Plag

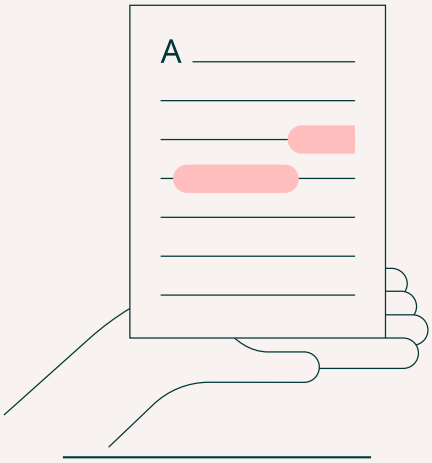
Звіт про оригінальність

● Оцінка схожості 19%

● Ризик плагіату НАЙВИЩИЙ

Ігор Кагало 2025-06-13 10:28

Посилання на звіт: 109h8 / Посилання користувача: qfC8



Ось вона –
Ваша звіт про оригінальність!

Ми раді повідомити, що перевірка вашого документа завершена, і результати вже готові! Наші алгоритми старанно працювали, щоб знайти збіги в наших базах даних.

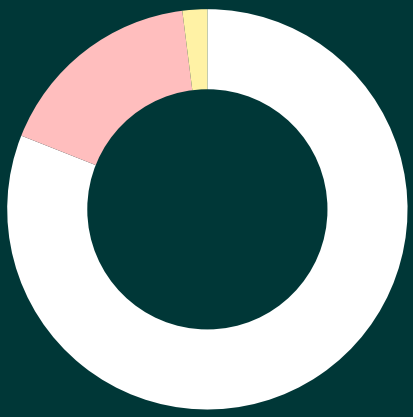
На наступних сторінках ви знайдете результати перевірки:

Бали
Збіги
Посилання

Ваш документ було перевірено за такими джерелами:

- ✓ База даних інтернет-джерел
- ✓ База даних наукових статей
- ○ Глибока перевірка (наш вдосконалений алгоритм)

Бали



Збіги тексту	17%
Перефразування	2%
Цитований текст	0%
Неправильне цитування	0%
Збігів не знайдено	81%

Ризик плагіату НАЙВИЩИЙ

Ризик плагіату вказує, як збіги тексту розподілені по документу. Вищий ризик виникає, коли збіги з'являються близько один до одного, наприклад, у тому самому абзаці або розділі.

Оцінка схожості %19

Оцінка схожості показує, скільки слів або символів у вашому документі збігаються з текстами інших документів, включаючи перефразовані тексти або неправильні цитати.

Збіги

1 ТЕОРЕТИЧНІ ОСНОВИ ЛОКАЛЬНИХ МЕРЕЖ І СЕРВЕРНИХ ТЕХНОЛОГІЙ

1.1 Основні поняття локальних мереж

Локальна мережа (local area network, LAN) – це група з декількох комп’ютерів, з’єднаних провідним чи безпровідним способом, використовують спільне 2 мережеве обладнання і програмне забезпечення і 2 знаходяться під єдиним адміністративним контролем.

2 Локальні мережі дозволяють забезпечити: колективну обробку даних; обмін 2 цими даним між усіма 2 користувачами; спільне використання програм; спільне використання обладнання 2 та периферійних пристроїв.

2 Класично 2 для об’єднання комп’ютерів у локальну мережу необхідно: забезпечити 2 кожен 2 комп’ютер, який підключається до мережі, мережевим 2 контролером (інколи його називають 2 «мережевий адаптер» або «мережева плата»), що 2 дозволить 2 комп’ютеру отримувати інформацію з локальної мережі і передавати її в мережу; з’єднати комп’ютери кабелями (якщо 2 це провідне з’єднання) для передавання 2 даних між комп’ютерами, а також іншими підключеними до мережі пристроями, зокрема 2 периферійними. 2 В деяких типах мереж - 2 однорангових - 2 кабелі з'єднують комп'ютери безпосередньо, в інших - на основі сервера або інших комунікаційних пристроїв - 2 з'єднання кабелів здійснюється через мережеві 2 пристрої.

2 Як згадувалася, 2 для забезпечення функціонування локальної мережі часто виділяють спеціальний комп'ютер - сервер, або декілька таких комп'ютерів. На дисках серверів розміщуються спільно використовувані програми, бази даних і т.д. Решта комп'ютерів локальної мережі часто називають робочими станціями. На тих робочих станціях, де вимагається опрацьовувати лише дані на сервері (наприклад, робота 2 з наповнення спільної бази даних), 2 часто для економії (або з огляду на безпеку) не встановлюють жорстких дисків. В мережах, які складаються більш ніж з 20-25 комп'ютерів, наявність сервера обов'язкова - інакше продуктивність мережі різко знижується. Сервер загалом необхідний під час спільної інтенсивної 2 роботи з будь-

якою базою даних.

2 Деколи серверам призначають визначену спеціалізацію (скажімо, зберігання даних чи програм, забезпечення віддаленого зв'язку, виведення 2 на друк та ін.). Сервери, як правило, не використовується 2 як робоче місце користувача. 2 Сервери, які забезпечують роботу з цінними даними, часто знаходяться в ізольованому приміщенні, доступ до якого мають уповноважені 2 люди (наприклад, 2 банківське сховище).

2 Для ефективної роботи користувачів у 2 локальній мережі часто 2 застосовують допоміжне програмне забезпечення, яке іноді надається 2 виробником разом із 2 мережевою операційною системою, а інколи його потрібно закуповувати окремо: електронна пошта; засоби віддаленого доступу які дозволяють підключатися до локальної мережі і працювати з нею так, ніби користувач є безпосередньо підключеним; 2 засоби групової роботи, які дозволяють спільно працювати над документами, забезпечують засоби для забезпечення документообігу 2 підприємства; програма резервування, Який 2 дозволяють створювати резервні копії даних, що зберігаються на комп'ютерах локальної мережі; засоби управління локальною мережею - дозволяють керувати ресурсами локальної мережі з одного робочого 2 місця.

2 Локальні мережі тому і називають локальними, що вони з'єднують комп'ютери, які знаходяться поруч. Але 10 багато підприємств (корпорації, банки та 10 ін.) 10 мають підрозділи, розташовані в різних кінцях міста або навіть в різних містах чи країнах. Для ефективної роботи їм, як правило, потрібно об'єднати свої підрозділи в єдину мережу. Такі мережі переважно 10 називають корпоративними.

7 Розглянемо випадок, коли 7 підрозділи підприємства розташовані не дуже далеко одне від одного (скажімо, у межах міста), тоді 7 можна прокласти власні лінії зв'язку між підрозділами (звісно, це коштує досить дорого). Але найчастіше доцільніше орендувати вже готові 7 лінії зв'язку у постачальників телекомунікаційних послуг. Тоді 7 достатньо прокласти лінію зв'язку 7 від кожного підрозділу підприємства до найближчого до цього підрозділу вузла мережі постачальника телекомунікаційних послуг - провайдера. Якщо об'єм даних, що передаються і приймається під розділом 7 підприємства, незначний, то вузлом мережі провайдера можна зв'язуватись навіть по комутованим лініям. Зазвичай, 7 у всіх випадках під 7 час створення корпоративної 7 мережі необхідно відповідне обладнання (сервери комутатори, маршрутизатори та ін.).

Власне корпоративна мережа (corporate network - CN) - це мережа, що об'єднує кілька структурних підрозділів організації у виглядіLAN за допомогою обладнання провайдера у єдину структуру.

Internet або глобальна мережа (Wide Area Network - WAN) - це всесвітня глобальна комп'ютерна мережа; така загальносвітова сукупність, грубо кажучи, складається з комп'ютерних мереж типу LAN і CN, з'єднує між собою мільйони комп'ютерів.

З погляду наповненості компонентами та їх характеру виділено 5 два основних типи мереж: одноранговi та мережі на основі сервера.

5 Одноранговi мережі всі комп'ютери рівноправні, тобто, немає ні ієрархії, ні виділеного (dedicated) сервера. Кожен комп'ютер може 21 працювати 5 І як клієнт, і як сервер, отже, 5 немає 5 комп'ютера, відповідального за адміністрування всієї мережі. Усі користувачі самостійно вирішують, які дані зробити загальнодоступними у мережі. Нині одноранговi мережі без перспективні. 5 Якщо до мережі підключено більше ніж 5 10 користувачів, тоді така 5 одноранговa мережа, де комп'ютери різні моменти часу виступають то в ролі клієнта, то сервера, є непродуктивною. Саме тому сучасні мережі 21 використовують виділені сервери.

21 Виділеним сервером називають такий комп'ютер, 5 який функціонує тільки як сервер. Виділені 5 сервери вже 5 стали промисловим стандартом і спеціально оптимізовані для швидкого оброблення 21 Запитів від мережевих клієнтів, 5 керування захистом файлів і каталогів та 5 багатьох інших функцій.

5 Звісно, є 5 і комбіновані типи мереж, що об’єднують у себе кращі аспекти і одноранговых мереж, і мережу 5 на основі сервера.

5 1.2 Види та функціональність серверів в локальних мережах

Щоб чітко визначити роль серверів у локальній мережі перш за все потрібно відштовхуватись від класифікації комп’ютерних мереж. Така класифікація допомагає зрозуміти, які сервіси необхідні для забезпечення ефективної роботи мережі, зокрема управління ресурсами, зберігання даних та комунікаційні служби. Орієнтація на види послуг дає можливість оптимізувати використання серверних ресурсів і правильно розподілити навантаження між серверами. Це також дозволяє забезпечити відповідність структури мережі потребам конкретної організації або установи, яка буде використовувати модельовану систему. Використання такої класифікації сприяє вибору найефективніших мережевих технологій і програмного забезпечення для кожного типу сервісу.

Крім того, аналіз послуг, що надаються мережею, дозволяє спростити процес адміністрування, підвищити безпеку та забезпечити стабільність роботи. Саме тому такий підхід є найбільш логічним і виправданим для побудови моделі локальної мережі із застосуванням виділеного сервера у середовищі Cisco Packet Tracer.

Він дає змогу чітко визначити вимоги до кожного сервера та налаштувати його відповідно до функціональних завдань. Завдяки цьому можна детально змоделювати взаємодію між клієнтами та серверами, що дозволить краще зрозуміти принципи роботи локальних мереж. Такий підхід також сприяє виявленню можливих вузьких місць у мережі та розробці рішень для їх усунення ще на етапі проектування. У підсумку, класифікація за видами надаваних послуг забезпечує структурований і системний підхід до побудови ефективної та надійної мережевої інфраструктури.

Якщо ми будемо ставити в основу нашого дослідження комп'ютерні мережі офісних приміщень (мережі відділів) та комп'ютерні мережі невеликих будівель (школа, коледж, державне підприємвство) то ми зауважимо, що інформаційні по слуги дані категорії підприємств можуть надавати тільки в межах зони їхньої відповідальності.

У зв'язку з цим можна сформувати орієнтовну таблицю залежностей видів діяльності підприємтств від необхідних телекомунікаційних серверів щодо надаваємих ними інформаційних послуг.

Таблиця 1.1 – Порівняння категорій

Категорія

Основні сервери

Додаткові сервери

Офісна мережа

DHCP-сервер, DNS-сервер, File-сервер, Mail-сервер

Web-сервер, Print-сервер

Навчальний заклад

DHCP-сервер, DNS-сервер, Web-сервер, FTP-сервер

Proxy-сервер, Термінальний сервер, Мультимедійний сервер

Підприємство

DHCP-сервер, DNS-сервер, Mail-сервер, VPN-сервер, ActiveDirectory, Firewall

Web-сервер, FTP-сервер, Backup-сервер

Якщо розглянути типи серверів, що вказані у таблиці з точки зору функціональності, то їх тоді можна об’єднати у наступні групи: сервери управління ресурсами, сервери

зберігання та передачі даних, сервери комунікацій, сервери безпеки та аутентифікації, інші спеціалізовані сервери.

Сервери управління ресурсами є ключовим компонентом локальних мереж, що відповідають за оптимізацію використання мережевих ресурсів. Основним завданням таких серверів є забезпечення автоматичного розподілу ресурсів, таких як IP-адреси, іменні записи 16 та доступ до різних служб. DHCP-сервер дозволяє автоматично призначати IP-адреси клієнтам у мережі, зменшуючи ручну працю адміністраторів і запобігаючи конфліктам адрес. DNS-сервер забезпечує перетворення доменних імен на IP-адреси, 16 дозволяючи користувачам легко отримувати доступ до ресурсів за зрозумілими назвами. Такі сервери значно підвищують ефективність адміністрування мережі та покращують її масштабованість.

Вони часто використовуються в організаціях для централізованого управління мережею та швидкого реагування на зміни у її конфігурації. Сервери управління ресурсами інтегруються з іншими елементами інфраструктури, такими як маршрутизатори й комутатори. Їхня робота базується на стандартизованих протоколах, які забезпечують сумісність між пристроями різних виробників. Завдяки таким серверам адміністратори отримують можливість гнучкого управління та моніторингу роботи мережі. Це дозволяє забезпечити стабільність, надійність і високу продуктивність локальних мереж.

Сервери зберігання та передачі даних 22 виконують важливу роль у забезпеченні доступу до інформації в локальних мережах. Вони дозволяють централізовано зберігати файли, документи та інші ресурси, забезпечуючи їх доступність для користувачів. Файлові сервери є основним інструментом для організації спільного доступу до даних, де можна налаштувати рівні доступу для різних користувачів. FTP-сервери використовуються для передачі файлів між пристроями, підтримуючи ефективний обмін великими обсягами інформації. Бекап-сервери забезпечують створення резервних копій даних, що критично важливо для захисту від втрати інформації в разі збоїв.

Такі сервери можуть бути інтегровані з хмарними рішеннями для забезпечення додаткового рівня надійності та зберігання. Робота серверів зберігання й передачі даних базується на різних протоколах, таких як SMB, NFS або FTP, що забезпечують сумісність із різними операційними системами. Вони також дозволяють реалізовувати різні сценарії доступу, від локального з'єднання до роботи через віддалений доступ. Сучасні сервери такого типу оснащуються інструментами шифрування для забезпечення безпеки переданих і збережених даних. Завдяки своїй функціональності сервери зберігання та передачі даних забезпечують безперервну роботу організацій, підтримуючи їхню інформаційну інфраструктуру.

Сервери комунікацій забезпечують обмін інформацією між користувачами та пристроями в локальній або глобальній мережі. Вони підтримують роботу електронної пошти, месенджерів, голосового та відеозв’язку, що є ключовим елементом сучасного бізнесу та корпоративних систем. Такі сервери можуть включати поштові сервери, сервери IP-телефонії (VoIP) та сервери відеоконференцій, які забезпечують швидку та ефективну взаємодію між співробітниками. Вони дозволяють централізовано зберігати та керувати комунікаційними даними, забезпечуючи їхню конфіденційність та безпеку. У CiscoPacketTracer можна змоделювати роботу деяких серверів комунікацій, зокрема поштових серверів та серверів VoIP, щоб перевірити їхню взаємодію з клієнтами. Адміністратори можуть налаштовувати протоколи комунікацій, такі як SMTP, POP3, IMAP для пошти або SIP для IP-телефонії, що дозволяє адаптувати мережу до потреб організації.

Сервери комунікацій можуть інтегруватися з іншими сервісами, такими як каталоги користувачів або системи керування доступом, що підвищує їхню ефективність. Використання таких серверів значно зменшує витрати на традиційні телефонні системи, оскільки IP-телефонія дозволяє здійснювати дзвінки через Інтернет. Вони також підтримують засоби шифрування та аутентифікації, що захищає дані від несанкціонованого доступу. Завдяки своїй важливості сервери комунікацій є невід’ємною частиною сучасних корпоративних та навчальних мереж, забезпечуючи безперервний і надійний зв’язок між користувачами.

Сервери безпеки та аутентифікації відіграють ключову роль у забезпеченні контролю доступу до ресурсів мережі та захисту конфіденційної інформації. Вони відповідають за ідентифікацію користувачів, перевірку їхніх облікових даних і надання відповідних прав доступу. До таких серверів належать RADIUS, LDAP, Active Directory, а також сервери контролю мережевого доступу (NAC). Вони дозволяють централізовано керувати обліковими записами користувачів, політиками безпеки та рівнями дозволів у мережі. У корпоративному середовищі сервери аутентифікації використовуються для інтеграції з іншими службами, такими як електронна пошта, файлові сховища або VPN-з'єднання.

Також вони можуть підтримувати багатофакторну аутентифікацію, що підвищує рівень захищеності від несанкціонованого доступу. Сервери безпеки можуть виконувати моніторинг активності користувачів і фіксувати спроби порушень політик безпеки. У Cisco Packet Tracer можна моделювати базові функції таких серверів, зокрема перевірку доступу та управління правами користувачів. Завдяки їх використанню мережеві адміністратори можуть 17 швидко реагувати на потенційні загрози та запобігати витоку даних. Таким чином, сервери безпеки та аутентифікації є важливим компонентом будь-якої захищеної інформаційної системи, що забезпечує її стабільну та безпечну роботу.

1.3 Огляд протоколів, що забезпечують роботу серверів

Протоколи відіграють ключову роль у функціонуванні серверів, забезпечуючи обмін даними між пристроями в мережі. Кожен протокол має свою специфіку та призначений для виконання певних завдань у рамках мережевого взаємодії.

DHCP (DynamicHostConfigurationProtocol) використовується для автоматичного призначення IP-адрес клієнтам у мережі, що спрощує адміністрування та зменшує ймовірність конфліктів адрес. Цей протокол працює за моделлю клієнт-сервер, де сервер DHCP видає IP-адреси та додаткові параметри, такі як шлюз і DNS-сервер. Завдяки DHCP користувачам не потрібно вручну налаштовувати параметри мережевого підключення, що особливо корисно у великих мережах. DHCP значно зменшує навантаження на адміністратора, автоматично розподіляючи IP-адреси та налаштування мережі.

DNS (Domain Name System) відповідає за перетворення доменних імен у відповідні IP-адреси, дозволяючи користувачам отримувати доступ до ресурсів за зрозумілими назвами, а не числовими значеннями. Сервери DNS працюють у ієрархічній структурі, що забезпечує швидкість та надійність пошуку адрес у глобальній мережі. Запити DNS можуть кешуватися, що дозволяє прискорювати доступ до часто відвідуваних ресурсів та знижувати навантаження на кореневі сервери. DNS, у свою чергу, робить Інтернет більш зручним для користувачів, усуваючи необхідність запам'ятовувати складні числові адреси серверів.

Протокол HTTP (Hypertext Transfer Protocol) використовується для передачі веб-сторінок між сервером і клієнтом, що є основою роботи Інтернету. Він працює за принципом запит-відповідь, де браузер надсилає запит до сервера, а той повертає HTML-документ разом із ресурсами. Для підвищення безпеки використовується HTTPS, який шифрує передані дані за допомогою SSL/TLS. HTTP не зберігає стан з'єднання, тому для підтримки сесій використовуються файли cookie або спеціальні механізми авторизації. HTTP є основою веб-технологій, що дозволяє переглядати веб-сторінки, взаємодіяти з веб-додатками та передавати інформацію через Інтернет. Завдяки захищеному HTTPS користувачі можуть безпечно здійснювати онлайн-транзакції та передавати конфіденційні дані.

FTP (File Transfer Protocol) забезпечує передачу файлів між сервером і клієнтом, дозволяючи як завантажувати, так і відвантажувати дані. Він підтримує два режими роботи: активний і пасивний, що визначає спосіб встановлення з'єднання між клієнтом і сервером. Для безпечної передачі даних застосовуються його захищені версії – FTPS та SFTP, які використовують шифрування для захисту інформації. FTP широко використовується для обміну великими файлами, розповсюдження програмного забезпечення та організації файлових сховищ. Важливість цих протоколів полягає у

забезпеченні стабільної та ефективної роботи мережевої інфраструктури.

Вони дозволяють автоматизувати процеси конфігурації, забезпечують зручний доступ до ресурсів та гарантують передачу даних між клієнтами та серверами. FTP залишається незамінним у сфері адміністрування серверів, резервного копіювання та обміну файлами між користувачами. Кожен із цих протоколів доповнює інші, забезпечуючи надійну інфраструктуру для роботи серверів у локальних і глобальних мережах. Разом вони створюють комплексну систему взаємодії, що дозволяє мережам функціонувати ефективно та безперебійно.

Завдяки цим протоколам користувачі отримують швидкий доступ до інформації, а адміністратори можуть легко управляти ресурсами мережі. Постійний розвиток мережевих технологій передбачає вдосконалення та адаптацію цих протоколів до сучасних потреб, зокрема зростання вимог до безпеки та швидкості обміну даними. У перспективі можна очікувати подальшого вдосконалення механізмів шифрування та оптимізації роботи мережевих протоколів.

1.4 Особливості використання Cisco Packet Tracer для моделювання мереж

Cisco Packet Tracer – це навчальне середовище для моделювання мережевої інфраструктури. Хоча він має широкі можливості, деякі функції обмежені через його навчальний характер.

У середовищі Cisco Packet Tracer можна налаштовувати різні типи серверів, які забезпечують критично важливі мережеві функції. Наприклад налаштувати DHCP-сервер, що дозволить автоматично розподіляти IP-адреси клієнтським пристроям у мережі, що спрощує адміністрування та зменшує кількість помилок у конфігурації. DNS-сервер, який виконуватиме перетворення доменних імен у відповідні IP-адреси, що дозволяє клієнтам швидко знаходити необхідні ресурси в мережі. FTP-сервер буде використовуватись для зберігання та передачі файлів між клієнтами і мережею, надаючи зручний спосіб доступу до спільних даних.

Web-сервер (HTTP/HTTPS) дозволяє хостити веб-сторінки та сервіси, що можуть бути доступні через браузер, що є корисним для навчальних та демонстраційних цілей. Mail-сервер (SMTP, POP3) відповідає за надсилання та отримання електронної пошти в локальній мережі або через Інтернет. Telnet і SSH-сервери дозволяють адміністратору підключатися до мережевих пристроїв для дистанційного керування та конфігурації. NTP-сервер синхронізує час на всіх пристроях у мережі, що є важливим для журналювання подій та безпеки. 12 Cisco Packet Tracer дозволяє налаштовувати всі ці сервери, що дозволяє моделювати реальні мережеві інфраструктури. Вони можуть працювати як окремі служби на єдиному сервері або бути розділеними між декількома

пристроями для імітації реальної корпоративної мережі.

Адміністратори можуть перевіряти роботу сервісів, налаштовувати доступ і контролювати підключення клієнтів. Кожен із цих серверів 25 відіграє важливу роль у підтримці роботи мережі та покращенні її продуктивності. Важливо правильно конфігурувати та тестувати ці сервіси для запобігання збоїв і помилок у мережевій інфраструктурі. 12 Cisco Packet Tracer дозволяє візуально аналізувати взаємодію між клієнтами та серверами, що сприяє кращому розумінню принципів роботи мереж. Використання цих серверів у моделюванні допомагає студентам та інженерам-початківцям освоїти налаштування мережевих служб. Це робить 12 Cisco Packet Tracer потужним інструментом для навчання та досліджень у сфері мережевих технологій.

У версіях 12 Cisco Packet Tracer до 7.0 можливості налаштування серверів були значно обмежені, оскільки ця програма ще не мала розширеного функціоналу. Основні сервери, які можна було налаштувати, включали DHCP, DNS, Web (HTTP) та FTP, що дозволяло моделювати базові мережеві сценарії. Проте складніші сервіси, такі як Mail-сервер (SMTP, POP3) та NTP, у цих версіях були або повністю відсутні, або мали дуже обмежену функціональність. Через це неможливо було реалізувати деякі сценарії корпоративних мереж із розширеними сервісами.

Крім того, інтерфейс та інструменти для налаштування мережевих служб були менш зручними у порівнянні з новішими версіями. Застарілі версії Packet Tracer також мали нижчий рівень емуляції мережевих пристроїв і протоколів. Через це їх використання на сьогодні є недоцільним для навчання сучасним мережевим технологіям. Оновлення до новіших версій дозволяє отримати більше можливостей для налаштування серверів і моделювання складніших мережевих сценаріїв.

У версіях 12 Cisco Packet Tracer 7.0 – 7.3 було значно розширено можливості роботи із серверами, що зробило програму більш гнучкою для моделювання мереж. Одним із важливих оновлень стала підтримка SMTP і POP3, що дозволило налаштовувати Mail-сервер для тестування надсилання та отримання електронної пошти. Також було покращено роботу з Telnet і SSH, що дало змогу ефективніше налаштовувати віддалене керування мережевими пристроями. У цих версіях користувачі отримали можливість одночасно налаштовувати декілька серверів для різних служб, що значно покращило моделювання складних мереж. Завдяки цьому стало можливим тестувати взаємодію між різними сервісами, наприклад, Web-сервером і DNS-сервером.

Покращення також торкнулися стабільності роботи та інтерфейсу, що зробило процес налаштування серверів зручнішим. Версії 7.0–7.3 стали перехідним етапом до більш потужних інструментів у наступних оновленнях. Вони залишаються актуальними для навчання, хоча новіші версії Packet Tracer пропонують ще більше можливостей.

Версії Cisco Packet Tracer 8.0+ мають найрозширеніший набір функцій для моделювання мережевих інфраструктур. Вони підтримують усі доступні типи серверів, зокрема DHCP, DNS, Web, FTP, Mail, Telnet/SSH та NTP, що дозволяє створювати складніші мережеві сценарії. Оновлена версія також має покращену візуалізацію, що спрощує аналіз та налаштування складних мережевих топологій. Значно покращено роботу з ACL (Access Control Lists), що дає можливість гнучко керувати доступом до ресурсів і тестувати базові функції мережевої безпеки. Додана краща підтримка емуляції фаєрволів, що дозволяє моделювати прості механізми захисту мережі. Завдяки оптимізованій симуляції мережевого трафіку стало легше аналізувати роботу серверів у реальних умовах. Розширена функціональність робить Packet Tracer 8.0+ ідеальним інструментом для навчання та тестування різних мережевих технологій. Ці версії залишаються найкращими для моделювання складних мереж у навчальних та дослідницьких цілях.

У середовищі Cisco Packet Tracer є певні обмеження щодо налаштування деяких типів серверів, які широко використовуються у реальних мережах. Active Directory (AD) неможливо реалізувати в Packet Tracer, оскільки ця технологія вимагає роботи з Windows Server і специфічними сервісами, такими як контролер домену, служби каталогів та керування користувачами. Це обмеження робить неможливим повноцінне моделювання корпоративних мереж із централізованою аутентифікацією. VPN-сервер підтримується частково, але не повністю емулюється, оскільки Packet Tracer не має повного функціоналу для створення реальних захищених тунелів між мережами. Доступні лише базові налаштування IPsec і GRE-тунелів, які не охоплюють усіх аспектів справжньої VPN-інфраструктури. Proxy-сервер також не можна налаштувати в повному обсязі, але його функції можна частково моделювати за допомогою Access Control Lists (ACL) для контролю доступу та обмеження трафіку.

Це дозволяє створити імітацію фільтрації мережевого трафіку, але без повноцінного кешування або аналізу контенту. Відсутність цих серверів у Cisco Packet Tracer пояснюється тим, що він розроблений переважно для навчання мережевим технологіям, а не для емуляції складних серверних середовищ. Для моделювання таких серверів необхідно використовувати віртуальні машини та реальні операційні системи, такі як Windows Server або спеціалізовані Linux-дистрибутиви. Це обмеження може впливати на можливості детального налаштування мереж у навчальних цілях. Однак Packet Tracer залишається ефективним інструментом для вивчення базових мережевих концепцій і налаштування основних серверних служб.

У випадку необхідності моделювання повноцінних серверів можна використовувати GNS3, EVE-NG або VMware для створення віртуальних мереж із реальними серверними ОС. Використання цих платформ дозволяє доповнити навчальний процес та отримати повне розуміння принципів роботи серверних технологій. Незважаючи на обмеження, Packet Tracer залишається популярним серед студентів і мережевих інженерів для

початкового рівня навчання. Розуміння обмежень цієї програми допомагає правильно підбирати інструменти для моделювання більш складних мереж.

Таким чином 29 можна зробити наступний висновок якщо потрібно налаштувати якомога більше серверів, найкраще використовувати Cisco Packet Tracer версії 8.0+, оскільки ця версія підтримує всі доступні сервери у середовищі. Вона дозволяє моделювати DHCP, DNS, Web, FTP, Mail, Telnet/SSH та NTP-сервери, що охоплює основні потреби навчальних і тестових мереж. Проте, якщо необхідно реалізувати складніші сценарії, такі як Active Directory, Proxy або VPN, Packet Tracer має обмежені можливості. Для моделювання реальних пристроїв Cisco можна використовувати GNS3, що дозволяє запускати справжні образи операційних систем мережевого обладнання.

Якщо потрібна емуляція Windows Server для налаштування Active Directory або інших корпоративних сервісів, найкращим вибором будуть VMware або VirtualBox. Ці платформи дозволяють створювати віртуальні машини з повноцінними серверними ОС, що відкриває доступ до всіх необхідних функцій. Таким чином, Cisco Packet Tracer підходить для навчання основам роботи серверів і мережевих технологій, але для більш складних завдань необхідно використовувати додаткові інструменти.

Поєднання Packet Tracer, GNS3 та віртуальних машин дає змогу створювати реалістичні мережеві топології та тестувати складні мережеві рішення. Використання різних середовищ дозволяє отримати більш глибоке розуміння роботи серверів у корпоративних мережах. Завдяки цьому можна ефективно навчатися та відпрацьовувати навички адміністрування мереж та серверних систем.

2 АНАЛІЗ ЗАВДАННЯ І ПРОЕКТУВАННЯ МЕРЕЖІ

2.1 Планування структури локальної мережі малого офісу

При плануванні малої офісної мережі для восьми приміщень потрібно врахувати особливості її структури, обладнання та безпеки. Перш за все, необхідно визначити кількість пристроїв у кожному підрозділі та передбачити резерв для майбутнього розширення. У кожному приміщенні буде два комп’ютери, а всі підрозділи мають бути підключені до центрального L3-комутатора. Основний комутатор повинен мати достатню кількість портів і підтримувати VLAN для розмежування трафіку між відділами. Враховуючи необхідність виходу в Інтернет, слід встановити маршрутизатор, який забезпечить NAT, DHCP, ACL і VPN. Для підключення комутаторів та серверів потрібно використовувати надійну структуровану кабельну систему зі схемою зірки для мінімізації простоїв у разі збою. У серверній кімнаті розміщується центральний сервер, на якому буде розгорнуто DNS, FTP, Web, Mail та інші необхідні сервіси. DHCP доцільно налаштувати на маршрутизаторі, щоб динамічно розподіляти IP-адреси між клієнтами мережі. Важливо впровадити систему моніторингу мережевого обладнання, яка

дозволить оперативно виявляти збої та перевантаження. Для підвищення рівня безпеки варто реалізувати політики доступу за допомогою ACL на маршрутизаторі. Використання VPN дозволить співробітникам безпечно підключатися до мережі ззовні. Захист внутрішнього трафіку від зовнішніх атак слід реалізувати через міжмережевий екран та контроль доступу. Окрему увагу потрібно приділити Wi-Fi-зоні, якщо вона необхідна, забезпечивши якісне покриття та обмеживши доступ гостей. Сервер зберігання даних повинен мати систему резервного копіювання, щоб уникнути втрати важливої інформації. Варто передбачити якісне електроживлення для маршрутизатора, комутатора та сервера, бажано через ДБЖ. Використання керованих комутаторів дозволить адміністратору ефективно керувати трафіком і налаштовувати VLAN. Додатково можна реалізувати централізовану систему логування подій для відстеження змін у мережі. Всі ці аспекти допоможуть створити стабільну, безпечну та ефективну малу офісну мережу, враховуючи специфіку її роботи та подальший розвиток.

Рисунок 2.1 – План розміщення обладнання малого офісу

В нашому випадку у малій офісній мережі розміщені такі підрозділи:

Приймальня (Reception) – містить 1–2 комп’ютери для секретаря та адміністратора, які обробляють документи, приймають відвідувачів і виконують основні організаційні завдання.

Кабінет керівника (Manager's Office) – окреме приміщення для керівника компанії, де встановлений комп’ютер із доступом до загальної мережі, а також засоби для відеоконференцій.

Відділ бухгалтерії (Accounting Department) – два комп’ютери для обліку фінансів, роботи з банківськими системами та ведення документації підприємства.

Відділ продажів (Sales Department) – два комп’ютери для менеджерів із продажу, які працюють із клієнтами, ведуть базу даних замовлень і спілкуються електронною поштою.

Відділ технічної підтримки (IT Support) – два комп’ютери для спеціалістів з обслуговування обладнання, мережі та системного адміністрування.

Маркетинговий відділ (Marketing Department) – два комп’ютери для фахівців із просування продукції, ведення соціальних мереж, аналітики та розробки рекламних матеріалів.

Загальна кімната для співробітників (Break Room / Meeting Room) – може мати один комп’ютер або інтерактивну панель для проведення презентацій і нарад.

Серверна кімната (Server Room) – приміщення, де розміщено сервер (наприклад, файловий або поштовий), мережеве обладнання, комутатор та маршрутизатор для забезпечення стабільної роботи мережі.

2.2 Планування структури локальної мережі комп'ютерного комплексу фахового коледжу

Комп'ютерна мережа комплексу комп'ютерних лабораторій навчального закладу є важливим елементом освітнього процесу. Вона повинна забезпечувати надійний доступ студентів і викладачів до необхідних інформаційних ресурсів, підтримувати високошвидкісне підключення до серверів та Інтернету, а також мати можливість гнучкого адміністрування. Оскільки в навчальному закладі регулярно проходять практичні заняття, тестування та лабораторні роботи, мережа повинна мати високу продуктивність і захищеність від зовнішніх та внутрішніх загроз.

У розглянутій моделі мережі передбачено чотири комп'ютерні лабораторії, у кожній з яких розташовано по 12 персональних комп’ютерів. Для їх підключення використовується керований комутатор рівня 2 CiscoCatalyst 2960, який забезпечує з'єднання всіх пристроїв у межах локального сегменту. Ці три комутатори підключаються до центрального комутатора рівня 3, який виконує маршрутизацію трафіку між лабораторіями, сервером та маршрутизатором, що забезпечує вихід у глобальну мережу Інтернет.

Рисунок 2.2 – План розміщення обладнання лабораторного комплексу лабораторій фахового коледжу

Функції мережі та її структура

Мережа комплексу комп'ютерних лабораторій повинна виконувати кілька важливих функцій:

Розподіл доступу до ресурсів. Усі користувачі мережі (студенти, викладачі, адміністратори) повинні мати доступ до навчальних матеріалів, серверних ресурсів та Інтернету відповідно до своїх ролей.

Захист даних. Використання VLAN для розподілу трафіку між лабораторіями дозволяє підвищити безпеку та уникнути конфліктів між пристроями.

Гнучке адміністрування. Централізоване управління мережею дозволяє швидко змінювати конфігурацію, створювати та видаляти облікові записи, налаштовувати доступ до серверів та блокувати небажаний трафік.

Підтримка сервісів. Для нормальної роботи необхідні такі сервіси, як DHCP

(автоматична видача IP-адрес), DNS (перетворення доменних імен на IP-адреси), FTP (обмін файлами між клієнтами) та Web-сервер (доступ до навчальних матеріалів через браузер).

Центральним елементом мережі є L3-комутатор, який розподіляє трафік між VLAN-сегментами, об'єднує всі лабораторії та підключає сервер, що виконує важливі функції. До нього також підключений маршрутизатор, що забезпечує доступ до Інтернету.

Серверна інфраструктура

Сервер у даній мережі відіграє важливу роль у підтримці всіх необхідних сервісів. До його основних функцій належать:

DHCP-сервер. Автоматично роздає IP-адреси всім пристроям у мережі, що значно спрощує адміністрування та виключає можливі конфлікти між IP-адресами.

DNS-сервер. Відповідає за розпізнавання доменних імен, що дозволяє використовувати зрозумілі URL-адреси замість IP.

FTP-сервер. Дозволяє завантажувати та скачувати навчальні матеріали, що є особливо корисним при проведенні лабораторних робіт.

Web-сервер. Використовується для створення локального навчального порталу, на якому можуть розміщуватися курсові матеріали, завдання та інша важлива інформація.

Сервер підключений до L3-комутатора через порт 100 Мбіт/с, що забезпечує стабільний зв’язок із мережею та 28 дозволяє оперативно обробляти запити користувачів.

28 VLAN у навчальній мережі

Щоб забезпечити ефективну роботу мережі та підвищити її безпеку, у навчальному закладі використовується розподіл на VLAN. Це дозволяє сегментувати трафік, щоб зменшити навантаження на мережу та обмежити доступ між різними групами користувачів. У цьому випадку можна створити такі VLAN:

VLAN 10 – для першої лабораторії.

VLAN 20 – для другої лабораторії.

VLAN 30 – для третьої лабораторії.

VLAN 40 – для четвертої лабораторії

VLAN 50– для адміністративного персоналу.

VLAN 60 – для сервера та мережевого обладнання.

Така сегментація дозволяє обмежити доступ студентів до адміністративних ресурсів, зменшити вплив потенційних атак та забезпечити більшу гнучкість управління трафіком.

Організація доступу до Інтернету

Вихід до глобальної мережі забезпечується маршрутизатором, який підключений до L3-комутатора. Він виконує кілька важливих функцій:

NAT (NetworkAddressTranslation) – трансляція локальних IP-адрес у зовнішні, що дозволяє забезпечити доступ до Інтернету всім пристроям.

Фільтрація трафіку – налаштування правил доступу для блокування небажаних сайтів та контролю використання мережевих ресурсів.

VPN (VirtualPrivateNetwork) – можливість створення безпечного доступу до ресурсів навчального закладу ззовні.

Використання сучасних технологій дозволяє забезпечити стабільне та безпечне з'єднання, що є критично важливим для навчального процесу.

Адміністрування та моніторинг

Оскільки комп'ютерна мережа навчального закладу є складною системою, необхідно ефективно її адмініструвати. Для цього використовується система моніторингу, яка 24 дозволяє контролювати стан мережевого обладнання, виявляти збої та аналізувати продуктивність. Адміністратор може використовувати інструменти для виявлення аномалій у трафіку та 24 вчасно реагувати на можливі загрози.

Система логування дозволяє зберігати інформацію про всі дії користувачів, що важливо для безпеки. У разі несанкціонованого доступу можна швидко визначити джерело загрози та вжити заходів щодо її усунення.

Висновки

Комп'ютерна мережа комплексу лабораторій навчального закладу є важливим інструментом у навчальному процесі. Використання сучасних технологій та методів адміністрування дозволяє забезпечити її стабільність, безпеку та гнучкість у керуванні ресурсами. Структурована побудова мережі з використанням VLAN, серверної інфраструктури та систем безпеки сприяє ефективному розподілу навантаження та захисту інформації. Запропонована модель забезпечує зручність у користуванні та надійність у роботі, що є ключовими вимогами для сучасного освітнього закладу.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ МЕРЕЖІ У СЕРЕДОВИЩІ CISCO PACKET TRACER

3.1 Вибір обладнання для проєктування мережі

Традиційно серія комутаторів компанії Cisco 2960-х отримала збільшення апаратної потужності в два рази і при цьому підвищила своє енергозбереження. (рисунок 3.1).

Рисунок 3.1 – Комутатор Cisco Catalyst серії 2960-X

Таблиця 3.1 – 15 Технічні характеристики комутатора Cisco Catalyst 2960

15 Характеристика

15 Опис

Тип пристрою

Керований комутатор рівня 2

Форм-фактор

Стаціонарний (rack-mountable) – 1U

Ширина

44.5 cm

Глибина

23.7 cm

Висота

4.4 cm

15 Вага

15 3.6 kg

15 Кількість портів

24 x 10/100 Ethernet + 2 x Dual-purpose uplink (SFP/1000BASE-T)

Мережеві протоколи

9 Ethernet, Fast Ethernet, VLAN, RSTP, MSTP, SNMP, CDP, IGMP

Адміністрування

CLI, Telnet, SNMP v1/v2/v3, RMON, веб-інтерфейс

Функції безпеки

Port Security, DHCP Snooping, Dynamic ARP Inspection, ACL, 802.1X

Підтримувані стандарти

IEEE 802.3, 802.3u, 802.3x, 802.1D, 802.1p, 802.1Q, 802.1x

Індикатори

Живлення, Статус, Активність, Швидкість, PoE

Живлення

Вбудований блок живлення, опційно підтримка PoE

CISCO 2911 9 – маршрутизатор для потреб невеликих підприємств, офісів і філіалів (до 36 робочих місць).

9 Рисунок 9 3.2 9 – Маршрутизатор CISCO 2911

9 Таблиця 3.2 9 – Технічні 6 характеристики маршрутизатора Cisco 2911 6 (рисунок 3.2)

6 Характеристики

6 Опис

6 Тип пристрою

6 Маршрутизатор

6 Форм-фактор

6 Зовнішній - modular - 1U

6 Ширина

6 43.69 cm

Глибина

39.88 cm

Висота

4.45 cm

Вага

7.2 kg

Пам’ять

RAM

512 MB (встановлено) / 2.5 GB 9 (максимально) - DDR2 SDRAM

9 Флеш-пам’ять

9 256 MB (встановлено) / 8 GB 6 (максимально)

6 Параметри мережі

6 Технологія підключення

6 Wired

6 Канальний протокол

6 Ethernet, Fast Ethernet, Gigabit 6 Ethernet

6 Мережевий / 6 Транспортний протокол

6 IPSec

6 Протокол віддаленого адміністрування

6 SNMP 3

6 Індикатори стану

6 Link activity, живлення

6 Характеристики

9 Modular design, firewall protection, 128-bit/256-bit 6 кодування, апаратне кодування, підтримка VPN, підтримка MPLS, 9 фільтрація URL, інтегрований захист, підтримка голосового трафіку

Підтримувані стандарти

IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.1Q, IEEE 802.1p

Сокети розширення / Інтерфейси зв’язку

Сокети розширення

3 (3) x EHWIC ¦ 1 (1) x ISM ¦ 2 (2) x DSP (PVDM3) ¦ 2 memory ¦ 6 1 CompactFlash Card

6 Інтерфейси

6 3 6 x network - Ethernet 10/100/1000 (2 routed, 1 switched) - RJ-45 ¦ 2 x USB 2.0 ¦ 6 1 x management - console - 9 RJ-45 ¦ 9 1 x 9 auxiliary - RJ-45

8 Мережевий комутатор (англ. network switch) або світч (від англ. switch – «перемикач») – пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного сегмента. На відміну від концентратора, що поширює трафік від одного під'єднаного пристрою до всіх інших, комутатор передає дані лише безпосередньо отримувачу (рисунок 3.3).

Рисунок 3.3 – L3-комутатор 3560-24PS

Таблиця 3.3 – Технічні характеристики комутатора Cisco Catalyst 3560-24PS

11 Характеристики

11 Опис

11 Тип пристрою

11 Комутатор

Форм-фактор

11 Зовнішній – standalone 11 – 1U

11 Ширина

11 44.5 cm

Глибина

33.0 cm

Висота

4.4 cm

Вага

~4.6 kg

Пам’ять

RAM

128 MB

Флеш-пам’ять

32 MB

11 Параметри мережі

11 Технологія підключення

11 Wired

11 Канальний протокол

11 Ethernet, Fast Ethernet, Gigabit Ethernet

Мережевий / Транспортний протокол

IPv4, IPv6, RIP, OSPF (частково підтримується в IP-Lite)

Протокол віддаленого адміністрування

SNMP v1/v2c/v3, Telnet, SSH, HTTP/HTTPS

11 Індикатори стану

11 Link activity, статус живлення, режим PoE

Характеристики

Layer 2 і базові функції Layer 3, PoE (802.3af) на всіх 24 портах, бюджет PoE до 370 Вт, підтримка QoS, ACL, портів VLAN, IP routing (статичний і RIP), підтримка безпеки, EnergyWise енергоменеджмент

Підтримувані стандарти

IEEE 802.3, 802.3u, 802.3ab, 802.3af, 802.1D, 802.1p, 802.1Q

Сокети розширення / Інтерфейси зв’язку

Сокети розширення

2 x SFP uplink слоти

Інтерфейси

24 x Ethernet 10/100/1000 - RJ-45 (з PoE) ¦ 1 x консольний порт - RJ-45 ¦ 11 1 x USB консольний 11 порт

3 Це підвищує продуктивність і безпеку мережі, рятуючи інші сегменти мережі від необхідності (і можливості) обробляти дані, які їм не призначалися. Комутатор працює на канальному рівні моделі OSI, і тому в загальному випадку може тільки поєднувати вузли однієї мережі по їхніх MAC-адресах. Для з'єднання декількох мереж на основі мережного рівня служать маршрутизатори. Комутатор зберігає в пам'яті таблицю, у якій вказуються відповідні MAC-адреси вузла порту комутатора. При включенні комутатора ця таблиця порожня, і він працює в режимі навчання. У цьому режимі дані, що поступають на який-небудь порт передаються на всі інші порти комутатора. При цьому комутатор аналізує кадри й, визначивши MAC-адресу хоста-відправника, заносить його в таблицю. Згодом, якщо на один з портів комутатора надійде кадр, призначений для хоста, MAC-адреса якого вже є в таблиці, то цей кадр буде переданий тільки через порт, зазначений у таблиці. Якщо MAC-адреса хоста-отримувача ще не відома, то кадр буде продубльований на всі інтерфейси. Згодом комутатор будує повну таблицю для всіх своїх портів, і в результаті трафік локалізується. Є 1 декілька видів загроз для мережевих комутаторів: DoS-атаки, ARP атаки, мережеві шторми, відстеження DHCP, несанкціонований доступ через порти. Атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні (англ. DoS attack, DDoS attack, (Distributed) Denial-of-service attack) – напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена. Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів (часто безглуздих або неправильно сформульованих) таким чином атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним. Взагалі відмова сервісу здійснюється: 1 a) 1 примусом атакованого устаткування до 1 зупинки роботи 1 програмного забезпечення/устаткування або до витрат наявних ресурсів, внаслідок чого устаткування не може продовжувати роботу; b) заняттям комунікаційних каналів між користувачами і атакованим устаткуванням, внаслідок чого якість сполучення перестає відповідати вимогам. У галузі комп'ютерних мереж, ARP spoofing (ARP cache poisoning – або ARP poison routing) – мережева атака, при якій зловмисник надсилає підроблені повідомлення протоколу ARP (Address 1 Resolution Protocol) в локальну мережу.. За допомогою ARP spoofing зловмисник посилає

підроблене ARP повідомлення на локальну мережу. Зазвичай мета полягає в тому, щоб зв'язати MAC-адресу 1 зловмисника з IP-адресою 1 хоста на який здійснюється атака, зазвичай це основний шлюз, щоб трафік замість цієї IP-адреси, був надісланий зловмиснику. ARP spoofing може дозволити зловмиснику перехоплювати пакети даних в мережі, змінювати трафік, або зупинити весь трафік. Часто ця атака є підготовкою для інших атак, таких як DoS-атака, атака «людина посередині», TCP hijacking. Атака може бути використана тільки в мережах, що працюють на основі Address Resolution Protocol. Оскільки в більшості мереж клієнти отримують IP адреси за допомогою DHCP, а не ручного налаштування, стає можливою захист від такої атаки за допомогою DHCP Snooping і Dynamic ARP Inspection на рівні комутаторів. Перша функція реалізує прив'язку MAC-адреси до отриманого через DHCP IPадресою. Друга перевіряє відповідність MAC-адреси відправника і змісту ARP-відповіді; в разі їх розбіжності кадр з ARP-відповіддю відкидається. Широкомовний шторм (мережевий шторм) – накопичення великих об'ємів broadcast та multicast трафіку в комп'ютерній мережі. Широкомовний шторм може спожити доступні ресурси мережі і не дати їй можливості транспортувати корисний трафік. Мережевий пакет що спричиняє такий шторм часом називаються «чорнобильським пакетом» (англ. Chernobyl packet). Комутатори для своєї роботи постійно використовують таблицю MAC адрес, яка також називається бруківці таблицею. Це поліпшення в порівнянні з функціонуванням концентраторів дозволяє знизити обсяг широкомовного трафіку в мережі. Однак бруківка таблиця не є нескінченною. Один з видів атак спрямований на переповнення таблиці MAC-адрес, що призводить до зниження швидкості передачі користувальницького трафіку аж 1 до 1 повної непрацездатності мережі. Стандартним рішенням цієї проблеми є обмеження кількості оброблюваних MAC-адрес для кожного порту комутатора. Розподіл фізичної мережі на кілька віртуальних зменшує масштаб проблеми і полегшує її діагностику, а також дозволяє більш оперативно відновити функціональність мережі. Класичний протокол основного дерева використовує ряд таймерів для забезпечення своєї роботи, що призводить до деякої затримки (близько 40 секунд) почала передачі користувальницького трафіку. Оскільки побудована топологія є деревом, в ній існує кореневої комутатор, через який проходить весь трафік. Все разом є вузьким місцем не тільки в сенсі швидкого і правильного функціонування мережі, але також і з точки зору її безпеки. Нехай спочатку в мережі було два комутатора: Root, кореневої, і Switch1. Потім зловмисник підключив контрольований ним комутатор Rogue, налаштований так, щоб стати кореневим вузлом дерева STP. Тепер весь легітимний трафік може бути перехоплений атакуючим, що є реалізацією атаки «людина посередині»

1 Вибір робочих станцій для офісної мережі

Для ефективної роботи працівників офісу необхідно обрати надійні та продуктивні персональні комп’ютери. Основними критеріями при виборі робочих станцій є

достатній рівень продуктивності для виконання типових завдань, енергоефективність, наявність сучасних інтерфейсів, а також можливість підключення до локальної мережі. Обрані моделі мають підтримувати роботу з офісними додатками, базами даних, мережею Інтернет, внутрішніми сервісами та електронною поштою. У межах проекту було обрано персональні комп’ютери на базі сучасних Intel Core i5 (рисунок 3.4), які мають оптимальне співвідношення ціни та якості.

Рисунок 3.4 – Робоча станція Lenovo Think Centre Neo 50t Gen 4

Таблиця 3.4 – Технічні характеристики типового ПК для офісної мережі

Характеристика

Опис

Модель

Lenovo ThinkCentre Neo 50t Gen 4

Форм-фактор корпусу

Tower

Процесор

Intel Core i5-13400 (10 ядер, до 4,6 GHz)

Оперативна пам’ять

8 GB DDR4 (можливість розширення до 4 GB)

Накопичувач

SSD 512 GB NVMe

Графіка

Intel UHD Graphics 730 (вбудована)

Мережевий адаптер

Gigabit Ethernet

Інтерфейси

USB 3.2, USB-C, HDMI, Display Port, Audio

Операційна система

Windows 11 Pro / Ubuntu (опційно)

Монітор

21,5” FHD LED (1920x1080)

Комплект

Клавіатура, миша, навушники

Гарантія

36 місяців

Переваги вибору:

- оптимальна конфігурація для офісних завдань та підключення до серверної інфраструктури.

- сучасний процесор забезпечує багатозадачність і енергоефективність.

- висока швидкість доступу до даних завдяки SSD-накопичувачу.

- можливість масштабування за рахунок додаткових слотів для оперативної пам’яті та накопичувачів.

Вибір робочих станцій для офісної мережі

DELL PowerEdge T40 – сервер початкового рівня, призначений для використання в малих офісних мережах. Підходить для розгортання базових служб, таких як DHCP, DNS, FTP, Web-сервер, файлове сховище або електронна пошта. Завдяки компактному форм-фактору та помірному енергоспоживанню добре інтегрується в офісну інфраструктуру. DELL PowerEdge T40 також підтримує базове апаратне резервування, що забезпечує надійність у щоденній роботі. Його конфігурація легко масштабується відповідно до потреб офісу завдяки наявності вільних слотів для оперативної пам’яті та накопичувачів. Сервер має сертифікацію на сумісність із основними серверними операційними системами, включаючи Windows Server та Ubuntu Server.

Рисунок 3.5 – DELL PowerEdge T40

Таблиця 3.5 – 14 Технічні характеристики сервера DELL PowerEdge T40

Характеристика

Опис

Тип пристрою

Сервер Tower формату

Форм-фактор корпусу

Mini Tower

Процесор

Intel Xeon E-2224G (4 ядра, 3.5-4.7 GHz, 8 МБ кеш)

Оперативна пам’ять(RAM)

8 GB DDR4 ECC UDIMM (макс. 64GB)

Жорсткий диск

1 x 1 TB SATA 7200 об/хв можливість встановлення до 3 HDD)

Слоти розширення

1 x PCIe x 16, 2 x PCIe x 1

Мережевий інтерфейс

1 x Gigabit Ethernet (Intel 1219-LM)

USB-порти

4 x USB 3.1, 14 2 x USB 2.0

14 Графіка

Intel UHD Graphics P630 (вбудована)

Операційна система (опційно)

Microsoft Windows Server / Ubuntu Server

Живлення

300W стандартний блок живленн

Вага

8.0кг

Переваги вибору:

- підтримує одночасну роботу кількох служб у невеликому офісі (до 20-30 клієнтів);

- надійна платформа для реалізації серверних сервісів у навчальному середовищі;

- простий в обслуговуванні і має потенціал для масштабування.

3.2 Налаштування мережі малого офісу

Рисунок 3.6 – Модель мережі малого офісу

3.2.1 Налаштування адресації комп'ютерів

Визначення підмереж та IP-діапазонів для VLAN'ів

У створеній моделі офісної мережі передбачено логічне поділення комп’ютерів за VLAN відповідно до їх функціонального призначення. Для кожного VLAN визначено окрему підмережу, що забезпечує ізоляцію трафіку та спрощує управління мережею.

Нижче наведено список VLAN'ів із відповідними IP-діапазонами:

VLAN_SERVER (VLAN 10): 192.168.10.0/24 – Серверний центр

VLAN_RECEPTION (VLAN 20): 192.168.20.0/24 – Приймальня

VLAN_BOSS (VLAN 30): 192.168.30.0/24 – Керівник

VLAN_ACCOUNTING (VLAN 40): 192.168.40.0/24 – Бухгалтерія

VLAN_GUEST (VLAN 50): 192.168.50.0/24 – Загальна кімната

VLAN_SALES (VLAN 60): 192.168.60.0/24 – Відділ продажів

VLAN_MARKETING (VLAN 70): 192.168.70.0/24 – Відділ маркетингу

VLAN_SUPPORT (VLAN 80): 192.168.80.0/24 – Відділ технічної підтримки.

Цей розподіл дозволяє чітко відокремити трафік між підрозділами, забезпечуючи як безпеку, так і зручність керування.

Призначення статичних IP-адрес адміністративним пристроям.

Для забезпечення стабільного з'єднання та можливості централізованого управління,

ключовим пристроям (серверу, маршрутизатору та SVI-інтерфейсам на L3-комутаторі) необхідно задати статичні IP-адреси.

Нижче наведений приклад такого призначення:

Server0 (DHCP, DNS, FTP тощо) – 192.168.10.2

SVI інтерфейси на L3-комутаторі: VLAN 10: 192.168.10.1

SVI VLAN 20: 192.168.20.1

SVI VLAN 30: 192.168.30.1

SVI VLAN 40: 192.168.40.1

SVI VLAN 50: 192.168.50.1

SVI VLAN 60: 192.168.60.1

SVI VLAN 70: 192.168.70.1

SVI VLAN 80: 192.168.80.1

Маршрутизатор (інтерфейс Gig0/0): 192.168.100.1 (як шлюз до інтернету)

L3-комутатор (інтерфейс до маршрутизатора): 192.168.100.2

Ці адреси є опорними точками для управління мережею та маршрутизації між VLAN'ами.

Перевірка адресації за допомогою командної строки

Після налаштування IP-адрес потрібно переконатися в правильності адресації та працездатності мережі. Для цього використовуються базові команди в командній строці на ПК:

Команда ipconfig – дозволяє переглянути IP-адресу, маску підмережі та шлюз за замовчуванням.

Рисунок 3.7 – Приклад результату перевірки адресації комп’ютера бухгалтерії

Команда ping – використовується для перевірки зв’язку:

• ping 192.168.20.1 – перевірка SVI приймальні

• ping 192.168.40.2 – перевірка зв’язку між приймальнею і бухгалтерією

• ping 192.168.10.2 – перевірка доступності сервера

3.2.2 Налаштування L3-комутатора

Наступним етапом після побудови локальної мережі є налаштування обладнання. Цей процес починається із налаштування L3-комутатора. У зв’язку з тим що наша мережа включає 8 підрозділів таким чином створимо 8 сегментів VLANI’ів для кожного підрозділу.

Для цього в консолі комутатора використовуємо наступні команди:

Switch# configuration 23 terminal

23 Switch(config)# vlan 10

Switch(config-vlan)# name SERVER

Switch(config-vlan)#exit

Для того, що б перевірити що наші налаштування увійшли в силу використовуємо наступну команду:

Switch# show vlan

В результаті ми отримали наступне повідомлення (рисунок 3.8)

Рисунок 3.8 – Вікно статусу створеного VLAN’у.

Таким чином створюємо VLAN’и для решти підрозділів (рисунок 3.9):

Створюємо VLAN для приймальні

Створюємо VLAN для керівника

Створюємо VLAN для бухгалтерії

Створюємо VLAN для загальної кімнати

Створюємо VLAN для відділу продажів

Рисунок – 3.9 Вікно статусу створених VLAN’ів

Наступним кроком додаємо порти ETHERNET для визначених VLAN’ів (рисунок 3.10)

Switch#

Switch# conf t

Switch (config-if)# interface range gigabitethernet 0/1

Switch (config-if)# 23 switchport mode access

23 Switch (config-if)# switchport access vlan10

Switch (config-if)# exit

Switch (config-if)# interface range gigabitethernet 0/2

Рисунок 3.10 – Додавання портів ETHERNET

Наступним кроком перевіряємо статус наших налаштувань (рисунок 3.11).

Switch# show vlan

Рисунок 3.11 – Вікно статусу створених VLAN'ів з вмістом портів у них.

3.2.3 Налаштування маршрутизатора

Відкриваємо режим конфігурування.

Задаємо ім'я маршрутизатора R1

Встановлюємо пароль на привілейований режим: class

R1 (config) # enable secret class

Налаштуємо консольний порт

R1 (config) # lineconsol 10

R1 (config-line) # logging synchronous

R1 (config-line) # exec-timeout 0 0

R1 (config-line) # password cisco

Додаємо аутентифікацію для доступу маршрутизатора

R1 (config-line) # login

R1 (config-line) # exit

Налаштовуємо баннер

R1 (config) # banner motd#Auothorized Access Only!#

Зашифруємо паролі на вхід до налаштувань маршрутизатора

R1 (config) # service password-encryption

R1 (config) # exit

Зберігаємо режим конфігурації

R1 # copy running-config startup-config

Задамо імя домену

R1 (config) # domain name cisco.com

Налаштовуємо ключ шифрування

R1 (config) # crypto key generate rsa modulus 1024

Створимо користувача і пароль для входу

R1 (config) # username secret password

Вказуємо режим підключення

R1 (config) # line vty 0 4

Вказуємо що це локальне логування

R1 (config-line) # login local

Налаштування буде тільки по SSH

R1 (config-line) # transport input ssh

R1 (config-line) # exit

R1 (config) # exit

Налаштовуємо зовнішній інтерфейс

R1# configure terminal

R1 (config) # interface gi0/2

R1 (config-if) # description Connection to ISP

R1 (config-if) # ip address dhcp

R1 (config-if) # no shutdown

Налаштувати внутрішній інтерфейс

R1 (config) # interface gi0/1

R1 (config-if) # description LAN

R1 (config-if) # ip address 192.168.1.1 255.255.255,0

R1 (config) # no shutdown

R1 (config) # exit

R1# copy running-config startup-config

3.2.4 Налаштування NAT у мережі малого офісу

У даній моделі офісної мережі всі внутрішні пристрої мають приватні IP-адреси з підмережі 192.168.0.0/24 і мають доступ до Інтернету через маршрутизатор. Щоб забезпечити вихід пристроїв в Internet з використанням однієї публічної IP-адреси, доцільно використовувати NAT типу PAT(Port Address Translation)

PAT дозволяє транслювати кілька приватних IP-адрес у одну публічну,при цьому розрізняючи сесії за номерами портів.

Почнемо з налаштування визначення Access Control List (ACL), яка визначає IP-адреси, що підлягають трансляції:

R1> enable

R1# configure terminal

R1 (config) # access-list 1 permit 192.168.0.0.0.0.0.255

R1 (config) # interface GigabitEthernet0/1

R1 (config-if) # ip address 203.0.113.1.255.255.255.0

R1 (config-if) # 13 ip nat outside

13 R1 (config-if) # no shutdown

Увімкнення PAT

R1 (config) # 13 ip nat inside source list 1 interface 13 GigabitEthernet0/1 overload

Перевірка конфігурації

13 R1# show ip nat translations

13 R1# show ip nat statistics

3.2.5 Налаштування DNS-сервера мережі малого офісу

У межах побудови малої офісної комп'ютерної мережі значну роль відіграє забезппечення зручного та централізованого доступу до внутрішніх 27 інформаційних ресурсів. До таких ресурсів належать веб-сервер, FTP-сервер,поштовий сервер,а також інші сервіси доступні в локальній мережі. 14 Для того щоб користувачі мали можливість звертатися до цих серверів за доменними іменами,а не за складними для запам'ятовування IP-адресами,доцільно впровадити та налаштувати DNS-сервер (Domain Name System)

Основною функцією DNS-сервера є трансляція доменних імен у відповідні IP-адреси. Наприклад замість введення IP-адреси 192.168.10.3 користувач може просто ввести ім'я ресурсу, наприклад www.office.local, отримати доступ до внутрішнього веб-сайту. Такий підхід не лише полегшує роботу користувачів, але й сприяє підвищенню продуктивності праці за рахунок зниження кількості помилок під час доступу до ресурсів.

У запланованій моделі DNS-сервер реалізовано як окремий пристрій на базі програмного сервера Cisco Packet Tracer, з IP-адресою 192,168,10,2. Цей сервер обслуговує всі внутрішні запити до локальних імен. Додатково ця адреса вказується у конфігурації DHCP-сервера,що дозволяє автоматично передавати її на всі клієнтські комп'ютери при отриманні ними IP-конфігурації.

Слід також зазначити що використання локального DNS-сервера зменшує залежність від зовнішніх DNS-служб і дозволяє внутрішнім службам функціонувати навіть у випадку втрати підключення до Інтернету. Це особливо важливо для таких критичних підрозділів, як бухгалтерія або адміністрація.

Таким чином,налаштування DNS-сервера в офісній мережі забезпечує централізоване управління іменами,покращує організацію мережевої інфраструктури,підвищує зручність і ефективність доступу до ресурсів,а також відповідає вимогам побудови сучасної локальної мережі.

Налаштування DNS-сервера включає в себе наступні етапи:

Підключення сервера до мережі.Сервер може бути підключений до L3-комутатора(або маршрутизатора). IP-адреса сервера – 192.168.10.2 Gateway: 192.168.10.1(інтерфейс VLAN 10).

Увімкнення DNS-служби

На сервері відкриваємо вкладку Services> DNS. У полі «DNS- Service» перемикаємо стан на «ON».У полі «Name» вводимо наприклад:www.office.local.У полі «Address» вводимо IP-адресу потрібного ресурсу, наприклад:192.168.30.10 (веб-сервер або FTP). Натиснемо «Add».

Рисунок 3.12 – Вікно статусу створення DNS- сервера малого офісу

Таблиця 3.6 Таблиця відповідності IP-адрес до деяких імен.

Імя

IP-адреса

Призначення

www.office.local

192.168.30.10

Веб-сервер

ftp.office.local

192.168.30.11

FTP-сервер

mail.office.local

192.168.30.12

Пошта

Files.office.local

192.168.20.5

Сервер бухгалтерії

На кожному ПК у випадку коли використовується DHCP – DNS-сервер автоматично видається. Якщо IP-адресацію налаштовано вручну – переходимо до наступних налаштувань:

Desktop> IP Configuration, і вводимо:

DNS Server: 192.168.10.2

Перевірка роботи DNS

На цей ПК відкриваємо CommandPrompt і виконуємо команду

ping www.office.local

Рисунок 3.13 – Статус перевірки DNS-сервера малого офісу

3.3 Налаштування мережі комплексу комп'ютерних лабораторій фахового коледжу

Рисунок 3.14 – Модель мережі комплексу комп'ютерних лабораторій фахового коледжу

3.3.1 Планування та адресація

Планування та адресація комп'ютерної мережі 19 є початковим і одним з найважливіших етапів створення сучасної інфраструктури. На цьому етапі визначається кількість пристроїв, які будуть підключені до мережі, типи підключення та необхідна кількість VLAN. Також потрібно розрахувати та призначити діапазони IP-адрес для кожного підрозділу відповідно до логічної структури мережі. Раціональне IP-планування дозволяє уникнути конфліктів адрес і спрощує адміністрування. Враховується поділ мережі на підмережі відповідно до функціонального призначення приміщень або відділів. У випадку мережі комп'ютерного комплексу важливо також передбачити резервні адреси для майбутнього розширення. Планування завершується створенням таблиці IP-адрес, яка стане основою для подальшого налаштування мережевого обладнання.

Визначаємо IP-адресацію для кожного VLAN. Адресація буде наступною:

VLAN10_Lab1: 192.168.10.0/24

VLAN10_Lab2: 192.168.20.0/24

VLAN10_Lab3: 192.168.30.0/24

VLAN10_Lab4: 192.168.40.0/24

VLAN_SUPPORT: 192.168.50.0/24

VLAN_SERVER: 192.168.99.0/24

3.3.2 Налаштування VLAN на L3-комутаторі Cisco 3560-24PS

Налаштування VLAN на L3-комутаторі Cisco3560-24PS є ключовим етапом для логічного поділу мережі на ізольовані сегменти. Це допомагає розмежувати трафік між різними підрозділами, підвищити безпеку та покращити продуктивність мережі. На створюються віртуальні локальні мережі (VLAN), кожна з яких відповідає окремій групі користувачів або відділу. Для кожного VLAN призначається свій унікальний ідентифікатор (номер VLAN) та шлюз у вигляді SVI- інтерфейсу з відповідною IP-адресою.Комутатор виконує маршрутизацію між VLAN, оскільки є пристроєм третього рівня, що забезпечує зв'язок між підмережами. Наявність VLAN спрощує управління доступом, дозволяє впроваджувати політики безпеки та контролювати трафік.Загалом, налаштування VLAN є фундаментом ефективної, структурованої та масштабованої мережі, в ізольованому сегменті мережі, із можливістю взаємодії через маршрутизацію.

Таблиця 3.7 – Реєстрація VLAN’ів структурним підрозділам фахового коледжу

VLAN ID

Назва

Призначення

10

VLAN10_Lab1

Лабораторія 1

20

VLAN10_Lab2

Лабораторія 2

30

VLAN10_Lab3

Лабораторія 3

40

VLAN10_Lab4

Лабораторія 4

50

VLAN10_SUPPORT

Служба підтримки

99

VLAN10_SERVER

Серверний сегмент

Цей крок створює Vlan і дозволяє в подальшому асоціювати їх із підключеними пристроями.

3.3.3. Налаштування віртуальних інтерфейсів (SVI) VLAN для маршрутизації між VLAN'ами.

Призначення портів до VLAN є необхідним кроком після створення віртуальних мереж на комутаторі. Кожен фізичний порт L3-комутатора закріплюється за певним VLAN відповідно до логічного розташування користувачів у мережі. Це дозволяє обмежити трафік у межах відповідного VLAN і забезпечити сегментацію мережі. Наприклад,порти, до яких підключені комп'ютери бухгалтерії, призначаються до VLAN "Accounting", а порти приймальні- до VLAN "Reception". Призначення портів виконується вручну через командний інтерфейс комутатора, що гарантує точне управління доступом. У результаті кожен пристрій в мережі отримує доступ лише до свого VLAN, якщо не передбачена міжвланова маршрутизація. Такий підхід підвищує безпеку та керованість офісної інфраструктури.

На комутаторах доступу (SW1-SW5) необхідно:

Щоб додати одразу кілька портів комутатора SW1 до одного VLAN у 20 Cisco Packet Tracer або на реальному обладнанні Cisco, потрібно скористатись командою range у консолі налаштувань.

Інтерфейси VLAN (SVI) для маршрутизації між VLAN налаштовуються на комутаторі третього рівня (L3-комутаторі).

У випадку з нашою моделлю мережі це Cisco3560-24PS – Multiplayer Switch який підтримує як комутацію (L2), так і маршрутизацію (L3).

Це логічні інтерфейси (SVI-Switched Virtual Interfaces), які працюють як шлюзи для кожного VLAN.

4 Switch (config)# interface vlan 10

4 Switch (config-if)# 4 Ip address 192.168.10.1 4 255.255.255.0

4 Switch (config-if)# No shutdown

4 Switch (config-if)# exit

4 Switch (config)# interface vlan 20

4 Switch (config-if)# 4 Ip address 192.168.20.1 4 255.255.255.0

4 Switch (config-if)# No shutdown

4 Switch (config-if)# exit

4 Switch (config)# interface vlan 30

Switch (config-if)# Ip address 192.168.30.1 4 255.255.255.0

4 Switch (config-if)# No shutdown

4 Switch (config-if)# exit

4 Switch (config)# interface vlan 40

Switch (config-if)# Ip address 192.168.40.1 4 255.255.255.0

4 Switch (config-if)# No shutdown

4 Switch (config-if)# exit

4 Switch (config)# interface vlan 50

Switch (config-if)# Ip address 192.168.50.1 4 255.255.255.0

4 Switch (config-if)# No shutdown

4 Switch (config-if)# exit

4 Switch (config)# interface vlan 99

4 Switch (config-if)# Ip address 192.168.99.1 255.255.255.0

4 Switch (config-if)# No shutdown

4 Switch (config-if)# exit

4 IP-адреса VLAN це шлюз для пристроїв у відповідному VLAN

Увімкнути маршрутизацію між VLAN

Ip routing

Без цієї команди маршрутизувати трафік між VLAN’ами буде неможливо, навіть за наявності SVI.

На звичайних L2-комутаторах (Cisco 2960) VLAN створюються,але маршрутизація між ними неможлива, тому що вони не мають підтримки IP- маршрутизації.

На L3-комутаторі створюютьсч інтерфейси VLAN (SVI), яким задаються IP-адреси, що слугують шлюзами для відповідних VLAN.

Ці IP-адреси дають змогу маршрутизувати трафік між VLAN без потреби в окремому маршрутизаторі.

3.3.4 Налаштування trunk-портів

Одним з найважливіших етапів при налаштуванні комп’ютерної мережі коледжу є конфігурація trunk-з’єднань між комутаторами. Trunk-з’єднання дозволяє передавати трафік кількох VLAN між комутаторами по одному фізичному каналу. У нашій мережі комутатори лабораторій підключаються до центрального комутатора третього рівня (L3),тому налаштування trunk є необхідним.

Для налаштування trunk-з’єднань потрібно виконати наступні дії на кожному комутаторі.

Увійти в конфігураційний режим відповідного інтерфейсу:

Interface FastEthernet0/13

Встановити режим trunk для інтерфейсу

Switchport mode trunk

За потреби дозволити лише певні VLAN

Switchport trunk allowed vlan 10, 20, 30, 50, 99

На стороні комутатора третього рівня також потрібно виконати аналогічні налаштування для портів, які зєднують його з іншими комутаторами. Це забезпечить коректну передачу VLAN-трафіку між всіма сегментами мережі.

Наявність trunk-з'єднань дозволяє розширювати мережу без порушення сегментації VLAN, зменшує кількість необхідних ліній зв'язку та забезпечує централізоване керування. Це критично важливо для ефективного функціонування комп'ютерного комплексу коледжу.

У нашій мережі фахового коледжу де використовується L3-комутатор (наприклад, Cisco 3560-24PS) як центральний пристрій, Trunk-порт налаштовується між L3-комутатором і кожним із L2 комутаторів (SW1, SW2, SW3, SW4, SW5), щоб передавати трафік із 26 кількох VLAN через одне фізичне з'єднання.

26 Trunk-з'єднання дозволяє одному фізичному кабелю передавати трафік з кількох VLAN, використовуючи тегування (802.1Q). Це необхідно, якщо:

- комп'ютери в різних VLAN'ах підключені до різних комутаторів;

- комутатори мають передавати VLAN-трафік один одному або до L3-комутатора.

Таблиця 3.8 Пояснення необхідності налаштування trunk-портів

З'єднання

Trunk

Пояснення

L3-комутатор SW1

Так

Передача VLAN-трафіку між ядром і лаб1

L3-комутатор SW2

Так

Аналогічно-для лабораторії 2

L3-комутатор SW3

Так

Аналогічно-для лабораторії 3

L3-комутатор SW4 (якщо є)

Так

Наприклад, для адмінчастини

L3-комутатор-Сервер

Ні

Сервер знаходиться в одному VLAN’і (наприклад Server-VLAN), отже наявність access-порту достатньо

L3-Комутатор-Маршрутизатор

Ні

(в більшості випадків)

Якщо лише для виходу в Інтернет – достатньо порту в режимі access. Trunk – лише якщо потрібна маршрутизація між кількома VLAN на маршрутизаторі(Router-on-a-stick), але у нашій мережі цю функцію виконує L3-комутатор

Рисунок 3.15 – Стан портів комутатора після базової конфігурації

Рисунок 3.16 – Вікно статусу додавання VlAN’ів для мережі фахового коледжу

Налаштувати зовнішній інтерфейс

Router# configure terminal

R1 (config) # interface gi0/2

R1 (config-if) # description Connection to ISP

R1 (config-if) # ip address dhcp

R1 (config-if) # no shutdown

Налаштувати внутрішній інтерфейс

R1 (config) # interface gi0/1

R1 (config-if) # description LAN

R1 (config-if) # ip address 192.168.1.1 255.255.255,0

R1 (config) # no shutdown

R1 (config) # exit

R1# copy running-config startup-config

3.3.5 Налаштування DHCP-сервера

Одним із важливих етапів побудови мережі є автоматичне призначення IP-адрес пристроям,що підключаються. Це забезпечується за допомогою DHCP-сервера

У середовищі Cisco Packet Tracer DHCP-сервер реалізовуємо на виділеному сервері типу “Server”, який підключений до мережі через комутатор або L3-комутатор. На цьому сервері у вкладці Services DHCP необхідно створити окремі пули IP-адрес для кожного VLAN’у, вказавши: ім’я пулу, мережеву адресу, маску підмережі, шлюз (Default Gateway) тобто IP-адресу відповідного SVI на L3- комутаторі. Для прикладу, для VLAN бухгалтерії з мережею 192.168.20.0/24 необхідно вказати шлюз 192.168.20.1 та діапазон адрес, наприклад від 192.168.20.10 до 192.168.20.50. Такі налаштування повторюються для кожного VLAN, щоб комп’ютери в різних підмережах автоматично отримували коректні параметри мережі. Після запуску DHCP та підключення клієнтських комп’ютерів до відповідних портів VLAN, можна перевірити успішність отримання адреси через команду ipconfig у вікні Command Promt на кожному ПК. Таким чином, DHCP-сервер забезпечує централізоване, ефективне, та гнучке керування IP-аресами в комп’ютерній мережі коледжу.

Рисунок 3.17 – Встановлення IP-адресації сегментів підмереж на сервері комп’ютерної мережі комплексу лабораторій фахового коледжу

3.3.6 Налаштування NAT на маршрутизаторі Router1

Для забезпечення доступу локальних пристроїв комп’ютерної мережі фахового коледжу до глобальної мережі Інтернет необхідно реалізувати технологію трансляції мережевих адрес NAT (Network Address Translation). У нашій мережі всі хости мають приватні IP-адреси, які не маршрутизуються в Інтернеті. Тому без NAT локальні адреси не зможуть взаємодіяти із зовнішніми ресурсами. NAT дає змогу транслювати приватні IP-адреси у публічну (зовнішню) адресу, призначену маршрутизатору, тим самим забезпечуючи вихід в Інтернет. У нашому випадку реалізовано динамічний NAT з використанням пулу адрес (якщо є декілька публічних IP-адрес) або PAT (Port Address Translation), коли використовується лише одна публічна IP-адреса. У середовищі Cisco Packet Tracer для спрощення використовується PAT(NAT Overload), що є найпоширенішим варіантом для навчальних і малих мереж.

Послідовність налаштування NAT (PAT) на маршрутизаторі Router1:

Переходимо в конфігураційний режим маршрутизатора:

Визначаємо внутрішні і зовнішні інтерфейси NAT:

Створюємо ACL (Access Control List), яка вказуватиме, які адреси транслювати:

Припускаємо налаштування, якщо внутрішня мережа матиме наступну IP-адресацію 192.168.0.0/16

Налаштування PAT (NAT Overload):

Рисунок 3.18 – Налаштування PAT (NAT Overload) для мережі комплексу лабораторій фахового коледжу

3.3.7 Налаштування DNS-сервера

У сучасних комп’ютерних мережах надзвичайно важливим є використання зручних механізмів ідентифікації ресурсів. Одним із таких механізмівє служба доменних імен (DNS), яка забезпечує перетворення зручних для сприйняття імен хостів у відповідні IP-адреси. Це дає змогу користувачам легко звертатися до серверів і сервісів за допомогою логічних назв, а не запам’ятовувати цифрові адреси. У межах реалізації мережі комп’ютерного комплексу фахового коледжу було передбачено налаштування локального DNS-сервера. Він обслуговує запити користувачів до внутрішніх ресурсів, зокрема FTP-сервера, веб-сервера, файлового сервера та інших. Це не лише підвищує зручність роботи, але й дозволяє краще управляти ресурсами у внутрішньому середовищі мережі. Нижче розглянуто послідовність дій з налаштуванням DNS-сервера у середовищі Cisco Packet Tracer.

Послідовність налаштування DNS-сервера в Cisco Packet Tracer:

1) Налаштовуємо IP - адресацію

2) Вмикаємо служби DNS

3) Створюємо записи доменних імен

4) Перевіряємо роботу DNS

5)Вказуємо DNS сервер в DHCP налаштуваннях

Рисунок 3.19 – Вікно статусу реєстрації DNS-сервера для робочих станцій мережі комплексу лабораторій фахового коледжу

3.3.8 Налаштування TFTP-сервера

У мережі фахового коледжу доцільно використовувати TFTP-сервер (Trivial File Transfer Protocol) для централізованого збереження та відновлення конфігурацій мережевого обладнання, зокрема комутаторів і маршрутизаторів. Це особливо важливо в середовищах з великою еількістю пристроїв, де резервне копіювання дозволяє швидко відновити мережу у разі збоїв або помилкоивх змін конфігурацій.

TFTP-сервер можна реалізувати на вбудованому сервері в Cisco Packet Tracer. Для цього потрібно перейти на сервер, увімкнути відповідну службу (TFTP), а також переконатися,що пристрої в мережі можуть з ним зв’язуватися. Після цього з комутаторів або маршрутизаторів можна виконати завантаження або збереження конфігурації за допомогою команд у CLI-режимі.

Наприклад для збереження конфігурації з маршрутизатора на TFTP-сервер використовуються такі команди:

Router>en

Router# 18 copy startup-config tftp

18 Address or name of remote host []? 192.168.10.10

Destination filename [running-config]? r1-backup.cfg

Writing running-config.....

Це забезпечує простий механізм резервного копіювання конфігурацій, що є важливим для підтримки безперебійної роботи мережі. Рекомендується регулярно створювати копії конфігурацій у TFTP-сервері після змін, а також мати доступ до серверу з усіх керованих пристроїв. У нашому випадку IP-адреса TFTP-сервера повинна бути в одному з VLAN, до яких мають доступ мережеві пристрої. У проєктованій мережі фахового коледжу це може бути окремий VLAN Management або Server VLAN.

Рисунок 3.20 Вікно створених серверів в мережі комплексу лабораторій фахового коледжу

Посилання

Це джерела виділених збігів у вашому документі. Кожен збіг позначено темно-зеленим числом, яке відповідає вказаному тут джерелу. Джерела впорядковані за схожістю — чим вищий бал, тим сильніше збіг.

#	Джерело	%
1	dspace.wunu.edu.ua	5.8%
2	ukrreferat.com	3.1%
3	dbpedia.org	1.8%
4	elar.khnu.km.ua	0.9%
5	ni.biz.ua	0.8%
6	inmad.vntu.edu.ua	0.7%
7	eprints.kname.edu.ua	0.5%
8	uk.wikipedia.org / Мережевий_комутатор	0.5%
9	dspace.wunu.edu.ua	0.5%
10	studfile.net	0.4%
11	jetiq.vntu.edu.ua	0.3%
12	ztu.edu.ua	0.3%
13	ccna7.com	0.2%
14	server-store.com.ua	0.2%
15	er.nau.edu.ua	0.1%
16	rep.knlu.edu.ua	0.1%
17	elartu.tntu.edu.ua	0.1%
18	cisco.com	0.1%
19	profitex.ua	0.1%
20	repositsc.nuczu.edu.ua	0.1%
21	comuedu.ru	0.1%
22	skid.lpnu.ua	0.1%
23	studyblue.com	0.1%

#	Джерело	%
24	key4.com.ua	0.1%
25	ua.machinepharmaceutical.com	0.1%
26	duikt.edu.ua	0.1%
27	rada.gov.ua	0.1%
28	ela.kpi.ua	0.1%
29	khnu.km.ua	0.1%

Plag

Дякуємо, що перевірили
свій документ за допомогою
Plag!