ЗМІСТ

ПЕРЕЛІК ПОЗНАЧЕНЬ

ACL – лист контролю доступу

VLAN – віртуальна локальна мережа

TCP – протокол керування передачей блоків

OSI – командна строка для обладнання CISCO

LAN – фізична локальна мережа

VPN – віртуальна приватна мережа

MAC – постійний ідентифікаційний номер пристрою в мережі

IP – ідентифікаційний номер вузла в мережі

TELNET – протокол реалізації термінального інтервейса

ROM – спеціальний режим для запуску системи

HTTP – протокол захисту веб-ресурсів

EXEC – привілейований режим доступу до маршрутизатора

ВСТУП

Інформаційна безпека сьогодні – одна з перспективних, складних і швидко розвиваються сфер IT. Ситуація в IT-галузі як ніколи цікавить світову спільноту, численні зломи і кіберудари по таким великим структурам, як торгові мережі, банки, об'єкти енергетичної та промислової інфраструктури викликають тривогу. Загострення інтересу до даної області підтверджують регулярні міжнародні та внутрішньодержавні конференції та з'їзди по темі захисту інформації.

Для компаній інформація є найціннішим ресурсом, тому її захист є першоступеневою задачею. При тому ж, корпоративна мережа має бути гнучкою, швидкою і комфортною для співробітників, бо це підвищую ефективність праці, зменшує навантаження та час на реагування у разі якихось проблем з робочими станціями. Паперова документація надійна, але її час вже минув, бо з електронною версією цих документів працювати легше й швидше. До цього треба ще додати той факт, що не на кожного співробітника компанія буде віділяти той ж принтер, тобто всім потрібен також доступ до нього чи до інших переферийних пристроїв.

Правильно спроектована і зібрана корпоративна мережа, побудована на надійних компонентах може забезпечити стабільну роботу інформаційної системи вцілому, можливість її довготривалої, ефективної експлуатації, адаптації і модернізації, згідно зі зменами умов чи завдань.

Щоб побудувати таку систему, описану вище, доцільніше за все використовувати програмні засоби та пристрої CISCO. Вони є лідерами в сфері захисту інформації у корпоративному сегменті. А для того, щоб обрати обладнання та розрахувати усі нюанси його встановлення, треба правильно розрахувати, продумати, які використовуватимуться методи та засоби забезпечення контролю доступу. Найбільш підходить для цього середовище моделювання мережі CISCO packet tracer. Основні розглянуті методи будуть

стосуватися VLAN, міжмережевих єкранів та фільтрації на основі MAC – адресів.

Тема роботи – дослідження методів забезпечення контролю доступу до сегментів корпоративної мережі з використанням технологій CISCO

Мета роботи – дослідити технології, завдяки яким можна розрахувати та побудувати систему контролю доступу до розгалуженної корпоративної мережі, де кожний відділ знаходиться в своїй підмережі і не має прямого доступу до інших і навпаки. Все це потрібно для того, щоб потім можна було в короткі сроки побудувати таку мережу з мінімальними затратами, адже середа, де буде виконуватись розрахунок – CISCO Packet Tracer, має у собі повний спектр пристроїв CISCO, на яких і доцільно будувати мережу.

Дипломна робота містить у собі 65 сторінки, 11 рисунків та 10 посилань.

1 ОРГАНІЗАЦІЯ ЗАХИСТУ МІЖМЕРЕЖЕВОГО ТРАФІКА НА ОСНОВІ МІЖМЕРЕЖЕВИХ ЕКРАНІВ

1.1 Види міжмережевих екранів

Міжмережевий екран, мережевий екран – програмний або програмно апаратний елемент комп'ютерної мережі, що здійснює контроль і фільтрацію проходить через нього мережевого трафіку відповідно до заданих правил.

Для захисту локальних мереж від небажаного трафіку і несанкціонованого доступу застосовуються різні види міжмережевих екранів. Залежно від способу реалізації, вони можуть бути програмними або програмно-апаратними. Програмний Firewall – це спеціальний софт, який встановлюється на комп'ютер і забезпечує захист мережі від зовнішніх загроз. Це зручне і недороге рішення для приватних ПК, а також для невеликих локальних мереж – домашніх або малого офісу. Вони можуть застосовуватися на корпоративних комп'ютерах, використовуваних за межами офісу. Для захисту більших мереж використовуються програмні комплекси, під які доводиться виділяти спеціальний комп'ютер. Міжмережеві екрани класифікують в залежності від застосовуваної технології фільтрації трафіку. Існуючі брандмауери істотно відрізняються один від одного, в залежності від рівня захисту і використаного у них способу захисту. Більшість брандмауерів, що поставляються як комерційні продукти, можно віднести до однієї з чотирьох категорій:

- Брандмауери з фільтрацією пакетів
- Шлюзи сеансового рівня
- Шлюзи прикладного рівня
- Брандмауери експертного рівня

Хоча більшість з представлених міжмережевих екранів і не відносяться тільки до однієї з перерахованих категорій, дамо визначення кожному з них.

Брандмауери з фільтрацією пакетів

Брандмауер з фільтрацією пакетів є маршрутизатор або працююча на сервері програма, сконфігуровані таким чином, щоб фільтрувати вхідні і вихідні пакети. Брандмауер пропускає або відбраковує пакети відповідно до інформації, що міститься в IP-заголовках пакетів. Наприклад, більшість брандмауерів з фільтрацією пакетів може пропускати або бракувати пакети на основі інформації, що дозволяє асоціювати даний пакет з конкретними відправником і отримувачем (повної асоціації), яка складається з наступних елементів:

- адреси відправника;
- адреси одержувача;
- інформацію про програму або протоколі;
- номера порту джерела;
- номера порту одержувача.

Усі маршрутизатори (навіть ті, які не налаштовані за допомогою фільтрації пакетів), зазвичай перевіряють повну асоціацію пакетів, щоб визначити, куди його скерувати. Крім того, брандмауер фільтрації пакетів порівнює повну асоціацію з таблицею правил перед тим, як відправити пакет одержувачу, відповідно до цих правил він повинен дозволяти або забороняти даний пакет. Брандмауер буде продовжувати перевіряти, поки не знайде відповідне правило, пов'язане з повним пакетом.

Якщо брандмауер отримує пакет, який не відповідає жодним правилам таблиці, він застосовуватиме правила за замовчуванням, які також повинні бути чітко визначені в таблиці брандмауера. З міркувань безпеки це правило зазвичай означає скидання всіх пакетів, які не відповідають іншим правилам.

Як правило, брандмауер з фільтрацією пакетів встановлюється на маршрутизаторі з фільтрацією пакетів, через який відбувається з'єднання з Інтернетом (чи підмережею), на якому конфігуруються правила фільтрації пакетів, що дозволяють блокувати або фільтрувати пакетів на підставі

протоколів і адрес. Зазвичай машинам внутрішньої мережі надається повний доступ до Інтернету, а доступ з боку Інтернету до всіх або майже до всіх систем внутрішньої мережі блокується. Проте, маршрутизатор може допускати вибірковий доступ до систем і сервісів (це залежить від політики). Зазвичай блокуються такі потенційно небезпечні сервіси, як NIS, NFS і X Windows.

Брандмауер з фільтрацією пакетів має ті ж самі недоліки, що і маршрутизатор з фільтрацією пакетів, тим більше що вони можуть виявитися серйознішими при ускладненні вимог до захищеності сайту. Ось вони:

- відсутня (або мається на вкрай обмеженому розмірі) можливість протоколювання, тому адміністратору буде нелегко виявити компрометацію маршрутизатора або атаку на мережу.
- правила фільтрації часто важко протестувати, що може привести до виникнення вразливих місць. При необхідності введення складних правил фільтрації вони часто стають некерованими
- кожен хост, до якого потрібно забезпечити доступ з Інтернету, буде вимагати свою реалізацію заходів посиленої аутентифікації.

Технологія фільтрації пакетів – це "найдешевший" спосіб реалізації брандмауера. Такий брандмауер може перевіряти пакети даних різних протоколів на високій швидкості, оскільки він лише розглядає інформацію про пакети даних (заголовки), щоб визначити його подальшу долю. Фільтр аналізує пакети даних на мережевому рівні і не залежить від використовуваної програми. Саме ця «свобода» забезпечує хорошу роботу.

До недоліків цього типу брандмауера можна віднести неможливість ідентифікації пакетів при імітації IP-адрес та неможливість відстеження конкретних мережевих сеансів. Імітація означає, що якщо використовується IP-адреса законного користувача, можливо легко проникнути в захищену мережу та отримати доступ до її ресурсів. Фільтр пакетів дозволить пакету потрапити в мережу незалежно від того, звідки йде розмова та хто ховається за адресою. Існує вдосконалена версія фільтрації пакетів, яка називається

динамічною фільтрацією пакетів. Одночасно проаналізується адреса, до якої є намагання отримати доступ (можливо, і потім визначить її як несанкціоновану) та виконає перевірку пінгу для цієї адреси. Неважко зрозуміти, що якщо внутрішня IP-адреса використовується зовні, то ping не зможе зв’язатися з відправником пакета. У цьому випадку спроба доступу буде відхилена, а сеанс не встановлений. Сьогодні пакетні фільтри займають чільне місце в системах мережевої безпеки. Вони майже марні для захисту зовнішньої мережі. Але завдяки своїй високій продуктивності та низькій вартості ці фільтри дуже підходять для захисту внутрішньої мережі. Організації можуть використовувати їх для розподілу мережі на кілька сегментів та встановлення брандмауерів у кожному сегменті[1].

Шлюзи сеансового рівня

Шлюз сеансового рівня, званий ще екрануючим транспортом, призначений ще для контролю віртуальних з'єднань і трансляції IP-адрес при взаємодії з зовнішньою мережею. Він функціонує на сеансовому рівні моделі OSI, охоплюючи в процесі своєї роботи також транспортний і мережевий рівні еталонної моделі. Захисні функції екрануючого транспорту відносяться до функцій посередництва. Захисні функції екрануючого транспорту відносяться до функцій посередництва.

Контроль віртуальних з'єднань полягає в контролі квітірованія зв'язку, а також контролі передачі інформації за встановленими віртуальних каналах. При контролі квітірованія зв'язку шлюз сеансового рівня стежить за встановленням віртуального з'єднання між робочою станцією внутрішньої мережі і комп'ютером зовнішньої мережі, визначаючи, чи є запитуваний сеанс зв'язку допустимим. Такий контроль грунтується на інформації, що міститься в заголовках пакетів сеансового рівня протоколу TCP. Однак, якщо пакетний фільтр при аналізі TCP-заголовків перевіряє тільки номери портів джерела і одержувача, то екранує транспорт аналізує інші поля, які стосуються процесу квітірованія зв'язку.

Щоб визначити, чи є запит на сеанс зв'язку допустимим, шлюз сеансового рівня виконує наступні дії. Коли робоча станція (клієнт) запитує зв'язок із зовнішньою мережею, шлюз приймає цей запит, перевіряючи, чи задовольняє він базовим критеріям фільтрації, наприклад, чи може DNS-сервер визначити IP-адресу клієнта і асоційоване з ним ім'я. Потім, діючи від імені клієнта, шлюз встановлює з'єднання з комп'ютером зовнішньої мережі і стежить за виконанням процедури квітірованія зв'язку по протоколу TCP. Ця процедура складається з обміну TCP-пакетами, які позначаються прапорами SYN (синхронізувати) і ACK (підтвердити)

Перший пакет сеансу TCP, позначений прапором SYN і містить проізвольное число, наприклад 100, є запитом клієнта на відкриття сеансу. Комп'ютер зовнішньої мережі, який отримав цей пакет, посилає у відповідь пакет, позначений прапором ACK і містить число, на одиницю більше, ніж вк прийнятому пакеті (в нашому випадку 101), підтверджуючи, таким чином, прийом пакета SYN від клієнта. Крім того, здійснюючи зворотний процедуру, комп'ютер зовнішньої мережі посилає також клієнту пакет SYN, але вже з порядковим номером байта переданих даних (наприклад, 200), а клієнт підтверджує його отримання передачею пакета ACK, що містить число 201. На цьому процес квитирования зв'язку завершується.

Для шлюзу сеансового рівня запитаний сеанс вважається допустимим тільки в тому випадку, якщо при виконанні процедури квітірованія зв'язку прапори SYN і ACK, а також числа, що містяться і заголовках TCP-пакетів, виявляються логічно пов'язаними між собою. Після того як шлюз визначив, що робоча станція внутрішньої мережі і комп'ютер зовнішньої мережі є авторизованими учасниками сеансу TCP, і перевірив допустимість даного сеансу, він встановлює з'єднання. Починаючи з цього моменту шлюз копіює і перенаправляє пакети туди і назад, контролюючи передачу інформації за встановленим віртуальному каналу. Він підтримує таблицю встановлених з'єднань, пропускаючи дані, що відносяться до одного з сеансів зв'язку, які

зафіксовані в цій таблиці. Коли сеанс завершується, шлюз видаляє відповідний елемент з таблиці і розриває ланцюг, що використовувалася в даному сеансі.

У процесі контролю передачі інформації по віртуальних каналах фільтрація пакетів екрануючим транспортом не здійснюється. Однак шлюз сеансового рівня здатний відстежувати кількість переданої інформації і розривати з'єднання після перевищення певної межі, перешкоджаючи тим самим несанкціонованого експорту інформації. Можливо також накопичення реєстраційної інформації про віртуальних з'єднаннях.

Для контролю віртуальних з'єднань в шлюзах сеансового рівня використовуються спеціальні програми, які називають канальними посередниками (pipe proxies). Ці посередники встановлюють між внутрішньою і зовнішньою мережами віртуальні канали, а потім контролюють передачу по цих каналах пакетів, що генеруються додатками TCP / IP. Канальні посередники орієнтовані на конкретні служби TCP / IP. Тому шлюзи сеансового рівня можуть використовуватися для розширення можливостей шлюзів прикладного рівня, робота яких грунтується на програмах-посередниках конкретних додатків.

Після встановлення зв'язку шлюзи мережевого рівня фільтрують пакети тільки на сеансовому рівні моделі OSI, тобто не можуть перевіряти вміст пакетів, переданих між внутрішньою і зовнішньою мережею на рівні прикладних програм. І оскільки ця передача здійснюється "наосліп", хакер, що знаходиться у зовнішній мережі, може "проштовхнути" свої "шкідливі" пакети через такий шлюз. Після цього хакер звернеться безпосередньо до внутрішнього Web-серверу, який сам по собі не може забезпечувати функції брандмауера. Іншими словами, якщо процедура квітірованія зв'язку успішно завершена, шлюз мережевого рівня встановить з'єднання і буде "сліпо" копіювати і перенаправляти всі наступні пакети незалежно від їх вмісту.

Шлюзи прикладного рівня

Для усунення багатьох притаманних недоліків фільтрації маршрутизаторів, брандмауери повинні використовувати додаткове

програмне забезпечення для фільтрації повідомлень від таких служб, як TELNET та FTP. Цей тип програмного забезпечення називається проксі-серверами, а хости, на яких воно працює, називаються шлюзами рівня додатків. Шлюз прикладного рівня виключає прямий зв'язок між авторизованими клієнтами та зовнішніми хостами. Шлюз фільтрує всі вхідні та вихідні пакети даних на рівні програми. Пов'язані з додатками сервери-посередники пересилають інформацію, що генерується певними серверами, через шлюз. Шлюз програми та маршрутизатор фільтрації можна поєднати в брандмауері для досягнення вищої безпеки та гнучкості. Як приклад я розгляну мережу, де вхідні з'єднання TELNET та FTP блокуються за допомогою маршрутизатора фільтрації. Цей маршрутизатор дозволяє доставляти пакети TELNET або FTP до одного шлюзу рівня додатку TELNET / FTP. Зовнішній користувач, який хоче підключитися до системи в мережі, повинен спочатку підключитися до шлюзу прикладного рівня, а потім підключитися до необхідного внутрішнього хоста. Це робиться наступним чином:

- По-перше, зовнішні користувачі встановлюють протокол TELNET із використанням TELNET для встановлення зв’язку із шлюзом прикладного рівня та вводять цікаве ім’я внутрішнього хосту;
- Шлюз перевіряє IP-адресу відправника і дозволяє або забороняє підключення відповідно до того чи іншого стандарту доступу;
- Користувачеві може знадобитися підтвердження особи (може знадобитися одноразовий пароль);
- Сервер-посередник встановлює з'єднання TELNET між шлюзом та внутрішнім хостом;
- проміжний сервер передає інформацію між цими двома з'єднаннями;
- Шлюз прикладного рівня реєструє з'єднання.

Авторизований сервер-посередники дозволяють їм надавати лише довірені їм послуги. Іншими словами, якщо шлюз прикладного рівня має дозвіл використовувати служби FTP та TELNET, тоді в захищеній мережі дозволятимуться лише FTP та TELNE, а всі інші служби будуть повністю заблоковані. Для деяких організацій ця безпека важлива, оскільки вона забезпечує, що через брандмауер дозволяється використовувати лише ті послуги, які вважаються безпечними. Авторизований проксі-сервер забезпечує функцію фільтрації протоколів. Наприклад, деякі брандмауери, які використовують шлюзи рівня додатків, можуть фільтрувати з'єднання FTP і відмовлятися використовувати команду FTPput, що може гарантувати, що користувачам заборонено записувати інформацію на анонімний сервер FTP.

На додаток до фільтрації пакетів, багато шлюзів додатків також фіксують всі операції сервера, а головне, попереджають адміністраторів мережі про потенційні уразливості системи безпеки. Наприклад, під час спроби проникнути в мережу ззовні, сервер брандмауера Border Ware захищеного обчислення записує адреси джерела та призначення пакетів, час цих спроб та використаний протокол. Брандмауер Milkyway Networks Black Hole фіксує всю активність сервера та попереджає адміністратора про можливі порушення, надіславши адміністратору електронний лист або пейджер. Багато інших шлюзів рівня додатків виконують подібні функції. Шлюзи на рівні додатків забезпечують найвищий рівень захисту, оскільки взаємодія із зовнішнім світом досягається завдяки невеликій кількості авторитетних проксі-серверів додатків, які повністю контролюють весь вхідний та вихідний трафік. У порівнянні з традиційною моделлю, шлюз програми має багато переваг. У традиційній моделі трафік програми направляється безпосередньо на внутрішній.

До недоліків шлюзів прикладного рівня відносяться:

- більш низька продуктивність у порівнянні з фільтруючими маршрутизаторами; зокрема, при використанні клієнт-серверних

протоколів, таких як TELNET, потрібно двох крокова процедура для вхідних і вихідних з'єднань;

- Більш висока вартість у порівнянні з фільтруючим маршрутизатором.

Брандмауери експертного рівня

Ці брандмауери поєднують в собі елементи всіх трьох описаних вище категорій. Як і брандмауери з фільтрацією пакетів, вони працюють на мережному рівні моделі OSI, фільтруючи вхідні і вихідні пакети на основі перевірки IP-адрес і номерів портів. Брандмауери експертного рівня також виконують функції шлюзу сеансового рівня, визначаючи, чи належать пакети до відповідного сеансу. І нарешті, брандмауери експертного рівня беруть на себе функції шлюзу прикладного рівня, оцінюючи вміст кожного пакета відповідно до політики безпеки, виробленої в конкретній організації.Як і шлюз прикладного рівня, брандмауер експертного рівня може бути налаштований для відбраковування пакетів, що містять певні команди, наприклад команди Put і Get служби FTP. Однак, на відміну від шлюзів прикладного рівня, при аналізі даних прикладного рівня такої брандмауер не порушує клієнт-серверної моделі взаємодії в мережі.

Шлюз прикладного рівня встановлює два з'єднання: одне – між авторизованим клієнтом і шлюзом, друге – між шлюзом і зовнішнім хостом. Після цього він просто пересилає інформацію між цими двома з'єднаннями. Незважаючи на високий рівень захисту, який забезпечується подібними шлюзами, така схема може позначитися на продуктивності роботи. На противагу цьому брандмауери експертного рівня допускають прямі з'єднання між клієнтами і зовнішніми хостами. Для забезпечення захисту такі брандмауери перехоплюють і аналізують кожен пакет на прикладному рівні моделі OSI. Замість застосування пов'язаних з додатками програм-посередників, брандмауери експертного рівня використовують спеціальні алгоритми розпізнавання та обробки даних на рівні додатків. За допомогою

цих алгоритмів пакети порівнюються з відомими шаблонами даних, що, теоретично, повинно забезпечити більш ефективну фільтрацію пакетів.

1.2 Фільтрація кадрів на основі MAC – адрес

Коли маршрутизатор приймає кадри, він використовує правила фільтрації, що були йому задані. Можна задати одну з таких дій:

- Переслати
- Пропустити
- Перевірити за наступним правилом, яке має бути виконане в разі відповідності чи не відповідности значень полів кадру правил фільтрації

Зміщення проходить в кадрі Ethernet над полем «MAC – адресу призначення». Формат кадру Ethernet складається з наступних елементів:

- MAC – адрес призначення – є вказівкою на цільовий вузол, якому було надіслано деякий кадр. Його поле має довжину в 6 байт.
- MAC – адрес джерела – є вказівкою на вузол, яким було надіслано деякий кадр. Його поле має довжину в 6 байт.
- Довжина (Тип) – у кадрі Ethernet це поле, довжиною 2 байта, використовується для вказівки протоколу верхнього рівня. Значення типу 08-00 притаманне для поля даних пакету IP. Для ARP (Протокол дозволу адрес) – значення 08-06. Але для Ethernet IEEE 802.3 в цьому полі міститься виражений в байтах розмір наступного поля – поля даних.
- Дані – поле містить дані протоколів верхнього рівня. Мінімальна довжина такого поля – 46 байт, а максимальна – 1500 байт.
- FCS – контрольна сума кадрів для розпізнавання можливих помилок. Розпізнає помилки за допомогою циклічного надмірного коду.

Мал. 1.1 Меню створення правил фільтрації пакетів

Для створення правил фільтрації кадрів налаштовуються наступні поля:

- Active (Активно): Переключаемо Activel на "Yes";
- Offset (Зсув) (у байтах): Встановлюємо '6, оскільки MAC-адреса джерела починається з 7-го байта, totрібно пропустити перші байти MAC-адреси призначення.
- Length (Довжина) (в байтах): Встановлюємо '6, оскільки MAC-адреса включає 6 байт.
- Mask (Маска) (у шістнадцятковій формі): Задаємо значення, за яким модем буде застосовувати логічну операцію "1" до даних в кадрі. У даному випадку пропонується встановити ffffffff для маскування MAC-адреси джерела вхідного кадру;
- Value (Значення) (у шістнадцятковій формі): Задаємо MAC-адресу [00-50- 22-30-0A-31],. яку модем буде використовувати для порівняння маскуючим кадром;
- Action Matehed D (Дія при відповідності): Вводимо дію, яка мае виконуватися у разі відповідності маскованого кадру зі значенням "Value'. У даному випадку пропонується скинути кадр (Drop): .

- Action Not Matched – (Дію при невідповідності): Вводимо дію, яка має виконуватися у випадку невідповідності маскованого кадру зі значенням Value'. У даному випадку пропонується переслати кадр (Forward). Якщо Ви хочете конфігурувати більше правил фільтрації, виберіть 'Check Next Rule' (Перевірити за наступним правилом) для активізації конфігурування наступного правила. Слід зазначити, що в полі Filter Type (Тип фільтра) має бути встановлено 'Generic Filter Rule' (Правило фільтрації кадрів). а не щось інше.

Щоб створений фільтр став активним, його потрібно приєднати до інтерфейсу LAN і визначити до яких даними вхідними або виходять його застосувати.

1.3 Основні функції віртуальних локальних мереж

Створення VLAN дозволяє підвищити продуктивність кожної з них і ізолювати мережі один від одного.

Окрім свого основного призначення – підвищення пропускної спроможності з'єднань в мережі – комутатор дозволяє локалізувати потоки інформації, а також контролювати ці потоки і управляти ними за допомогою механізму користувальницьких фільтрів. Однак для користування фільтр здатний перешкодити передачі кадрів лише за конкретними адресами, тоді як широкомовний трафік він передає всім сегментам мережі. Такий принцип дії реалізованого в комутаторі алгоритму роботи моста, тому мережі, створені на основі мостів і комутаторів, іноді називають плоскими – через відсутність бар'єрів на шляху широкомовного трафіку.

З’явившись кілька років тому, технологія віртуальних локальних мереж (Virtual LAN, VLAN) дозволяє подолати вказане обмеження. Віртуальної мережею називається група вузлів мережі, трафік якої, в тому числі і широкомовний, на канальному рівні повністю ізольований від інших вузлів

(див. Малюнок 1). Це означає, що безпосередня передача кадрів між різними віртуальними мережами неможлива, незалежно від типу адреси – унікального, групового або широкомовного. У той же час усередині віртуальної мережі кадри передаються відповідно до технології комутації, т. е. тільки на той порт, до якого приписаний адреса призначення кадру.

Віртуальні мережі можуть перетинатися, якщо один або декілька комп'ютерів включено до складу більш ніж однієї віртуальної мережі. Якщо ж якийсь комп'ютер віднесений тільки до однієї віртуальної мережі, то його кадри до іншої мережі доходити не будуть, але він може взаємодіяти з комп'ютерами тієї мережі через загальний поштовий сервер.

Віртуальна мережа утворює широкомовний домен трафіку (broadcast domain), за аналогією з доменом колізій, який утворюється повторювачами мереж Ethernet.

ПРИЗНАЧЕННЯ VLAN

Технологія VLAN полегшує процес створення ізольованих мереж, зв'язок між якими здійснюється за допомогою маршрутизаторів з підтримкою протоколу мережевого рівня, наприклад IP. Таке рішення створює набагато більш потужні бар'єри на шляху помилкового трафіку з однієї мережі в іншу. Сьогодні вважається, що будь-яка велика мережа повинна включати маршрутизатори, інакше потоки помилкових кадрів, зокрема широкомовних, через прозорі для них комутатори будуть періодично «затоплювати» її цілком, приводячи в неробочий стан.

Технологія віртуальних мереж надає гнучку основу для побудови великої мережі, з'єднаної маршрутизаторами, так як комутатори дозволяють створювати повністю ізольовані сегменти програмним шляхом, не вдаючись до фізичної комутації.

До появи технології VLAN для розгортання окремої мережі використовувалися або фізично ізольовані відрізки коаксіальногокабелю, або не пов'язані між собою сегменти на базі повторювачів і мостів. Потім мережі об'єднувалися за допомогою маршрутизаторів в єдину складену мережу.

Зміна складу сегментів (перехід користувача в іншу мережу, дроблення великих ділянок) при такому підході мало на увазі фізичну перекомутацію роз'ємів на передніх панелях повторювачів або в кросових панелях, що не дуже зручно у великих мережах – це дуже трудомістка робота, а ймовірність помилки дуже висока. Тому для усунення необхідності фізичної перекоммутации вузлів стали застосовувати багатосегментні концентратори, щоб склад розділяється сегмента можна було перепрограмувати без фізичної перекоммутации.

Однак зміна складу сегментів з допомогою концентраторів накладає великі обмеження на структуру мережі – кількість сегментів такого повторювача зазвичай невелика, і виділити кожному вузлу власний, як це можна зробити за допомогою комутатора, нереально. Крім того, при подібному підході вся робота по передачі даних між сегментами лягає на маршрутизатори, а комутатори зі своєю високою продуктивністю залишаються «поза справами». Таким чином мережі на базі повторювачів з конфігураційної комутацією як і раніше передбачають спільне використання середовища передачі даних великою кількістю вузлів і, отже, мають набагато меншою продуктивністю в порівнянні з мережами на базі комутаторів.

При використанні в комутаторах технології віртуальних мереж одночасно вирішуються дві задачі:

- підвищення продуктивності в кожній з віртуальних мереж, так як комутатор передає кадри тільки вузлу призначення;
- ізоляція мереж друг від друга керувати правами доступу користувачів і створення захисних бар'єрів на шляху широкомовних штормів.

Об'єднання віртуальних мереж в загальну мережу виконується на мережевому рівні, перехід на який можливий за допомогою окремого маршрутизатора або програмного забезпечення комутатора. Останній в цьому випадку стає комбінованим пристроєм – так званим комутатором третього рівня.

Технологія формування і функціонування віртуальних мереж за допомогою комутаторів довгий час не стандартизовані, хоча і була реалізована в дуже широкому спектрі моделей комутаторів різних виробників. Ситуація змінилася після прийняття в 1998 р стандарту IEEE 802.1Q, де визначаються базові правила побудови віртуальних локальних мереж незалежно від того, який протокол канального рівня підтримується комутатором.

З огляду на тривалу відсутність стандарту на VLAN кожна велика компанія, що випускає комутатори, розробила свою технологію віртуальних мереж, причому, як правило, є несумісною з технологіями інших виробників. Тому, незважаючи на появу стандарту, не так уже й рідко зустрічається ситуація, коли віртуальні мережі, створені на базі комутаторів одного вендора, які не розпізнаються і, відповідно, не підтримуються комутаторами іншого. При створенні віртуальних мереж на основі одного комутатора зазвичай використовується механізм групування в мережі портів комутатора. При цьому кожен з них приписується тій чи іншій віртуальній мережі. Кадр, що надійшов від порту, що належить, наприклад, віртуальної мережі 1, ніколи не буде переданий порту, який не входить до її складу. Порт можна приписати декільком віртуальним мережам, хоча на практиці так надходять рідко – пропадає ефект повної ізоляції мереж.

Групування портів одного комутатора – найбільш логічний спосіб утворення VLAN, так як в даному випадку віртуальних мереж не може бути більше, ніж портів. Якщо до якогось порту підключений повторювач, то вузли відповідного сегмента не має сенсу включати в різні віртуальні мережі – все одно їх трафік буде загальним.

Такий підхід не вимагає від адміністратора великого обсягу ручної роботи – досить кожен порт приписати до однієї з декількох заздалегідь названих віртуальних мереж. Зазвичай ця операція виконується за допомогою спеціальної програми, що додається до комутатора. Адміністратор створює віртуальні мережі шляхом перетягування графічних символів портів на графічні символи мереж.

Інший спосіб утворення віртуальних мереж заснований на групуванні MAC-адрес. Кожен відомий комутатора MAC-адресу приписується тій чи іншій віртуальній мережі. Якщо в мережі є безліч вузлів, адміністратору доведеться виконувати чимало операцій вручну. Однак при побудові віртуальних мереж на основі декількох комутаторів подібний спосіб більш гнучкий, ніж групування портів.Якщо вузли будь-якої віртуальної мережі підключені до різних комутаторів, то для з'єднання комутаторів кожної такої мережі повинна бути виділена окрема пара портів. В іншому випадку інформація про приналежність кадру тієї чи іншої віртуальної мережі при передачі з комутатора в комутатор буде загублена. Таким чином, при методі групування портів для з'єднання комутаторів потрібно стільки портів, скільки віртуальних мереж вони підтримують, – в результаті порти і кабелі використовуються дуже марнотратно. Крім того, для організації взаємодії віртуальних мереж через маршрутизатор кожної мережі необхідний окремий кабель і окремий порт маршрутизатора, що також веде до великих накладних витрат.

Групування MAC-адрес у віртуальну мережу на кожному комутаторі позбавляє від необхідності їх з'єднання через кілька портів, оскільки в цьому випадку міткою віртуальної мережі є MAC-адресу. Однак такий спосіб вимагає виконання великої кількості ручних операцій по маркуванню MAC-адрес вручну на кожному комутаторі мережі.

Два описані підходи засновані тільки на додаванні інформації до адресних таблиць моста і не передбачають включення в переданий кадр інформації про приналежність кадру до віртуальної мережі. Решта підходи використовують наявні або додаткові поля кадру для запису інформації про приналежність кадру при його переміщеннях між комутаторами мережі. Крім того, немає необхідності запам'ятовувати на кожному комутаторі, яким віртуальним мережам належать MAC-адреси об'єднаної мережі.

Додаткове поле з позначкою про номер віртуальної мережі використовується тільки тоді, коли кадр передається від комутатора до

комутатора, а при передачі кадру кінцевому вузлу воно зазвичай видаляється. При цьому протокол взаємодії «комутатор-комутатор» модифікується, тоді як програмне і апаратне забезпечення кінцевих вузлів залишається незмінним. Прикладів подібних фірмових протоколів багато, але загальний недолік у них один – вони не підтримуються іншими виробниками. Компанія Cisco запропонувала в якості стандартної добавки до кадрів будь-яких протоколів локальних мереж заголовок протоколу 802.10, призначення якого – підтримка функцій безпеки обчислювальних мереж. Сама компанія звертається до такого методу в тих випадках, коли комутатори об'єднуються між собою по протоколу FDDI. Однак ця ініціатива не була підтримана іншими провідними виробниками комутаторів.

Для зберігання номера віртуальної мережі в стандарті IEEE 802.1Q передбачений додатковий заголовок в два байта, який використовується спільно з протоколом 802.1p. Крім трьох біт для зберігання значення пріоритету кадру, як це описується стандартом 802.1p, в цьому заголовку 12 біт служать для зберігання номера віртуальної мережі, якій належить кадр. Ця додаткова інформація називається тегом віртуальної мережі (VLAN TAG) і дозволяє комутаторів різних виробників створювати до 4096 загальних віртуальних мереж. Такий кадр називають «зазначений» (tagged). Довжина зазначеного кадру Ethernet збільшується на 4 байт, так як крім двох байтів власне тега додаються ще два байта.

Поява стандарту 802.1Q дозволило подолати відмінності в фірмових реалізаціях VLAN і домогтися сумісності при побудові віртуальних локальних мереж. Техніку VLAN підтримують виробники як комутаторів, так і мережевих адаптерів. В останньому випадку мережевий адаптер може генерувати і приймати відмічені кадри Ethernet, що містять поле VLAN TAG. Якщо мережевий адаптер генерує відмічені кадри, то тим самим він визначає їх приналежність до тієї чи іншої віртуальної локальної мережі, тому комутатор повинен обробляти їх відповідним чином, т. Е. Передавати або не передавати на вихідний порт в залежності від приналежності порту. Драйвер

мережевого адаптера отримує номер своєї (або своїх) віртуальної локальної мережі від адміністратора мережі (шляхом конфігурації вручну) або від деякого додатка, що працює на даному вузлі. Таке додаток здатне функціонувати централізовано на одному з серверів мережі і управляти структурою всієї мережі.

За підтримки VLAN мережевими адаптерами можна обійтися без статичного конфігурації шляхом приписування порту певної віртуальної мережі. Проте метод статичного конфігурації VLAN залишається популярним, так як дозволяє створити структуровану мережу без залучення програмного забезпечення кінцевих вузлів [2].

2 НАЛАШТУВАННЯ МАРШРУТИЗАТОРІВ CISCO НА РЕЖИМ РОБОТИ МІЖМЕРЕЖЕВОГО ЕКРАНУ

2.1 Інтерфейс командного рядка IOS CISCO

Інтерфейс командного рядка (CLI) Cisco IOS – основний інтерфейс, який використовується для конфігурації, моніторингу та обслуговування пристроїв Cisco. Цей інтерфейс дозволяє безпосередньо виконувати команди Cisco IOS за допомогою консолі маршрутизатора, терміналу або з використанням віддаленого доступу.

Додаткові інтерфейси користувача – це режим установки (використовується при першому запуску), веб-оглядач Cisco і призначені для користувача меню, що настроюються системним адміністратором. Інформація про режим установки викладена в частині цього керівництва "Конфігурація за допомогою процедур настройки і автоматичної установки". Інформація про виконання команд в середовищі веб-оглядача Cisco приведена в розділі цього керівництва "Використання інтерфейсу користувача веб-оглядача Cisco". Інформація про користувача меню наведена в главі цього керівництва "Управління підключеннями, меню і системними банерами".

Щоб полегшити конфігурування пристроїв Cisco, інтерфейс командного рядка Cisco IOS розділений на окремі командні режими. У кожному командному режимі передбачений власний набір команд для конфігурації, обслуговування та моніторингу роботи маршрутизатора та мережі. Сукупність доступних в конкретний момент командзавісіт від поточного командного режиму. Введення знаку (?) Після системного запрошення дозволяє вивести список доступних команд для кожного командного режіма.Прімененіе певних команд забезпечує перехід від одного командного режиму до іншого. Стандартний порядок, вякому користувачеві слід здійснювати доступ до режимів, такий: призначений для користувача режим EXEC, привілейований режим EXEC; режим глобальної конфігурації; режими спеціальної

конфігурації, подрежімиконфігурациі і підрежими конфігурації 2-го уровня.Сеанс на маршрутизаторі зазвичай починається в призначеному для користувача режимі EXEC, який являє собою один з дворівневого доступу режиму EXEC. З метою безпеки в призначеному для користувача режимі EXEC є лише ограніченноеподмножество команд EXEC. Цей рівень доступу призначений для завдань, що не змінюють конфігурацію маршрутізатора, наприклад, визначення статусу маршрутізатора.Для отримання доступу до всіх команд необхідно перейти в привілейований режим EXEC, який обеспечіваетвторой рівень доступу режиму EXEC. Зазвичай для входу в привілейований режим EXEC потрібно ввести пароль. В прівілегірованном режимі EXEC можна вводити будь-яку команду EXEC, так як він передбачає набір команд, розширений по відношенню до призначеного для користувача режиму EXEC. Більшість команд режиму EXEC є "одноразовими" командами, наприклад, команди show або more, коториепоказивают статус поточної конфігурації, і команди clear, скидають лічильники або інтерфейси. Команди режіма EXEC не зберігаються після перезавантаження маршрутізатора. Із привілейованого режиму EXEC можна перейти в режим глобальної конфігурації. В цьому режимі можливе введення команд, що дозволяють конфігурувати загальні характеристики системи. Режим глобальної конфігурації може використовуватися також для переходу в специфічні режими конфігурації. Режими конфігурації, включая режім глобальної конфігурації, дозволяють вносити зміни в поточну конфігурацію. Якщо конфігурація пізніше сохраняется, то ці команди зберігаються після перезавантаження маршрутізатора.Із режиму глобальної конфігурації можна перейти в безліч режимів конфігурації, специфічних для конкретних протоколу або функції. Ієрархія CLI передбачає, що вхід в ці специфічні режіми конфігурування проводиться тільки з режиму глобальної конфігурації. Як приклад в цьому розділі описаний один з зазвичай використовуваних режимів конфігурації – режим конфігурації інтерфейса. Із режимів конфігурації можна перейти в підрежими конфігурації. Підрежими

конфігурування використовуються для настройки певних функцій в межах даного режиму конфігурації. Як приклад ветой чолі описаний режим конфігурації субінтерфейса, який є підлеглим по відношенню до режімуконфігурірованія інтерфейса.Режім монітора ROM – це окремий режим, який використовується в тому випадку, коли маршрутизатор не завантажується належним чином. Якщо система (маршрутизатор, комутатор або сервер доступу) не знаходить правильний образ системи, що завантажується в процесі запуску, то система переходить в режим монітора ROM. В режим монітора ROM (ROMMON) можна увійти також шляхом переривання послідовності завантаження в ході запуску.

1. Призначений для користувача режим

В цей режим ми потрапляємо спочатку, тут доступний тільки обмежений перелік команд, виконання яких не повинно зашкодити функціонуванню пристрою. Наприклад, з цього режиму можна подивитися версію операційної системи командою show version або запустити команду ping. Зазвичай доступ до цього режиму дають молодшим технікам, щоб вони могли діагностувати деякі проблеми самостійно, але не могли нічого зіпсувати в конфігурації.

2. Привілейований режим

Для переходу в цей режим необхідно з призначеного для користувача режиму виконати команду enable і в разі необхідності ввести пароль. Після переходу, нам доступний повний перелік команд і можливість переходу в режим конфігурації без пароля. Таким чином, знаючи пароль на вхід на пристрій і пароль на привілейований режим, людина має повний доступ до маршрутизатора, так як далі вже ніяких паролів вводити не потрібно. Для виходу назад в призначений для користувача режим використовується команда disable.

3. Режим глобальної конфігурації

Цей режим дозволяє вносити зміни в конфігурацію пристрою. Для входу в нього необхідно з привілейованого режиму, виконати команду configure terminal. Введення паролів в даному випадку не буде потрібно.

4. Режими специфічної конфігурації

Цих режимів безліч і вони є подрежімамі режиму глобальної конфігурації. Наприклад, ввівши в режимі глобальної конфігурації команду interface FastEthernet 0/0 ми перейдемо в подрежим настройки відповідного інтерфейсу (config-if). Безліч режимів специфічної конфігурації відповідає безлічі різних гілок глобальної конфігурації[3].

2.2 Стандартні списки доступу

ACL (Access Control List) – це набір текстових виразів, які щось дозволяють, або щось забороняють. Зазвичай ACL дозволяє або забороняє IP-пакети, але крім усього іншого він може заглядати всередину IP-пакета, переглядати тип пакету, TCP і UDP порти. Також ACL існує для різних мережевих протоколів (IP, IPX, AppleTalk і так далі). В основному застосування списків доступу розглядають з точки зору пакетної фільтрації, тобто пакетна фільтрація необхідна в тих ситуаціях, коли у вас коштує обладнання на кордоні Інтернет і вашої приватної мережі і потрібно відфільтрувати непотрібний трафік. Розміщується ACL на вхідний напрямку і блокує надлишкові види трафіку.

Функціонал ACL складається в класифікації трафіку, потрібно його перевірити спочатку, а потім щось з ним зробити в залежності від того, куди ACL застосовується. ACL застосовується скрізь, наприклад:

- На інтерфейсі: пакетна фільтрація
- На лінії Telnet: обмеження доступу до маршрутизатора
- VPN: який трафік потрібно шифрувати
- QoS: який трафік обробляти приоритетнее
- NAT: які адреси транслювати

Для застосування ACL для всіх цих компонентів потрібно зрозуміти як вони працюють. І ми в першу чергу будемо торкатися пакетної фільтрації.

Стосовно до пакетної фільтрації, ACL розміщуються на інтерфейсах, самі вони створюються незалежно, а вже потім вони прикручуються до інтерфейсу. Як тільки ви його прикрутили до інтерфейсу маршрутизатор починає переглядати трафік. Маршрутизатор розглядає трафік як вхідний і вихідний. Той трафік, який входить в маршрутизатор називається входять, той який з нього виходить – вихідний. Відповідно ACL розміщуються на вхідному або на вихідному напрямі.

З приватної мережі приходить пакет на інтерфейс маршрутизатора fa0/ 1, маршрутизатор перевіряє чи є ACL на інтерфейсі чи ні, якщо він є, то далі обробка ведеться за правилами списку доступу строго в тому порядку, в якому записані вирази, якщо список доступу дозволяє проходити пакету, то в даному випадку маршрутизатор відправляє пакет провайдеру через інтерфейс fa0 / 0, якщо список доступу не дозволяє проходити пакету, пакет знищується. Якщо списку доступу немає – пакет пролітає без всяких обмежень. Перед тим як відправити пакет провайдеру, маршрутизатор ще перевіряє інтерфейс fa0 / 0 на наявність вихідного ACL. Справа в тому, що ACL може бути прикріплений на інтерфейсі як вхідний чи. Наприклад є ACL з правилом заборонити всім вузлам в Інтернеті посилати в нашу мережу пакети.

Сам же ACL являє собою набір текстових виразів, в яких написано permit (дозволити) або deny (заборонити), і обробка ведеться строго в тому порядку в якому задані вирази. Відповідно коли пакет потрапляє на інтерфейс він перевіряється на першу умову, якщо перша умова збігається з пакетом, подальша його обробка припиняється. Пакет або перейде далі, або знищиться.

Ще раз, якщо пакет збігся з умовою, далі він не обробляється. Якщо перша умова не співпало, йде обробка другого умови, якщо воно співпало, обробка припиняється, якщо немає, йде обробка третього умови і так далі поки не перевірятися всі умови, якщо жодне з умов не збігається, пакет просто знищується. Пам'ятайте, в кожному кінці списку стоїть неявний deny any (заборонити весь трафік). Будьте дуже уважні з цими правилами, які я виділив, тому що дуже часто відбуваються помилки при конфігурації.

ACL поділяються на два типи:

- Стандартні (Standard): можуть перевіряти тільки адреси джерел
- Розширені (Extended): можуть перевіряти адреси джерел, а також адреси отримувачів, в разі IP ще тип протоколу і TCP / UDP порти

Позначаються списки доступу або номерами, або символьними іменами. ACL також використовуються для різних мережевих протоколів. Позначаються в стандартному списку від 1 до 99.

Символьні ACL поділяються теж на стандартні і розширені. Розширені нагадаю можуть перевіряти набагато більше, ніж стандартні, а й працюють вони повільніше, так як доведеться заглядати всередину пакета, на відміну від стандартних де ми дивимося тільки поле Source Address (Адреса відправника). При створенні ACL кожен запис списку доступу позначається порядковим номером, за замовчуванням в рамках десяти (10, 20, 30 і т.д). Завдяки чому, можна видалити певний запис і на її місце вставити іншу, але ця можливість з'явилася в Cisco IOS 12.3, до 12.3 доводилося ACL видаляти, а потім створити заново повністю. Не можна розмістити понад 1 списку доступу на інтерфейс, на протокол, на напрям. Пояснюю: якщо у нас є маршрутизатор і у нього є інтерфейс, ми можемо на вхідне напрямок для IP-протоколу розмістити тільки один список доступу, наприклад під номером 10. Ще одне правило, яке стосується самих маршрутизаторів, ACL не діє на трафік, згенерований самим маршрутизатором .

Для фільтрації адрес в ACL використовується WildCard-маска. Це зворотна маска. Беремо шаблонне вираз: 255.255.255.255 і віднімаємо від шаблону звичайну маску.

255.255.255.255-255.255.255.0, у нас виходить маска 0.0.0.255, що є звичайною маски 255.255.255.0, тільки 0.0.0.255 є WildCard маскою.

Види ACL:

Динамічний (Dynamic ACL)

Дозволяє зробити наступне, наприклад у вас є маршрутизатор, який підключений до якогось сервера і нам потрібно закрити доступ до нього з

зовнішнього світу, але в той же час є кілька людей, які можуть підключатися до сервера.

Налаштовуємо динамічний список доступу, прикріплюємо його на вхідному напрямку, а далі людям, яким потрібно підключитися, підключатися через Telnet Цей пристрій, в результаті динамічний ACL відкриває прохід до сервера, і вже людина може зайти скажімо через HTTP потрапити на сервер. За замовчуванням через 10 хвилин цей прохід закривається і користувач змушений ще раз виконати Telnet щоб підключитися до пристрою.

Рефлексивний (Reflexive ACL)

Тут ситуація дещо відрізняється, коли вузол в локальній мережі відправляє TCP запит в Інтернет, у нас повинен бути відкритий прохід, щоб прийшов TCP відповідь для установки з'єднання. Якщо проходу не буде – ми не зможемо встановити з'єднання, і ось цим проходом можуть скористатися зловмисники, наприклад проникнути в мережу. Рефлексивні ACL працюють таким чином, блокується повністю не пройшли ідентифікацію (deny any) але формується ще один спеціальний ACL, який може читати параметри сесії користувачів, які сгенерірованни з локальної мережі і для них відкривати прохід в deny any, в результаті виходить що з Інтернету не зможуть встановити з'єднання. А на сесії сгенерірованни з локальної мережі будуть приходити відповіді.

Обмеження за часом (Time-based ACL)

Звичайний ACL, але з обмеженням по часу, ви можете ввести спеціальний розклад, яке активує ту чи іншу запис списку доступу. І зробити так, наприклад пишемо список доступу, в якому забороняємо HTTP-доступ протягом робочого дня і вішаємо його на інтерфейс маршрутизатора, тобто, співробітники підприємства прийшли на роботу, їм закривається HTTP-доступ, робочий день закінчився, HTTP-доступ відкривається ,

Налаштування

Самі ACL створюються окремо, тобто це просто якийсь список, який створюється в глобальному конфіги, потім він присвоюється до інтерфейсу і

тільки тоді він і починає працювати. Необхідно пам'ятати деякі моменти, для того, щоб правильно налаштувати списки доступу:

Обробка ведеться строго в тому порядку, в якому записані умови

- Якщо пакет збігся з умовою, далі він не обробляється
- В кінці кожного списку доступу варто неявний deny any (заборонити все)
- Розширені ACL потрібно розміщувати як можна ближче до джерела, стандартні ж якомога ближче до одержувача
- Не можна розмістити понад 1 списку доступу на інтерфейс, на протокол, на напрям
- ACL не діє на трафік, згенерований самим маршрутизатором
- Для фільтрації адрес використовується WildCard маска

Стандартний список доступу

Router (config) # access-list <номер списку від 1 до 99> {permit | deny | remark} {address | any | host} [source-wildcard] [log]

permit: дозволити

deny: заборонити

remark: коментар про список доступу

address: забороняємо або дозволяємо мережу

any: дозволяємо або забороняємо все

host: дозволяємо або забороняємо хосту

source-wildcard: WildCard маска мережі

log: включаємо логгіроване пакети проходять через даний запис ACL

Прикріплюємо до інтерфейсу

Router (config-if) #ip access-group <номер списку або ім'я ACL> {in | out}

- in: вхідний напрямок
- out: віхідний напрямок

Ущільнення ACL

Маски підмереж можна також представити у вигляді запису фіксованої довжини. Наприклад, 192.168.10.0/24 відповідає 192.168.10.0 255.255.255.0.
В списку вказано принцип ущільнення діапазону мереж в єдину мережу для оптимізації списку ACL. Враховуються такі мережі.

192.168.32.0/24

192.168.33.0/24

192.168.34.0/24

192.168.35.0/24

192.168.36.0/24

192.168.37.0/24

192.168.38.0/24

192.168.39.0/24

Перші два октету і останній октет однакові для кожної мережі. Дана таблиця служить поясненням принципу ущільнення мереж в єдину мережу.

Третій октет попередніх мереж може бути записаний так, як зазначено в цій таблиці, відповідно до позиції біта октету і значенням адреси для кожного біта [4].

Десятичное значение	128	64	32	16	8	4	2	1
32	0	0	1	0	0	0	0	0
33	0	0	1	0	0	0	0	1
34	0	0	1	0	0	0	1	0
35	0	0	1	0	0	0	1	1
36	0	0	1	0	0	1	0	0
37	0	0	1	0	0	1	0	1
38	0	0	1	0	0	1	1	0
39	0	0	1	0	0	1	1	1
	M	M	M	M	M	D	D	D

Рисунок 2.1 – Адреси бітів октету

2.3 Розширені списки доступу

Розширений список доступу (ACL) дозволяють фільтрувати трафік по великій кількості критеріїв.

Отже, розширений ACL може бути іменований і нумерований. У будь-якому випадку, він дозволяє фільтрувати трафік за такими параметрами:

- Адреса відправника
- Адреса одержувача
- TCP / UDP порт відправника
- TCP / UDP порт одержувача
- Протоколу, загорнутий в ip (відфільтрувати тільки tcp, тільки udp, тільки icmp, тільки gre і т.п.)
- Типу трафіку для даного протоколу (наприклад, для icmp відфільтрувати тільки icmp-reply).
- Відокремити TCP трафік, що йде в рамках встановленої TCP сесії від TCP сегментів, які тільки встановлюють з'єднання.

Нумерований розширений ACL

Нумерований розширений ACL повинен мати номер з 100-го по 199 або з 2000 по 2699. Причому номер відноситься до всього ACL (до всіх його рядках). Наприклад, щоб заборонити web трафік з адреси 192.168.0.1 треба написати наступний стандартний ACL:

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access-list 110 deny tcp host 192.168.0.1 any eq 80
R1(config)#access-list 110 permit ip any any
```

Рисунок 2.2 – написання команди для ACL

Перший рядок забороняє tcp-трафік із зазначеної адреси на 80-й порт, друга – дозволяє інший трафік. access-list 110 – позначає приналежність рядки до ACL з номером 110, далі йде дію (permit – дозволити, deny – заборонити,

або remark – коментар «для себе»). Потім йде протокол (в CCNA розглядаються тільки три протоколи tcp, udp і ip). Потім йде інформація про відправника пакета (адреса, можливо, wildcard маска, можливо, порт відправника), за тим - те ж саме про одержувача. У нашому прикладі першого рядка порт відправника не заданий, тобто трафік, який буде заборонений може відправлятися з будь-якого порту відправника, порт ж одержувача повинен бути 80.

Нумерований ACL не можна відредагувати, можна тільки додати рядок в кінець. У нашому прикладі додавати рядок в кінець не має сенсу, так як permit ip any any дозволяє весь трафік і далі перевірка не проводиться. Єдиний спосіб відредагувати нумерований ACL – вивести шматок конфіга з ним, скопіювати в блокнот існуючий ACL, відредагувати його, видалити старий, вставити новий. Припустимо, нам треба додати в ALC 110 заборона трафіку ще й з другої половини мережі 192.168.0.0, з портів вище 1024 на порт 80. Цей рядок повинна встати за логікою вещей між першою і другою. Виводимо конфиг (весь, або тільки частину, з acl):

```
R1#show running-config
…
!
access-list 110 deny tcp host 192.168.0.1 any eq 80
access-list 110 permit ip any any
!
…
```

Рисунок 2.3 – Додавання команди заборони трафіку в ACL

Іменований розширений ACL

ACL з ім'ям MY_ACL, який робить те ж саме, що і ACL 110. Як аргумент команди ip access-list необхідно вказати не тільки ім'я, але і тип ACL (standard – стандартний і extended – розширений), так як маршрутизатор не може сам визначити тип. У разі використання нумерованного, тип визначався за номером (з 100-го по 199 або з 2000 по 2699). Усередині іменованого ACL вже не треба згадувати імені або номера, так як ми потрапляємо в режим редагування конкретного ACL (config-ext-nacl) і все рядки ACL вводимо відразу починаючи зі слова deny, permit або remark.

На відміну від нумерованного, іменований ACL можна редагувати через підрядник кожному рядку іменованого ACL призначається номер із зсувом 10, тобто рядки нумеруються 10,20,30,40, і т.п. Завдяки цьому, можна вставити рядок між існуючими. Наприклад, якщо ми зайдемо в редагування ACL MY_ACL[5].

2.4 Списки керування доступом

Access-lists, Access-control-lists (ACL) – списки контролю доступу. Існує кілька різновидів аксесуари-листів, що застосовуються на маршрутизаторах і комутаторах Cisco. Аксесуари-листи використовуються для фільтрації трафіку або для визначення класів трафіку при застосуванні політик. Список доступу являє собою набір рядків виду умова-дія. Рядок аксесуари-листа називається access-control-entry (ACE). Умовою може бути відповідність пакету певним протоколу або набору параметрів. Дією може бути дозвіл пакета (permit), або заборона (deny). Для списків доступу справедливі наступні правила:

- Створений список доступу не діє, поки він не застосований до конкретного інтерфейсу.
- Список доступу застосовується на інтерфейсі в конкретному напрямку – для вихідного, або вхідного трафіку (inbound / outbound).
- До інтерфейсу можна застосувати тільки по одному аксесуари-листу на протокол (ip), на напрям (in / out).
- Список доступу перевіряється рядок за рядком до першого збігу. Решта рядки ігноруються.
- В кінці будь-якого IP аксесуари-листа мається на увазі що забороняє правило (implicit deny). Пакет, який не потрапив ні під одну умову в списку, відкидається, відповідно до правила implicit deny.
- Рекомендується більш специфічні правила вказувати на початку аксесуари-листа, а більш загальні – в кінці.

- Нові рядки за умовчанням дописують в кінець списку.
- Окремий рядок можна видалити з іменованого аксесуари-листа, інші ACL видаляються лише цілком.
- Список доступу повинен мати принаймні один permit, інакше він буде блокувати весь трафік.
- Інтерфейс, якому призначений неіснуючий аксесуари-лист не фільтрує трафік.
- IP Extended Access-lists застосовуються якомога ближче до джерела трафіку.

За способом створення списки доступу діляться на стандартні, розширені, і іменовані. Найзручніше працювати з іменованими.

Стандартний Access-list

Фільтрує тільки по ip адресою джерела. Повинен мати номер в діапазоні 1-99.

Розширений Access-list

Фільтрує за адресами джерела і одержувача, по протоколам 3, 4 рівня. Повинен мати номер в діапазоні 100-199.

Стандартні і розширені нумеровані списки доступу підтримують наступні види списків доступу для IP:

- Стандартні списки доступу (перевіряють адресу відправника пакета)
- Розширені списки доступу (перевіряють адресу відправника, адресу одержувача і ще ряд параметрів пакета).[6]

3 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ ДОСТУПУ ДО ЇЇ СЕГМЕНТІВ В CISCO

Сегментація мережі – важливий інструмент забезпечення інформаційної безпеки (ІБ), що дозволяє значно знизити ймовірність інцидентів безпеки і пов'язаний з ними збиток навіть у разі проникнення зловмисників всередину.

3.1 Важливість використання сегментації в корпоративній мережі

Корпоративна мережа стала критично важливим інструментом бізнесу багатьох компаній, оскільки саме вона забезпечує роботу безлічі бізнес-процесів, пов'язаних з передачею інформації. У той же час загрози інформаційній безпеці безперервно еволюціонують, і потреба в ефективних засобах захисту зростає з кожним днем.

Довгий час увагу фахівців з інформаційної безпеки було зосереджено в основному на захист периметра мережі. Але в сучасних мережах класичне поняття периметра поступово розмивається. Користувачі підключаються до мережі різними способами, включаючи доступ через дротові і бездротові сегменти, а також VPN-підключення. При цьому в рамках IT-інфраструктури організації, як правило, існує безліч типів користувачів і пристроїв, яким для виконання своєї роботи потрібен доступ до різних ресурсів мережі. Реалізація належного розмежування доступу в сучасних розподілених і динамічних IT-інфраструктурах є досить непростим завданням. З урахуванням великої кількості векторів атаки, що дозволяють зловмисникам і шкідливому програмному забезпеченню проникати в корпоративну IT-інфраструктуру, ймовірність порушення інформаційної безпеки можна вважати вкрай високою, як правило, це питання часу.

Одним з популярних заходів, спрямованих на зниження шкоди від проникнення зловмисника в корпоративну IT-інфраструктуру, є сегментація

мережі. Мається на увазі попереднім етапом сегментації є поділ користувачів і ресурсів мережі на ізольовані одна від одної групи (закриті групи користувачів і ресурсів). Обмін даними між цими групами контролюється або взагалі блокується в залежності від вимог політики безпеки організації.

Принципи, які використовуються для поділу користувачів на групи, визначаються прийнятою в організації політикою безпеки. В якості одного з типових варіантів поділу користувачів і пристроїв за категоріями можна навести такий: співробітники, тимчасовий персонал, гості, користувачі з пристроями, що не відповідають корпоративній політиці (карантин і так далі. Крім того, співробітники можуть бути розміщені не в одну групу, а розділені на кілька груп, наприклад рядові співробітники, керівництво, топ-менеджмент, бухгалтерія тощо.

Сегментація мережі допомагає значно знизити ризики інформаційної безпеки за рахунок обмеження можливостей зловмисників по нанесенню збитку в разі їх проникнення всередину периметра, що захищається.

Поділ користувачів на групи і сегментація мережі не є самоціллю, але можуть бути дуже важливими для підвищення безпеки бізнес-процесів. У цьому сенсі такі бізнес-процеси спираються на сегментацію. Політика безпеки організації може вимагати, щоб співробітники різних категорій отримували доступ тільки до тих корпоративних ресурсів, до яких їм необхідно мати доступ для виконання своєї роботи. Наприклад, доступ до групи серверів системи ERP з конфіденційною бізнес-інформацією може надаватися тільки керівництву, а доступ до конфіденційних баз HR – тільки співробітникам HR-підрозділу і, можливо, керівництву. У той же час персонал нижчої ланки або тимчасові співробітники можуть отримувати доступ тільки до обмеженого набору корпоративних додатків, наприклад до кооперативної системи CRM і електронній пошті, і не мати права доступу до всіх інших ресурсів мережі.

Вплив сегментації на бізнес-процеси в описуваних випадках полягає в тому, що сегментація важлива для забезпечення інформаційної безпеки, а оскільки інциденти в області ІБ можуть призводити до порушення

доступності, то сегментація також сприяє підвищенню доступності бізнес-процесів.

Крім того, існує ціла група бізнес-процесів, впровадження яких при відсутності сегментації є вкрай небажаним. Наприклад, до цієї групи належать процеси, пов'язані з доступом до корпоративної мережі користувачів, які не є співробітниками організації. Типовим прикладом є надання доступу в мережу (або в Інтернет) так званим гостьовим користувачам. В якості інших варіантів можна згадати доступ співробітників компанії-партнера, доступ аудиторів, підключення в мережу пристроїв, що належать іншим організаціям, наприклад банкоматів, цифрових вивісок, платіжних терміналів. Ще одним сценарієм, в якому рекомендується використання сегментації, є розмежування доступу між співробітниками афілійованих структур, що використовують одну і ту ж мережу.

Подібних сценаріїв може бути багато, але всі вони призводять до задачі реалізації сегментації на практиці.

3.2 Приклади традиційних методів сегментації

При реалізації сегментації мережі необхідно вирішити 3 ключові завдання:

- визначити приналежність користувача до потрібної групи при його підключенні до мережі (задача 1).
- ізолювати трафік користувача даної групи від трафіку користувачів інших груп при передачі по мережі (задача 2).
- забезпечити доступ користувача до тих ресурсів, до яких він повинен мати доступ і, як правило, заблокувати доступ до всіх інших ресурсів (завдання 3).

Завдання 1 зазвичай вирішується за допомогою аутентифікації та авторизації з використанням протоколу 802.1x на RADIUS-сервері (часто з використанням даних з корпоративної служби каталогів, наприклад Active

Directory). Можливе застосування і інших методів – статичного приміщення користувачів в залежності від порту підключення, VLAN'a, IP-підмережі, авторизації по MAC-адресу і так далі в залежності від можливостей використовуваного сервера AAA і обладнання.

Завдання 2 традиційно вирішується шляхом створення окремих віртуальних топологій для кожної групи користувачів. Як правило, це робиться за допомогою тих чи інших засобів віртуалізації мережі. У разі невеликих мереж цими засобами зазвичай є VLAN-и і транки 802.1Q. Також часто використовуються технології Рівня 3, наприклад Multi-VRF CE (VRF-Lite). Для великих мереж характерно застосування MPLS VPN.

Завдання 3, як правило, вирішується пакетної фільтрацією на основі IP-адрес. Контроль доступу може бути реалізований як такими «грубими» засобами, як списки контролю доступу (ACL) на елементах мережевої інфраструктури, так і «тонкої» фільтрацією на системах захисту нового покоління (NGFW, NGIPS), але фундаментальний принцип залишається тим же – базовим критерієм для прийняття рішення про допуск / недопуск є IP-адреса. Фільтрація проводиться в одному або декількох місцях, призначених для обміну трафіком між групами користувачів.

Іноді пакетну фільтрацію використовують без створення віртуальних топологій, тобто пакетні фільтри одночасно служать для вирішення як завдання 2, так і завдання 3. [7]

3.3 Проектування корпоративної мережі з використанням традиційних методів сегментації

Відповідно по поставленої задачі, для адресації підмереж робочих станцій виділено адресні простори мережі 168.142.0.0 /16. Простір 168.142.0.0 /16 дозволяє виділити близько 65536 IP-адрес.

Слід врахувати, що кожна підмережа підключається до відповідного маршрутизатора єдиної мережі передачі даних. Для коректної маршрутизації і

обміну інформацією між вузлами підмережі потрібно 29 IP-адрес на кожну підмережу робочих станцій, з яких 28 IP-адрес призначаються відповідним робочим станціям, а одна IP-адреса призначається маршрутизатору, підключеному через вказаний інтерфейс до даної підмережі.

Необхідно використовувати 5 біт, які дозволять адресувати 32 вузла (2^5 = 32 IP-адрес). Додаткові адреси можна використовувати при розширенні підмережі або як резерв.

Використовуючи нотацію CIDR і безперервне виділення блоків IP-підмереж, виділимо 6 IP-підмереж (S_H) з 32 доступними IP-адресами в кожній підмережі. Слід пам'ятати, що перші 2 байта мережі 168.142.0.0 /16 не зміняться, а для виділення підмереж можна використовувати тільки останні 2 байта. Застосуємо маску підмережі довжиною 27 біт (32 – 5 = 27 біт для адресації мережі, 5 біт для адресації вузлів). Запис першої IP-підмережі в двійковій нотації буде мати вигляд:

168.142.0.0 – 10101000 10001110 00000000 00000000

255.255.255.224 – 11111111 11111111 11111111 11100000

Перша IP-адреса мережі буде відрізняться тільки одним молодшим бітом:

168.142.0.1 – 10101000 10001110 00000000 00000001

Далі послідовно другий, третій і наступні адреси формуються з 3 молодших біт:

168.142.0.2 – 10101000 10001110 00000000 00000010

168.142.0.3 – 10101000 10001110 00000000 00000011

168.142.0.4 – 10101000 10001110 00000000 00000100

168.142.0.5 – 10101000 10001110 00000000 00000101

168.142.0.6 – 10101000 10001110 00000000 00000110 … і т.д.

Аж до широкомовної адреси мережі, в якої всі молодші біти дорівнюють одиниці:

168.142.0.31 – 10101000 10001110 00000000 00011111

Відповідно, наступна IP-підмережа буде мати адресу 168.142.32.0 /27, або у двійковій нотації:

168.142.0.32 – 10101000 10001110 00000000 00100000

255.255.255.224 – 11111111 11111111 11111111 11100000

З пулом IP-адрес, що відповідають масці підмережі:

168.142.0.33 – 10101000 10001110 00000000 00100001

168.142.0.34 – 10101000 10001110 00000000 00100010

168.142.0.35 – 10101000 10001110 00000000 00100011

168.142.0.36 – 10101000 10001110 00000000 00100100

168.142.0.37 – 10101000 10001110 00000000 00100101

168.142.0.38 – 10101000 10001110 00000000 00100110

168.142.0.39 – 10101000 10001110 00000000 00100111

168.142.0.40 – 10101000 10001110 00000000 00101000 … і т.д.

Широкомовна адреса мережі 168.142.0.63 /27:

168.142.0.63 – 10101000 10001110 00000000 00111111

Наступні мережі знаходяться аналогічним чином. Нарешті, шоста IP-підмережа буде мати адресу мережі 168.142.0.160 /27, або у двійковій нотації:

168.142.0.160 – 10101000 10001110 00000000 10100000

255.255.255.224 – 11111111 11111111 11111111 11100000

З пулом IP-адрес, що відповідають масці підмережі:

168.142.0.161.0 – 10101000 10001110 00000000 10100001

168.142.0.162.0 – 10101000 10001110 00000000 10100010

168.142.0.163.0 – 10101000 10001110 00000000 10100011

168.142.0.164.0 – 10101000 10001110 00000000 10100100

168.142.0.165.0 – 10101000 10001110 00000000 10100101

168.142.0.166.0 – 10101000 10001110 00000000 10100110

168.142.0.167.0 – 10101000 10001110 00000000 10100111

168.142.0.168.0 – 10101000 10001110 00000000 10101000 … і т.д.

Широкомовна адреса мережі 168.142.0.191.0 /27:

168.142.0.191 – 10101000 10001110 00000000 10111111

Адресний простір, що залишився дозволяє організувати додатковий резерв при розширенні мережі. Доступний пул IP-адрес в двійковій і десятковій нотації для кожної з 6 підмереж наведено в додатку А.

Складемо план адресації для підмереж маршрутизаторів. Відповідно до завдання, для адресації підмереж (S_R) виділено адресний простір мережі 176.119.77.0 /24. Даний простір дозволяє виділити близько 256 IP-адрес (32 – 24 = 8 біт, 2^8 = 256). Мережа 176.119.77.0 /24 використовує 3 байти для адресації мережі, останній байт вільний. Запис мережі в двійковій нотації матиме вигляд:

176.119.77.0 – 10110000 01110111 01001101 00000000
255.255.255.0 – 11111111 11111111 11111111 00000000

Маршрутизація пакетів між будь-якими підмережами забезпечується при наявності 6 IP-підмереж. Використовуємо 8 підмереж маршрутизаторів.

Кожна підмережа маршрутизаторів об'єднує 2 маршрутизатора. Необхідно використовувати 2 біта, які дозволять адресувати 4 адреси (2^2 = 4 IP-адрес).

Використовуючи нотацію CIDR і безперервне виділення блоків IP-підмереж, виділимо 6 IP-підмереж з 4 доступними IP-адресами в кожній підмережі. Перші 3 байти мережі 176.119.77.0/24 не змінюються, для виділення підмереж варто використовувати останній байт. Маска підмережі буде довжиною 30 біт (32 – 2 = 30 біт для адресації мережі, 2 біти для адресації маршрутизаторів). Запис першої IP-підмережі в двійковій нотації матиме вигляд:

176.119.77.0 – 10110000 01110111 01001101 00000000

255.255.255.252 – 11111111 11111111 11111111 11111100

Відповідно до маски, мережа має наступні IP-адреси (змінюються два молодших біта):

176.119.77.1 – 10110000 01110111 01001101 00000001

176.119.77.2 – 10110000 01110111 01001101 00000010

Широкомовна адреса мережі 176.119.77.0 /30

176.119.77.3 – 10110000 01110111 01001101 00000011

Наступна IP-підмережа матиме адресу 176.119.77.4 /30, або в двійковій нотації:

176.119.77.4 – 10110000 01110111 01001101 00000100

255.255.255.252 – 11111111 11111111 11111111 11111100

176.119.77.5 – 10110000 01110111 01001101 00000101

176.119.77.6 – 10110000 01110111 01001101 00000110

Широкомовна адреса мережі 176.119.77.7 /30

176.119.77.7 – 10110000 01110111 01001101 00000111

Наступна IP-підмережа матиме адресу 176.119.77.8 /30, або в двійковій нотації:

176.119.77.8 – 10110000 01110111 01001101 00001000

255.255.255.252 – 11111111 11111111 11111111 11111100

176.119.77.9 – 10110000 01110111 01001101 00001001

176.119.77.10 – 10110000 01110111 01001101 00001010

Широкомовна адреса мережі 176.119.77.11 /30

176.119.77.11 – 10110000 01110111 01001101 00001011

Наступна IP-підмережа матиме адресу 176.119.77.12 /30, або в двійковій нотації:

176.119.77.12 – 10110000 01110111 01001101 00001100

255.255.255.252 – 11111111 11111111 11111111 11111100

176.119.77.13 – 10110000 01110111 01001101 00001101

176.119.77.14 – 10110000 01110111 01001101 00001110

Широкомовна адреса мережі 176.119.77.15 /30

176.119.77.15 – 10110000 01110111 01001101 00001111

Наступна IP-підмережа матиме адресу 176.119.77.16 /30, або в двійковій нотації:

176.119.77.16 – 10110000 01110111 01001101 00010000

255.255.255.252 – 11111111 11111111 11111111 11111100

176.119.77.17 – 10110000 01110111 01001101 00010001

176.119.77.18 – 10110000 01110111 01001101 00010010

Широкомовна адреса мережі 176.119.77.19 /30

176.119.77.19 – 10110000 01110111 01001101 00010011

Нарешті, шоста IP-підмережа буде мати адресу 176.119.77.20 /30, або в двійковій нотації:

176.119.77.20 – 10110000 01110111 01001101 00010100

255.255.255.252 – 11111111 11111111 11111111 11111100

Пул IP-адрес:

176.119.77.21 – 10110000 01110111 01001101 00010101

176.119.77.22 – 10110000 01110111 01001101 00010110

Широкомовна адреса мережі 176.119.77.23 /30

176.119.77.23 – 10110000 01110111 01001101 00010111

Доступний пул IP-адрес в двійковій і десятковій нотації для кожної з 6 підмереж наведено в додатку Б.

Також варто згадати про адресацію бездротового сегмента мережі., кількість бездротових клієнтів в даній мережі прирівнюється до 30, адресація бездротового сегмента мережі представлена в додатку В.

Для використання wi-fi роутера (маршрутизатора) в корпоративнй мережі, варто використовувати режим безпеки – WPA2 Enterprice, але для його використання варто налаштувати сервер та роутер.

RADIUS сервер (Remote Authentication Dial In User Service) забезпечує централізоване управління аутентифікацією і авторизацією комп'ютерів, які «хочуть» підключитися до мережі і скористатися наданими нею послугами. Провайдери послуг Інтернету і компанії часто використовують сервіс RADIUS для управління доступом в Інтернет або у внутрішні мережі, бездротові мережі або до вбудованих послуг електронної пошти. [8]

Налаштування RADIUS server на Router3, має наступний вигляд :

```
Router> en
Router#conf t
Router(config)#username Admin3 secret admin3
Router(config)#radius-server host 168.142.0.66
```

```
Router(config)#radius-server key radius33
Router(config)#aaa new
Router(config)#aaa new-model
Router(config)#aaa authentication login default group radius
local
Router(config)#line console 0
Router(config-line)#login authentication default
Router(config-line)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
ex

Router con0 is now available

Press RETURN to get started.


User Access Verification

Username: Admin3
Password:

Router>en
Router#
```

Безпосереднє налаштування на сервері, представлено на рисунку.

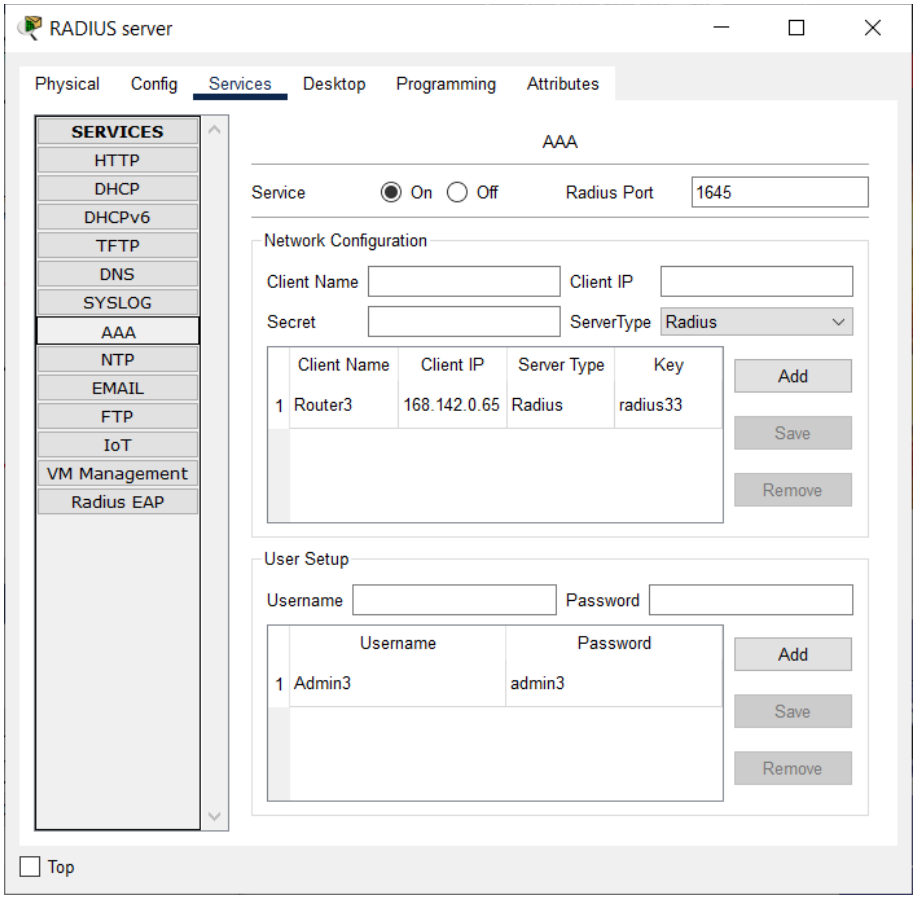

Рисунок 3.1 – Налаштування RADIUS server

VLAN (Virtual Local Area Network, віртуальна локальна мережа) – це функція в роутерах і комутаторах, що дозволяє на одному фізичному мережевому інтерфейсі (Ethernet, Wi-Fi інтерфейсі) створити кілька віртуальних локальних мереж. VLAN використовують для створення логічної топології мережі, яка ніяк не залежить від фізичної топології. [9]

Технологія VLAN забезпечує:

- гнучку побудову мережі (VLAN дозволяє зробити сегментацію локальної мережі на підмережі за функціональною ознакою незалежно від територіального розташування пристроїв. Тобто пристрої однієї підмережі VLAN можуть бути підключені до різних комутаторів, віддаленим один від одного. І навпаки, до одного комутатора можуть бути підключені пристрої, що відносяться до різних підмереж VLAN);
- збільшення продуктивності (VLAN розділяє підмережу на окремі широкомовні домени. Це означає, що широкомовні повідомлення отримуватимуть тільки пристрої, що знаходяться в одній VLAN-підмережі. Побудова системи з використанням технології VLAN дозволяє зменшити широкомовний трафік усередині мережі, тим самим знижується навантаження на мережеві пристрої і поліпшується продуктивність системи в цілому);

Поліпшення безпеки (Пристрої з різних підмереж VLAN не можуть спілкуватися один з одним, що зменшує шанси провести несанкціонований доступ до пристроїв системи. Зв'язок між різними підмережами можлива тільки через маршрутизатор. Крім того, використання маршрутизатора дозволяє налаштувати політики безпеки, які можуть бути застосовані відразу до всієї групи пристроїв, що належить одній підмережі). [10]

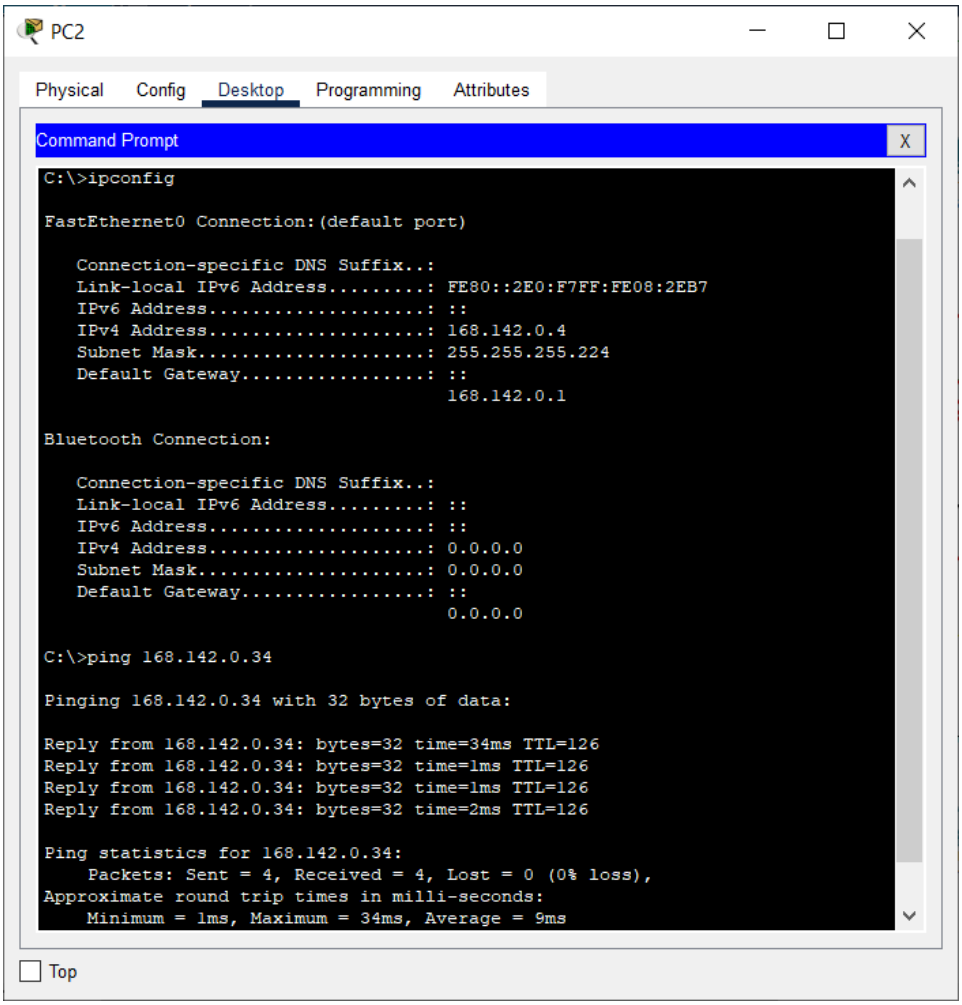

Рисунок 3.2– Виконання команди ping між PC2 (відділ роботи з персоналом) та PC6 (відділ Керівництво)

Налаштування VLAN у відділі «Керівництво», створюємо VLAN 2, оскільки VLAN 1 заданий та є дефолтним. До VLAN 2, буде входити діапазон інтерфейсів fa (Fast Ethernet) 0/3 – 5 (відповідні персональні комп'ютери – PC5, PC6, PC7).

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#interface range fastEthernet 0/3-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#ex
Switch(config)#ex
Switch#sh vl br
```

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1
2    leadership32_62                   active    Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

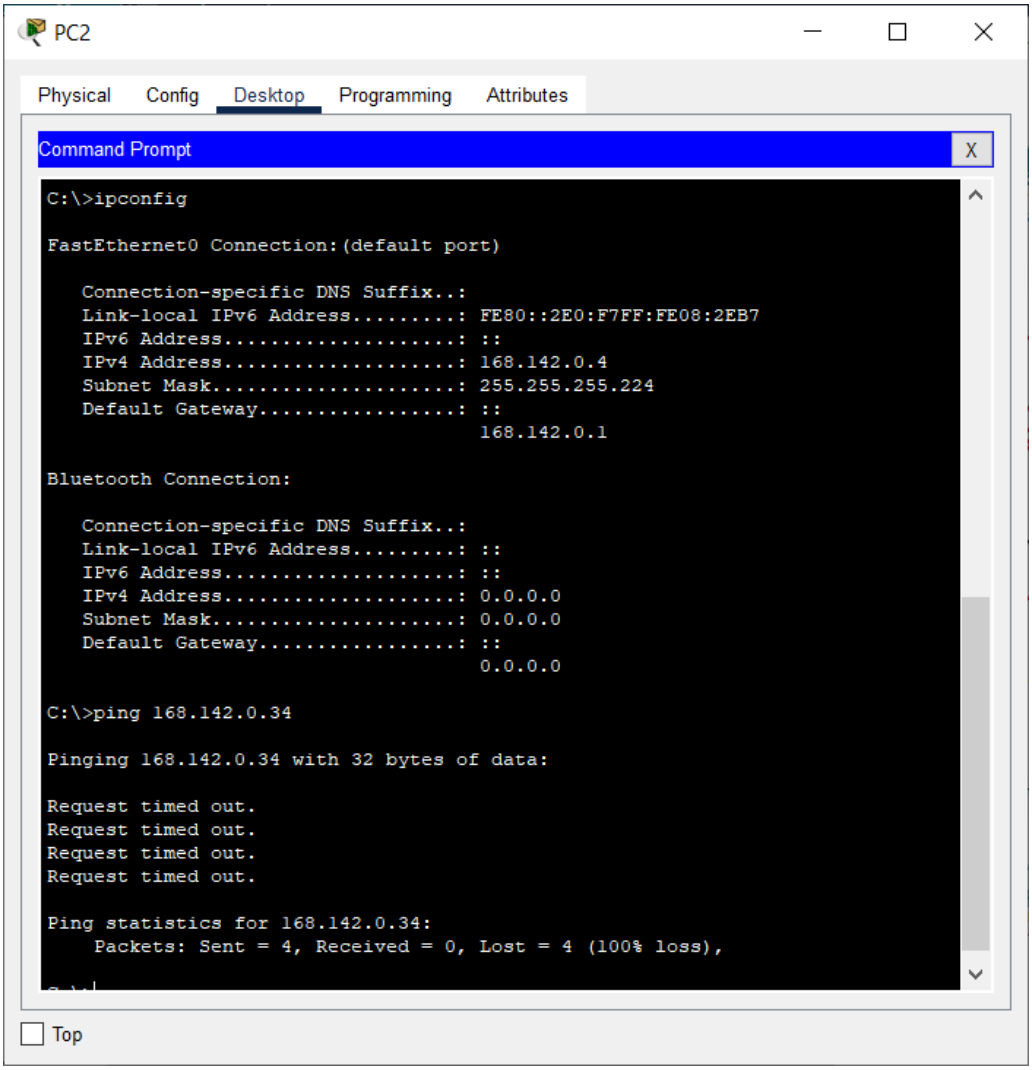

Рисунок 3.3 – Повторне виконання команди ping між PC2та PC6 (після налаштування VLAN у відділі Керівництво)

По аналогії необхідно створити VLAN у відділі IT-фахівці. До створеного VLAN буде входити діапазон інтерфейсів Fast Ethernet 0/3 – 5 (відповідні персональні комп’ютери – PC20, PC21, PC22).

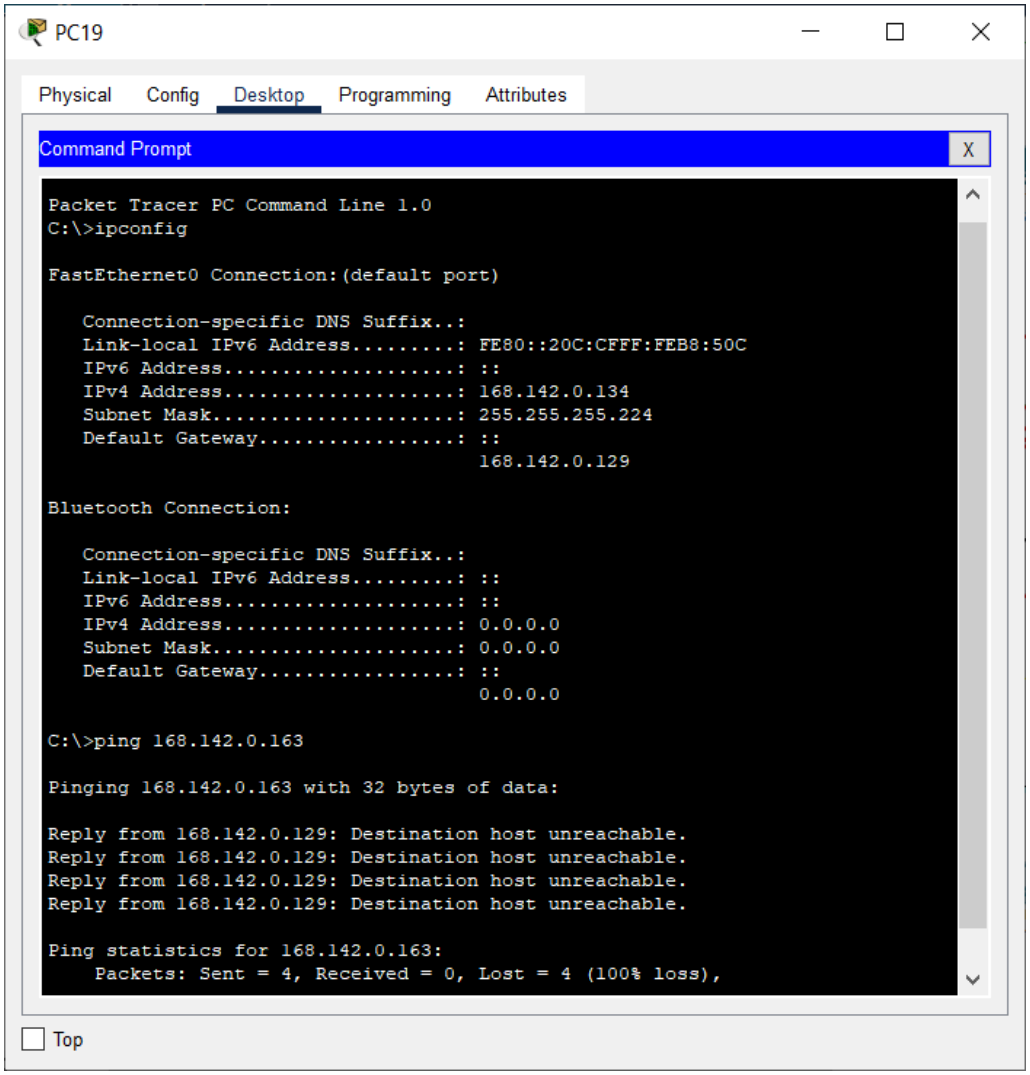

Рисунок 3.4– Виконання команди ping між PC19 (відділ маркетингу та реклами) та PC21 (відділ IT-фахівці)

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#name IT_specialist_160_180
Switch(config-vlan)#interface range fastEthernet 0/3-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 2
Switch(config-if-range)#ex
Switch(config)#ex
Switch#sh vl br
```

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, 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
2    IT_specialist_160_180             active    Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

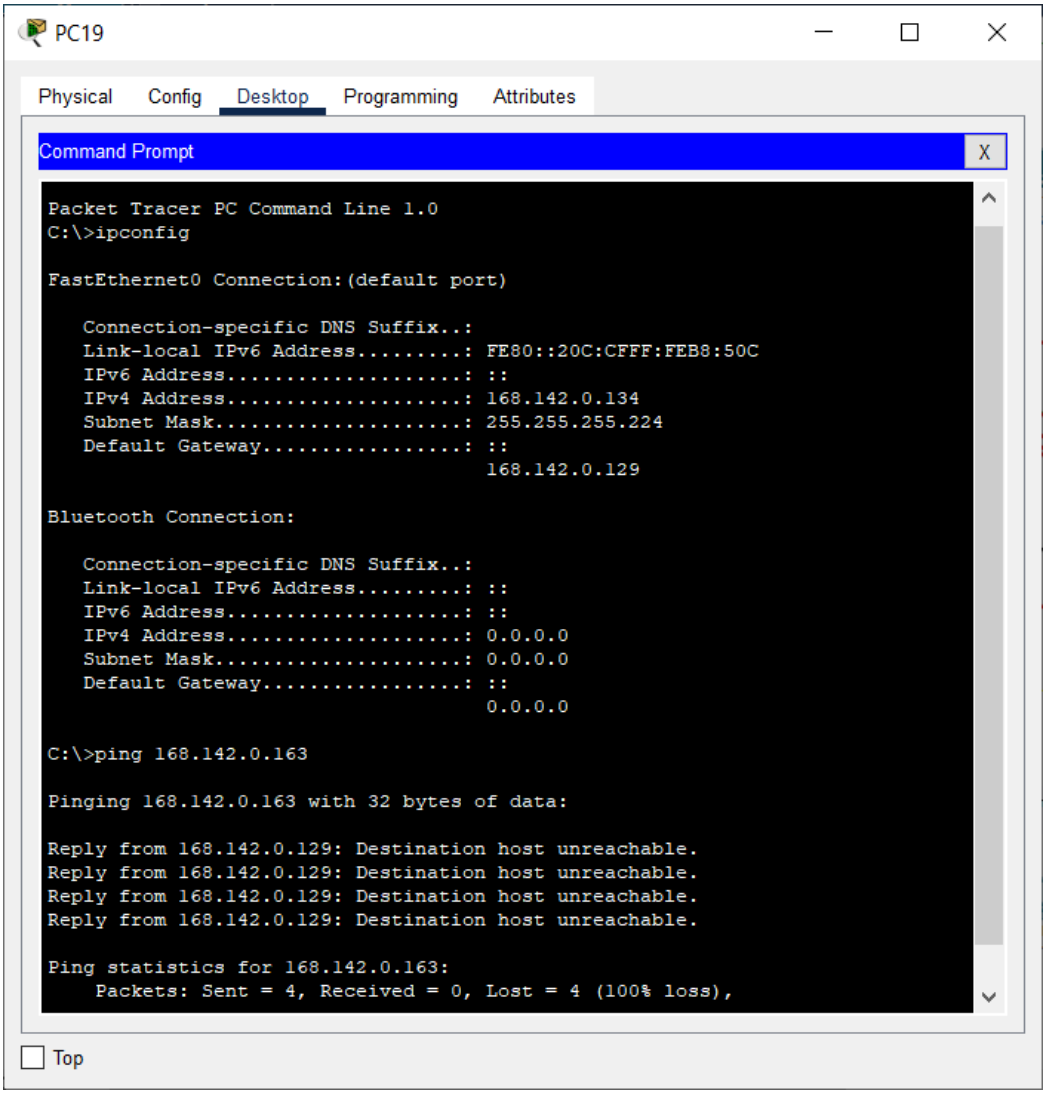

Рисунок 3.5– Повторне виконання команди ping між PC19 та PC21 (після налаштування VLAN у відділі IT-фахівці)

Наступним кроком в проектуванні мережі є використання AccessPoint, як точку доступу для роздачі Wi-Fi. Так як, вірогідність того, що дана мережа буде рости і розташовуватися не на одному, а на декількох поверхах будівлі, ні один Wi-Fi роутер (маршрутизатор) – не зможе надсилати сигнал на такі далекі відстані та площі. Тому є доцільним використовувати саме AccessPoint.

Даний AccessPoint для Wi-Fi буде розташовуватися в гостьовій кімнаті. Для налаштування AccessPoint, впершу чергу варто ввести ідентифікатор мережі WiFi-Guest та вибрати один з типів аутентифікації, краще використовувати WPA2-PSK та вводимо пароль, при необхідності можна змінити тип шифрування даних.

Також варто продумати те, що дана мережа повинна бути в окремому сегменті, для цього на комутаторі варто створити VLAN. В даному випадку, ніяких раніше створених VLAN на цьому комутаторі не було, тому створюємо VLAN 2. Після створення VLAN 2, необхідно на порт, який з'єднується з офісним маршрутизатором додати щойно створений VLAN в trunkport.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config-if)#switchport access vlan 2
Switch(config-if)#description WiFi-Guest-AP
Switch(config-if)#end
Switch#
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface FastEthernet0/3
Switch(config-if)#switchport trunk allowed vlan 2
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport access vlan 2
Switch(config-if)#description WiFi-Guest-AP
Switch(config-if)#end
Switch#
```

Після створення VLAN, необхідно створити subinterface на маршрутизатори. Для цього необхідно виконати команди, які представлені нижче.

```
Router>en
Router#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa1/0.2
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet1/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet1/0.2, changed state to up

Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 168.142.1.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#end
```

Дана точка доступу не роздає IP-адреси, тому варто використовувати виділений DHCP-сервер, щоб потім використовувати DHCP Relay. Функція DHCP Relay призначена для того, щоб пристрої в обраному сегменті вашої мережі отримували настройки від зовнішнього DHCP-сервера.

Або ж замість DHCP-сервер, можна прямо з роутера роздавати адреси для Wi-Fi користувачів. Далі представлені команди, які допоможуть виконати це завдання, за допомогою можливостей маршрутизатора (роутера).

```
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp ?
excluded-address Prevent DHCP from assigning certain addresses
pool Configure DHCP address pools
relay DHCP relay agent parameters
Router(config)#ip dhcp pool ?
WORD Pool name
Router(config)#ip dhcp pool WiFi-pool
Router(dhcp-config)#?
default-router Default routers
dns-server Set name server
domain-name Domain name
exit Exit from DHCP pool configuration mode
network Network number and mask
no Negate a command or set its defaults
option Raw DHCP options
Router(dhcp-config)#network 168.142.1.0 255.255.255.0
Router(dhcp-config)#default-router 168.142.1.1
Router(dhcp-config)#ex
Router(config)#ip dhcp excluded-address 168.142.1.1
Router(config)#end
Router#
```

На рис. представлено успішне підключення користувачів після проектування гостьового Wi-Fi.

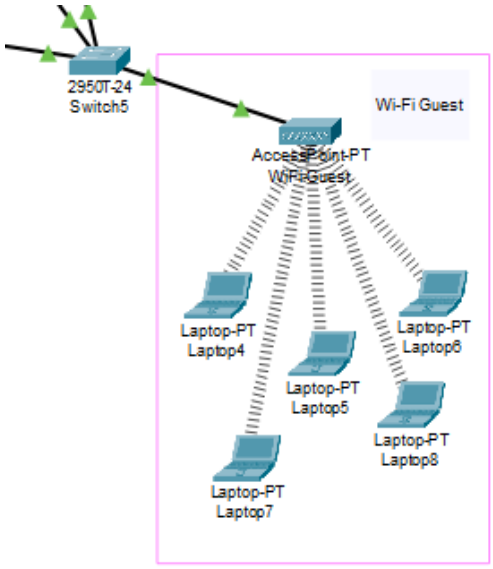

Рисунок 3.6– Підключення користувачів до гостьового Wi-Fi

Результат моделювання корпоративної мережі з використанням методів забезпечення контролю доступу до її сегментів в Cisco Packet Tracer, представлено на рис. .

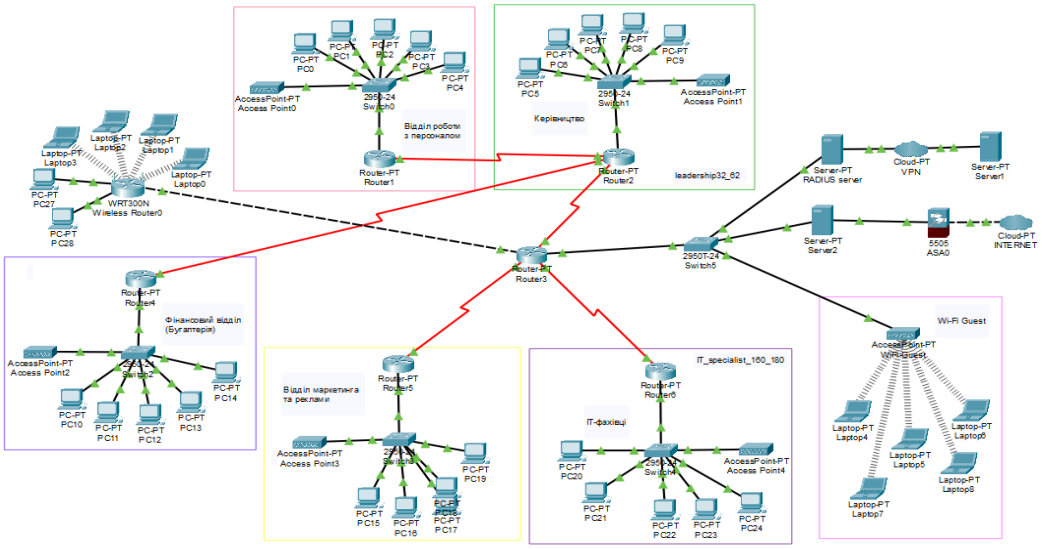

Рисунок 3.7– Модель єдиної мережі передачі даних

ВИСНОВКИ

Безпека інформації – важлива справа для будьякої фірми. Для цього наймаються спеціалісти з безпеки, які і вибудовують невидиму стіну, через яку шахраї не зможуть отримати доступа до мережі.

Одним з найпопулярніших прийомів є файєрволл чи брандмауер – програмний або програмно-апаратний елемент комп'ютерної мережі, що здійснює контроль і фільтрацію проходить через нього мережевого трафіку відповідно до заданих правил. Серед завдань, які вирішують міжмережеві екрани, основний є захист сегментів мережі або окремих хостів від несанкціонованого доступу з використанням вразливих місць в протоколах мережевий моделі OSI або в програмному забезпеченні, встановленому на комп'ютерах мережі. Міжмережеві екрани пропускають або забороняють трафік, порівнюючи його характеристики з заданими шаблонами.

Також, широке використання мають віртуальні локальні мережі – являє собою групу хостів із загальним набором вимог, які взаємодіють так, як якщо б вони були підключені до широковещательному домену незалежно від їх фізичного місцезнаходження. Має ті ж властивості, що й фізична локальна мережа, але дозволяє кінцевим членам групуватися разом, навіть якщо вони не знаходяться в одній фізичній мережі. Така реорганізація може бути зроблена на основі програмного забезпечення замість фізичного переміщення пристроїв.

Моделювання мережі в спеціальних застосунках дозволяє істотно зменшити витрати часу та грошей, бо по заздалегідь спроєкотованому макету зібрати та налагодити роботу мережі можна швидко, і до того ж не виявиться, що деяке з обладнань виявиться зайвим. Тому йя робота є майже обов’язковою для компанії.

Виявлені всі потреби, поставлена задача Змодельована мережа, відповідає стандартам безпеки,

Під час виконання роботи були визначені ті критерії, яким повина відповідати система. Було обрано технології, якими були реалізовані усі використані рішення. У підсумку була розроблема система, змодельована і перевірена на робоспособність. Вона відповідає усім нормам безпеки. При її моделюванні використовувалось надійне обладнання, з якого цю систему можна зібрати на підприємстві простим переносом налаштувань з моделі мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1 Про міжмережеві екрани – URL: https://www.smart-soft.ru/blog/mezhsetevye-ekrany-vidy/ (Дата звернення 25.05.2021)

2 Про віртуальні локальні мережі – URL: https://www.osp.ru/lan (Дата звернення 25.05.2021)

3 Про режим командної строки CISCO – URL: http://ciscotips.ru/cli-modes (Дата звернення 25.05.2021)

4 Про листи контролю доступу – URL: https://habr.com/ru/post/121806/ (Дата звернення 25.05.2021)

5 Про списки контролю доступу – URL: https://www.opennet.ru/base/cisco/access_list_intro.txt.html (Дата звернення 25.05.2021)

6 Настройка списків контрою доступу – URL: http://ciscotips.ru/acl (Дата звернення 25.05.2021)

7 Про сегментацію мережі – URL: https://www.osp.ru/lan/2017/01-02/13051372 (Дата звернення 25.05.2021)

8 Про RADIUS сервер – URL: https://qnap.ru/features/radius_serverv (Дата звернення 25.05.2021)

9 Про віртуальні локальні мережі – URL: https://www.technotrade.com.ua/Articles/what_is_vlan.php (Дата звернення 25.05.2021)

10 Про віртуальні локальні мережі – URL: https://moxa.ru/tehnologii/ethernet_network/tech-vlan/ (Дата звернення 25.05.2021)

ДОДАТКИ

ДОДАТОК А

Адресація підмереж робочих станцій

Таблиця А.1 – Опис IP-адрес

Підмережа	Пул IP-адрес	Двійкова нотація	Призначення
1	168.142.0.0 /27	10101000 10001110 00000000 00000000	Адреса підмережі
	255.255.255.224	11111111 11111111 11111111 11100000	Маска підмережі
	168.142.0.1	10101000 10001110 00000000 00000001	R1, інтерфейс 0
	168.142.0.2	10101000 10001110 00000000 00000010	H1
	168.142.0.3	10101000 10001110 00000000 00000011	H2
	168.142.0.4	10101000 10001110 00000000 00000100	H3
	168.142.0.5	10101000 10001110 00000000 00000101	H4
	168.142.0.6	10101000 10001110 00000000 00000110	H5
	168.142.0.7	10101000 10001110 00000000 00000111	
	168.142.0.8	10101000 10001110 00000000 00001000	Резерв
	……		
	168.142.0.30	10101000 10001110 00000000 00011110	Резерв
	168.142.0.31	10101000 10001110 00000000 00011111	Широкомов. адр.
2	168.142.0.32 /27	10101000 10001110 00000000 00100000	Адреса підмережі
	255.255.255.224	11111111 11111111 11111111 11100000	Маска підмережі
	168.142.0.33	10101000 10001110 00000000 00100001	R2, інтерфейс 0
	168.142.0.34	10101000 10001110 00000000 00100010	H1
	168.142.0.35	10101000 10001110 00000000 00100011	H2
	168.142.0.36	10101000 10001110 00000000 00100100	H3
	168.142.0.37	10101000 10001110 00000000 00100101	H4
	168.142.0.38	10101000 10001110 00000000 00100110	H5
	168.142.0.39	10101000 10001110 00000000 00100111	
	168.142.0.40	10101000 10001110 00000000 00101000	Резерв
	……		
	168.142.0.62	10101000 10001110 00000000 00111110	Резерв
	168.142.0.63	10101000 10001110 00000000 00111110	Широкомов. адр.
3	168.142.0.64 /27	10101000 10001110 01000000 01000000	Адреса підмережі
	255.255.255.224	11111111 11111111 11111111 11100000	Маска підмережі

	168.142.0.65	10101000 10001110 00000000 01000001	R3, інтерфейс 1
	168.142.0.66	10101000 10001110 00000000 01000010	H1
	168.142.0.67	10101000 10001110 00000000 01000011	H2
	168.142.0.68	10101000 10001110 00000000 01000100	H3
	168.142.0.69	10101000 10001110 00000000 01000101	H4
	168.142.0.70	10101000 10001110 00000000 01000110	H5
	168.142.0.71	10101000 10001110 00000000 01000111	H6
	168.142.0.72	10101000 10001110 00000000 01001000	Резерв
	……		
	168.142.0.94	10101000 10001110 00000000 01011110	Резерв
	168.142.0.95	10101000 10001110 00000000 01011111	Широкомов. адр.
4	168.142.0.96 /27	10101000 10001110 00000000 01100000	Адреса підмережі
	255.255.255.224	11111111 11111111 11111111 11100000	Маска підмережі
	168.142.0.97	10101000 10001110 00000000 01100001	R4, інтерфейс 0
	168.142.0.98	10101000 10001110 00000000 01100010	H1
	168.142.0.99	10101000 10001110 00000000 01100011	H2
	168.142.0.100	10101000 10001110 00000000 01100100	H3
	168.142.0.101	10101000 10001110 00000000 01100101	H4
	168.142.0.102	10101000 10001110 00000000 01100110	H5
	168.142.0.103	10101000 10001110 00000000 01100111	H6
	168.142.0.104	10101000 10001110 00000000 01101000	Резерв
	……		
	168.142.0.126	10101000 10001110 00000000 01111110	Резерв
	168.142.0.127	10101000 10001110 00000000 01111111	Широкомов. адр.
5	168.142.0.128 /27	10101000 10001110 00000000 10000000	Адреса підмережі
	255.255.255.224	11111111 11111111 11111111 11100000	Маска підмережі
	168.142.0.129	10101000 10001110 00000000 10000001	R5, інтерфейс 0
	168.142.0.130	10101000 10001110 00000000 10000010	H1
	168.142.0.131	10101000 10001110 00000000 10000011	H2
	168.142.0.132	10101000 10001110 00000000 10000100	H3
	168.142.0.133	10101000 10001110 00000000 10000101	H4
	168.142.0.134	10101000 10001110 00000000 10000110	H5
	168.142.0.135	10101000 10001110 00000000 10000111	H6
	168.142.0.136	10101000 10001110 00000000 10001000	Резерв
	……		
	168.142.158	10101000 10001110 00000000 10011110	Резерв

	168.142.159	10101000 10001110 00000000 10011111	Широкомов. адр.
6	168.142.0.160 /27	10101000 10001110 00000000 10100000	Адреса підмережі
	255.255.255.224	11111111 11111111 11111111 11100000	Маска підмережі
	168.142.0.161	10101000 10001110 00000000 10000001	R6, інтерфейс 0
	168.142.0.162	10101000 10001110 00000000 10000010	H1
	168.142.0.163	10101000 10001110 00000000 10000011	H2
	168.142.0.164	10101000 10001110 00000000 10100100	H3
	168.142.0.165	10101000 10001110 00000000 10000101	H4
	168.142.0.166	10101000 10001110 00000000 10100111	H5
	168.142.0.167	10101000 10001110 00000000 10100111	H6
	168.142.0.168	10101000 10001110 00000000 10101000	Резерв
	……		
	168.142.0.190	10101000 10001110 00000000 10111110	Резерв
	168.142.0.191	10101000 10001110 00000000 10111111	Широкомов. адр.

ДОДАТОК Б

План IP-адресації підмереж маршрутизаторів

Таблиця Б.1 – Опис IP-адрес

Підмережа S_R	Пул IP-адрес	Двійкова нотація	Призначення
1	176.119.77.0 /30	10110000 01110111 01001101 00000000	Адреса підмережі
	255.255.255.252	11111111 11111111 11111111 11111100	Маска підмережі
	176.119.77.1	10110000 01110111 01001101 00000001	R1, інтерфейс 2
	176.119.77.2	10110000 01110111 01001101 00000010	R2, інтерфейс 3
	176.119.77.3	10110000 01110111 01001101 00000011	Широкомов. адреса
2	176.119.77.4 /30	10110000 01110111 01001101 00000100	Адреса підмережі
	255.255.255.252	11111111 11111111 11111111 11111100	Маска підмережі
	176.119.77.5	10110000 01110111 01001101 00000101	R4, інтерфейс 2
	176.119.77.6	10110000 01110111 01001101 00000110	R2, інтерфейс 2
	176.119.77.7	10110000 01110111 01001101 00000111	Широкомов. адреса
3	176.119.77.8 /30	10110000 01110111 01001101 00001000	Адреса підмережі
	255.255.255.252	11111111 11111111 11111111 11111100	Маска підмережі
	176.119.77.9	10110000 01110111 01001101 00001001	R3, інтерфейс 6
	176.119.77.10	10110000 01110111 01001101 00001010	R2, інтерфейс 6
	176.119.77.11	10110000 01110111 01001101 00001011	Широкомов. адреса
4	176.119.77.12 /30	10110000 01110111 01001101 00001100	Адреса підмережі
	255.255.255.252	11111111 11111111 11111111 11111100	Маска підмережі
	176.119.77.13	10110000 01110111 01001101 00001101	R5, інтерфейс 2
	176.119.77.14	10110000 01110111 01001101 00001110	R3, інтерфейс 3
	176.119.77.15	10110000 01110111 01001101 00001111	Широкомов. адреса
5	176.119.77.16 /30	10110000 01110111 01001101 00010000	Адреса підмережі
	255.255.255.252	11111111 11111111 11111111 11111100	Маска підмережі
	176.119.77.17	10110000 01110111 01001101 00010001	R6, інтерфейс 2
	176.119.77.18	10110000 01110111 01001101 00010010	R3, інтерфейс 2
	176.119.77.19	10110000 01110111 01001101 00010011	Широкомов. адреса

ДОДАТОК В

Адресація бездротового сегмента мережі

Таблиця В.1 – Опис IP-адрес

Пул IP-адрес	Двійкова нотація	Призначення
168.142.0.192 /27	10101000 10001110 00000000 11000000	Адреса підмережі
255.255.255.224	11111111 11111111 11111111 11100000	Маска підмережі
168.142.0.193	10101000 10001110 00000000 11000001	R3, інтерфейс 0
168.142.0.194	10101000 10001110 00000000 11000010	Точка доступу
168.142.0.195	10101000 10001110 00000000 11000011	Бездротовий клієнт 1
168.142.0.196	10101000 10001110 00000000 11000100	Бездротовий клієнт 2
168.142.0.197	10101000 10001110 00000000 11000101	Бездротовий клієнт 3
168.142.0.198	10101000 10001110 00000000 11000110	Бездротовий клієнт 4
168.142.0.199	10101000 10001110 00000000 11000111	Бездротовий клієнт 5
168.142.0.200	10101000 10001110 00000000 11001000	Бездротовий клієнт 6
168.142.0.201	10101000 10001110 00000000 11001001	Бездротовий клієнт 7
168.142.0.202	10101000 10001110 00000000 11001010	Бездротовий клієнт 8
168.142.0.203	10101000 10001110 00000000 11001011	Бездротовий клієнт 9
168.142.0.204	10101000 10001110 00000000 11001100	Бездротовий клієнт 10
168.142.0.205	10101000 10001110 00000000 11001101	Бездротовий клієнт 11
168.142.0.206	10101000 10001110 00000000 11001110	Бездротовий клієнт 12
168.142.0.207	10101000 10001110 00000000 11001111	Бездротовий клієнт 13
168.142.0.208	10101000 10001110 00000000 11010000	Бездротовий клієнт 14

168.142.0.209	10101000 10001110 00000000 11010001	Бездротовий клієнт 15
168.142.0.210	10101000 10001110 00000000 11010010	Бездротовий клієнт 16
168.142.0.211	10101000 10001110 00000000 11010011	Бездротовий клієнт 17
168.142.0.212	10101000 10001110 00000000 11010100	Бездротовий клієнт 18
168.142.0.213	10101000 10001110 00000000 11010101	Резерв
168.142.0.214	10101000 10001110 00000000 11010110	Резерв
168.142.0.215	10101000 10001110 00000000 11010111	Резерв
168.142.0.216	10101000 10001110 00000000 11011000	Резерв
168.142.0.217	10101000 10001110 00000000 11011001	Резерв
168.142.0.218	10101000 10001110 00000000 11011010	Резерв
168.142.0.219	10101000 10001110 00000000 11011011	Резерв
168.142.0.220	10101000 10001110 00000000 11011100	Резерв
168.142.0.221	10101000 10001110 00000000 11011101	Резерв
168.142.0.222	10101000 10001110 00000000 10111110	Резерв
168.142.0.223	10101000 10001110 00000000 10111111	Широкомовна адреса