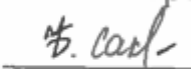
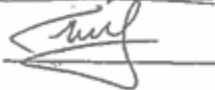


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

Пояснювальна записка

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

Виконала студентка 4-го курсу, групи КБ-1
спеціальності 125 «Кібербезпека»

		Сак Б. С.
Керівник		Єфіменко А. А.
Рецензент		Покотило О. А.

Житомир – 2021

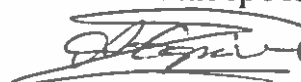
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри

комп'ютерної інженерії

та кібербезпеки

 Сфіменко А. А.

«12» квітня 2021 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента Сак Богдани Сергіївни

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

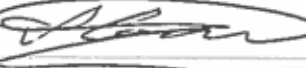
затверджена Наказом по університету від «12» Квітня 2021 р. № 134/С

Термін здачі студентом закінченої роботи – «22» Червня 2021 р.

Вихідні дані для роботи:

1. Фізична топологія мережі
2. Логічна топологія мережі
3. Маршрутизатори Cisco
4. Комутатори Cisco
5. Симулятор Packet Tracer

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Сфіменко А. А.		
2	Сфіменко А. А.		
3	Сфіменко А. А.		

Керівник



Сфіменко А. А.

Календарний план

№ з/п	Назва етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка задачі. Пошук, огляд та аналіз аналогічних розробок. Формулювання технічного завдання. Опрацювання літературних джерел.	21 лютого 2021 – 20 квітня 2021	
2	Проектування структури системи	21 квітня 2021 – 25 квітня 2021	
3	Налаштування системи	26 квітня 2021 – 19 травня 2021	
4	Тестування	20 травня 2021 – 19 червня 2021	
5	Захист	24 червня 2021	

Студент Б.Сак Сак Б.С.

Керівник Л.Л.Сіменко Сіменко Л.Л.

РЕФЕРАТ

Випускна кваліфікаційна робота бакалавра складається з підсистеми дзеркалювання трафіку системи безпеки комп'ютерної мережі організації та пояснювальної записки до неї. Пояснювальна записка містить 83 сторінки, 34 ілюстрації та 3 таблиці.

Метою роботи є розробка підсистеми дзеркалювання трафіку системи безпеки комп'ютерної мережі організації. Система має бути оптимізована задля економії IP-адрес, пристроїв та кабелів підключення, а також для можливості розміщення якомога більшої кількості робочих станцій. Усі пристрої мережі мають коректно і безперервно працювати. Також необхідно детально розглянути технології дзеркалювання, а саме їх переваги і недоліки.

Пояснювальна записка кваліфікаційної роботи складається з трьох розділів, які включають в себе розгляд теоретичних відомостей, пов'язаних з дзеркалюванням даних, розробку логічної та фізичної топології структури мережі, постановки технічного завдання, вибір обладнання та каналів зв'язку, налаштування мережі і перевірка її працездатності. В додатки винесено 2 таблиці, а саме параметри інтерфейсів пристроїв і параметри адресації мережі. Також в додатки винесено конфігураційні файли пристроїв.

КЛЮЧОВІ СЛОВА: КОМП'ЮТЕРНА МЕРЕЖА, SPAN, PSPAN, PING, DHCP, OSPF, SSH, CISCO.

					КІК.КВ.Б-125-16-ПЗ				
Зм.	Арк.	№ докум.	Підпис	Дата	Проект підсистеми дзеркалювання трафіку системи безпеки комп'ютерної мережі організації				
Розроб.	Сак Б. С.								
Керівник	Єфіменко А. А.								
Рецензент	Покотило О. А.								
Зав. каф.	Єфіменко А. А.				Літ. Арк. Аркушів 4 82 Державний університет «Житомирська політехніка», Група КБ-1				

ABSTRACT

The bachelor's thesis consists of a traffic mirroring subsystem of the organization's computer network security system and an explanatory note to it. The explanatory note contains 82 pages, 34 illustrations and 3 tables.

The purpose of the work is to develop a traffic mirroring subsystem of the security system of the computer network of the organization. The system should be optimized to save IP addresses, devices and connection cables, as well as to be able to accommodate as many workstations as possible. All network devices must work correctly and continuously. It is also necessary to consider in detail the mirroring technologies, namely their advantages and disadvantages.

Qualification work will consist of three sections, which will include consideration of theoretical information related to data mirroring, development of logical and physical topology of network structure, technical task setting, selection of equipment and communication channels, network setup and verification of its operability. The application will contain 2 tables, namely the parameters of device interfaces and network addressing parameters. Device configuration files will also be added to applications.

KEY WORDS: COMPUTER NETWORK, SPAN, PSPAN, PING, DHCP.

ЗМІСТ

ВСТУП	7
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ОРГАНІЗАЦІЇ СИСТЕМ ДЗЕРКАЛЮВАННЯ ТРАФІКУ	9
1.1. Базові принципи та підходи щодо дзеркалювання трафіку у комп'ютерних мережах	9
1.2. Аналіз принципів роботи технологію Port Mirroring	13
1.3. Порівняння принципів роботи технологій SPAN/RSPAN/ ERSPAN	20
1.4. Технічне завдання	27
РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ ДЗЕРКАЛЮВАННЯ ТРАФІКУ СИСТЕМИ БЕЗПЕКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ	28
2.1. Розробка топології комп'ютерної мережі	28
2.2. Розробка схеми адресації пристроїв мережі	35
2.3. Логічне проектування підсистеми дзеркалювання трафіку	37
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ СИСТЕМИ ДЗЕРКАЛЮВАННЯ ТРАФІКУ	41
3.1. Вибір обладнання для побудови комп'ютерної мережі організації	41
3.2. Налаштування комп'ютерної мережі та підсистеми дзеркалювання трафіку	44
3.3. Тестування роботи підсистеми дзеркалювання трафіку	51
ВИСНОВКИ	56
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	58
ДОДАТКИ	61

ВСТУП

Технології дзеркалювання портів широко використовується в сучасному світі при налаштуванні комп'ютерних мереж для того, щоб аналізувати, який трафік передається через мережу. Деякі мережеві комутатори можуть пересилати копію всього вхідного і вихідного трафіку (пакетів) з одного порту (або декількох портів, таких як група VLAN) на інший порт, призначений адміністратором, водночас не впливаючи на нормальну роботу комутатора. Це потрібно для моніторингу мережевого трафіку (наприклад, за допомогою аналізатора протоколу), моніторингу продуктивності комутатора і т. д.

Технології дзеркалювання портів мають свої функції, а саме:

- Моніторинг мережі: віддзеркалення портів можна використовувати для моніторингу трафіку комутатора для додатків, наприклад, для забезпечення дотримання політик, що стосуються використання мережі, спільного використання файлів і т.д.
- Виявлення вторгнень (IDS): віддзеркалення портів можна використовувати для відстеження всього вхідного трафіку на предмет аномальної поведінки.
- Запобігання витоку даних через Інтернет. Деякі додатки використовують віддзеркалення портів для відстеження трафіку, що відправляється користувачами в Інтернет. Це може дозволити цим DLP-додаткам аналізувати, чи відправляється деяка конфіденційна інформація, така як медичні записи / інформація про кредитні картки / дизайн IP і т.д.

Перевагою віддзеркалення портів, є те, що один або кілька портів можуть контролюватися через звичайний мережевий комутатор (без необхідності будь-яких додаткових компонентів). Також віддзеркалення портів є більш економічним, простим в налаштуванні, простим у використанні.

Недоліками віддзеркалення портів є те, що віддзеркалення може викликати переповнення буфера і втрату пакетів, оскільки всі пакети проходять через буфер в комутаторі. Крім того, на ЦП комутатора накладається додаткове навантаження, що впливає на його робочі характеристики.

Об'єктом дослідження є процеси дзеркалювання трафіку комп'ютерної мережі організації.

Предметом дослідження є технології дзеркалювання SPAN та RSPAN.

Метою роботи полягає у побудові підсистеми дзеркалювання трафіку системи безпеки комп'ютерної мережі організації. Система має бути оптимізована задля економії IP-адрес, пристроїв та кабелів підключення, а також для можливості розміщення якомога більшої кількості робочих станцій. Усі пристрої мережі мають коректно і безперервно працювати.

Результатом роботи є реалізована комп'ютерна мережа, яка відображатиме реалізацію технологій дзеркалювання та інших допоміжних протоколів, які необхідні для працездатної мережі.

Перед нами стоятиме декілька завдань:

- аналіз технологіями дзеркалювання трафіку;
- аналіз налаштування технологій дзеркалювання трафіку;
- дослідження переваг та недоліків технологій дзеркалювання трафіку;
- визначення алгоритму побудови комп'ютерної мережі на базі даних технологій;
- розробка топології комп'ютерної мережі;
- логічне проектування мережі;
- розробка IP-адресації підмереж;
- обґрунтування вибору кабелів, інтерфейсів, обладнання та ПЗ;
- налаштування мережі і перевірка її працездатності.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ОРГАНІЗАЦІЇ СИСТЕМ ДЗЕРКАЛЮВАННЯ ТРАФІКУ

1.1. Базові принципи та підходи щодо дзеркалювання трафіку у комп'ютерних мережах

Дзеркальне відображення трафіку дозволяє відстежувати мережевий трафік, що проходить у / або поза набором портів. Воно дає змогу передати цей трафік до порту призначення на тому ж маршрутизаторі.

Дзеркалювання трафіку копіює трафік з одного / або декількох вихідних портів і надсилає скопійований трафік до одного / або декількох пунктів призначення для аналізу мережевим аналізатором, або іншим пристроєм контролю. Однак трафік з одного джерела порта можна скопіювати лише в один порт призначення. Дзеркальне відображення не впливає на потік трафіку на вихідні порти і дозволяє надсилати пакети до порту призначення [2].

Наприклад, нам потрібно підключити до маршрутизатора аналізатор трафіку, якщо ми хочемо зафіксувати трафік Ethernet, який передається хостом А хосту В, рисунок 1.1. Трафік між хостами А і В також відображатиметься на порту призначення.

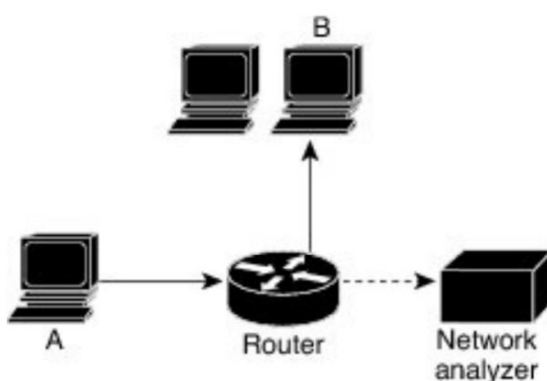


Рисунок 1.1 – Функціонування дзеркального відображення трафіку

Коли ввімкнено дзеркалювання локального трафіку, аналізатор приєднується безпосередньо до порту того ж маршрутизатора, який

налаштований на отримання копії кожного пакету, який надсилає хост А. Цей порт називається портом дзеркального відображення трафіку.

Ключовими концепціями дзеркалювання трафіку є:

- Ціль – пункт призначення дзеркального трафіку;
- Фільтр – набір правил, що визначає трафік, який копіюється в сеансі;
- Сеанс – сутність, яка описує дзеркальне відображення трафіку від джерела до цілі за допомогою фільтрів.

Дзеркальне відображення трафіку поділяється на декілька типів, а саме:

- Дзеркальне відображення локального трафіку являється найпоширенішою формою відображення. Мережевий аналізатор безпосередньо приєднаний до інтерфейсу призначення, тобто всі контрольовані порти знаходяться на тому ж маршрутизаторі, що і порт призначення.
- Дзеркальне відображення трафіку 2 та 3 рівня.
- Дзеркальне відображення трафіку на основі ACL: трафік відображається на основі конфігурації інтерфейсу ACL. Даний тип дає змогу відображати трафік на основі визначення списку контролю доступу до інтерфейсу.

Дзеркальне відображення трафіку пропонує такі переваги:

- Спрощена робота, яка полягає в дзеркалюванні будь-якого діапазону VPC-трафіку без необхідності управління його пакетами.
- Покращена безпека, яка полягає у захопленні пакетів через еластичний мережевий інтерфейс, який неможливо відключити або підробити з простору користувача.
- Розширені можливості моніторингу, які дозволяють надсилати дзеркальний трафік на будь-який захисний пристрій [1].

Не дивлячись на переваги дзеркального відображення трафіку, він має ряд недоліків таких, як обмежена кількість дзеркальних інтерфейсів, навантаження

на комутатор, блокування передачі на дзеркальний порт трафіку, який містить бітові помилки і т.д.

Для боротьби з цими недоліками існує спеціальний пристрій – Test Access Point або Network TAP (відгалужувач трафіку). Даний прилад підключається в розрив каналу зв'язку або може прийняти на себе трафік з кількох дзеркальних портів і потім видати його копію на кілька своїх портів для підключення різних систем ІТ. Використання TAP-пристроїв передбачено для аналізаторів трафіку, в системах запобігання вторгнень (IPS) і в системах виявлення мережових атак (NIDS).

Перевагами TAP-пристроїв є:

- створення 100-відсоткової копії двонаправленого мережевого трафіку;
- не змінюються тимчасові співвідношення між кадрами, інтервалом і часом відгуку;
- TAP не вносять ніякого спотворення пакетів;
- TAP пропускають весь трафік: IPv4 або IPv6, помилкові пакети, короткі або великі кадри;
- Дані пристрої є відмовостійкими;
- TAP не є адресними мережевими пристроями і тому не можуть бути зламані, що гарантує безпеку;
- TAP-пристрої не мають проблем з налаштуванням або командним рядком. Відгалужувачі – прості для користувача пристрої, що не потребують спеціального налаштування;
- TAP не вимагають завантаження оновлень вбудованого ПЗ, вони не мають доступу до чого-небудь, крім локальної мережі [3].

Дзеркальне відображення портів використовується на мережевому комутаторі або маршрутизаторі для відправки копії мережових пакетів, видимих для вибраних портів (вихідних портів), на інші зазначені порти (порти

призначення). З включеним дзеркалюванням портів пакети можна відстежувати і аналізувати.

Локальне та віддалене віддзеркалення портів – це два типи віддзеркалення портів, засновані на різних робочих діапазонах дзеркалювання. Вони діють за різними принципами.

Віддзеркалення локального порту – це найголовніша форма віддзеркалення. Всі вихідні порти розташовані на тому ж мережевому пристрої, що і порти призначення. Як показано на рисунку 1.2, дзеркальне відображення локального порту дозволяє мережному комутатору пересилати 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.

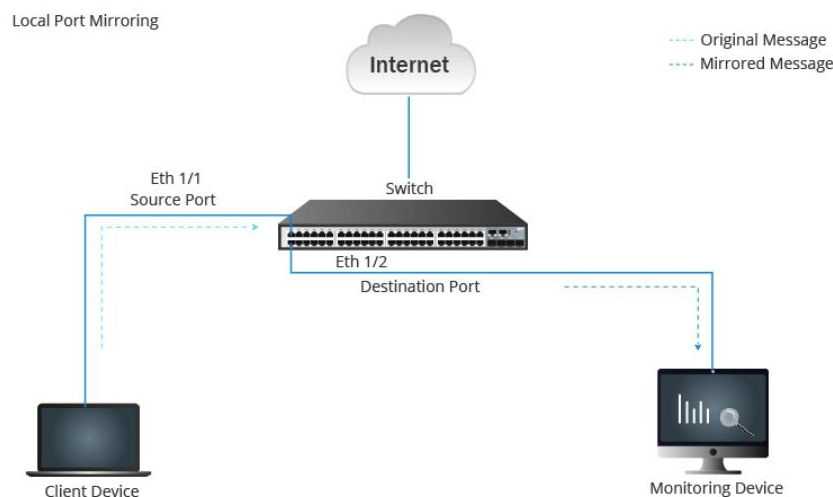


Рисунок 1.2 – Функціонування локального віддзеркалення портів

Що стосується дзеркалювання віддалених портів, вихідні порти і порти призначення не перебувають на одному пристрої. Як показано на рисунку 1.3, порт джерела (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 вихідне з'єднання, що забезпечується портом (Eth 1/4) на двох комутаторах. Отже, віддзеркалення локального порту може реалізувати моніторинг і аналіз даних на різних пристроях.

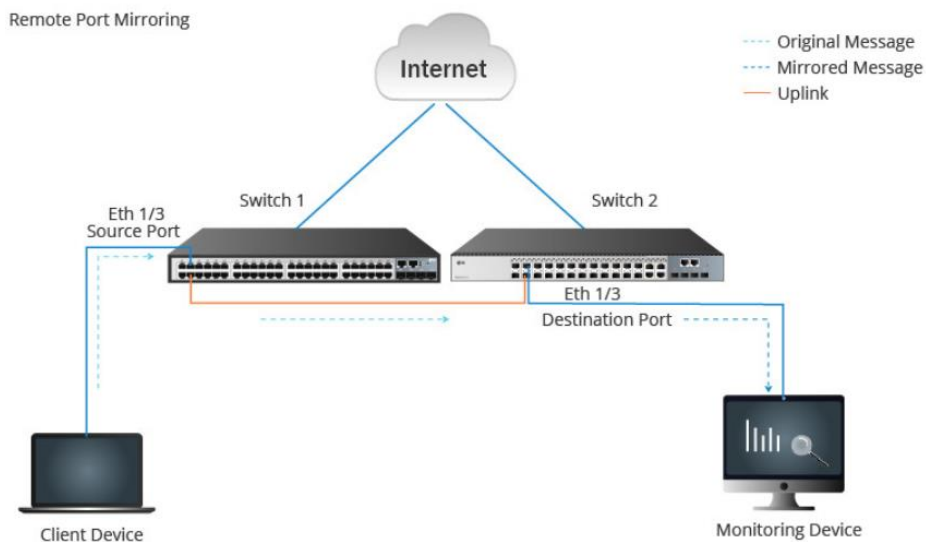


Рисунок 1.3 – Функціонування віддаленого віддзеркалювання портів

1.2. Аналіз принципів роботи технологію Port Mirroring

За мережею можна спостерігати за допомогою методу, званого дзеркалюванням портів. Коли віддзеркалення портів включено, кожен пакет даних, який надходить на певний порт комутатора або з нього, копіюється і відправляється на порт призначення. Як тільки скопійований пакет досягає порту призначення, він може бути перевірений додатком безпеки або відстежений програмним забезпеченням. Після впровадження дзеркальне відображення може попереджати адміністраторів про мережеві проблеми і сприяти усуненню несправностей. Дзеркальне відображення портів і управління портами комутатора налаштовуються адміністраторами або через додаток безпеки. Для цього вони призначають один порт для копіювання даних, а другий – для прийому і оцінки дзеркальних даних.

В процесі віддзеркалення портів ключовим моментом є аналізатор протоколу. Аналізатор розташований на порту, який приймає дзеркальні пакети. Цей аналізатор може також називатися аналізатором мережі або сніффером пакетів, оскільки він регулярно перевіряє і оцінює дані. Аналізатор може бути фізичним пристроєм або програмним забезпеченням, яке оцінює

пакети. Віддзеркалення портів – це стандартний термін ІТ-індустрії. Виробники використовують інші назви для технологій, які вони використовують при описі характеристик своїх мережевих продуктів. Умови постачальника включають аналізатор комутованого порту (SPAN) і порт аналізу рівінгу (RAP) [5].

Віддзеркалення портів і аналізатори відправляють мережевий трафік на пристрої, на яких запущені додатки-аналізatori. Дзеркало порту копіює ІР-трафік рівня 3 на інтерфейс. Аналізатор копіює мостові пакети (рівня 2) в інтерфейс. Дзеркальний трафік може бути отриманий від одного або декількох інтерфейсів. Ми можемо використовувати пристрій, підключений до дзеркального вихідного інтерфейсу, на якому запущено додаток-аналізатор, для виконання таких завдань, як моніторинг відповідності, застосування політик, виявлення вторгнень, моніторинг продуктивності мережі, кореляція подій і інші проблеми в мережі.

На маршрутизаторах, що містять спеціалізовану інтегральну схему (ASIC) Інтернет-процесора ІІ або Інтернет-процесор серії Т, віддзеркалення портів копіює одноадресні пакети, що входять або виходять з порту або входять до VLAN, і відправляє ці копії на локальний інтерфейс для локального моніторингу або в VLAN, для віддаленого моніторингу. Дзеркальний трафік отримує додатки, які допомагають аналізувати цей трафік.

Віддзеркалення портів відрізняється від вибірки трафіку. При вибірці трафіку ключ вибірки на основі заголовка ІРv4 відправляється в механізм маршрутизації, де ключ поміщається в файл або cflowd. Пакети на основі цього ключа відправляються на сервер cflowd. При створенні дзеркал портів весь пакет копіюється і відправляється через вказаний інтерфейс, де його можна захопити і детально проаналізувати.

Ми можемо налаштувати як вибірку трафіку, так і віддзеркалення портів, встановивши незалежну частоту вибірки і довжину прогону для дзеркальних пакетів порту. Однак, якщо пакет обраний як для вибірки трафіку, так і для

дзеркального відображення порту, виконується тільки дзеркальне відображення порту, оскільки воно має пріоритет. Іншими словами, якщо ми сконфігуруємо інтерфейс на вибірку трафіку кожного пакета, що входить в інтерфейс, і дзеркальне відображення порту також вибере цей пакет для копіювання і відправки на порт призначення, виконується тільки процес дзеркального копіювання порту. Пакети з вибіркою трафіку, які не вибрані для віддзеркалення портів, як і раніше відбираються і перенаправляються на сервер cflowd.

Ми можемо використовувати віддзеркалення портів для копіювання:

- Всі пакети, що входять в інтерфейс або виходять з нього, в будь-якій комбінації. Копії пакетів, що входять до деяких інтерфейсів, і пакетів, що виходять з інших інтерфейсів, можуть бути відправлені на той же локальний інтерфейс або VLAN. Якщо ми налаштуємо дзеркальне відображення портів для копіювання пакетів, що виходять з інтерфейсу, трафік, що виходить від цього комутатора або пристрою вузла, що не копіюється при виході. На виході копіюється тільки комутований трафік.
- Будь-які або всі пакети, що входять в VLAN. Ми не можемо використовувати віддзеркалення портів для копіювання пакетів, що виходять з VLAN.
- Відфільтрований фаєрволом зразок пакетів, що надходять на порт або VLAN.

Щоб налаштувати віддзеркалення портів, необхідно налаштувати екземпляр одного з наступних типів:

- Примірник аналізатора – необхідно вказати вхід і вихід для екземпляра. Цей тип примірника корисний для гарантії того, що весь трафік, що проходить через інтерфейс або входить в VLAN, віддзеркалювався і відправлявся аналізатору.

- Примірник дзеркального відображення порту – необхідно створити фільтр брандмауера, який ідентифікує бажаний трафік і копіює його на дзеркальний порт. Вказуєте введення для цього типу примірника не потрібно. Цей тип примірника корисний для управління типами дзеркального трафіку. Направляти на нього трафік необхідно за допомогою таких дій:
 - Вказати ім'я екземпляра дзеркального відображення портів в фільтрі брандмауера за допомогою дії, якщо декілька примірників дзеркального відображення портів. *port-mirror-instance instance-name*
 - Надіслати дзеркальні пакети на вихідний інтерфейс, визначений в екземплярі, за допомогою *port-mirror* дії, коли визначено тільки один екземпляр дзеркального відображення порту.

Дзеркальне відображення тільки пакетів, необхідних для аналізу, знижує можливість зниження загальної продуктивності. Якщо ми відзеркалюємо трафік з кількох портів, дзеркальний трафік може перевищувати ємність вихідного інтерфейсу. Пакети переповнення відкидаються. Рекомендується обмежити обсяг дзеркального трафіку, вибравши певні інтерфейси і уникаючи використання *all* ключового слова. Ми також можемо обмежити обсяг дзеркального трафіку, використовуючи фільтр брандмауера для відправки певного трафіку на екземпляр дзеркального відображення порту.

Наступні обмеження застосовуються до локального і віддаленого віддзеркалення портів:

- Всього можна створити чотири конфігурації віддзеркалення портів.
- Кожна група вузлів підпорядковується наступним обмеженням:
 - Для віддзеркалення локального порту можна використовувати до чотирьох конфігурацій.

- Для віддзеркалення віддаленого порту можна використовувати до трьох конфігурацій.
- Незалежно від того, налаштовуємо ми автономний комутатор або групу вузлів:
 - Може бути не більше двох конфігурацій, віддзеркалюється вхідний трафік. Якщо ми налаштовуємо фільтр брандмауера для відправки дзеркального трафіку на порт, це вважається вхідною конфігурацією дзеркального відображення для комутатора або групи вузлів, до яких застосовується фільтр.
 - Може бути не більше двох конфігурацій, що відбивають вихідний трафік.
 - У системах немає загальносистемного обмеження на загальну кількість дзеркальних сеансів.
- Ми можемо налаштувати тільки один тип виведення в одній конфігурації дзеркального відображення порту для виконання оператора: *set analyzer name output*
 - interface
 - ip-address
 - vlan
- Необхідно налаштувати віддзеркалення в аналізаторі (з *set forwarding-options analyzer*) тільки на одному логічному інтерфейсі для одного і того ж фізичного інтерфейсу. Якщо ми спробуємо налаштувати дзеркальне відображення на декількох логічних інтерфейсах, налаштованих на фізичному інтерфейсі, буде успішно налаштований тільки перший логічний інтерфейс; інші логічні інтерфейси повертають помилки конфігурації.
- Якщо ми дзеркалюємо вихідні пакети, не можна налаштовувати більше 2000 VLAN на автономному комутаторі. У цьому випадку деякі пакети

VLAN можуть містити невірні ідентифікатори VLAN. Це відноситься до будь-яких пакетів VLAN, а не тільки до дзеркальних копій.

- Параметри *ratio* і *loss-priority* не підтримуються.
- Пакети з помилками фізичного рівня не відправляються на вихідний порт або VLAN.
- Якщо ми використовуємо моніторинг sFlow для вибірки трафіку, він не виконує вибірку дзеркальних копій, коли вони виходять з вихідного інтерфейсу.
- Ми не можемо створювати дзеркальні пакети, що виходять або входять до наступних портів:
 - Виділені інтерфейси віртуального шасі
 - Інтерфейси управління (me0 або vme0)
 - Інтерфейси Fibre Channel
 - Інтегровані інтерфейси маршрутизації і моста (IRB) (також відомі як маршрутизовані інтерфейси VLAN або RVI)
- Агрегований інтерфейс Ethernet не може бути вихідним інтерфейсом, якщо входом є VLAN або якщо трафік відправляється на аналізатор з використанням фільтра брандмауера.
- Коли дзеркальні пакети відправляються з вихідного інтерфейсу, вони не змінюються для будь-яких змін, які можуть бути застосовані до вихідних пакетів на виході, таких як перезапис CoS.
- Інтерфейс може бути інтерфейсом введення тільки для однієї конфігурації дзеркального відображення. Не можна використовувати той же інтерфейс, що і вхідний, для декількох конфігурацій дзеркального відображення.
- Пакети, згенеровані ЦП (такі як пакети ARP, ICMP, BPDU і LACP), не можуть бути дзеркально відображені на виході.

- Дзеркальне відображення на основі VLAN не підтримується для трафіку STP.
- Істинне вихідне дзеркальне відображення визначається як дзеркальне відображення точного числа копій і математичних моделей пакетів, відправлених через вихідний порт. Оскільки процесори на комутаторах реалізують віддзеркалення вихідного трафіку у вхідному конвеєрі, ці комутатори не забезпечують математичної моделі вихідних пакетів, тому що вихідний дзеркальний трафік може містити неправильні теги VLAN, які відрізняються від тегів у вихідному трафіку.
- Якщо ми налаштовуємо екземпляр дзеркального відображення портів для дзеркального відображення трафіку, що виходить з інтерфейсу, який виконує інкапсуляцію VLAN, вихідні і цільові MAC-адреси дзеркальних пакетів не збігаються з MAC-адресами вихідних пакетів.
- Дзеркальне відображення вихідної VLAN не підтримується.

Використовувати віддзеркалення портів для відправки трафіку на пристрої, які аналізують трафік в таких цілях, як моніторинг відповідності, застосування політик, виявлення вторгнень, моніторинг і прогнозування шаблонів трафіку, і т.д. Дзеркальне відображення портів необхідно, коли ми хочемо виконати аналіз трафіку, оскільки комутатор зазвичай відправляє пакети тільки на порт, до якого підключено пристрій призначення. Поширеною альтернативою є налагодження віддзеркалення портів для відправки копій одноадресного трафіку на інший інтерфейс і запуск програми аналізатора на пристрій, підключений до цього інтерфейсу.

Щоб налаштувати віддзеркалення портів, ми налаштовуємо екземпляр дзеркального відображення портів. Ми не вказуємо введення для цього примірника. Замість цього ми створюємо фільтр брандмауера, який визначає необхідний трафік і направляє його до примірника, включаючи *port-mirror* дію

в *then* член фільтра. Фільтр брандмауера повинен бути налаштований як *family inet*.

Необхідно пам'ятати про продуктивність при налаштуванні віддзеркалення портів. Налаштування фільтра брандмауера для віддзеркалення тільки необхідних пакетів знижує ймовірність зниження продуктивності.

Дзеркальне відображення може знадобитися для аналізу трафіку на комутаторі, оскільки комутатор, на відміну від концентратора, що не передає пакети на кожен порт на цільовому пристрої. Комутатор відправляє пакети тільки на порт, до якого підключений цільовий пристрій.

Дзеркальне відображення портів використовується для копіювання пакетів на локальний інтерфейс для локального моніторингу або в VLAN для віддаленого моніторингу. Ми можемо використовувати аналізатори для забезпечення дотримання політик, що стосуються використання мережі та спільного використання файлів, а також для виявлення джерел проблем у нашій мережі шляхом виявлення аномального або інтенсивного використання смуги пропускання певними станціями або додатками [4].

1.3. Порівняння принципів роботи технологій SPAN/RSPAN/ ERSPAN

Аналізатор портів комутатора (SPAN) – це ефективна і високопродуктивна система моніторингу трафіку. Він направляє або віддзеркалює трафік з вихідного порту або VLAN на порт призначення. Іноді це називають моніторингом сеансу. SPAN використовується, для усунення проблем з підключенням і розрахунку використання і продуктивності мережі.

У продуктах Cisco підтримуються три типи SPAN:

- SPAN або місцевий SPAN.
- Віддалений SPAN (RSPAN).
- Інкапсульований віддалений SPAN (ERSPAN).

На рисунку 1.4 представлена діаграма, яка відображає всі три типи SPAN.

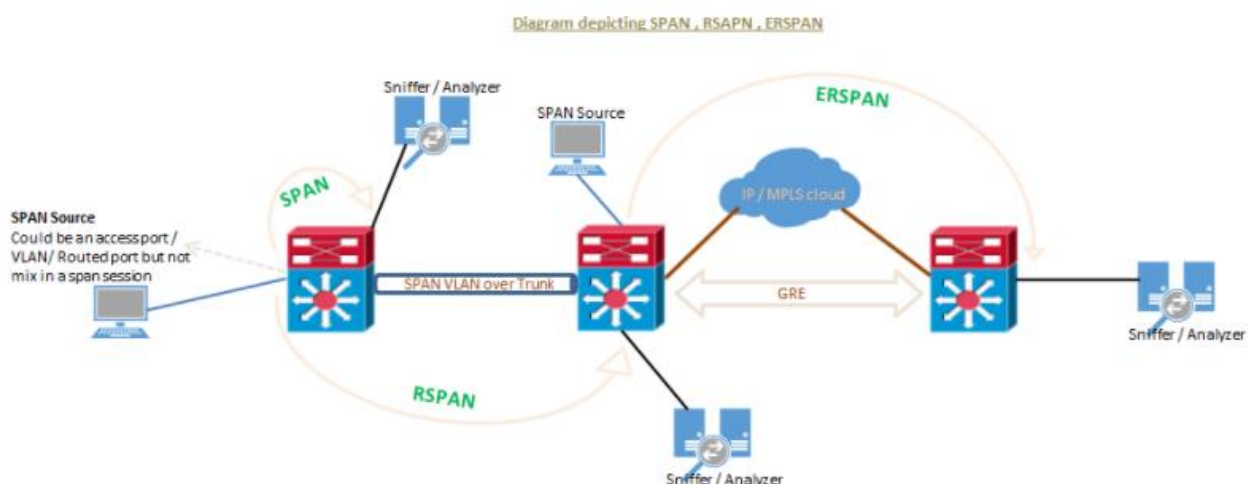


Рисунок 1.4 – Діаграма, яка зображує технології SPAN, RSPAN та ERSPAN

Віддзеркалення портів / трафіку (SPAN) використовується для багатьох цілей, деякі з них описані нижче:

- Впровадження IDS / IPS в нерозбірливому режимі.
- Рішення для запису розмов по VOIP.
- Причини відповідності вимогам безпеки для моніторингу та аналізу трафіку.
- Усунення проблем з підключенням, моніторинг трафіку.

Незалежно від запущеного типу SPAN, джерелом SPAN може бути будь-який тип порту, наприклад, порт маршрутизації, фізичний порт комутатора, порт доступу, магістраль, VLAN (всі активні порти комутатора відслідковуються), EtherChannel (порт або весь порт – каналні інтерфейси) і т.д. Звернемо увагу на те, що порт, налаштований для призначення SPAN, не може бути частиною VLAN джерела SPAN.

Сеанси SPAN підтримують моніторинг вхідного трафіку (вхідний SPAN), вихідного трафіку (вихідний SPAN) або трафіку, що проходить в обох напрямках.

- Ingress SPAN (RX) копіює трафік, отриманий вихідними портами і VLAN, в порт призначення. SPAN копіює трафік перед будь-якою модифікацією (наприклад, перед будь-яким фільтром VACL або ACL, QoS або політикою входу або виходу).
- Вихідний SPAN (TX) копіює трафік, що передається з вихідних портів і віртуальних локальних мереж, в порт призначення. Вся відповідна фільтрація або модифікація за допомогою VACL або ACL-фільтра, QoS, вхідного або вихідного трафіку виконуються до того, як комутатор перенаправляє трафік на порт призначення SPAN.
- Коли використовується ключове слово both, SPAN копіює мережевий трафік, отриманий і переданий вихідними портами і VLAN, в порт призначення.
- SPAN / RSPAN зазвичай ігнорує кадри CDP, STP BPDU, VTP, DTP і RAgP. Однак ці типи трафіку можуть бути перенаправлені, якщо налаштована команда реплікації інкапсуляції.

SPAN віддзеркалює трафік від одного або декількох інтерфейсів комутатора до одного або декількох інтерфейсів на тому ж комутаторі; тому SPAN найчастіше називають LOCAL SPAN.

Рекомендації або обмеження для місцевого SPAN:

- Комутовані порти рівня 2 і порти рівня 3 можуть бути налаштовані як порти джерела або призначення.
- Джерелом може бути один або кілька портів або VLAN, але не їх поєднання.
- Магістральні порти – це допустимі вихідні порти, змішані з вихідними не магістральними портами.
- На комутаторі можна налаштувати до 64 портів призначення SPAN.

- Коли ми налаштовуємо порт призначення, його вихідна конфігурація перезаписується. Якщо конфігурація SPAN видалена, вихідна конфігурація цього порту відновлюється.
- Під час налаштування порту призначення порт видаляється з будь-якого пакета EtherChannel, якщо він був його частиною. Якщо це був порт маршрутизації, конфігурація призначення SPAN перевизначає конфігурацію маршрутизації порту.
- Порти призначення не підтримують безпеку портів, аутентифікацію 802.1x або приватні VLAN.
- Порт може діяти як порт призначення лише для одного сеансу SPAN.
- Порт не може бути налаштований в якості порту призначення, якщо він є портом-джерелом зв'язкового сеансу або частиною вихідної VLAN.
- Інтерфейси каналу порту (EtherChannel) можуть бути налаштовані як вихідні порти, але не як порт призначення для SPAN.
- Напрямок трафіку за замовчуванням для джерел SPAN – «обидва».
- Порти призначення ніколи не беруть участь в екземплярі сполучного дерева. Не може підтримувати DTP, CDP і т.д. Локальний SPAN включає в себе BPDU в відстежуваному трафіку, тому будь-які BPDU, видимі на порту призначення, копіюються з порту джерела. Отже, не можна підключати комутатор до цього типу SPAN, так як це може викликати петлю в мережі.
- Коли VLAN налаштований як джерело SPAN (найчастіше званий VSPAN) з налаштованими параметрами входу і виходу, необхідно надсилати пакети, які дублюються з вихідного порту тільки в тому випадку, якщо пакети комутуються в одній і тій же VLAN. Одна копія пакету відноситься до вхідного трафіку на вхідному порту, а інша копія пакету – до вихідного трафіку на вихідному порту.

- VSPAN відстежує тільки трафік, який залишає або входить в порти рівня 2 в VLAN.

Remote SPAN (RSPAN) схожий на SPAN, але підтримує вихідні порти, вихідні VLAN і цільові порти на різних комутаторах, які забезпечують віддалений моніторинг трафіку з вихідних портів, розподілених по декількох комутаторах, і дозволяють цільовим призначенням централізувати пристрої захоплення мережі. Кожен сеанс RSPAN передає трафік SPAN через виділену користувачем RSPAN VLAN на всіх, що беруть участь комутаторах. Потім ця VLAN з'єднується з іншими комутаторами, дозволяючи передавати трафік сеансу RSPAN через кілька комутаторів і доставляти його на станцію захоплення призначення. RSPAN складається з вихідного сеансу RSPAN, RSPAN VLAN і цільового сеансу RSPAN.

Рекомендації або обмеження для RSPAN:

- Певна VLAN повинна бути налаштована для призначення SPAN, який буде проходити через проміжні комутатори через магістральні канали до порту призначення.
- Можна створити джерело одного і того ж типу – принаймні, один порт або хоча б одну VLAN, але не може бути змішаним.
- Призначенням сеансу є RSPAN VLAN, а не єдиний порт в комутаторі, тому всі порти в RSPAN VLAN отримуватимуть дзеркальний трафік.
- Потрібно налаштувати будь-яку VLAN, як RSPAN VLAN, якщо всі мережеві пристрої, які беруть участь підтримують конфігурацію RSPAN VLAN, і використовувати одну і ту ж RSPAN VLAN для кожного сеансу RSPAN.
- VTP може поширювати конфігурацію VLAN з номерами від 1 до 1024 як RSPAN VLAN, необхідно вручну налаштувати VLAN з номерами за 1024

як RSPAN VLAN на всіх вихідних, проміжних і цільових мережесих пристроях.

- Вивчення MAC-адрес відключено в RSPAN VLAN.

Інкапсульований віддалений SPAN (ERSPAN) забезпечує універсальну інкапсуляцію маршрутизації (GRE) для всього захопленого трафіку і дозволяє поширювати його на домени рівня 3.

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

Рекомендації або обмеження для ERSPAN:

- Вихідні сеанси ERSPAN копіюють інкапсульований ERSPAN GRE трафік з вихідних портів. Кожен вихідний сеанс ERSPAN може мати в якості джерел або порти, або VLAN, але не те й інше разом.
- Незалежно від будь-якого налаштованого розміру MTU, ERSPAN створює пакети рівня 3, довжина яких може досягати 9202 байта. Трафік ERSPAN може бути відкинутий будь-яким інтерфейсом в мережі, який вимагає, щоб розмір MTU був менше 9 202 байта.
- ERSPAN не підтримує фрагментацію пакетів. Біт «не фрагментувати» встановлено в IP-заголовку пакетів ERSPAN. Сеанси призначення ERSPAN не можуть повторно зібрати фрагментовані пакети ERSPAN.
- ERSPAN ID відрізняє трафік ERSPAN, що надходить на одну і ту ж IP-адресу призначення, з різних вихідних сеансів ERSPAN; налаштований ERSPAN ID повинен збігатися на вихідному і цільовому пристроях.
- Для вихідного порту або вихідної VLAN ERSPAN може відстежувати вхідний, вихідний або і вхідний, і вихідний трафік. За замовчуванням

ERSPAN відстежує весь трафік, включаючи багатоадресну розсилку і кадри блоку даних протоколу моста (BPDU).

- Інтерфейс тунелю, підтримуваний в якості вихідних портів для вихідного сеансу ERSPAN – це GRE, IPinIP, SVTI, IPv6, IPv6 через IP-тунель, багатоточковий GRE (mGRE) і безпечні віртуальні тунельні інтерфейси (SVTI).
- Параметр фільтрації VLAN не працює в сеансі моніторингу ERSPAN на інтерфейсах WAN.
- ERSPAN на маршрутизаторах Cisco ASR серії 1000 підтримує тільки інтерфейси рівня 3. Інтерфейси Ethernet не підтримуються ERSPAN, якщо вони налаштовані як інтерфейси рівня 2.
- Коли сеанс налаштовується через інтерфейс командного рядка конфігурації ERSPAN, ідентифікатор сеансу і тип сеансу не можуть бути змінені. Щоб змінити їх, необхідно спочатку використовувати форму *по* команди конфігурації, щоб видалити сеанс, а потім переналаштувати сеанс.

Щоб використовувати ERSPAN для моніторингу трафіку через один або кілька портів або VLAN на одному пристрої, ми повинні створити сеанси джерела ERSPAN і призначення ERSPAN на одному пристрої, потік даних відбувається всередині маршрутизатора, що аналогічно локальному SPAN.

При використанні ERSPAN як локального SPAN діють наступні фактори:

- Обидва сеанси мають однаковий ідентифікатор ERSPAN.
- Обидва сеанси мають однакову IP-адресу. Ця IP-адреса є власною IP-адресою маршрутизатора; тобто IP-адреса зворотньої петлі або IP-адреса, налаштована для будь-якого порту [6].

1.4. Технічне завдання

Мета дипломного проекту полягає в ознайомленні з методикою і принципами налаштування технологій дзеркалювання трафіку. Буде закріплено знання в процесі дослідження даної тематики, а саме під час розробки топології мережі, логічного проектування, розробки адресації та налаштування створеної нами комп'ютерної мережі. В результаті ми отримаємо розроблений проект комп'ютерної мережі на базі технологій SPAN/RSPAN.

Необхідно оптимізувати нашу мережу задля економії IP-адрес, пристроїв та кабелів підключення, а також для можливості розміщення якомога більшої кількості робочих станцій.

Комп'ютерна мережа має поділятися на дві частини, кожна з яких буде відповідати окремій технології SPAN , або RSPAN. Підмережі, які будуть входити в частину мережі з технологією SPAN будуть містити по одному концентратору в підмережі. В свою чергу, підмережі технології RSPAN будуть містити по два концентратори, які будуть з'єднанні між собою. Обидві частини мережі будуть під'єднанні до головного маршрутизатора, який, також, буде під'єднаний до сервера.

У роботі необхідно реалізувати модель мережі в симуляторі мережі передачі даних Packet Tracer.

Результатом реалізації даного проекту є коректно працююча комп'ютерна мережа та детальний план дій по її налаштуванню. Проект може бути корисним при розробці плану розташування обладнання і його налагодження для будь-якої компанії.

РОЗДІЛ 2. ПРОЕКТУВАННЯ ПІДСИСТЕМИ ДЗЕРКАЛЮВАННЯ ТРАФІКУ СИСТЕМИ БЕЗПЕКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ

2.1. Розробка топології комп'ютерної мережі

Топологія мережі характеризується, як фізичне розташування комп'ютерів, кабелів та інших компонентів мережі. Існує кілька способів організувати мережу. У кожного з них є свої переваги і недоліки, і в залежності від потреб нашої компанії певні заходи можуть дати нам велику ступінь підключення і безпеки.

Існує два підходи побудови топології мережі: фізичний і логічний. Топологія фізичної мережі, відноситься до фізичних з'єднань і взаємозв'язків між вузлами і мережею – проводами, кабелями і т.д. Логічна топологія мережі є трохи більш абстрактною і стратегічною, маючи на увазі розуміння того, як і чому мережа влаштована так, як вона є, і як дані переміщаються по ній.

Фізичне і логічне представлення нашої мережі дуже важливе з кількох причин. Перш за все, воно відіграє важливу роль в тому, як і наскільки добре працюватиме наша мережа в житті. Вибір правильної топології для операційної моделі нашої компанії може підвищити продуктивність, спростивши виявлення несправностей та усунення помилок, а також допоможе більш ефективно розподіляти ресурси по мережі для забезпечення оптимального стану мережі. Оптимізована і правильно керована топологія мережі може підвищити ефективність використання енергії та даних, що, в свою чергу, може допомогти знизити експлуатаційні витрати і витрати на обслуговування.

Дизайн і структура мережі зазвичай відображаються і управляються, на створеній програмним забезпеченням, схемою топології мережі. Ці діаграми важливі з кількох причин, але особливо для того, як вони можуть забезпечити

візуальне уявлення як фізичних, так і логічних схем, дозволяючи адміністраторам бачити з'єднання між пристроями при усуненні неполадок.

Спосіб організації мережі може поліпшити або порушити функціональність мережі, можливість підключення і захист від інших простоїв.

Представлення мережі поділяється на:

- Фізичне – фізична топологія мережі відноситься до фактичних з'єднань (дроти, кабелі і т. д.) до того, як влаштована мережа. Завдання налаштування, обслуговування та ініціалізації вимагають розуміння фізичної мережі.
- Логічне – логічна топологія мережі являє собою високоріневе уявлення про те, як налаштована мережа, в тому числі про те, які вузли з'єднуються один з одним і якими способами, а також про те, як дані передаються через мережу. Логічна топологія мережі включає будь-які віртуальні і хмарні ресурси.

Ефективне управління і моніторинг мережі вимагають чіткого розуміння фізичної і логічної топології мережі, щоб забезпечити її ефективність і працездатність. Саме тому, при проектуванні мережі було використано зіркоподібну модель мережі, рисунок 2.1.

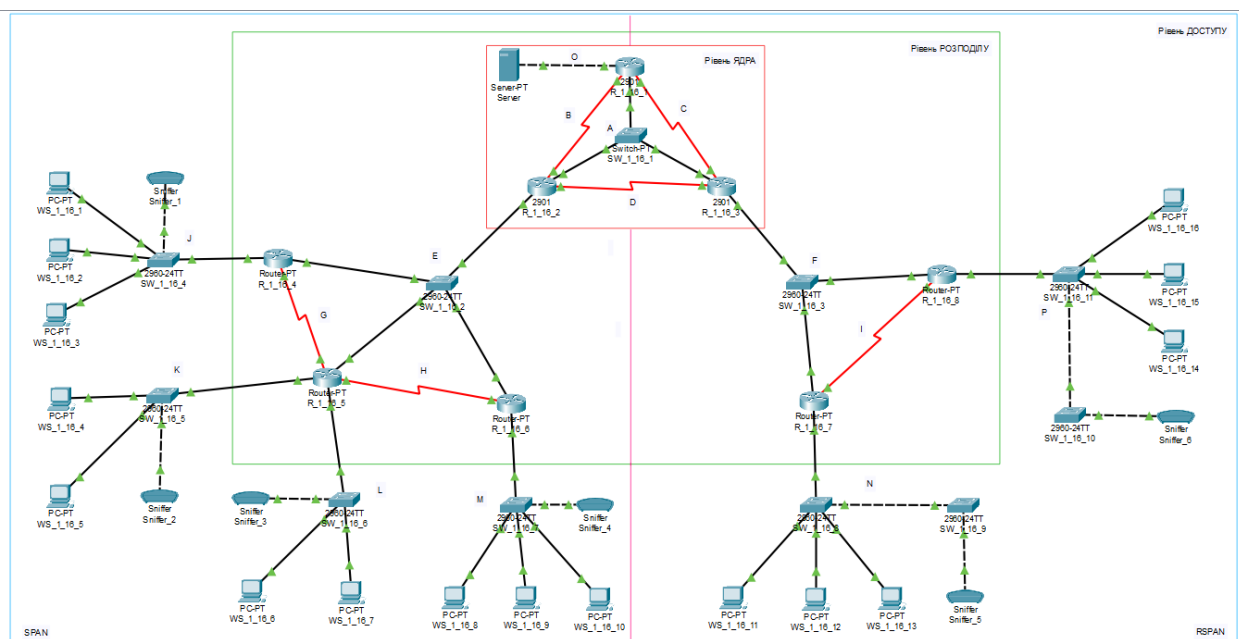


Рисунок 2.1 – Топологія мережі

Зіркоподібна модель мережі є реалізацією системи розподілу мережі на хости, які підключені до центрального концентратора, або комутатора. Тобто, центральний концентратор діє як канал для передачі повідомлень. Зіркоподібна мережа є однією з найбільш поширених топологій комп'ютерних мереж.

Комутатори і робочі станції, а також лінії передачі між ними утворюють граф з топологією зірки. Дані в зіркоподібній мережі проходять через концентратор, перш ніж перейти до місця призначення. Комутатор управляє і контролює всі функції мережі. Він також діє як повторювач для потоку даних.

Топологія «зірка» знижує вплив відмови лінії передачі за рахунок незалежного підключення кожної робочої станції до концентратора. Таким чином, кожен хост може зв'язуватися з усіма іншими, передаючи і отримуючи від концентратора потрібні дані. Відмова лінії передачі, що з'єднує будь-яку робочу станцію з комутатором, призведе до ізоляції цієї станції від усіх інших, але інша частина мережі не постраждає.

Конфігурація зірки зазвичай використовується з кабелем витвої пари і оптоволоконним кабелем. Однак його також можна використовувати з коаксіальним кабелем.

Розташування вузлів в зіркоподібній топології дає деякі переваги:

- Кожен вузол підключається окремо, тому відмова одного вузла або його ланки, не впливає на інші вузли.
- Нові вузли можуть бути додані в мережу, просто підключивши їх до комутатора.
- Зіркоподібні мережі, як правило, мають більш високу продуктивність, оскільки повідомлення передається тільки передбачуваному одержувачу.
- Легко усуваються неполадки, налаштовується і вносяться зміни.
- Висока продуктивність з невеликою кількістю вузлів і дуже низьким мережевим трафіком.

Однак у зіркоподібних топологій є і свої недоліки, такі як:

- Вся мережа виходить з ладу, якщо комутатор виходить з ладу, оскільки жоден вузол не може спілкуватися.
- Топологія зірки вимагає великої кількості кабелю – у великій мережі це може бути затратно.
- Іноді інтенсивний мережевий трафік може значно сповільнити роботу мережі.
- Продуктивність залежить від ємності комутатора (концентратора).
- Пошкоджений кабель може вивести мережу з ладу.

Зіркоподібні топології зазвичай використовуються в великих організаціях, таких як освітні установи і підприємства, де висока продуктивність є обов'язковою.

Також в побудові мережі було використано трирівневу ієрархічну модель мережі, яка містить в собі:

- Рівень ядра
- Рівень розподілу
- Рівень доступу.

Оскільки наша мережа має бути складною, з безліччю протоколів і різноманітними технологіями, багаторівнева ієрархічна модель є чудовим виходом для проектування надійної мережевої інфраструктури. Ця трирівнева модель допомагає проектувати, впроваджувати та підтримувати масштабовану, надійну і економну мережу. Кожен з шарів має свої особливості і функції, що знижує складність мережі.

- Рівень доступу – контролює доступ користувачів і робочих груп до ресурсів в мережі. Цей рівень зазвичай включає комутатори рівня 2 і точки доступу, які забезпечують зв'язок між робочими станціями і серверами. Ми маємо змогу управляти контролем доступу і політикою,

створювати окремі домени конфліктів і реалізовувати безпеку портів на цьому рівні.

- Рівень розподілу – служить точкою зв'язку між рівнем доступу і ядром. Його основні функції – забезпечувати маршрутизацію, фільтрацію і доступ до глобальної мережі, а також визначати, як пакети можуть отримати доступ до ядра. Цей рівень визначає найшвидший спосіб доступу до запитів мережесервісів – наприклад, як запит файлу пересилається на сервер – і, при необхідності, пересилає запит на базовий рівень. Цей рівень зазвичай складається з маршрутизаторів і багаторівневих комутаторів.
- Рівень ядра – також званий магістраллю мережі, цей рівень відповідає за швидке транспортування великих обсягів трафіку. Базовий рівень забезпечує взаємодію між пристроями рівня розподілу. Зазвичай він складається з високошвидкісних пристроїв, таких як високопродуктивні маршрутизатори і комутатори з надлишковими каналами.

Загалом мережа складається з 16 підмереж і символічно розділена на дві частини, кожна з яких відповідає технологіям SPAN та RSPAN.

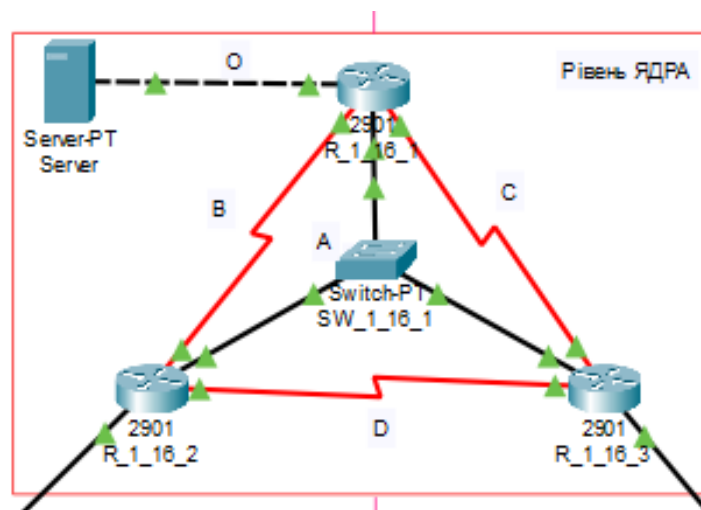


Рисунок 2.2 – Рівень ядра

Рівень ядра складається з трьох трьох маршрутизаторів, одного комутатора і сервера, рисунок 2.2. Так, як рівень ядра є магістраллю мережі, він

має працювати швидко, тому з'єднання між високопродуктивними пристроями здійснюється за допомогою кабелів Gigabit Ethernet між маршрутизаторами і комутатором чи сервером.

Gigabit Ethernet також відомий як 1000BaseT. Він являє собою звичайну версію Ethernet, що працює на швидкостях до 1.000 мегабіт в секунду, тобто в десять разів швидше ніж 100BaseT.

Оскільки Gigabit Ethernet забезпечує в десять разів більший канал, ніж звичний 100BaseT, природним застосуванням стандарту є з'єднання ділянок, що вимагають високу пропускну здатність. Як приклад, це може бути зв'язок між серверами, комутаторами і магістральними вузлами. Саме тут Gigabit Ethernet буде необхідний, потрібний і корисний.

В нашому випадку, це є чудовим вирішенням проблеми з передачею "великих файлів". Так як, наша мережа передбачає налаштування на резервування всіх комп'ютерів на один файловий сервер, то Gigabit Ethernet дозволить вам прискорити цей процес.

На рівні ядра маршрутизатори з'єднанні між собою завдяки послідовним каналам Serial. Також в процесі налаштування буде визначено, які роутери будуть виступати в ролі DTE, а які в ролі DCE.

Даний рівень містить в собі п'ять підмереж, а саме підмережі А, В, С, D та О. Три з них розташовані між маршрутизаторами, а одна з'єднує головний маршрутизатор з сервером.

Рівень розподілу складається з п'яти маршрутизаторів і двох комутаторів, рисунок 2.3. Аналогічно, до рівня ядра з'єднання між маршрутизаторами і комутаторам здійснюється за допомогою каналів зв'язку витвої пари Gigabit Ethernet. Маршрутизатори рівня розподілу з'єднані між собою за допомогою послідовних каналів зв'язку Serial.

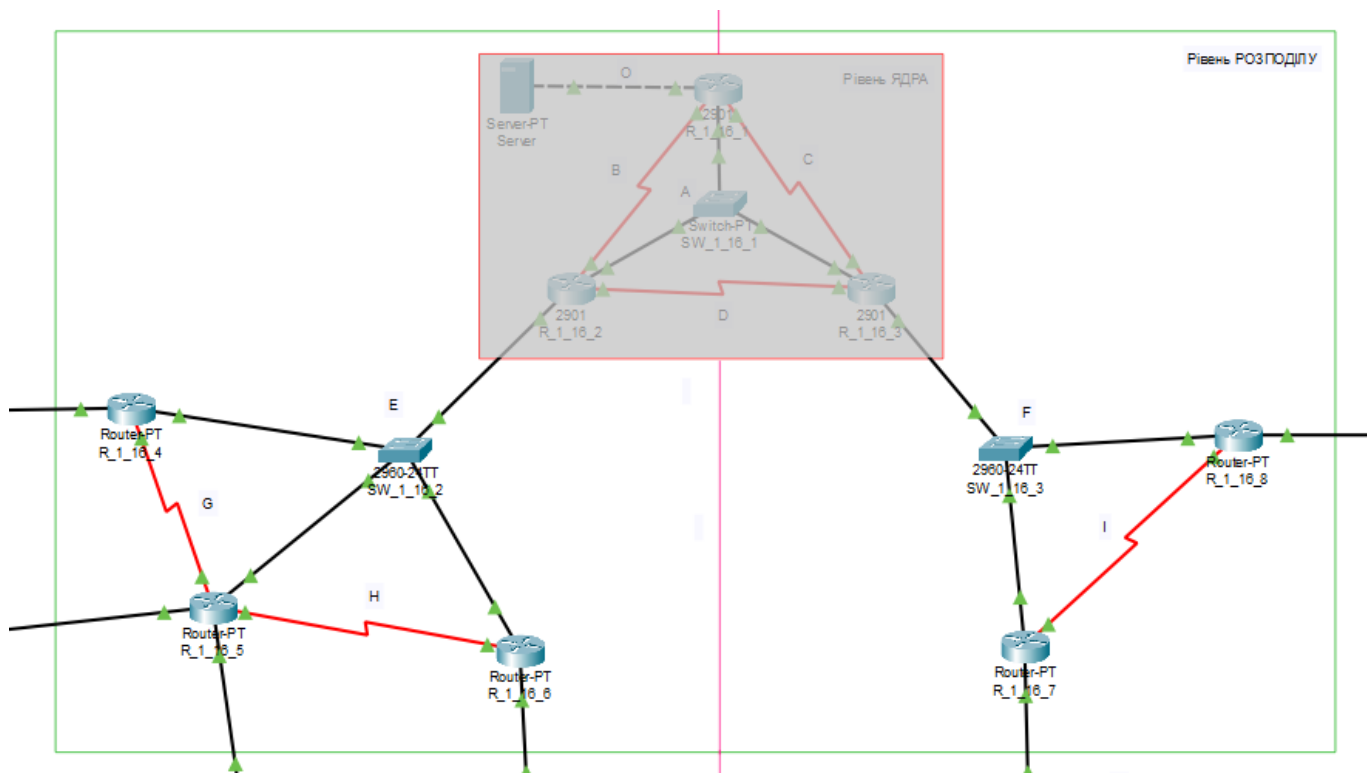


Рисунок 2.3 – Рівень розподілу

Рівень розподілу представляє собою два набори обладнання, що в свою чергу виступають підмережами Е та F. Підмережі G, Н, І розташовані між маршрутизаторами.

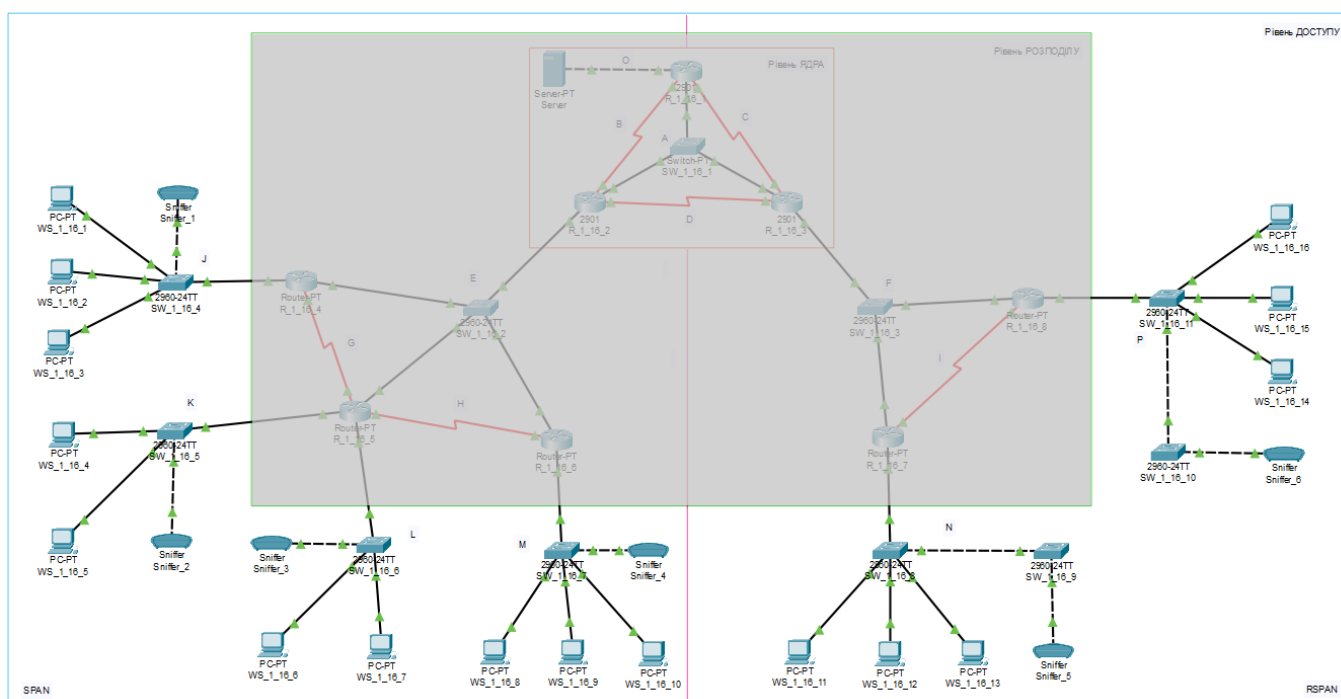


Рисунок 2.4 – Рівень доступу

Рівень доступу складається з шести підмереж, рисунок 2.4, а саме з підмереж J, K, L, M, N та P. З'єднання в підмережах відбувається за допомогою виті пари технології Fast Ethernet. На невеликих відстанях виті пара дозволяє передавати дані з тією ж швидкістю, що і коаксіальний кабель, але мережа виходить більш дешевою і зручною в експлуатації. Кожна з цих підмереж обладнана сніффером, що дозволяє перехоплювати і пересилати всі пакети по певному каналу на віддалену машину, на якій працює програмне забезпечення аналізатора пакетів. Ці пакети містять інформацію про відмітки часу, потужності сигналу, розмірах пакетів і т. д. Сніффери дозволяють відстежувати і записувати мережеву активність, а також виявляти проблеми. В підмережах технології SPAN є можливість підключити до кожного комутатора близько двадцяти двох робочих станцій. В підмережах технології RSPAN є можливість підключити до кожного комутатора близько сорока робочих станцій.

2.2. Розробка схеми адресації пристроїв мережі

Після того, як було визначено топологію мережі, необхідно розробити схему адресації комп'ютерної мережі.

Нижче буде наведено неповну таблицю, в якій буде описано адресацію пристроїв мережі, таблиця 2.1. Таблиці параметрів інтерфейсів пристроїв та параметрів адресації мережі будуть представлені в додатках.

Таблиця 2.1 – Параметри адресації мережі

Підмережа	Інтерфейс	ІР-адреса	Маска	Преф.
Підмережа А	-	191.1.16.0	255.255.255.248	/29
Підмережа В	-	191.1.16.8	255.255.255.252	/30
Підмережа С	-	191.1.16.12	255.255.255.252	/30
Підмережа D	-	191.1.16.16	255.255.255.252	/30
Підмережа Е	-	192.1.16.0	255.255.255.248	/29

Підмережа F	-	193.1.16.0	255.255.255.248	/29
Підмережа G	-	194.1.16.0	255.255.255.252	/30
Підмережа H	-	194.1.16.4	255.255.255.252	/30
Підмережа I	-	195.1.16.0	255.255.255.252	/30
Підмережа J	-	196.1.16.0	255.255.255.0	/24
Підмережа K	-	197.1.16.0	255.255.255.128	/25
Підмережа L	-	197.1.16.128	255.255.255.128	/25
Підмережа M	-	198.1.16.0	255.255.255.0	/24
Підмережа N	-	199.1.16.0	255.255.255.0	/24
Підмережа P	-	200.1.16.0	255.255.255.0	/24
Підмережа O	-	190.1.16.0	255.255.255.252	/30
Маршрутизатор R_1_16_1	Gig0/0	191.1.16.1	255.255.255.248	/29
	Se0/0/0	191.1.16.9	255.255.255.252	/30
	Se0/0/1	191.1.16.13	255.255.255.252	/30
	Gig0/1	190.1.16.1	255.255.255.252	/30
Маршрутизатор R_1_16_2	Gig0/0	191.1.16.2	255.255.255.248	/29
	Se0/0/0	191.1.16.10	255.255.255.252	/30
	Se0/0/1	191.1.16.17	255.255.255.252	/30
	Gig0/1	192.1.16.1	255.255.255.248	/29
Маршрутизатор R_1_16_3	Gig0/0	191.1.16.3	255.255.255.248	/29
	Se0/0/1	191.1.16.14	255.255.255.252	/30
	Se0/0/0	191.1.16.18	255.255.255.252	/30
	Gig0/1	193.1.16.1	255.255.255.248	/29
Маршрутизатор R_1_16_4	Gig0/0	192.1.16.2	255.255.255.248	/29
	Se3/0	194.1.16.1	255.255.255.252	/30
	Fa1/0	196.1.16.1	255.255.255.0	/24
Маршрутизатор R_1_16_5	Gig0/0	192.1.16.3	255.255.255.248	/29
	Se3/0	194.1.16.2	255.255.255.252	/30
	Se4/0	194.1.16.5	255.255.255.252	/30

	Fa1/0	197.1.16.1	255.255.255.128	/25
	Fa2/0	197.1.16.129	255.255.255.128	/25
Маршрутизатор R_1_16_6	Gig0/0	192.1.16.4	255.255.255.248	/29
	Se4/0	194.1.16.6	255.255.255.252	/30
	Fa1/0	198.1.16.1	255.255.255.0	/24
Маршрутизатор R_1_16_7	Gig0/0	193.1.16.2	255.255.255.248	/29
	Se3/0	195.1.16.1	255.255.255.252	/30
	Fa1/0	199.1.16.1	255.255.255.0	/24
Маршрутизатор R_1_16_8	Gig0/0	193.1.16.3	255.255.255.248	/29
	Se3/0	195.1.16.2	255.255.255.252	/30
	Fa1/0	200.1.16.1	255.255.255.0	/24
Сервер Server	Мережний адаптер	190.1.16.2	255.255.255.252	/30
	Інтерфейс за замовчуванням	190.1.16.1	-	-

IP-адресацію на робочих станціях налаштуємо за допомогою протоколу динамічної конфігурації DHCP.

2.3. Логічне проектування підсистеми дзеркалювання трафіку

Для початку необхідно буде налаштувати IP-адресацію. Це необхідно для того, щоб робочі станції мали змогу відправляти та отримувати інформацію. Існує чотири різних типи IP-адрес: загальнодоступні, приватні, статичні і динамічні. Загальнодоступна і приватна адреси вказують на місце розташування мережі – приватна використовується всередині мережі, а загальнодоступна використовується поза мережею.

Статична IP-адреса створюється вручну, а не призначається системою. Статична адреса не змінюється, у той час, як динамічна IP-адреса призначається сервером протоколу динамічної конфігурації хоста (DHCP) і

може бути зміна. Динамічні IP-адреси є найбільш поширеним типом адрес інтернет-протоколу. Динамічні IP-адреси активні тільки протягом певного часу, після закінчення якого термін їх дії закінчується. Комп'ютер або автоматично запросить нову оренду, або комп'ютер може отримати нову IP-адресу.

Оскільки наша мережа велика, то статично задавати IP-адреси буде складно і трудомістко, тому адреси для робочих станцій ми будемо задавати за допомогою протоколу DHCP.

Також в мережі нам необхідно налаштувати протокол маршрутизації OSPF. Саме OSPF було обрано протоколом маршрутизації для даної мережі, оскільки він має багато переваг. Основна перевага протоколу маршрутизації стану, такого як OSPF, полягає в тому, що повне знання топології дозволяє маршрутизаторам обчислювати маршрути, що задовольняють певні критерії, швидше ніж інші протоколи маршрутизації. Це може бути корисно для цілей організації трафіку, коли маршрути можуть бути обмежені відповідно до конкретних вимог щодо якості обслуговування. Основним недоліком протоколу маршрутизації є те, що він погано масштабується, оскільки в домен маршрутизації додається більше маршрутизаторів. Збільшення кількості маршрутизаторів збільшує розмір і частоту оновлень топології, а також час, необхідний для розрахунку наскрізних маршрутів.

Далі нам необхідно буде налаштувати мережевий протокол SSH. Даний протокол використовується для віддаленого управління операційними системами та передачею файлів. Ключова особливість замикається в тому, що SSH шифрує трафік, робить підключення безпечними. Аббревіатура розшифровується, як Secure Shell.

З протоколом SSH необхідно налаштувати ключ шифрування RSA. Система RSA використовується для захисту програмного забезпечення. Також вона використовується у відкритій системі шифрування PGP та інших системах

шифрування у відношенні з симметричними алгоритмами. Найбільш популярним використанням у даний час є змішаний алгоритм шифрування, у якому початком шифрування є сеансовий ключ, а потім вже з його допомогою шифруються повідомлення симметричними системами. Після завершення сеансу сеансовий ключ, як правило, знищується.

В нашій мережі необхідно налаштувати технологію NAT. Трансляція мережевих адрес (NAT) призначена для збереження IP-адреси. Вона дозволяє приватним IP-мережам, які використовують незареєстровані IP-адреси, підключатися до Інтернету. NAT працює на маршрутизаторі, як правило, з'єднуючи дві мережі разом, і переробляє приватні (не унікальні в глобальному масштабі) адреси у внутрішніх мережах в юридичні адреси, перш ніж пакети будуть перероблені в іншій мережі.

У рамках цієї можливості NAT може бути налаштований на оголошення лише однієї адреси для всієї мережі зовнішнього світу. Це забезпечує додаткову безпеку, ефективно приховуючи за цією адресою всю внутрішню мережу. NAT пропонує подвійні функції безпеки та збереження адреси та, як правило, реалізується в середовищі віддаленого доступу. По суті, NAT дозволяє одному пристрою, наприклад, маршрутизатору, діяти як агент між Інтернетом (або загальнодоступною мережею) та локальною мережею (або приватною мережею).

Для serial інтерфейсів необхідно визначити яку роль буде мати кожен з маршрутизаторів. Це буде залежати від serial кабелю, яким ми будемо підключати маршрутизатори – один кінець використовується для підключення до DCE, а інший до DTE. DCE і DTE – відповідно Data Circuit-terminating Equipment і Data Terminal Equipment – старі терміни з галузі зв'язку, що позначають кінцеве обладнання провайдера (DCE) і клієнта (DTE). DCE-роль зазвичай виконує кабельний модем, який знаходиться на кінці лінії провайдера і знає, як представляти / передавати дані в операторську мережу. Для клієнта

же DCE надає якийсь стандартний стик. Завдяки цьому виділені лінії можуть змінюватися в плані технологій, а від клієнтського маршрутизатора-DTE до операторського модему-DCE буде один і той же кабель. Тобто DCE – це проміжний пристрій зв'язку, який не створює трафік, а лише передає його далі, а DTE – кінцевий пристрій, який через найближчий DCE-пристрій обмінюється трафіком з віддаленим DTE.

Дуже важливо мати правильно налаштований час в нашій мережі. Для автоматичної установки годин мережевого пристрою найкраще використовувати протокол NTP. NTP – це дуже важливий етап налаштування часу, так як найменше неспівпадіння часу може привести до поганих наслідків. Даний мережевий протокол синхронізує внутрішній час, використовуючи NTP-сервер для налаштування точного часу на маршрутизаторі.

В кінці налаштуємо технології SPAN та RSPAN. Механізми SPAN (Switch Port Analyzer) і RSPAN (Remote Switch Port Analyzer) використовуються в обладнанні Cisco Systems. Дані технології віддзеркалення трафіку, дозволяють налаштувати комутатор так, щоб всі пакети, що приходять на один порт або групу портів комутатора, дублювалися на іншому, з метою їх подальшого аналізу і моніторингу. Технологія SPAN – локальне віддзеркалення, яке використовується для копіювання трафіку з порту або vlan на інший порт цього ж комутатора. В свою чергу, технологія RSPAN – віддалене віддзеркалення, яке використовується для копіювання трафіку з порту або vlan на порт віддаленого комутатора. Дзеркальне відображення портів слід налаштувати як засіб отримання мережевого трафіку для кожного комутатора мережі, який необхідно відстежувати. В нашому випадку, ліву частину мережі ми будемо налаштовувати за допомогою технології SPAN, а праву частину за допомогою – RSPAN.

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ СИСТЕМИ ДЗЕРКАЛЮВАННЯ ТРАФІКУ

3.1. Вибір обладнання для побудови комп'ютерної мережі організації

При виборі моделі маршрутизатора необхідно враховувати як він маршрутизує пакети в складній мережі з різними видами топологій. Маршрутизатор повинен містити достатню кількість портів, забезпечувати легке розширення мережі, забезпечувати необхідну швидкість передачі даних та швидкість їх обробки.

Для мережі було використано наступні прилади:

- Маршрутизатор Cisco 2901;
- Комутатор Cisco 2960-24TT;
- Сервер Cisco;
- Робоча станція;
- Sniffer.

Маршрутизатор CISCO 2901 від компанії Cisco (рисунок 3.1) – модульний роутер з двома 10/100/1000 Gigabit Ethernet портами, 512 Mb DRAM (max: 2 Gb), 256 Mb Flash (max: 4 Gb), 4 слоти EHWIC, 2 DSP, 1 ISM, АС блок живлення.



Рисунок 3.1 – Маршрутизатор Cisco 2901

Маршрутизатор Cisco ISR серії 2900 розроблено для малих і середніх підприємств, яким потрібні сучасні технологічні рішення, що забезпечують надійне високопродуктивне підключення до мережі Інтернет. Серія

маршрутизаторів Cisco ISR G2 2900 представлена 4 фіксованими і декількома розширеними моделями, у даній серії маршрутизаторів є велика кількість різних інтерфейсів і модулів.

Маршрутизатор з інтегрованими сервісами Cisco ISR серії 2900 надає користувачеві безліч переваг за рахунок кращих на ринку функцій безпеки, комутації, уніфікованих комунікацій, відео, бездротового зв'язку і прикладних сервісів. Вбудовані служби маршрутизаторів серії Cisco 2900 зменшують початкові витрати, розділяючи програмне забезпечення від апаратних складових опційних службових модулів. Універсальний образ IOS, здатний включати весь багатий набір можливостей IOS і дозволяє швидко розширювати нові служби. Серія Cisco 2900 зменшує витрати на розширення і підвищує гнучкість системи та має значне підвищення продуктивності в порівнянні з ISR попередніх поколінь.

Комутатори Cisco Catalyst 2960 серії (рисунок 3.2) є лінійкою комутаторів з фіксованою конфігурацією і портами Fast Ethernet і Gigabit Ethernet, що мають розширені LAN сервіси для підприємств початкового рівня і мереж віддаленого офісу. Комутатори Cisco Catalyst 2960 підтримують передачу голосу, даних і відео, а також безпечний доступ. Крім того, вони надають управління, яке масштабується в міру зміни потреб нашого бізнесу.



Рисунок 3.2 – Комутатор Cisco Catalyst 2960

Комутатори Cisco Catalyst 2960 підтримують Intelligent features (створення складних списків управління доступом, розширена безпека), комбіновані гігабітні аплінки (мідний 10/100 / 1000BASE-T Ethernet або SFP-модуль для переходу в інше середовище – Cisco 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX, 100BASE-FX, 100BASE-LX, CWDM SFP). Також, пристрої Catalyst 2960 підтримують QoS, покроковий Rate Limiting, ACL (на базі MAC або IP адрес, портів UDP / TCP) і multicast services, можливість регулювати швидкість передачі на кожному порту з кроком 64 Кбіт, Link Aggregation для організації більш швидкісних з'єднань між комутаторами і серверами, можливість організації транкових з'єднань на кожному порту за допомогою тегів 802.1q, до 255 VLAN на комутатор, до 4000 VLAN ID і управління через Cisco Network Assistant (підтримує широкий спектр моделей комутаторів від Cisco Catalyst 2960 до Cisco Catalyst 4506).

Прошивка комутаторів Cisco Catalyst 2960 випускається в образах LAN Base і Lan Lite Image. LAN Base має більш широкий функціонал, включаючи поліпшену безпеку (ACLs), DHCP Snooping і додаткові функції по контролю доступу – Web authentication і розширення 802.1x, додаткові можливості установок якості обслуговування QoS, підтримка надлишкового харчування RPS і великої кількості SFP-портів. Функції Flex Links і Link State Tracking, збільшена кількість підтримуваних VLANs (до 256), IPv6 Host, MLD Snooping, LLDP-MED, RSPAN, MVR, DHCP Option 82, і IP SLA (responder) та інше.

Комутатор дозволяє нам налаштувати точку доступу як мережевий "сніффер", який фіксує та пересилає усі пакети на певному каналі на віддалену робочу станцію, на якій запущено програмне забезпечення аналізатора пакетів. Ці пакети містять інформацію про позначки часу, потужність сигналу, розміри пакетів тощо.

Сніффери дозволяють контролювати та реєструвати мережеву активність та виявляти проблеми у мережі.

3.2. Налаштування комп'ютерної мережі та підсистеми дзеркалювання трафіку

Налаштування мережі розпочнемо з базового налаштування маршрутизаторів. Для початку відключимо на маршрутизаторі функції пошуку по DNS, які в багатьох випадках не потрібні для виконання стандартних операцій. Далі в режимі глобальної конфігурації ввійдемо в режим конфігурації рядка для консолі і скористаємось командою `exec-timeout` для того, щоб при бездіяльності користувача протягом деякого часу стався процес розлогінування. Команда `logging synchronous` допоможе нам заборонити вивід будь-яких консольних повідомлень, які в свою чергу можуть перервати введення команд в командному режимі, рисунок 3.3.

```
R_1_16_1(config)#no ip domain-lookup
R_1_16_1(config)#line console 0
R_1_16_1(config-line)#logg syn
R_1_16_1(config-line)#exec-timeout 0 0
R_1_16_1(config-line)#exit
R_1_16_1(config)#exit
R_1_16_1#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.3 – Базове налаштування маршрутизатора

На комутаторах також налаштуємо вище згадані команди, а також IP-адресацію на VLAN, рисунок 3.4.

```
SW_1_16_4#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW_1_16_4(config)#no ip domain-lookup
SW_1_16_4(config)#line console 0
SW_1_16_4(config-line)#logg syn
SW_1_16_4(config-line)#exec-timeout 0 0
SW_1_16_4(config-line)#int vlan 1
SW_1_16_4(config-if)#ip add 196.1.16.5 255.255.255.0
SW_1_16_4(config-if)#no shutdown

SW_1_16_4(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
to up

SW_1_16_4(config-if)#exit
SW_1_16_4(config)#exit
SW_1_16_4#
%SYS-5-CONFIG_I: Configured from console by console

SW_1_16_4#copy run
SW_1_16_4#copy running-config sta
SW_1_16_4#copy running-config startup-config
Destination filename [startup-config]?
```

Рисунок 3.4 – Базове налаштування комутатора і IP-адресації на ньому

Далі необхідно налаштувати IP-адреси на відповідних інтерфейсах для маршрутизаторів усієї мережі, рисунок 3.5.

```
R_1_16_1(config)#int gig0/0
R_1_16_1(config-if)#ip add 191.1.16.1 255.255.255.248
R_1_16_1(config-if)#no shutdown

R_1_16_1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
exit
R_1_16_1(config)#int se0/0/0
R_1_16_1(config-if)#ip add 191.1.16.9 255.255.255.252
R_1_16_1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R_1_16_1(config-if)#exit
R_1_16_1(config)#int se0/0/1
R_1_16_1(config-if)#ip add 191.1.16.13 255.255.255.252
R_1_16_1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
R_1_16_1(config-if)#exit
```

Рисунок 3.5 – Налаштування IP-адресації на маршрутизаторі

За допомогою команд статичного NAT задаємо внутрішній і зовнішній інтерфейси. Внутрішній інтерфейс з'єднує маршрутизатор з внутрішньою частиною мережі, а зовнішній – з'єднує маршрутизатор з зовнішньою частиною мережі. Також необхідно за допомогою команди `ip nat inside source static` задати перетворення адрес. У нашому випадку внутрішня адреса 191.1.16.1 завжди буде перетворюватись на зовнішню адресу 190.1.16.0, рисунок 3.6.

```
R_1_16_1(config)#ip nat inside source static 191.1.16.1 190.1.16.0
R_1_16_1(config)#int gig0/0
R_1_16_1(config-if)#ip nat inside
R_1_16_1(config-if)#exit
R_1_16_1(config)#int gig0/1
R_1_16_1(config-if)#ip nat outside
R_1_16_1(config-if)#exit
R_1_16_1(config)#exit
R_1_16_1#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.6 – Налаштування технології NAT

Для коректної роботи протокола динамічної конфігурації DHCP, нам необхідно виключити деякі адреси підмережі з діапазону адрес, які будуть назначатися робочим станціям. Це потрібно для того, щоб деякі IP-адреси з пулу, які призначені мережевим пристроям, таким як маршрутизатори, сервери чи комутатори, яким потрібні статичні адреси, не були призначені іншим пристроям мережі. Також для зручності задамо назву пулу, яка буде відповідати назві підмережі. Далі необхідно вказати адресу підмережі, шлюзу за замовчуванням і адресу dns-серверу, рисунок 3.7.

```
R_1_16_5(config)#ip dhcp excluded-address 197.1.16.1
R_1_16_5(config)#ip dhcp pool Network_K
R_1_16_5(dhcp-config)#network 197.1.16.0 255.255.255.128
R_1_16_5(dhcp-config)#default-router 197.1.16.1
R_1_16_5(dhcp-config)#dns-server 8.8.8.8
R_1_16_5(dhcp-config)#exit
R_1_16_5(config)#ip dhcp excluded-address 197.1.16.129
R_1_16_5(config)#ip dhcp pool Network_L
R_1_16_5(dhcp-config)#network 197.1.16.128 255.255.255.128
R_1_16_5(dhcp-config)#default-router 197.1.16.129
R_1_16_5(dhcp-config)#dns-server 8.8.8.8
R_1_16_5(dhcp-config)#exit
R_1_16_5(config)#exit
```

Рисунок 3.7 – Налаштування протокола динамічної конфігурації DHCP

На кожному маршрутизаторі мережі необхідно налаштувати протокол маршрутизації OSPF (рисунок 3.8). Для початку, необхідно створити процес OSPF командою `router ospf` і описати всі мережі, що входять в процес маршрутизації за допомогою команди `network`. Коли ми вказуємо деяку мережу, це призводить до двох наслідків:

- Інформація про цю мережі починає передаватися іншим маршрутизаторам (за умови, що на маршрутизаторі є робочий інтерфейс в даній мережі);
- Через інтерфейс, що знаходиться в цій мережі маршрутизатор починає спілкуватися з сусідами.

```

R_1_16_5(config)#router ospf 1
R_1_16_5(config-router)#network 192.1.16.0 0.0.0.7 area 0
R_1_16_5(config-router)#network 194.1.16.0 0.0.0.3 area 0
R_1_16_5(config-router)#network 194.1.16.4 0.0.0.3 area 0
R_1_16_5(config-router)#network 197.1.16.0 0.0.0.127 area 0
R_1_16_5(config-router)#network 197.1.16.128 0.0.0.127 area 0
R_1_16_5(config-router)#exit
R_1_16_5(config)#exit
R_1_16_5#
%SYS-5-CONFIG_I: Configured from console by console

```

Рисунок 3.8 – Налаштування протокола маршрутизації OSPF

Для можливості віддаленого підключення пристроїв мережі, необхідно створити на маршрутизаторі нового користувача, пароль і надати йому рівень привілеїв. Також необхідно назначити локальний пароль доступу в привілейований режим консолі в відкритому вигляді і зберігти в зашифрованому вигляді для користувачів всіх рівнів привілеїв. Для того, щоб увімкнути доступ по SSH, спочатку необхідно прописати домен і згенерувати ключ RSA. Далі вмикаємо доступ до консолі і отримуємо можливість підключення по SSH, рисунок 3.9.

```

R_1_16_3(config)#username admin privilege 15 secret cisco
R_1_16_3(config)#username user privilege 1 secret cisco
R_1_16_3(config)#enable secret cisco
R_1_16_3(config)#ip domain-name cisco.net
R_1_16_3(config)#crypto key generate rsa
The name for the keys will be: R_1_16_3.cisco.net
Choose the size of the key modulus in the range of 360 to 2048
for your
  General Purpose Keys. Choosing a key modulus greater than 512
may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK]

R_1_16_3(config)#ip ssh version 2
*Mar 1 0:3:59.251: %SSH-5-ENABLED: SSH 1.99 has been enabled
R_1_16_3(config)#ip ssh time-out 60
R_1_16_3(config)#ip ssh authentication-retries 5
R_1_16_3(config)#line vty 0 4
R_1_16_3(config-line)#login local
R_1_16_3(config-line)#transport input ssh
R_1_16_3(config-line)#transport output ssh
R_1_16_3(config-line)#logging synchronous
R_1_16_3(config-line)#exit
R_1_16_3(config)#exit

```

Рисунок 3.9 – Налаштування мережевого протокола SSH

На маршрутизаторі налаштуємо можливість відображення локального часу в логах в пам'яті пристрою. Далі налаштуємо ntp-клієнта, увімкнемо аутентифікацію NTP і вкажемо дійсний ключ для данної аутентифікації, рисунок 3.10.

```
R_1_16_1(config)#service timestamps log datetime msec
R_1_16_1(config)#service timestamps debug datetime msec
R_1_16_1(config)#clock timezone EET 2
R_1_16_1(config)#ntp server 190.1.16.2 key 250999
R_1_16_1(config)#ntp authenticate
R_1_16_1(config)#ntp authentication-key 250999 md5 cisco
R_1_16_1(config)#ntp trusted-key 250999
R_1_16_1(config)#ntp update-calendar
R_1_16_1(config)#exit
R_1_16_1#
*Mar 01, 03:45:49.4545: SYS-5-CONFIG_I: Configured from console
by console
```

Рисунок 3.10 – Налаштування мережевого протоколу часу NTP на маршрутизаторі

На рисунку 3.11 показано налаштування протоколу часу NTP на сервері мережі.

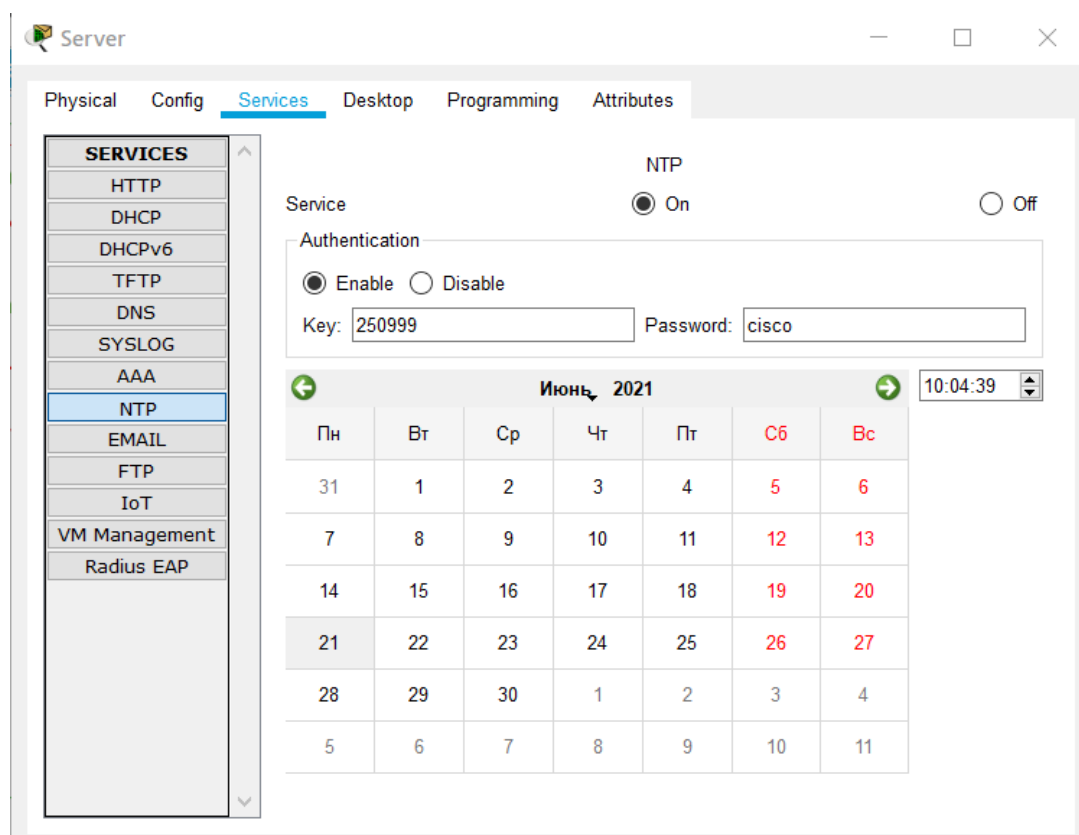


Рисунок 3.11 – Налаштування мережевого протоколу часу NTP на сервері

В рамках SPAN сесії захоплення (копіювання) мережевого трафіку відбувається з порту джерела (source port) і відправляється на порт призначення (destination port). На рисунку 3.12 показано створення сесії 1, в якій портами джерелами виступають – fa0/2, fa0/3, fa0/4 (які виходять до робочих станцій), портом призначення виступає порт fa0/1.

```
SW_1_16_7#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW_1_16_7(config)#monitor session 1 source int fa0/2
SW_1_16_7(config)#monitor session 1 source int fa0/3
SW_1_16_7(config)#monitor session 1 source int fa0/4
SW_1_16_7(config)#monitor session 1 destination int fa0/1
SW_1_16_7(config)#exit
SW_1_16_7#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.12 – Налаштування технології SPAN на маршрутизаторі

Технологія RSPAN є покращеною версією технології SPAN, вона дасть змогу зеркалювати трафік між комутаторами по L2 через транкові порти. Копія трафіку буде відправлятися у віддалений VLAN, у нашому випадку це VLAN 50, поки не буде прийнята на комутаторі призначення. Тому для початку, нам необхідно визначити, який комутатор буде виконувати роль джерела, а який роль комутатора призначення.

Спочатку розглянемо налаштування технології RSPAN на комутаторі джерелі, рисунок 3.13.

```
SW_1_16_8#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW_1_16_8(config)#vlan 50
SW_1_16_8(config-vlan)#remote-span
SW_1_16_8(config-vlan)#name Remote_SPAN
SW_1_16_8(config-vlan)#
SW_1_16_8(config-vlan)#do show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
50 Remote_SPAN	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

```
SW_1_16_8(config-vlan)#
```

Рисунок 3.13 – Налаштування технології RSPAN на комутаторі джерелі

Створюємо Remote VLAN на комутаторі джерелі (пристрій на який будемо передавати дані з source порту) і перевіряємо активність нашого щойно створеного VLAN. За допомогою команди monitor активуємо RSPAN-моніторинг і створюємо сесію, до якої прив'язуємо порт-джерело і VLAN-приймач, рисунок 3.14.

```
SW_1_16_8(config)#monitor session 1 source int fa0/3
SW_1_16_8(config)#monitor session 1 source int fa0/4
SW_1_16_8(config)#monitor session 1 source int fa0/5
SW_1_16_8(config)#monitor session 1 destination remote vlan 50 reflector-port
fastEthernet 0/24
```

Рисунок 3.14 – Налаштування технології RSPAN на комутаторі джерелі

Далі розглянемо налаштування технології RSPAN на комутаторі одержувачі рисунок 3.15. Аналогічно до попередніх налаштувань створюємо Remote VLAN на комутаторі одержувачі.

```
SW_1_16_9(config)#vlan 50
SW_1_16_9(config-vlan)#remote-span
SW_1_16_9(config-vlan)#name Remote-SPAN
SW_1_16_9(config-vlan)#do show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
50	Remote-SPAN	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

Рисунок 3.15 – Налаштування технології RSPAN на комутаторі одержувачі

Відмінність в налаштуваннях між комутаторами джерело і одержувач є те, що на комутаторі одержувачі портом джерелом виступає VLAN-приймач комутатора джерела, а портом отримувачем виступає порт, який виходить до сніффера, рисунок 3.16.

```
SW_1_16_9(config-vlan)#exit
SW_1_16_9(config)#
SW_1_16_9(config)#monitor session 1 destination int fa0/10
SW_1_16_9(config)#monitor session 1 source remote vlan 50
SW_1_16_9(config)#exit
SW_1_16_9#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.16 – Налаштування технології RSPAN на комутаторі одержувачі

3.3. Тестування роботи підсистеми дзеркалювання трафіку

Для перевірки зв'язку між сусідніми пристроями необхідно пропінгувати пристрої однієї підмережі, рисунок 3.17.

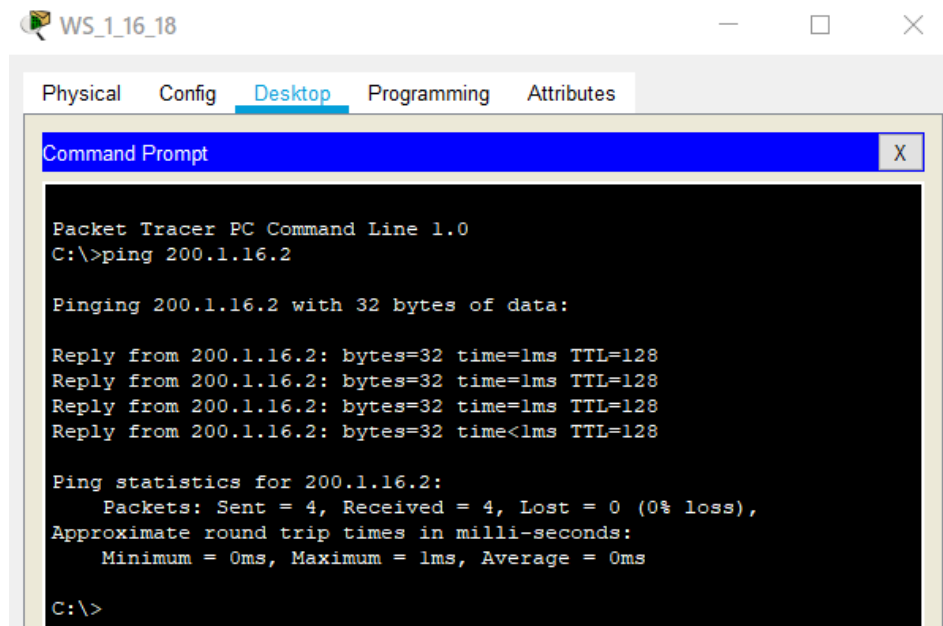


Рисунок 3.17 – Перевірка зв'язку між сусідніми пристроями

Після налаштування протокола маршрутизації OSPF, між вузлами віддалених підмереж має з'явитися зв'язок, тому перевіримо це за допомогою команди ping, рисунок 3.18.

```
R_1_16_1#ping 197.1.16.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 197.1.16.3, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R_1_16_1#ping 198.1.16.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.1.16.4, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

R_1_16_1#ping 199.1.16.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 199.1.16.3, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

R_1_16_1#ping 200.1.16.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.1.16.3, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

Рисунок 3.18 – Перевірка зв'язку між пристроями віддалених підмереж

Командою для перевірки роботи NAT є команда show ip nat translations. Ця команда показує активні трансляції NAT, рисунок 3.19.

```
R_1_16_6>en
Password:
R_1_16_6#show ip nat translations
Pro  Inside global      Inside local      Outside local
Outside global
---  192.1.16.0           198.1.16.1       ---              ---
```

Рисунок 3.19 – Перевірка налаштувань технології NAT

На рисунку 3.20 бачимо, що динамічне призначення IP-адреси для робочої станції пройшло успішно. Тому налаштований нами протокол динамічної конфігурації працює коректно.

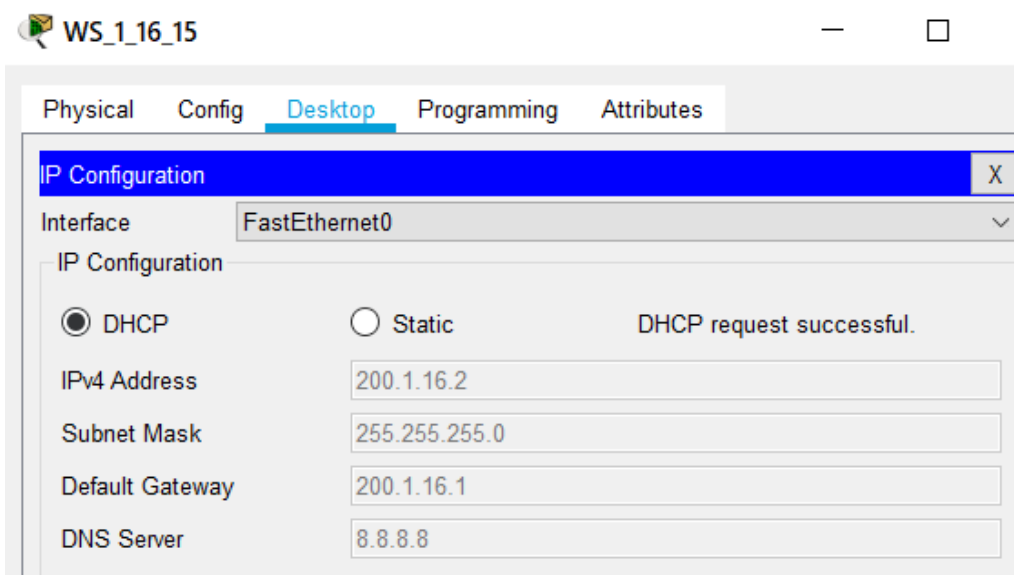


Рисунок 3.20 – Перевірка налаштування протоколу динамічної конфігурації DHCP

Для перевірки роботи мережевого протокола SSH нам потрібно підключитись до будь-якого пристрою мережі з командного рядка будь-якої робочої станції. У нашому випадку, ми будемо підключатися до маршрутизатора R_1_16_1 з робочої станції WS_1_16_5. Для цього нам необхідно вказати в командному дяку робочої станції протокол віддаленого

доступу SSH, ім'я користувача, створеного на маршрутизаторі і IP-адресу маршрутизатора, рисунок 3.21.

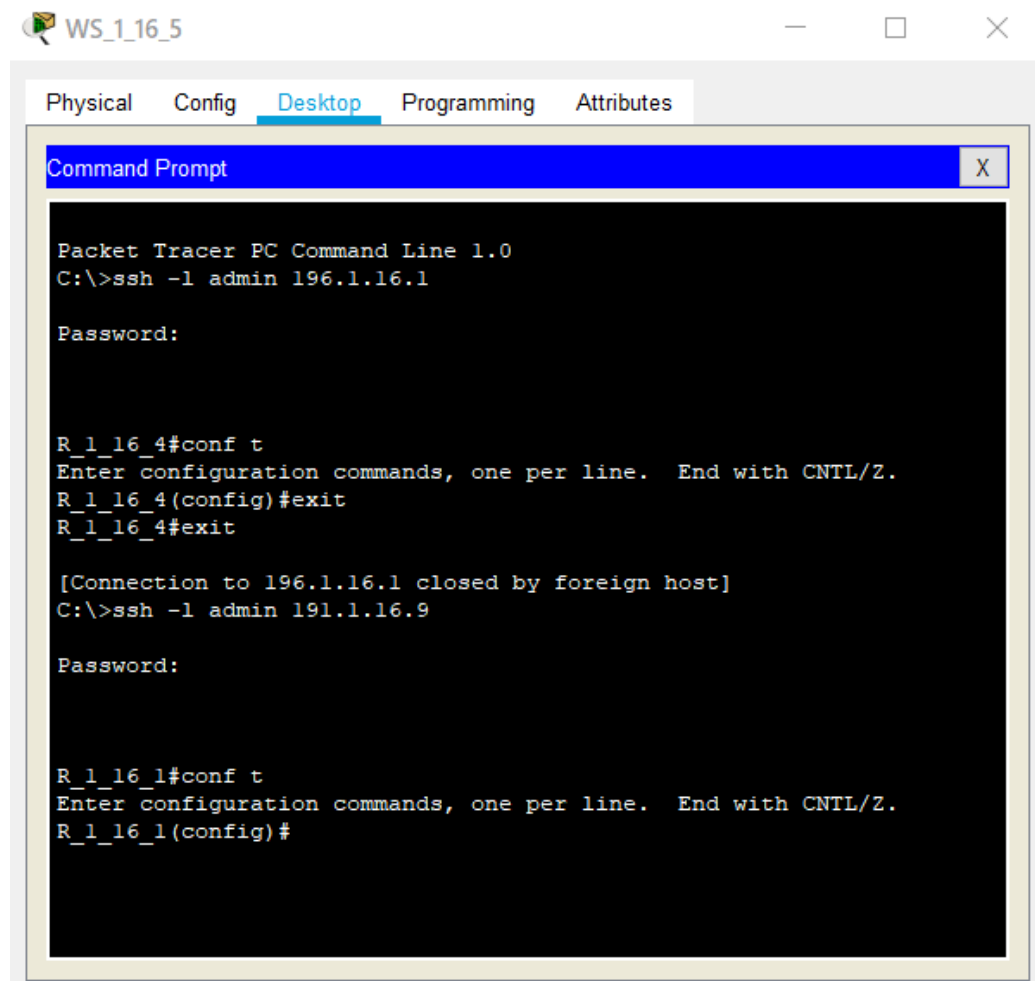


Рисунок 3.21 – Перевірка налаштування мережевого протокола SSH

За допомогою команди `show monitor` ми можемо перевірити коректність налаштування технології дзеркалювання SPAN, а саме, які порти виступають портами призначення і портами джерелами, рисунок 3.22.

```

SW_1_16_7#show monitor
Session 1
-----
Type                : Local Session
Description          : -
Source Ports         :
    Both             : Fa0/2, Fa0/3, Fa0/4
Destination Ports    : Fa0/1
    Encapsulation     : Native
    Ingress           : Disabled
  
```

Рисунок 3.22 – Перевірка налаштування технології SPAN

За допомогою сніффера ми можемо проконтролювати та зареєструвати мережеву активність та виявляти проблеми у мережі. У нашому випадку, ми пропінгуємо одну з робочих станцій мережі з будь-якого маршрутизатора і за допомогою сніффера перехопити трафік, а саме трафік пов'язаний з протоколом ICMP, який в свою чергу є протоколом на якому заснована утиліта ping, рисунок 3.23.

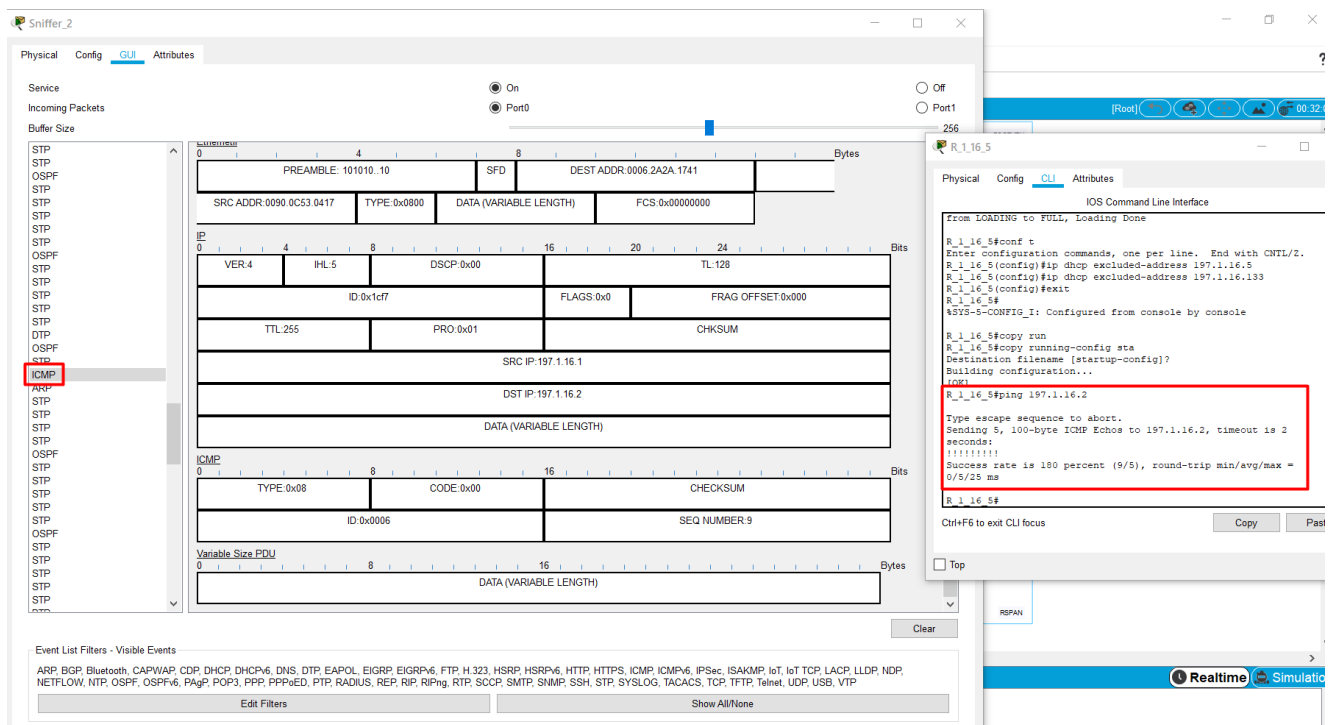


Рисунок 3.23 – Перевірка налаштування технології SPAN

Аналогічно до технології дзеркалювання SPAN перевіряємо роботу технології RSPAN, рисунок 3.24 та рисунок 3.25.

```
SW_1_16_8#show monitor
Session 1
-----
Type                : Remote Destination Session
Description          : -
Source Ports         :
Both                 : Fa0/3, Fa0/4, Fa0/5
Dest RSPAN VLAN      : 50
```

Рисунок 3.24 – Перевірка налаштування технології RSPAN на комутаторі джерелі

```

SW_1_16_9#show monitor
Session 1
-----
Type                : Remote Source Session
Description         : -
Source RSPAN VLAN   : 50
Destination Ports   : Fa0/10
Encapsulation       : Native
Ingress             : Disabled

```

Рисунок 3.25 – Перевірка налаштування технології RSPAN на комутаторі отримувачі

Для технології дзеркалювання RSPAN також за допомогою команди ping та sniffера підключеного до комутатора отримувача перевіряємо правильність налаштування технології, рисунок 3.26. У нашому випадку, ми пінгуємо робочу станцію, яка підключена до комутатора джерела з маршрутизатора рівня ядра R_1_16_1.

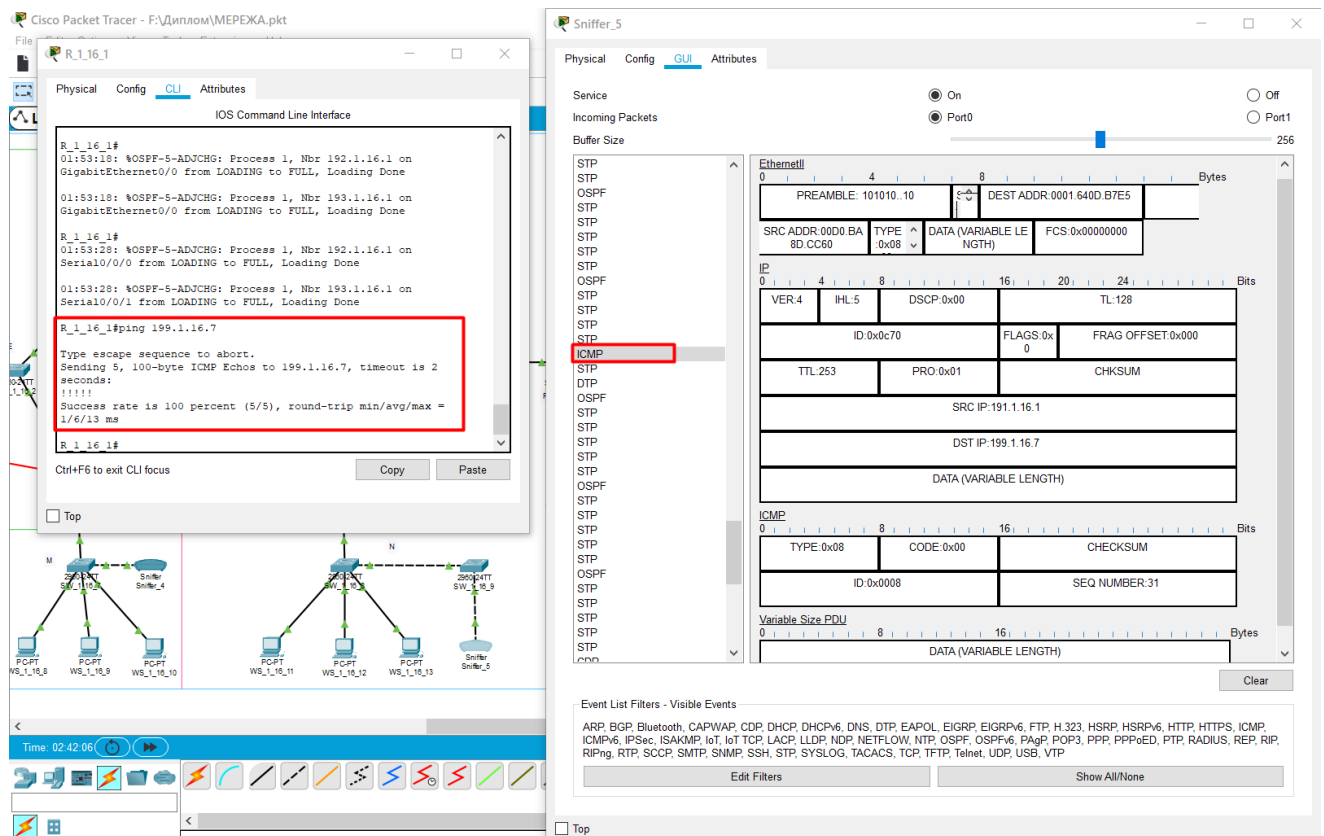


Рисунок 3.26 – Перевірка налаштування технології RSPAN

По результатам перевірки налаштувань мережі, можемо зробити висновок, що всі налаштування виконанні правильно. Налаштовані протоколи і технології працюють коректно.

ВИСНОВКИ

Технології дзеркалювання портів широко використовуються в комп'ютерних мережах для того, щоб аналізувати, який трафік передається через мережу.

Дзеркальне відображення трафіку має свої переваги такі, як: спрощена робота, яка полягає в дзеркалюванні будь-якого діапазону VPC-трафіку без необхідності управління його пакетами; покращена безпека, яка полягає у захопленні пакетів через еластичний мережевий інтерфейс, який неможливо відключити або підробити з простору користувача; розширені можливості моніторингу, які дозволяють надсилати дзеркальний трафік на будь-який захисний пристрій.

Не дивлячись на переваги дзеркального відображення трафіку, він має ряд недоліків таких, як обмежена кількість дзеркальних інтерфейсів, навантаження на комутатор, блокування передачі на дзеркальний порт трафіку, який містить бітові помилки і т.д.

Технологія SPAN є ефективною і високопродуктивною системою моніторингу трафіку. Вона направляє або віддзеркалює трафік з вихідного порту або VLAN на порт призначення. Дана технологія використовується, для усунення проблем з підключенням і розрахунку використання і продуктивності мережі.

Remote SPAN (RSPAN) схожий на SPAN, але підтримує вихідні порти, вихідні VLAN і цільові порти на різних комутаторах, які забезпечують віддалений моніторинг трафіку з вихідних портів, розподілених по декількох комутаторах, і дозволяють цільовим призначенням централізувати пристрої захоплення мережі. Кожен сеанс RSPAN передає трафік SPAN через виділену користувачем RSPAN VLAN на всіх, що беруть участь комутаторах.

Для відслідковування дзеркалювання трафіку є можливість використання пристроїв, таких як сніфери. Сніфери дозволяють контролювати та реєструвати мережеву активність та виявляти проблеми у мережі.

В даній роботі нами було спроектовано топологію комп'ютерної мережі, яка символічно розділена на дві частини, кожна з яких відповідає технологіям SPAN та RSPAN. Було розглянуто підмережі, пристрої, використані у них, з'єднання між пристроями, а також було визначено основні складові підмережі. Ми визначили кількість підмереж та їх призначення. Також було розроблено адресацію даної комп'ютерної мережі.

Таким чином у даній роботі було виконано наступні завдання:

- Аналіз процесів технологій дзеркалювання трафіку;
- Аналіз та налаштування технологій дзеркалювання трафіку;
- Дослідження переваг та недоліків технологій дзеркалювання трафіку;
- Визначення алгоритму побудови комп'ютерної мережі;
- Розробка топології комп'ютерної мережі;
- Логічне проектування мережі;
- Розробка IP-адресації підмереж;
- Обґрунтування вибору кабелів, інтерфейсів, обладнання та ПЗ;
- Налаштування мережі;
- Перевірка працездатності комп'ютерної мережі.

У висновку виконання випускної кваліфікаційної роботи бакалавра, ми отримали коректно працюючу мережу, яку в майбутньому можна використати, як план чи приклад для мережі організації чи підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Traffic mirroring // Amazon Virtual Private Cloud. [2019-2021]. URL: https://docs.amazonaws.cn/en_us/vpc/latest/mirroring/vpc-tm.pdf#traffic-mirroring-how-it-works.
2. Configuring Traffic Mirroring // Cisco Web Site. URL: https://www.cisco.com/c/en/us/td/docs/iosxr/ncs5000/interfaces/65x/b-interfaces-hardware-component-cg-ncs5000-65x/b-interfaces-hardware-component-cg-ncs5000-65x_chapter_01010.pdf.
3. Understanding Network TAPs // Gigamon. [2019-2020]. URL: <https://www.gigamon.com/content/dam/resource-library/english/white-paper/wp-network-taps-first-step-to-visibility.pdf>.
4. Port Mirroring and Analyzers // Juniper. [2021]. URL: <https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/topics/topic-map/port-mirroring-and-analyzers.html#d407e261>.
5. Port Mirroring // Comms Express. [2021]. URL: <https://www.comms-express.com/infozone/article/port-mirroring/>.
6. SPAN, RSPAN, ERSPAN // Cisco. [2020]. URL: <https://learningnetwork.cisco.com/s/article/span-rspan-erspan>.
7. Understanding SPAN, RSPAN and ERSPAN // Cisco Community. [2013-2019]. URL: <https://community.cisco.com/t5/networking-documents/understanding-span-rspan-and-erspan/ta-p/3144951>.
8. Catalyst Switched Port Analyzer (SPAN) // Cisco. [2019]. URL: <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41.html#anc0/>.
9. Interface and Hardware Component Configuration Guide for Cisco NCS 6000 Series Routers, IOS XR Release 6.3.x // Cisco. [2020]. URL: <https://www.cisco.com/c/en/us/td/docs/routers/ncs6000/software/ncs6k-r6-3/interfaces/configuration/guide/b-interfaces-hardware-component-cg-ncs6000-63x/m-configuring-traffic-mirroring-ncs6000.html>.

10. Use traffic mirroring // Alibaba Cloud. [2021]. URL: <https://www.alibabacloud.com/help/doc-detail/207514.htm>.
11. Port Mirroring Explained // FS Community. [2019]. URL: <https://community.fs.com/ru/blog/port-mirroring-explained-basis-configuration-and-fa-qs.html>.
12. Catalyst 3750-X and 3560-X Switch Software Configuration Guide, Release 12.2(55)SE // Cisco. [2018]. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swspan.html.
13. Type of Network Topology: Bus, Ring, Star, Mesh, Tree, P2P, Hybrid // Guru. URL: <https://www.guru99.com/type-of-network-topology.html>.
14. Network topologies, protocols and layers // BBC. [2018]. URL: <https://www.bbc.co.uk/bitesize/guides/zr3yb82/revision/3>.
15. Cisco Catalyst 9800 Series Wireless Controller Software // Cisco. [2021]. URL: https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/configuration/b_wl_16_10_cg/sniffer-mode.html#reference_A2586939DD7A4C59AA6433BDC2DF2C9E.
16. IP Addressing and Subnetting for New Users // Cisco. [2021]. URL: <https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html>.
17. OSPF // Cisco Learning. [2016-2017]. URL: <https://ciscolearning.ru/cisco-router/ospf/>.
18. Network Address Translation (NAT) // Cisco. [2020]. URL: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html>.
19. Настройка зеркального отображения портов // Microsoft. [2018]. URL: <https://docs.microsoft.com/ru-ru/advanced-threat-analytics/configure-port-mirroring>.

20. Catalyst 2960 Switch Software Configuration Guide // Cisco. URL:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_37_se/configuration/guide/scg/swspan.html.
21. Introduction to RSPAN, SPAN and ERSPAN // IPWITHEASE. URL:
<https://ipwithease.com/introduction-to-span-and-rspan/>.
22. SPAN/RSPAN — НАСТРОЙКА // Admindoc. URL:
<http://admindoc.ru/788/spanrspan/>.
23. Configuring SPAN and RSPAN // Cisco. [2007]. URL:
<https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/span.html#wp1021995>.
24. Configure Remote Switch Port Analyzer (RSPAN) Settings on the Network // Cisco. [2020]. URL:
<https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-350-series-managed-switches/smb5327-configure-remote-switch-port-analyzer-rspan-settings-on-the.html>.
25. Remote SPAN Configuration on Packet Tracer // IPCisco. URL:
<https://ipcisco.com/lesson/remote-span-configuration-on-packet-tracer/>.

ДОДАТКИ

					КІК.КВ.Б-125-16-ПЗ	61

Параметри інтерфейсів пристроїв

Таблиця А.1 – Параметри інтерфейсів пристроїв

Пристрій	Інтерфейс	Підключення до пристрою	Підключення до інтерф.
Маршрутизатор R_1_16_1	Se0/0/0	Маршрутизатор R_1_16_2	Se0/0/0
	Se0/0/1	Маршрутизатор R_1_16_3	Se0/0/1
	Gig0/0	Комутатор SW_1_16_1	Gig0/1
	Gig0/1	Сервер Server	Fa0
Маршрутизатор R_1_16_2	Se0/0/0	Маршрутизатор R_1_16_1	Se0/0/0
	Se0/0/1	Маршрутизатор R_1_16_3	Se0/0/0
	Gig0/0	Комутатор SW_1_16_1	Gig1/1
	Gig0/1	Комутатор SW_1_16_2	Gig0/1
Маршрутизатор R_1_16_3	Se0/0/1	Маршрутизатор R_1_16_1	Se0/0/1
	Se0/0/0	Маршрутизатор R_1_16_2	Se0/0/1
	Gig0/0	Комутатор SW_1_16_1	Gig2/1
	Gig0/1	Комутатор SW_1_16_3	Gig0/1
Маршрутизатор R_1_16_4	Se3/0	Маршрутизатор R_1_16_5	Se3/0
	Gig0/0	Комутатор SW_1_16_2	Fa0/1
	Fa1/0	Комутатор SW_1_16_4	Fa0/1
Маршрутизатор R_1_16_5	Se3/0	Маршрутизатор R_1_16_4	Se3/0
	Se4/0	Маршрутизатор R_1_16_6	Se4/0
	Gig0/0	Комутатор SW_1_16_2	Fa0/2
	Fa1/0	Комутатор SW_1_16_5	Fa0/1
	Fa2/0	Комутатор SW_1_16_6	Fa0/1
Маршрутизатор R_1_16_6	Se4/0	Маршрутизатор R_1_16_5	Se4/0
	Gig0/0	Комутатор SW_1_16_2	Fa0/3
	Fa1/0	Комутатор SW_1_16_7	Fa0/1
Маршрутизатор R_1_16_7	Se3/0	Маршрутизатор R_1_16_8	Se3/0
	Gig0/0	Комутатор SW_1_16_3	Fa0/1
	Fa1/0	Комутатор SW_1_16_8	Fa0/1
Маршрутизатор R_1_16_8	Se3/0	Маршрутизатор R_1_16_7	Se3/0
	Gig0/0	Комутатор SW_1_16_3	Fa0/2
	Fa1/0	Комутатор SW_1_16_11	Fa0/1
Комутатор SW_1_16_1	Gig0/1	Маршрутизатор R_1_16_1	Gig0/0
	Gig1/1	Маршрутизатор R_1_16_2	Gig0/0
	Gig2/1	Маршрутизатор R_1_16_3	Gig0/0
	Gig0/1	Маршрутизатор R_1_16_2	Gig0/1

Комутатор SW_1_16_2	Fa0/1	Маршрутизатор R_1_16_4	Gig0/0
	Fa0/2	Маршрутизатор R_1_16_5	Gig0/0
	Fa0/3	Маршрутизатор R_1_16_6	Gig0/0
Комутатор SW_1_16_3	Gig0/1	Маршрутизатор R_1_16_3	Gig0/1
	Fa0/1	Маршрутизатор R_1_16_7	Gig0/0
	Fa0/2	Маршрутизатор R_1_16_8	Gig0/0
Комутатор SW_1_16_4	Fa0/1	Маршрутизатор R_1_16_4	Fa1/0
	Fa0/2	Робоча станція WS_1_16_1	Fa0
	Fa0/3	Робоча станція WS_1_16_2	Fa0
	Fa0/4	Робоча станція WS_1_16_3	Fa0
	Fa0/10	Sniffer_1	Eth0
Комутатор SW_1_16_5	Fa0/1	Маршрутизатор R_1_16_5	Fa1/0
	Fa0/2	Робоча станція WS_1_16_4	Fa0
	Fa0/3	Робоча станція WS_1_16_5	Fa0
	Fa0/10	Sniffer_2	Eth0
Комутатор SW_1_16_6	Fa0/1	Маршрутизатор R_1_16_5	Fa2/0
	Fa0/2	Робоча станція WS_1_16_6	Fa0
	Fa0/3	Робоча станція WS_1_16_7	Fa0
	Fa0/10	Sniffer_3	Eth0
Комутатор SW_1_16_7	Fa0/1	Маршрутизатор R_1_16_6	Fa1/0
	Fa0/2	Робоча станція WS_1_16_8	Fa0
	Fa0/3	Робоча станція WS_1_16_9	Fa0
	Fa0/4	Робоча станція WS_1_16_10	Fa0
	Fa0/10	Sniffer_4	Eth0
Комутатор SW_1_16_8	Fa0/1	Маршрутизатор R_1_16_7	Fa1/0
	Fa0/2	Комутатор SW_1_16_9	Fa0/2
	Fa0/3	Робоча станція WS_1_16_11	Fa0
	Fa0/4	Робоча станція WS_1_16_12	Fa0
	Fa0/5	Робоча станція WS_1_16_13	Fa0
Комутатор SW_1_16_9	Fa0/2	Комутатор SW_1_16_8	Fa0/2
	Fa0/10	Sniffer_5	Eth0
Комутатор SW_1_16_10	Fa0/2	Комутатор SW_1_16_11	Fa0/2
	Fa0/10	Sniffer_6	Eth0
Комутатор SW_1_16_11	Fa0/1	Маршрутизатор R_1_16_8	Fa1/0
	Fa0/2	Комутатор SW_1_16_10	Fa0/2
	Fa0/3	Робоча станція WS_1_16_16	Fa0
	Fa0/4	Робоча станція WS_1_16_15	Fa0
	Fa0/5	Робоча станція WS_1_16_14	Fa0
Сервер Server	Fa0	Маршрутизатор R_1_16_1	Gig0/1

Робоча станція WS_1_16_1	Fa0	Комутатор SW_1_16_4	Fa0/2
Робоча станція WS_1_16_2	Fa0	Комутатор SW_1_16_4	Fa0/3
Робоча станція WS_1_16_3	Fa0	Комутатор SW_1_16_4	Fa0/4
Робоча станція WS_1_16_4	Fa0	Комутатор SW_1_16_5	Fa0/2
Робоча станція WS_1_16_5	Fa0	Комутатор SW_1_16_5	Fa0/3
Робоча станція WS_1_16_6	Fa0	Комутатор SW_1_16_6	Fa0/2
Робоча станція WS_1_16_7	Fa0	Комутатор SW_1_16_6	Fa0/3
Робоча станція WS_1_16_8	Fa0	Комутатор SW_1_16_7	Fa0/2
Робоча станція WS_1_16_9	Fa0	Комутатор SW_1_16_7	Fa0/3
Робоча станція WS_1_16_10	Fa0	Комутатор SW_1_16_7	Fa0/4
Робоча станція WS_1_16_11	Fa0	Комутатор SW_1_16_8	Fa0/3
Робоча станція WS_1_16_12	Fa0	Комутатор SW_1_16_8	Fa0/4
Робоча станція WS_1_16_13	Fa0	Комутатор SW_1_16_9	Fa0/5
Робоча станція WS_1_16_14	Fa0	Комутатор SW_1_16_9	Fa0/5
Робоча станція WS_1_16_15	Fa0	Комутатор SW_1_16_10	Fa0/3
Робоча станція WS_1_16_16	Fa0	Комутатор SW_1_16_10	Fa0/4
Sniffer_1	Eth0	Комутатор SW_1_16_4	Fa0/10
Sniffer_2	Eth0	Комутатор SW_1_16_5	Fa0/10
Sniffer_3	Eth0	Комутатор SW_1_16_6	Fa0/10
Sniffer_4	Eth0	Комутатор SW_1_16_7	Fa0/10
Sniffer_5	Eth0	Комутатор SW_1_16_8	Fa0/10
Sniffer_6	Eth0	Комутатор SW_1_16_9	Fa0/10

Параметри адресації мережі

Таблиця В.1 – Параметри адресації мережі

Підмережа	Інтерфейс	ІР-адреса	Маска	Преф.
Підмережа А	-	191.1.16.0	255.255.255.248	/29
Підмережа В	-	191.1.16.8	255.255.255.252	/30
Підмережа С	-	191.1.16.12	255.255.255.252	/30
Підмережа D	-	191.1.16.16	255.255.255.252	/30
Підмережа Е	-	192.1.16.0	255.255.255.248	/29
Підмережа F	-	193.1.16.0	255.255.255.248	/29
Підмережа G	-	194.1.16.0	255.255.255.252	/30
Підмережа H	-	194.1.16.4	255.255.255.252	/30
Підмережа I	-	195.1.16.0	255.255.255.252	/30
Підмережа J	-	196.1.16.0	255.255.255.0	/24
Підмережа K	-	197.1.16.0	255.255.255.128	/25
Підмережа L	-	197.1.16.128	255.255.255.128	/25
Підмережа M	-	198.1.16.0	255.255.255.0	/24
Підмережа N	-	199.1.16.0	255.255.255.0	/24
Підмережа P	-	200.1.16.0	255.255.255.0	/24
Підмережа O	-	190.1.16.0	255.255.255.252	/30
Маршрутизатор R_1_16_1	Gig0/0	191.1.16.1	255.255.255.248	/29
	Se0/0/0	191.1.16.9	255.255.255.252	/30
	Se0/0/1	191.1.16.13	255.255.255.252	/30
	Gig0/1	190.1.16.1	255.255.255.252	/30
Маршрутизатор R_1_16_2	Gig0/0	191.1.16.2	255.255.255.248	/29
	Se0/0/0	191.1.16.10	255.255.255.252	/30
	Se0/0/1	191.1.16.17	255.255.255.252	/30
	Gig0/1	192.1.16.1	255.255.255.248	/29
Маршрутизатор R_1_16_3	Gig0/0	191.1.16.3	255.255.255.248	/29
	Se0/0/1	191.1.16.14	255.255.255.252	/30
	Se0/0/0	191.1.16.18	255.255.255.252	/30
	Gig0/1	193.1.16.1	255.255.255.248	/29
Маршрутизатор R_1_16_4	Gig0/0	192.1.16.2	255.255.255.248	/29
	Se3/0	194.1.16.1	255.255.255.252	/30
	Fa1/0	196.1.16.1	255.255.255.0	/24
	Gig0/0	192.1.16.3	255.255.255.248	/29

Маршрутизатор R_1_16_5	Se3/0	194.1.16.2	255.255.255.252	/30
	Se4/0	194.1.16.5	255.255.255.252	/30
	Fa1/0	197.1.16.1	255.255.255.128	/25
	Fa2/0	197.1.16.129	255.255.255.128	/25
Маршрутизатор R_1_16_6	Gig0/0	192.1.16.4	255.255.255.248	/29
	Se4/0	194.1.16.6	255.255.255.252	/30
	Fa1/0	198.1.16.1	255.255.255.0	/24
Маршрутизатор R_1_16_7	Gig0/0	193.1.16.2	255.255.255.248	/29
	Se3/0	195.1.16.1	255.255.255.252	/30
	Fa1/0	199.1.16.1	255.255.255.0	/24
Маршрутизатор R_1_16_8	Gig0/0	193.1.16.3	255.255.255.248	/29
	Se3/0	195.1.16.2	255.255.255.252	/30
	Fa1/0	200.1.16.1	255.255.255.0	/24
Сервер Server	Мережний адаптер	190.1.16.2	255.255.255.252	/30
	Шлюз за замовчуванням	190.1.16.1	-	-
Комутатор SW_1_16_4	Vlan 1	196.1.16.5	255.255.255.0	/24
Комутатор SW_1_16_5	Vlan 1	197.1.16.5	255.255.255.128	/25
Комутатор SW_1_16_6	Vlan 1	197.1.16.133	255.255.255.128	/25
Комутатор SW_1_16_7	Vlan 1	198.1.16.5	255.255.255.0	/24
Комутатор SW_1_16_8	Vlan 1	199.1.16.5	255.255.255.0	/24
Комутатор SW_1_16_9	Vlan 1	199.1.16.6	255.255.255.0	/24
Комутатор SW_1_16_10	Vlan 1	200.1.16.5	255.255.255.0	/24
Комутатор SW_1_16_11	Vlan 1	200.1.16.6	255.255.255.0	/24

Конфігураційні файли пристроїв мережі

Конфігураційний файл маршрутизатора 1

R_1_16_1#show running-config	duplex auto
Building configuration...	speed auto
Current configuration : 1639 bytes	!
!	interface GigabitEthernet0/1
version 15.1	ip address 190.1.16.1 255.255.255.252
service timestamps log datetime msec	ip nat outside
service timestamps debug datetime msec	duplex auto
no service password-encryption	speed auto
!	!
hostname R_1_16_1	interface Serial0/0/0
!	ip address 191.1.16.9 255.255.255.252
enable secret 5	clock rate 2000000
\$1\$mERr\$hx5rVt7rPNoS4wqbXKX7m0	!
!	interface Serial0/0/1
clock timezone EET 2	ip address 191.1.16.13 255.255.255.252
!	clock rate 2000000
no ip cef	!
no ipv6 cef	interface Vlan1
!	no ip address
username admin privilege 15 secret 5	shutdown
\$1\$mERr\$hx5rVt7rPNoS4wqbXKX7m0	!
username user secret 5	router ospf 1
\$1\$mERr\$hx5rVt7rPNoS4wqbXKX7m0	log-adjacency-changes
!	network 191.1.16.0 0.0.0.7 area 0
license udi pid CISCO2901/K9 sn	network 191.1.16.8 0.0.0.3 area 0
FTX152460IB-	network 191.1.16.12 0.0.0.3 area 0
!	network 190.1.16.0 0.0.0.3 area 0
ip ssh version 2	!
ip ssh authentication-retries 5	ip nat inside source static 191.1.16.1 190.1.16.0
ip ssh time-out 60	ip classless
no ip domain-lookup	!
ip domain-name cisco.net	ip flow-export version 9
!	!
spanning-tree mode pvst	no cdp run
!	!
interface GigabitEthernet0/0	line con 0
ip address 191.1.16.1 255.255.255.248	exec-timeout 0 0
ip nat inside	logging synchronous

```

!
line aux 0
!
line vty 0 4
logging synchronous
login local
transport input ssh
transport output ssh
!
ntp authentication-key 250999 md5
0822455D0A16 7
ntp authenticate
ntp trusted-key 250999
ntp server 190.1.16.2 key 250999
ntp update-calendar
!
end

```

Конфігураційний файл маршрутизатора 2

```

R_1_16_2#sho running-config
Building configuration...
Current configuration : 1620 bytes
!
version 15.1
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname R_1_16_2
!
enable secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
clock timezone EET 2
!
no ip cef
no ipv6 cef
!
username admin privilege 15 secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
username user secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
license udi pid CISCO2901/K9 sn
FTX1524DJ07-
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
no ip domain-lookup
ip domain-name cisco.net
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 191.1.16.2 255.255.255.248
ip nat outside
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.1.16.1 255.255.255.248
ip nat inside
duplex auto
speed auto
!
interface Serial0/0/0
ip address 191.1.16.10 255.255.255.252
!
interface Serial0/0/1
ip address 191.1.16.17 255.255.255.252
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 191.1.16.0 0.0.0.7 area 0
network 191.1.16.8 0.0.0.3 area 0
network 191.1.16.16 0.0.0.3 area 0
network 192.1.16.0 0.0.0.7 area 0
!
ip nat inside source static 192.1.16.1 191.1.16.0
ip classless
!
ip flow-export version 9
!
no cdp run
!
line con 0
exec-timeout 0 0

```

```
ntp authentication-key 250999 md5
0822455D0A16 7
ntp authenticate
ntp trusted-key 250999
ntp server 190.1.16.2 key 250999
ntp update-calendar
!
en
```

```

interface GigabitEthernet0/0
ip address 191.1.16.3 255.255.255.248
ip nat outside
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 193.1.16.1 255.255.255.248
ip nat inside
duplex auto
speed auto
!
interface Serial0/0/0
ip address 191.1.16.18 255.255.255.252
!
interface Serial0/0/1
ip address 191.1.16.14 255.255.255.252
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
network 191.1.16.0 0.0.0.7 area 0
network 191.1.16.12 0.0.0.3 area 0
network 191.1.16.16 0.0.0.3 area 0
network 193.1.16.0 0.0.0.7 area 0
!
ip nat inside source static 193.1.16.1 191.1.16.0
ip classless
!
ip flow-export version 9
!
no cdp run

```

```

!
line con 0
exec-timeout 0 0
logging synchronous
!
line aux 0
!
line vty 0 4
logging synchronous
login local
transport input ssh

```

```

transport output ssh
!
ntp authentication-key 250999 md5
0822455D0A16 7
ntp authenticate
ntp trusted-key 250999
ntp server 190.1.16.2 key 250999
ntp update-calendar
!
end

```

Конфігураційний файл маршрутизатора 4

```

R_1_16_4#show running-config
Building configuration...
Current configuration : 1701 bytes
!
version 12.2
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname R_1_16_4
!
enable secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip dhcp excluded-address 196.1.16.1
ip dhcp excluded-address 196.1.16.5
!
ip dhcp pool Network_J
network 196.1.16.0 255.255.255.0
default-router 196.1.16.1
dns-server 8.8.8.8
clock timezone EET 2
!
ip cef
no ipv6 cef
!
username admin privilege 15 secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
username user secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
no ip domain-lookup

```

```

ip domain-name cisco.net
!
interface GigabitEthernet0/0
ip address 192.1.16.2 255.255.255.248
ip nat outside
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 196.1.16.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
duplex auto
speed auto
shutdown
!
interface Serial3/0
ip address 194.1.16.1 255.255.255.252
clock rate 2000000
!
interface Serial4/0
no ip address
clock rate 2000000
shutdown
!
router ospf 1
log-adjacency-changes
network 192.1.16.0 0.0.0.7 area 0
network 194.1.16.0 0.0.0.3 area 0
network 196.1.16.0 0.0.0.255 area 0
!

```

```

ip nat inside source static 196.1.16.1 192.1.16.0
ip classless
!
ip flow-export version 9
!
line con 0
exec-timeout 0 0
logging synchronous
!
line aux 0
!
line vty 0 4
logging synchronous

```

```

login local
transport input ssh
transport output ssh
!
ntp authentication-key 250999 md5
0822455D0A16 7
ntp authenticate
ntp trusted-key 250999
ntp server 190.1.16.2 key 250999
ntp update-calendar
!
end

```

Конфігураційний файл маршрутизатора 5

```

R_1_16_5#show running-config
Building configuration...
Current configuration : 2043 bytes
!
version 12.2
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname R_1_16_5
!
enable secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip dhcp excluded-address 197.1.16.1
ip dhcp excluded-address 197.1.16.129
ip dhcp excluded-address 197.1.16.5
ip dhcp excluded-address 197.1.16.133
!
ip dhcp pool Network_K
network 197.1.16.0 255.255.255.128
default-router 197.1.16.1
dns-server 8.8.8.8
ip dhcp pool Network_L
network 197.1.16.128 255.255.255.128
default-router 197.1.16.129
dns-server 8.8.8.8
clock timezone EET 2
!
ip cef
no ipv6 cef

```

```

!
username admin privilege 15 secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
username user secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
no ip domain-lookup
ip domain-name cisco.net
!
interface GigabitEthernet0/0
ip address 192.1.16.3 255.255.255.248
ip nat outside
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 197.1.16.1 255.255.255.128
ip nat inside
duplex auto
speed auto
!
interface FastEthernet2/0
ip address 197.1.16.129 255.255.255.128
ip nat inside
duplex auto
speed auto
!
interface Serial3/0

```

```

ip address 194.1.16.2 255.255.255.252
!
interface Serial4/0
ip address 194.1.16.5 255.255.255.252
clock rate 2000000
!
router ospf 1
log-adjacency-changes
network 192.1.16.0 0.0.0.7 area 0
network 194.1.16.0 0.0.0.3 area 0
network 194.1.16.4 0.0.0.3 area 0
network 197.1.16.0 0.0.0.127 area 0
network 197.1.16.128 0.0.0.127 area 0
!
ip nat inside source static 197.1.16.1 192.1.16.0
ip nat inside source static 197.1.16.129
192.1.16.0
ip classless
!
ip flow-export version 9
!

```

```

line con 0
exec-timeout 0 0
logging synchronous
!
line aux 0
!
line vty 0 4
logging synchronous
login local
transport input ssh
transport output ssh
!
ntp authentication-key 250999 md5
0822455D0A16 7
ntp authenticate
ntp trusted-key 250999
ntp server 190.1.16.2 key 250999
ntp update-calendar
!
end

```

Конфігураційний файл маршрутизатора 6

```

R_1_16_6#show running-config
Building configuration...
Current configuration : 1681 bytes
!
version 12.2
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname R_1_16_6
!
enable secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip dhcp excluded-address 198.1.16.1
ip dhcp excluded-address 198.1.16.5
!
ip dhcp pool Network_M
network 198.1.16.0 255.255.255.0
default-router 198.1.16.1
dns-server 8.8.8.8
clock timezone EET 2
!
ip cef
no ipv6 cef

```

```

!
username admin privilege 15 secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
username user secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
no ip domain-lookup
ip domain-name cisco.net
!
interface GigabitEthernet0/0
ip address 192.1.16.4 255.255.255.248
ip nat outside
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 198.1.16.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface FastEthernet2/0

```

```

no ip address
duplex auto
speed auto
shutdown
!
interface Serial3/0
no ip address
clock rate 2000000
shutdown
!
interface Serial4/0
ip address 194.1.16.6 255.255.255.252
!
router ospf 1
log-adjacency-changes
network 192.1.16.0 0.0.0.7 area 0
network 194.1.16.4 0.0.0.3 area 0
network 198.1.16.0 0.0.0.255 area 0
!
ip nat inside source static 198.1.16.1 192.1.16.0
ip classless
!
ip flow-export version 9
!
line con 0
exec-timeout 0 0
logging synchronous
!
line aux 0
!
line vty 0 4
logging synchronous
login local
transport input ssh
transport output ssh
!
ntp authentication-key 250999 md5
0822455D0A16 7
ntp authenticate
ntp trusted-key 250999
ntp server 190.1.16.2 key 250999
ntp update-calendar
!
end

```

Конфігураційний файл маршрутизатора 7

```

R_1_16_7#show running-config
Building configuration...
Current configuration : 1737 bytes
!
version 12.2
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
!
hostname R_1_16_7
!
enable secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip dhcp excluded-address 199.1.16.1
ip dhcp excluded-address 199.1.16.5
ip dhcp excluded-address 199.1.16.6
!
ip dhcp pool Network_N
network 199.1.16.0 255.255.255.0
default-router 199.1.16.1
dns-server 8.8.8.8
clock timezone EET 2
!
ip cef
no ipv6 cef
!
username admin privilege 15 secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
username user secret 5
$1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
no ip domain-lookup
ip domain-name cisco.net
!
interface GigabitEthernet0/0
ip address 193.1.16.2 255.255.255.248
ip nat outside
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 199.1.16.1 255.255.255.0

```

```
ip nat inside source static 199.1.16.1 193.1.16.0
ip classless
!
ip flow-export version 9
!
line con 0
exec-timeout 0 0
logging synchronous
!
line aux 0
!
line vty 0 4
logging synchronous
login local
transport input ssh
transport output ssh
!
ntp authentication-key 250999 md5
0822455D0A16 7
ntp authenticate
ntp trusted-key 250999
ntp server 190.1.16.2 key 250999
ntp update-calendar
!
end
```

```
default-router 200.1.16.1
dns-server 8.8.8.8
clock timezone EET 2
!
ip cef
no ipv6 cef
!
username admin privilege 15 secret 5
$1$mERr$hX5rVt7rPNoS4wqbXKX7m0
username user secret 5
$1$mERr$hX5rVt7rPNoS4wqbXKX7m0
!
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
no ip domain-lookup
ip domain-name cisco.net
!
interface GigabitEthernet0/0
```

```

ip address 193.1.16.3 255.255.255.248
ip nat outside
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 200.1.16.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface FastEthernet2/0
no ip address
duplex auto
speed auto
shutdown
!
interface Serial3/0
ip address 195.1.16.2 255.255.255.252
!
interface Serial4/0
no ip address
clock rate 2000000
shutdown
!
router ospf 1
log-adjacency-changes
network 193.1.16.0 0.0.0.7 area 0
network 195.1.16.0 0.0.0.3 area 0

```

```

network 200.1.16.0 0.0.0.255 area 0
!
ip nat inside source static 200.1.16.1 193.1.16.0
ip classless
!
ip flow-export version 9
!
line con 0
exec-timeout 0 0
logging synchronous
!
line aux 0
!
line vty 0 4
logging synchronous
login local
transport input ssh
transport output ssh
!
ntp authentication-key 250999 md5
0822455D0A16 7
ntp authenticate
ntp trusted-key 250999
ntp server 190.1.16.2 key 250999
ntp update-calendar
!
end

```

Конфігураційний файл комутатора 4

```

SW_1_16_4#show running-config
Building configuration...
Current configuration : 1323 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW_1_16_4
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1

```

```

!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!

```

```

interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!

```

```

interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 196.1.16.5 255.255.255.0
!
line con 0
logging synchronous
exec-timeout 0 0
!
line vty 0 4
login
line vty 5 15
login
!
monitor session 1 source interface Fa0/2
monitor session 1 source interface Fa0/3
monitor session 1 source interface Fa0/4
monitor session 1 destination interface Fa0/1
!
end

```

Конфігураційний файл комутатора 5

```

SW_1_16_5#show running-config
Building configuration...
Current configuration : 1284 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW_1_16_5
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!

```

```

interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!

```

```

interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 197.1.16.5 255.255.255.128
!
line con 0
logging synchronous
exec-timeout 0 0
!
line vty 0 4
login
line vty 5 15
login
!
monitor session 1 source interface Fa0/2
monitor session 1 source interface Fa0/3
monitor session 1 destination interface Fa0/1
!
end

```

Конфігураційний файл комутатора 6

```

SW_1_16_6#show running-config
Building configuration...
Current configuration : 1286 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW_1_16_6
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!

```

```

interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!

```

```

interface GigabitEthernet0/2
!
interface Vlan1
ip address 197.1.16.133 255.255.255.128
!
line con 0
logging synchronous
exec-timeout 0 0
!
line vty 0 4
login
line vty 5 15
login
!
monitor session 1 source interface Fa0/2
monitor session 1 source interface Fa0/3
monitor session 1 destination interface Fa0/1
!
end

```

Конфігураційний файл комутатора 7

```

SW_1_16_7#show running-config
Building configuration...
Current configuration : 1323 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW_1_16_7
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!

```

```

interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!

```

```

interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 198.1.16.5 255.255.255.0
!
line con 0
logging synchronous
exec-timeout 0 0
!
line vty 0 4
login
line vty 5 15
login
!
monitor session 1 source interface Fa0/2
monitor session 1 source interface Fa0/3
monitor session 1 source interface Fa0/4
monitor session 1 destination interface Fa0/1
!
end

```

Конфігураційний файл комутатора 8

```

SW_1_16_8#show running-config
Building configuration...
Current configuration : 1354 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW_1_16_8
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!

```

```

interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 199.1.16.5 255.255.255.0
!
line con 0

```

```

logging synchronous
exec-timeout 0 0
!
line vty 0 4
login
line vty 5 15
login
!
monitor session 1 source interface Fa0/3
monitor session 1 source interface Fa0/4
monitor session 1 source interface Fa0/5
monitor session 1 destination remote vlan 50
reflector-port Fa0/24
!
end

```

Конфігураційний файл комутатора 9

```

SW_1_16_9#show running-config
Building configuration...
Current configuration : 1241 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW_1_16_9
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8

```

```

!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!

```

```

interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 199.1.16.6 255.255.255.0

line con 0
logging synchronous

```

```

exec-timeout 0 0
!
line vty 0 4
login
line vty 5 15
login
!
monitor session 1 destination interface Fa0/10
monitor session 1 source remote vlan 50
!
end

```

Конфігураційний файл комутатора 10

```

SW_1_16_10#show running-config
Building configuration...
Current configuration : 1242 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW_1_16_10
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9

```

```

!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!

```

```

interface GigabitEthernet0/2
!
interface Vlan1
ip address 200.1.16.5 255.255.255.0
!
line con 0
logging synchronous
exec-timeout 0 0
!

```

```

line vty 0 4
login
line vty 5 15
login
!
monitor session 1 destination interface Fa0/10
monitor session 1 source remote vlan 50
!
end

```

Конфігураційний файл комутатора 11

```

SW_1_16_11#show running-config
Building configuration...
Current configuration : 1355 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SW_1_16_11
!
no ip domain-lookup

spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11

```

```

!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 200.1.16.6 255.255.255.0

line con 0
logging synchronous

```

exec-timeout 0 0
!
line vty 0 4
login
line vty 5 15
login
!

monitor session 1 source interface Fa0/3
monitor session 1 source interface Fa0/4
monitor session 1 source interface Fa0/5
monitor session 1 destination remote vlan 50
reflector-port Fa0/24
!
end