МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ ЕКОЛОГІЧНИЙ УНІВЕРСИТЕТ

Факультет комп'ютерних наук,
управління та адміністрування
Кафедра інформаційних технологій

Кваліфікаційна робота бакалавра

на тему: Розробка проекту захищеної комп'ютерної мережі

Виконав студент групи К-19і
спеціальності 122 Комп'ютерні науки
Іванченко Юрій Юрійович

Керівник к.т.н., доцент
Фразе-Фразенко Олексій
Олексійович

Рецензент к.т.н., Домаскін Олег
Михайлович

Одеса 2021

ЗМІСТ

ВСТУП

У сучасному світі активно розвиваються мережні й інформаційні технології. В даний час неможливо знайти підприємство, яке функціонує без впровадженої мережі передач даних. Подібна мережа дозволяє виконувати величезну кількість завдань, максимально спрощуючи різні дії, такі як:

– обмін інформацією;
– робота з документами;
– доступ до всіляких ресурсів;
– управління додатками;
– зберігання інформації.

Інформація є дуже цінним ресурсом, тому зловмисники нерідко намагаються отримати доступ до системи підприємства. Вони можуть завдати шкоди, що складається в крадіжці персональних даних і даних компанії, і зараженні системи з повним знищенням ресурсів. Засоби масової інформації дуже часто повідомляють про кібератаки на різні підприємства. Виходить, щоб цього уникнути, потрібно дуже уважно підійти до питання модернізації мережі, особливо з боку безпеки. Все це вказує на високу актуальність даної дипломної роботи.

Часи, коли до інтернету могли підключатися тільки комп'ютери, залишилися давно в минулому. Сьогодні вихід у Всесвітню павутину мають планшети і смартфони, Smart TV, медіа-приставки і навіть побутова техніка – холодильники, системи кондиціонування, кавоварки та багато іншого. Великою популярністю користуються системи «Розумний будинок». Електроніка та програми, безумовно, спрощують життя людини, але разом з тим створюють додаткові проблеми і ризики, яких раніше не було.

Актуальність і значимість проблеми забезпечення інформаційної безпеки обумовлена наступними факторами:

- застосовувані засоби забезпечення інформаційної безпеки не відповідають високому рівню розвитку інформаційних технологій;
- повсюдне використання Інтернет тягне до появи загроз з боку віддалених користувачів;
- постійне збільшення кількості персональних комп'ютерів, захист яких не відповідає вимогам безпеки;
- зростання обсягів інформації, що обробляється і зберігається з використанням інформаційних технологій;
- недосконалість програм і мережевих технологій з точки зору інформаційної безпеки.

Тому перед керівництвом будь-якої компанії рано чи пізно постає питання про об'єднання своєї комп'ютерної мережі з віддаленими майданчиками. Філії в інших містах, замовники, партнери, віддалені співробітники – багатьом групам користувачів може знадобитися надання безпечного доступу до внутрішніх ресурсів.

1 АКТУАЛЬНІСТЬ ЗАХИЩЕНИХ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Передумови створення захищеної комп'ютерної мережі

Комп'ютерна мережа – система, що забезпечує обмін даними між обчислювальними пристроями (комп'ютери, сервери, маршрутизатори та інше обладнання). Для передачі інформації можуть бути використані різні середовища.

В даний час використання комп'ютерних мереж є невід'ємною частиною нашого життя, область їх застосування охоплює всі сфери людської діяльності. Комп'ютерна мережа – це сукупність комп'ютерів і різних пристроїв, що забезпечують інформаційний обмін між комп'ютерами в мережі без використання будь-яких проміжних носіїв інформації. Розвиток комп'ютерних мереж пов'язано як з розвитком власне ЕОМ, що входять до складу мережі, так і з розвитком засобів телекомунікацій [2]. Роботи зі створення комп'ютерних мереж почалися ще в 60-х роках XX століття. Прообразом комп'ютерних мереж з'явилися системи телеобробки даних, побудовані на базі великих (а пізніше і міні ЕОМ). Як засоби передачі даних використовувалася існуюча телефонна мережа.

Загрози для IT-інфраструктури з кожним роком стають все складніше, для захисту від них потрібно застосовувати різні системи і засоби. П'ятнадцять років тому для захисту комп'ютера досить було встановити на ньому антивірус. З розвитком мережевих технологій виникла потреба в міжмережевих екранах, потім в системах запобігання вторгнень. Зараз для захисту персональних даних, крім антивіруса, брандмауера і засобів запобігання вторгнень, необхідно також використовувати засоби контролю цілісності і сканер вразливостей.

Коли мережа піддається вторгненню, DoS-атаці або вірусної епідемії, під загрозою опиняється діяльність всієї організації. Це відбувається тому, що збільшується небезпека для операційних ресурсів, призначених для

користувача даних, власних коштів і технологій. Інтелектуальна власність може бути вкрадена і неправомірно використано третьою стороною.

Захист локальних мереж підприємств з кожним роком стає все більш складним завданням і сьогодні є одним з основних факторів, з якими стикається бізнес. Нові загрози з'являються на регулярній основі, і жодна організація від них не застрахована. Варто зазначити, що кожен раз при появі нового виду небезпечних загроз змінюється саме поняття «безпечна мережа».

Створення захищеної комп'ютерної мережі – це найкращий спосіб організації єдиного інформаційного середовища підприємства. Завдяки їй користувачі отримають доступ до загальних ресурсів, зможуть спільно використовувати принтери та інше мережеве обладнання. Правильно налаштувавши мережу, адміністратор може забезпечити належний рівень секретності і запобігти витоку даних, що становлять комерційну таємницю [3].

Актуальність і значимість проблеми забезпечення інформаційної безпеки обумовлена наступними факторами:

– застосовувані засоби забезпечення інформаційної безпеки не відповідають високому рівню розвитку інформаційних технологій;
– повсюдне використання Інтернет тягне до появи загроз з боку віддалених користувачів;
– постійне збільшення кількості персональних комп'ютерів, захист яких не відповідає вимогам безпеки;
– зростання обсягів інформації, що обробляється і зберігається з використанням інформаційних технологій;
– недосконаліть програм і мережевих технологій з точки зору інформаційної безпеки.

Мета концепції захищеної корпоративної мережі – закрити трафік корпоративної мережі засобами захисту інформації мережевого рівня і організувати фільтрацію інформації в точках з'єднання з відкритими мережами.

В якості фільтрації інформації на інтерфейсах з відкритими мережами застосовуються традиційні рішення: міжмережевий екран (firewall) або сервіси захисту типу proxy.

Важливим елементом захисту від несанкціонованого проникнення в корпоративну мережу з відкритою є послідовне (каскадне) включення декількох фільтрів-ешелонів захисту. Як правило, між відкритою і корпоративною мережею встановлюється зона контрольованого доступу.

Весь процес організації захищеної комп'ютерної мережі можна розділити на наступні етапи:

1) Розробка мережі. На цьому етапі фахівці обстежують територію підприємства, вислуховують побажання замовника по функціоналу, складають план, ТЗ і готують обладнання, необхідне для її установки.
2) Монтаж. На цьому етапі прокладаються кабелі, проводиться монтаж обладнання та налаштування необхідного програмного забезпечення.
3) Тестування. Фахівці перевіряють роботу, відповідність встановленої мережі загальноприйнятим стандартам якості.
4) Обслуговування. Цей етап включає модернізацію і при необхідності усунення неполадок.

Створена мережа підприємства повинна задовольняти таким основним вимогам:

– Бути легко керованою.
– Бути захищеною від хакерських атак. Захист корпоративної мережі передбачає установку спеціального програмного забезпечення – файрвола.
– Бути адаптованої до основних типів мережевих пристроїв і кабелів. Завдяки цьому мережа в будь-який момент можна модернізувати.

1.2 Мережеві атаки і методики захисту від них

Як приклади найбільш поширених мережевих атак можна навести такі види впливу:

– Застосування нестандартних протоколів. Тип протоколу пакета даних визначається по вмісту в ньому спеціальному полю. При зміні зловмисниками значення в цьому полі здійснюється передача даних, яку система не може визначити.
– Ping Flooding. Така атака може бути реалізована тільки за умови доступу до високошвидкісного інтернету. Вона передбачає застосування флудинг замість стандартної команди контролю пинга. В результаті створюється надмірне навантаження на мережу, що призводить до порушень в її роботі.
– Фрагментація даних. При передачі по IP пакет даних ділиться на частини, а на стороні одержувача – збирається. У разі атаки виконується відправка значного числа подібних фрагментів із засміченням буфера обміну і порушень роботи мережі.

У зв'язку з швидким розвитком інформаційних технологій і технічних засобів статичні механізми захисту від мережевих погроз часто виявляються неефективними. Забезпечити ефективний захист інформації дозволяють динамічні методи, здатні оперативно виявляти і усувати загрози. Робота динамічних технологій будується на оцінки рівня підозрілості дій в мережі з боку певної служби або процесу [6].

Алгоритм дії щодо усунення атак спрямований на ідентифікацію підозрілих об'єктів. Після цього система реагує необхідним чином на діяльність таких об'єктів, яка може бути націлена на ресурси мережі або комп'ютерного обладнання.

Для захисту мереж від зовнішніх загроз можуть застосовуватися наступні основні методи і технології:

– застосування портів високої надійності, шифрування даних;

– використання ефективних антивірусів і сканерів;
– застосування програмного або апаратного мережевого екрану;
– установка блокіраторів руткітів і сніфферов.

На сьогоднішній день відомі наступні види мережевих атак [7]:

– mailbombing;
– застосування спеціалізованих додатків;
– переповнення буфера;
– мережева розвідка (збір відомостей за допомогою додатків, які перебувають у вільному доступі);
– IP-спуфинг (хакер видає себе за законного користувача);
– DDOS-атака (шляхом перевантаження обслуговування звичайних користувачів унеможливлюється);
– Man-in-the-Middle (впровадження з метою отримання пакетів, переданих всередині системи);
– XSS-атака (ПК клієнта піддаються атаці через уразливості на сервері);
– фішинг (обман жертви шляхом відправки повідомлень з нібито знайомого адреси).

Різноманітність видів мережевих атак, яким можуть піддаватися корпоративні і приватні мережі, вимагає вироблення ефективних заходів щодо їх захисту. Такі заходи повинні розроблятися і застосовуватися завчасно. Ефективний захист від загроз допоможе зберегти недоторканними конфіденційні дані і забезпечити стабільну роботу мережі. Завдяки цьому багато разів окупаються витрати, понесені на впровадження такого захисту.

1.2.1 Mailbombing

Суть дії в тому, що e-mail користувача буквально завалюється листами. Для цього використовується масова розсилка. Мета – відмова роботи поштової скриньки або всього поштового сервера.

Для проведення цієї атаки не потрібні особливі навички. Досить знати електронну адресу потенційної жертви і адреса сервера, з якого можна відправляти повідомлення анонімно.

Перше правило захисту, до якого може вдатися кожен – не давати адресу своєї поштової адреси сумнівним джерелам. Спеціалісти задають певні настройки на web-сайті провайдера. Ліміт кількості листів, що надходять з певного IP, обмежений. Коли прикладна програма «бачить», що число повідомлень перевалило межа норми, листи «на автоматі» відправляються в кошик. Але ніщо не заважає злочинцеві проводити розсилку з різних адрес.

1.2.2 Застосування спеціалізованих додатків

Використання особливих додатків – найпоширеніший спосіб виведення серверів з ладу. У хід йдуть віруси, трояни, руткіти, сніфери.

Вірус – шкідливий софт, заточений на виконання певної функції. Впроваджується в інші програми (легальні в тому числі) на ПК жертви. Після вбудовування приступає до здійснення прописаної «місії». Наприклад, проводить шифровку файлів, блокує завантаження комп'ютерної платформи, прописавши себе в BIOS [6].

«Троянський кінь» – це вже не програмна вставка, а повноцінне шкідливий додаток, яке маскується під нешкідливе. Троян може виглядати, наприклад, як гра. Якщо користувач її запустить, почнеться поширення файлу. Програма розсилає свої копії за всіма електронними адресами, які є на

ПК жертви. Найчастіше «троянський кінь» викрадає дані банківських карт, електронних гаманців – словом, прагне отримати доступ до фінансових ресурсів.

Сніффер краде пакети даних, переправлялися ПК на різні сайти. Для цього використовується мережева плата, яка функціонує в режимі promicuous mode. У такому режимі всі пакети, переправлені через карту, відправляються на обробку додатком. Таким чином, може бути відкритий доступ до конфіденційної інформації – наприклад, списку паролів і логінів від банківських рахунків.

Руткіт приховує сліди злочинів зловмисників, маскує шкідливу діяльність, через що адміністратор не помічає того, що відбувається.

1.2.3 Переповнення буфера

Зловмисник зайнятий пошуком програмних або системних вразливостей. При виявленні таких провокується порушення кордонів оперативної пам'яті, робота додатки завершується в аварійному режимі, виконується будь двійковий код.

Захист полягає в тому, щоб виявити і усунути вразливості. Також використовуються нездійсненні буфера, але цей метод здатний запобігти тільки ті атаки, в яких застосовується код.

2 АНАЛІЗ ІСНУЮЧИХ ПРОГРАМ ТА ВИБІР АКТУАЛЬНОГО ВАРІАНТУ

2.1 Огляд і аналіз аналогів програм

Завдання комп'ютерного моделювання телекомунікаційних систем на сьогоднішній день має досить багато рішень різного роду. Одними з популярних продуктів є OPNET, OMNET ++, NS2, NS3, які є потужним засобом моделювання за рахунок об'єктно-орієнтованих мов програмування як вбудованої мови опису моделей телекомунікаційних систем. Так само існують вузькоспеціалізовані симулятори, створені лише для моделювання певного обладнання. Як правило, подібне програмне забезпечення випускається виробниками телекомунікаційного обладнання.

Компанією Cisco Systems, що є виробником мережевого устаткування, були запропоновано програмне забезпечення для моделювання мереж, яке дозволяє експериментувати з різними топологіями мереж і їх поведінкою всередині: симулятори Packet Tracer, Dynamips, GNS3.

2.1.1 Симулятор GNS3

Graphical Network Simulator (рис. 2.1) – це графічний симулятор мережі, який дозволяє змоделювати віртуальну мережу з маршрутизаторів і віртуальних машин. Незамінний інструмент для навчання та тестів. Працює практично на всіх платформах. Дуже добре підходить для створення стендів на десктопних машинах [8].

Залежно від апаратної платформи, на якій буде використовуватися GNS3, можлива побудова комплексних проектів, що складаються з маршрутизаторів Cisco, Cisco ASA, Juniper, а також серверів під управлінням мережевих операційних систем.

GNS3 має декілька серйозних недоліків:

- Сильно вимогливий до CPU і пам'яті. 10 маршрутизаторів вже всерйоз навантажать ПК. Використання процесора можна знизити за допомогою механізму Idle PC. Без цього і 3-4 насилу б, мабуть, пішли.
- Дуже слабо підтримує функції L2. Є тільки подобу комутаторів, на яких можна максимум налаштувати Access / Trunk порти і свічовие плати для маршрутизаторів, L2-функціонал яких також дуже обмежений.
- Відсутність можливості повноцінної симуляції комутаторів другого рівня Cisco. Цей недолік не буде виправлений в нових версіях, так як його причиною є кардинальна відмінність в апаратній платформі маршрутизаторів і світчей Cisco.
- До складу GNS3 не належать образи IOS / IPS / PIX / ASA / JunOS, так як вони є частиною комерційних продуктів відповідних компаній, і ніякого прямого відношення до проекту GNS3 не мають.

Однією з найцікавіших особливостей GNS3 є можливість з'єднання проектованої топології з реальною мережею. Це дає просто унікальну можливість перевірити на практиці будь-який проект, без використання реального обладнання. Використання WireShark дозволяє провести моніторинг трафіку всередині проектованої топології, що дає додаткову інформацію для розуміння досліджуваних технологій.

При відсутності можливості отримати доступ до реального обладнання, GNS3 стане практично повноцінної лабораторією.

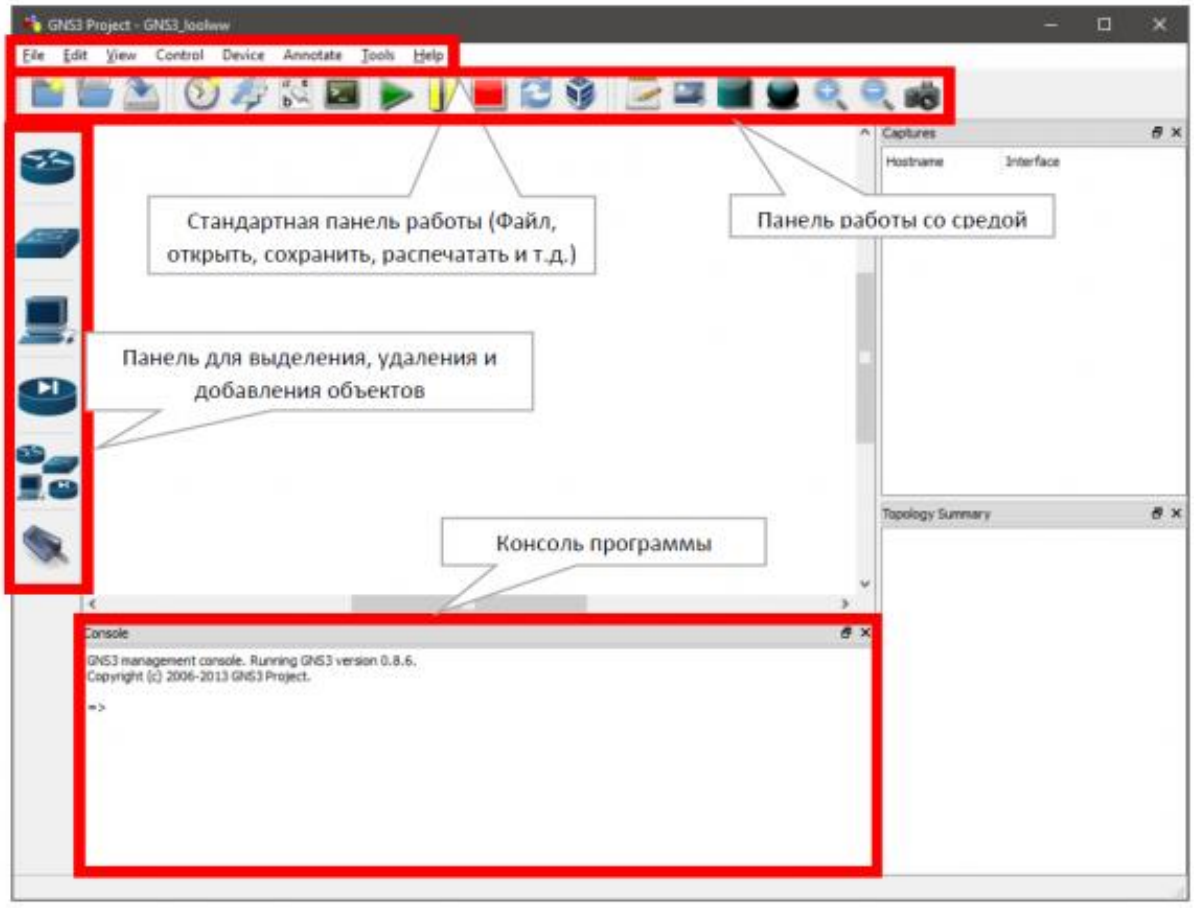

Рисунок 2.1 – Вікно програми GNS3 і його структура

2.1.2 Симулятор Verax SNMP Agent Simulator

Verax SNMP agent simulator дозволяє IT-персоналу створювати віртуальні моделюються мережі пристроїв без придбання будь-якого додаткового обладнання, наприклад, для тестування [9].

Verax SNMP Simulator (рис. 2.2) – це інструмент, який може імітувати кілька агентів SNMPv1 / v2c на одному хості через стандартний порт 161 через мульти-мережу. Окремі відповіді змодельованого агента можуть бути спочатку отримані з існуючих пристроїв і змінені під час виконання за визначеними користувачем правилами.

Продукт може комбінувати різні поведінки агентів, налаштовувати події і шаблони поведінки або пасток. У варіанті віддаленого управління і в розподілених системах може бути кілька симуляторів, кожен має власне движок і графічну консоль управління. У множині варіанті застосування симуляторів – центральне управління має одна проста консоль.

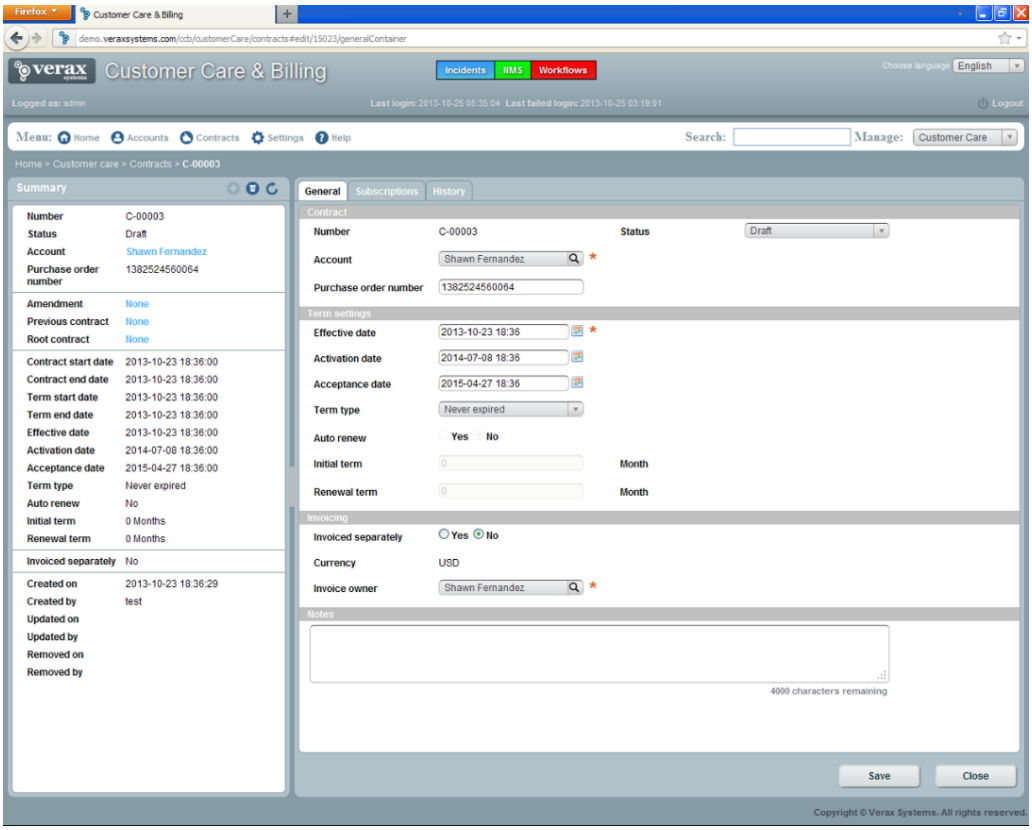

Рисунок 2.2 – Вікно симулятора Verax SNMP Simulator

Особливості:

1) Консоль для управління типами пристроїв, адресами і їх екземплярами;
2) Підтримка декількох агентів і декількох мереж на одному хості;
3) Файли конфігурації відповідей SNMP, сумісні з вихідними даними SNMP, для легкого створення початкових змодельованих відповідей агента з існуючих пристроїв;
4) Багатий набір правил для зміни відповідей агента;

5) Генерація випадкових MAC-адрес і IP-адрес, включаючи розширені сценарії, такі як рандомізація тільки частини адреси (наприклад, мережева частина IP-адреси є фіксованою, хостової частина змінюється);
6) Генерація випадкового цілого числа, лічильника і строкових значень, включаючи сценарії «один раз» або «кожен раз»;
7) Підтримка цілочисельних арифметичних операцій (наприклад, яке значення на основі суми двох інших значень);
8) Генерація значень на основі тренда (напрямок, діапазон кроків, порогове значення скидання), наприклад, для збільшення лічильників.

2.1.3 Емулятор Dynamips

Dynamips – це комп'ютерна програма емулятора (рис.2.3), яка була написана для емуляції маршрутизаторів Cisco. Він був створений Крістофом Філло, який почав свою роботу в серпні 2005 року.

Емулятор маршрутизаторів Cisco, який може працювати в Windows, Linix і Mac OS X. Розповсюджується за ліцензією GNU GPLv2 (чого не можна сказати про образи, які він використовує). Дозволяє запускати віртуальну машину з оригінальним чином ОС від старих маршрутизаторів сімейств 1700, 3725, 7200 і деяких інших. Дозволяє імітувати інтерфейси Ethernet і вимираючі ATM і Serial. При цьому Dynamips не може працювати з прошивками комутаторів, так як їх ОС орієнтовані на використання ASIC, які у великій кількості зустрічаються в комутаторах і дуже складно імітуються на x86 системах.

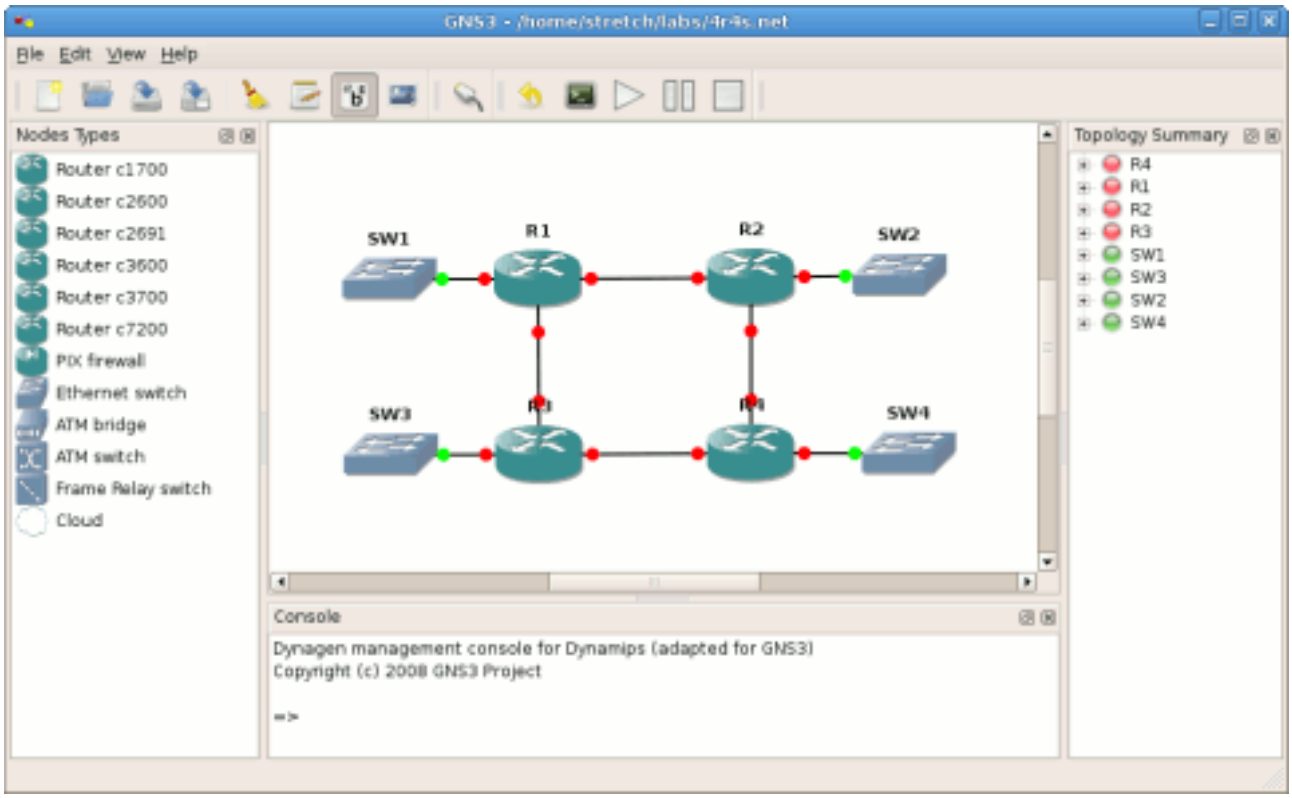

Рисунок 2.3 – Вікно емулятора Dynamips

2.2 Опис симулятора Cisco Packet Tracer

Даний програмний продукт розроблений компанією Cisco і рекомендований використовуватися при вивченні телекомунікаційних мереж і мережевого устаткування [1]. На основі програмного продукту Packet Tracer є можливість створювати мережеві топології з широкого безлічі маршрутизаторів і комутаторів компанії Cisco, робочих станцій і мережних з'єднань типу Ethernet, Serial, ISDN, Frame Relay. Функції симулятора можуть бути придатні як для навчання, так і для роботи, настройки мережі ще на етапі планування.

Packet Tracer включає наступні особливості:

– Робочий простір для створення мережі будь-якого розміру і складності;
– Моделювання в режимі реального часу;

- Моделювання в режимі симуляції;
- Графічний інтерфейс для взаємодії з користувачем під час налаштування мережевих пристроїв;
- Зображення мережевого обладнання з підтримкою додавання, видалення, переміщення різних компонентів.

Даний симулятор дозволяє студентам проектувати свої власні мережі, створюючи і відправляючи різні пакети даних, зберігати і коментувати свою роботу. Надається можливість вивчати і використовувати такі мережеві пристрої, як комутатори, маршрутизатори, робочі станції, визначати типи зв'язків між ними і з'єднувати їх.

Відмінною особливістю даного симулятора є наявність в ньому режиму симуляції (рис. 2.4). В даному режимі всі пакети, що пересилаються всередині мережі, відображаються графічно. Ця можливість дозволяє студентам наочно продемонструвати, за яким інтерфейсу в дані момент переміщається пакет, який протокол використовується. Працюючи в симуляторі в іншому режимі, режимі реального часу, не можна простежити за переміщенням пакетів, відразу відображається кінцевий результат виконаних дій.

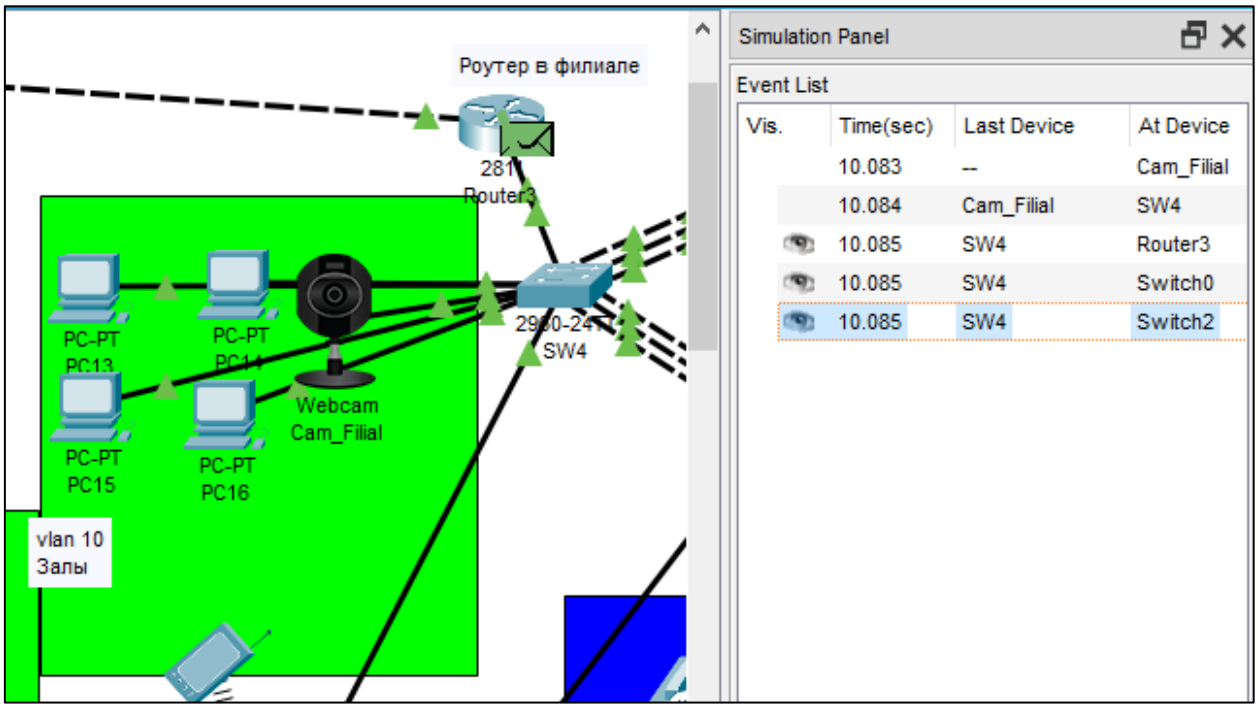

Рисунок 2.4 – Режим симуляції в Packet Tracer

Однак, це не всі переваги Packet Tracer: в режимі симуляції студент може не тільки відслідковувати використовувані протоколи, а й бачити, на якому з семи рівнів моделі OSI даний протокол задіяний, а так само вміст пакета, його формат. Tracer здатний моделювати велику кількість пристроїв різного призначення, а так само чимало різних типів зв'язків, що дозволяє проектувати мережі будь-якого розміру на високому рівні складності [5].

Моделюються пристрої:

– Комутатори другого і третього рівня
– Маршрутизатор
– Мережеві концентратори
– Кінцеві пристрої (робочі станції, ноутбуки, сервери, принтери)
– Бездротові пристрої (точки доступу, бездротові маршрутизатори)
– Глобальна мережа WAN

Підтримувані типи зв'язків між пристроями:

– Консоль

– Мідний кабель з прямим підключенням
– Мідний кабель з перехрещуванням
– Волоконно-оптичний кабель
– Телефонна лінія
– Serial DCE / DTE

Кожен пристрій в програмному продукті Cisco Packet Tracer може бути налаштоване через вікно властивостей, яке викликається по подвійному кліку на пристрої. Перша вкладка Physical (рис. 2.5) відповідає за фізичні параметри пристрою. Під час налаштування маршрутизаторів і комутаторів в них можна додавати нові модулі, в робочі станції і сервери – вставляти мережеві адаптери.

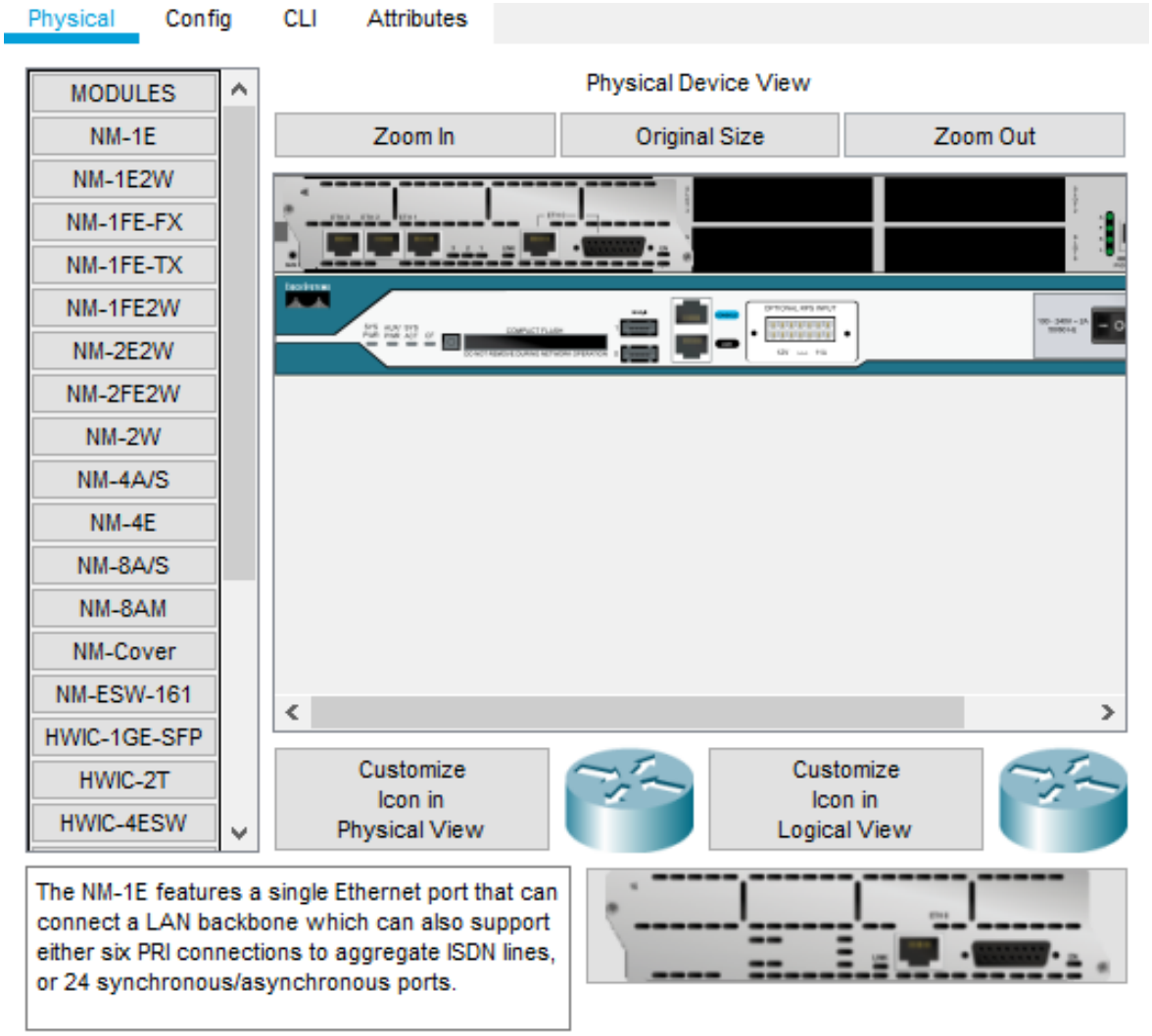

Рисунок 2.5 – Фізичний вигляд пристрою (маршрутизатора)

На вкладці Config (рис. 2.6) можна задавати основні параметри мережевих інтерфейсів (IP-адреси, маски підмережі, параметри бездротової мережі та ін.) У мережевих пристроях також можна конфігурувати маршрутизацію – статичну або динамічну, у серверів – конфігурувати служби.

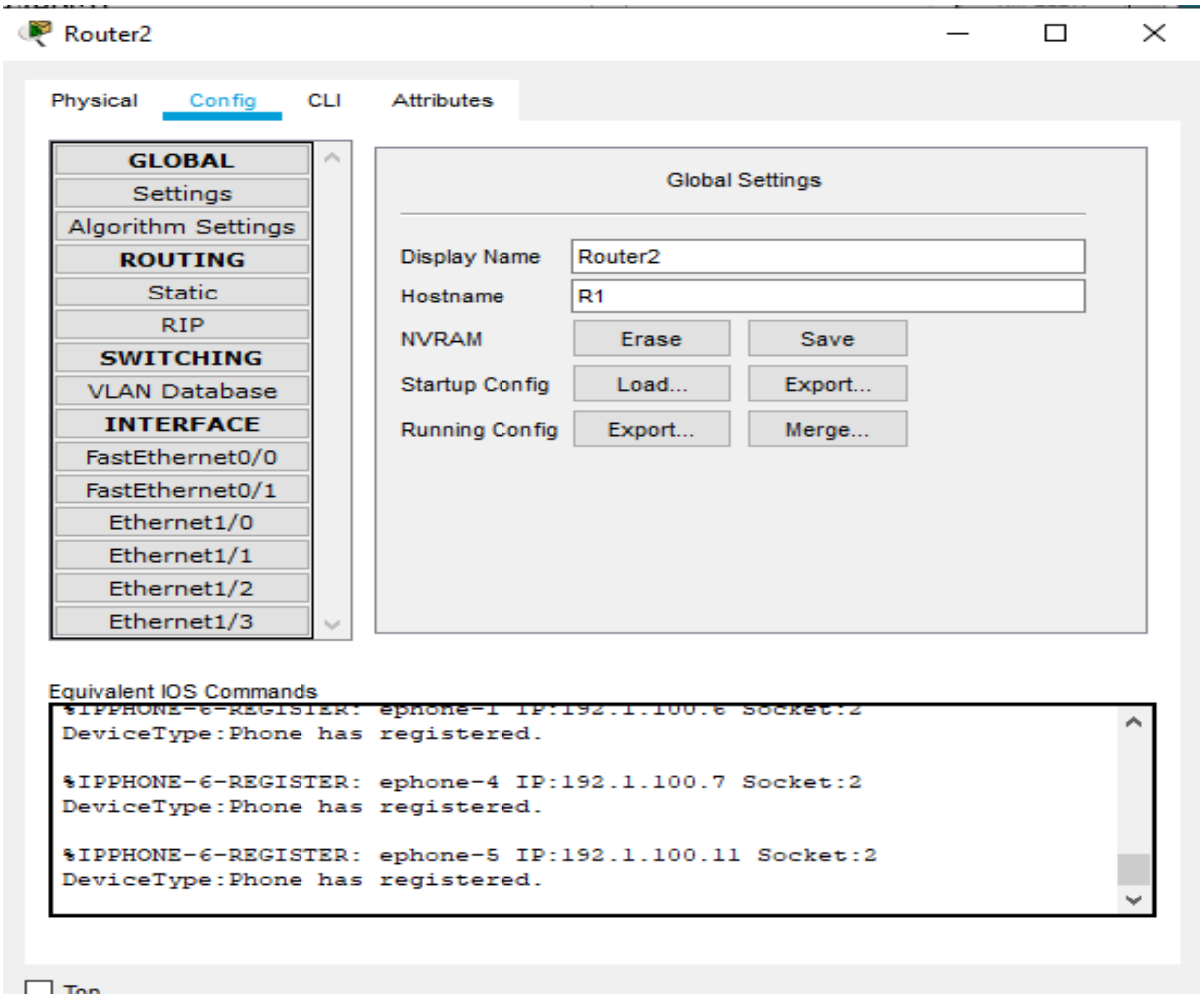

Рисунок 2.6 – Конфігурація сервера

При запуску програми відкривається головне вікно симулятора (рис. 2.7):

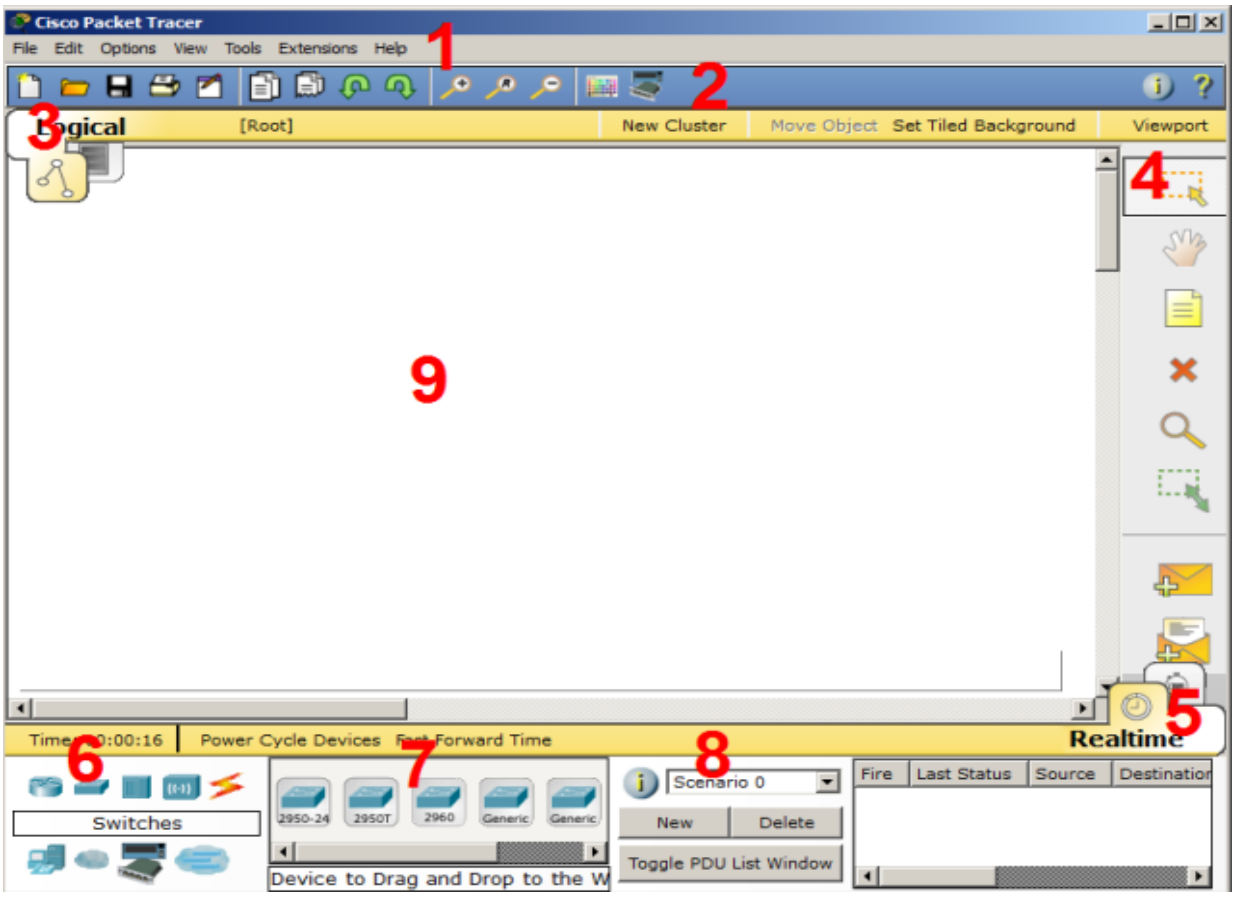

Рисунок 2.7 – Інтерфейс програми Cisco Packet Tracer

1) Головне меню програми з наступним змістом:

– Файл – містить операції відкриття / збереження документів;

– Виправлення – стандартні операції "копіювати / вирізати, скасувати / повторити";

– Налаштування - говорить сама за себе;

– Вид - масштаб робочої області і панелі інструментів;

– Інструменти - колірна палітра і кастомізація кінцевих пристроїв;

– Розширення - майстер проектів, розрахований на багато користувачів режим і кілька приблуд, які з CPT (так я іноді буду ласкаво називати Cisco Packet Tracer) можуть зробити цілу лабораторію;

– Допомога – містить інформацію про програму та містить посилання на додатки допомоги в використані програми;

2) Панель інструментів, частина яких просто дублює пункти меню;
3) Перемикач між логічного і зниження фізичної організацією;
4) Ще одна панель інструментів, містить інструменти виділення, видалення, переміщення, масштабування об'єктів, а так само формування довільних пакетів;
5) Перемикач між реальним режимом (Real-Time) і режимом симуляції;
6) Панель з групами кінцевих пристроїв і ліній зв'язку;
7) Самі кінцеві пристрої, тут містяться всілякі комутатори, вузли, точки доступу, провідники.
8) Панель створення призначених для користувача сценаріїв;
9) Робочий простір.

Симулятор Packet Tracer підтримує широкий діапазон мережевих з'єднань (таблиця 2.1). Кожен тип кабелю може бути з'єднаний лише з певним типом інтерфейсу.

Таблиця 2.1 – Типи кабелів в Cisco Packet Tracer

Тип кабелю	Описання
Консоль 	Консольне з'єднання може бути виконано між ПК і маршрутизаторами або комутаторами. Повинні бути виконані деякі вимоги для роботи консольного сеансу з ПК: швидкість з'єднань з обох сторін повинна бути однакова, має бути 7 біт даних (або 8 біт) для обох сторін, контроль парності повинен бути однаковий, має бути 1 або 2 степових бита (але вони не обов'язково повинні бути однаковими), а потік даних може бути чимось завгодно для обох сторін.
Мідний прямий 	Цей тип кабелю є стандартним середовищем передачі Ethernet для з'єднання пристроїв, який функціонує на різних рівнях OSI. Він повинен бути з'єднаний з наступними типами портів: мідний 10 Мбіт / с (Ethernet), мідний 100 Мбіт / с (Fast Ethernet) і мідний 1000 Мбіт / с (Gigabit Ethernet).

Мідний кросовер 	Цей тип кабелю є середовищем передачі Ethernet для з'єднання пристроїв, які функціонують на однакових рівнях OSI. Він може бути з'єднаний з наступними типами портів: мідний 10 Мбіт / с (Ethernet), мідний 100 Мбіт / с (Fast Ethernet) і мідний 1000 Мбіт / с (Gigabit Ethernet)
Оптика 	Оптоволоконне середовище використовується для з'єднання між оптичними портами (100 Мбіт / с або 1000 Мбіт / с).
Телефонний 	З'єднання через телефонну лінію може бути здійснено тільки між пристроями, що мають модемні порти. Стандартне подання модемного з'єднання – це кінцевий пристрій (Наприклад, ПК), додзвонюється в мережеве хмара.
Коаксиальний 	Коаксиальне середовище використовується для з'єднань між коаксіальними портами, такі як кабельний модем, з'єднаний з хмарою Packet Tracer.
Серійний DCE Серійний DTE	З'єднання через послідовні порти, часто використовуються для зв'язків WAN. Для настройки таких з'єднань необхідно встановити синхронізацію на стороні DCE-пристроїв. Синхронізація DTE виконується за вибором.

Packet Tracer є зручним засобом моделювання мереж передачі даних. Робота з симулятором дає вельми правдоподібне відчуття настройки реальної мережі, що складається з різних пристроїв. Налаштування мережевого обладнання можна проводити як за допомогою команд операційної системи Cisco IOS, так і за допомогою графічного інтерфейсу. Завдяки режиму симуляції можна простежити переміщення даних по мережі, поява і зміна параметрів пакетів при проходженні даних через мережеві пристрої, швидкість і шляхи переміщення пакетів. Аналіз подій, що відбуваються в мережі, дозволяє зрозуміти механізм її роботи і виявити несправності.

2.3. Обладнання, яке були застосовано в проекті Cisco Packet Tracer

2.3.1 Комутатори

Мережевий комутатор (рис. 2.8) – пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного або декількох сегментів мережі. Комутатор працює на канальному (другому) рівні моделі OSI. Комутатори були розроблені з використанням мостових технологій і часто розглядаються як багатопортові мости. Для з'єднання декількох мереж на основі мережевого рівня служать маршрутизатори.

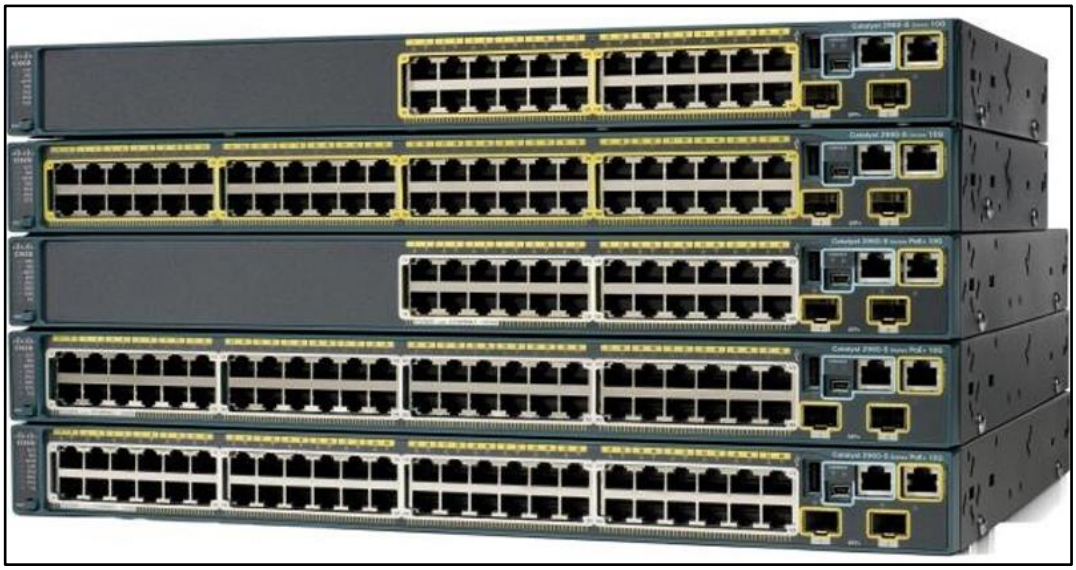

Рисунок 2.8 – Комутатор

Комутатор зберігає в пам'яті таблицю комутації (що зберігається в асоціативної пам'яті), в якій вказується відповідність MAC-адреси вузла порту комутатора. При включенні комутатора ця таблиця порожня, і він працює в режимі навчання. В цьому режимі надходять на якийсь порт дані передаються на всі інші порти комутатора. При цьому комутатор аналізує кадри (фрейми) і, визначивши MAC-адресу хоста-відправника, заносить його в таблицю на деякий час. Згодом, якщо на один з портів комутатора надійде

кадр, призначений для хоста, MAC-адресу якого вже є в таблиці, то цей кадр буде переданий тільки через порт, зазначений у таблиці. Якщо MAC-адресу хоста-одержувача не асоційований з яким-небудь портом комутатора, то кадр буде відправлений на всі порти, за винятком того порту, з якого він був отриманий. Згодом комутатор будує таблицю для всіх активних MAC-адрес, в результаті трафік локалізується. Варто відзначити малу латентність (затримку) і високу швидкість пересилки на кожному порту інтерфейсу.

Існує три способи комутації. Кожен з них – це комбінація таких параметрів, як час очікування і надійність передачі [5].

– З проміжним зберіганням (Store and Forward). Комутатор читає всю інформацію в кадрі, перевіряє його на відсутність помилок, вибирає порт комутації і після цього посилає в нього кадр.
– Наскрізний (cut-through). Комутатор зчитує в кадрі тільки адреса призначення і після виконує комутацію. Цей режим зменшує затримки при передачі, але в ньому немає методу виявлення помилок.
– Безфрагментний (fragment-free) або гібридний. Цей режим є модифікацією наскрізного режиму. Передача здійснюється після фільтрації фрагментів колізій (кадри розміром 64 байта обробляються за технологією store-and-forward, інші – за технологією cut-through).

Комутатори поділяються на керовані і некеровані (найбільш прості). Більш складні комутатори дозволяють управляти комутацією на мережевому (третьому) рівні моделі OSI. Зазвичай їх називають відповідно, наприклад Layer 3 Switch або просто, скорочено L3. Управління комутатором може здійснюватися за допомогою протоколу Web-інтерфейсу, SNMP, RMON (протокол, розроблений Cisco).

Багато керовані комутатори дозволяють виконувати додаткові функції: VLAN, QoS, агрегування, віддзеркалення. Складні комутатори можна поєднувати в один логічний пристрій – стек, з метою збільшення числа

портів (наприклад, можна об'єднати 4 комутатори з 24 портами і отримати логічний комутатор з (4 * 24-6 = 90) портами, або з 96-ю портами (якщо для стекування використовуються спеціальні порти).

2.3.2 Маршрутизатор

Маршрутизатор (рис. 2.9) – спеціалізований мережевий комп'ютер, який має мінімум два мережевих інтерфейсу і пересилає пакети даних між різними сегментами мережі, що приймає рішення про пересилку на підставі інформації про топологію мережі і певних правил, заданих адміністратором.

Рисунок 2.9 – Маршрутизатор

Маршрутизатор діляться на програмні і апаратні. Маршрутизатор працює на більш високому «мережевому» рівні 3 мережевий моделі OSI, ніж комутатор і мережевий міст, які працюють на 2 рівні і 1 рівні моделі OSI відповідно.

Зазвичай маршрутизатор використовує адресу одержувача, вказану в пакетних даних, і визначає по таблиці маршрутизації шлях, по якому слід передати дані. Якщо в таблиці маршрутизації для адреси немає описаного маршруту, пакет відкидається.

Існують і інші способи визначення маршруту пересилки пакетів, коли, наприклад, використовується адреса відправника, використовувані протоколи верхніх рівнів і інша інформація, що міститься в заголовках пакетів мережевого рівня. Нерідко маршрутизатори можуть здійснювати трансляцію адрес відправника і одержувача, фільтрацію транзитного потоку даних на основі певних правил з метою обмеження доступу, шифрування / розшифрування даних, що передаються.

Маршрутизатор допомагають зменшити завантаження мережі, завдяки її розділенню на домени колізій або широкомовні домени, а також завдяки фільтрації пакетів. В основному їх застосовують для об'єднання мереж різних типів, часто несумісних з архітектури і протоколів, наприклад для об'єднання локальних мереж Ethernet і WAN-з'єднань, що використовують протоколи xDSL, PPP, ATM, Frame relay. Нерідко маршрутизатор використовується для забезпечення доступу з локальної мережі в глобальну мережу Інтернет, здійснюючи функції трансляції адрес і міжмережевого екрану.

В якості маршрутизатора може виступати як спеціалізований (апаратне) пристрій, так і звичайний комп'ютер, що виконує функції маршрутизатора. Існує кілька пакетів програмного забезпечення (на основі ядра Linux, на основі операційних систем BSD) за допомогою якого можна перетворити ПК в високопродуктивний і багатофункціональний маршрутизатор, наприклад, Quagga, IPFW або простий в застосуванні PF.

Залежно від області застосування, маршрутизатори можна розділити на три класи:

– Верхній. У таких маршрутизаторів дуже високий рівень продуктивності. Вони застосовуються для створення і забезпечення мережі в крупних компаніях. Верхні маршрутизатори можуть

використовувати нестандартні інтерфейси і протоколи. Такі маршрутизатори можуть містити велику кількість портів для різних глобальних і локальних мереж.

– Середній. Застосовується для того, щоб створити мережу в невеликій організації або в окремій будівлі.
– Нижній. Такий маршрутизатор застосовується для створення локальної мережі в маленькому офісі або для використання в домашніх умовах. Нижній маршрутизатор має до 2 портів глобальної мережі і 4 порту локальної.

Існує всього 2 способи, якими можна підключити маршрутизатори до мережі. Він може підключатися дротовим або бездротовим способом. Теж саме відноситься і до можливості розподілу мережі по різних пристроїв.

У маршрутизатора, який підключається бездротовим способом, є невелика перевага. Він може здійснювати передачу інформації ще й за допомогою дротів. На даний момент за допомогою використання технологій бездротового підключення можуть передавати дані без застосування проводів більшість пристроїв. Більш старі версії обладнання не підтримують таку роботу і для них необхідно використовувати дроти. За допомогою бездротового роутера можна об'єднати різні пристрої в одну загальну мережу з можливістю доступу в інтернет.

Дротовий маршрутизатор обов'язково підключається до кожного пристрою, яке знаходиться в мережі. Провідні маршрутизатори використовуються для мережі, в якій є не більше 8 пристроїв. При цьому ці пристрої повинні перебувати постійно на одному і тому ж місці. За допомогою проводового підключення можна легко досягти доступу між всіма учасниками цієї мережі. При такому підключенні з одного пристрою можна отримати дані іншого.

По областях застосування маршрутизатори діляться на кілька класів.

– Магістральні маршрутизатори (backbone routers) призначені для побудови центральної мережі корпорації. Центральна мережа може

складатися з великої кількості локальних мереж, розкиданих по різних будівель і використовують найрізноманітніші мережеві технології, типи комп'ютерів і операційних систем. Магістральні маршрутизатори – це найбільш потужні пристрої, здатні обробляти кілька сотень тисяч або навіть кілька мільйонів пакетів в секунду, які мають велику кількість інтерфейсів локальних і глобальних мереж.

– Маршрутизатор регіональних відділень сполучають регіональні відділення між собою і з центральною мережею. Мережа регіонального відділення, так само як і центральна мережа, може складатися з декількох локальних мереж. Такий маршрутизатор зазвичай є деякою спрощену версію магістрального маршрутизатора.
– Маршрутизатор віддалених офісів з'єднують, як правило, єдину локальну мережу віддаленого офісу з центральною мережею або мережею регіонального відділення по глобальної зв'язку. У максимальному варіанті такі маршрутизатори можуть підтримувати і два інтерфейси локальних мереж. Як правило, інтерфейс локальної мережі – це Ethernet 10 Мбіт / с, а інтерфейс глобальної мережі – виділена лінія зі швидкістю 64 Кбіт / с, 1,544 або 2 Мбіт / с. Маршрутизатор віддаленого офісу може підтримувати роботу віддаленого підключення в якості резервної зв'язку для виділеного каналу.
– Маршрутизатор локальних мереж (комутатори 3-го рівня) призначені для поділу великих локальних мереж на підмережі. Основна вимога до них – висока швидкість маршрутизації, так як в такій конфігурації відсутні низько-швидкісні порти, такі як модемні порти 33,6 Кбіт / с або цифрові порти 64 Кбіт / с.

Залежно від області застосування маршрутизатори мають різні основними і додатковими технічними характеристиками.

2.3.3 Сервер

Сервер (рис. 2.10) – це апаратно-програмний комплекс в локальній мережі, здатний регулювати роботу всіх призначених для користувача комп'ютерів.

Рисунок 2.10 – Сервер Cisco UCS S3260

В основі апаратної частини сервера лежить потужний комп'ютер з високою продуктивністю, багатозадачністю і найкращою оптимізацією для швидкої обробки команд від клієнтських ПК. Такий сервер повинен бути багатоядерним, відмовостійким, з гарячою заміною свого обладнання (hotswap) тобто завжди на «ходу». Чого не можна сказати про клієнтські комп'ютери, які частіше потребують ремонту через знос запчастин.

Основні функції сервера локальної мережі можна класифікувати на:

1) Файловий сервер – це одна з ключових ролей кожного сервера. Локальна мережа з файловим сервером забезпечує користувачам необмежений доступ до будь-яких зберігаються на центральному

комп'ютері файлів, а також управління директоріями. Ключова особливість сервера полягає в управлінні типом доступу до файлів: він може призначити загальний доступ до папок або персональний доступ в свою робочу директорію для кожного користувача.

2) Термінальний сервер – це сервер, який надає користувачам мережі свої обчислювальні ресурси. На практиці використання такого сервера часто носить бюджетний характер, оскільки на сервері можна запускати необхідне для роботи ліцензійне ПЗ. Кожен користувач на своєму комп'ютері використовує встановлений клієнт RDP (Remote Desktop Protocol) – протокол віддаленого робочого стола. При коректної установки зв'язку з термінальним сервером користувач бачить вміст робочого столу з необхідними програмами і працює віддалено, використовуючи обчислювальні ресурси сервера, тобто без навантаження на свій комп'ютер. Переваги термінального сервера полягають в зниженні витрат електроенергії, зменшення витрат на програмне забезпечення та підвищення безпеки методом обмеженого робочого місця користувача.
3) Сервер друку необхідний для колективної роботи з принтером або факсом. Даний метод має на увазі віддалену друк на пристрої, не підключеному до вашого робочого місця. Сервер друку може обробляти багатопотокових операції, а також забезпечувати друк інформації від декількох комп'ютерів без «простою».

   Крім того, розташування всіх друкуючих пристроїв в одній кімнаті значно спрощує офісну роботу. Знаючи IP-адреса сервера можна вибрати загальнодоступне пристрій друку для локальної мережі (або віддаленої групи користувачів).

   Також управління печаткою на сервері дозволяє відстежувати обробник завдань друку, який реєструє в журналі кількість роздрукованого паперу.

4) Сервер бази даних – відповідає за цілісність і збереження sql-даних. Робота з даними відбувається у вигляді обробки sql-запитів від користувача безпосередньо до бази даних. Такий набір обробки правил працює з таблицями, секціями, звітами і формулами. Клієнт-користувач, підключаючись до бази даних, використовує обчислювальну потужність сервера. Прикладом такого сервера бази даних може служити комп'ютер з таким поширеним ПО, як: 1С-підприємство, Парус-Бухгалтерія, моніторинг мережі cmysql та багато інших.
5) Веб-сервер – це сервер, робота якого полягає на інформаційному обміні між користувачами не тільки в локальній мережі, але і в мережі Інтернет. Сервер зберігає всі ресурси веб-сайту, верстки сторінок, шаблонів-стилів, виконуваних скриптів, html-документів. Функції сервера локальної мережі полягають в прийомі / відправлення http - пакетів з необхідної користувачеві інформацією. Такий сервер для локальної мережі може реалізувати відеохостинг, трансляцію конференцій, мультимедіа, інформаційний портал, публікації документів. Веб-сервер багатогранний. Можна задіяти до нього СУБД (mysql-web), моніторинг локальної мережі (mrtg, cacti, nagios), проксі-сервер на веб (nginx) і багато інших корисних в роботі програм.
6) Поштовий сервер – призначений для зберігання листів і обміну текстовою інформацією між користувачами мережі. Також функції сервера електронної пошти поширюються на зберігання адрес («ящиків») всіх користувачів мережі, обміну кореспонденцією між ними, відправки звітів, участі в групах розсилки, а також створення календарних проектів для особистих зустрічей.

2.3.4 Точка доступу Wi-Fi

Точка доступу – це бездротова базова станція (рис. 2.11), призначена для забезпечення бездротового доступу до вже існуючої мережі (безпроводовий або провідний) або створення абсолютно нової бездротової мережі. Бездротовий зв'язок здійснюється за допомогою технології Wi-Fi.

Рисунок 2.11 – Точка доступу Wi-Fi Cisco Air-CAP3702E

Бездротові мережі з декількох точок доступу встановлюються у великих офісних приміщеннях, будівлях і на інших великих об'єктах, в основному для того, щоб створити одну бездротову локальну мережу (WLAN). До кожної точки доступу можна підключити до 254 клієнтських комп'ютерів. У більшості випадків недоцільно підключати до однієї точки доступу більше 10 комп'ютерів, тому що швидкість передачі даних на кожного користувача розподіляється в рівних пропорціях і чим більше в однієї точки доступу «клієнтів», тим менше швидкість у кожного з них.

При побудові територіально розподілених мереж або бездротових мереж в будинках, точки доступу об'єднуються в одну загальну мережу через

радіоканал або локальну мережу (дротову). При цьому користувач може вільно переміщатися зі своїм мобільним пристроєм в радіусі дії цієї мережі

Точка доступу аналогічна за своїм устроєм з бездротовим роутером (бездротового маршрутизатора). Бездротові роутери використовуються для створення окремого сегмента мережі і підтримують підключення до них всіх комп'ютерів з вбудованими бездротовими мережевими адаптерами. На відміну від точки доступу в бездротової роутер інтегрований мережевий перемикач (світч), для того щоб до нього могли додатково підключатися клієнти по протоколу Ethernet або для підключення інших маршрутизаторів при створенні мережі з декількох бездротових роутерів. Крім того, бездротові роутери мають вбудований брандмауер, який запобігає небажане вторгнення в мережу зловмисників. В іншому ж, бездротові роутери схожі по влаштуванню з точками доступу.

Існує три основні режими роботи точки доступу:

– "точка доступу"

У новому обладнанні режим «точка доступу» встановлено за умовчанням. В цьому режимі користувач підключається зі свого комп'ютера, оснащеного Wi-Fi адаптером, до бездротової мережі точки доступу. У більшості випадків для роботи в цьому режимі специфічні настройки не потрібні.

– «Повторювач»

В даному режимі точка доступу працює як приймально-передавач або «повторювач». Вона приймає слабкий сигнал від іншої точки доступу і, посилюючи його, передає на цій же частоті далі до необхідного адресата.

– «Міст»

В цьому режимі точка доступу об'єднує фізично віддалені сегменти мережі в одне ціле. Використовується при побудові «лінків» або, іншими словами, забезпечення зв'язку між віддаленими об'єктами.

3 РОЗРОБКА МОДЕЛІ КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ ПІДПРИЄМСТВА

При детальному аналізі існуючих програм в другому розділі, було вирішено розроблювати комп'ютерну мережу в середовищі моделювання Cisco Packet Tracer.

3.1 Побудова моделі захищеної комп'ютерної мережі

Комп'ютерна мережа організації складається з (рис. 3.1): 3 маршрутизаторів, 6 комутаторів, 3 сервера, 3 точки доступу Wi-Fi.

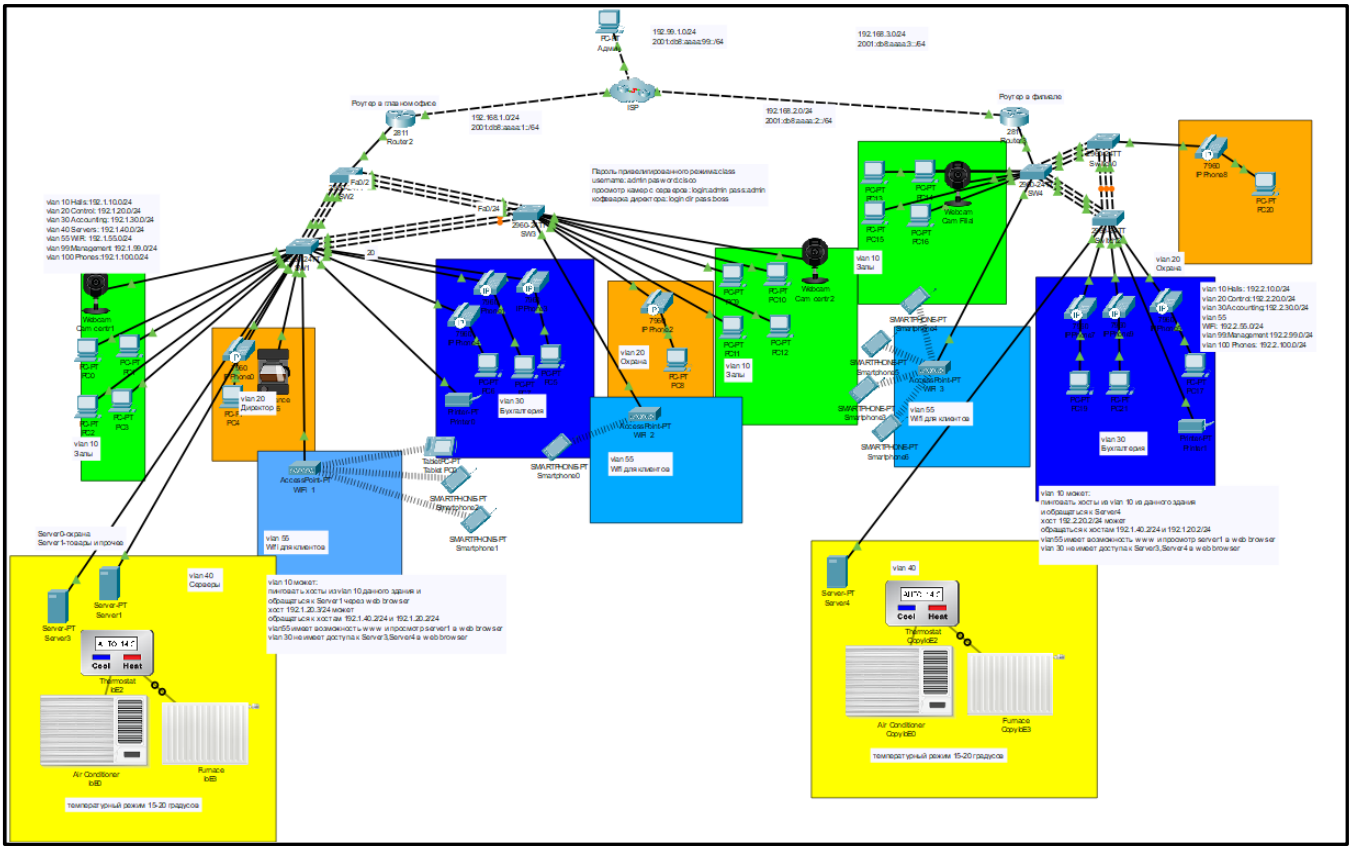

Рисунок 3.1 – Модель захищеної комп'ютерної мережі в програмі Cisco Packet Tracer

- Маршрутизатори забезпечують маршрутизацію пакетів між різними фізичними мережами, вихід в інтернет, а також віддалений доступ для адміністратора.
- Комутатори працюють на рівнях "доступу" і "розподілу", вони комутують пакети між користувачами як з однієї підмережі VLAN, так і з різних.
- Сервер являє собою високопродуктивну робочу станцію і настроюється під потреби користувачів організації. Він може представлятись як файлове сховище, центр обробки даних, DHCP-сервер, сервер камер відеоспостереження.
- Точка доступу Wi-Fi використовує ЕМВ певної частоти, щоб надати користувачам доступ в локальну мережу.

3.1.1 Опис підприємства, для якого будується комп'ютерна мережа

Проектом захищеної комп'ютерної мережі виступає – "Магазин побутової техніки та електроніки".

Передбачається, що у організації є головний офіс та одна філія.

В головному офісі розташовується:

- два робочих кабінети по чотири комп'ютери та по одній IP-камері;
- кабінет бухгалтерії з трьома комп'ютерами та трьома IP-телефонами;
- кабінет охорони з одним комп'ютером та одним IP-телефоном;
- кабінет директора має один комп'ютер, один IP-телефон та кавову машину;
- серверна кімната з двома серверами (перший сервер призначений для охорони, другий для бази даних клієнтів та товарів) та з контролем температури в проміжку 15-20 градусів.

В філіалі розташовується:

- робочій кабінет з чотирма комп’ютерами та з однією IP-камерою;
- кабінет бухгалтерії з трьома комп’ютерами та трьома IP-телефонами;
- кабінет охорони з одним комп’ютером та одним IP-телефоном;
- серверна кімната з одним сервером та з контролем температури в проміжку 15-20 градусів.

Корпоративна мережа для даного підприємства є розподіленою мережею. Вона включає в себе високу пропуску здатність, має IP телефонію, а також високий ступінь захищеності.

3.1.2 Розбиття локальної мережі на віртуальні локальні підмережі VLAN

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.

Дана технологія дозволяє гнучко налаштувати використання мережевих ресурсів в залежності від завдань користувачів конкретного VLAN'a.

3.1.3 Маршрутизація між мережами VLAN

При введенні VLAN необхідно налаштувати маршрутизацію, щоб користувачі з різних підмереж могли взаємодіяти один з одним. В даному бюджетному рішенні застосовується статична маршрутизація, що підходить для малих підприємств, у яких рідко з'являються і / або видаляються пристрої.

Статична маршрутизація – це вид маршрутизації, при якому маршрути вказуються в явному вигляді при конфігурації маршрутизатора.

При установці статичного маршруту вказується:

– Адреса мережі (на яку маршрутизується трафік), маска мережі;
– Адреса шлюзу (вузла), який сприяє подальшій маршрутизації (або підключений до маршрутизації мережі безпосередньо).

3.1.4 Динамічна маршрутизація між мережами

Маршрутизація – процес визначення кращого шляху, по якому пакет може бути доставлений одержувачу. Вибір протоколу маршрутизації стає актуальним на середніх і великих підприємствах, адже неправильна конфігурація може позначитися на якості обслуговування.

Для забезпечення узгодженості дій всіх маршрутизаторів в мережі, мінімізації помилок і спрощення роботи адміністратора застосовуються мережеві протоколи маршрутизації, які регламентують вибір найбільш оптимального маршруту слідування пакету даних в мережах.

Розрізняють два види маршрутизації: програмна та апаратна.

– Програмна маршрутизація – це спеціалізоване програмне забезпечення, встановлене на комп'ютері з кількома мережевими інтерфейсами, які входять до складу різних мереж.
– Апаратна маршрутизація здійснюється спеціальним обладнанням, здатним аналізувати і перенаправляти вхідні потоки даних.

Динамічна маршрутизація – вид маршрутизації, при якому таблиця маршрутизації редагується програмно.

Демони маршрутизації обмінюються між собою інформацією, яка дозволяє їм заповнити таблицю маршрутизації найбільш оптимальними маршрутами. Протоколи, за допомогою яких проводиться обмін інформацією між демонами, називаються протоколами динамічної маршрутизації.

Кожен протокол маршрутизації працює з пакетами даних, які відносяться до одного з існуючих протоколів. У процесі обробки інформації протокол визначає формат пакета даних, виділяє адресу одержувача і будує маршрут подальшого проходження сигналу.

В даному бюджетному рішенні застосовується протокол EIGRP (Enhanced Interior Gateway Routing Protocol) – вдосконалений дистанційно-векторний протокол динамічної маршрутизації, розроблений компанією Cisco динамічний протокол маршрутизації.

EIGRP має безліч переваг в порівнянні з протоколом RIP (Routing Information Protocol) і своїм безпосереднім попередником, протоколом IGRP (Interior Gateway Routing Protocol). По суті, EIGRP це розширена версія протоколу IGRP. Як і RIP, IGRP відомий як дистанційно-векторний протокол, але в порівнянні з ним він має поліпшені характеристики алгоритму розрахунку оптимального шляху до пункту призначення.

Метрики IGRP ґрунтуються на таких параметрах як смуга пропускання і затримка, в той же час для протоколу RIP важливим є довга маршруту, виражена в «хопах», тобто кількості вузлів на шляху прямування.

Основними перевагами EIGRP є:

– низьке споживання мережевих ресурсів в режимі нормальної експлуатації (в умовах стабільної мережі передаються тільки пакети "hello")
– при виникненні змін по мережі передаються тільки зміни, що відбулися в маршрутної таблиці, а не вся таблиця цілком. Це дозволяє зменшити навантаження на мережу, створювану протоколом маршрутизації
– малий час конвергенції в разі зміни в топології мережі (в окремих випадках збіжність забезпечується майже миттєво).

3.1.5 Налаштування розширених списків контролю доступу ACL

Списки контролю доступу є список правил для обробки мережевого пакету, який визначає необхідні дії для його обробки. Списки контролю доступу корисні для фільтрації, приорітизації інформації, а також для її вибіркової обробки в залежності від необхідності. Перевага розширених ACL полягає в тому, що вони можуть перевіряти адреси джерел, а також адреси отримувачів, в разі IP ще тип протоколу і TCP / UDP порти, а не тільки адреси джерел

3.1.6 Налаштування зв'язку між філіями

Проводиться об'єднання кількох філій в рамках одного міста в масштабну локальну мережу (рис. 3.2) – WAN. Для забезпечення надійності також налаштовується резервний канал зв'язку між філіями.

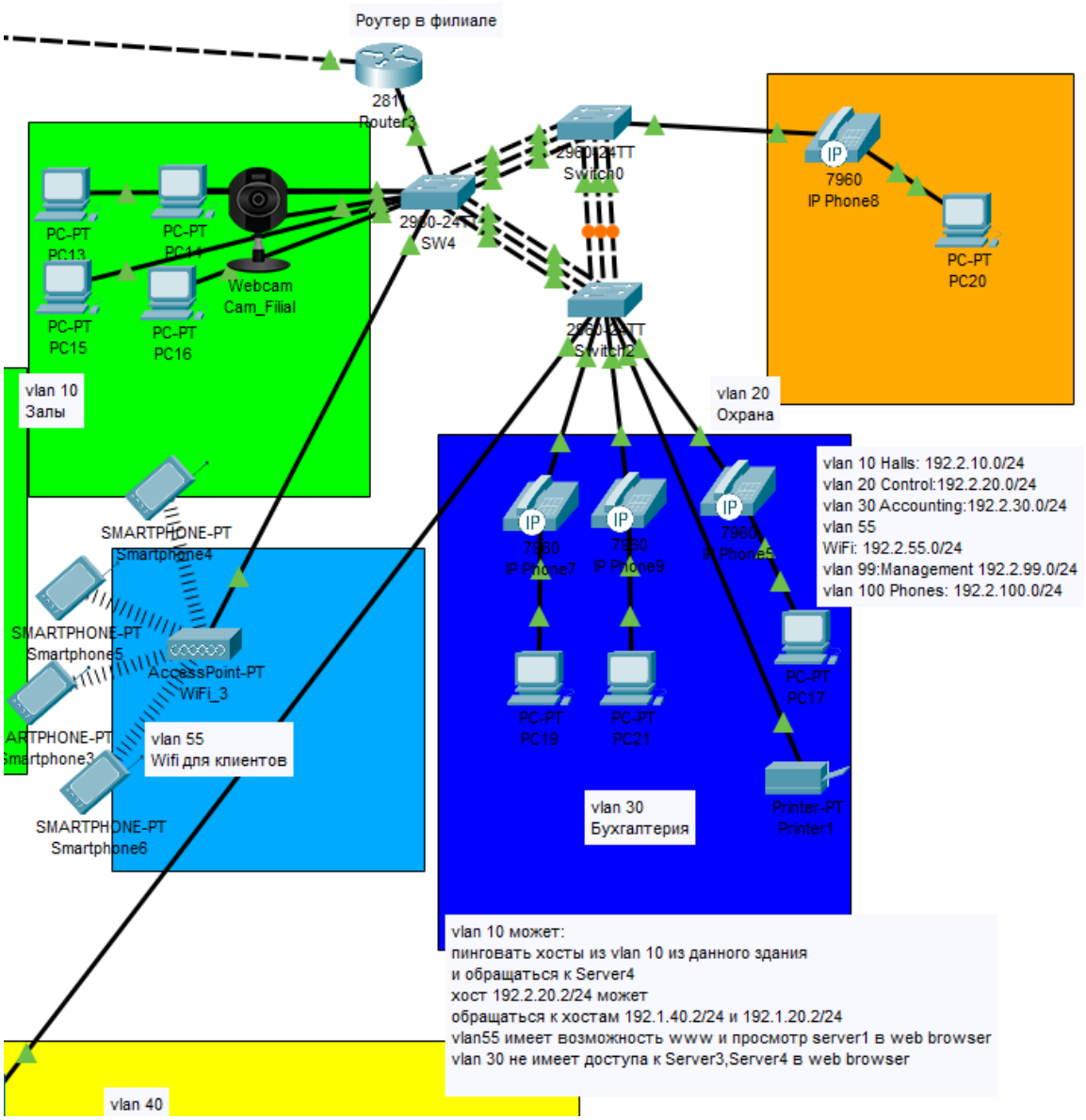

Рисунок 3.2 – Налаштування зв'язку між філіями

3.1.7 IP-телефонія

IP-телефонія (або VoIP – Voice over Internet protocol) – технологія (рисунок), яка використовує мережу з пакетною комутацією повідомлень на базі протоколу IP для передачі голосу в режимі реального часу (рис. 3.3).

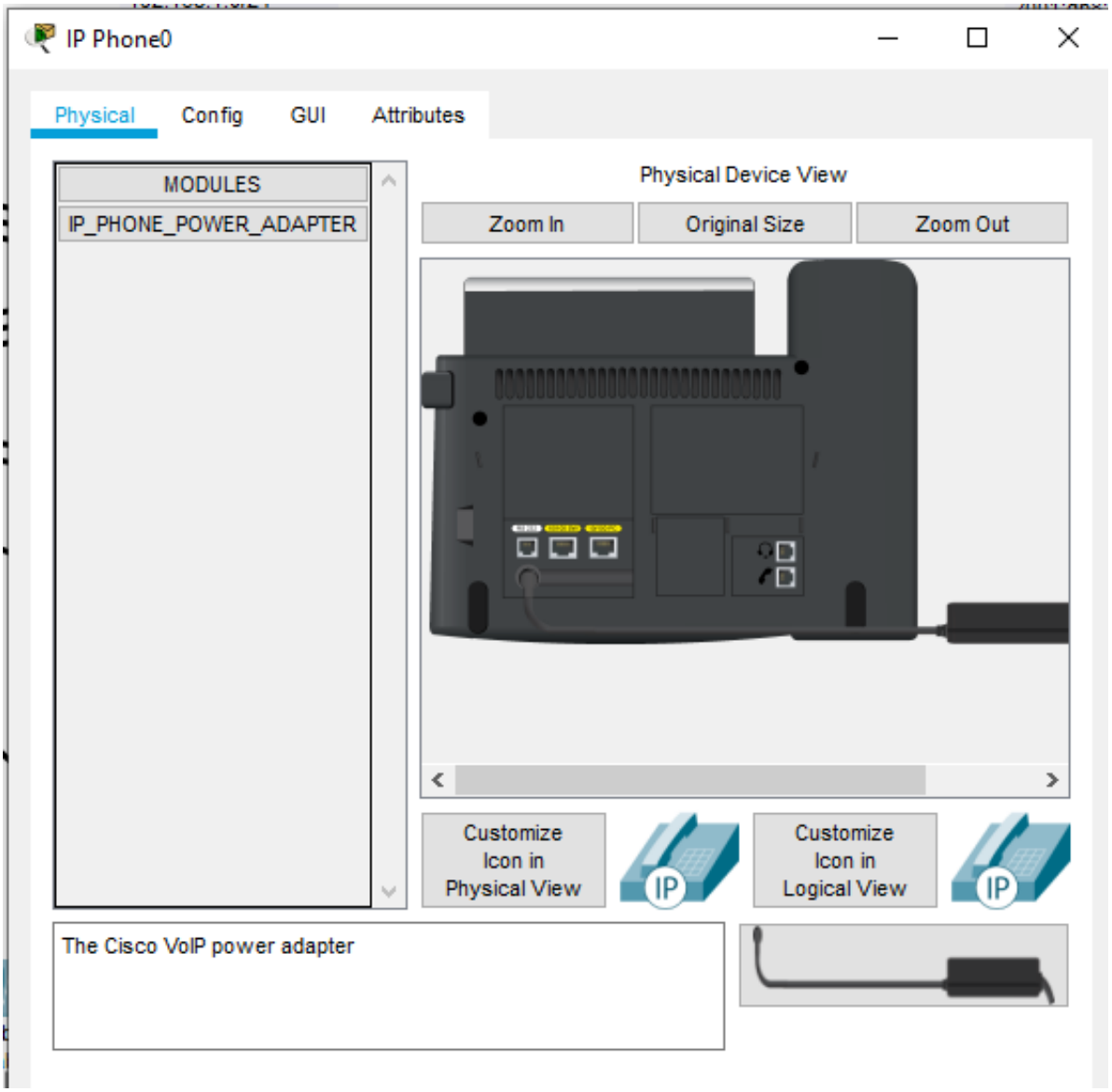

Рисунок 3.3 – Вигляд IP-телефонії в Cisco Packet Tracer

При розмові наші голосові сигнали перетворюються в пакети даних, які потім стискаються. Далі ці пакети даних посилаються через Інтернет приймальній стороні. Коли пакети даних досягають адресата, вони декодуються в аналоговий голосовий сигнал.

IP-телефонія в чистому вигляді може застосовуватися в якості ліній передачі голосу, для чого можуть використовуватися спеціально виділені цифрові канали.

На відміну від аналогової телефонії, IP-телефонія створює "підключення по запиту" і не має зарезервованих ліній зв'язку, що зменшує витрати на телефонні розмови.

Переваги, особливості та підтримувані функції:

- Передача голосового та факсимільного трафіку через IP. Як транспорт можуть використовуватися будь-які середовища (виділені лінії, ISDN, Frame Relay, Ethernet, Token Ring, ATM)
- Рішення засновані на єдиній лінії маршрутизаторів Cisco і не вимагають додаткового апаратного забезпечення
- Модульна, нарощувана архітектура
- Передача голосу і факсів через один порт
- Сумісність зі стандартом H.323
- Висока продуктивність, заснована на використанні DSP (цифрових сигнальних процесорів)
- Підтримка протоколів компресії голосу G.729 і G.711, дозволяє передавати один голосовий канал зі швидкістю 8 kbps
- Висока якість голосових з'єднань засноване на використанні RSVP архітектури і черг з пріоритетами
- Придушення пауз
- Симуляція шумів в лінії
- Розвинуте управління планом внутрішньої нумерації і відображенням IP-адрес на цей план
- Підтримка DTMF
- Підтримка протоколу T.30. (Передача факсів)
- Виділена телефонна лінія (наскрізне з'єднання)

При звичайному способі передачі мови (аналогової телефонії) використовується канал пропускною спроможністю 64 Кбіт / с незалежно від того, розмовляє абонент або мовчить під час з'єднання. У разі передачі мови по IP-мереж, за рахунок оцифровки і компресії (стиснення), мова передається у вигляді цифрової інформації, причому якщо абонент мовчить або робить

паузи в розмові, цифрова інформація в канал не передається і канал не заповнюється. Це дозволяє в одному каналі 64 Кбіт / с передавати від 8 і більше з'єднань одночасно, що в свою чергу забезпечує зниження тарифів, і, відповідно, оплата зменшується.

3.2 Налаштування протоколів захисту

3.2.1 Налаштування віддаленого доступу адміністратора по протоколу SSHv2

У разі неполадок в мережі адміністратора не обов'язково знаходиться поруч з обладнанням – ви можете надати йому віддалений доступ з безпечного протоколу SSHv2

3.2.2 Налаштування протоколу DHCP

DHCP – протокол прикладного рівня моделі TCP / IP, служить для призначення IP-адреси клієнта. Це випливає з його назви – Dynamic Host Configuration Protocol. IP-адресу можна призначати вручну кожного клієнта, тобто комп'ютера в локальній мережі. Але у великих мережах це дуже трудомісткий, до того ж, чим більше локальна мережа, тим вище зростає ймовірність помилки при налаштуванні. Тому для автоматизації призначення IP був створений протокол DHCP.

Протокол DHCP дозволяє здійснювати автоматичну настройку мережевих пристроїв. Налаштування DHCP сервера на маршрутизаторі вигідна тим, що дозволяє по максимум задіяти працює маршрутизатор, повісивши на нього максимальну кількість функціоналу (інтернет, NAT, DHCP і т.п.). DCHP дозволить маршрутизатора автоматично налаштовувати на клієнтах наступні основні параметри:

- IP адреса;
- Основний шлюз;
- Маска підмережі;
- DNS сервера;
- ім'я домену.

Робота протоколу DHCP здійснюється за принципом клієнт-сервер. Для отримання налаштувань використовується схема DORA (Discover-Offer-Request-Acknowledge). Сам процес складається з наступних етапів:

- Виявлення (Discover). Після підключення клієнта починається процес його ініціалізації в мережі. Він знаходить відповідний DHCP-сервер шляхом відправки спеціального запиту DHCPDISCOVER на адресу 255.255.255.255. З огляду на відсутність власного IP, в такому запиті вказується 0.0.0.0 і MAC. Запит надходить на всі ПК у відповідному сегменті мережі. При цьому відповідь на нього автоматично відправляється тільки DHCP-серверами.
- Пропозиція (Offer). Отримавши від клієнта запит, DHCP-сервер здійснює його обробку і виконує підбір мережеву конфігурацію. Ця конфігурація направляється клієнту прийде в повідомленні DHCPOFFER, яке, як правило, передається на вказаний MAC. Однак в деяких випадках застосовується широкомовлення. При знаходженні декількох серверів в межах мережі клієнтові приходить відповідну кількість DHCPOFFER, з яких він вибирає один (зазвичай перший за часом отримання).
- Запит (Request). Після отримання DHCPOFFER клієнт передає серверу спеціальне повідомлення DHCPREQUEST, яке містить запит налаштувань. У цьому запиті дублюється інформація з DHCPDISCOVER, а також вказує IP-адреса обраного на попередньому етапі DHCP-сервера.

– Підтвердження (Acknowledge). Після отримання DHCPREQUEST обраний DHCP-сервер виконує фіксацію відповідної прив'язки для клієнта і направляє йому у відповідь повідомлення DHCPACK. У ньому підтверджуються надані автоматично настройки. Це повідомлення передається на адресу MAC клієнта, яка була вказана на попередньому етапі. Отримавши DHCPACK, клієнт проводить автоматичну перевірку наданих налаштувань і застосовує конфігурацію мережі, отриману від сервера.

3.2.3 Налаштування протоколу NAT

Мережі зазвичай проектуються з використанням приватних IP адрес. Це адреси 10.0.0.0/8, 172.16.0.0/12 і 192.168.0.0/16. Ці приватні адреси використовуються всередині організації або майданчика, щоб дозволити пристроям спілкуватися локально, і вони не маршрутизуються в інтернеті. Щоб дозволити пристрою з приватним IPv4-адресою звертатися до пристроїв і ресурсів за межами локальної мережі, приватний адресу спочатку повинен бути переведений на загальнодоступний публічний адресу.

І ось якраз NAT переводить приватні адреси, в загальнодоступні. Це дозволяє пристрою з приватною адресою IPv4 звертатися до ресурсів за межами його приватної мережі. NAT в поєднанні з приватними адресами IPv4 виявився корисним методом збереження загальнодоступних IPv4-адрес. Один загальнодоступний IPv4-адрес може бути використаний сотнями, навіть тисячами пристроїв, кожен з яких має приватний IPv4-адрес. NAT має додаткову перевагу, що полягає в додаванні ступеня конфіденційності і безпеки в мережу, оскільки він приховує внутрішні IPv4-адреси з зовнішніх мереж.

Маршрутизатор з підтримкою NAT можуть бути налаштовані з одним або декількома дійсними загальнодоступними IPv4-адресами. Ці

загальнодоступні адреси називаються пулом NAT. Коли пристрій з внутрішньої мережі відправляє трафік з мережі назовні, то маршрутизатор з підтримкою NAT переводить внутрішній IPv4-адрес пристрою на загальнодоступний адреса з пулу NAT. Для зовнішніх пристроїв весь трафік, що входить і виходить з мережі, виглядає мають загальнодоступний IPv4 адресу.

3.2.4 Налаштування обладнання на протоколі IPv4 та IPv6

Налаштоване обладнання для адресації по протоколам IPv4, а також по більш сучасному IPv6.

Основна зовнішня відмінність четвертої і шостої версії протоколу – структура IP-адреси. IPv4 використовує чотири однобайтових десяткових числа, між якими ставиться крапка (172.268.0.1). IPv6 – шістнадцяткові числа, розділені двокрапкою (fe70 :: d5a9: 4521: d1d7: d8f4b11) [4].

3.2.5 Налаштування протоколу STP (зокрема, Rapid STP і PVST)

STP (Spanning Tree Protocol) – мережевий протокол (або сімейство мережевих протоколів) призначений для автоматичного видалення циклів (петель комутації) з топології мережі на канальному рівні в Ethernet-мережах (рис. 3.4).

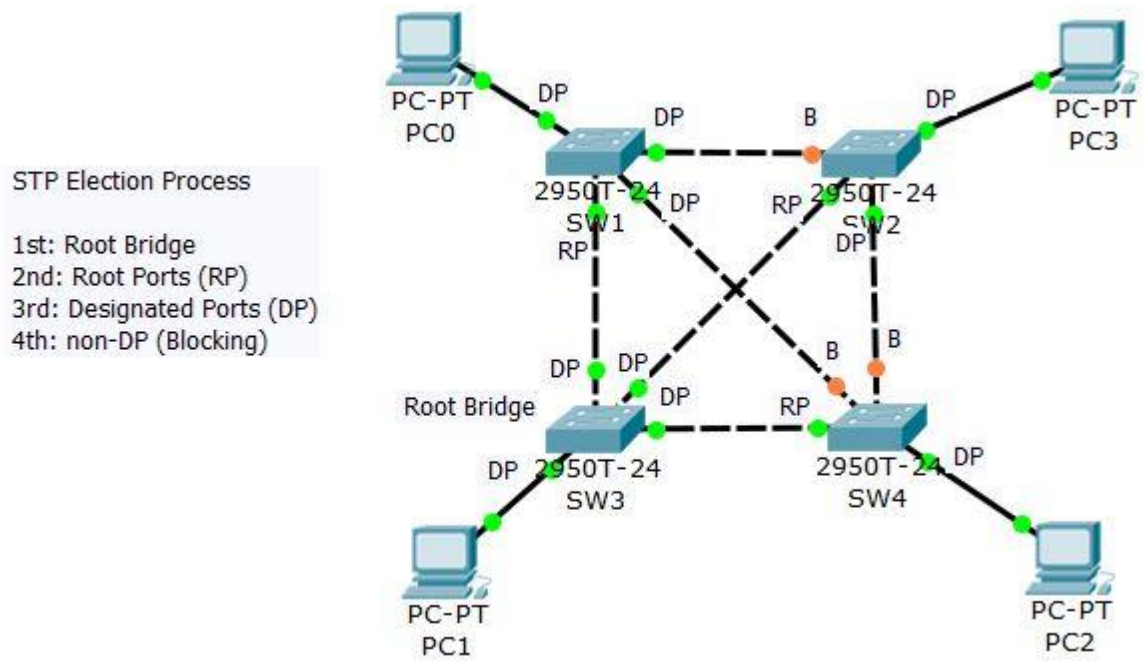

Рисунок 3.4 – Алгоритм дії протоколу STP

Алгоритм дії STP:

– Після включення комутаторів в мережу, за замовчуванням кожен комутатор вважає себе кореневим (root).
– Кожен комутатор починає посилати по всіх портах конфігураційні Hello BPDU пакети раз в 2 секунди, максимальний проміжок 20 секунд.
– Якщо міст отримує BPDU з ідентифікатором моста (Bridge ID) меншим, ніж свій власний, він припиняє генерувати свої BPDU і починає ретранслювати BPDU з цим ідентифікатором. Таким чином в кінці кінців в цій мережі Ethernet залишається тільки один міст, який продовжує генерувати і передавати власні BPDU. Він і стає кореневим мостом (root bridge).
– Решта мости ретранслюють BPDU кореневого моста, додаючи в них власний ідентифікатор і збільшуючи лічильник вартості шляху (path cost).

– Для кожного сегмента мережі, до якого приєднані два і більше портів мостів, відбувається визначення designated port – порту, через який BPDU, що приходять від кореневого моста, потрапляють в цей сегмент.
– Після цього всі порти в сегментах, до яких приєднані 2 і більше портів моста, блокуються за винятком root port і designated port.
– Кореневої міст продовжує посилати свої Hello BPDU раз в 2 секунди.

RSTP або як його ще називають у більш розгорнутому вигляді Rapid spanning tree protocol, по суті той же STP але більш швидкий де час збіжності мить, ви втратите один пакет. Включити RSTP можна командою з режимі глобального конфігурування, де потрібно змінити режим на rapid-pvst.

3.2.6 Налаштування протоколу EtherChannel

Etherchannel (рис. 3.5) – це технологія, що дозволяє об'єднувати (агрегувати) кілька фізичних проводів (каналів, портів) в єдиний логічний інтерфейс. Як правило, це використовується для підвищення відмовостійкості і збільшення пропускної здатності каналу. Зазвичай, для з'єднання критично важливих вузлів (комутатор-комутатор, комутатор-сервер).

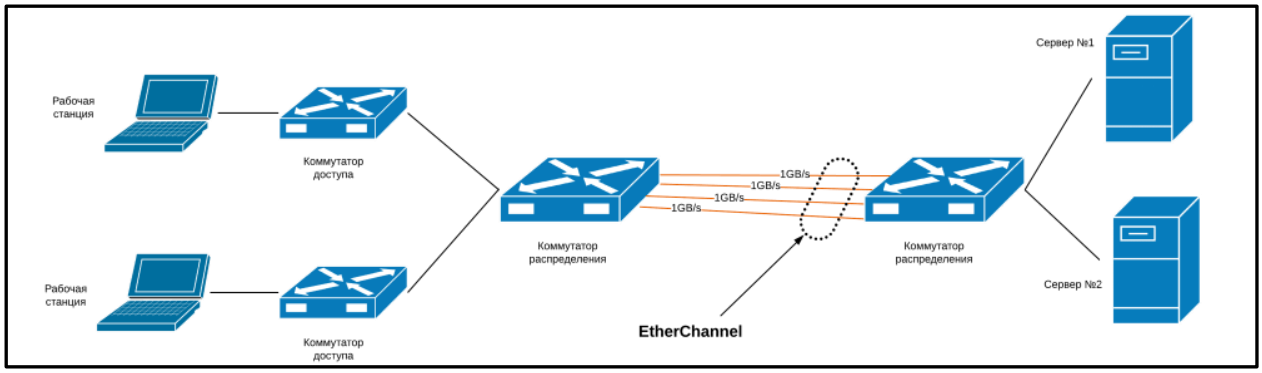

Рисунок 3.5 – Налаштування протоколу EtherChannel

Технологія EtherChannel має багато переваг.

– Більшість завдань конфігурації виконується на інтерфейсі EtherChannel, а не на окремих портах. Це забезпечує узгоджену конфігурацію на всіх каналах.
– EtherChannel використовує існуючі порти комутатора. Для забезпечення більш високої пропускної здатності не потрібно дорога заміна каналу на більш швидкий.
– Між каналами, які є частиною одного і того ж EtherChannel, відбувається розподіл навантаження. Залежно від використовуваного обладнання може бути реалізований один або кілька методів балансування навантаження.
– EtherChannel створює об'єднання, яке розглядається, як один логічний канал. Якщо між двома комутаторами існує декілька об'єднань EtherChannel, протокол STP може блокувати одне з об'єднань щоб уникнути петель комутації.
– EtherChannel надає функції надмірності, оскільки загальний канал вважається одним логічним з'єднанням. Крім того, втрата одного фізичного з'єднання в межах каналу не призводить до зміни в топології. Тому перерахунок дерева найкоротших шляхів не потрібно.
– EtherChannel продовжує працювати навіть в тому випадку, якщо загальна пропускна здатність знижується через втрати з'єднання в межах EtherChannel

3.2.7 Налаштування протоколу SSHv2

SSH або Secure Shell (безпечна оболонка) – мережевий протокол прикладного рівня, що дозволяє виробляти віддалене управління

операційною системою і тунелювання TCP-з'єднань (наприклад, для передачі файлів).

SSH робить віддалене управління операційною системою безпечним, так як шифрує весь трафік, включаючи і передаються паролі. При цьому можливий вибір різних алгоритмів шифрування.

Крім віддаленого управління, SSH дозволяє безпечно передавати в незахищеній середовищі практично будь-який мережевий протокол. Таким чином, можна не тільки віддалено працювати на комп'ютері через командну оболонку, але і передавати по шифрованому каналу звуковий потік або відео (наприклад, з веб-камери), виробляти роботу з базами даних та іншими сховищами, а також використовувати будь-які інші протоколи. Також SSH може використовувати стиснення переданих даних для подальшого їх шифрування, що зручно для віддаленого запуску клієнтів X Window System.

Захист SSH базується на досить простих правилах, дотримання яких істотно знижує ризик злому:

- Заборона віддаленого root-доступу за паролем.
- Заборона підключення з порожнім паролем або відключення входу по паролю (використання ключів).
- Вибір нестандартного порту для SSH-сервера (стандартний – 22).
- Використання довгих SSH2 RSA-ключів (2048 біт і більше) для аутентифікації.
- Обмеження списку IP-адрес, з яких дозволений доступ (наприклад, блокуванням порту на рівні брандмауера).
- Відмова від використання поширених або широко відомих системних логінів для доступу по SSH.
- Блокування спроб перебору паролів (бан по IP, наприклад)
- Регулярний перегляд повідомлень про помилки аутентифікації.
- Установка систем виявлення вторгнень (IDS).
- Використання пасток, що підроблюють SSH-сервіс (honeypot).

3.3 Додаткові елементи мережі

3.3.1 Елементи розумного будинку

Налаштування програмованих датчиків температури і вологості для забезпечення комфортних умов навколишнього середовища для серверної кімнати (рис. 3.6).

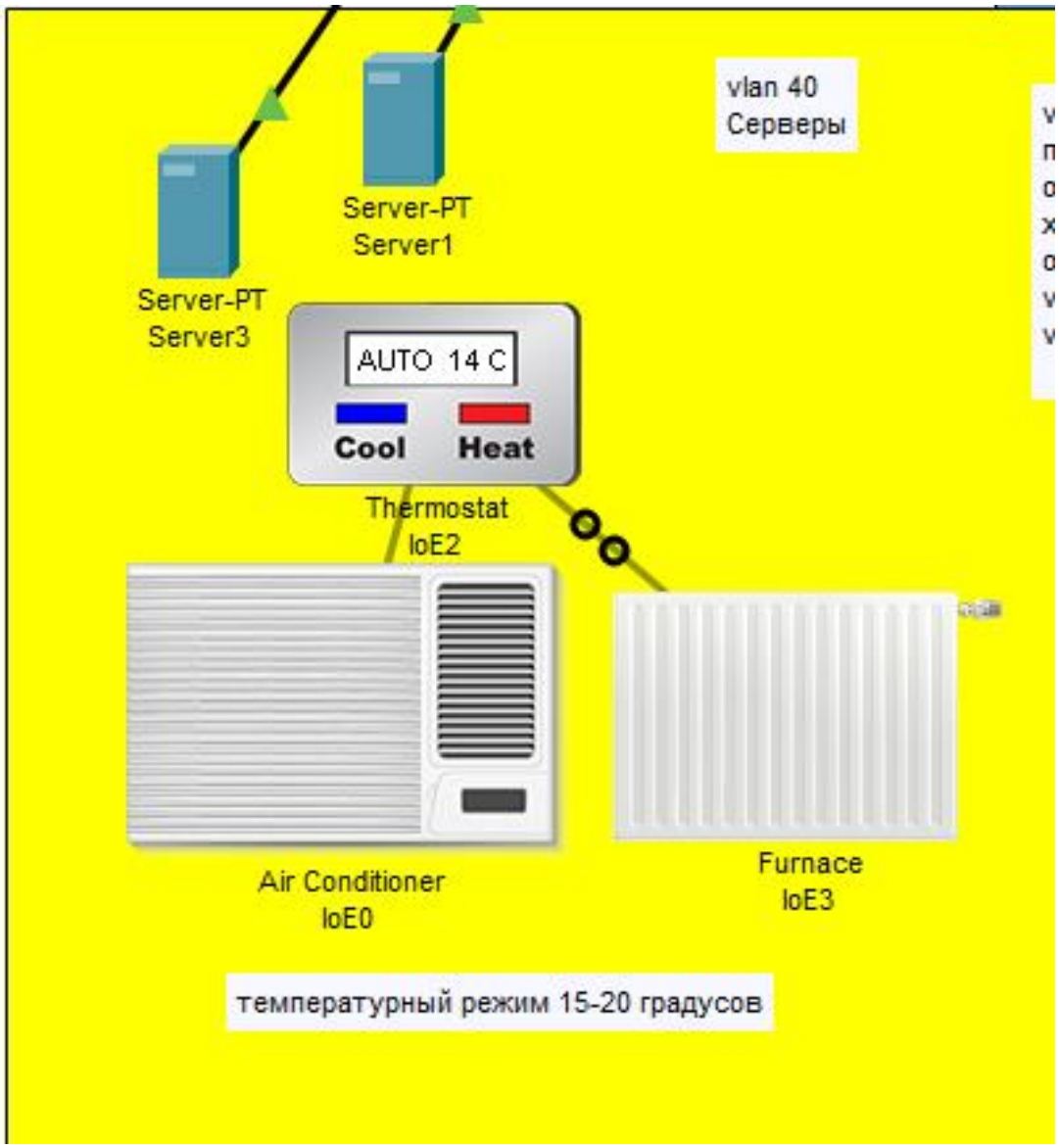

Рисунок 3.6 – Налаштування датчиків температури і вологості

3.3.2 Налаштування бездротової гостьовий локальної мережі Wi-FI

Гостьова локальна мережа ізольована від внутрішньої мережі організації в окремому VLAN. Відвідувачі отримують IP-адреса, адреса DNS сервера і маршрут за замовчуванням від DHCP-сервера.

3.3.3 Установка систем відеоспостереження

Встановлюються IP-камери в важливих місцях підприємства для забезпечення безпеки і моніторингу, що відбувається.

Як і в звичайних камерах, в IP-моделях об'єктив фокусує зображення на матриці, яка в свою чергу перетворює світло в електричний сигнал. Він передається на процесор, який обробляє кольору, яскравість і інші параметри зображення. Після цього відео надходить на компресор, який стискає дані для передачі їх через мережевий контролер.

Кожній IP-камері при підключенні присвоюється власний IP-адреса, як і інших пристроїв, які працюють через інтернет. Він необхідний для того, щоб камера могла синхронізуватися з реєстратором, що відбувається за допомогою спеціальної програми або команди. Без IP-адреси забезпечити спільну роботу і доступ до камери з мобільних гаджетів буде не можна.

ВИСНОВКИ

У дипломній роботі було спроектовано захищену комп'ютерну мережу для підприємства з декількома філіями. Проект був змодельований в симуляторі Cisco Packet Tracer. Cisco Packet Tracer є зручним засобом проектування віртуальних мереж, дозволяючи створювати образи як нечисленних фізичних пристроїв, так і складних топологій, що включають в себе тривалу настройку конфігурацій

Були всебічно вивчені і проаналізовані теоретичні відомості, які стосуються комп'ютерних мереж в загальному та способів захисту мережі. Також було проаналізовано, які актуальні на даний момент існують симулятори розробки комп’ютерних мереж, для того щоб обрати найбільш підходящий симулятор.

Завдання побудови віртуальної захищеної мережі вимагає комплексного підходу, врахування всіх тонкощів, особливостей роботи устаткування і глибоких системних знань з побудови мереж в цілому.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Офіційний сайт компанії Cisco Packet Tracer (Електронний ресурс) Режим доступу: www/ URL: https://www.cisco.com/
2. В. Оліфер, Н. Оліфер Комп'ютерні мережі. Принципи, технології, протоколи – 5 видання (2016).
3. Керівництво за технологіями об'єднаних мереж. 4 видання. - М .: Вільямс, 2005
4. Протоколи передачі даних: що це, які бувають і в чому відмінності? (Електронний ресурс). Режим доступу: www/ URL: https://tproger.ru/explain/protokoly-peredachi-dannyh-chto-jeto-kakie-byvajut-i-v-chjom-razlichija/
5. У. Одом "Офіційне керівництво Cisco по підготовці до сертіфікаціонним іспитів CCNA ICND2 200-101. Маршрутизація і комутація" (2016)
6. Боршевніков, А. Е. Мережеві атаки. Види. Способи боротьби (2011)
7. Новини в світі технологій (Електронний ресурс). Режим доступу: www/ URL: https://www.internet-technologies.ru/
8. Офіційний сайт емулятора GNS 3 (Електронний ресурс). Режим доступу: www/ URL: https://gns3.com/
9. Офіційний сайт емулятора SNMP Agent Simulator (Електронний ресурс). Режим доступу: www/ URL: https://veraxsystems.com/