МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЄРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЇ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

_____ Одарченко Р.С.

«____» _____2021р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСНИЦІ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «Модель віртуальної локально-обчислювальної мережі»

Виконавець: _____ Онопрієнко А.А.
(підпис)

Керівник: _____ Тараненко А.Г.
(підпис)

Нормоконтролер: _____ Бахтіяров Д.І.
(підпис)

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій

Кафедра телекомунікаційних та радіоелектронних систем

Спеціальність 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ

Завідувач кафедри

Одарченко Р.С.

«____» _____2021р.

ЗАВДАННЯ

на виконання дипломної роботи

Онопрієнко Анастасія Анатоліївна

1. Тема дипломної роботи: «Модель віртуальної локально-обчислювальної мережі» затверджена наказом ректора від «06» квітня 2021 р. №559/ст.
2. Термін виконання роботи: з 17.05.2021 р. по 20.06.2021 р.
3. Вихідні дані до роботи: топологія мережі, комутатор, маршрутизатор, локально-обчислювальна мережа, комп'ютерне моделювання, коллізія, сегментування.

4. Зміст пояснювальної записки: віртуальне сегментування локально-обчислювальних мереж; сегментування локально-обчислювальних мереж; комп’ютерне моделювання віртуальної локально-обчислювальної мережі.

5. Перелік обов’язкового графічного матеріалу: основні поняття; переваги використання VLAN; мережеві атаки та методи захисту від них у VLAN; комп’ютерне моделювання віртуальної локально-обчислювальної мережі; налаштування VLAN; перевірка правильності налаштувань віртуальних локально-обчислювальної мереж.

6. Календарний план-графік

№	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів диплому	18.05.2021-03.06.2021	Виконано
2	Вступ	21.05.2021-10.06.2021	Виконано
3	Віртуальне сегментування локально-обчислювальних мереж	18.05.2021-12.06.2021	Виконано
4	Сегментування локально-обчислювальних мереж	18.05.2021-13.06.2021	Виконано
5	Комп’ютерне моделювання віртуальної локально-обчислювальної мережі	18.05.2021-14.06.2021	Виконано
6	Усунення недоліків дипломної роботи	10.06.2021-15.06.2021	Виконано

7. Дата видачі завдання: 26 квітня 2021 р.

Керівник дипломної роботи: _____ Тараненко А.Г.

Завдання прийняв до виконання: _____ Онопрієнко А.А.

РЕФЕРАТ

Дипломна робота «Модель віртуальної локально-обчислювальної мережі» містить 50 сторінок, 19 рисунків, 11 використаних джерел.

VLAN, ВІРТУАЛЬНА ЛОКАЛЬНО-ОБЧИСЛЮВАЛЬНА МЕРЕЖА, СЕГМЕНТУВАННЯ, МОДЕЛЮВАННЯ, CISCO PACKET TRACER.

Об’єкт дослідження:. процес сегментування локально-обчислювальної мережі.

Предмет дослідження: віртуальне сегментування локально-обчислювальної мережі.

Мета дипломної роботи: комп’ютерне моделювання віртуальної локально-обчислювальної мережі в середовищі Cisco Packet Tracer.

Для досягнення сформованої мети необхідно виконати такі завдання:

1. Проаналізувати сегментування локально-обчислювальних мереж.
2. Проаналізувати віртуальне сегментування локально-обчислювальних мереж.
3. Побудувати комп’ютерну модель віртуальної локально-обчислювальної мережі.

Мета дослідження:

1. Аналіз процесу сегментування локально-обчислювальної мережі.
2. Аналіз віртуального сегментування локально-обчислювальної мережі.
3. Комп’ютерна модель віртуальної локально-обчислювальної мережі в середовищі Cisco Packet Tracer.

ЗМІСТ

ВСТУП

Актуальність теми. Сьогодні світ значною мірою покладається на технології для виконання повсякденної роботи. Розвиток технологій допоміг поліпшити способи передачі інформації. Використання віртуальної локальної мережі (VLAN) зараз більш популярно, ніж будь-коли. Мережі VLAN прості, але вони пропонують широкий спектр можливостей і опцій для поліпшення мережі. Функціонально мережі VLAN дозволяють адміністратору розділити локальну мережу на окремі незалежні мережі. Основна причина поділу мережі на VLAN - зменшити перевантаження у великій LAN. Щоб зрозуміти цю проблему, потрібно коротко поглянути на те, як ЛВС розвивалася за роки. Спочатку локальні мережі були дуже простими - все робочі станції були підключені до єдиного коаксіального кабелю. У простій локальній мережі кожен пакет, як і будь-який пристрій поміщає в провід відправку на всі інші пристрої в локальній мережі. У міру того, як кількість робочих станцій в типовій локальної мережі росло, вони почали безнадійно перевантажуватися, було занадто багато зіткнень, тому що більшу частину часу, коли робоча станція намагалась відправити пакет, він виявляв, що лінія вже зайнятий пакетом, відправленим якимось іншим пристроєм. Тому використання віртуально локальної мережі, вирішує всі ці проблеми.

Використовування локально-обчислювальних мереж супроводжується необхідністю збільшення протяжності.

Мета і завдання дослідження:

- Проаналізувати сегментування локально-обчислювальних мереж.
- Проаналізувати віртуальне сегментування локально-обчислювальних мереж.
- Побудувати комп’ютерну модель віртуальної локально-обчислювальної мережі.

Об’єкт дослідження - процес сегментування локально-обчислювальної мережі.

Предмет дослідження - віртуальне сегментування локально-обчислювальної мережі.

Методи дослідження. Комп'ютерне моделювання віртуальної локально-обчислювальної мережі в середовищі Cisco Packet Tracer.

Практичне значення отриманих результатів.

Оптимізування мережевого трафіку, забезпечення надійності та безпеки поведінки таких мереж при збільшенні кількості її користувачів. Ізольовування проблеми тільки в рамках одного сегменту. Розподіл навантаження між сегментами. Обмеження доступу користувачам поза даним сегментом.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2020 р.

РОЗДІЛ 1
СЕГМЕНТУВАННЯ ЛОКАЛЬНО-ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

1.1 Аналізування передумов, призначення та способів сегментування локально обчислювальних мереж

Сьогодні світ значною мірою покладається на технології для виконання повсякденної роботи. Розвиток технологій допоміг поліпшити способи передачі інформації. Використання віртуальної локальної мережі (VLAN) зараз більш популярно, ніж будь-коли. Але що таке VLAN? Мережі VLAN прості, але вони пропонують широкий спектр можливостей і опцій для поліпшення мережі. VLAN - це технологія, яка забезпечує поділ фізичної мережі на логічну на другому рівні. Функціонально мережі VLAN дозволяють адміністратору розділити локальну мережу на окремі незалежні мережі. Мережі VLAN часто реалізуються як в великих, так і в невеликих мережах VLAN. Я розповім процес сегментації LAN в VLAN і настройку комутатора для формування окремих сегментів LAN. Компанія вважає своїм обов'язком захистити мережу від будь-яких зловмисників, які намагаються вкрасти інформацію компанії. Технології мережевої безпеки забезпечують захист мережі від крадіжки і неправомірного використання конфіденційних даних, а також захист від зловмисних атак з боку вірусів. Без рішення щодо забезпечення безпеки компанія ризикує несанкціонованим вторгненням, простоєм мережі, порушенням обслуговування, недотриманням нормативних вимог і навіть судовими позовами. Компанії використовують VLAN як спосіб з'єднання мереж в своїй компанії [1] [2]. Хороші системи повинні легко працювати з різними системами, бути зрозумілими клієнтам, забезпечувати віддалений доступ і підтримувати високий рівень виконання. З іншого боку, безпечні системи забезпечують конфіденційність даних, стабільну роботу системи і підкреслюють респектабельність інформації [3].

Основна причина поділу мережі на VLAN - зменшити перевантаження у великій LAN. Щоб зрозуміти цю проблему, потрібно коротко поглянути на те, як ЛВС розвивалася за роки. Спочатку локальні мережі були дуже простими - все робочі станції були підключені до єдиного коаксіального кабелю. У простій локальній мережі кожен пакет, як і будь-який пристрій поміщає в провід відправку на всі інші пристрої в локальній мережі. У міру того, як кількість робочих станцій в типовій локальної мережі росло, вони почали безнадійно перевантажуватися, було занадто багато зіткнень, тому що більшу частину часу, коли робоча станція намагалась відправити пакет, він виявляв, що лінія вже зайнятий пакетом, відправленим якимось іншим пристроєм.

У цьому розділі описані три вирішення цієї проблеми:

- Використання маршрутизаторів для сегментації локальних мереж.
- Використання перемикачів для сегментації ЛВС.
- Використання VLAN для сегментації LAN.

Першим рішенням цієї проблеми було сегментування мережі за допомогою маршрутизаторів. Це б розділило мережу на кілька менших локальних мереж. На кожному було б менше робочих місць LAN і так менше завантаженості. Звичайно, маршрутизована передача даних між локальними мережами, повинні бути маршрутизованою, тому рівень 3 адреси має бути організован так, щоб кожна локальна мережа мала ідентифікований набір адрес який може бути направлений, наприклад, в IP-підмережу або зону AppleTalk. Немаршрутизовані протоколи повинні бути з'єднані мостами, що не зовсім знижує застої, тому що мости пересилають всі трансляції. Але, по крайній мірі, для одноадресних пакетів, міст пересилає пакети тільки в тому випадку, якщо він знає, що адреса призначення знаходиться не в локальній мережі відправника.

Використання комутаторів для сегментування локальних мереж. У міру того, як комутатори стали більш доступними, відбувся перехід від ланцюгових концентраторів до набору концентраторів підключених до світчу. Комутатор відправляє трафік на заданий порт тільки в тому випадку, якщо трафік повинен йти на цей порт. Таким чином, комутатори зменшують перевантаження робочих

станцій, зупиняючи робочі станції від перегляду всього трафіку з інших портів комутатора. Однак в простій комутованої мережі як і раніше потрібні маршрутизатори, щоб встановити межі того, де відправляються трансляції (звані «стримування трансляції»). Отже, типова локальна мережа була налаштована, як показано на наступній схемі:

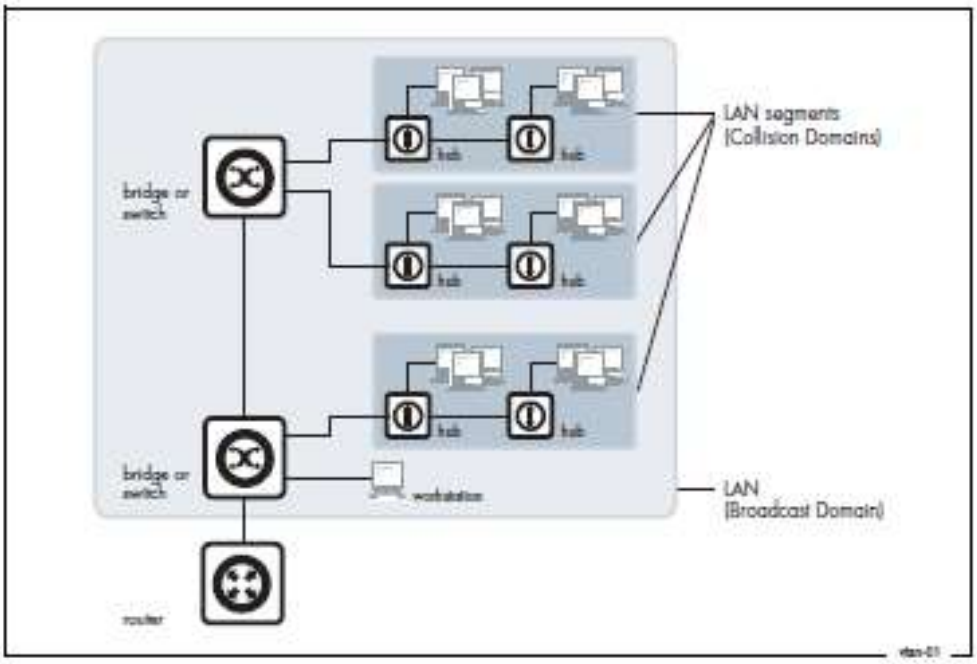

Рис.1.1. Налаштування типової локольної мережі

На рис.1.1. наведена концепція сегмента LAN. Це також називається домен зіткнення, тому що, коли пристрій намагається відправити пакет, він може зіткнутися тільки з пакетами, відправленими іншими пристроями в тому ж сегменті. Кожен сегмент LAN складається з усіх пристроїв, підключених до одного порту комутатора - комутатор зупиняє пакети з різних портів від зіткнення один з одним. Сама локальна мережа називається широкомовним доменом, тому що якщо будь-який пристрій в локальній мережі відправляє широкомовний пакет, він буде переданий на всі пристрої в цій локальній мережі, але не на пристрої за межами локальної мережі.

Використання віртуальних локальних мереж для сегментації локальних мереж. У міру зростання локальних мереж швидкість передачі даних ставала все

вище, а користувачі бажали більшої гнучкості, маршрутизатори в мережі стали вузьким місцем. Це тому що:

- Маршрутизатор зазвичай пересилають дані в програмному забезпеченні, тому працюють не так швидко, як комутатори.
- Поділ локальної мережі з використанням маршрутизаторів означало, що локальна мережа зазвичай відповідала певному фізичному місцезнаходженню. Це стало обмежуючим фактором, коли у багатьох користувачів були ноутбуки, і вони хотіли переміщатися між будівлями, але при цьому мати однакову мережеву середу всюди де вони підключилися.

Тому виробники комутаторів почали впроваджувати методи визначення «віртуальних локальних мереж» - наборів комутаторів. Порти, зазвичай розподілені за кількома комутаторами, які так чи інакше взаємодіяли, як якщо б вони знаходилися в єдиній ізольованою ЛВС. Таким чином, робочі станції можна було розділити на окремі локальні мережі без фізичного поділу маршрутизаторів.

Приблизно в той же час хаби стали менш популярними і були в значній мірі замінені на L2 перемикачі. Це зробило всю концепцію області колізій в деякій мірі історичною. У сучасних мережах «домен колізій» в основному складається з одного пристрою, підключеного до L2 порту комутатора або, можливо, ПК з підключеним до нього чимось на зразок IP-телефону.

Таким чином, замість локальних мереж, відповідних фізичним областям, розділеним один від одного маршрутизаторами, в мережі розподілені віртуальні локальні мережі. Наприклад, всі пристрої в різні області, помічені як «VLAN A», все належать одній віртуальної локальної мережі.

Переваги використання VLAN:

1. Продуктивність. Як згадувалося вище, маршрутизатори, які пересилають дані в програмному забезпеченні, стають вузьке місце в міру збільшення швидкості передачі даних по LAN. Відмова від маршрутизаторів усуває це вузьке місце.

2. Формування віртуальних робочих груп. Тому що робочі місця можна переносити з одного VLAN на інший, просто змінивши конфігурацію на комутаторах, що працюють разом над певним проектом, об'єднані в єдину VLAN. Тоді буде простіше обмінюватися файлами і ресурсами один з одним. Хоча, чесно кажучи, віртуальні робочі групи здаються хорошою ідеєю в теорії, але часто це так не працює на практиці. Виявляється, користувачів зазвичай більше цікавить доступ до ресурсу компанії (файлові сервери, принтери і т. д.), ніж файли на комп'ютерах один одного.

3. Більша гнучкість. Якщо користувачі переміщують свої столи або просто переміщаються за місцем зі своїми ноутбуки, то, якщо VLAN налаштовані правильно, вони можуть підключити свій ПК до нового місце розташування, і як і раніше перебувати в тій же VLAN. Це набагато складніше, коли мережу фізично розділені маршрутизаторами.

4. Легкість поділу ресурсів. Якщо є сервери або інше обладнання, до якого адміністратор мережі бажає обмежити доступ, тоді їх можна відкласти в власне VLAN. Тоді користувачам в інших VLAN можна буде надати доступ вибірково.

Впровадження VLAN на основі портів. Створення VLAN на комутаторі включає визначення набору портів і визначення критеріїв членства в VLAN для робочих станцій, підключених до цих портів. Безумовно, найбільш поширений критерій членства в VLAN заснований на портах. У віртуальних локальних мережах на основі портів порти комутатора просто призначаються віртуальним локальним мережам без будь-яких додаткових критеріїв. Всі пристрої, підключені до даного порту, автоматично стають членами VLAN, до якої цей порт був призначений. Фактично, це просто ділить перемикач на набір незалежних суб-перемикачів.

Таблиця 1.1

Port	VLAN
1	1
2	1
3	2
4	1

Розподіл однієї VLAN за кількома комутаторами. На малюнку в розділі «Використання VLAN для сегментації локальних мереж» показаний приклад мережі на основі VLAN. Він показує частину VLAN A, підключену до одного комутатора, і ще кілька VLAN A підключеного до іншого комутатора. Ви можете запитати: «Чи є вони частиною однієї VLAN A або окремих мереж VLAN, які все випадково називається VLAN A? » Відповідь полягає в тому, що всі вони є частинами однієї і тієї ж VLAN - існує одна VLAN A, яка є розподілені за двома світча. Як цього добитися? Як один комутатор дізнається, що при отриманні широкомовного пакета що він зв'язується з VLAN A, що він також повинен пересилати цю трансляцію передачу інших комутаторів? Це можна зробити різними способами, і на зорі створення віртуальних локальних мереж майже кожен з цих способів був випробуваний. Деякі виробники використовували в своїх комутаторах пропріетарний протокол для інформування один одного про свої таблиці VLAN, деякі постачальники використовували розділені за часом мультиплексування, при якому різні часові інтервали виділялися різним VLAN, інші постачальники використовувала маркування кадрів. Зрештою, маркування кадрів стала загальноприйнятим стандартом. Як ми побачимо, в більшості випадків це просте і елегантне рішення. Однак спочатку у нього був один великий недолік: він вимагав принципову зміну формату заголовка Ethernet. Це розділило світові пристрої Ethernet в ті, які розпізнають тегованих заголовки, і ті, які не розпізнають тегованих заголовки. Іншими словами, більша частина обладнання Ethernet застаріла.

1.2 Аналізування роботи тегів у віртуальних локально-обчислюванних мережах

Як працюють теги? Просто, 4 байта вставляються в заголовок пакета Ethernet. Він складається з 2 байтів Ідентифікатор протоколу тегів (TPID) і 2 байта інформації управління тегами (TCI):

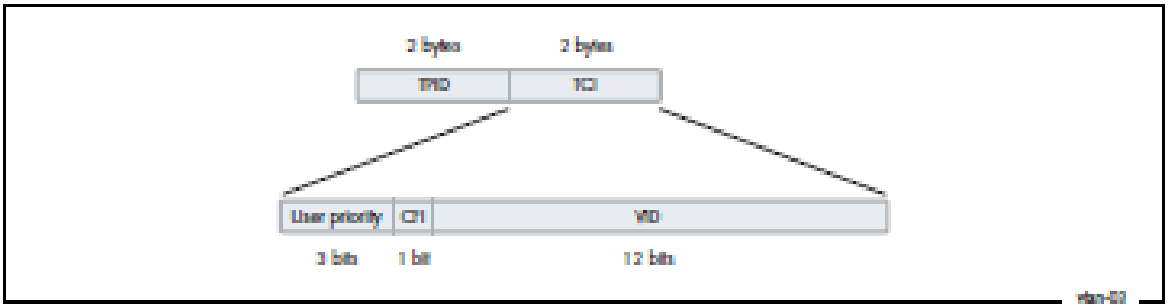

Рис.1.3. Схема налаштування тегів

TPID - це ідентифікатор протоколу тега, який вказує, що заголовок тега стоїть за ним і містить пріоритет користувача, індикатор канонічного формату (CFI) і ідентифікатор VLAN. Пріоритет користувача - це 3-бітове поле, яке дозволяє кодувати інформацію про пріоритет в кадрі. Вісім дозволених рівнів пріоритету, де нуль - найнижчий пріоритет, а сім – найвищий пріоритет.

CFI - це 1-бітний індикатор, який завжди встановлюється в нуль для комутаторів Ethernet. CFI використовується для сумісність між мережами Ethernet і Token Ring. Якщо кадр отриманий через Ethernet порт має CFI, встановлений на 1, то цей кадр не повинен передаватися по мосту на нетегірованний порт. Потім поле VID містить ідентифікатор VLAN. Насправді тільки поле VID дійсно необхідно для розподілу VLAN між комутаторами, але IEEE вирішив, що вони поки міняли формат заголовка Ethernet, вони могли також додати User Пріоритет і CFI теж. Як тег спрощує розподіл віртуальних локальних мереж між комутаторами. Розглянемо широкомовний пакет, що надходить на порт комутатора. За якимось критерієм пакет пов'язаний з VLAN 47, тобто VLAN з VLAN ID = 47. Тепер порт 17 цього комутатора підключений до порт 12 іншого комутатора, який також має кілька портів в VLAN 47. Адміністратору необхідно налаштувати порт 17 комутатора 1 і порт 12 комутатора 2 як «помічені» порти-члени VLAN 47. Це вказує комутатора 1 відправити вихідний порт 17 широкомовної передачі у вигляді тегованих пакета

з VID = 47 в тезі. І він повідомляє комутатора 2 прийняти цей позначений пакет і зв'язати його з VLAN 47. Потім комутатор 2 відправить пакет через всі вхідні в нього порти VLAN 47, тому що це те, що він робить з широкомовними розсилками, пов'язаними з VLAN 47.

Тег дозволяє другому комутатору дуже легко дізнатися, що робити з пакетом, тому що тег позначає цей пакет як принадлежний до VLAN 47, а комутатор 2 точно знає, що повинно відбуватися з пакетами, що належать VLAN 47. Отже, дійсно є тільки два простих правила:

- Якщо порт є тегованих членом VLAN, то будь-які пакети, відправлені через цей порт цієї VLAN повинен мати тег, вставлений в заголовок.
- Якщо тегованих пакет надходить в порт, і порт є тегованих членом VLAN відповідний VID в тезі пакета, то пакет асоціюється з цієї VLAN.

За допомогою цих двох простих правил можна розподілити мережі VLAN за кількома комутаторів.

Змішування пакетів з тегами і без тегів на одному порту. У попередньому розділі ми обговорили використання тегів для позначення приналежності пакетів до VLAN які передаються з одного комутатора на інший. Але також можливо, що немарковані пакети будуть транспортуватися по тому каналу, який з'єднує два комутатора. Наприклад, порт 17 комутатора 1 може бути непоміченими членом VLAN 56, і порт 12 комутатора 2 є нетегірованним членом VLAN 56. У цьому випадку, якщо комутатора 1 необхідно транспортувати пакети VLAN 56 на комутатор 2, він буде відправляти їх без тегів, коли ті непомічені пакети прийдуть на комутатор 2, комутатор 2 якої мережі VLAN вирішить зв'язати їх пакети з, врахуванням, що у них немає тега, що вказує на їх членство в VLAN? Ну фактично, комутатор 2 зрозуміє, що VLAN 56 є нетегірованной VLAN на приймаючому порту, тому непомічені пакети будуть вважатися належними VLAN 56.

Очевидно, порт може бути нетегірованним членом тільки однієї VLAN на основі порту, в іншому випадку виникне невизначеність щодо того, до якого VLAN відносяться немарковані пакети. Часто ви можете не захотіти пов'язувати

власну VLAN з портом, який з'єднує комутатор до іншого комутатора, тому всі пакети, що надходять в цей порт, повинні використовувати тег VLAN, щоб вказати їх членство в VLAN. Це зупиняє прийом комутатором будь-яких немаркованих пакетів на порт. У AlliedWare Plus це досягається шляхом настройки порту на транковий режим, а не настройка на ньому власної VLAN. У AlliedWare це досягається установкою параметра accept = vlan на порту, так що порт буде приймати тільки пакети з тегами VLAN. Приймати тільки пакети, відповідні конфігурації VLAN порту

Розглянемо порт, до якого підключена звичайна робоча станція. Нормальні додатки на робочу станцію ніколи не буде відправляти помічені пакети, тому порт комутатора не потрібно приймати пакети з тегами.

Для захисту від зловмисних дій в більшості комутаторів передбачена можливість настройки «вхідного трафіку» фільтрація . Коли до порту застосовується фільтрація, пакети будуть прийматися тільки в порт. якщо вони відповідають конфігурації VLAN цього порту. Отже, якщо порт є непомічені членом одного VLAN і нічого більше, тоді на порт будуть прийматися тільки немарковані пакети. Якщо порт позначений для набору VLAN, то позначений пакет буде прийнятий в порт тільки в тому випадку, якщо він позначений VID однією з помічених VLAN, налаштованих на порту.

ВИСНОВКИ ДО РОЗДІЛУ 1

В цьому розділі проаналізовано варіації сегментування локально-обчислювальних мереж. За наслідками аналізу установлено, що сегментування допамагає з вирішенням більшості питань побудови та налаштування праці локально-обчислювальних мереж. Приміром, розглянуто основи віртуального сегментування локально-обчислювальних мереж.

РОЗДІЛ 2
ВІРТУАЛЬНЕ СЕГМЕНТУВАННЯ ЛОКАЛЬНО-ОБЧИСЛЮВАЛЬНИХ МЕРЕЖ

2.1 Сегментація та безпека віртуальної локальної мережі(VLAN)

Інтернет, найбільша безпеку віртуальної локальної мережі (VLAN). Інтернет, найбільша мережа, представляє собою глобальну систему взаємопов'язаних комп'ютерних мереж, які використовують набір Інтернет-протоколів (TCP / IP) для з'єднання мільярдів комп'ютерів і електронних пристроїв по всьому світу. Він складається з мільйонів приватних, державних, академічних, ділових і урядових мереж, від місцевого до глобального. Він містить великий і широкий спектр інформаційних ресурсів та послуг, таких як WorldWideWeb (WWW), електронна пошта, телефонія, голос і відео по IP, а також обмін файлами з використанням тимчасових мереж. Інтернет - це мережа мереж. Потім ми розглянемо різні типи мереж. ЛВС з'єднує комп'ютери і пристрої на обмеженій території, наприклад в житловому будинку, кампусі, школі, лабораторії або офісі. З іншого боку, є глобальна мережа (WAN), яка покриває більше географічне відстань у порівнянні з LAN. Мережа більше LAN і менше WAN може розглядатися як Metropolitan Area Network (MAN), що охоплює територію від декількох кварталів міста до площі всього міста. Якщо LAN використовує фізичне адміністрування для створення мережі, VLAN була створена з використанням логічних мереж для поділу фізичного комутатора і окремих хостів, які не повинні мати доступ один до одного. VLAN дозволяє створювати різні мережі на одному фізичному комутаторі на канальному рівні. Щоб розділити мережу на VLAN, потрібно налаштувати мережевий комутатор або маршрутизатор. Це дозволяє різним відділам компанії мати різні мережі на одному фізичному комутаторі. Це знижує витрати, оскільки потрібно тільки один фізичний комутатор, і може повністю спростити реалізацію і проектування мережі, оскільки його можна налаштувати за допомогою програмного

забезпечення, а не обладнання. Мережі VLAN дозволяють адміністратора групувати вузли разом, навіть якщо вузли не знаходяться на одному мережевому комутаторі. Без VLAN вузли групування повинні будуть переміщати вузли або перенаправляти канали передачі даних [10]. VLAN дозволяє гнучко вносити зміни в разі необхідності перенастроювати мережу [11]. Однак мережі VLAN і раніше уразливі для мережевих атак. Від захисту даних користувачів від зростаючого числа загроз до забезпечення безперервності бізнесу - IT-безпека є важливим елементом IT-інфраструктури будь-якої організації. Для фахівців у галузі інформаційних ключовим моментом є можливість порівнювати з колегами, оцінювати загрозу або просто розуміти, чому проект безпеки важливий для бізнесу. Було виявлено безліч методів вирішення цієї проблеми. Однак ці методи зажадають удосконалення з роками, оскільки мережеві зловмисники стають все краще в атаці на VLAN [[1] [2] .

Більша мережа розбита на більш дрібні ділянки шляхом реалізації віртуальних локальних мереж. Це називається сегментацією мережі, яка спрощує управління мережею. ЛВС - це комбінація комп'ютерів і пристроїв, підключених один до одного на невеликій території для взаємодії і спільного використання ресурсів. Маршрутизатор перевіряють мережеву адресу пакетів і використовують різні протоколи маршрутизації для ефективної відправки пакета за призначенням. Комутація може зменшити кількість вузлів за рахунок використання одного і того ж сегмента мережі, що призведе до зниження перевантаження в кожному сегменті. У комутованих концентраторах або мостах кожен вузол може мати свій власний сегмент мережі і, отже, мати доступ до всієї смуги пропускання мережі цього сегмента. Комутаційні мости можуть глибоко заглядати в пакет і використовувати інформацію протоколу і т.п. для забезпечення певного рівня фільтрації і приоритизации.

2.2 Типи віртуально – обчислювальних мереж

Існує два типи VLAN:

Статичні VLAN налаштовуються адміністратором мережі, головним чином з міркувань безпеки. Оскільки а призначається VLAN вручну, завжди буде виконуватися пошук і обслуговування. Цей тип обладнання, звичайно, легко встановити і налаштувати, але ручне оновлення потрібно, якщо будь-які зміни в хості. Неможливо реалізувати статичні VLAN у великій мережі, яка вимагає частих оновлень. У цьому випадку пропонується динамічне рішення.

Динамічні мережі VLAN можуть бути призначені автоматично за допомогою програмного забезпечення на основі апаратного адреси (MAC), протоколів і додатків. Наприклад, припустимо, що MAC-адреси були перераховані в централізованому програмному забезпеченні VLAN. Якщо він підключений до непризначення порту комутатора, база даних управління VLAN може шукати апаратну адресу, призначати і налаштовувати порт комутатора в правильну VLAN. Складність цього методу полягає в тому, щоб налаштувати базу даних на початковому рівні [11].

У сучасних мережах існує кілька різних типів віртуальних локальних мереж. Деякі з них можна пояснити і класифікувати в залежності від їх класів трафіку. Інші типи VLAN можуть визначатися конкретною функцією, яку вони обслуговують.

VLAN для передачі даних і налаштування її для передачі трафіку, що генерується користувачем. Він не буде включати VLAN, яка транслює голосової або керуючий трафік. Загальноприйнято розрізняти голосовий трафік і трафік управління від трафіку даних. Іноді його називають користувальницької VLAN. Ці VLAN розроблені для поділу мережі на групи осіб чи груп пристроїв.

VLAN за замовчуванням, коли конфігурація за замовчуванням завантажується при початковому завантаженні, всі порти комутатора стають частиною VLAN за замовчуванням. Ці порти комутатора, які тепер є частиною VLAN за замовчуванням, фактично є частиною того ж широкомовного домену. Це означає, що будь-який пристрій, підключений до будь-якого порту комутатора, може взаємодіяти з іншими пристроями на інших портах

комутатора. VLAN 1 особа вважається такою VLAN за замовчуванням для комутаторів Cisco.

Власна VLAN визначається для магістрального порту 802.1Q, який розглядається як зв'язок між комутаторами для забезпечення передачі трафіку, пов'язаного з більш ніж VLAN. Він підтримує трафік, що надходить з багатьох VLAN, а також трафік, що виходить не з VLAN, який вважається відповідно тегованих і немаркованих трафіком. Магістральний порт (802.1Q) направляє немаркований трафік в VLAN 1 за замовчуванням, яка відома як власна VLAN. Власні VLAN визначені для підтримки зворотної сумісності з немаркованих трафіком, звичайним для успадкованих сценаріїв LAN. Радимо встановити власну VLAN як невикористану VLAN, відмінну від VLAN 1 і інших VLAN. Він може бути виділений як фіксована VLAN для виконання ролі власної VLAN для всіх магістральних портів в коммутируемом домені.

Керуюча VLAN, налаштована для доступу до можливостей управління комутатором, розглядається як керуюча VLAN, яка за замовчуванням є VLAN1. Привласнюючи IP-адреса і маску підмережі віртуальному інтерфейсу комутатора (SVI), керуюча VLAN може створюватися і управлятися через HTTP, Telnet, SSH або SNMP. Не рекомендується вибирати VLAN 1 в якості керуючої VLAN (яка використовується за замовчуванням) через нестандартної конфігурації комутатора Cisco. У минулому керуюча VLAN для комутатора серії 2960 була єдиним активним SVI. У версіях 15.x Cisco IOS для комутаторів Catalyst 2960 можливе використання декількох активних SVI. Однак наявність декількох керуючих VLAN, які теоретично може мати комутатор, дасть можливість зловмисникам. Існує ризик, якщо власна VLAN збігається з керуючою. Отже, власна VLAN повинна відрізнятися від будь-яких інших VLAN, якщо вона використовується.

Голосові VLAN, для підтримки передачі голосу по IP (VoIP). Для VoIP-трафіку необхідно наступне:

-Забезпечення пропускна здатність для забезпечення прийнятної якості голосу

-Пріоритет передачі в порівнянні з іншими типами мережевого трафіку

Можливість маршрутизації в перевантажених областях мережі

- Менша затримка (менше 150 мс) по мережі

-Ці вимоги повинні бути виконані для підтримки VoIP.

Однак настройка цих вимог виходить за рамки даної статті, але корисно коротко обговорити, як голосова VLAN працює між комутатором, комп'ютером і IP-телефоном Cisco.

Ідентифікація VLAN

Порт на комутаторі може бути пов'язаний тільки з однієї VLAN або з усіма VLAN. Порт можна налаштувати вручну як порт доступу або магістральний порт. Нехай протокол динамічного транкинга (DTP) працює для кожного порту, щоб встановити режим порту комутатора. Це можна зробити шляхом узгодження з портом на іншому кінці каналу [11]. У комутованої мережі є два різних типи посилань:

1) Порти доступу: порт доступу зазвичай передає трафік тільки однієї VLAN. В цьому випадку трафік відправляється і приймається у власному форматі без тегів VLAN. Все, що надходить на порт доступу, просто вважається належить VLAN, призначеної цього порту. Будь-який пристрій, підключений до каналу доступу, не знає про членство в VLAN; пристрій просто приймає свою частину того ж широкомовного домену і не розпізнає фізичну топологію мережі. Пристрої Access-Link не можуть відправляти і отримувати дані від пристроїв за межами їх VLAN, якщо не налаштована маршрутизація. Він може зробити порт комутатора або портом доступу, або магістральним портом, але не обома відразу. Слід зазначити, що порт доступу може бути підключений тільки до однієї VLAN [11]

2) Магістральні порти. Магістральні порти, з іншого боку, можуть передавати кілька VLAN одночасно. Магістральний канал - це двоточковий канал зі швидкістю 100 або 1000 Мбіт / с між двома комутаторами, комутатором і маршрутизатором або навіть між комутатором і сервером, і він передає трафік декількох VLAN від 1 до 4094 одночасно. Це відмінна функціональність, тому

що порти можуть бути налаштовані так, щоб сервер одночасно знаходився в двох окремих широкомовних доменах, тому користувачам не доведеться перетинати пристрій мережевого рівня (рівень 3), щоб увійти в систему і отримати до нього доступ. Інша перевага полягає в тому, що магістральні канали можуть передавати по каналу різні обсяги даних VLAN [11].

Метод ідентифікації VLAN

Ідентифікація VLAN - це те місце, де комутатори можуть відстежувати всі кадри, коли вони проходять через коммутируемую мережу. Він визначає, як комутатори можуть визначати, які кадри належать яким VLAN, де існує більше одного методу транкинга.

1) Зв'язок між комутаторами (ISL): Зв'язок між комутаторами (ISL) - це метод, який маркує дані VLAN у фреймі Ethernet. Це маркування даних дозволяє мультиплексировать VLAN по магістралі за допомогою методу зовнішньої інкапсуляції (ISL). Фактично, вона дозволяє комутатора розпізнавати приналежність кадру до VLAN по транкові каналу. Шляхом реалізації ISL можна виконати з'єднання декількох комутаторів, зберігши при цьому інформацію про VLAN при переміщенні трафіку; між комутаторами на магістральних каналах. ISL працює на другому рівні шляхом інкапсуляції кадру даних з новим заголовком і циклічної перевіркою надмірності (CRC). Він використовується тільки для каналів Fast Ethernet і Gigabit Ethernet. Маршрутизація ISL універсальна і може використовуватися на порте комутатора, інтерфейсі маршрутизатора і інтерфейсних платах сервера для з'єднання сервера [11].

2) IEEE 802.1Q: це стандартний метод, створений IEEE для маркування кадрів, IEEE 802.1Q вставляє поле в кадр для ідентифікації VLAN. Якщо необхідно виконати транкінг між комутованих каналом Cisco і комутатором іншої марки, для роботи магістралі необхідно використовувати 802.1Q. Основна мета методів маркування кадрів ISL і 802.1Q - забезпечити зв'язок між комутаторами VLAN. Також слід зазначити, що будь-яка маркування кадру ISL або 802.1Q видаляється, якщо кадр пересилається за посиланням доступу; тегування використовується тільки для магістральних посилань [11].

2.3 Віртуальна розширена локальна мережа (VXLAN)

Тепер, коли ми дізналися, що традиційна сегментація мережі забезпечується віртуальними локальними мережами, які стандартизовані в рамках групи IEEE 802.1Q. Мережі VLAN забезпечують логічну сегментацію кордонів рівня 2 або широкомовних доменів. Однак через неефективне використання доступних мережевих каналів з використанням VLAN, жорстких вимог до розміщення пристроїв в мережі центру обробки даних і обмеженою масштабованості до 4094 VLAN, використання VLAN стало обмежуючим фактором для IT-відділів і постачальників хмарних послуг, оскільки вони будують великі мультіарендние центри обробки даних. У цьому розділі ми обговоримо стандарт VXLAN, який Cisco у співпраці з іншими провідними постачальниками запропонувала IETF як рішення мережевих проблем центру обробки даних, що створюються традиційною технологією VLAN. Стандарт VXLAN забезпечує гнучке розміщення робочих навантажень і більш високу масштабованість сегментації рівня 2, яка потрібна сьогоднішніми більшими вимогами додатків.

Переваги VXLAN. Пропонується, щоб VXLAN надавала ті ж мережеві служби Ethernet Layer 2, що і VLAN сьогодні, але з більшою гнучкістю і розширюваністю. VXLAN пропонує наступні переваги в порівнянні з VLAN :

1. Гнучке розміщення сегментів з кількома орендарями по всьому центру обробки даних дозволяє розширити сегменти другого рівня за базовою загальною мережевої інфраструктури. Таким чином, робоче навантаження клієнта може бути розподілена між фізичними модулями в центрі обробки даних.

2. Більш висока масштабованість для адресації більшої кількості сегментів другого рівня в порівнянні з VLAN, що призводить до обмеження масштабованості тільки 4094 VLAN. VXLAN використовує 24-бітний ідентифікатор сегмента, відомий як мережевий ідентифікатор VXLAN (VNID).

Це дозволяє співіснувати до 16 мільйонів сегментів VXLAN в одному адміністративному домені.

3. Краще втратити зв'язок із мережею шляхів, доступних в базовій інфраструктурі, де VLAN використовує протокол сполучного дерева для запобігання петель. Слід зазначити, що він використовує половину мережевих посилань в мережі, блокуючи надлишкові шляху. Навпаки, пакети VXLAN передаються через нижележащую мережу на основі її заголовка рівня 3 і можуть в повній мірі використовувати переваги маршрутизації рівня 3, маршрутизації по багатоколійні маршрутами з рівною вартістю (ECMP) і протоколів агрегації каналів, щоб мати можливість використовувати всі доступні шляхи. Було обговорено широке коло тем, пов'язаних з мережевою безпекою, і було надано хороше резюме проблеми мережевої безпеки. Хороші мережі повинні безперебійно працювати з іншими мережами, бути прозорими для користувачів, забезпечувати віддалений доступ і підтримувати максимальну продуктивність. З іншого боку, безпечні мережі захищають конфіденційну інформацію, забезпечують надійність і цілісність даних. Ці два виміри часто суперечать один одному [3].

VXLAN має більш високу масштабованість для адресації більшої кількості сегментів рівня 2. VLAN використовують 12-розрядний ідентифікатор VLAN для адресації сегментів рівня 2, що призводить до обмеження масштабованості тільки 4094 VLAN. VXLAN використовує 24-бітний ідентифікатор сегмента, відомий як мережевий ідентифікатор VXLAN (VNID), який дозволяє співіснувати до 16 мільйонів сегментів VXLAN в одному адміністративному домені. Тепер ми обговоримо инкапсуляцию VXLAN і формат пакета. VXLAN - це схема накладення рівня 2 в мережі рівня 3. Він використовує інкапсуляцію протоколу MAC-адрес в призначених для користувача дейтаграммах (MAC-in-UDP), щоб забезпечити засоби для розширення сегментів рівня 2 по мережі центру обробки даних. VXLAN - це рішення для підтримки гнучкої великомасштабної багатокористувацької середовища через загальну загальну фізичну інфраструктуру. Транспортний протокол у фізичній мережі центру

обробки даних - IP плюс UDP. VXLAN визначає схему інкапсуляції MAC-in-UDP, в якій до вихідного кадру рівня 2 доданий заголовок VXLAN, який потім поміщається в пакет UDP-IP. Завдяки цій інкапсуляції MAC-in-UDP VXLAN тунелює мережу рівня 2 по мережі рівня 3. VXLAN представляє 8-байтовий заголовок VXLAN, який складається з 24-бітного VNID і декількох зарезервованих бітів. Тема VXLAN разом з вихідним кадром Ethernet входить в корисне навантаження UDP. 24-бітний VNID використовується для ідентифікації сегментів рівня 2 і для підтримки ізоляції рівня 2 між сегментами. Маючи всі 24 біта в VNID, VXLAN може підтримувати 16 мільйонів сегментів LAN. VXLAN використовує пристрої VXLAN Tunnel EndPoint (VTEP) для зіставлення кінцевих пристроїв клієнтів з сегментами VXLAN і для виконання інкапсуляції і деінкапсуляціі VXLAN. Кожна функція VTEP має два інтерфейси: один - це інтерфейс комутатора в сегменті локальної мережі для підтримки локальної зв'язку кінцевих точок через міст, а інший - IP-інтерфейс для транспортної IP-мережі. IP-інтерфейс має унікальний IP-адреса, яка ідентифікує Ваш пристрій VTEP в транспортній IP-мережі, відомої як інфраструктурна VLAN. Пристрій VTEP використовує цей IP-адреса для інкапсуляції кадрів Ethernet і передає інкапсульовані пакети в транспортну мережу через IP-інтерфейс. Пристрій VTEP також виявляє віддалені VTEP для своїх сегментів VXLAN і вивчає зіставлення віддалених MAC-адрес і VTEP через свій IP-інтерфейс.

Основна IP-мережу між VTEP не залежить від накладення VXLAN. Він направляє інкапсульовані пакети на основі заголовка зовнішнього IP-адреси, в якому ініціює VTEP є вихідним IP-адресою, а завершальний VTEP - IP-адресою призначення.

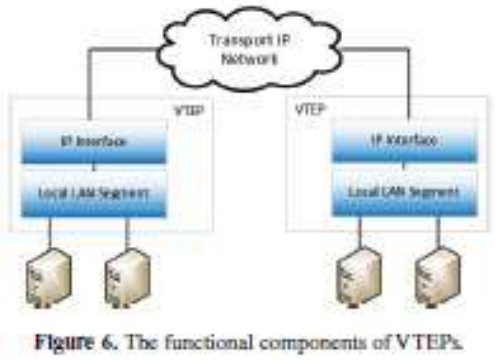

Figure 6. The functional components of VTEPs.

Рис.2.1. Функціональні компоненти VTEP.

2.4 Мережеві атаки та методи захисту від них на VLAN

З розвитком технологій зростає і потреба в мережевої безпеки. Це пов'язано з тим, що розвиток технологій також збільшує доступність широкого спектру інструментів злому. Ці хакерські інструменти використовуються в різних типах мереж, наприклад, в глобальній і локальної мережі. Хоча VLAN важлива для підтримки гнучкості мережі [11], вона також піднімає проблеми безпеки, оскільки корпорації зберігають важливі дані, які передаються за допомогою VLAN. Питання мережевої безпеки в VLAN дуже важливі і повинні бути розглянуті, обговорені та проаналізовані. Тут ми розглянемо деякі з найбільш поширених мережевих атак на VLAN. Атаки з використанням підміни протоколу дозволу адрес (ARP): підміна ARP, отруєння кешу ARP або отруєна маршрутизація ARP - це метод, за допомогою якого зловмисник відправляє (підміняє) повідомлення протоколу дозволу адрес (ARP) в локальну мережу. Основна мета зловмисника - зв'язати свій MAC-адресу з IP-адресою іншого вузла, наприклад, шлюзу. Отже, зловмисник може замість цього відправити зловмисникові будь-який трафік, призначений для цього конкретного IP-адреси. Як показано на малюнку 3, зловмисник відправляє підроблені пакети, IP-адреса яких аналогічний вихідного IP-адресою, серверу, який стверджує, що він є справжнім хостом. Коли сервер отримує пакет і вважає MAC-адресу зловмисника передбачуваним місцем призначення для пакетів, оскільки

зловмисник використовує IP-адреса, аналогічний вихідного хосту, він замість цього починає відправляти дані зловмисникові. Зловмисник може отримати дані, призначені для справжнього одержувача. Підміна ARP може дозволити зловмиснику перехопити фрейми даних в мережі, змінити трафік або зупинити весь трафік .

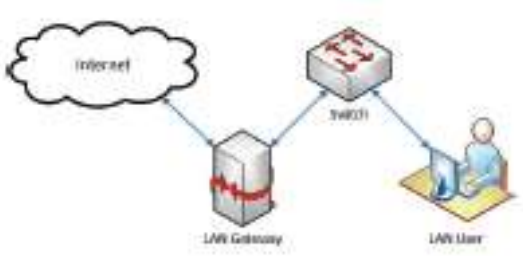

Рис.2.2. Маршрутизація при нормальній роботі

Перемикання LAN: перемикання VLAN розглядається як вразливість комп'ютерної безпеки, коли зловмисник може атакувати мережеві ресурси в VLAN. Основна концепція всіх цих видів атак полягає в тому, щоб атакуючий хост в VLAN отримав доступ до трафіку в інших VLAN, які не повинні бути доступні.

Рис.2.3. Приклад атаки ARP із зловмисним користувачем

При атаці з перескоком VLAN зловмисник буде відправляти тегованих пакети з ідентифікатором VLAN цільової VLAN. Потім перевіряється ідентифікатор VLAN, і пакет передається в цільову VLAN. На рис.2.4 зловмисник атакує VLAN через магістраль мережі. Пакет, який надійшов зловмисником, буде містити ідентифікатор VLAN цільової VLAN.

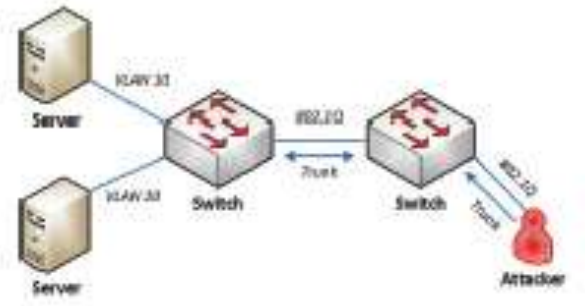

Рис.2.4. Атака VLAN через магістраль мережі.

MAC-лавинна розсилка: MAC-лавинна розсилка - це метод, реалізований для змови з безпекою мережевих комутаторів. У цій атаці зловмисник відправить безліч різних підроблених MAC-адрес джерела. Мета зловмисника - використовувати обмежену пам'ять, виділену в комутаторі, для зберігання таблиці MAC-адрес. Потім трафік переповнюється і стає доступним, оскільки комутатор не може зберігати в пам'яті конкретну адресу призначення. Оскільки трафік переливається, зловмисник може просто побачити генерований трафік і отримати інформацію. На рис. 2.5. показано, як зловмисник відправляє комутатора різні MAC-адреси з наміром обмежити таблицю MAC-адрес комутатора.

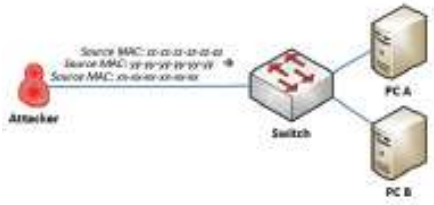

Рис.2.5. Затоплення MAC-адреси

Статичні записи ARP: одним з методів запобігання мережевих атак є використання статичних записів ARP в таблиці ARP на комутаторі. Зіставлення

IP-адрес і MAC-адрес в локальному кеші ARP можна вводити статично, щоб вузли відхиляли відповідні пакети ARP. Хоча статичні записи забезпечують деякий захист від атак з підміною ARP, це вимагає великих зусиль з обслуговування, оскільки зіставлення адрес всіх систем в мережі повинні виконуватися статично по одній. Запис статичного протоколу дозволу адрес (ARP) - це постійний запис в кеші ARP. Статичної записом ARP можна керувати за вузла / пристрої або з робочої станції. Він не використовується регулярно при нормальних обставинах, однак він використовується, коли необхідно додати або видалити запис з кеша. Наступна команда може використовуватися для додавання статичної записи кеша ARP:

```
C:\>arp -s 192.168.1.17 6c-fc-03-a3-7f-81
```

Команда arp створює статичну запис в кеші ARP, щоб запустити сеанс зв'язку з вузлом, що має IP-адресу 192.168.1.17, немає необхідності запускати процес із запитом ARP, оскільки MAC-адресу цільового вузла вже відомий. Якщо аналогічна запис ARP не було додано до цільового вузла / хосту, цільової хост повинен відправити запит ARP на комп'ютер, щоб дізнатися MAC-адресу. Після додавання статичної записи ARP кеш ARP на комп'ютері може виглядати наступним чином:

```
C:\>arp -a
Interface: 192.168.1.137 --- 0x50006
Internet Address   Physical Address   Type
192.168.1.17       6c-fc-03-a3-7f-81  static
192.168.1.254      77-d8-e5-f2-43-6d  dynamic
```

З'єднання з вузлом за адресою 192.168.1.17 підтримується до тих пір, поки не зміниться MAC-адресу цільового комп'ютера, що може бути пов'язано зі зміною мережевої карти або, можливо, через операцію, що змінює MAC-адресу. В цьому випадку необхідно видалити неприпустиму запис ARP за допомогою команди arp -d, наприклад arp -d 192.168.1.17. Маршрутизатор Cisco зберігає записи ARP в кеші протягом чотирьох годин (240 хвилин), в той час як робочі станції Windows можуть зберігати не більше десяти хвилин. Це звичайне явище для маршрутизаторів, оскільки вони, як правило, проводять більшу частину

свого часу, працюючи з одними і тими ж вузлами. Маршрутизатор зазвичай налаштовується як шлюз для пристроїв мережі, тому вони бачать, що одні й ті ж вузли обмінюються даними з ним більшу частину часу протягом дня, і поки ці вузли продовжують відправляти дані через маршрутизатор, вони будуть залишаються в кеші ARP. Для маршрутизатора, підключеного до великих сегментах мережі, це призведе до досить великим списком ARP або таблиці ARP. Велика частина пам'яті маршрутизатора буде зайнята великою таблицею ARP, тому час кешування, яке вибрала Cisco, було результатом використання пам'яті кешем ARP в порівнянні з потребою ARP в свіжої інформації MAC. Щоб створити статичну запис ARP для маршрутизатора, це можна зробити, увійшовши в режим глобальної конфігурації, який команда arp виглядає наступним чином:

```
#arp 192.168.1.17 6cfc.03a3.7f81 arpa
```

Після введення цієї команди кеш ARP буде містити пару IP-MAC-адрес, які не будуть застарівати з кеша. Це видно по тире в стовпці «Вік». Статичні записи ARP зазвичай не розпізнаються інтерфейсом, як динамічні записи.

```
Router\#show arp

Prot. Address      Age(min) Hardware Addr   Type
Int.  192.168.1.1     -     0050.43bf.7c82  ARPA
Int.  192.168.1.17    -     6cfc.03a3.7f81  ARPA
```

Якщо запис більше не потрібна або її потрібно змінити на щось ще, команда no arp видаляє початковий запис:

```
Router(config)\#no arp 192.168.1.17
```

Якщо два вузла постійно обмінюються даними один з одним протягом дня, буде додано статичний ARP. Додаючи статичні записи ARP для обох систем в кеш ARP один одного, можна зменшити деякі мережеві накладні витрати у вигляді запитів ARP і відповідей ARP. Це також добре для запобігання атак лавинної розсилки, коли кеш ARP переповнюється випадковими записами. Статичний ARP може допомогти визначити, які записи дозволені, а які слід відкинути.

Вхідна фільтрація: використання входить фільтрації - це метод забезпечення того, щоб вхідні пакети дійсно приходили з мереж, які, за їх твердженням, виходять. Комутатор налаштований з вхідною фільтрацією, щоб приймати тільки дозволені пакети. Будь-маршрутизатор, який застосовує входить фільтрацію, перевіряє поле IP-адреси джерела одержуваних IP-пакетів, і якщо пакети не мають IP-адреси в блоці IP-адрес, пакети будуть відкинуті. Однак адреси можуть бути підроблені, і входить фільтрація все одно буде приймати пакети, якщо зловмисник буде використовувати ту ж адресу, дозволений вхідний фільтрацією [20]. Вхідна фільтрація - це підтвердження того, надходять чи вхідні пакети в мережу з джерела, від якого, за їхніми твердженнями, до того, як буде дано вхід (або вхід), чи ні.

Він використовує можливість фільтрації IP-адрес другого рівня маршрутизатора на кордоні мережі, і, якщо висока ймовірність того, що він є шкідливим, трафік буде заблокований. У найпростішому випадку входить фільтрація включає створення списку управління доступом. Цей список містить IP-адреси дозволених вихідних адрес. І навпаки, список управління доступом також може використовуватися для блокування адрес заборонених джерел. Наступні вихідні IP-адреси будуть блокуватися входить фільтрацією:

• Уже використовується IP-адреса, IP-адреса у внутрішній мережі. Блокуючи вихідний IP-адреса, зловмисник може підмінити внутрішній IP-адреса, щоб скористатися погано написаним правилом брандмауера.

• Приватні IP-адреси. Блокуючи ці адреси, можна запобігти шкідливий трафік, що надходить з неправильно налаштованого хоста в Інтернеті або з підробленого адреси зловмисника.

• петльові IP-адреси. Якщо петля підроблена, це допомагає запобігти цей тип трафіку.

• адреси під LGPL. Блокування багатоадресних адрес може допомогти запобігти небажаному багатоадресний трафік, який здається спамом.

• IP-адреси мережі обслуговування або управління. Зловмисник не має права використовувати загальнодоступний Інтернет для отримання

несанкціонованого доступу до мережних служб, що працюють на рівні мережевих додатків і вище. Трафік з певних регіонів світу може бути внесений в білий список адміністратором мережі і може бути внесений до чорного списку, щоб заборонити конкретному регіону доступ до свого середовища. Можна знайти деякі безкоштовні послуги на основі передплати для створення списків контролю доступу для мережевих прикордонних маршрутизаторів.

ВИСНОВКИ ДО РОЗДІЛУ 2

Оскільки технології щодня розвиваються і поліпшуються швидкими темпами, розробляються нові методи управління мережею цих технологій. Оскільки по всьому світу існують мільйони мереж, одним із спеціальних методів управління цими мережами є створення логічної адресації. Одним із способів управління мережами є створення фізичного способу адресації, який називається локальною мережею (LAN). Щоб вирішити проблему з обробкою безлічі мереж, була створена логічна адресація, при якій компоненту потрібно було тільки знаходитися в одній підмережі для взаємодії один з одним. У зв'язку з широким використанням VLAN виникає проблема безпеки мережі, а також масштабованості та управління мережею, які обговорювалися в цій статті. Оскільки конфіденційні дані передаються по мережі, існує кілька ризиків і загроз для мережі. Мережі VLAN можуть мінімізувати цю загрозу, розміщуючи тільки тих користувачів, які мають доступ до мережевих даними в мережі VLAN, у якій є доступ. Це знизить шанси доступу зловмисника. З впровадженням VLAN ми також можемо контролювати широкомовні домени, налаштовувати міжмережеві екрани, забороняти доступ і попереджати адміністратора мережі в разі атаки сторонньої особи. У цій статті ми можемо зробити висновок, що використання віртуальних локальних мереж, безумовно, може спростити управління мережею, а також забезпечити мережі з підвищеною безпекою.

РОЗДІЛ 3
КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ ВІРТУАЛЬНОЇ ЛОКАЛЬНО-ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ

3.1 Обґрунтування вибору середовища комп'ютерного моделювання

VLAN (віртуальна LAN) - це підмережа, яка може групувати набори пристроїв в окремих фізичних локальних мережах (LAN). ЛВС - це група комп'ютерів і пристроїв, які спільно використовують лінію зв'язку або бездротової канал зв'язку з сервером в одній і тій же географічній області.

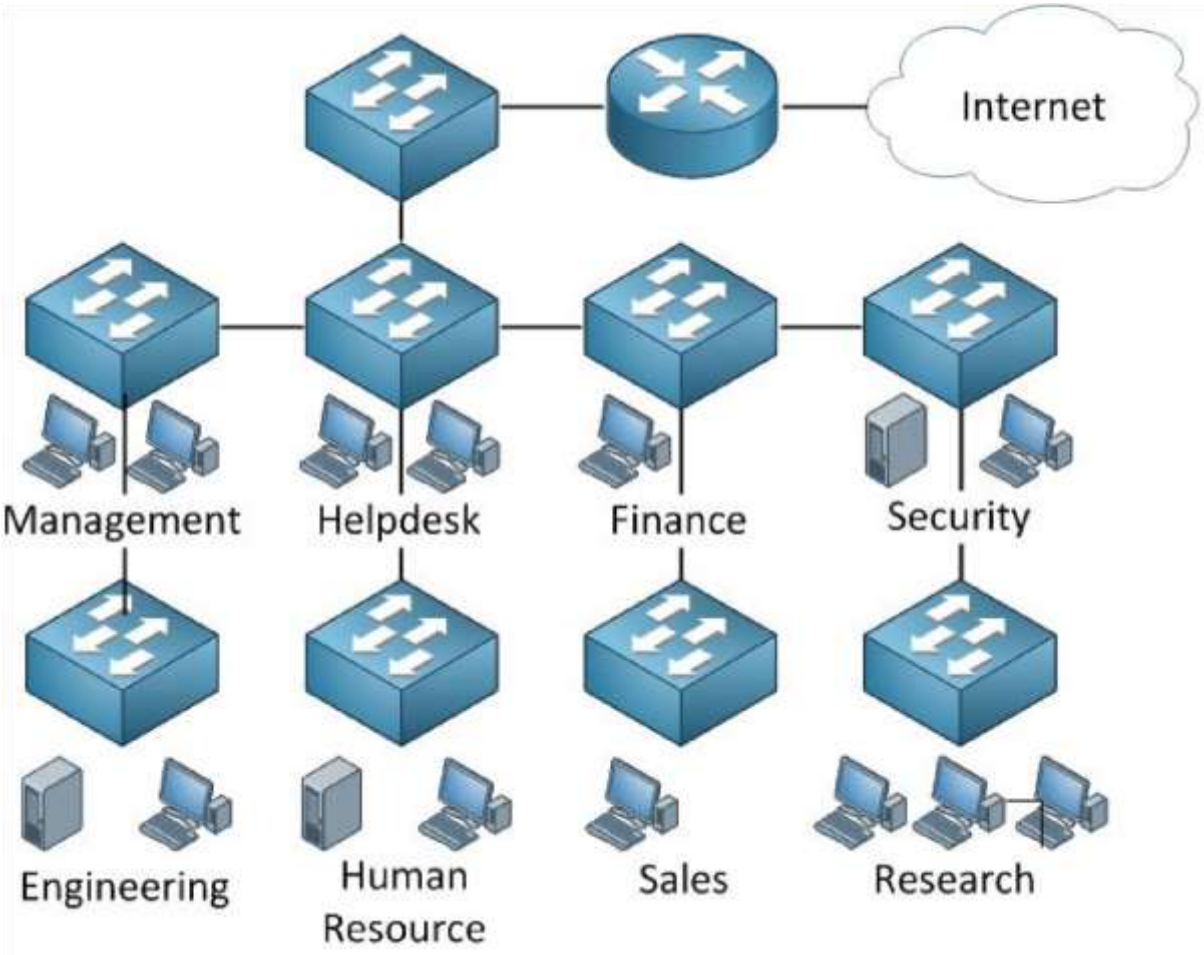

Рис. 3.1. огляд VLAN

VLAN також важливі, тому що вони можуть допомогти поліпшити загальну продуктивність мережі за рахунок угруповання пристроїв, які

обмінюються даними найбільш часто. VLAN також забезпечують безпеку в більших мережах, дозволяючи в більшій мірі контролювати, які пристрої мають доступ один до одного. Мережі VLAN мають тенденцію бути гнучкими, оскільки вони засновані на логічних з'єднаннях, а не на фізичних.

Типи VLAN включають засновані на протоколі, статичні і динамічні VLAN.

Протокольна VLAN - трафік, що обробляється на основі її протоколу. Комутатор буде розділяти або пересилати трафік на основі протоколу трафіку.

Статична VLAN, також звана VLAN на основі портів, вимагає, щоб адміністратор мережі міг призначити порти на мережевому комутаторі віртуальної мережі; Бувай:

Динамічна VLAN - дозволяє адміністратора просто визначати членство в мережі на основі характеристик пристрою, а не розташування порту комутатора.

Порти (інтерфейси) на комутаторах можуть бути призначені одній або декільком VLAN, що дозволяє розділяти системи на логічні групи - залежно від того, з яким відділом вони пов'язані - і встановлювати правила про те, як системам в окремих групах дозволено зв'язуватися з один з одним . Ці групи можуть варіюватися від простих і практичних (комп'ютери в одній VLAN можуть бачити принтер в цій VLAN, але комп'ютери поза цією VLAN не можуть) до складних і законних (наприклад, комп'ютери у відділах роздрібного банку не можуть взаємодіяти з комп'ютерами в цій VLAN). торгові відділи.

Кожна VLAN забезпечує доступ до каналу даних для всіх хостів, підключених до портів комутатора, налаштованим з одним і тим же ідентифікатором VLAN. Тег VLAN - це 12-бітове поле в заголовку Ethernet, що забезпечує підтримку до 4096 VLAN на домен комутації. Маркування VLAN стандартизована в IEEE (Інститут інженерів з електротехніки та електроніки) 802.1Q і часто називається Dot1Q.

Коли нетегірованний кадр отриманий від підключеного хоста, тег VLAN ID, налаштований на цьому інтерфейсі, додається в заголовок кадру каналу даних з використанням формату 802.1Q. Потім кадр 802.1Q пересилається до

місця призначення. Кожен комутатор використовує тег для відділення трафіку кожної VLAN від інших VLAN, перенаправляючи його тільки туди, де налаштована VLAN. Магістральні канали між комутаторами обробляють кілька VLAN, використовуючи тег для їх поділу. Коли кадр досягає порту комутатора призначення, тег VLAN видаляється перед передачею кадру на пристрій призначення.

Кілька VLAN можуть бути налаштовані на одному порте з використанням конфігурації магістралі, в якій кожен кадр, що відправляється через порт, позначений ідентифікатором VLAN, як описано вище. Інтерфейс сусіднього пристрою, який може знаходитися на іншому комутаторі або на хості, що підтримує тегування 802.1Q, повинен буде підтримувати конфігурацію режиму магістралі для передачі і прийому тегованих кадрів. Будь-які немарковані кадри Ethernet призначаються VLAN за замовчуванням, яку можна вказати в конфігурації комутатора.

Коли комутатор з підтримкою VLAN отримує немаркований кадр Ethernet від підключеного хоста, він додає тег VLAN, призначений вхідного інтерфейсу. Кадр пересилається на порт хоста з MAC-адресою призначення (адреса управління доступом до середовища). Широкомовне, невідома одноадресная і многоадресная розсилка (трафік BUM) пересилається на всі порти в VLAN. Коли раніше невідомий хост відповідає на невідомий одноадресний кадр, комутатори дізнаються розташування цього хоста і не розсилають наступні кадри, адресовані цьому хосту.

Таблиці комутації-переадресації оновлюються двома механізмами. По-перше, старі записи пересилання періодично видаляються з таблиць пересилання, часто за допомогою настроюваного таймера. По-друге, будь-яка зміна топології призводить до скорочення таймера поновлення таблиці пересилання, запускающему оновлення.

Протокол зв'язуючого дерева (STP) використовується для створення топології без петель між комутаторами в кожному домені рівня 2. Можна використовувати екземпляр STP для кожної VLAN, що дозволяє

використовувати різні топології рівня 2, або можна використовувати STP з декількома екземплярами (MISTP) для зменшення накладних витрат STP, якщо топологія однакова для кількох VLAN. STP блокує пересилання по посиланнях, які можуть створювати петлі пересилання, створюючи сполучна дерево з обраного кореневого комутатора. Це блокування означає, що деякі посилання не будуть використовуватися для пересилання до тих пір, поки збій в іншій частині мережі не змусить STP зробити посилання частиною активного шляху пересилання.

На малюнку вище показаний домен комутатора з чотирма комутаторами і двома віртуальними локальними мережами. Комутатори підключені по кільцевій топології. STP переводить один порт в стан блокування, так що формується деревоподібна топологія (т. Е Петлі пересилання відсутні). Порт на комутаторі D до комутатора C заблокований, на що вказує червона смуга на засланні. Канали між комутаторами і маршрутизатором є транкінговими VLAN 10 (помаранчевий) і VLAN 20 (зелений). Хости, підключені до VLAN 10, можуть обмінюватися даними з сервером O. хости, підключені до VLAN 20, можуть обмінюватися даними з сервером G. Маршрутизатор має підмережа IPv4, налаштовану в кожної VLAN, щоб забезпечити можливість підключення для будь-яких комунікацій між двома VLAN.

Для створення комп'ютерної моделі обрано оточення Cisco Packet Tracer [10]. Cisco Packet Tracer – симулятор мережі передачі даних, що створений фірмою Cisco Systems. Який позволяє створювати робочі моделі мережі, налаштовувати маршрутизатори і комутатори, і перевіряти взаємодію між кількома користувачами (через хмару).

У цьому варінті взяті серії маршрутизаторів Cisco 800, 1800, 1900, 2600, 2800, 2900 і комутаторів Cisco Catalist 2950, 2960, 3560, і міжмережевий екран ASA 5505. Бездротові прилади показані маршрутизатором Linksys WRT300N, точками доступу і стільниковими вишками. Окрім того є сервери DHCP, HTTP, TFTP, FTP, DNS, AAA, SYSLOG, NTP і EMAIL, робочі станції, відмінні модулі до комп'ютерів та маршрутизаторів, IP-фони, смартфони, хаби. З'єднувати

мережеві прилади можна задопомогою різноманітних типів кабелів, отаких як прямі і зворотні, оптичні та коаксіальні кабелі, послідовні кабелі та телефонні пари.

Успішно позволяє зробити навіть складні макети мереж, перевірити їх на працездатність топології. Однак, потрібно звернути увагу, що реалізований функціонал приладів обмежений і має можливості надає весь функціонал реального обладнання. Cisco Packet Tracer є в безкоштовному доступі для учасників Програми Мережевої Академії Cisco.

Програмне рішення Cisco Packet Tracer позволяє імітувати функціонал різноманітних мережевих приладів: маршрутизаторів, комутаторів, точок бездротового доступу, персональних комп'ютерів, мережевих принтерів, IP-телефонів і т.д. Робота з інтерактивним симулятором дає дуже близьке відчуття налаштування справжньої мережі, що має в складі десять або навіть кілька сотень приладів. Налаштування, залежать від характеру прилада: деякі можна налаштувати задопомогою команд операційної системи Cisco IOS, а інші – за допомогою графічного веб-інтерфейсу, і також – через командний рядок операційної системи або графічні меню.

Задопомогою такії властивості Cisco Packet Tracer у режимі візуалізації позволяє користувачу простежити перебіг даних у мережі. Зокрема, з'явлення і переміну параметрів IP-пакетів при проходженні даних через мережеві прилади, швидкість і шляхи перебігу IP-пакетів. Аналіз подій, що здійснюються в мережі, позволяє зрозуміти механізм її роботи і знайти проблеми.

Також, за сприянням Cisco Packet Tracer користувач має моливість симулювати створення не тільки логічної, але й фізичної моделі мережі і, отже, здобути навички проектування. Схему мережі також можна накласти на реально існуючу будову або навіть міста і спланувати всю його кабельну проводку, розташувати прилади в будівлях і приміщеннях з враховуванням їх фізичних обмежень, таких як довжина і тип кабелю або радіус зони покриття бездротової мережі.

Cisco Packet Tracer має можливість використання не тільки як симулятора, але і як мережевий застосунока для створення симуляції віртуальної мережі через реальну мережу, в тому числі Інтернет. Користувачі ріноманітних комп'ютерів, неважливо від їх розташування, мають можливість працювати над однією мережевий топологією, витворяючи її налаштування або усуваючи дефект. Цей функціонал Cisco Packet Tracer широко використовується для організації командної праці, а також для проведення ігор та змагань між учасниками які віддалені один від одного.

Багатокористувацький режим, симуляція, візуалізація і можливість створення роблять Cisco Packet Tracer унікальним інструментом для вивчення мережевих технологій. Програма розповсюджується безкоштовно, але доступна тільки зареєстрованим користувачам і інструкторам Мережевих академій Cisco. Крім перерахованих функцій, в Cisco Packet Tracer є можливості, створені саме для викладачів. А саме – режим автоматичного перевірки проведення лабораторних робіт. Завдання інструктора – створити завдання або використати вже розроблені навчальними шаблонами, а висновок автоматично проконтролює сама програма. Особливо програма Cisco Packet Tracer незамінна під час лекцій, так як дає можливість, будучи в класі, показати як саме поведе себе мережеве приладдя. Якщо до стравжнього обладнання важко знайти доступ в лабораторних цілях, а робота потребує проведення досліду і застосування великого числа мережевих приладів, віртуальні можливості Cisco Packet Tracer легко виконують завдання, що стоять перед інструкторами.

Cisco Packet Tracer не має можливості замінити досвід праці в реальній мережі, але, данна програма здатна полегшити процес викладання і зробити його більш ефективним, і також зробити вивчення мережевих технологій в захоплюючий процес, який доступний в будь-якому місці і часу.

3.2 Визначення елементів віртуальної локально-обчислювальної мережі та побудова віртуальної локальної мережі

Створення віртуальної локально-обчислювальої мережі в колі Cisco Packet Tracer розглянемо на зразку 7 персональних комп’ютерів (див. рис. 3.2).

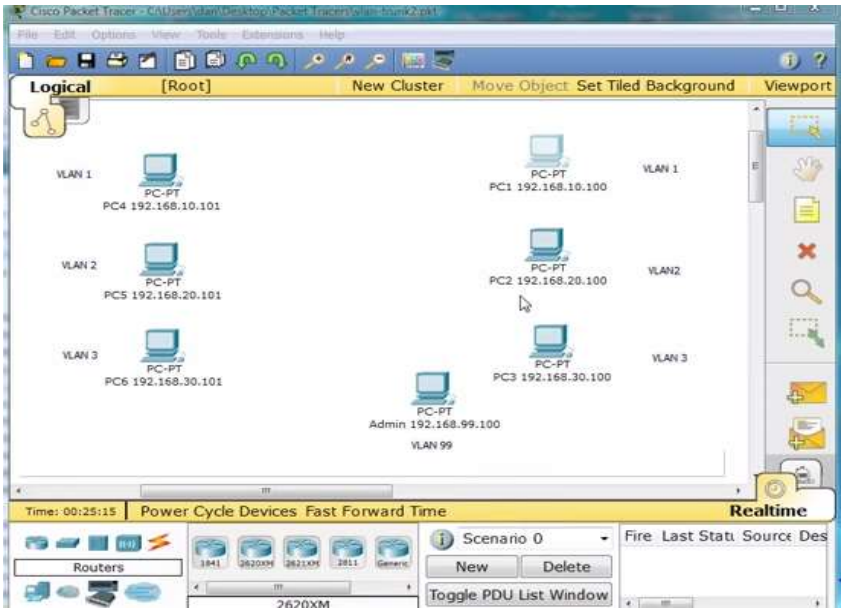

Рис. 3.2. Робоче поле Cisco Packet Tracer

На рис. 3.1 видно, що є головний комп’ютер(адмін), і ще 6 компютерів в 3-ьох різних лабараторіях, в кожного з комп’ютерів є своя IP адреса. Заплановано здійснити такі з’єднання:

192.168.10.101 з 192.168.10.100 (VLAN1);

192.168.20.101 з 192.168.20.100 (VLAN2);

192.168.30.101 з 192.168.30.100 (VLAN3).

При цьому планується поєднати всі комп’ютери задопомогою трьох комутаторів, а саме (див. рис. 3.3):

Switch 0;

Switch1;

Switch2).

Мережевий комутатор – прилад, що має призначення для поєднання декількох вузлів комп’ютерної мережі в межах одного або декількох сегментів мережі. Комутатор робить на канальному (другому) рівні моделі OSI. Комутатори були створені з застосовуванням мостових технологій і часто

роздивляються як багатопортові мости. Для поєднання декількох мереж на основі мережного рівня служать маршрутизатори (3 рівень OSI) [1].

На переміну від концентратора (1 рівень OSI), який проводить трафік від одного підключеного пристрою до всіх інших, комутатор доводить дані тільки самому одержувачу (виключення є лише широкомовний трафік всіх вузлів мережі і трафік для приладів, для яких невідомий вихідний порт комутатора). Це збільшує продуктивність і безпеку мережі, відбираючи інші сегменти мережі від потрібності (і можливості) обробляти дані, які їм не призначалися [1, 2].

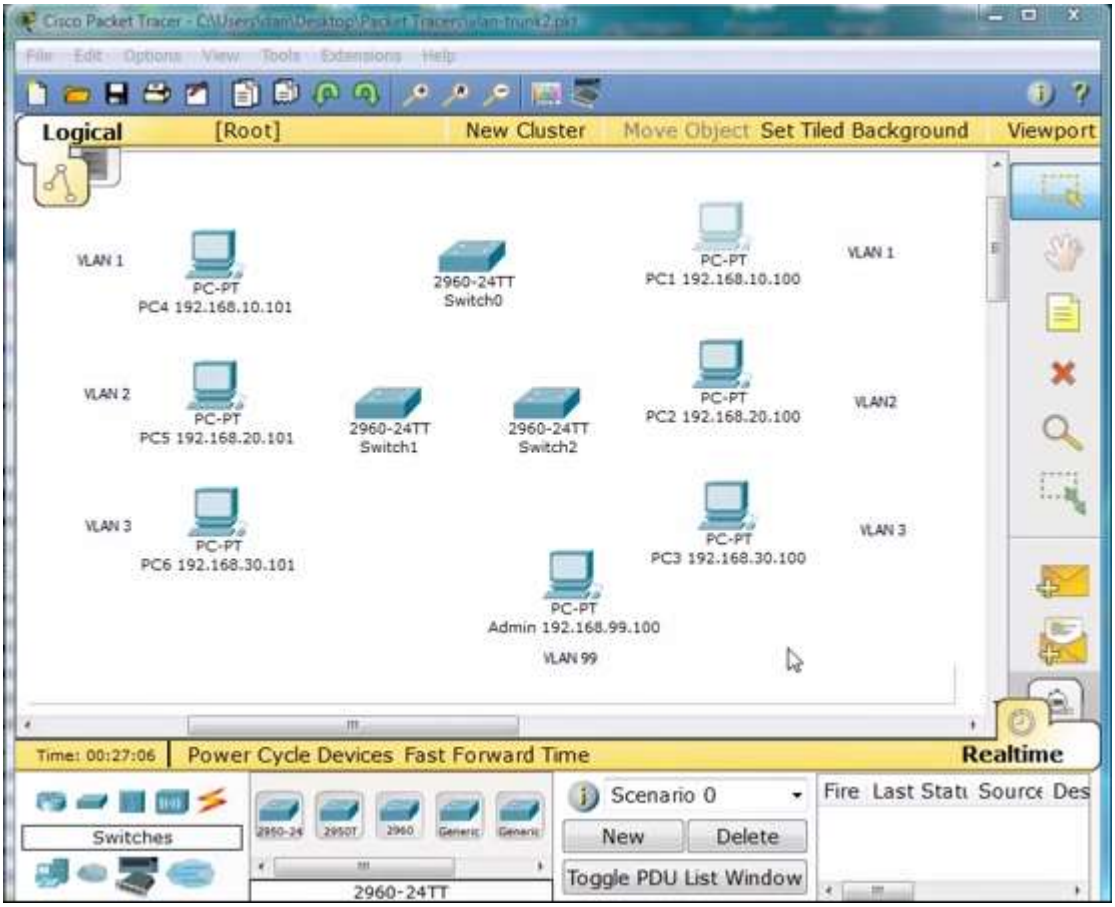

Рис. 3.3. Зразок використання комутаторів

Правило роботи комутатора [1]

Комутатор береже в пам’яті (асоціативної пам’яті) таблицю комутації, в якій записуються відповідність MAC-адреси вузла порту комутатора. При включанні комутатора ця таблиця пуста і він робить в режимі навчання. В цьому режимі приходять на якийсь порт дані, що прийдуть на всі інші порти

комутатора. При цьому комутатор аналізує фрейми (кадри) і, встановивши MAC-адресу хоста-відправника, записує його в таблицю на певний час. Потім, якщо на якийсь з портів комутатора прийде кадр, який прикріплений для хоста, MAC-адресу якого вже є в таблиці, то цей кадр буде поданий тільки через порт, записаний в таблиці. Якщо MAC-адресу хоста-одержувача не записаний з яким-небудь портом комутатора, то кадр буде передано на всі порти, за виключенням того порту, з якого він був одержаний. З часом комутатор створює таблицю для всіх діяльних MAC-адрес, в наслідку трафік локалізується. Варто також зазначити малу латентність (затримку) і велику швидкість передавання на кожному порту інтерфейсу.

З огляду на це, під'єднаємо комутатори між собою за сприянням витої пари, типу перехресний кабель (crossover cable) (див. рис. 3.4).

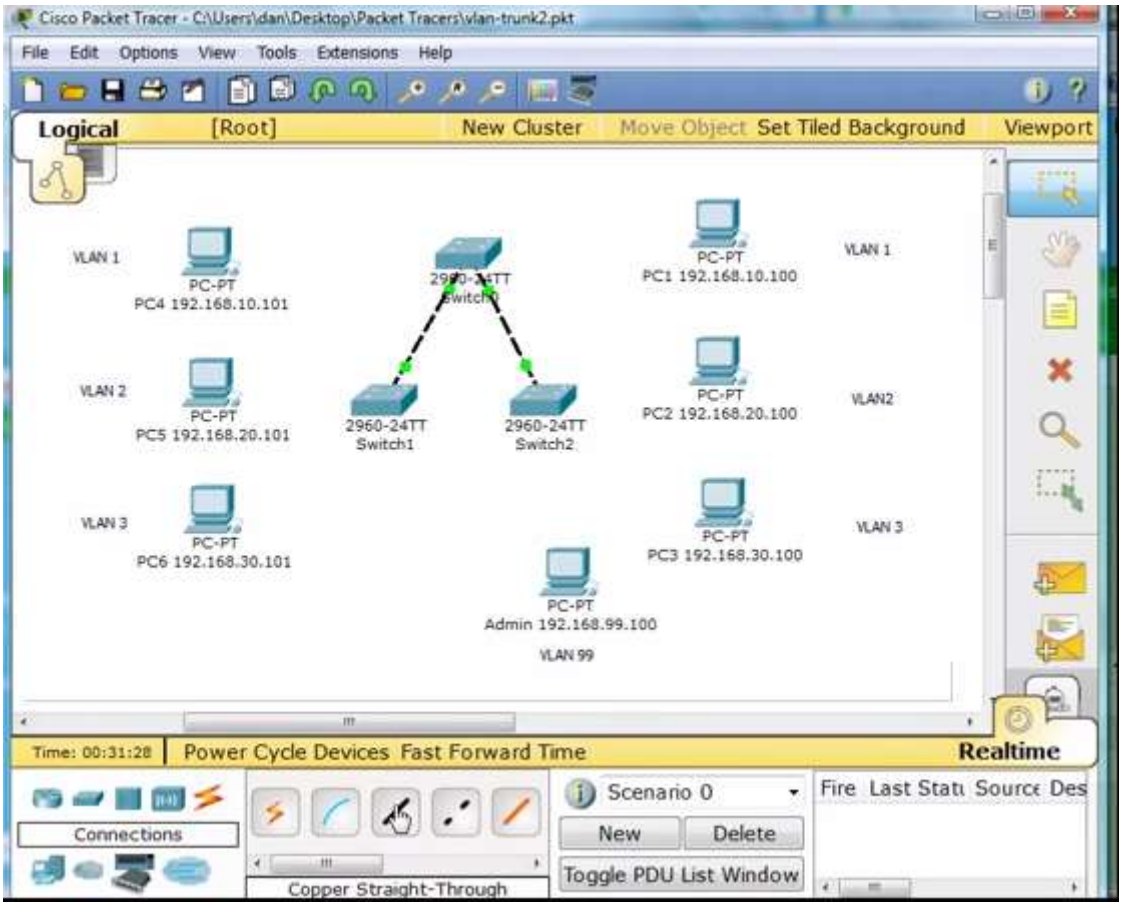

Рис. 3.4. Зразок з'єднання комутаторів

Вита пара (англ. Twisted pair) – тип кабелю зв’язку, що являє собою одну або кілька пар ізольованих провідників, скручених між собою (з невеликим числом витків на одиницю довжини), покритих оболонкою [2, 3].

Вита пара – один з компонентів нових структурованих кабельних систем. Використовується в телекомунікаційних мережах як фізичне коло передачі сигналу та підтримується багатьма технологіями, а саме [3]: Ethernet, Arcnet і Token ring.

Перехресний кабель (crossover cable) [10]

Створений для сполучення однотипного обладнування (зразок, комп’ютер-комп’ютер). Однак більшість новітніх мережевих приладів здатне автоматично встановити метод сполучення кабелю і підлаштуватися під нього (Auto MDI / MDI-X).

Далі об’єднуємо всі комп’ютери з комутаторами за сприянням витої пари різновидом прямий кабель (straight through cable) (див. рис. 3.5).

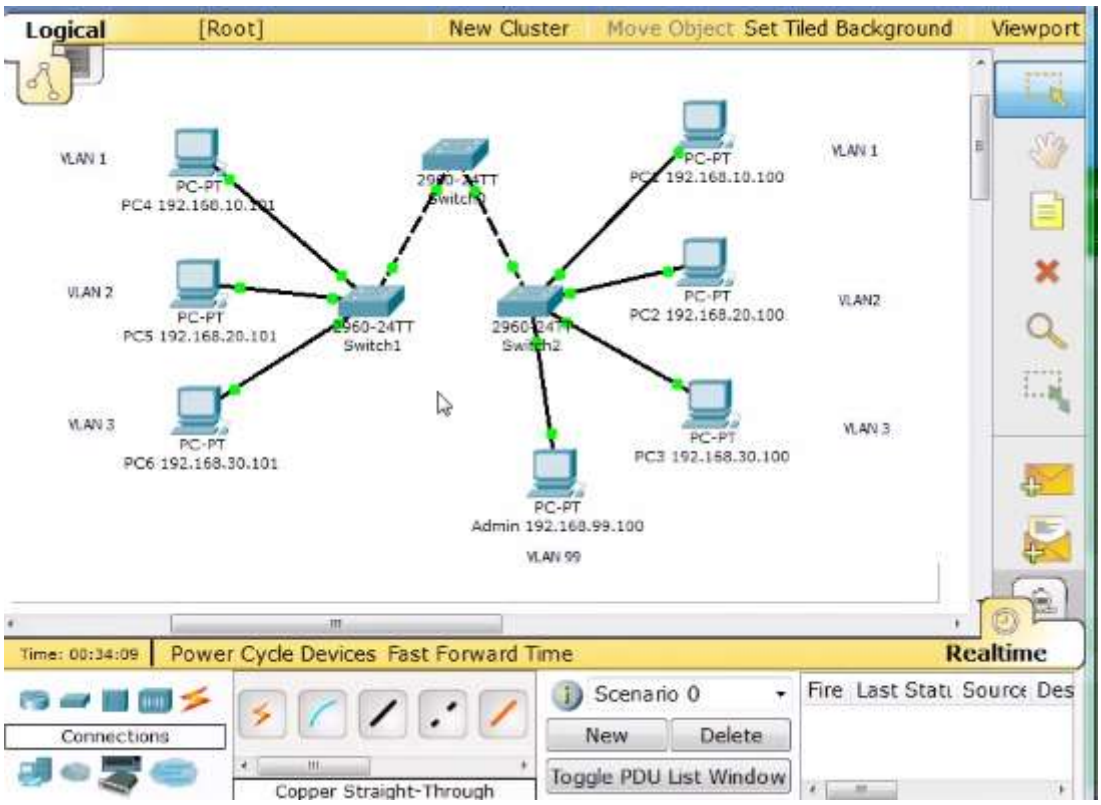

Рис. 3.5. Зразок підключення комп’ютерів до комутаторів

Таким чином, визначені всі складники, що потрібні для виробництва віртуальної локально-обчислюванної мережі.

Розглянемо налаштування віртуальної локально-обчислювальної мережі за конфігурацією на рис. 3.4. Так, комутатор 0 до комутатора 1 під'єднано за сприянням перехресного кабелю до Fast Ethernet 0/1 на обох їх порті. Тоді як при під'єднання комутатора 0 до комутатора 2 узято Fast Ethernet 0/2 на комутаторі 0 та Fast Ethernet 0/1 на комутаторі 2. Виходить що , за інтерфейсом Fast Ethernet 0/1 під'єднано порти на комутаторах 1 та світча 2, а також Fast Ethernet 0/1 і Fast Ethernet 0/2 на портах комутатора 0.

Далі під'єднуючи компютер PC1 до світча 2 оббираємо порт з інтерфесом Fast Ethernet 0/6 на комп'ютері. На PC2 – Fast Ethernet 0/11. На PC3 – Fast Ethernet 0/18. Також під'єднуємо Admin PC до комутатора 2 й беремо порт з Fast Ethernet 0/24 на компютері. За аналогією ми під'єднуємо PC4, PC5, PC6 до комутатора 1. Після того як налаштування компонентів мережі виконано, перейдемо до виготовлення віртуальної локально-обчислювальної мережі.

Розпочнемо з написання налаштувань для комутатора 0. Для цього вибираємо вкладку CLI (Command Line Interface). Спочатку, налагоджуємо VLAN 99.(див рис. 3.6). Даємо значення йому Native VLAN, тобто це значитиме, що всі кадри які назначає VLAN на комутаторі ідуть без тега. Тоді трафік перейде не тегованим. Якщо комутатор здобуває такі кадри на транковому порту, він автоматично вписує їх до Native VLAN. І також кадри, які створюються з не розподілених портів, при дохоженні в транк-порт записуються до Native VLAN.

Трафік, який припадає іншим VLANам, тегується із значенням відповідного VLAN ID всередині тега. Далі налагоджуємо інші три VLAN.

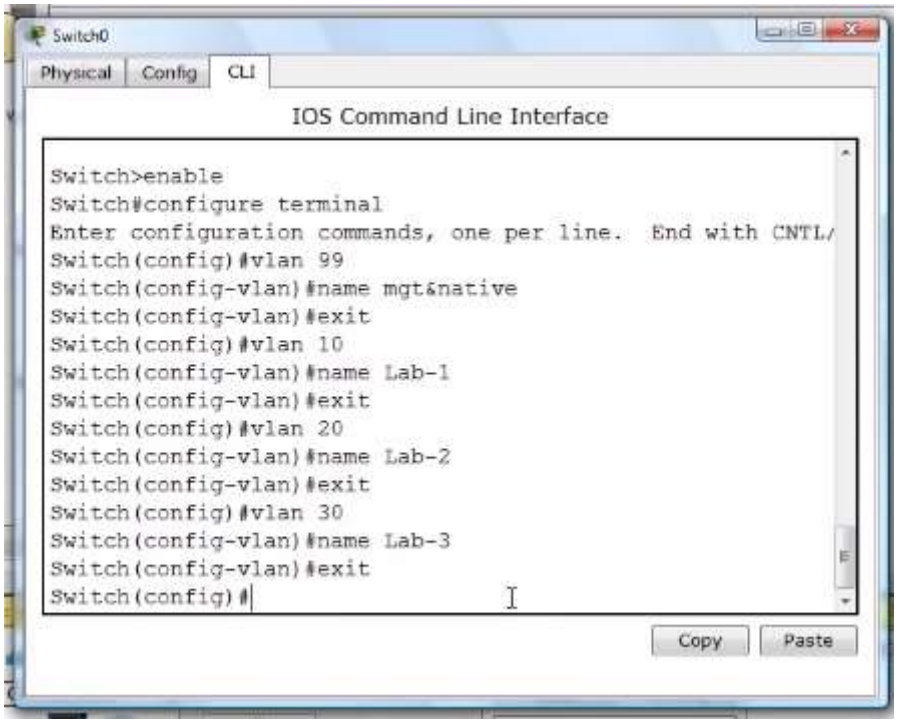

Рис. 3.6. Зразок налаштування VLAN

Далі за допомогою рядка «#copy running-config startup-config» зберігаємо налаштування й запускаємо їх. Після цього за допомогою «#show vlan brief» отримуємо інформацію про про VLAN і порти, які до них під'єднані (див. рис. 3.7).

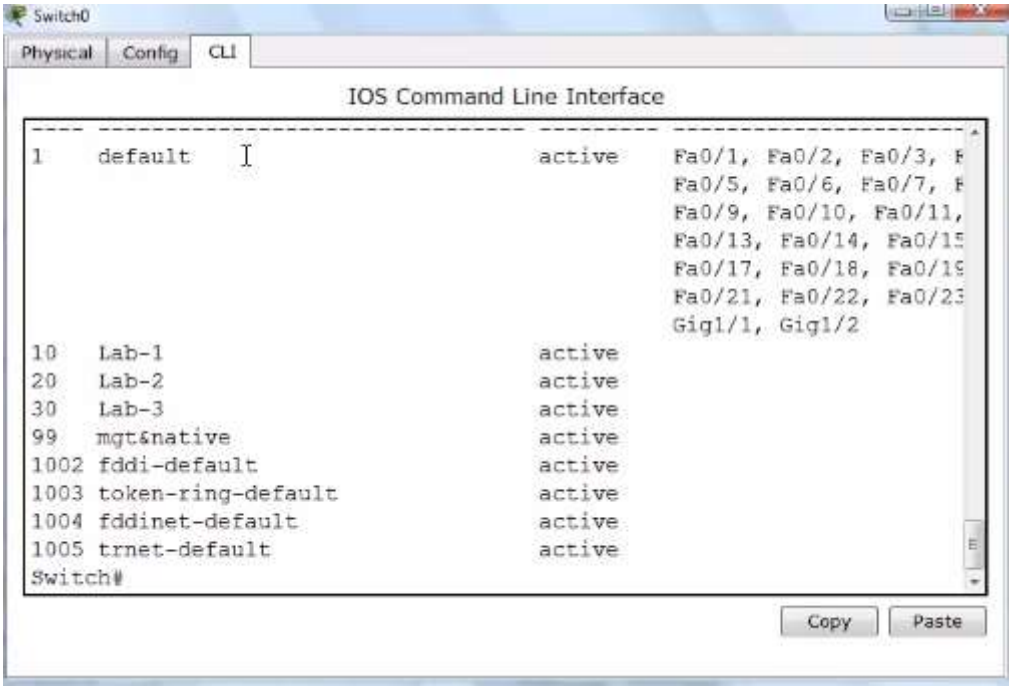

Рис. 3.7. Зразок отримання відомостей про VLAN

На данний момент всі три VLAN діяльні на 3ьох світчах, а саме: VLAN (10, 20, 30) й також VLAN 99. Повернемо до налаштування комутатора 0. Потрібно налагодити порти (див. рис.3.8).

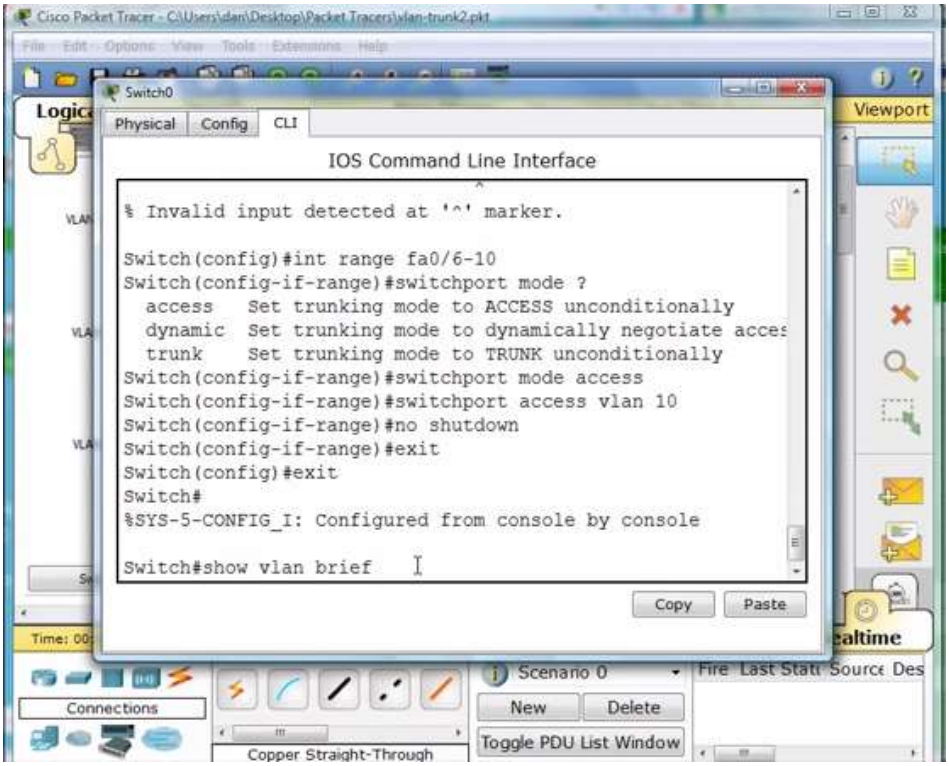

Рис. 3.8. Зразок налаштування портів

Потім задопомогою команди #show vlan brief визнаємо, які порти відгукуються VLAN 1. (див. рис. 3.9). За цим же правилом налагоджуємо VLAN 20, VLAN 30 на світчу 0. За аналогією налагоджуємо всі VLAN на комутаторах 1 і 2.

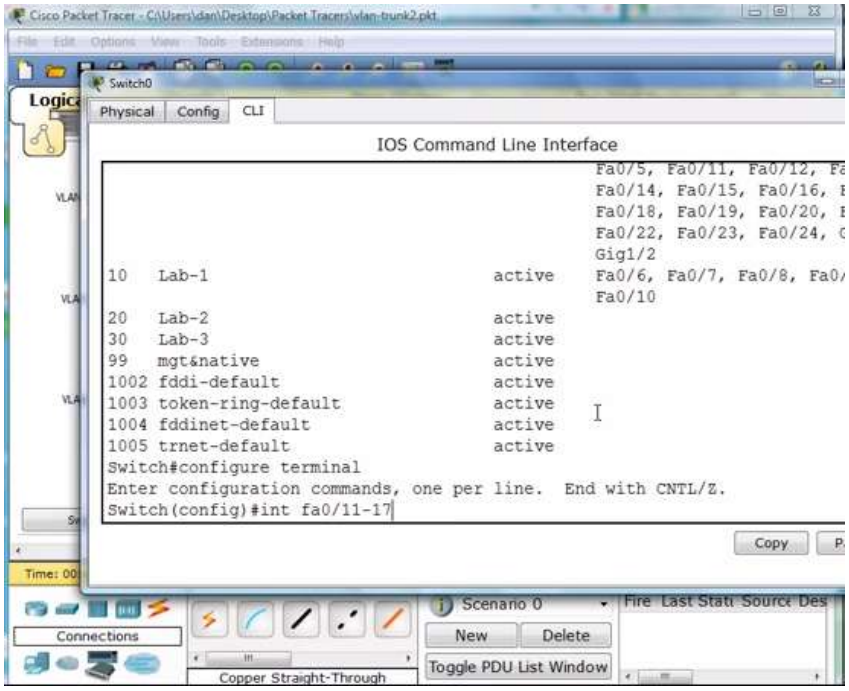

Рис. 3.9. Зразок відображення відомостей про порти комутатора

Виходить що, створивши модель та налагодивши всі компоненти одержуємо мережу з трьома VLAN (див. рис. 3.10).

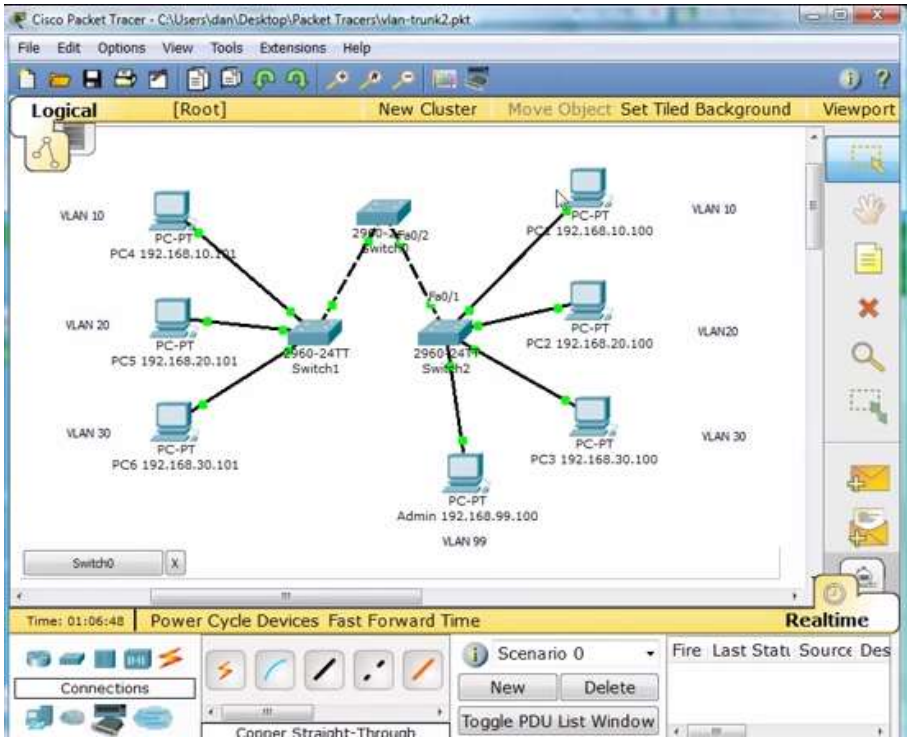

Рис. 3.10. Зразок віртуальної локально-обчислювальної мережі

Для перевірки чи працює, віртуально локально-обчислювальна мережа натискуємо на PC1 і вибираємо Command Prompt де пишемо ping 192.168.10.101 і дивимось за вдалим тестуванням (рис. 3.11).

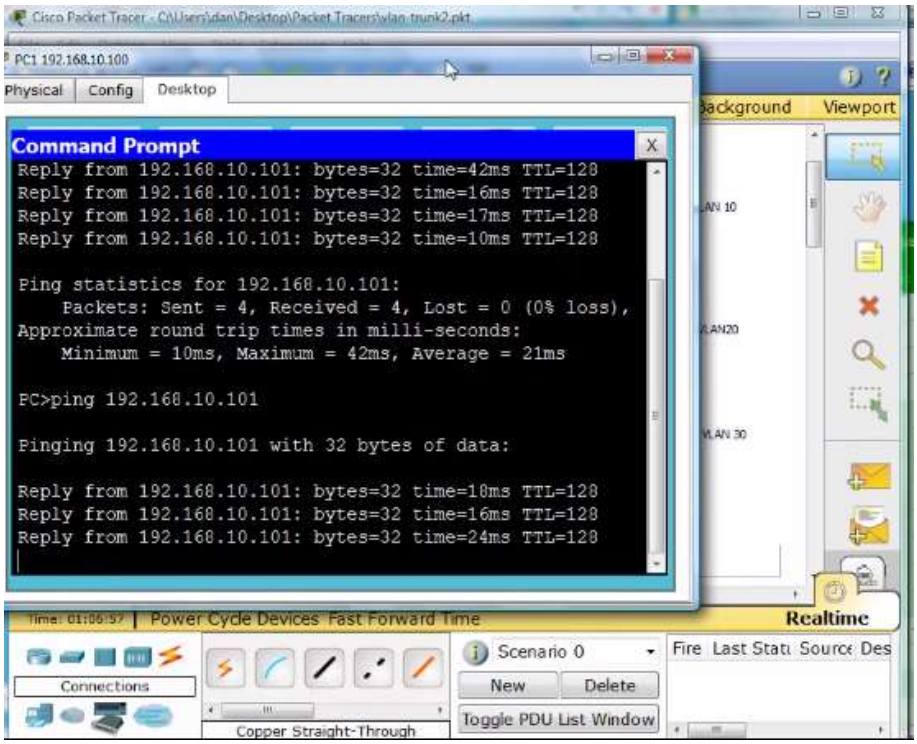

Рис. 3.11. Перевірка правильності налаштувань віртуальнох локально-обчислювальної мережі

ВИСНОВОК ДО РОЗДІЛУ 3

У цьому розділі ознайомились з колом Cisco Packet Tracer. Він являє собою симулятор мережі передачі даних та дає моливість імітувати роботу мережевих приладів: маршрутизаторів, комутаторів, точок бездротового доступу, персональних комп'ютерів, мережевих принтерів, IP-телефонів і т.д.

В цьому колі створена комп’ютерну модель віртуальної локально-обчислювальної мережі та звірено правильність її налаштувань.

ВИСНОВКИ

1. Застосовування віртуального сегментування локально-обчислювальної мережі позволяє оптимізувати мережевий трафік, забезпечити надійність та безпеку діяльності комп'ютерної мережі при збільшенні кількості користувачів. Це досягається завдяки територіальному розподіленню користувачів, та сворення можливості їх переміщення, обмеженості впливу широкомовних інформувань визначеним сегментом.

2. Віртуальні локально-обчислювальні мережі створюються за підбором портів, MAC-адреосою, протоколом. Зокрема, застосовування портів дає змогу обійти змін топології при переміщенні користувачів та затруднити внесення зміну у VLAN. Особливою властивістю підходу на основі MAC-адреси є уникнення переналаштувань комутатора та присутність часових затримок. Тоді як створеня VLAN за протоколом дає змогу вивести одну або декілька таких мереж призначенням однієї або декількох IP-адрес визначеному порту комутатора.

3. З урахуванням п. 1 і 2 створено комп’ютерну модель віртуальної локально-обчислювальної мережі в середовищі Cisco Packet Tracer. Для цього означено список компонентів такої мережі та описано їх налаштування, правильність яких перевірено задопомогою утиліти ping.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Олифер В.Г. Комрьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А. Олифер. – М.: Питер, 2014. – 944 с.

2. Гетель А.В. Компъютерные сети и сетевые технологии / А.В. Гетель, 2007. – 107 с.

3. ОДОМ У. CISCO Официальное руководство по подготовке к сертификационным экзаменам CCENTCCNA ICND2 / У. Одом. – М.: Вильямс, 2013. – 752 с.

4. Lammle T. CCNA Routing and Switching Study Guide / T. Lammle, 2013. – 1176 p.

5. Lacoste R. CCNP routing and switching tshoot 300-135 official cert guide / R. Lacoste, K. Wallace, 2014. – 1024 p.

6. Шыхалиев Р.Г. Анализ и классификация сетевого трафика компьютерных сетей / Р.Г. Шыхалиев // Проблемы информационных технологий. – 2010. – №2. – С. 15-23.

7. Матичин І.І. Моделювання та аналіз трафіку в телекомунікаційних системах та мережах / І.І. Матичин, В. В. Онищенко // Вісник ДУІКТ. – 2013. – №4. – С. 20-27.

8. Принцип работы и пример настройки VLAN в Ethernet-коммутаторах ZyXEL [Електронний ресурс]. – Режим доступу: http://zyxel.ua/kb/1439. – Дата доступу: травень 2023. – Назва з екрану.

9. Что такое VLAN? [Електронний ресурс]. – Режим доступу: http://www.technotrade.com.ua/Articles/what_is_vlan.php. – Дата доступу: травень 2023. – Назва з екрану.

10. Cisco Packet Tracer [Електронний ресурс]. – Режим доступу: http://www.packettracernetwork.com/. – Дата доступу: травень 2022. – Назва з екрану.

11. Пал, Г. Пракаш і Гян Пракаш Пал, «Віртуальний Локальна мережа (VLAN)», Міжнародний журнал науково-дослідної техніки та технологій (IJSRET), 1: 006-010, 2013.