ЗМІСТ

СПИСОК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ І ТЕРМІНІВ

Сокращения

ПК – персональний комп’ютер

ОС – операційна система

ПЗ – програмне забезпечення

ARP – Address Resolution Protocol

ASA – Adaptive Security Appliance

CCNA – Cisco Certified Network Associate

CCNP – Cisco Certified Network Professional

CPU – Central Processing Unit

CDP – Cisco Discovery Protocol

CLI – Command Line Interface

DECT – Digital Enhanced Cordless Telecommunication

DNS – Domain Name Service

DRAM – Dynamic Random Access Memory

DARPA – Defense Research Projects Agency

DCE – Distributed Computing Environment

DTE – Data Terminal Equipment

DHCP – Dynamic Host Configuration Protocol

ETSI – European Telecommunications Standards Institute

EWC – Enhanced Wireless Consortium

EIGRP – Enhanced Interior Gateway Routing Protocol

FTP – File Transfer Protocol

GNS3 – Graphical Network Simulator

GUI – Graphical User Interface

HTTP – HyperText Transfer Protocol

IEEE – Institute of Electrical and Electronic Engineers

ICMP – Internet Control Message Protocol

IOS – Internet Operating System

IGRP – Interior Gateway Routing Protocol

IP – Internet Protocol

ISDN – Integrated Services Digital Network

LAN – Local Area Network

MAC – Media Access Control

MPLS – Multiprotocol Label Switching

NAT – Network Address Translation

OSPF – Open Shortest Path First

RAM – Random Access Memory

RIP – Royals Internet Portal

RTP – Real-time Transport Protocol

SNMP – Simple Network Management Protocol

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

VLAN – Virtual Local Area Network

ВСТУП

При викладанні дисципліни «Комп’ютерні мережі» важливе значення має можливість придбання студентами практичних навичок роботи з різним мережевим комунікаційним устаткуванням. Уміння проводити конфігурацію мережі, налаштування протоколів передачі даних і тестування її працездатності. Бажано, щоб лабораторні роботи проходили з використанням реального мережевого обладнання. Проте, організація подібних лабораторних стендів не завжди можлива, тому що це вимагає додаткових фінансових вкладень. У такій ситуації відмінним рішенням є використання в лабораторному практикумі різних програмних мережевих емуляторів. З їх допомогою можна безболісно здійснювати будь-які маніпуляції з мережевим устаткуванням і його конфігурування. У студентів з’являється можливість тестувати, симулювати і експериментувати, але не з реальним обладнанням, а у віртуальному середовищі. У зв’язку з цим, актуальним завданням є розробка навчальних завдань, адаптованих під програмне середовище емулятора. Так званих віртуальних лабораторних стендів – шаблонів мереж для конфігурації.

Метою кваліфікаційної роботи є розробка завдань лабораторного практикуму з дисципліни «Комп’ютерні мережі» засобами програмного емулятора IP-мереж для вивчення мережевих технологій.

Для досягнення поставленої мети в рамках кваліфікаційної роботи необхідно вирішити наступні завдання:

– провести огляд та порівняльний аналіз можливостей сучасних мережевих програмних емуляторов;

– обґрунтувати вибір емулятора для розробки лабораторного практикуму;

– проаналізувати вбудовані засоби емулятора для створення шаблонів мереж і різних навчальних сценаріїв;

– розробити структуру лабораторного практикуму і варіанти тестуючих завдань;

– провести аналіз можливості впровадження лабораторного практикуму в навчальний процес.

У ході створення варіантів завдань буде проаналізовано можливість розробки тестуючих прикладів – файлів з шаблонами мереж для самопідготовки студентів. Файли будуть видаватися студентам для підготовки до занять у вільний час. Студенти повинні будуть провести конфігурування обладнання мережі відповідно до завдання і продемонструвати викладачеві працездатну мережу перед виконанням лабораторної роботи. Це дасть можливість студентам засвоїти теоретичні основи побудови мереж, особливо розділи, що традиційно викликають складності в освоєнні: безкласова IP-адресація, розбиття мережі на підмережі (subnetting) і настройка базової маршрутизації.

1 ОГЛЯД СУЧАСНИХ МЕРЕЖЕВИХ СИМУЛЯТОРІВ І ЕМУЛЯТОРІВ

Для побудови моделей телекомунікаційних мереж перш за все користувачу необхідно обрати певну систему моделювання, яка найбільш підходить для його моделі мережі зв'язку.

Існує досить велика кількість симуляторів і емуляторів для побудови моделей телекомунікаційних мереж. У цьому розділі будуть показані найбільш популярні інструменти, які вирішують цю задачу.

Розглянемо основні характеристики і можливості сучасних мережевих симуляторів і емуляторів. При формуванні їхнього переліку, будемо в якості основної вимоги враховувати можливість використання даного програмного засобу мережевого моделювання в навчальному процесі. Засоби повинні бути простими в освоєнні і не перевантажені складними додатковими функціями.

Слід розрізняти програмні продукти типу симулятор і емулятор.

Симулятор – імітує якийсь набір команд, який є незмінним і не дозволяє користувачеві вийти за цей набір. При спробі виконання непідтримуваної команди, ми відразу отримаємо повідомлення про помилку.

Класичний приклад програм – симуляторів:

– Cisco Packet Tracer [1][1];

– Boson NetSim [2,3][23];

Емулятори ж навпаки – дозволяють програвати (виконуючи байт трансляцію) образи (прошивки) реальних пристроїв, найчастіше без видимих обмежень. Прикладом емулятора є програмний продукт GNS3/Dynamips [4][4].

---

[1] Cisco Packet Tracer// Офіційний сайт. URL: https://www.netacad.com/ ru/courses/packet-tracer (дата звернення: 27.02.2019)

[2] Boson NetSim// Офіційний сайт. URL:http://www.boson.com/netsim-cisco-network-simulator (дата звернення: 27.02.2019)

[3] Boson NetSim 12. User Manual. URL:http://www.boson.com/Files/ Support/NetSim-12-User-Manual.pdf дата звернення: 27.02.2019)

Зупинимося на цих програмних продуктах детальніше і проведемо порівняльний аналіз їх можливостей з метою подальшого обґрунтування вибору програмного засобу моделювання IP – мереж в лабораторному практикумі з дисципліни «Комп'ютерні мережі».

Безумовно будемо враховувати той факт, що Одеський державний екологічний університет починаючи з 2012 року є партнером компанії Cisco в програмі Мережевих Академій. Тому почнемо огляд саме з симулятора Cisco Packet Tracer.

1.1 Симулятор Boson NetSim

Boson NetSim – програмне забеспечення, яке моделює роботу мережевого устаткування Cisco, і розроблено, щоб допомогти користувачеві у вивченні Cisco IOS. Програмні продукти фірми Boson дають можливість створювати мережеві топології (до 200 пристроїв) з широкого спектру маршрутизаторів і комутаторів компанії Cisco, робочих станцій і мережевих з'єднань типа Ethernet, Serial, ISDN, Frame Relay. Ця функція може бути виконана як для навчання, так і для роботи. Наприклад, щоб зробити настройку мережі ще на етапі планування або щоб створити копію робочої мережі з метою усунення несправностей.

NetSim має дуже розвинену підтримку, яка забезпечується компанією Boson (це пов'язано, звичайно ж, з бурхливими темпами розвитку телекомунікаційних мереж). У зв'язку з цим, компанія Cicso рекомендує використовувати цей продукт для підготовки до здачі іспитів. Тому Boson випускає різні версії NetSim'у, кожна з яких орієнтована на певний іспит і, відповідно, рівень знання користувача.

Boson NetSim випускається тільки під Windows. Являє собою збірник лабораторних робіт, згрупований за темами іспиту. Інтерфейс складається з

[4] GNS3/Dynamips// Офіційний сайт. URL: https://www.gns3.com/ (дата звернення: 27.02.2019)

декількох секцій: опис завдання, карта мережі, в лівій частині знаходиться список всіх лабораторних робіт. Зовнішній вигляд програми представлений на рис.1.1.

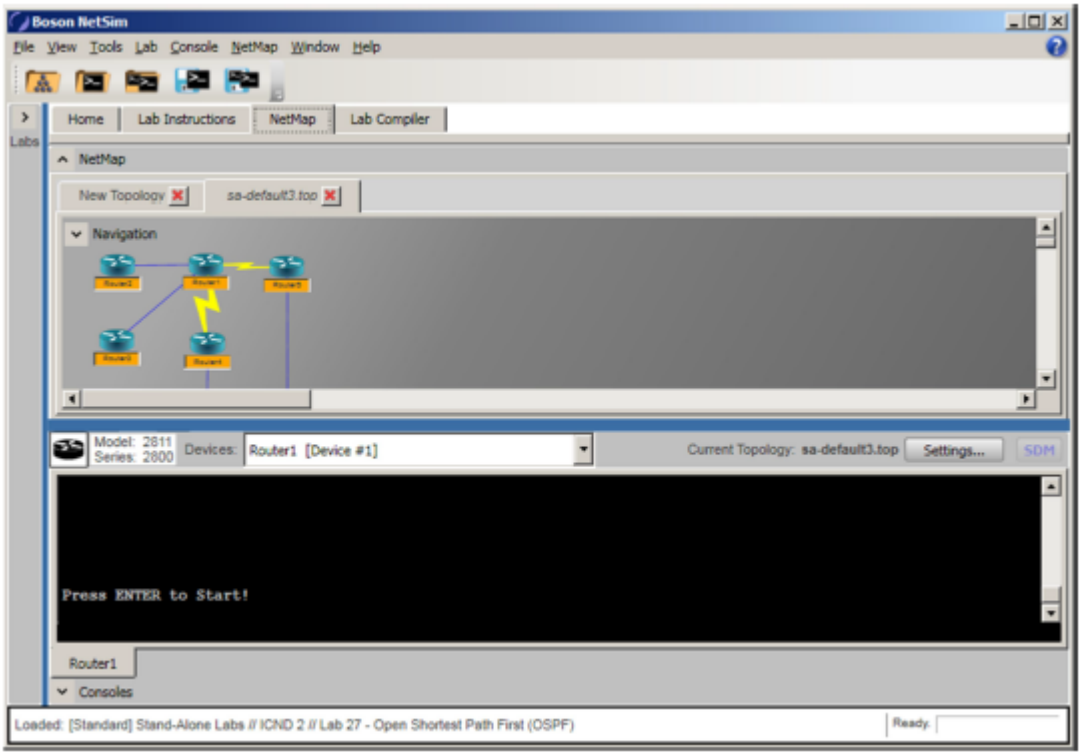

Рисунок 1.1 – Зовнішній вигляд програми Boson NetSim

Закінчши виконання лабораторних робіт, можна перевірити результат, дізнатися, чи все було зроблено.

Основні переваги Boson NetSim:

– симулює мережевий трафік за допомогою технології віртуальних пакетів;

– надає два різні стилі перегляду: режим Telnet'a або режим підключення по консолі;

– підтримує до 200 пристроїв на одній топології;

– включає в себе лабораторії, які підтримують симуляцію SDM;

– включає в себе безліч Cisco пристроїв.

Недоліки Boson NetSim:

– іноді можуть проявлятися різноманітні зависання програми, які виправляються тільки перезапуском програми;

– мережевий стимулятор Boson NetSim платний і для його використання необхідно придбати ліцензію.

Одним з важливих недоліків даного стимулятора є те, що дане програмне забезпечення розроблене для комерційного використання.

1.2 Симулятор Cisco Packet Tracer

Даний програмний продукт розроблений компанією Cisco і рекомендований до використання при вивчені телекомунікаційних мереж і мережевого устаткування. Вигляд головного окна продукту наведений на рис.1.2.

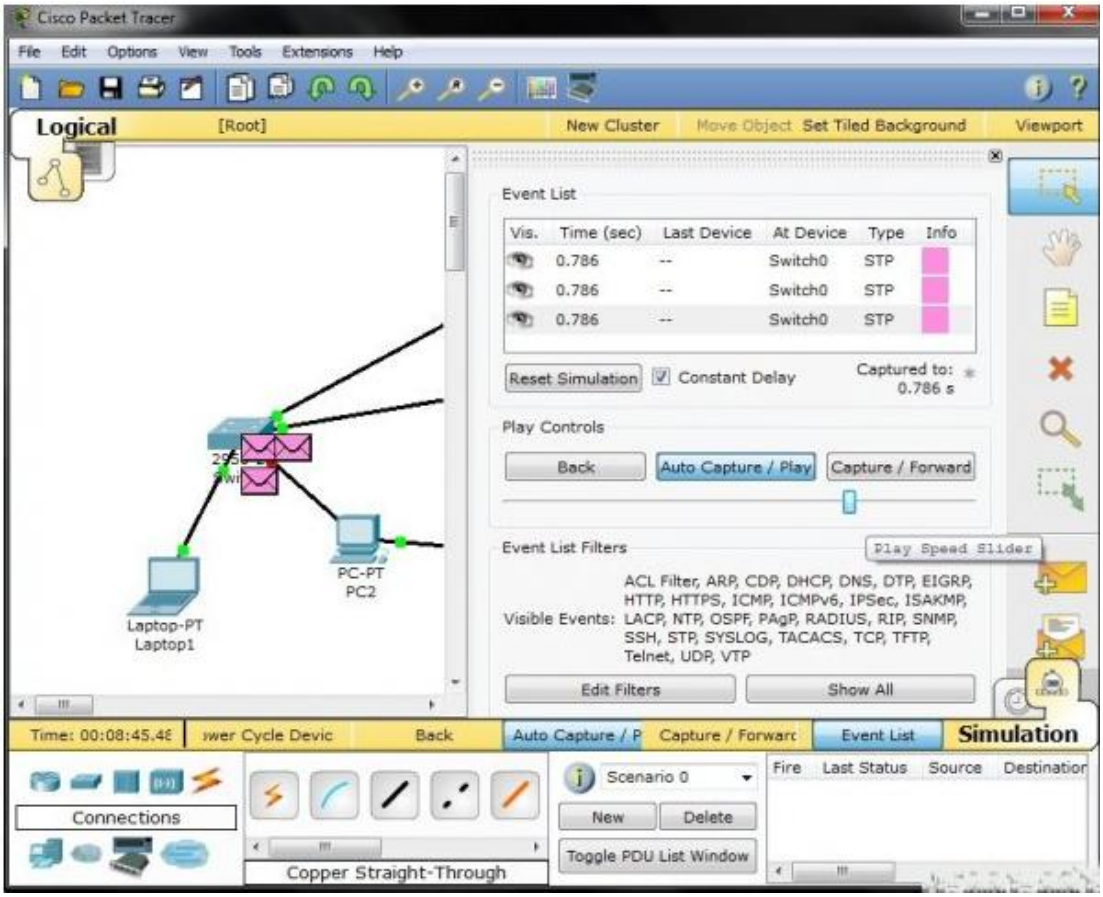

Рисунок 1.2 – Вигляд головного окна мережевого емулятору Packet Tracer

Пакет пропонується відділенням Networking Academy, що відповідають за освіту і підготовку різних курсів. Задача програми: допомогти закріпити на практиці отримані студентом теоретичні навики. Для її вирішення Packet Tracer має все необхідне, дозволяючи "будувати" мережі різної складності з практично необмеженою кількістю пристроїв. За допомогою даного програмного продукту викладачі можуть придумувати, будувати, конфігурувати мережі і проводити в них пошук несправностей. Packet Tracer дає можливість більш докладно представляти новітні технології, тим самим роблячи навчальний процес надзвичайно корисним з точки зору засвоєння отриманого матеріалу.

Всі установки здійснюються за допомогою логічної діаграми мережі, для симуляції представлений весь спектр обладнання, що випускається Cisco (роутери, свитчи, точки доступу тощо). Можна змінювати налаштування об’єктів, моделювати потоки даних та багато іншого. Підтримується велика кількість протоколів і технологій, що використовуються в обладнанні Cisco (повний список наведений в документації на сайті).

Packet Tracer 5.0 включає наступні особливості:

– моделювання логічної топології: робочий простір для того, щоб створити мережі будь-якого розміру на CCNA-рівні складності;

– моделювання в режимі реального часу;

– режим симуляції;

– моделювання фізичної топології: більш зрозуміла взаємодія з фізичними пристроями, використовуючи такі поняття як місто, будинок, стійка і т.д.;

– покращений GUI, необхідний для більш якісного розуміння організації мережі, принципів роботи пристрою;

– багатомовна підтримка: можливість перекладу даного програмного продукту практично на будь-яку мову, необхідну користувачеві;

– удосконалене зображення мережевого устаткування зі здатністю додавати/видаляти різні компоненти;

– наявність Activity Wizard дозволяє студентам і викладачам створювати шаблони мереж і використовувати їх надалі.

Робота з обладнанням хоч і віртуальна, але виглядає так, ніби доводиться використовувати реальні пристрої. Можна додавати плати розширення, настроювати параметри в командному рядку або використовуючи графічний інтерфейс. Весь процес обміну даними представлений у вигляді діаграм і таблиць, що допомагає візуально оцінити поточні настройки і роботу устаткування.

Офіційно у вільному доступі Packet Tracer не знайти, він призначений тільки для зареєстрованих викладачів і студентів курсів. Під час установки ніяких ключів не потрібно, сам процес стандартний.

Всі настройки проводяться в великому вікні посередині. Внизу зліва знаходяться групи пристроїв, після вибору трохи правіше з'являються самі пристрої. Відзначаємо потрібне і подвійним клацанням на вільному місці в полі посередині переносимо його на карту мережі. Підтримка drag'n'drop робить процес дуже простим, пристрої потім можна рухати, видаляти і т.п. Зручно, що Packet Tracer самостійно пов'язує деякі девайси, наприклад, при появі Wireless світча до нього автоматично підключаються всі пристрої, що підтримують цей вид з'єднання. При протяжці кабелю вибираємо порт, до якого його підключаємо. Один із значків відповідає за автоматичне визначення типу з'єднання, що прискорює складання мережі на стадії вивчення. Якщо в процесі буде допущена помилка, то користувач отримує попередження з коротким описом (наприклад, немає вільного роз'єму).

Поки всі налаштування логічної мережі проводилися у вкладці Logical Workspace (Ctrl+L). Щоб перейти до фізичного пристрою і подивитися порядок підключення, слід вибрати у верхньому лівому куті вкладку Physical Workspace (Ctrl+P). Також Packet Tracert надає два режими відображення роботи мережі: Realtime Mode (Ctrl+R) і Simulations Mode (Ctrl+S). Перемикання проводиться за допомогою ярликів у правому нижньому куті або гарячих клавіш. У Realtime мережа працює у звичайному ре-

жимі, в режимі Simulations можна спостерігати і контролювати процеси, що відбуваються в мережі (роботу пристроїв, інтервали часу, механізми передачі даних і т.д.) Майстер Activity Wizard допоможе створити власні навчальні сценарії [5][5]. Симулятор доступний як під Windows, так і для Linux. За допомогою програми Packet Tracert можна будувати цілі мережі між віртуальними офісами

Переваги Packet Tracer – дружність і логічність інтерфейсу. Крім цього в ньому зручно перевіряти роботу різних мережевих сервісів, на зразок DHCP / DNS / HTTP / SMTP / POP3 і NTP, можливість візуально побачити на якому з рівнів моделі OSI працює той чи інший протокол. Найголовніший плюс – це можливість перейти в режим симуляції і побачити переміщення пакетів з уповільненням часу.

Основним недоліком симулятора Cisco Packet Tracer є відсутність підтримки розширених команд конфігурування різних протоколів, що не дозволяє використовуватися даний мережевий симулятор для виконання лабораторних робіт вище рівня CCNA.

Отже, даний симулятор має масу плюсів і один недолік, що не вплине на виконання даного курсу лабораторних робіт.

1.3 Емулятор GNS3

GNS3 (graphical network simulator) – дуже потужний симулятор мереж Cisco, що випускається під вільною ліцензією і дозволяє емулювати мережі великого розміру. На сьогоднішній день є одним з найбільш зручних інструментів для емуляції Cisco. GNS3 – графічний інтерфейс (на Qt) для емулятора Dynamips. Вільний проект, доступний під Linux, Windows і Mac OS X. Але більшість його функцій, покликаних поліпшити продуктивність, працюють

[5] CCNA Security 1.0 Student Packet Tracer Manual. URL:http://www.scribd.com/doc/25536606/CCNA-Security-Student-Packet-Tracer-Manual (дата звернення: 27.02.2019)

тільки під Linux, 64 бітна версія так само тільки для Linux. Це емулятор, який працює з реальними прошивками IOS. Зовнішній вигляд програми наведений на рис.1.3.

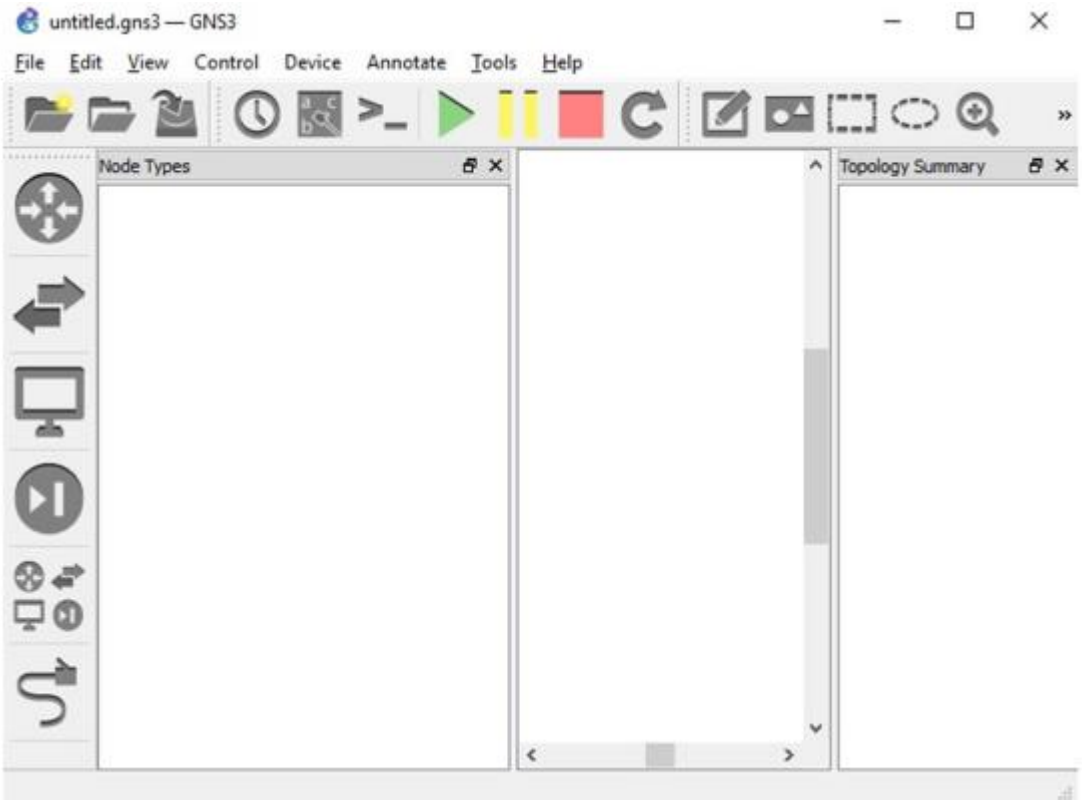

Рисунок 1.3 – Вигляд головного окна мережевого емулятору GNS3

До GNS3 можна підключати віртуальні машини VirtualBox [6][6] або VMware Workstation [7][7] і створювати досить складні схеми, при бажанні можна піти далі і випустити його в реальну мережу. Крім того, Dynamips вміє емулювати як старі Cisco PIX (Private Internet Exchange – міжмережевий екран з перетворенням мережевих адрес, що випускався американською компанією Cisco Systems), так і відому Cisco ASA (Adaptive Security Appliance – серія апаратних міжмережевих екранів, розроблених компанією Cisco

[6] Software Oracle VM VirtualBox URL: http://download.virtualbox.org/virtualbox/UserManual.pdf (дата звернення: 27.02.2019)

[7] Software VMware Workstation. URL: http://www.vmware.com/ (дата звернення: 27.02.2019)

Systems).

GNS3 має інтуітивно зрозумілий інтерфейс (наприклад, ппідрахунок значення IdlePC можна запустити, натиснувши правою кнопкою на віртуальному маршрутизаторі і вибравши відповідний пункт меню).

Робота з GNS3 не складна. Після установки і першого запуску не потрібно шукати документацію і глибоко в неї вчитуватися. Складність розуміння першого запуску тільки лише в тому, що для запуску тестової віртуальної мережі необхідно дещо додаткове: образи ПЗ IOS, тому що програмний комплекс емулює апаратну частину, використовуючи реальний образ ПЗ. Однак GNS3 вже містить у собі dynamips і всі необхідні інтерфейси для управління ним. Так що додатково знайти доведеться тільки пару образів IOS.

Але при всьому цьому у GNS3 є маса недоліків:

– кількість платформ строго обмежена: запустити можна тільки ті шасі, які передбачені розробниками Dynamips;

– неможливо повноцінно використовувати комутатори серії Catalyst, це пов'язане з тим, що на них використовується велика кількість специфічних інтегральних схем, які відповідно вкрай складно емулювати.Залишається використовувати мережеві модулі (NM) для маршрутизаторів;

– при використанні великої кількості пристроїв гарантовано буде спостерігатися зниження продуктивності.

Отже, даний емулятор має велику кількість плюсів, але так само є вагомі недоліки, один з них – це відсутність можливості емуляції комутаторів, які використовуються в рамках даного курсу лабораторних робіт.

1.4 Обґрунтування вибору системи моделювання

Наведемо порівняльну табліцу переваг та недоліків розглянутих систем моделювання (табл.1.1).

Серед розглянутих емуляторів IP-мереж найбільш прийнятним варіантом для використаннях в рамках лабораторного практикуму, що розробляється, слід признати програму Cisco Packet Tracer.

Таблиця 1.1 – Порівняльний аналіз систем моделювання

ПЗ	Переваги	Недоліки
Cisco Packet Tracer	– дружній інтерфейс (GUI); – моделювання в режимі реального часу; – великий вибір обладнання режим симуляції; – зручність роботи з мережевими сервісами.	відсутність підтримки розширених команд конфігурації різних протоколів, що не дозволяє використовувати даний симулятор для виконання лабораторних робіт вище рівня CCNA
Boson NetSim	– симулює мережевий трафік за допомогою технології – віртуальних пакетів; – два стилю перегляду: режим Telnet'a або режим підключення по консолі; – підтримує до 200 пристроїв на одній топології; – включає в себе лабораторії, які підтримують симуляцію вже готових робіт	– рідкісні зависання програми; – платний.
GNS3	– можливість створювати віртуальні машини VirtualBox або VMware Workstation; – вихід в реальну мережу; – можливість емулювати як старі Cisco PIX, так і Cisco ASA	– кількість платформ строго обмежена; – неможливо повноцінно використовувати комутатори Catalyst

На тому рівні начальної підготовки, для якого розроблюються лабораторні роботи, всі емулятори Cisco-мереж мають приблизно однакові властивості і характеристики. Однак пакет Cisco Packet Tracer в порівнянні з іншими має більш розвинутий інтерфейс, з ним легко починати роботу, він дуже простий у використані. Наявність режиму симуляції дозволяє мережевим фахівцям наочно продемонструвати (для кращого сприйняття) за яким інтерфейсом переміщається пакет, який протокол використовується і на якому з семи рівнів моделі OSI даний протокол задіяний. Packet Tracer спеціально розроблений для початкового вивчення сучасних телекомунікаційних систем, і більше за інші емулятори відповідає цьому завданню. Крім того, пакет легко інсталюється і безкоштовний для слухачів курсів Cisco.

Boson NetSim – не дивлячись на всі його плюси є один великий недолік – даний симулятор платний.

У GNS3 відсутня повноціна підтримка комутаторів.

Навчальне середовище на основ моделей розвиває навички усунення несправностей в мережі, дозволяє застосовувати творчий підхід до вирішення завдань. На основі Cisco Packet Tracer можуть розроблятися як індивідуальні лабораторні роботи, так і групові заняття. За допомогою даного стимулятора можна навчитися створювати, настроювати, вивчати мережі і усувати неполадки, використовуючи віртуальне обладнання та моделі з'єднань.

Зрозуміло, жоден симулятор не може повністю замінити досвід роботи в реальної мережі. Однак існуюче програмне забезпечення в цій сфері сприяє ефективному навчанню мережевим технологіям.

2 ЕТАПИ НАЛАШТУВАННЯ СТАТИЧНОЇ МАРШРУТИЗАЦІЇ

В цьому розділі розглянемо докладніші принципи налаштування статичної маршрутизації для маршрутизаторів Cisco. Надалі, будемо використовувати ці теоретичні засади при розробці завдання відповідної лабораторної роботи.

Протоколи маршрутизації – це правила за якими здійснюється обмін інформації про шляхи передачі пакетів між маршрутизаторами.

Одна з головних задач маршрутизатора – визначення найкращого шляху передачі даних до отримувача. Обмін інфрмацією про існуючі маршрути виконується за допомогою протоколів маршрутизації. Маршрутизатор також може визначати маршрути на підставі статичної конфігурації, введеної мережевим адміністратором. Таким чином, маршрутизація поділяється на:

– статичну маршрутизацію, коли адміністратор вручну визначає маршрути до мереж призначення.

– динамічну маршрутизацію, коли маршрутизатори дотримуються правил, що визначаються протоколами маршрутизації, тобто вибір найкращого шляху відбувається на підставі роботи протоколів, які обмінюються інформацією про маршрути передачі.

Маршрутизатор зберігає таблиці маршрутів в оперативній пам’яті в таблиці маршрутизації. Переглянути таблицю маршрутизації можна за допомогою команди show ip route.

Для конфігурації статичної маршрутизації Cisco використовують дві версії команди ip route. Перша версія:

ip route АдресаМережіПризначення МаскаМережіПризначення Інтерфес

Команда вказує маршрутизатору, що всі пакети, що призначені для АдресаМережіПризначення-МаскаМережіПризначення слід направляти на свій інтерфейс Інтерфес. Якщо інтерфейс Інтерфес – типа Ethernet, то фізичні (MAC) адреси вихідних пакетів будуть широкомовними.

Друга версія:

ip route АдресаМережіПризначення МаскаМережіПризначення Адреса

Команда вказує маршрутизатору, що всі пакети, які призначені для АдресаМережіПризначення-МаскаМережіПризначення, слід направляти на той свій інтерфейс, з якого досяжна IP адреса Адреса. Як правіло, Адреса це адреса наступного хопа на шляху до АдресаМережіПризначення. Вихідний інтерфейс і фізичні адреси вихідних пакетів визначаються маршрутизатором за своїми ARP таблицями на підставі IP адрес Адреса. Наприклад, ip route 10.6.0.0 255.255.0.0 Serial1 (1) та ip route 10.7.0.0 255.255.0.0 10.4.0.2 (2).

Перший приклад відображає мережевий префікс 10.6.0.0/16 на локальний інтерфейс маршрутизатора Serial1. Наступний приклад відображає мережевий префікс 10.7.0.0/16 на IP адресу 10.4.0.2 наступного хопа по шляху до 10.7.0.0/16. Обидві ці команді додадуть статичні маршрути в таблицю маршрутизації (мітка S):

```
S 10.6.0.0 via Serial1
S 10.7.0.0 [1/0] via 10.4.0.2
```

Зауважимо, що для мереж типа Ethernet рекомендується завжди використовувати команду (2) команди ip route. Ethernet інтерфейс на маршрутизаторі, як правило, з'єднаний з декількома Ethernet інтерфейсами інших пристроїв в мережі. Вказівка в команді ip route IP адреси дозволить маршрутизатору вірно сформувати фізичну адресу вихідного пакету за своїми ARP таблицям.

Для діагностики можливості встановлення зв'язку в мережах використовуються протоколи типу запит-відповідь або протокол луна-пакетів. Результати роботи такого протоколу можуть допомогти в оцінці надійності путі до іншого пристрою, величин затримок в цілому і між проміжними пристроями. Для того щоб така команда працювала, необхідно, щоб не тільки локальний мережевий пристрій знав як потрапити до пункту призначення, але і щоб пристрій в пункті призначення знав, як дістатися до джерела.

Команда ping посилає ICMP (Internet Control Message Protocol) луна-пакети для верифікації з'єднання. У наведеному нижче прикладі час проходження одного луна-пакету перевищило заданий, про що свідчить точка (.) в інформації, що виведена нижче, а чотири пакета пройшли успішно, про що свідчить знак оклику (!).

```
Switch> ping 172.16.101.1
Type escape sequence to abort.
Sending 5 100-byte ICMP echoes to 172.16.10.1 timeout is 2 seconds:
.!!!!
Success rate is 80 percent, round-trip min/avg/max = 6/6/6 ms
```

Символи, які відображають результати виконання команди ping наведені в табл.2.1.

Таблиця 2.1 – Результати команди ping

Символ	Значення
!	Успішний прийом луна-відповіді
.	Перевищений час очікування
U	Пункт призначення недосяжний
C	Перевантаження мережі
I	Виконання команди перервано адміністратором
?	Невідомий тип пакету
&	Пакет перевищив значення параметру часу життя TTL пакету

Команди traceroute показує адреси проміжних інтерфейсів (хопов) на путі пакетів в пункт призначення.

```
Switch> traceroute 172.16.101.1
```

Команда trace є ідеальним засобом для з'ясування того, куди відправляються дані в мережі. Ця команда використовує ту ж технологію протоколу ICMP, що і команда ping, тільки замість перевірки наскрізного зв'язку між

відправником і одержувачем, вона перевіряє кожний крок на шляху. Команда trace використовує здібність маршрутизаторів генерувати повідомлення про помилки при перевищенні пакетом свого встановленого часу життя (Time To Live, TTL). Ця команда посилає декілька пакетів і виводить на екран дані про час проходження туди і назад для кожного з них. Перевага команді trace полягає в тому, що вона показує черговий досягнутий маршрутизатор на шляху до пункту призначення. Це дуже потужний засіб для локалізації відмов на шляху від відправника до одержувача. Варіанти відповідей утиліти trace наведені в табл.2.2.

Таблиця 2.2 – Варіанти відповідей утиліти trace

Символ	Значення
!H	Зондуючий пакет був прийнятий маршрутизатором, але не переадресований, що звичайно буває через список доступу
P	Протокол недосяжний
N	Мережа недосяжна
U	Порт недосяжний
*	Перевищення межі очікування

3 ПРОТОКОЛИ ДИНАМІЧНОЇ МАРШРУТИЗАЦІЇ

Оскільки тематика лабораторних робіт безпосередньо пов'язана з налаштуванням маршрутизаторів, то вибір протоколу динамічної маршрутизації для подальшого використання в лабораторних роботах є одним із завдань даної кваліфікаційної роботи. Розглядати, в рамках лабораторних робіт, всі можливі протоколи динамічної маршрутизації не представляється можливим. У цьому розділі будуть надані короткий огляд і порівняльна характеристика протоколів динамічної маршрутизації, найбільш поширених в мережах і запропоновані деякі рекомендації по вибору протоколу в залежності від розмірів і вимог мережі.

За умови збільшення розмірів мережі компанії для підтримки її нормальної працездатності адміністратору доводиться переходити від статичної маршрутизації до динамічної і, отже, до використання одного з протоколів динамічної маршрутизації. Оскільки вибір протоколу робить істотний вплив на ефективність і надійність роботи мережі організації в цілому, то він повинен бути добре обгрунтований. Для початкового вибору бажано мати коротку порівняльну характеристику протоколів.

Мета завдання по вибору протоколу динамічної маршрутизації – виділити найбільш істотні критерії порівняння протоколів і фактори, що впливають на їх вибір, а також привести коротку порівняльну характеристику протоколів і деякі загальні рекомендації щодо їх застосування.

3.1 Основні вимоги до протоколів динамічної маршрутизації

Як відомо, протоколи динамічної маршрутизації дозволяють маршрутизаторам мереж автоматично створювати таблиці оптимальних маршрутів і динамічно модифікувати їх відповідно до змін, що відбуваються в топології мережі. Перелічимо основні фактори від яких залежить вибір протоколу маршрутизації:

1) Топологія і складність мережі.

2) Розміри мережі і необхідність в її подальшому масштабуванні (можливості деяких протоколів для цього обмежені).

3) Завантаженість мережі. Для мереж з високим коефіцієнтом завантаженості ліній зв'язку має значення здатність протоколу до перерозподілу потоків даних.

4) Вимоги до надійності мережі. Допустимий час простоїв або нестабільності в роботі мережі через відмову її вузлів.

5) Вимоги до захисту інформації в мережі.

6) Необхідність підключення сегмента, що маршрутизується, до вже існуючої мережі.

7) Можливість організації програмних маршрутизаторів. При невеликому трафіку в мережі або на окремих її ділянках від маршрутизатоів не потрібна висока продуктивність.

3.2 Огляд протоколів динамічної маршрутизації

Розглянемо найбільш поширені протоколи динамічної маршрутизації (без урахування Exterior Gateway Protocol):

1) RIP (Routing Information Protocol) [8][8];

2) IGRP (Interior Gateway Routing Protocol) [9][9];

3) EIGRP (Enhanced Interior Gateway Routing Protocol) [10][10];

4) OSPF (Open Shortest Path First) [11][11].

---

[8] RIP Version 2 protocol. URL: http://muff.kiev.ua/files/books/ 2453_RIPv2.pdf (дата звернення: 27.02.2019)

[9] An Introduction to IGRP. Cisco Systems, Inc. URL: https://ru.scribd.com/document/75310948/An-Introduction-to-IGRP (дата звернення: 27.02.2019)

[10] An Introduction to EIGRP. Cisco Systems, Inc. URL: https://ru.scribd.com/document/20190928/Introduction-to-EIGRP (дата звернення: 27.02.2019)

[11] An Introduction to OSPF protocol URL: https://ru.scribd.com/document/23941805/Introduction-to-OSPF (дата звернення: 27.02.2019)

3.2.1 Протокол RIP

Протокол заснований на дистанційно - векторному алгоритмі і в більшості реалізацій використовує найпростішу метрику – кількість проміжних маршрутизаторів до мережі призначення.

Головною перевагою протоколу є легкість конфігурування, що не вимагає високої кваліфікації обслуговуючого персоналу. пПротокол є відкритим і підтримується практично всіма виробниками мережевого обладнання. Також є реалізації протоколу в ПЗ і підтримка в ряді ОС.

Основними недоліками протоколу є: повільна збіжність і великий обсяг службового трафика. Це обмежило сферу застосування протоколу мережами з кількістю маршрутизаторів не більше п'ятнадцяти.

В протокол RIP версії 2 додана підтримка маски змінної довжини, мультикастінгова (багатоадресна) розсилка замість широкомовної і засоби захисту при обміні маршрутної інформацією у вигляді аутентифікації по ключу MD5 і відкритого (нешифрованого) тексту. Протокол досить поширений в невеликих, що не прагнуть до розширення локальних мережах з невисокими вимоги до надійності мережі. У новій версії протоколу Riping організована підтримка протоколу IPv6[12][12].

3.2.2 Протокол IGRP

Закритий дистанційно - векторний протокол IGRP компанії Cisco Systems був спроектований для усунення ряду недоліків протоколу RIP, і мав на меті забезпечити кращу підтримку великих мереж (до 255 маршрутизаторів), які містять канали зв'язку з відмінними характеристиками смуги пропускання і величини затримки. Протокол використовує комбіновану метрику,

[12] Джером Ф. Димарцио. Маршрутизаторы Cisco. Пособие для самостоятельного изучения – М: Издательство «Символ-Плюс», 2003. – 508 с.: ил.

яка включає затримку, смугу пропускання, надійність і завантаженість маршруту. Вагові коефіцієнти, що визначають внесок цих характеристик в результуючу метрику, задаються користувачем, забезпечуючи гнучку адаптацію до його конкретним завданням. Показники затримки і смуги пропускання конфигурируются для кожної лінії зв'язку попередньо, а показники надійності і завантаженості можуть обчислюватися в процесі обробки реального трафіку в мережі [13][13].

Протокол IGRP забезпечує швидшу збіжність, ніж RIP завдяки застосування пакетів оновлення з миттєвою розсилкою (інформація про зміни в мережі відправляється відразу, як тільки стає доступною, що не чекаючи чергового часу поновлення). протокол підтримує балансування навантаження між декількома маршрутами навіть в тому випадку, якщо їх метрики не рівні, але знаходяться в межах певного діапазону показників найкращого маршруту. При цьому співвідношення обсягів відправляються по кожній колії даних буде пропорційно співвідношенню їх метрик.

До недоліків протоколу можна віднести відсутність підтримки масок підмереж змінної довжини і можливості об'єднання маршрутів. Періодичні розсилки маршрутної інформації сусіднім маршрутизаторам залишаються широкомовними. Засоби забезпечення безпеки обмежені. Відсутні засоби аутентифікації при обміні маршрутною інформацією. Протокол сумісний з RIP.

3.2.3 Протокол EIGRP

Компанія Cisco Systems пропонує покращену версію вихідного протоколу IGRP. Протокол є гібридним і заснований на алгоритмі поновлення Diffusing-Update Algorithm (DUAL). Він поєднує в собі кращі якості дista-

[13] Аллан Леинванд, Брюс Пински. Конфигурирование маршрутизаторов Cisco. 2 издание. – М.: Издательский дом «Вильямс», 2001. – 368 с.: ил.

ційно - векторних протоколів (простота алгоритму вибору оптимального маршруту) і протоколів стану каналів зв'язку (швидка збіжність і економія смуги пропускання мережі за рахунок повідомлень тільки про стани зв'язків і про їх зміну). Всі розсилки протоколу є мультикастними або індивідуальними. Таким чином, інформація розсилається тільки при змінах і тільки тим маршрутизаторам, яких вона стосується. З метою підвищення масштабованості протоколу в нього додана підтримка масок підмереж змінної довжини і можливість об'єднання маршрутів [14][14].

В останніх версіях EIGRP є засоби захисту, що не дозволяють дописувати елементи в таблицю маршрутизації, і аутентифікація по ключу MD5. Крім того, в даний час для EIGRP розробляють засоби підтримки IPv6, так що цей протокол буде розвиватися надалі.

Основним недоліком EIGRP, як і його попередника, є закритість і реалізація тільки на обладнанні Cisco Systems. Протокол добре сумісний з IGRP, а також з RIP.

3.2.4 Протокол OSPF

Найбільш універсальним і гнучким у налаштуванні протоколом динамічної маршрутизації в корпоративних мережах на сьогоднішній день є відкритий протокол вибору першого найкоротшого шляху OSPF. Протокол спочатку був орієнтований на роботу в великих мережах (до 65536 маршрутизаторів) зі складною топологією. Він заснований на алгоритмі стану каналів зв'язку і має високою стійкістю до змін топології мережі і швидкої збіжністю. При виборі маршруту використовується метрика пропускної здатності складеної мережі (тобто передача даних за найбільш швидкісними каналами зв'язку). Протокол може підтримувати різні вимоги IP-пакетів на якість обслуго-

[14] Джо Хабракен. Как работать с маршрутизаторами Cisco. – СПб.: Издательство «ДМК-Пресс», 2005. – 317 с.: ил

вування (пропускна здатність, затримка і надійність) за допомогою побудови окремої таблиці маршрутизації для кожного з цих показників [15][15].

Протокол володіє і іншими перевагами, корисними в великих сучасних мережах. До них відносяться можливість балансування навантаження між каналами з рівними метриками і засоби аутентифікації як по нешифрованому паролю, так і по шифрованому (шляхом додавання до пакету дайджесту ключа і тіла пакета за алгоритмом MD5). Нумерація пакетів виключає їх повторюваність і таким чином можливість повторної атаки.

Відкритість протоколу визначає його підтримку практично всіма виробниками мережевого устаткування, реалізації в ПЗ під всі популярні ОС, а також безпосередню інтеграцію в ряд ОС.

До недоліків проколу слід віднести високу обчислювальну складність і, отже, високі вимоги, що пред'являються до ресурсів маршрутизатора. Обчислювальна складність OSPF зростає зі збільшенням розмірів мережі. Тому для збільшення масштабованості протоколу застосовується поділ мережі на логічні області, з'єднані магістральною областю. Внутрішня топологічна інформація між областями НЕ передається. Скорочення обсягів таблиць маршрутизації і зниження службового трафіку при оновленні топологічної інформації служить можливістю об'єднання декількох адрес мереж в один при виявленні у них загального префікса, і заміна широкомовних розсилок мультикастинговими.

Платою за ці переваги є складність конфігурації і необхідність ретельного попереднього планування мережі для її оптимальної роботи (розбивка на області, виділення магістралі, розподіл функцій між маршрутизаторами з урахуванням їх обчислювальної потужності: рядові, виділені в зоні, прикордонні та ін.

В якості перспективних функцій OSPF слід назвати підтримку протоколу Ipv6 і можливість вибору маршруту на підставі поточного коефіцієнта

---

[15] Вито Амато. Основы организации сетей Cisco. Том2 – М.: Издательский дом «Вильямс», 2004. – 464 с.: ил.

завантаженості каналів зв'язку (розширена версія OSPF отримала назву Constrained Shortest Path First – CSPF). Протокол сумісний з RIP.

3.3 Вибір протоколу динамічної маршрутизації

Вибір протоколу динамічної маршрутизації залежить від розмірів і вимог мережі. В табл.3.1 представлена порівняльна характеристика основних протоколів динамічної маршрутизації [16][16].

Таблиця 3.1 – Порівняльна характеристика протоколів динамічної маршрутизаці

Критерії	RIP	IGRP	OSPF	EIGRP
Безпека	Відкритий пароль чи аутентифікаціяпо ключу MD5	–	Відкритий пароль чи аутентифікаціяпо ключу MD5	Аутентифікаціяпо ключу MD5
Тип алгоритму	Вектор відстані	Вектор відстані	Стан каналов зв’язку	Комбінований
Балансування навантаження	–	Різні метрики	Однакові метрики	Різні метрики
Об’єднання маршрутів	–	–	+	+
Маска підмереж змінної довжини	+	–	+	+

[16] Брюс Александер, Тони Аллен, Матт Карлинг и др. Руководство по технологиям объединенных сетей Cisco. Изд. 4-е. – М.: Издательский дом «Вильямс», 2005. – 1040 с.: ил.

Продовження таблиці 3.1

Критерії	RIP	IGRP	OSPF	EIGRP
Максимальна кількість маршрутизаторів в мережі	15	255	65534	255
Підтримка IPv6	–	–	+	+
Доступність реалізації	Відкритость	Тільки на обладнанні Cisco	Відкритий	Тільки на обладнанні Cisco
Врахування у метриці різних характеристик	Одна основна	Комбінована	Одна основна і три додаткові	Комбінована
Оновлення маршрутної інформації	Вся таблиця	Вся таблиця	Тільки зміни	Тільки зміни

Порівняльна характеристика показує, що досконалими внутрішніми протоколами динамічної маршрутизації є OSPF і EIGRP. Але так як лабораторні роботи виконуються на обладнанні cisco, то найбільш раціональним є протокол EIGRP.

Причини:

1) Надійність і додаткові технічні переваги устаткування фірми Cisco Systems можуть зіграти вирішальну роль на користь побудови мережі. Тоді найбільший ефект дасть використання протоколу EIGRP.

2) Алгоритм DUAL піддається гнучкому налаштування (комбінована метрика, балансування навантаження шляхів з різними значеннями метрики), це дозволяє мережі забезпечувати її максимальну продуктивність, оскільки добре відомо, що перед мережею можуть ставитися найрізноманітніші завдання, і тільки великі функціональні можливості і гнучкість їх використання допоможуть вирішити будь-яке поставлене завдання.

4 РОЗРОБКА ЗАВДАНЬ ДО ЛАБОРАТОРНОГО ПРАКТИКУМУ

Лабораторним практикумом повинні бути охоплені наступні теми курсу «Комп’ютерні мережі»:

– Устаткування локальних мереж;

– Підмережі. Конфігурування маршрутизаторів;

– Статична маршрутизація в IP – мережах;

– Динамічна маршрутизація в IP – мережах;

Передбачається створення засобами емулятору Packet Tracer чотирьох завдань з зазначених тем лекційного курсу. Кожне завдання буде поділена на загальну практичну частину і індивідуальну частину для самостійної роботи. Практична частина – загальне завдання, яке треба виконати перед тим, як починати індивідуальну частину. В кожній частині студентам буде запропонована деяка логічна схема мережі (назвемо її віртуальний лабораторний стенд), яка складається з різних мережевих устаткувань. Студенти повинні провести конфігурацію цих пристроїв і домогтися працездатності мережі. В практичній частині лабораторної роботи буде наведений приклад подібної конфігурації. Виконуючи поетапно завдання цієї частини, студенти зможуть отримати необхідні практичні навички для виконання самостійної частини.

4.1 Віртуальний лабораторний стенд «Устаткування локальних мереж»

Практична частина лабораторної роботи представлена логічною схемою мережі, яка наведена на рис. 4.1. Мережа структурована за допомогою двох комутаторів Cisco. Студентам необхідно провести конфігурацію мережі, присвоїти ком’пютерам IP – адреси і за допомогою мережевих утиліт переконатися в її працездатності. Нижче наведений порядок виконання практичної частини.

1) Додати на робочу область програми 2 комутатора Switch-PT.

2) Додати 4 комп’ютера з іменами за замовчуванням PC0, PC1, PC2, PC3.

3) З’єднати устаткування в мережу Ethernet, як показано на рис.4.1.

4) Зберегти створену топологію, натиснувши кнопку Save (в меню File->Save).

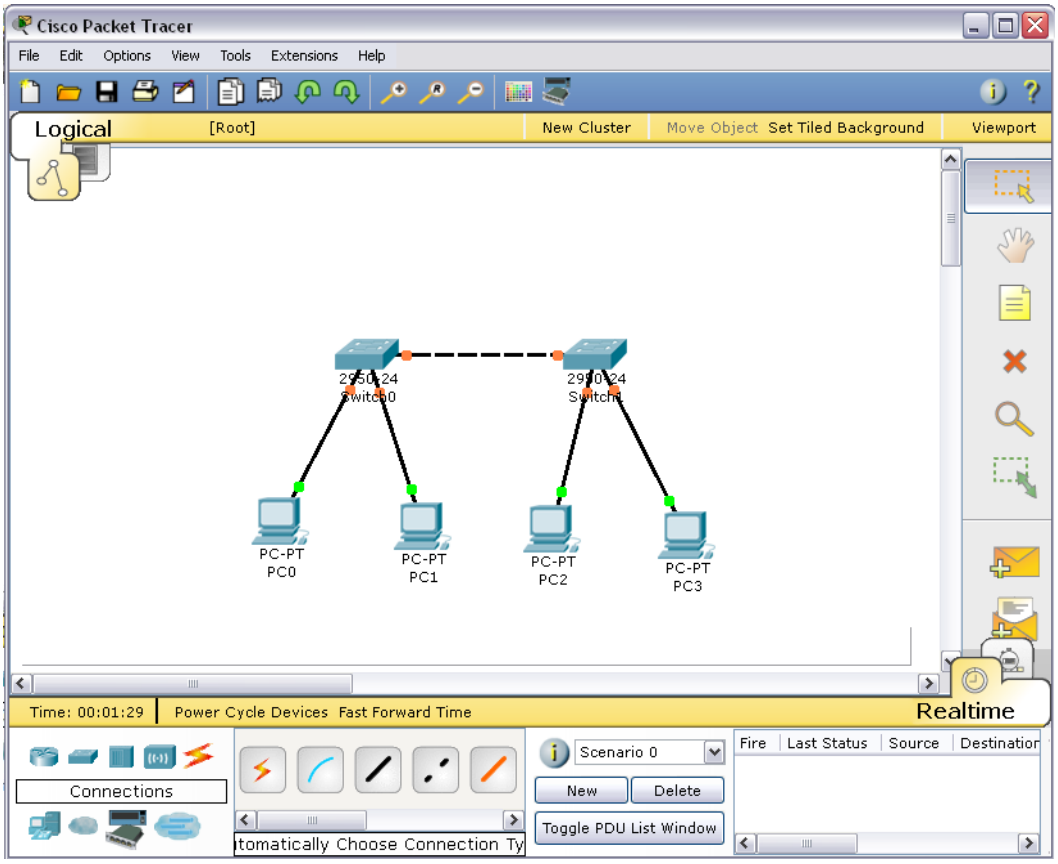

Рисунок 4.1 – Логічна топологія мережі для емуляції

5) Відкрити властивості устаткування PC0 натиснув на його зображені. Перейти до вкладки Desktop і виконати симуляцію роботи run натиснувши Command Prompt.

6) Для конфігурування комп’ютера слід скористатися командой ipconfig з командного рядка, наприклад, ipconfig 192.168.1.2 255.255.255.0

IP адресу і маску також можна вводити в графічному інтерфейсі устаткування (рис.4.2).

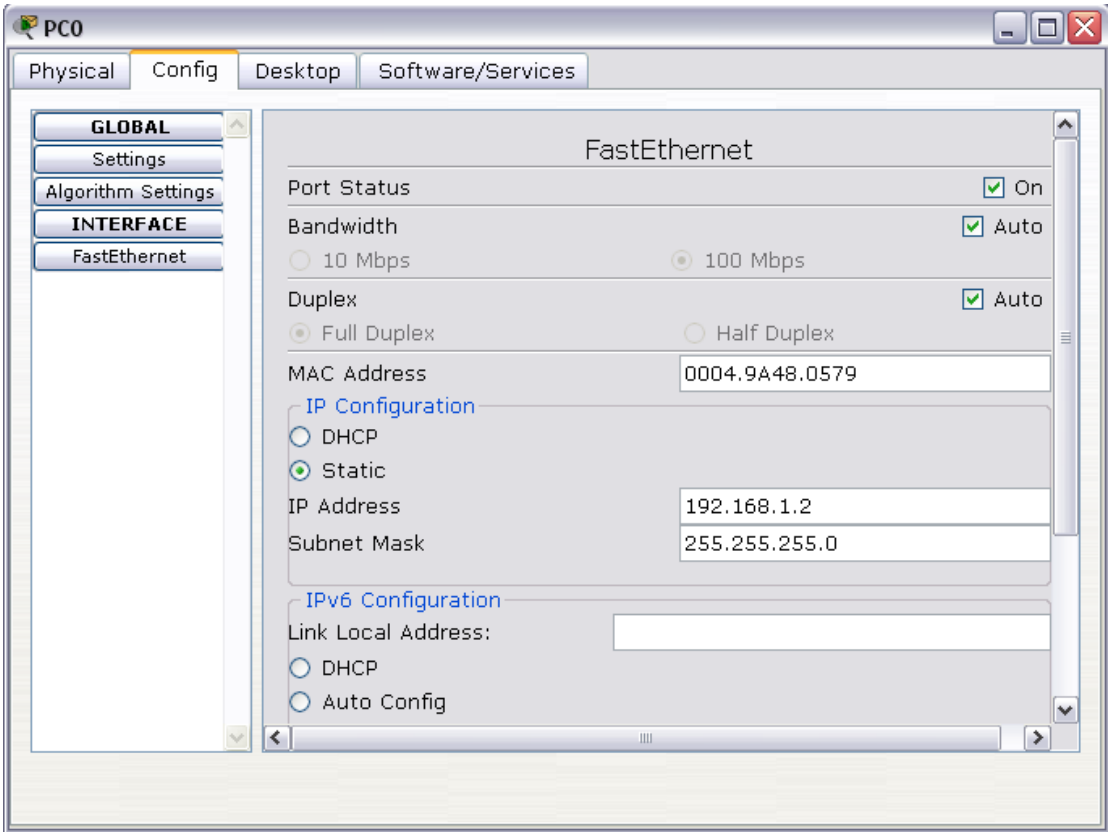

Рисунок 4.2 – Вкладка Config робочої станції PC0

7) На кожному комп'ютері переглянути назначені адреси командою ipconfig без параметрів.

8) Якщо всі пункти виконані вірно, то можна пропінгувати будь-який комп'ютер з будь-якого іншого комп'ютера. Наприклад, з комп'ютера PC3 виконати пінгування до комп'ютера PC0. Звіт про виконання команди ping наведений на рис.4.3.

В індивідуальній частині студентам необхідно реалізувати логічну структуру мережі, яка зображена на рис.4.4.

Потрібно створити запропоновану топологію, вибрав вірно мережеве устаткування і типи з'єднувального кабелю. Призначити комп'ютерам IP - адреси за допомогою командного рядка згідно варіанту. Якщо все буде зроблено вірно, то стане можливим пропінгувати будь-який комп'ютер з іншого.

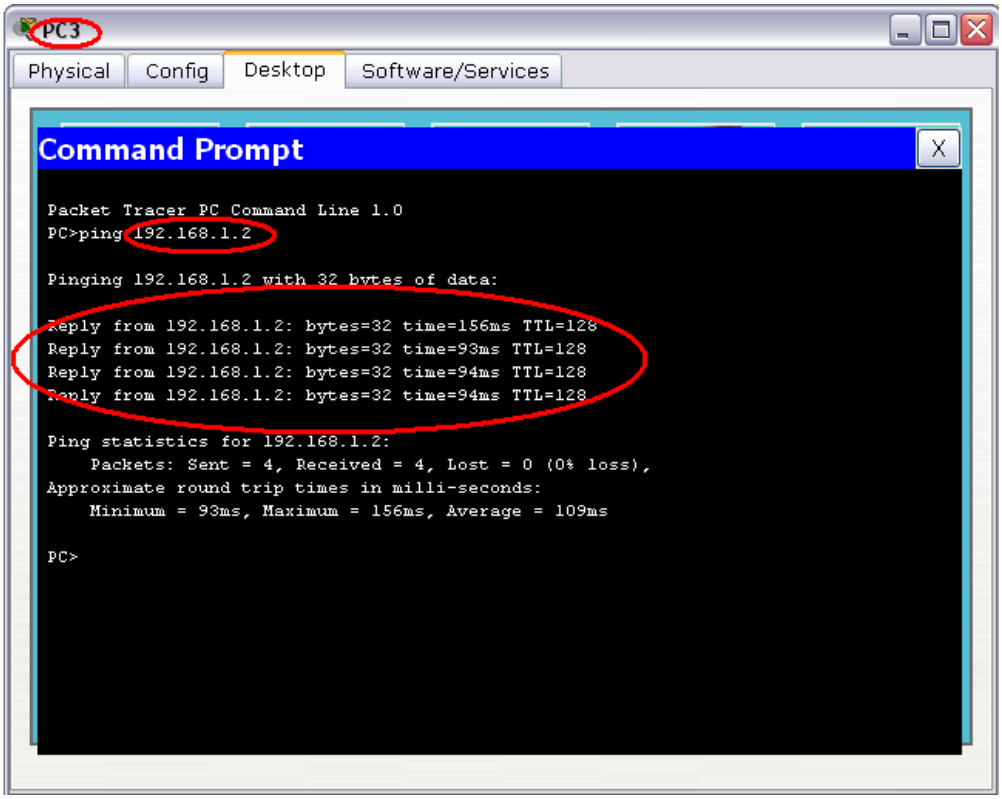

Рисунок 4.3 – Звіт про виконання команди ping між вузлами PC3 і PC0

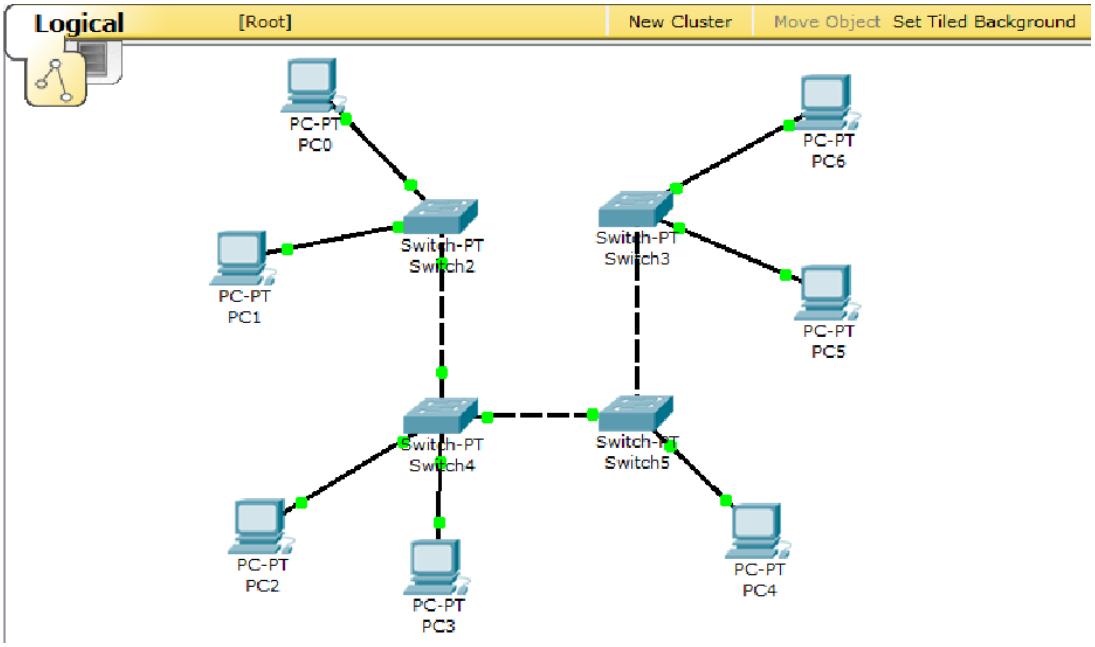

Рисунок 4.4 – Логічна топологія мережі для самостійної емуляції

5.2 Віртуальний лабораторний стенд «Підмережі. Конфігурування маршрутизаторів»

В лабораторній роботі виконавцям буде запропоновано створити складену мережу, тобто мережу, яка складається з декілька підмереж, що з'єднані маршрутизатором. Крім того, в мережі буде використаний DNS сервер, конфігурацію якого теж треба буде виконати. Введеня в мережу мережевого пристрою – маршрутизатора Cisco, потребує його конфігурації, яка здійснюється за допомогою командного рядка операційної системи IOS.

Для встановлення на мережевому інтерфейсі IP адреси використовується команда:

```
Router(config-if)#ip address [ip-address][subnet-mask],
Router(config-if)#no shut
```

Команда no shut (скорочення від no shutdown) використовується для того, щоб інтерфейс був активним.

Реалізуємо поділ мережі на підмережі. Нехай адміністратор виконав розбиття мережі 192.168.8.0/24 на 6 підмереж. Використовуючи адреси 4-х перших підмереж, представимо їх логічну структуру за допомогою програми. Адреси підмереж наведені в табл. 4.1. Для цього студентам слід виконати наступні дії:

1) Побудувати мережу з 4-ма підмережами (рис. 4.5).
2) Сконфігурувати стек протоколів кожного вузла мережі відповідно з даними табл.4.2.
3) Здійснити тестування мережі використовуючи команду ping.
4) Сконфігурувати DNS – сервер. Продемонструвати завантаження html сторінки з сервера в браузер будь-якого комп'ютера.

Порядок конфігурування маршрутизатора за допомогою CLI Cisco IOS в практичній частині лабораторної роботи наведений у додатку А.

Пропанується в рамках індивідуальної частини лабораторної роботи виконати наступні дії:

1) Розрахувати кількість підмереж згідно з індивідуальним варіантом.

2) Побудувати схему мережі згідно результатів попереднього розрахунку.

3) Сконфігурувати стек протоколів кожного вузла мережі.

Таблиця 4.1 – Адреси підмереж

Адреса мережі	Широкомовний адрес	Адреси хостів	
192.168.8.32	192.168.8.63	від 192.168.8.33	до 192.168.8.62
192.168.8.64	192.168.8.95	від 192.168.8.65	до 192.168.8.94
192.168.8.96	192.168.8.127	від 192.168.8.97	до 192.168.8.126
192.168.8.128	192.168.8.159	від 192.168.8.129	до 192.168.8.158

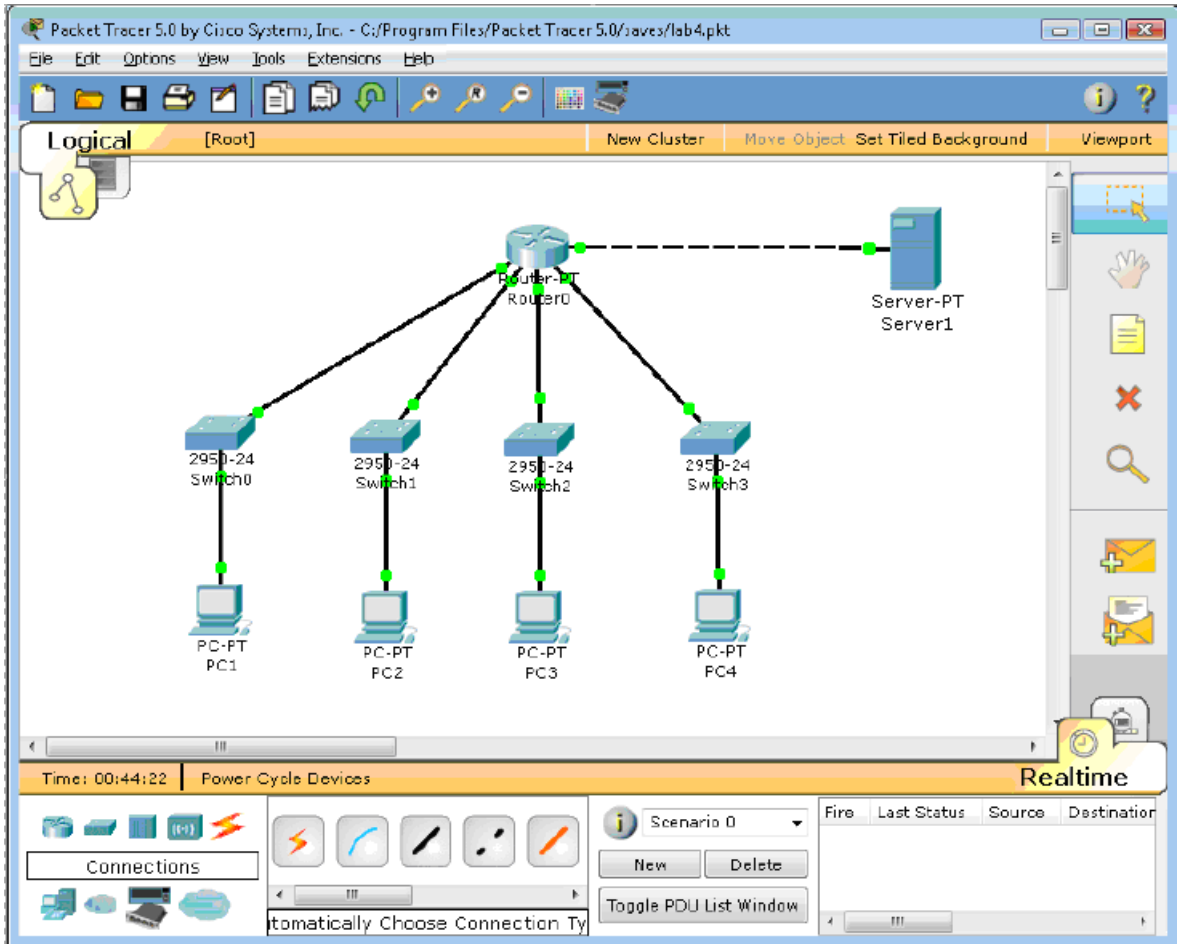

Рисунок 4.5 – Логічна топологія мережі з 4-ма підмережами

Таблиця 4.2 – Параметри стеку TCP/IP для вузлів мережі

Пристрій	IP-адреса	Маска	Шлюз
PC1	192.168.8.33	255.255.255.224	192.168.8.62
PC2	192.168.8.65	255.255.255.224	192.168.8.94
PC3	192.168.8.97	255.255.255.224	192.168.8.126
PC4	192.168.8.129	255.255.255.224	192.168.8.158
Server1	213.33.168.60	255.255.255.0	213.33.168.254
Router0(порт 0/0)	192.168.8.62	255.255.255.224	
Router0(порт 1/0)	192.168.8.94	255.255.255.224	
Router0(порт 6/0)	192.168.8.126	255.255.255.224	
Router0(порт 7/0)	192.168.8.158	255.255.255.224	
Router0(порт 8/0)	213.33.168.254	255.255.255.0	

4.3 Віртуальний лабораторний стенд «Статична маршрутизація»

Практична частина лабораторної роботи представлена логічною схемою мережі, яка наведена на рис. 4.6. Мережа складається з трьох маршрутизаторів Cisco. Студентам необхідно провести аналіз конфігурації мережі, присвоїти інтерфейсам маршрутизаторів IP – адреси, налаштувати статичну маршрутизацію і за допомогою мережевих утиліт переконатися в її працездатності.

Нижче наведений порядок виконання практичної частини.

1) Створіть в Packet Tracer топологію, зображену на рис.4.6.

2) Командою hostname змініть імена маршрутизаторів. Задайте конфігурацію їх інтерфейсів відповідно з рисунком. Увімкніть інтерфейси.

3) На маршрутизаторі Router1 введемо команду для виводу стану всіх інтерфейсів на яких працює CDP.

```
Router1#show cdp interface
```

4) Переконавшись, що мережевий пристрій посилає і одержує CDP-оновлення, можемо використовувати CDP для отримання інформації про безпосередньо підключені пристрої.

```
Router1#show cdp neighbors
```

5) Виконаємо команди ping і traceroute. Підключимося до пристрою Router1. Пропінгуємо безпосередньо приєднаний інтерфейс FastEthernet 0/0 на пристрої Router2

```
Router1# ping 10.1.1.2
```

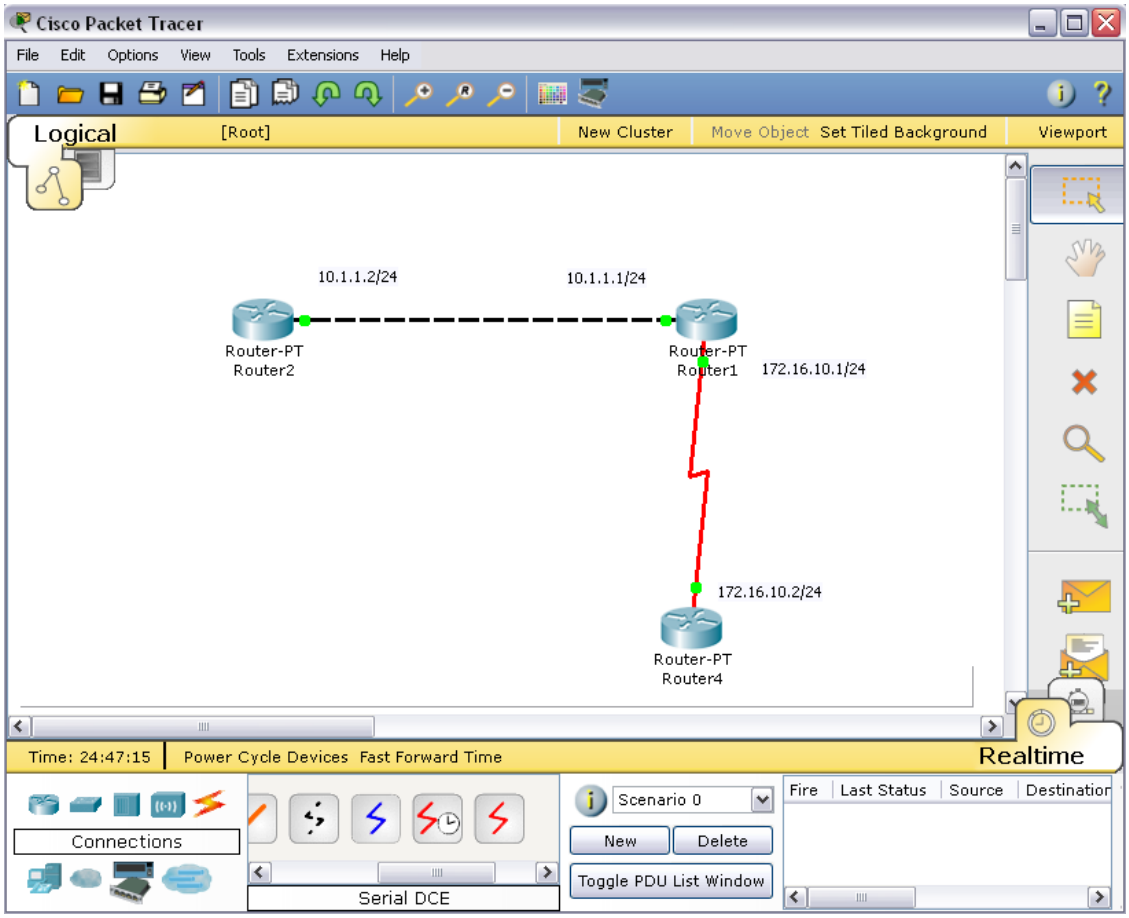

Рисунок 4.6 – Логічна топологія мережі для практичного завдання

6) Протокол ARP. Приєднайтеся до маршрутизатора Router1 і подивіться його ARP таблицю

```
Router1#show arp
```

7) Маршрутизація за замовчуванням. Мережеві пристрої Router2 і Router4 мають тільки по одному виходу у зовнішній світ: через інтерфейси з адресами 10.1.1.1 і 172.16.10.1, відповідно. Тому можна не визначати на які підмережі ми маршрутизуємо пакети і використовувати маршрутизацію за замовчуванням.

Спочатку видалимо старі маршрути

```
Router2(config)#no ip route 172.16.10.0 255.255.255.0 10.1.1.1
Router4(config)# no ip route 10.1.1.0 255.255.255.0 172.16.10.1
```

Далі призначимо маршрути за замовчуванням

```
Router2(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.1
Router4(config)# ip route 0.0.0.0 0.0.0.0 172.16.10.1
```

Подивіться таблицю маршрутів на всіх пристроях.

```
Router2#sh ip route
Router4#sh ip route
```

Всі мережеві інтерфейси в мережі пінгуються з кожного мережевого пристрою.

В індивідуальній частині студентам необхідно реалізувати логічну структуру мережі, яка зображена на рис.4.7. Провести конфігурацію обладнання і налаштувати статичну маршрутизацію.

Докладний план виконання індивідуального завдання представлений нижче:

1) Побудувати в Packet Tracer топологію, що представлена на рис. 4.7. Використовувати необхідні маршрутизатори. В мережі шість підмереж, кожний маршрутизатор підключений до трьох підмереж.

2) На кожному маршрутизаторі підійміть інтерфейси, що використовуються, і подивіться сусідів командою show cdp neighbors. Зробіть скріншот.

3) Призначте інтерфейсам мережі адреси згідно варіанту.

4) Перевірте факт призначення адрес шляхом виконання на кожному маршрутизаторі команд show running-config і show ip interface brief. Для комп’ютерів використовуйте команду ipconfig.

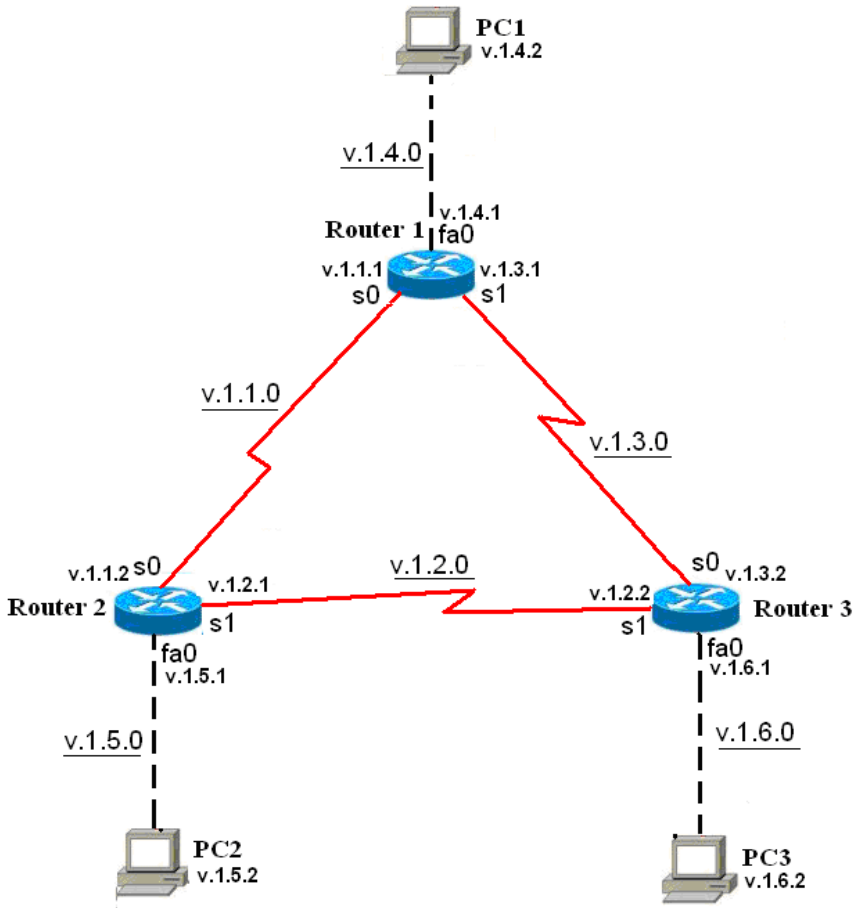

Рисунок 4.7 – Логічна структура мережі для виконання індивідуального завдання

5) Перевірте правильність призначення адрес шляхом виконання на кожному маршрутизаторі команд ping до безпосередніх сусідів.

6) Поставимо перед собою завдання зв’язати між собою комп’ютери PC1, PC2 і PC3. Для цього здійснимо на маршрутизаторах настройку статичної маршрутизації. В кожному маршрутизаторі пропишемо маршрути на віддалені Ethernet мережі. Для вирішення поставленого завдання маршрутизувати пакети на віддалені мережі послідовних з’єднань не треба.

У кожного маршрутизатора є по два маршруту на віддалені Ethernet мережі. Всього треба прописати шість статичних маршрутів.

Щоб з маршрутизатора Router1 досягти віддалену Ethernet мережу v.1.5.0/24, пакети можна направляти на IP адресу v.1.1.2 найближчого зовнішнього інтерфейсу на шляху в цю мережу. Це зробить команда

Router1(config)#ip route v.1.5.0 255.255.255.0 v.1.1.2

Задайте інші п’ять команд маршрутизації.

7) На кожному маршрутизаторі подивіться таблицю маршрутизації командою show ip route. Зробіть скріншоти.

8) На кожному маршрутизаторі зробить скріншоти розширених пінчів: на маршрутизаторі Router1 від PC2 до PC3, на маршрутизаторі Router2 від PC1 до PC3, на маршрутизаторі Router3 від PC1 до PC2

Наприклад, результат розширеного пінгу на маршрутизаторі Router1 від PC2 до PC3 для варіанта 12 (v=12) має вигляд:

```
Router1#ping
Protocol [ip]:
Target IP address: 12.1.6.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 12.1.5.2
% Invalid source
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.1.6.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 62/62/63 ms
```

9) На кожному комп’ютері зробіть скріншоти виконання команд трасіровкі tracert інших комп’ютерів. Всього шість скріншотів. Наприклад, трасіровка з PC1 на PC2 для варіанта 12 (v=12)

```
PC>tracert 12.1.5.2
Tracing route to 12.1.5.2 over a maximum of 30 hops:
  1   17 ms     31 ms     32 ms     12.1.4.1
  2   47 ms     63 ms     63 ms     12.1.1.2
  3   94 ms     94 ms     78 ms     12.1.5.2
Trace complete.
```

4.4 Віртуальний лабораторний стенд «Динамічна маршрутизація»

Метою даної лабораторної роботи є знайомство з протоколом маршрутизації EIGRP.

Протокол EIGRP – це високопродуктивний протокол маршрутизації на основі векторів відстані, порівняно нескладний при налаштуванні базових мереж.

В ході даної лабораторної роботи треба:

1) Побудувати мережу і перевірити з'єднання.
2) Налаштувати маршрутизацію EIGRP.
3) Перевірити маршрутизацію EIGRP.
4) Змінити пропускну здатність і налаштувати пасивний інтерфейс, щоб підвищити ефективність роботи EIGRP.

Топологія складається з трьох маршрутизаторів Cisco 1941 трьох комутаторів Cisco 2960 і трьох вузлів, які використовують тільки порти Ethernet (рис. 4.8).

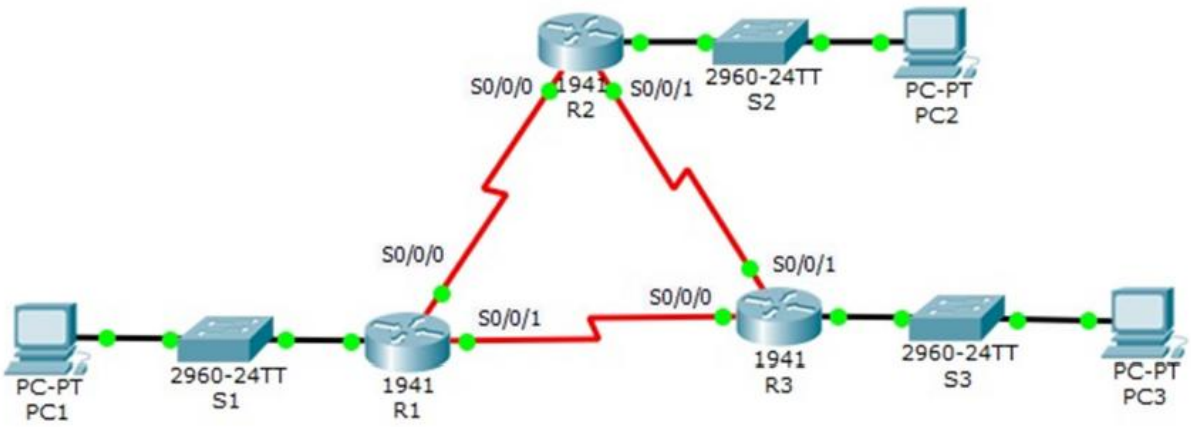

Рисунок 4.8 – Топологія мережі до лабораторної роботи «Динамічна маршрутизація»

Після виконання лабораторної роботи студенту необхідно відповісти на контрольні питання, а так само закріпити свої знання оформленням звіту.

ВИСНОВКИ

Метою кваліфікаційної роботи була розробка завдань до лабораторного практикуму з дисципліни «Комп'ютерні мережі» засобами програмного емулятору IP мереж.

В ході виконання роботи був проведений порівняльний аналіз сучасних мережевих емуляторів і пакетів імітаційного моделювання. Основними вимогами за якими проводився вибір були: простота використання, інтуїтивно зрозумілий інтерфейс і можливості установки і придбання пакету. За всіма цим вимогами був обраний пакет Cisco Packet Tracer.

Пакет призначений для роботи з обладнанням фірми Cisco – світового лідеру у галузі мережних технології. Фірма відома своїми високопродуктивними маршрутизаторами, комутаторами та іншим устаткуванням. Як показує аналіз ринку, все більше компаній і підприємств обирають для впровадження саме обладнання Cisco, тому вивчення їх компонентів і вбудованої операційної системи IOS слід вважати дуже перспективним і доцільним для майбутнього IT спеціаліста. В роботі наводиться опис основних компонентів Cisco маршрутизаторів і операційної системи IOS. Крім того, емулятор Packet Tracer має вбудовані засоби Activity Wizard, які дозволяють створювати шаблони мереж для подальшого конфігурування і виконання різних навчальних сценаріїв.

В роботі була розроблена структура лабораторного практикуму, що складається з четирьох частин, які базуються на темах: «Устаткування локальних мереж», «Підмережі. Конфігурування маршрутизаторів», «Статична маршрутизація», «Динамічна маршрутизація». Кожна робота складається з теоретичної, практичної і індивідуальної частин. По кожній роботі розроблений віртуальний лабораторний стенд вбудованими засобами Activity Wizard.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cisco Packet Tracer// Офіційний сайт. URL: https://www.netacad.com/ru/courses/packet-tracer (дата звернення: 27.02.2019)

2. Boson NetSim// Офіційний сайт. URL:http://www.boson.com/netsim-cisco-network-simulator (дата звернення: 27.02.2019)

3. Boson NetSim 12. User Manual. URL:http://www.boson.com/Files/Support/NetSim-12-User-Manual.pdf дата звернення: 27.02.2019)

4. GNS3/Dynamips// Офіційний сайт. URL: https://www.gns3.com/ (дата звернення: 27.02.2019)

5. CCNA Security 1.0 Student Packet Tracer Manual. URL: http://www.scribd.com/doc/25536606/CCNA-Security-Student-Packet-Tracer-Manual (дата звернення: 27.02.2019)

6. Software Oracle VM VirtualBox. URL: http://download.virtualbox.org/virtualbox/UserManual.pdf (дата звернення: 27.02.2019)

7. Software VMware Workstation. URL: http://www.vmware.com/ (дата звернення: 27.02.2019)

8. RIP Version 2 protocol. URL: http://muff.kiev.ua/files/books/2453_RIPv2.pdf (дата звернення: 27.02.2019)

9. An Introduction to IGRP. Cisco Systems, Inc. URL: https://ru.scribd.com/document/75310948/An-Introduction-to-IGRP (дата звернення: 27.02.2019)

10. An Introduction to EIGRP. Cisco Systems, Inc. URL: https://ru.scribd.com/document/20190928/Introduction-to-EIGRP (дата звернення: 27.02.2019)

11. An Introduction to OSPF protocol URL: https://ru.scribd.com/document/23941805/Introduction-to-OSPF (дата звернення: 27.02.2019)

12. Джером Ф. Димарцио. Маршрутизаторы Cisco. Пособие для самостоятельного изучения – М: Издательство «Символ-Плюс», 2003. – 508 с.: ил.

13. Аллан Леинванд, Брюс Пински. Конфигурирование маршрутизаторов Cisco. 2 издание. – М.: Издательский дом «Вильямс», 2001. – 368 с.: ил.

14. Джо Хабракен. Как работать с маршрутизаторами Cisco. – СПб.: Издательство «ДМК-Пресс», 2005. – 317 с.: ил.

15. Вито Амато. Основы организации сетей Cisco. Том2 – М.: Издательский дом «Вильямс», 2004. – 464 с.: ил.

16. Брюс Александер, Тони Аллен, Матт Карлинг и др. Руководство по технологиям объединенных сетей Cisco. Изд. 4-е. – М.: Издательский дом «Вильямс», 2005. – 1040 с.: ил.

Д О Д А Т К И

Додаток А

Конфігурування маршрутизатора за допомогою CLI Cisco IOS

Для вибору мережевого пристрою Router0 натисніть в робочій області програми на його зображення. Відкриється вікно настройок мережевого пристрою. Вибираємо вкладку CLI для керування маршрутизатором.

1) В середині екрану ви побачити:

Continue with configuration dialog? [yes/no]:

Введіть “no” і натисніть клавішу <Enter>.

З’явиться запрошення виду:

Router>

Це означає, що ви підключені до мережевого пристрою і знаходитесь в командному рядку режиму користувача. Тут “Router” – це і’мя мережевого пристрою, а “>” позначає режим користувача.

2) Далі введіть команду enable, щоб потрапити в привілейований режим.

Router> enable

Router#

3) Перегляньте список доступних команд в привілейованому режимі:

Router#?

4) Перейдемо в режим конфігурації:

Router# config terminal

Router(config)#

5) Ім’я хосту мережевого пристрою використовується для локальної ідентифікації. Коли ви входите до мережевого пристрою, ви бачите ім’я хосту перед символом режиму (“>” або “#”). Це ім’я може бути використано для визначення місця знаходження. Встановіть “ Router0” как ім’я вашого мереженого пристрою.

Router(config)# hostname Router0

Router0(config)#

6) Пароль доступу дозволяє контролювати доступ в привілейованому режимі. Це дуже важливий пароль, тому що в привілейованому режимі можна вносити зміни в конфігурації пристрою. Встановіть пароль доступу “cisco”

Router0(config)#enable password cisco

7) Випробуємо цій пароль. Вийдіть з мережевого пристрою і спробуйте зайти в привілейований режим:

Router0>en

Password:*****

Router0#

Тут знаки: ***** - це ваш введений пароль. Ці знаки на екрані не видно.

Основні Show команди

Перейдіть до контексту користувача командою disable. Введіть команду для перегляду всіх доступних show команд.

Router0>show ?

1) Команда show version використовується для отримання типу платформи мережевого пристрою, версії операційної системи, імені файлу образу операційної системи, часу роботи системи, об’єму пам’яті, кількості інтерфейсів і регістру конфігурації.

2) Можна побачити часи

Router0>show clock

3) Во флеш-пам’яті мереженого пристрою зберігається файл-образ операційної системи Cisco IOS. На відміну від операційної пам’яті, в реальних устаткуваннях флеш-пам’ять зберігає файл-образ навіть при збої живлення.

Router0>show flash

4) Інтерфейс командного рядка мереженого пристрою за замовчуванням зберігає 10 останніх введених команд

Router0>show history

5) Дві команди дозволяють повернуться до команд, що були введені раніше. Натисніть на стрілку вгору або <ctrl>P.

6) Дві команди дозволяють перейти до наступної команди, яка зберігається в буфері. Натисніть на стрілку вниз або <ctrl>N.

7) Можна побачити список хостів і IP-адреси всіх їх інтерфейсів:

Router0>show hosts

8) Наступна команда виводить детальну інформацію про кожний інтерфейс:

Router0>show interfaces

9) Команда

Router0>show sessions

Виведе інформацію про кожну telnet сесію.

10) Команда

Router0>show terminal

показує параметри конфігурації терміналу.

11) Список всіх користувачів, що приєднані до пристрою по термінальним лініям можна побачити використовуючи команду:

Router0>show users

12) Команда

Router0>show controllers

показує стан контролерів інтерфейсів.

13) Перейдемо до привілейованого режиму

Router0>en

14) Введіть команд для перегляду всіх доступних show команд.

Router0# show ?

Привілейований режим включає до себе всі show команди контексту користувача і ряд нових.

15) Подивимося активну конфігурацію в пам’яті мереженого пристрою.

Router0# show running-config

Активна конфігурація автоматично не зберігається і буде втрачена в разі збою живлення. Для продовження перегляду наступної сторінки конфігурації натисніть на клавішу пробіл.

16) Наступна команда дозволяє переглянути поточний стан протоколів третього рівня

Router0# show protocols

Конфігурація інтерфейсів

Розглянемо команди, які дозволяють вмикати (піднімати) інтерфейси мережевого пристрою та переводити їх в стан UP.

1) На мережевому пристрої Router0 увійдемо в контекст конфігурації

Router0#conf t

Router0(config)#

2) Щоб настроїти Ethernet інтерфейс, треба зайти в контекст конфігурації інтерфейсу:

Router0(config)#interface FastEthernet 0/0

Router0(config-if)#

3) Переглянемо усі доступні в цьому контексті команди

Router0(config-if)#?

Для виходу в контекст глобальної конфігурації наберіть exit. Знову увійдіть в контекст конфігурації інтерфейсу:

Router0(config)#int fa0/0

Ми використали скорочене ім’я інтерфейсу.

4) Встановимо IP адресу Ethernet інтерфейсу

Router0(config-if)#ip address 192.168.8.62 255.255.255.224

5) Увімкнемо цей інтерфейс

Router0(config-if)#no shutdown

6) Додамо до інтерфейсу опис:

Router0(config-if)#description Ethernet interface on Router 0

Щоб побачити опис цього інтерфейсу, перейдіть в привілейований режим і виконайте команду show interface.

Router0(config-if)#end

Router0# show interface

7) Після того, як виконано конфігурування усіх інтерфейсів можна переглянути активну конфігурацію пристрою і переконатися, що з’явилися призначені IP - адреси

Router0# show running-config

8) Перегляньте детальну IP інформацію про кожний інтерфейс та переконайтеся, що інтерфейси, що були сконфігуровані, перейшли до стану UP

Router0# show ip interface

Коротку інформацію можна отримати командою show ip interface brief

Router0# show ip in bri

```
Interface        IP-Address      OK? Method          Status         Protocol
FastEthernet0/0  194.138.33.62    YES manual up               up
FastEthernet1/0  194.138.33.94    YES manual   up               up
Serial2/0         unassigned      YES unset  administratively down   down
Serial3/0         unassigned      YES unset  administratively down   down
FastEthernet4/0   unassigned      YES unset                   down     down
FastEthernet5/0   unassigned      YES unset  administratively down   down
FastEthernet6/0   194.138.33.126  YES manual   up               up
FastEthernet7/0   194.138.33.158  YES manual   up               up
FastEthernet8/0   213.33.168.254  YES manual   up               up
FastEthernet9/0    unassigned     YES unset  administratively down   down
```

Додаток Б

Приклад завдання для тестування знань студентів

Для виконання тестового завдання було створена мережу для тренування вміння виконувати розподіл мережі на підмережі (subnetting) і визначення базових правил маршрутизації (рис.Б.1).

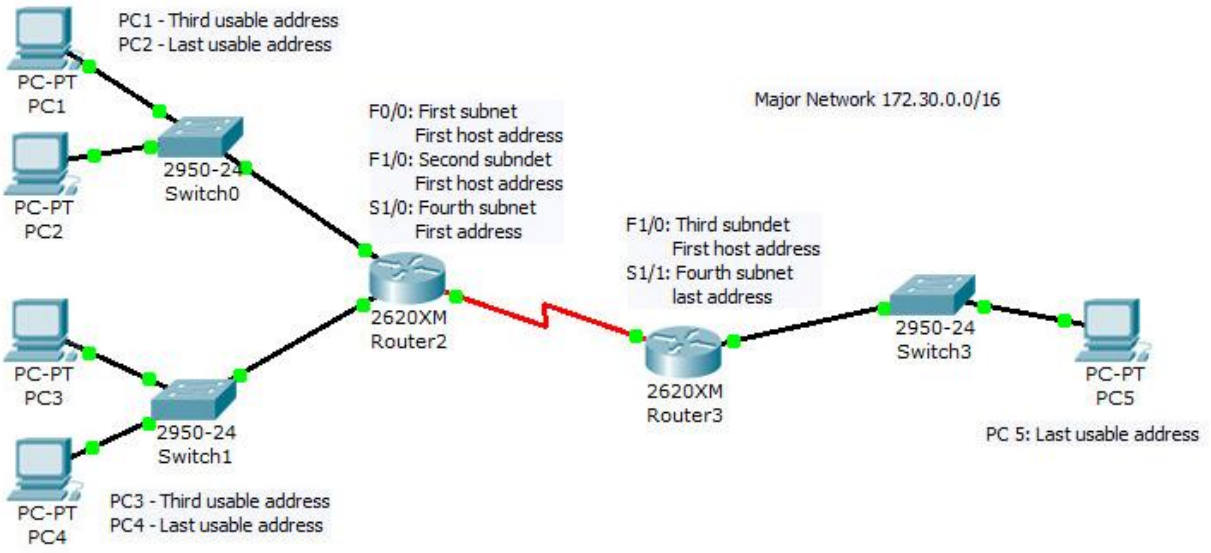

Рисунок Б.1. – Логічна топологія мережі для тестування

У даній топології студентам запропоновано розбити мережу 172.30.0.0/16 на 4 підмережі і відповісти на супутні питання. На самій топології додано декілька текстових блоків, що пояснюють, які саме IP адреси з підмереж слід привласнити кінцевим станціям і інтерфейсам маршрутизаторів.

Самі маршрутизатори повинні бути налаштовані по повній програмі, що включає основний набір заходів безпеки, у вигляді паролів на консольний і мережевий інтерфейси і т.п. – цю звичку треба виробляти у студентів з самого початку.

Інструкції до завдання мають такий вигляд:

Разделение на подсети (subnetting) и маршрутизация по умолчанию (default route)

В этом упражнении вы потренируетесь:

- Разделять сеть на подсети
- Производить базовую конфигурацию маршрутизатора
- Конфигурировать маршрут по умолчанию

Этап 1 – Разделение сети на подсети

Ответьте на следующие вопросы:

1. Сколько сетей существует на топологии?
2. Какая маска подсети подойдет к данной топологии?

Используйте сеть 172.30.0.0/16 для разделения на подсети с помощью выбранной маски подсети.

1. LAN 1 должен использовать первую подсеть.
2. LAN 2 должен использовать вторую подсеть.
3. LAN 3 должен использовать третью подсеть.
4. WAN 1 должен использовать четвертую подсеть.
5. Присвойте всем LAN интерфейсам обоих маршрутизаторов первый годный к употреблению IP адрес в соответствующей подсети.
6. Присвойте интерфейсу S1/0 маршрутизатора Router 2 первый годный к употреблению IP адрес подсети WAN.
7. Присвойте интерфейсу S1/1 маршрутизатора Router 3 последний годный к употреблению IP адрес подсети WAN.
8. Присвойте конечной станции PC1 третий годный к употреблению IP адрес в соответствующей подсети.
9. Присвойте конечной станции PC2 последний годный к употреблению IP адрес в соответствующей подсети.
10. Присвойте конечной станции PC3 третий годный к употреблению IP адрес в соответствующей подсети.
11. Присвойте конечной станции PC4 последний годный к употреблению IP адрес в соответствующей подсети.
12. Присвойте конечной станции PC5 последний годный к употреблению IP адрес в соответствующей подсети.

Этап 2 – базовая конфигурация маршрутизатора

1. Присвойте маршрутизаторам имена R2 и R3 в соответствии с топологией.
2. Установите пароль class на консольное соединение.
3. Установите зашифрованный пароль cisco на привилегированный доступ к маршрутизатора.
4. Установите пароль telnet на соединение telnet.
5. Все пароли должны быть зашифрованы.
6. Сконфигурируйте интерфейсы F0/0 ,F1/0 и S1/0 для маршрутизатора Router 2 в соответствии с выбранными вами адресами.
7. Сконфигурируйте интерфейсы F1/0 и S1/1 для маршрутизатора Router 3 в соответствии с выбранными вами адресами.
8. Сконфигурируйте частоту синхронизации в 4000000 bps на маршрутизаторе Router 2 и установите протокол ppp для серийных интерфейсов на обоих маршрутизаторах.
9. Присвойте всем конечным станциям IP адреса в соответствии с выбранной схемой.

Этап 3 – проверка

1. Выполните ping с конечной станции PC1 к станции PC2? Был ли ping успешным?
2. Выполните ping с конечной станции PC1 к станции PC3? Был ли ping успешным?
3. Выполните ping с конечной станции PC1 к станции PC5? Был ли ping успешным? Какое сообщение вы получили? Объясните, почему оно было получено?

Этап 4 – маршрутизация

1. Сконфигурируйте статическую маршрутизацию на Router 2. Снова попробуйте выполнить ping с конечной станции PC1 к станции PC5? Какое сообщение получено на этот раз? Какова разница между этим и прошлым сообщениями?
2. Сконфигурируйте статическую маршрутизацию на Router 3. Снова попробуйте выполнить ping с конечной станции PC1 к станции PC5? Был ли ping успешным?
3. Проверьте, что все конечные станции всех сетей доступны со всех остальных станций.

Удачи.

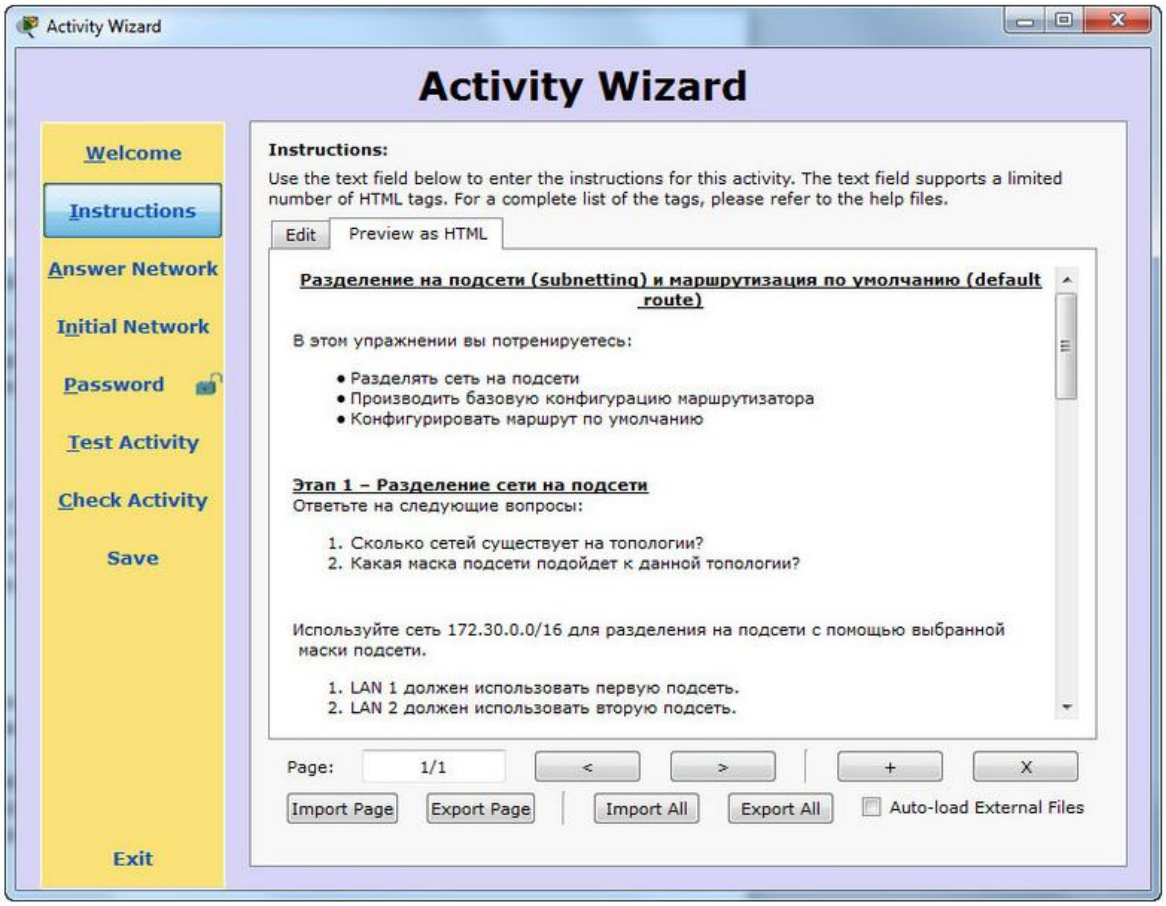

Рисунок Б.2 – Вигляд завдання в окні Activity Wizard

Вид розробленого тестового завдання в пакеті Packet Tracer зображений на рис. Б.3. Під час виконання завдання студенти можуть використовувати інструкції, які з’являються в окремому вікні. По кнопці Reset Activity можна обнулити всі вже проведені настройки і повернутися до початкового стану мережі. Кнопка Check Result дозволяє студенту або викладачеві переглянути які налаштування були виконані вірно і загальну кількість набраних балів за виконання завдання (рис.Б.4).

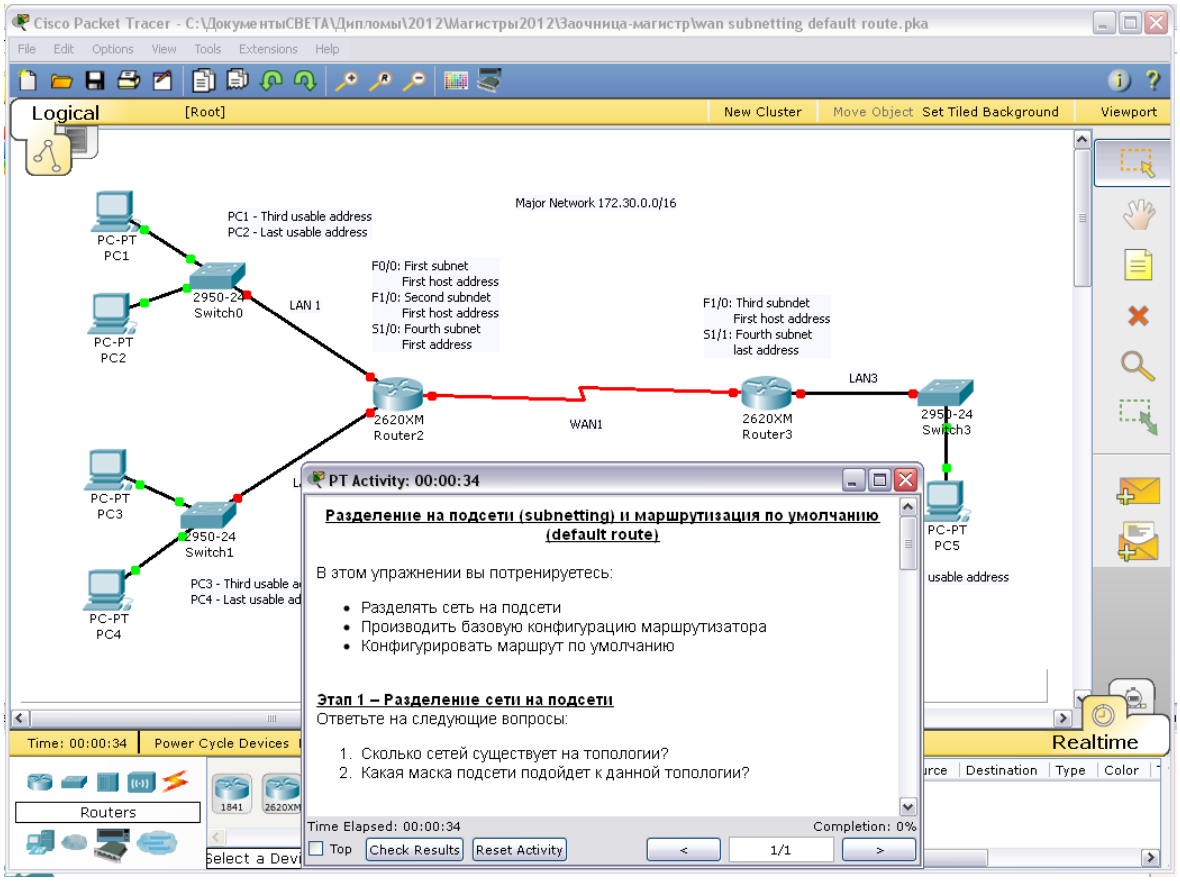

Рисунок Б.3 – Вид тестового завдання при роботі з емулятором

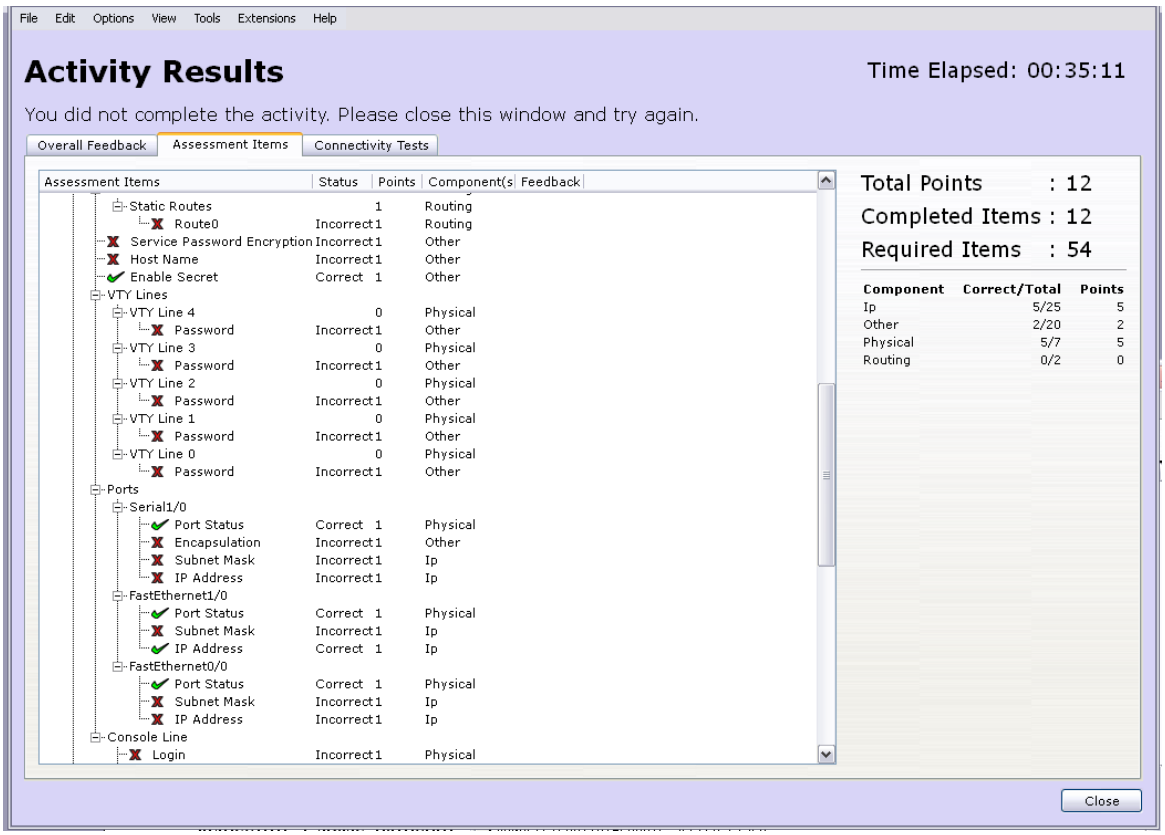

Рисунок Б.4 – Вікно Activity Result