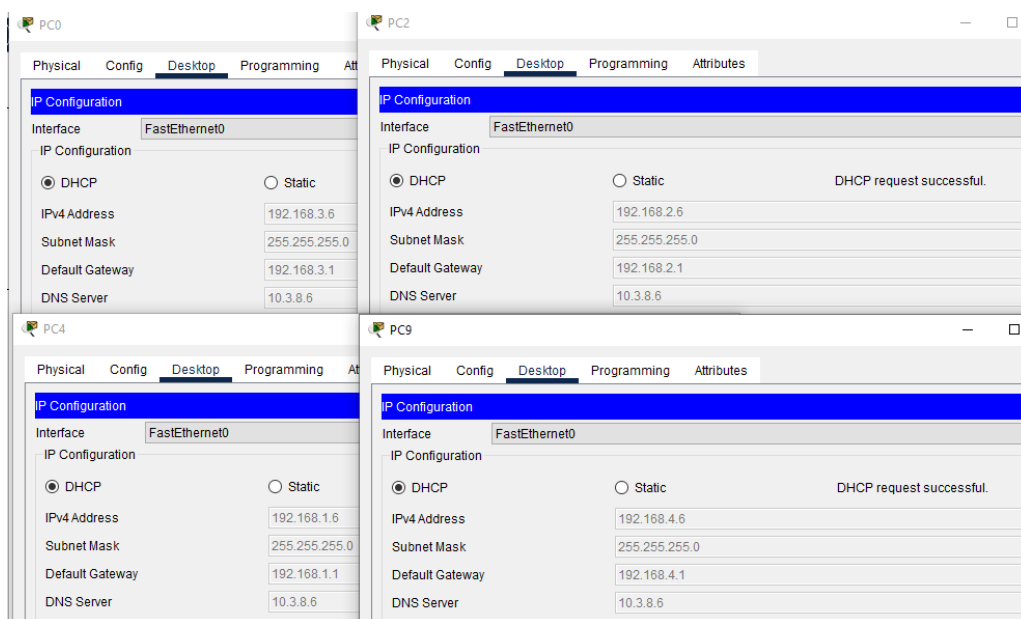


Рисунок 3.1 – Успішне отримання IP-адреси кінцевими вузлами підмережі А.

```

PC1> ip dhcp
DDORA IP 10.3.8.19/28 GW 10.3.8.17

PC1> show ip

NAME       : PC1[1]
IP/MASK    : 10.3.8.19/28
GATEWAY    : 10.3.8.17
DNS        : 10.3.8.6
DHCP SERVER : 10.3.8.17
DHCP LEASE  : 86396, 86400/43200/75600
MAC        : 00:50:79:66:68:00
LPORT      : 10025
RHOST:PORT  : 127.0.0.1:10026
MTU        : 1500

PC1>

```

Рисунок 3.2 – Успішне отримання IP-адреси кінцевими вузлами підмережі В.

Можемо зробити висновок, що налаштовані DHCP-сервери працюють коректно.

Також перевіримо зв'язок між кінцевими вузлами мережі.

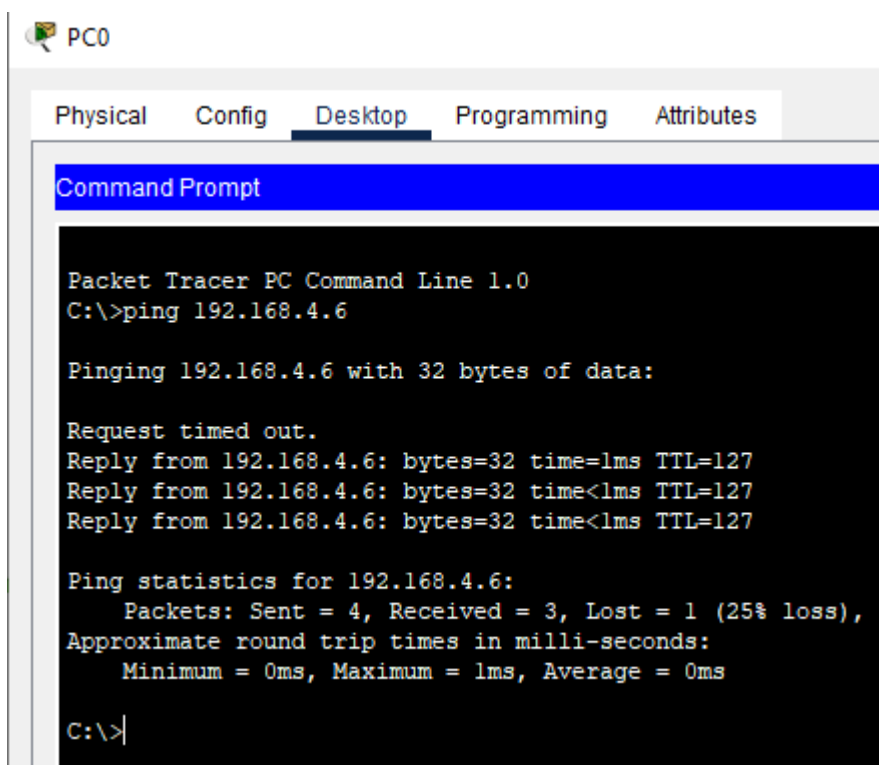


Рисунок 3.3 – Успішна відправка ехо-запитів на робочу станцію іншої VLAN.

На рисунку 3.3 можемо бачити, що один пакет втрачено, відбулося це через відправку ARP-запитів. Так як на 3 з 4 запитів була отримана відповідь, можна сказати, що зв'язок між VLAN`ами успішний.

Також перевіримо справність налаштованої трансляції NAT за допомогою діагностичних команд *show ip nat statistics* та *show ip nat translations*.

```
R_3_8_1#show ip nat translations
Pro Inside global      Inside local      Outside local     Outside global
icmp 32.135.10.1:13    192.168.3.6:13   32.135.10.2:13   32.135.10.2:13
icmp 32.135.10.1:14    192.168.3.6:14   32.135.10.2:14   32.135.10.2:14
icmp 32.135.10.1:15    192.168.3.6:15   32.135.10.2:15   32.135.10.2:15
icmp 32.135.10.1:16    192.168.3.6:16   32.135.10.2:16   32.135.10.2:16
icmp 32.135.10.1:1     192.168.4.8:1    32.135.10.2:1    32.135.10.2:1
icmp 32.135.10.1:2     192.168.4.8:2    32.135.10.2:2    32.135.10.2:2
icmp 32.135.10.1:3     192.168.4.8:3    32.135.10.2:3    32.135.10.2:3
icmp 32.135.10.1:4     192.168.4.8:4    32.135.10.2:4    32.135.10.2:4

R_3_8_1#show ip nat statistics
Total translations: 8 (0 static, 8 dynamic, 8 extended)
Outside Interfaces: GigabitEthernet2/0
Inside Interfaces: GigabitEthernet0/0 , GigabitEthernet1/0 , GigabitEthernet0/0.10 ,
GigabitEthernet0/0.20 , GigabitEthernet0/0.30 , GigabitEthernet0/0.40
Hits: 24 Misses: 33
Expired translations: 16
Dynamic mappings:
```

Рисунок 3.4 – Виконання діагностичних команд на маршрутизаторі R_3_8_1

Тепер перевіримо роботу налаштованого RSPAN. Для цього відправимо ехо-запити з комп'ютера мережі VLAN 10 на комп'ютер мережі VLAN 40. Оберемо на Sniffer1 фільтрацію вхідного трафіку, а саме відображення лише запитів ICMP. Також відправимо ехо-запит з комп'ютеру PC0, та переглянемо інформацію, що прийшла на Sniffer2.

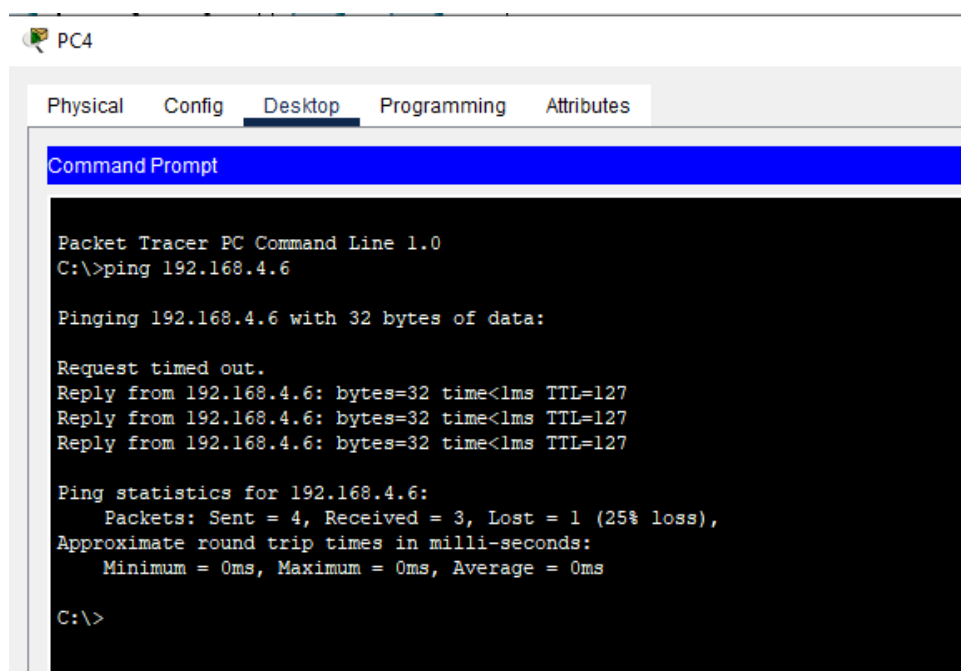


Рисунок 3.5 – Відправка ехо-запитів з комп'ютеру підмережі VLAN10 на комп'ютер підмережі VLAN40.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

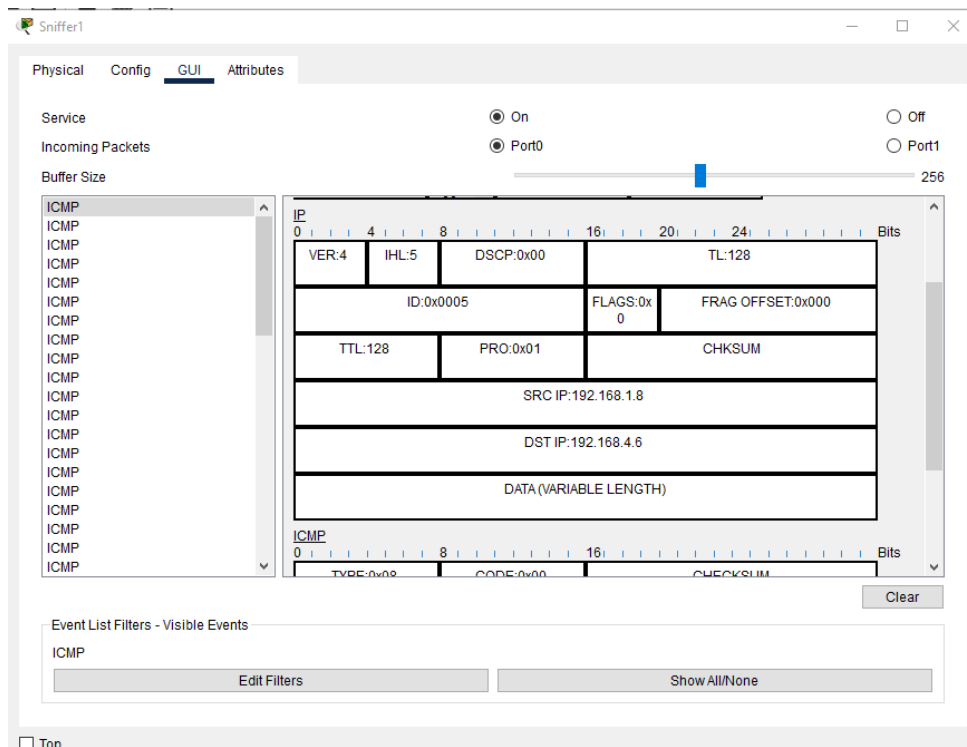


Рисунок 3.6 – Успішне отримання та перегляд відзеркалених ехо-запитів на Sniffer1.

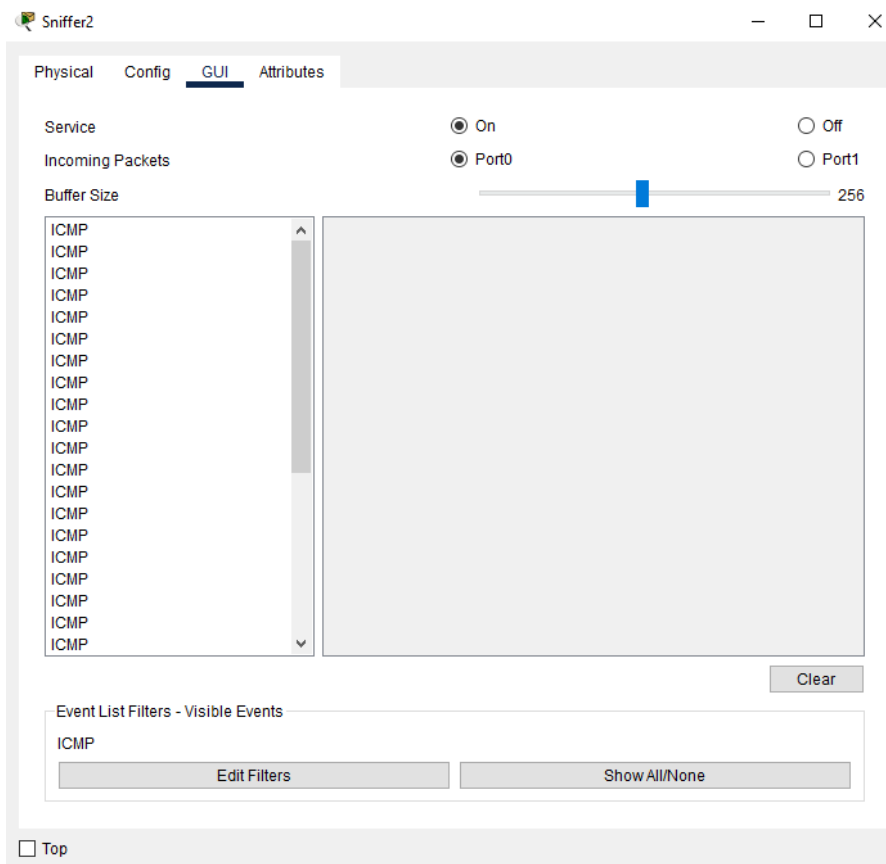


Рисунок 3.7 – Успішне отримання та перегляд відзеркалених ехо-запитів на Sniffer2.

Тепер перевіримо роботу налаштованого в GNS3 локального SPAN. Для цього необхідно встановити на комп'ютер, який виступає в ролі сніфера, програму для захвату та відстежування вхідного трафіку – Wireshark.

Далі відкриваємо її та обираємо пункт «Подключение по локальной сети». Оберемо фільтрування – лише пакети ICMP.

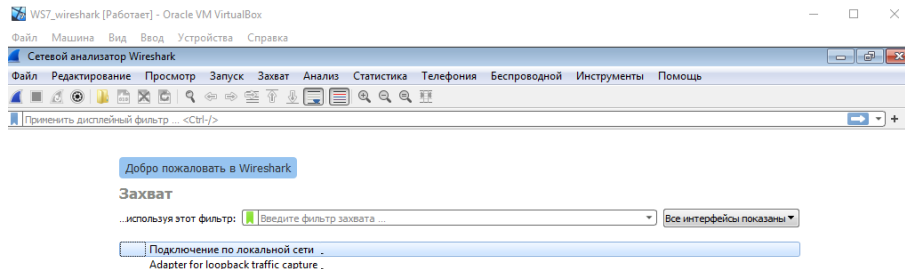


Рисунок 3.8 – Відкрита програма Wireshark на WS_wireshark_1

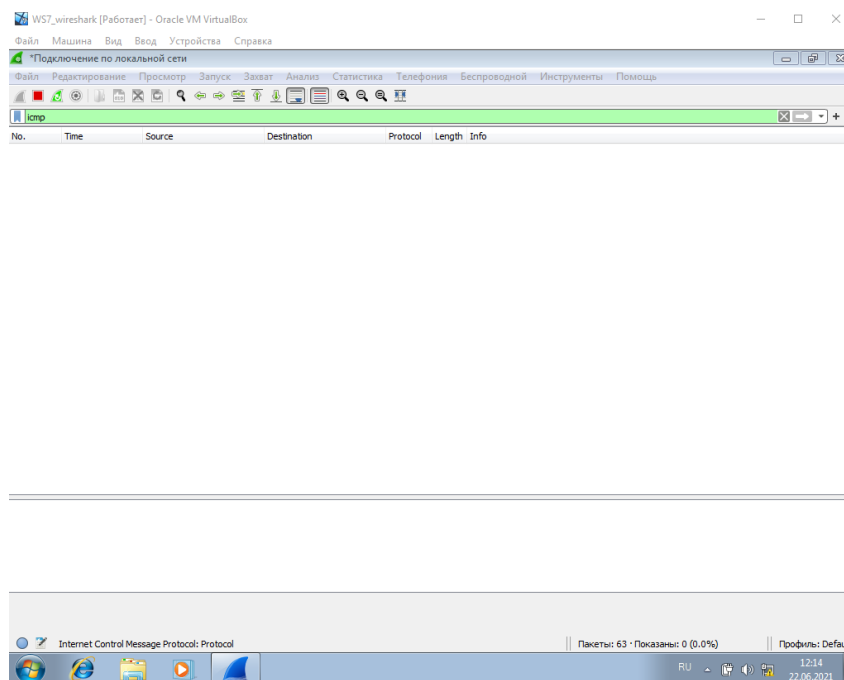


Рисунок 3.9 – Фільтрування вхідних пакетів – пакети ICMP.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росси́нский Ю.М.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

```
PC1> ip dhcp
DDORA IP 10.3.8.20/28 GW 10.3.8.17

PC1> ping 10.3.8.19
84 bytes from 10.3.8.19 icmp_seq=1 ttl=64 time=1.798 ms
84 bytes from 10.3.8.19 icmp_seq=2 ttl=64 time=1.651 ms
84 bytes from 10.3.8.19 icmp_seq=3 ttl=64 time=1.706 ms
84 bytes from 10.3.8.19 icmp_seq=4 ttl=64 time=1.874 ms
84 bytes from 10.3.8.19 icmp_seq=5 ttl=64 time=1.341 ms

PC1> █
```

Рисунок 3.10 – Відправка ехо-запитів між комп’ютерами локальної мережі.

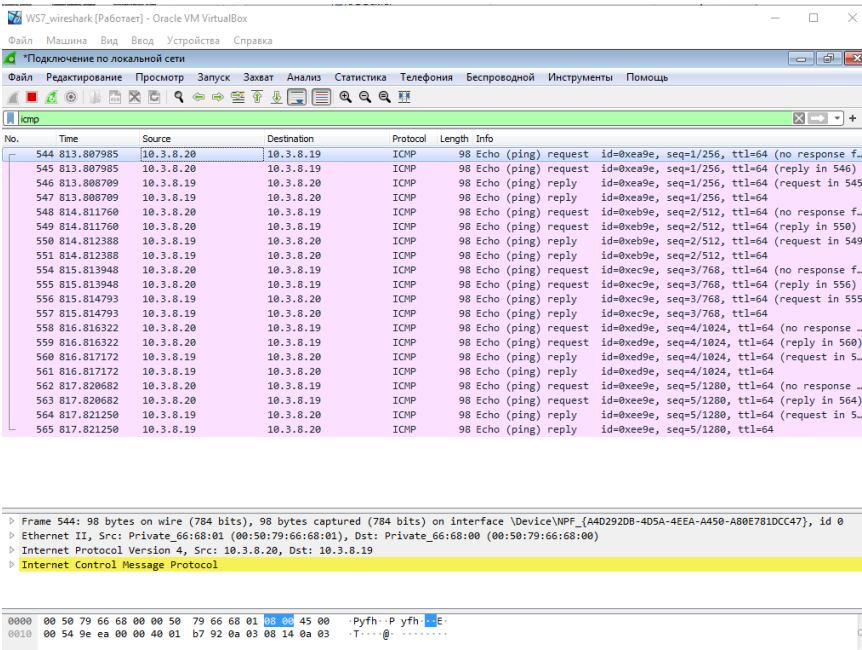


Рисунок 3.11 – Відображення відфільтрованих вхідних пакетів.

На рисунку 3.11 можемо побачити що кожен пакет дублюється, відбувається через те, що відслідковується весь вхідний і вихідний трафік на портах комутатора.

Також за допомогою додатку Wireshark можна переглядати усі пакети, різні види трафіку підсвічуються різними кольорами. Так наприклад пакети ICMP – рожеві, а пакети протоколу ARP – оранжеві, що значно полегшує знаходження потрібних пакетів трафіку.

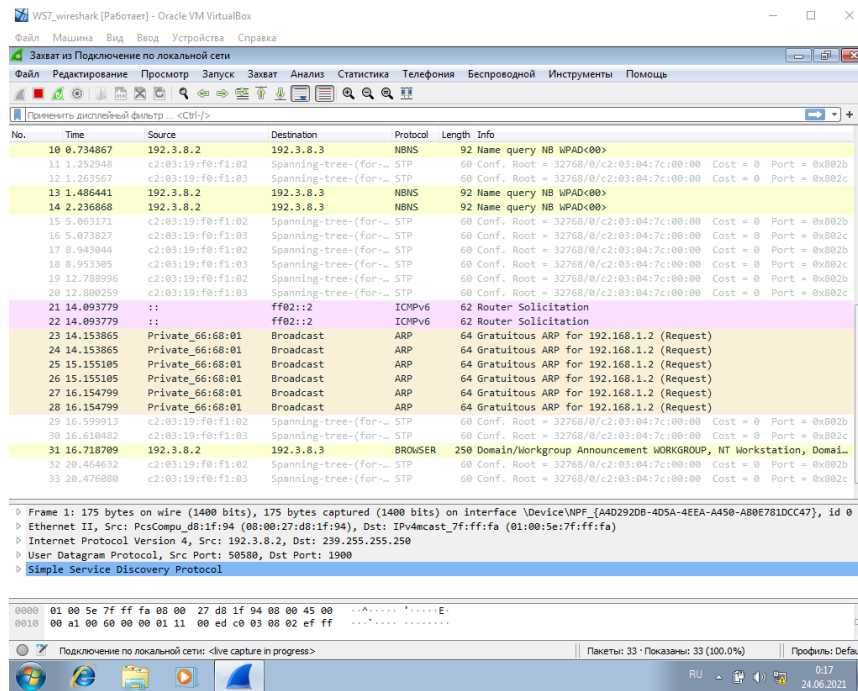


Рисунок 3.12 – Відображення усіх вхідних пакетів.

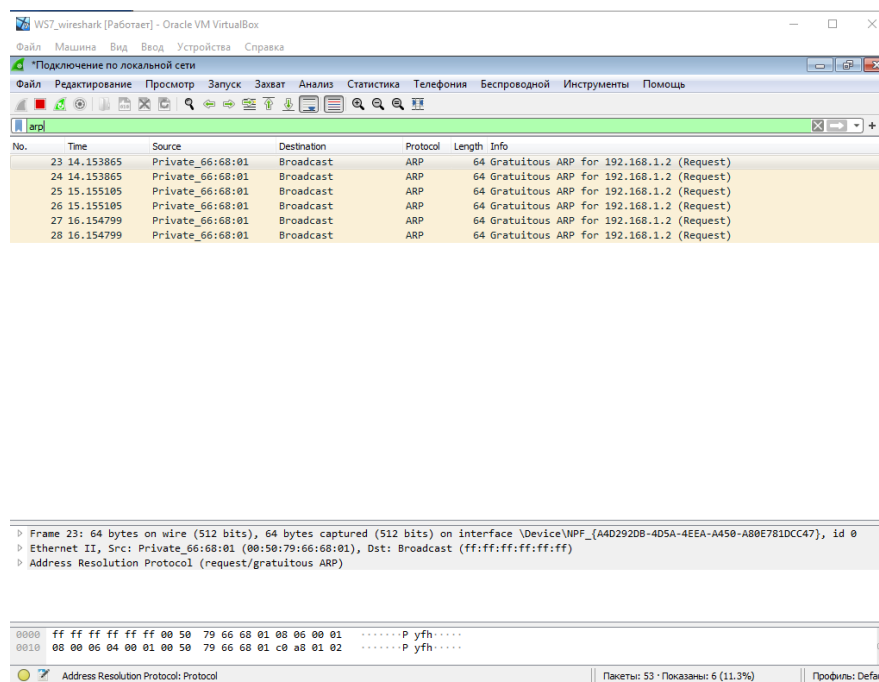


Рисунок 3.13 – Відображення вхідних пакетів протоколу ARP.

ВИСНОВКИ

Підчас роботи над даною кваліфікаційною роботою було досягнуто її мету, а саме спроектовано та налагоджено підсистему дзеркалювання трафіку комп'ютерної мережі організації.

В ході роботи над першим розділом було розглянуто та проаналізовано відомості про налаштування дзеркалювання трафіку та дзеркалювання трафіку на мережовому обладнанні компанії Cisco. Також були розглянуті основні відомості про захолення трафіку та програму Wireshark.

В ході аналізу принципів побудови комп'ютерних мереж організацій з використанням технології дзеркалювання трафіку було виявлено, що дзеркалювання трафіку – це технологія дублювання пакетів одного порту на іншому. На обладнанні Cisco можливе налаштування трьох видів дзеркалювання портів: локальний SPAN, віддалений SPAN та інкапсульований віддалений SPAN. Дзеркалювання портів зазвичай використовується для подальшого їх аналізу. Однією з програм за допомогою яких можливе захоплення віддзеркаленого трафіку – Wireshark яку в подальшому можна буде використовувати для перевірки працездатності мережі. Після аналізу викладеного матеріалу було поставлене технічне завдання для подальшої роботи.

У другому розділі було розроблено загальну структуру мережі, розроблено схему адресації вузлів в мережі, та розроблено проект підсистеми дзеркалювання трафіку.

В ході розробки топології мережі було вирішено спроектувати згорнуте ядро, що поєднує в собі функції ядра та рівня розподілу. Під час розробки схеми адресації мережі організації було обрано IP-адреси мереж та VLAN'ів. Надані статичні адреси усім комутаторам та серверам у мережі. Вирішено надавати IP-адреси кінцевим вузлам динамічно. Також в другому розділі було вирішено реалізовувати три функції дзеркалювання трафіку на комутаторах Cisco, а саме локальний SPAN, RSPAN та ERSPAN.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

В ході виконання завдань третього розділу було виконано основну роботу для досягнення мети кваліфікаційної роботи а саме обрано та налагоджено всі пристрої мережі.

Спершу було створено та налагоджено роботу віртуальних локальних мереж (VLAN), надано усім комутаторам статичних IP-адрес та налаштовано DHCP сервер для надання IP-адрес кінцевим вузлам. Також на головному маршрутизаторі підмережі було налаштовано NAT з метою відокремлення локальних IP-адрес від глобальної мережі. Для підвищення пропускної здатності мережі комутатори між собою з'єднали агрегованими каналами.

Підчас налаштування підсистеми дзеркалювання трафіку було налагоджено дві локальні підмережі. В першій використовувався вітдалений SPAN (RSPAN), в другій – локальний SPAN.

Останнім етапом третього розділу було тестування мережі. В цьому пункті було протестовано правильність роботи DHCP сервера, перевірено зв'язок пристроїв між собою. Далі було проведено тестування правильності налагодження SPAN, а саме було перевірено чи усі пакети копіюються та приходять на порт призначення завдяки налаштованим SPAN та RSPAN.

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – СПб.: Питер, 2005. – 958 с.
2. CCNA Security 210-260. Official Cert Guide / Omar Santos, John Stuppi. – Cisco Press, 2015. – 658 p
3. CCNA Security 640-554. Official Cert Guide / Keith Barker, Scott Morris. – Cisco Press, 2013. – 740 p.
4. Catalyst Switched Port Analyzer (SPAN) Configuration Example [Электронный ресурс] / Cisco Web Site // Cisco – Режим доступа до ресурсу: <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41.html>.
5. Chapter: SPAN, RSPAN, and ERSPAN [Электронный ресурс] // Cisco – Режим доступа до ресурсу: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/span.html#wp1020380>.
6. Cisco IOS SPAN and RSPAN [Электронный ресурс] – Режим доступа до ресурсу: <https://networklessons.com/switching/cisco-ios-span-rspan>.
7. Configuring SPAN and RSPAN [Электронный ресурс] / Cisco Web Site // Cisco – Режим доступа до ресурсу: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_40_se/configuration/guide/scg/swspan.pdf.
8. Configuring ERSPAN [Электронный ресурс] / Cisco Web Site // Cisco – Режим доступа до ресурсу: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus3548/sw/system_mgmt/602/b_N3548_System_Management_Config_602A11/b_N3548_Sysetm_Management_Config_602A11_chapter_010000.pdf.
9. Configuring Traffic Mirroring [Электронный ресурс] / Cisco Web Site // Cisco – Режим доступа до ресурсу:

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

<https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/iosxr/cisco8000/Interfaces/70x/b-interfaces-config-guide-cisco8kr70x/configuring-traffic-mirroring.html.xml>.

10. Configuring 802.1Q Trunking Between a Catalyst 3550/3560/3750 and Catalyst Switches That Run Cisco IOS Software [Электронный ресурс] / Cisco Web Site // Cisco – Режим доступа до ресурсу: <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6000-series-switches/10599-88.html>.

11. Configuring Network Address Translation [Электронный ресурс] // Cisco – Режим доступа до ресурсу: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html>.

12. Mini Protocol Analyzer [Электронный ресурс] / Cisco Web Site // Cisco – Режим доступа до ресурсу: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/mpa.html>.

13. SPAN, RSPAN, ERSPAN [Электронный ресурс] // Cisco – Режим доступа до ресурсу: <https://learningnetwork.cisco.com/s/article/span-rspan-erspan>.

14. Network Analysis Module (NAM) Products [Электронный ресурс] – Режим доступа до ресурсу: <https://www.cisco.com/c/en/us/products/cloud-systems-management/network-analysis-module-nam/index.html>.

15. Wireshark Wiki [Электронный ресурс] // Wireshark – Режим доступа до ресурсу: <https://wiki.wireshark.org/FrontPage>.

ДОДАТКИ

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

Додаток А – схема загальної топології мережі

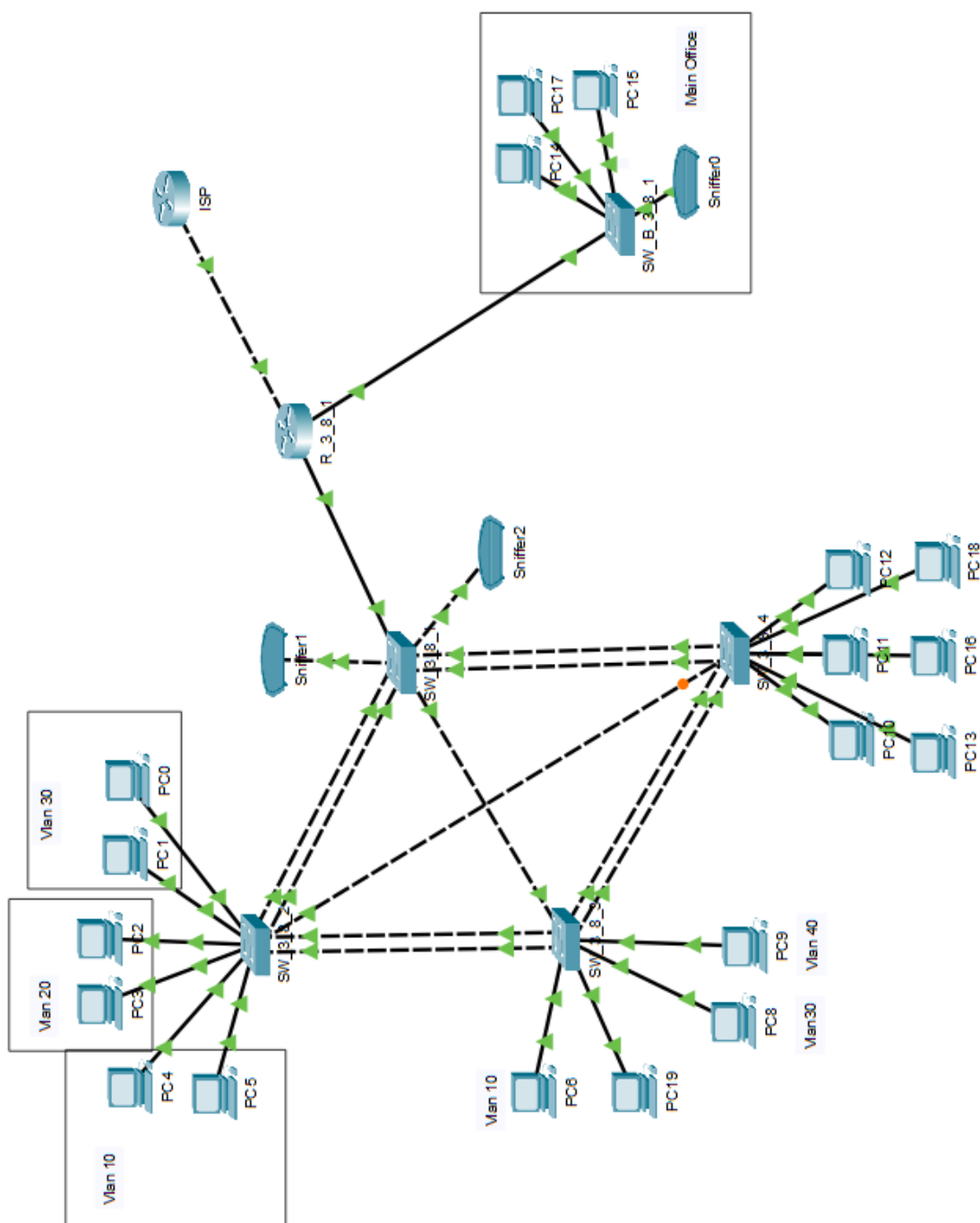


Рисунок А.1 – Частина загальної топології комп'ютерної мережі організації

		Кондратюк І. А.		
		Росси́нский Ю.М.		
Змн.	Арк.	№ докум.	Підпис	Дата

KIK.KP.B – 123 – 08 – ПЗ

Арк.

52

Додаток Б – порівняння комутаторів Cisco

Таблиця Б.1 – Підтримка SPAN, RSPAN, ERSPAN комутаторами

Cisco Catalyst

Комутатор Catalyst	Підтримка SPAN	Підтримка RSPAN	Підтримка ERSPAN
Catalyst Express 500 / 520 Series	+	-	-
Catalyst 6500/6000 Series	+	+	+
Catalyst 5500/5000 Series	+	-	-
Catalyst 4900 Series	+	+	-
Catalyst 4500/4000 Series (includes 4912G)	+	+	-
Catalyst 3750 Metro Series	+	+	-
Catalyst 3750 / 3750E /3750X Series	+	+	-
Catalyst 3560 / 3560E/ 3650X Series	+	+	-
Catalyst 3550 Series	+	+	-
Catalyst 3500 XL Series	+	-	-
Catalyst 2970 Series	+	+	-
Catalyst 2960 Series	+	+	-
Catalyst 2955 Series	+	+	-
Catalyst 2950 Series	+	+	-
Catalyst 2940 Series	+	-	-
Catalyst 2948G-L3	-	-	-
Catalyst 2948G-L2, 2948G-GE-TX, 2980G-A	+	+	-
Catalyst 2900XL Series	+	-	-
Catalyst 1900 Series	+	-	-

Додаток В – Конфігураційні файли налагоджених пристроїв

Файл конфігурації комутатора SW_3_8_1

```
Current configuration : 2259 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW_3_8_1
...
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
!
interface Port-channel1
switchport mode trunk
switchport nonegotiate
spanning-tree vlan 10,20,30,40 port-priority 16
!
interface Port-channel2
switchport mode trunk
switchport nonegotiate
spanning-tree vlan 10,20,30,40 port-priority 16
!
interface FastEthernet0/1
ip dhcp snooping limit rate 100
switchport mode trunk
switchport nonegotiate
channel-group 2 mode on
!
interface FastEthernet0/2
switchport mode trunk
switchport nonegotiate
channel-group 2 mode on
!
interface FastEthernet0/3
switchport mode trunk
switchport nonegotiate
channel-group 1 mode on
!
interface FastEthernet0/4
switchport mode trunk
switchport nonegotiate
channel-group 1 mode on
!
interface FastEthernet0/5
...
interface FastEthernet0/24
!
interface GigabitEthernet0/1
```

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

```

switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/2
switchport mode trunk
switchport nonegotiate
spanning-tree vlan 10,20,30,40 port-priority 16
!
interface Vlan1
ip address 10.3.8.2 255.255.255.240
!
interface Vlan10
ip address 192.168.1.2 255.255.255.0
!
interface Vlan20
ip address 192.168.2.2 255.255.255.0
!
interface Vlan30
ip address 192.168.3.2 255.255.255.0
!
interface Vlan40
ip address 192.168.4.2 255.255.255.0
!
no cdp run
...
line con 0
!
line vty 0 4
login
line vty 5 15
login
!

monitor session 1 destination interface Fa0/7
monitor session 1 source remote vlan 100
monitor session 2 destination interface Fa0/5
monitor session 2 source remote vlan 101
!

End

```

Файл конфігурації комутатора SW_3_8_2

```

Current configuration : 3119 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW_3_8_2
!
...
spanning-tree mode rapid-pvst

```

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

```

spanning-tree extend system-id
spanning-tree vlan 1 priority 28672
!
interface Port-channel1
switchport mode trunk
switchport nonegotiate
spanning-tree vlan 10,20,30,40 port-priority 32
!
interface Port-channel2
switchport mode trunk
switchport nonegotiate
spanning-tree vlan 10,20,30,40 port-priority 64
!
interface FastEthernet0/1
switchport mode trunk
switchport nonegotiate
channel-group 2 mode on
!
interface FastEthernet0/2
switchport mode trunk
switchport nonegotiate
channel-group 2 mode on
!
interface FastEthernet0/3
switchport mode trunk
switchport nonegotiate
channel-group 1 mode on
!
interface FastEthernet0/4
switchport mode trunk
switchport nonegotiate
channel-group 1 mode on
!
interface FastEthernet0/5
!
interface FastEthernet0/6
switchport access vlan 30
ip dhcp snooping limit rate 100
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/7
switchport access vlan 30
ip dhcp snooping limit rate 100
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/8
switchport access vlan 20
ip dhcp snooping limit rate 100
switchport mode access
switchport port-security mac-address sticky

```

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		56

```

!
interface FastEthernet0/9
switchport access vlan 20
ip dhcp snooping limit rate 100
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/10
switchport access vlan 10
ip dhcp snooping limit rate 100
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/11
switchport access vlan 10
ip dhcp snooping limit rate 100
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/12
...
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet0/2
spanning-tree vlan 10,20,30,40 port-priority 48
!
interface Vlan1
ip address 10.3.8.3 255.255.255.240
!
interface Vlan10
ip address 192.168.1.3 255.255.255.0
!
interface Vlan20
ip address 192.168.2.3 255.255.255.0
!
interface Vlan30
ip address 192.168.3.3 255.255.255.0
!
interface Vlan40
ip address 192.168.4.3 255.255.255.0
!
no cdp run
!
!
!
!
line con 0

```

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		57

```

!
line vty 0 4
login
line vty 5 15
login
!
!
monitor session 1 source vlan 10 tx
monitor session 1 source vlan 20 tx
monitor session 1 source vlan 30 tx
monitor session 1 source vlan 40 tx
monitor session 1 destination remote vlan 100 reflector-port Fa0/24
monitor session 2 source interface Fa0/6 tx
monitor session 2 destination remote vlan 101 reflector-port Fa0/24
!
end

```

Файл конфігурації SPAN_SW

```

Current configuration : 3038 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service dhcp
!
hostname SPAN_SW
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
monitor session 1 source interface Fa1/2 - 6
monitor session 1 destination interface Fa1/1
memory-size iomem 5
no ip routing
no ip icmp rate-limit unreachable
no ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
macro name add_vlan
end
vlan database
vlan $v
exit

```

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

```

@
macro name del_vlan
end
vlan database
no vlan $v
exit
@
!
vtp file nvram:vlan.dat
archive
log config
hidekeys
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
description *** Unused for Layer2 EtherSwitch ***
no ip address
no ip route-cache
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
description *** Unused for Layer2 EtherSwitch ***
no ip address
no ip route-cache
shutdown
duplex auto
speed auto
!
interface FastEthernet1/0
duplex full
speed 100
!
...
interface FastEthernet1/15
duplex full
speed 100
!
interface Vlan1
ip address 10.3.8.18 255.255.255.240
no ip route-cache
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex

```

Файл конфігурації R 3 8 1

		Кондратюк І. А.			KIK.KP.B – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

```

Current configuration : 2257 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R_3_8_1
!
ip dhcp excluded-address 192.168.1.1 192.168.1.5
ip dhcp excluded-address 192.168.2.1 192.168.2.5
ip dhcp excluded-address 192.168.3.1 192.168.3.5
ip dhcp excluded-address 192.168.4.1 192.168.4.5
ip dhcp excluded-address 10.3.8.17 10.3.8.18
!
ip dhcp pool VLAN10
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 10.3.8.6
ip dhcp pool VLAN20
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
dns-server 10.3.8.6
ip dhcp pool VLAN30
network 192.168.3.0 255.255.255.0
default-router 192.168.3.1
dns-server 10.3.8.6
ip dhcp pool VLAN40
network 192.168.4.0 255.255.255.0
default-router 192.168.4.1
dns-server 10.3.8.6
ip dhcp pool LAN_B
network 10.3.8.16 255.255.255.240
default-router 10.3.8.17
dns-server 10.3.8.6
!
no ip cef
no ipv6 cef
!
interface GigabitEthernet0/0
ip address 10.3.8.1 255.255.255.240
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.1.1 255.255.255.0
ip nat inside
!
interface GigabitEthernet0/0.20
encapsulation dot1Q 20

```

		Кондратюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		60

```

ip address 192.168.2.1 255.255.255.0
ip nat inside
!
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.3.1 255.255.255.0
ip nat inside
!
interface GigabitEthernet0/0.40
encapsulation dot1Q 40
ip address 192.168.4.1 255.255.255.0
ip nat inside
!
interface GigabitEthernet1/0
ip address 10.3.8.17 255.255.255.240
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet2/0
ip address 32.135.10.1 255.255.255.252
ip nat outside
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
network 32.135.10.0 0.0.0.3 area 0
!
ip nat inside source list 1 interface GigabitEthernet2/0 overload
ip classless
!
ip flow-export version 9
!
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.0.255
access-list 1 permit 10.3.8.0 0.0.0.15
access-list 1 permit 10.3.8.16 0.0.0.15
!
line con 0
!
line aux 0
!
line vty 0 4
login
! end

```

		Кондратьюк І. А.			КІК.КР.Б – 123 – 08 – ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		61