МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
УМАНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Факультет економіки, підприємництва та інформаційних технологій

Кафедра інформаційних технологій

Допущено до захисту
"_____" _____ 2026 р.
Зав. кафедри, к.т.н., доцент
_____ Ліщук Р.І.

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

РОЗРОБКА ДОДАТКУ ДЛЯ АВТОМАТИЗАЦІЇ КОНФІГУРУВАННЯ СПИСКІВ ДОСТУПУ НА МЕРЕЖЕВОМУ ОБЛАДНАННІ CISCO

Виконав – студент 4 курсу, групи 41 з-кн
освітньої програми "Комп'ютерні науки"
спеціальності 122 Комп'ютерні науки
Смілянець Валентин Олександрович

Науковий керівник – к.е.н., доцент
Концеба Сергій Михайлович

Умань – 2026

Реферат
на кваліфікаційну роботу "Розробка додатку для автоматизації конфігурування списків доступу на мережевому обладнанні Cisco"
студента факультету економіки, підприємництва та інформаційних технологій
Уманського національного університету
Смілянця Валентина Олександровича

Структура та обсяг роботи. Пояснювальна записка кваліфікаційної роботи складається з трьох розділів, містить 61 сторінку, 34 рисунки, 1 додаток, 44 джерела наукової літератури.

Метою роботи є розробка веборієнтованого додатку для автоматизації конфігурування розширених списків контролю доступу на мережевому обладнанні Cisco та перевірка його працездатності в середовищі моделювання комп'ютерних мереж.

У першому розділі проаналізовано базові відомості про списки контролю доступу, функціонал ACL та ідентифікація списків контролю доступу. Здійснено постановку задач з розробки додатку для автоматизації конфігурування списків доступу на мережевому обладнанні Cisco.

У другому розділі здійснено моделювання мережі з використанням емулятора Cisco Packet Tracer

У третьому розділі розроблено графічний інтерфейс у вигляді веб-сторінки з використанням мови програмування JavaScript, а також технологій HTML, CSS. В інтерфейсі можливо згенерувати код налаштування розширених списків контролю доступу після введення вхідних даних.

Анотація

Розроблено графічний інтерфейс у вигляді веб-сторінки з використанням мови програмування JavaScript, а також технологій HTML, CSS. В інтерфейсі можливо згенерувати код налаштування розширених списків кон-тролю доступу після введення вхідних даних. Інтерфейс було протестовано у емульованій комп'ютерній мережі в Cisco Packet Tracer.

Ключові слова: списки контролю доступу, роутер, Cisco Packet Tracer, комп'ютерна мережа, графічний інтерфейс.

Annotation

A graphical interface in the form of a web page has been developed using the JavaScript programming language, as well as HTML and CSS technologies. The interface can generate code for configuring extended access control lists after entering input data. The interface was tested in an emulated computer network in Cisco Packet Tracer.

Keywords: access control lists, router, Cisco Packet Tracer, computer network, graphical interface.

ЗМІСТ

ВСТУП 4

РОЗДІЛ 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧ ДОСЛІДЖЕННЯ 7

1.1. Базові відомості про списки контролю доступу 7

1.2. Функціонал ACL 9

1.3. Ідентифікація списків контролю доступу 14

1.4. Постановка задачі 22

РОЗДІЛ 2 МОДЕЛЮВАННЯ МЕРЕЖІ З ВИКОРИСТАННЯМ ЕМУЛЯТОРА CISCO PACKET TRACER 25

2.1. Емулятор Cisco Packet Tracer 25

2.2. Створення топології мережі на базі емулятора Packet Tracer 27

2.3. Конфігурація розширених списків доступу в емуляторі Cisco Packet Tracer 29

РОЗДІЛ 3 ІНФОРМАЦІЙНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ГРАФІЧНОГО ІНТЕРФЕЙСУ НАЛАШТУВАННЯ РОЗШИРЕНИХ СПИСКІВ КОНТРОЛЮ ДОСТУПУ 42

3.1. Розробка графічного інтерфейсу з використанням мови програмування JavaScript та технологій HTML і CSS 42

3.2. Огляд функціоналу розробленої веборієнтованої системи 44

3.3 Тестування графічного інтерфейсу в емуляторі Cisco Packet Tracer 50

ВИСНОВКИ 57

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 59

ДОДАТКИ 62

ВСТУП

Сучасний етап розвитку інформаційних технологій характеризується стрімким зростанням кількості комп’ютерних мереж, підвищенням вимог до їх продуктивності, надійності та безпеки. Корпоративні мережі забезпечують функціонування інформаційних систем підприємств, установ та організацій, тому захист мережевої інфраструктури від несанкціонованого доступу є одним із пріоритетних завдань мережевого адміністрування. Одним із найпоширеніших механізмів реалізації політик безпеки на мережевому обладнанні Cisco є списки контролю доступу (Access Control Lists, ACL), які дозволяють здійснювати фільтрацію мережевого трафіку відповідно до встановлених правил.

Незважаючи на широке використання ACL у сучасних мережах, процес їх налаштування часто виконується вручну через командний рядок операційної системи Cisco IOS. Такий підхід вимагає від адміністратора глибоких знань мережевих технологій та синтаксису конфігураційних команд. Помилки під час створення правил можуть призвести до порушення роботи мережевих сервісів, втрати доступу до ресурсів або виникнення загроз інформаційній безпеці. У зв’язку з цим особливої актуальності набуває розробка програмних засобів, які дозволяють автоматизувати процес створення та налаштування списків контролю доступу.

Сучасні тенденції розвитку мережевих технологій передбачають активне впровадження засобів автоматизації та програмованого керування мережею. Використання веборієнтованих систем для формування конфігурацій мережевого обладнання дає змогу значно спростити процес адміністрування, скоротити час налаштування та мінімізувати ймовірність виникнення помилок. Саме тому розробка додатку для автоматизації конфігурування списків доступу на мережевому обладнанні Cisco є актуальним завданням, що має практичне значення для підвищення ефективності управління мережевою інфраструктурою.

Метою роботи є розробка веборієнтованого додатку для автоматизації конфігурування розширених списків контролю доступу на мережевому обладнанні Cisco та перевірка його працездатності в середовищі моделювання комп'ютерних мереж.

Для досягнення поставленої мети необхідно вирішити такі завдання**:**

- проаналізувати принципи побудови та функціонування списків контролю доступу на обладнанні Cisco;
- дослідити особливості використання стандартних і розширених ACL у корпоративних мережах;
- виконати моделювання мережевої інфраструктури підприємства в середовищі Cisco Packet Tracer;
- дослідити механізми налаштування та застосування розширених списків контролю доступу;
- обрати технології для реалізації веборієнтованого графічного інтерфейсу;
- розробити програмний засіб для автоматичного формування конфігурацій ACL;
- реалізувати механізми перевірки коректності введених користувачем даних;
- виконати тестування розробленої системи та оцінити правильність згенерованих конфігурацій;
- провести аналіз результатів роботи програмного засобу та визначити перспективи його подальшого розвитку.

Об'єктом дослідження є процес конфігурування та управління списками контролю доступу в корпоративних комп'ютерних мережах на базі обладнання Cisco.

Предметом дослідження є методи та засоби автоматизації створення розширених списків контролю доступу, а також програмна реалізація веборієнтованого інтерфейсу для генерації конфігурацій ACL.

У процесі виконання роботи використовувалися методи аналізу та синтезу інформаційних систем, моделювання комп’ютерних мереж, об’єктно-орієнтованого проєктування програмного забезпечення, а також методи тестування програмних продуктів. Для моделювання мережевої інфраструктури застосовано середовище Cisco Packet Tracer, а для розробки програмного засобу використано сучасні вебтехнології HTML5, CSS3 та JavaScript.

Практичне значення отриманих результатів полягає у створенні програмного засобу, який дозволяє автоматизувати процес формування конфігурацій ACL, скоротити час налаштування мережевого обладнання Cisco та зменшити ймовірність виникнення помилок під час адміністрування мереж. Розроблений додаток може бути використаний як навчальний інструмент для вивчення мережевих технологій Cisco, а також як допоміжний засіб для мережевих адміністраторів у процесі забезпечення мережевої безпеки.

РОЗДІЛ 1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧ ДОСЛІДЖЕННЯ

1.1 Базові відомості про списки контролю доступу

Списки контролю доступу (Access Control Lists, ACL) є одним із базових механізмів забезпечення безпеки комп'ютерних мереж. Під терміном ACL розуміють набір правил, які визначають умови дозволу або заборони передачі мережевого трафіку. Такі правила можуть ґрунтуватися на різних параметрах пакетів, зокрема IP-адресах джерела та призначення, номерах портів транспортного рівня, типах протоколів, а в окремих реалізаціях - іменах доменів або інших мережевих атрибутах. Основне призначення ACL полягає у фільтрації трафіку та реалізації політик інформаційної безпеки організації.

Технологія ACL є невід'ємною складовою програмного забезпечення мережевого обладнання Cisco IOS (Internetwork Operating System), яке використовується на маршрутизаторах і комутаторах компанії Cisco. Завдяки ACL адміністратори можуть контролювати доступ до мережевих ресурсів, обмежувати взаємодію між окремими сегментами мережі, а також підвищувати рівень захисту інформаційної інфраструктури від несанкціонованого доступу. Крім того, ACL широко застосовуються для реалізації вимог корпоративних політик безпеки та сегментації мережевого середовища.

Історично ACL належать до найстаріших механізмів мережевої фільтрації. Перші стандартні списки контролю доступу в Cisco IOS виконували перевірку пакетів виключно за IP-адресою відправника. Незважаючи на значний вік цієї технології, вона продовжує активно використовуватися завдяки простоті реалізації, високій продуктивності та інтеграції з мережевим обладнанням. Водночас сучасні мережі дедалі частіше використовують більш гнучкі засоби захисту, такі як міжмережеві екрани нового покоління (Next-Generation Firewall, NGFW), системи виявлення та запобігання вторгненням (IDS/IPS), а також механізми контролю доступу на основі ролей (RBAC) та політик безпеки.

Для розуміння важливості ACL необхідно розглянути загальний принцип передачі даних у мережі. Обмін інформацією між вузлами здійснюється шляхом передачі пакетів, кожен з яких містить корисне навантаження та службову інформацію, необхідну для маршрутизації. Після отримання пакета маршрутизатор виконує послідовність операцій:

1. Аналізує адресу призначення, зазначену в заголовку пакета.
2. Здійснює пошук відповідного запису в таблиці маршрутизації.
3. У разі знаходження маршруту пересилає пакет через відповідний вихідний інтерфейс.
4. Якщо відповідний маршрут відсутній, пакет відкидається.

За замовчуванням маршрутизатор приймає рішення про пересилання пакетів виключно на основі маршрутної інформації. Це означає, що будь-який вузол, який має можливість сформувати пакет із коректною адресою призначення, потенційно може надсилати трафік через мережеве обладнання. У випадках, коли така поведінка суперечить політиці безпеки організації, адміністратор може застосувати ACL для контролю доступу до окремих ресурсів або сегментів мережі. Після налаштування відповідних правил небажаний або потенційно небезпечний трафік буде автоматично блокуватися ще на етапі його проходження через мережевий пристрій.

Списки контролю доступу можуть застосовуватися не лише на маршрутизаторах і комутаторах, але й на серверах, міжмережевих екранах, шлюзах безпеки та інших мережевих пристроях. Багато сучасних технологій захисту інформації фактично базуються на концепції ACL або використовують її як складову частину власних механізмів фільтрації. Ефективність ACL значною мірою залежить від актуальності правил, тому в процесі експлуатації необхідно передбачати регулярний перегляд, оновлення та аудит списків контролю доступу. Особливо це актуально для великих корпоративних мереж, де зміна структури мережі або поява нових сервісів потребують оперативного коригування політик доступу [2].

Слід зазначити, що концепція ACL виникла задовго до появи сучасних комп’ютерних мереж. Однією з перших реалізацій подібного механізму вважається файлова система операційної системи Multics, розроблена у 1965 році. У подальшому ідея списків контролю доступу була адаптована до різних операційних систем, зокрема UNIX, Windows та Linux, де ACL використовуються для керування правами доступу до файлів, каталогів та інших системних ресурсів. Таким чином, ACL є універсальним механізмом контролю доступу, який знайшов застосування як у мережевих технологіях, так і в системах керування ресурсами операційних систем.

Сьогодні ACL залишаються важливим елементом багаторівневої архітектури кібербезпеки. Незважаючи на появу більш складних механізмів захисту, вони продовжують виконувати роль першого рубежу контролю мережевого трафіку, забезпечуючи ефективне обмеження доступу до ресурсів та зменшення поверхні атаки інформаційних систем.

1.2 Функціонал ACL

Операційна система Cisco IOS містить розвинений набір інструментів для реалізації контролю доступу до мережевих ресурсів за допомогою списків контролю доступу (Access Control Lists, ACL). Завдяки широким можливостям налаштування ACL можуть використовуватися як для простих завдань фільтрації трафіку, так і для реалізації складних політик безпеки в корпоративних мережах. Після аналізу та класифікації мережевого трафіку ACL визначає подальшу долю кожного пакета: дозволити його проходження, заборонити передачу або застосувати додаткові дії залежно від конфігурації пристрою.

Списки контролю доступу використовуються в багатьох мережевих технологіях і службах. Основними сферами їх застосування є:

- пакетна фільтрація трафіку на мережевих інтерфейсах;

• обмеження адміністративного доступу до маршрутизаторів через Telnet або SSH;

• визначення трафіку, який необхідно шифрувати під час використання VPN;

• класифікація пакетів для механізмів забезпечення якості обслуговування (Quality of Service, QoS);

• визначення адрес, які підлягають трансляції засобами Network Address Translation (NAT);

• контроль доступу до мережевих сервісів і серверів;

• сегментація мережі та реалізація політик мікросегментації;

• захист від несанкціонованих підключень і окремих типів мережевих атак.

Особливий інтерес для даного дослідження становить застосування ACL для пакетної фільтрації. Саме цей функціонал використовується при реалізації графічного інтерфейсу керування списками доступу. Для забезпечення фільтрації необхідно спочатку створити ACL із відповідними правилами, а потім прив'язати його до конкретного інтерфейсу маршрутизатора. Після активації списку доступу весь мережевий трафік, що проходить через даний інтерфейс, буде перевірятися відповідно до визначених правил [4].

ACL можуть застосовуватися як до вхідного (inbound), так і до вихідного (outbound) трафіку. Напрямок перевірки визначається під час прив'язки списку доступу до інтерфейсу. Загальний формат відповідної команди в Cisco IOS має вигляд:

Router(config-if)# {protocol} access-group {номер ACL} {in | out} [5].

Наприклад, ви хочете відправити певний запит з приватної мережі в ISP (Internet) (рис. 1.1). Спочатку маршрутизатор визначить, чи є ACL на інтерфейсі fa0/1. Якщо є, то обробка відправленого пакету буде вестись згідно з правилами цього списку доступу, в результаті йому або буде дозволено відправитись на вихідний інтерфейс fa0/0, або пакет буде видалено. Те ж саме на інтерфейсі fa0/0, якщо пакет успішно потрапив на нього, спочатку відбувається пошук ACL, у

випадку його відсутності пакет відсилається в ISP, у випадку наявності, за результатом перевірки пакет або видаляється, або відсилається в ISP [4].

При надходженні пакета на інтерфейс маршрутизатор спочатку перевіряє наявність прив'язаного ACL. Якщо список доступу присутній, пакет послідовно аналізується на відповідність заданим правилам. Лише після успішного проходження перевірки виконується його подальша маршрутизація. У випадку невідповідності політикам безпеки пакет відкидається ще до потрапляння на наступний етап обробки.

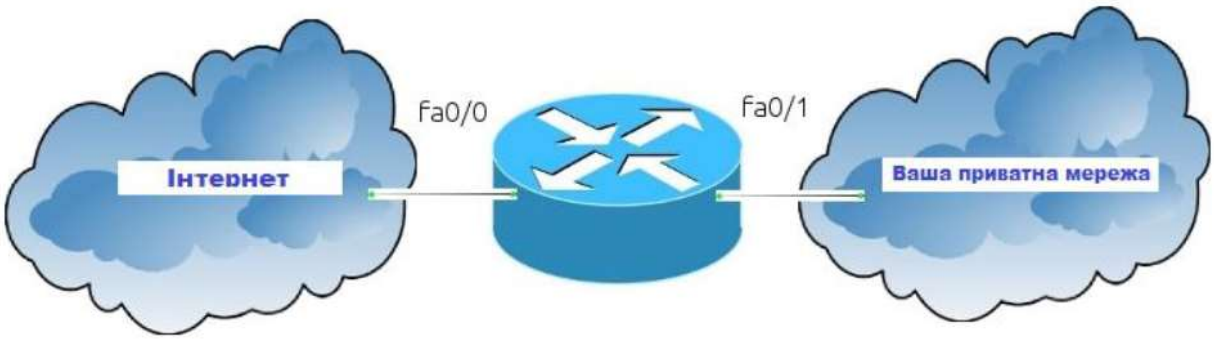


Рис. 1.1. Приклад мережевого зв'язку

Вибір між вхідним і вихідним ACL безпосередньо впливає на продуктивність мережевого обладнання. Практика показує, що небажаний трафік доцільно блокувати якомога раніше, тобто на вхідному інтерфейсі. Такий підхід дозволяє зменшити навантаження на центральний процесор маршрутизатора, скоротити обсяг службових операцій та підвищити загальну ефективність роботи мережі.

Списки контролю доступу підтримують різні мережеві протоколи, включаючи IPv4 та IPv6. Раніше ACL також використовувалися для роботи з протоколом IPX, який сьогодні практично не застосовується. Під час перевірки пакета ACL можуть аналізувати один або декілька параметрів:

- IP-адресу джерела;
- IP-адресу призначення;
- тип мережевого протоколу;

• номер порту транспортного рівня;

• тип повідомлення ICMP;

• прапорці TCP-з'єднання;

• інші параметри залежно від типу ACL (рис. 1.2).



Рис. 1.2. Схема роботи списку контролю доступу на рівні пакету

Кожний інтерфейс маршрутизатора може містити окремий список досту-пу для вхідного та вихідного трафіків і для кожного встановленого мережевого протоколу. Наприклад, на трьох інтерфейсах маршрутизатора (рис. 1.3), з двома мережевими протоколами, IPv4 та IPv6, може бути створені 12 окремих списків доступу: шість для IPv4 і шість для IPv6. Тобто, на кожному інтерфейсі по 4 списки: 2 для того, що входить і 2 для вихідного трафіку.

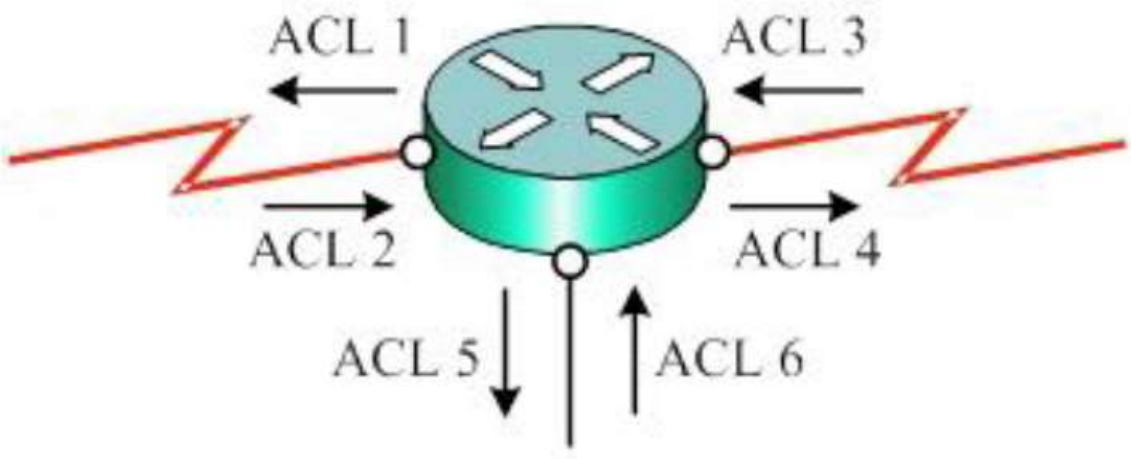


Рис. 1.3. Приклад розміщення ACL на інтерфейсах маршрутизатора

У сучасних мережах особливо поширені розширені списки доступу (Extended ACL), які дозволяють одночасно враховувати кілька характеристик трафіку. Наприклад, можна дозволити доступ до веб-сервера лише за протоколом HTTPS (порт 443), заборонивши всі інші види з'єднань.

Кожен інтерфейс маршрутизатора може мати окремі ACL для вхідного та вихідного напрямків трафіку. Якщо пристрій одночасно підтримує IPv4 та IPv6, для кожного протоколу можуть бути створені власні списки доступу. Таким чином, на одному фізичному інтерфейсі можуть одночасно функціонувати окремі ACL для IPv4 Inbound, IPv4 Outbound, IPv6 Inbound та IPv6 Outbound.

Однією з важливих переваг ACL є можливість гнучкого керування використанням мережевих ресурсів. Наприклад, адміністратор може обмежити доступ до потокового відео або файлообмінних сервісів, щоб зменшити навантаження на канали зв'язку та забезпечити пріоритет критично важливому бізнес-трафіку. Аналогічним чином ACL можуть дозволяти роботу електронної пошти та веб-сервісів, одночасно блокуючи небажані протоколи або сервіси віддаленого доступу.

Особливістю роботи ACL є послідовний принцип перевірки правил. Кожен запис ACL являє собою окремий рядок конфігурації, який аналізується в порядку його розташування. Під час надходження пакета маршрутизатор починає перевірку з першого правила та продовжує її до моменту знаходження першого збігу. Після цього подальша перевірка припиняється, а до пакета застосовується відповідна дія. Саме тому порядок розташування правил має критичне значення для коректної роботи списку доступу [6, 7].

Одним із фундаментальних принципів функціонування ACL є наявність так званого неявного правила «deny any». Це правило автоматично додається наприкінці кожного списку доступу та не відображається в конфігурації. Його призначення полягає у блокуванні всього трафіку, який не відповідає жодному із явно визначених правил. Таким чином, якщо адміністратор не додасть до ACL жодного дозволяючого запису, весь трафік, що потраплятиме під дію цього списку, буде автоматично заборонений.

Для підвищення ефективності адміністрування в сучасних версіях Cisco IOS підтримуються іменовані ACL (Named ACL), які дозволяють використовувати зрозумілі назви замість числових ідентифікаторів. Це значно спрощує супровід великих конфігурацій та зменшує ймовірність помилок під час налаштування мережевого обладнання [4, 6].

Найчастіше ACL розміщуються на прикордонних маршрутизаторах, через які корпоративна мережа взаємодіє із зовнішнім середовищем. У такому випадку маршрутизатор виконує частину функцій міжмережевого екрана (firewall), контролюючи вхідний та вихідний трафік. Поєднання ACL із сучасними засобами захисту, такими як міжмережеві екрани нового покоління, системи IDS/IPS та технології сегментації мережі, дозволяє створювати багаторівневу систему кібербезпеки, що відповідає актуальним вимогам захисту інформаційних ресурсів.

1.3. Ідентифікація списків контролю доступу

Для ідентифікації списків контролю доступу в операційній системі Cisco IOS використовується два основні підходи: нумеровані (Numbered ACL) та іменовані (Named ACL) списки доступу. У випадку нумерованих ACL усі правила, що належать до одного списку, об'єднуються спільним числовим ідентифікатором. Для іменованих ACL замість числового номера використовується унікальне символьне ім'я, яке задається адміністратором. Номер або ім'я ACL застосовується для подальшого посилання на весь набір правил як на єдиний логічний об'єкт під час прив'язки до інтерфейсів або використання в інших механізмах мережевої безпеки.

У Cisco IOS для різних типів ACL передбачені окремі діапазони номерів. Наприклад, стандартні ACL традиційно використовують номери від 1 до 99 та від 1300 до 1999, тоді як розширені ACL використовують діапазони від 100 до 199 та від 2000 до 2699. Такий поділ дозволяє операційній системі автоматично визначати тип списку доступу під час його створення.

У сучасних мережах перевага зазвичай надається іменованим ACL. Основною причиною цього є зручність адміністрування та підтримки конфігурації. Використання зрозумілих назв, наприклад «WEB_SERVERS», «VPN_USERS» або «INTERNET_FILTER», значно спрощує роботу мережевих адміністраторів, особливо у великих корпоративних мережах, де можуть одночасно використовуватися десятки або навіть сотні списків доступу.

Раніше одним із суттєвих недоліків нумерованих ACL була обмежена можливість їх редагування. У перших версіях Cisco IOS для внесення змін до такого списку адміністратор змушений був повністю видаляти ACL за допомогою команди:

no access-list <номер>

після чого створювати його заново з урахуванням необхідних змін. Такий підхід міг призводити до тимчасового порушення політик безпеки та створював ризик виникнення помилок під час повторного введення правил.

Починаючи з версії Cisco IOS 12.3 було реалізовано механізм порядкових номерів записів (Sequence Numbers), який значно спростив процес адміністрування ACL. При створенні нового списку кожному правилу автоматично присвоюється номер із кроком 10 (10, 20, 30, 40 тощо). Завдяки цьому адміністратор отримує можливість додавати нові правила між вже існуючими без необхідності повного перевизначення списку. Наприклад, між записами з номерами 20 та 30 можна вставити нове правило з номером 25.

ACL може містити як один запис, так і сотні правил залежно від складності мережевої політики. При цьому всі записи розглядаються як складові одного списку доступу та обробляються послідовно відповідно до їхнього порядку розташування.

Важливою особливістю Cisco IOS є те, що на одному інтерфейсі для одного мережевого протоколу та одного напрямку передачі трафіку може бути прив'язаний лише один ACL. Наприклад, на інтерфейсі можна одночасно використовувати один вхідний та один вихідний список доступу для IPv4 і окремо один вхідний та один вихідний ACL для IPv6. У випадку необхідності

реалізації складніших політик усі правила повинні бути об'єднані в межах одного списку доступу.

Для аналізу IP-адрес у правилах ACL використовується спеціальний механізм Wildcard Mask (маска підстановки). На відміну від звичайної маски підмережі, яка визначає мережеву та хостову частини адреси, wildcard-маска вказує, які біти адреси повинні збігатися, а які можуть приймати будь-яке значення під час перевірки пакета.

Wildcard-маска фактично є інверсією стандартної маски підмережі. Для її обчислення необхідно відняти кожен октет звичайної маски від значення 255. Наприклад:

255.255.255.255 − 255.255.255.0 = 0.0.0.255

Отримане значення 0.0.0.255 буде wildcard-маскою для мережі 192.168.1.0/24.

У wildcard-масці діє наступний принцип:

• біт зі значенням 0 означає обов'язковий збіг відповідного біта адреси;

• біт зі значенням 1 означає ігнорування відповідного біта під час порівняння.

Наприклад, запис:

access-list 10 permit 192.168.1.0 0.0.0.255

дозволяє доступ для всіх вузлів мережі 192.168.1.0/24.

Для дозволу лише однієї конкретної адреси використовується wildcard-маска 0.0.0.0:

access-list 10 permit 192.168.1.10 0.0.0.0

У практиці адміністрування мереж wildcard-маски дозволяють створювати дуже гнучкі правила фільтрації, які можуть охоплювати як окремі вузли, так і цілі підмережі або навіть декілька мереж одночасно. Саме завдяки використанню wildcard-масок ACL забезпечують високу масштабованість та ефективність керування доступом у сучасних корпоративних мережах.

У сучасних версіях Cisco IOS додатково підтримуються динамічні ACL (Dynamic ACL), часові ACL (Time-Based ACL) та рефлексивні ACL (Reflexive

ACL), які дозволяють враховувати часові обмеження, автоматично формувати правила для відповідного трафіку та реалізовувати більш складні сценарії захисту мережі. Це значно розширює можливості традиційних списків контролю доступу та наближає їх функціональність до можливостей сучасних міжмережевих екранів.

Залежно від функціональних можливостей та рівня деталізації аналізу мережевого трафіку списки контролю доступу поділяються на два основних типи: стандартні (Standard ACL) та розширені (Extended ACL). Кожен із цих типів має власні особливості, переваги та сфери застосування.

Стандартні списки контролю доступу є найпростішим механізмом фільтрації трафіку в операційній системі Cisco IOS. Вони дозволяють приймати рішення щодо дозволу або заборони пакетів виключно на основі IP-адреси джерела. У рамках навчальної програми Cisco Certified Network Associate (CCNA) саме цей критерій розглядається як основний принцип роботи стандартних ACL.

Оскільки стандартні ACL аналізують лише адресу відправника, їх можливості є відносно обмеженими порівняно з розширеними списками доступу. Проте вони мають важливу перевагу — мінімальне навантаження на обчислювальні ресурси маршрутизатора. Перевірка лише одного параметра пакета потребує значно менше процесорного часу, ніж аналіз кількох полів заголовків транспортного та мережевого рівнів.

Наприклад, якщо необхідно дозволити доступ до мережі Інтернет лише для трьох визначених вузлів локальної мережі, можна використати наступну конфігурацію:

```
access-list 1 permit host 192.168.10.50
access-list 1 permit host 192.168.10.53
access-list 1 permit host 192.168.10.60
```

У такому випадку доступ до зовнішньої мережі отримають лише зазначені хости, тоді як весь інший трафік буде заблоковано неявним правилом deny any.

Стандартні ACL найчастіше застосовуються для реалізації таких завдань:

• контроль доступу до ресурсів маршрутизатора;

• фільтрація пакетів, що проходять через маршрутизатор;

• керування процесами розподілу маршрутів між протоколами маршрутизації;

• обмеження доступу до адміністративних служб пристрою;

• реалізація базових політик мережевої безпеки.

Процес конфігурування стандартного ACL зазвичай складається з двох етапів:

1. Створення списку доступу в режимі глобального конфігурування.

2. Прив'язка створеного списку до відповідного інтерфейсу маршрутизатора.

Загальний формат створення стандартного ACL має вигляд:

Router(config)# access-list {номер} {permit | deny} {адреса_джерела} {wildcard-маска}

де:

• номер ACL належить до діапазону 1–99 або 1300–1999;

• адреса джерела визначає вузол або підмережу, до якої застосовується правило;

• wildcard-маска визначає шаблон порівняння IP-адрес.

Під час перевірки пакета маршрутизатор порівнює адресу відправника з адресним шаблоном, сформованим адресою та wildcard-маскою. Якщо збіг знайдено, виконується відповідна дія (permit або deny). У разі відсутності збігу аналіз продовжується з наступним правилом ACL.

Wildcard-маски дозволяють формувати як дуже точні, так і узагальнені правила фільтрації. Наприклад:

• 192.168.15.22 0.0.0.0 - перевіряється повна відповідність конкретній IP-адресі;

• host 192.168.15.22 - скорочена форма попереднього запису;

• any або 0.0.0.0 255.255.255.255 - правило застосовується до будь-якої адреси;

• 192.168.18.128 0.0.0.31 - охоплює діапазон адрес від 192.168.18.128 до 192.168.18.159.

Стандартні ACL є найстарішим різновидом списків доступу та використовуються ще з ранніх версій Cisco IOS. Незважаючи на обмежений функціонал, вони залишаються актуальними для реалізації простих політик контролю доступу та оптимізації використання ресурсів мережевого обладнання.

Значно ширші можливості надають розширені списки контролю доступу. На відміну від стандартних ACL, вони аналізують не лише адресу джерела, а й низку додаткових параметрів пакета. Саме тому розширені ACL вважаються основним інструментом побудови політик мережевої безпеки в сучасних корпоративних мережах.

Розширені ACL можуть виконувати фільтрацію за такими критеріями:

• IP-адреса джерела;

• IP-адреса призначення;

• тип мережевого протоколу (IP, TCP, UDP, ICMP, GRE, ESP та інші);

• номер TCP або UDP порту джерела;

• номер TCP або UDP порту призначення;

• тип та код ICMP-повідомлень;

• стан TCP-з'єднання;

• параметри VPN-трафіку та тунельних протоколів.

Завдяки цьому адміністратор може реалізовувати складні сценарії контролю доступу. Наприклад, дозволити користувачам доступ до вебсервера лише через HTTPS (порт 443), заборонити використання Telnet (порт 23), але дозволити SSH (порт 22).

Загальний формат створення розширеного ACL має вигляд:

Router(config)# access-list {номер} {permit | deny} {протокол} {адреса_джерела} {адреса_призначення} {умови_портів}

Для розширених ACL використовуються номери з діапазонів:

• 100 – 199;

• 2000 – 2699.

При роботі з портами Cisco IOS підтримує спеціальні оператори порівняння:

• eq (equal) - дорівнює зазначеному порту;

• neq (not equal) - не дорівнює зазначеному порту;

• gt (greater than) - більше заданого значення;

• lt (less than) - менше заданого значення;

• range - належить певному діапазону портів.

Наприклад:

access-list 101 permit tcp any any eq 443

дозволяє лише HTTPS-трафік.

Формат команди прив'язки списку доступу до інтерфейсу аналогічний команді стандартного списку:

Router(config-if)# {протокол} access-group {номер} {in або out}

На відміну від стандартних списків, розширені списки фільтрують трафік більш "тонко". При створенні розширених списків в правилах доступу можна включати фільтрацію трафіку по протоколах і портам. Для вказівки портів в правилі доступу вказуються спеціальні позначення (рис 1.5). Наприклад, запис eq означає вимогу аналізу пакетів тільки з даним номером порту призначення. В свою чергу, neq означає вимогу аналізу пакетів з іншими номерами, за винят-ком даного. Запис range означає вимогу аналізу пакетів з номерами портів в за-значеному діапазоні [12].

Визначення	Дія, яка виконується
lt n	Все номера портов, меньшие n.
gt n	Все номера портов, большие n.
eq n	Порт n
neq n	Все порты, за исключением n.
range n m	Все порты от n до m включительно.

Рис.1.5. Налаштування портів у ACL

Для підвищення функціональності розширених ACL у Cisco IOS були реалізовані додаткові механізми.

Динамічні ACL (Dynamic ACL або Lock-and-Key ACL) дозволяють тимчасово активувати певні правила після успішної автентифікації користувача через Telnet або SSH. Такий підхід забезпечує контрольований доступ до внутрішніх ресурсів мережі.

Рефлексивні ACL (Reflexive ACL) реалізують механізм динамічного контролю зворотного трафіку. Вони автоматично створюють тимчасові правила для пакетів-відповідей на з'єднання, ініційовані з внутрішньої мережі. За принципом роботи цей механізм нагадує функціональність Stateful Firewall.

Часові ACL (Time-Based ACL) дозволяють активувати або деактивувати правила залежно від часу доби, дня тижня чи календарної дати. Наприклад, можна дозволити доступ до певного ресурсу лише в робочий час або блокувати використання соціальних мереж під час навчального процесу.

У сучасних мережах також використовуються IPv6 ACL, які забезпечують аналогічні можливості контролю доступу для мереж нового покоління. На відміну від IPv4 ACL, вони мають дещо інший синтаксис, але підтримують більшість функцій розширеної фільтрації.

Слід враховувати, що розширені ACL потребують більшого обсягу ресурсів маршрутизатора, оскільки для кожного пакета виконується аналіз декількох полів заголовка. Проте саме вони забезпечують високий рівень гнучкості та дозволяють реалізувати складні політики кібербезпеки.

Практика експлуатації мереж Cisco виробила низку рекомендацій щодо розміщення ACL. Стандартні ACL рекомендується встановлювати якомога ближче до адресата, оскільки вони не можуть розрізняти типи сервісів і можуть ненавмисно блокувати корисний трафік. Розширені ACL, навпаки, доцільно розташовувати максимально близько до джерела потенційно небажаного трафіку, щоб зменшити навантаження на мережеву інфраструктуру.

Важливим аспектом роботи будь-якого ACL є порядок розташування правил. Cisco IOS використовує принцип First Match, тобто перевірка припиняється після знаходження першого відповідного правила. Тому найбільш специфічні умови рекомендується розташовувати на початку списку, а більш загальні — наприкінці.

Кожен ACL автоматично завершується неявним правилом:

deny any

або для розширених списків:

deny ip any any

Це правило не відображається в конфігурації, проте фактично існує завжди. Якщо пакет не відповідає жодному з явно визначених правил, він автоматично відкидається. У багатьох випадках маршрутизатор додатково може сформувати ICMP-повідомлення про недоступність ресурсу, якщо це не заборонено політикою безпеки.

Стандартні та розширені ACL є фундаментальними інструментами захисту мережевої інфраструктури. Вони забезпечують контроль доступу до ресурсів, обмеження небажаного трафіку, підтримку політик безпеки та ефективне керування потоками даних у сучасних комп'ютерних мережах.

1.4. Постановка задачі

На основі проведеного аналізу наукової літератури, технічної документації Cisco та теоретичних відомостей щодо технології списків контролю доступу (Access Control Lists, ACL) можна зробити висновок, що налаштування розширених списків доступу є одним із найважливіших етапів забезпечення безпеки сучасних комп'ютерних мереж. Водночас процес конфігурування ACL потребує від адміністратора глибоких знань мережевих технологій, розуміння принципів маршрутизації та досвіду роботи з командним інтерфейсом Cisco IOS. Навіть незначні помилки в конфігурації можуть призвести до порушення роботи мережевих сервісів або виникнення вразливостей у системі захисту.

У зв'язку з цим основною метою даної кваліфікаційної роботи є розробка веб-орієнтованої інформаційної системи для автоматизації процесу створення та налаштування розширених списків контролю доступу на мережевому обладнанні Cisco. Запропонована система повинна спростити процес формування конфігурацій ACL, зменшити кількість можливих помилок під час ручного введення команд та підвищити ефективність роботи мережевих адміністраторів.

Результатом функціонування розробленого програмного засобу має стати автоматична генерація готового набору команд Cisco IOS на основі параметрів, введених користувачем через графічний інтерфейс. Сформована конфігурація повинна бути сумісною як з емулятором мережевого обладнання Cisco Packet Tracer, так і з реальними маршрутизаторами та комутаторами Cisco, що дозволить використовувати систему як у навчальних, так і в практичних цілях.

Особлива увага приділяється зручності використання програмного продукту. Оскільки потенційними користувачами системи можуть бути не лише досвідчені мережеві адміністратори, а й студенти, викладачі та початківці у сфері комп'ютерних мереж, інтерфейс повинен бути інтуїтивно зрозумілим, логічно структурованим та не вимагати поглиблених знань синтаксису команд Cisco IOS. Використання графічних елементів керування дозволить значно спростити процес створення правил фільтрації та скоротити час, необхідний для підготовки конфігурації.

У процесі реалізації програмного забезпечення планується створення веб-додатка, який відображатиме топологію мережі та надаватиме користувачу можливість взаємодіяти з її елементами через графічний інтерфейс. Система повинна забезпечувати введення необхідних параметрів ACL, вибір типу правил фільтрації, перевірку коректності введених даних та автоматичне формування відповідних команд конфігурації. У разі успішної валідації введених параметрів користувач отримуватиме готовий код Cisco IOS, який можна безпосередньо використовувати для налаштування мережевого обладнання.

Крім генерації команд, перспективним напрямом розвитку системи є реалізація додаткових функцій, таких як автоматична перевірка конфігурації на наявність логічних помилок, візуалізація правил ACL, підтримка різних версій Cisco IOS та можливість експорту створених конфігурацій у текстові файли.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Дослідити принципи функціонування стандартних і розширених списків контролю доступу, а також проаналізувати особливості їх використання в мережах на базі обладнання Cisco.

2. За допомогою емулятора Cisco Packet Tracer розробити базову топологію комп'ютерної мережі та виконати налаштування маршрутизації між мережевими сегментами.

3. Реалізувати та протестувати різні сценарії використання розширених ACL у створеній мережевій топології.

4. Провести аналіз вимог до програмного забезпечення та спроєктувати архітектуру веб-орієнтованої системи автоматизації налаштування ACL.

5. Розробити графічний інтерфейс користувача для формування правил розширених списків контролю доступу без необхідності ручного введення команд Cisco IOS.

6. Реалізувати модуль автоматичної генерації конфігураційних команд на основі введених користувачем параметрів.

7. Забезпечити перевірку коректності введених даних та формування валідних конфігурацій ACL відповідно до синтаксису Cisco IOS.

8. Провести тестування розробленої системи в середовищі Cisco Packet Tracer та перевірити працездатність згенерованих конфігурацій.

9. Оцінити ефективність використання розробленого програмного засобу шляхом порівняння ручного та автоматизованого способів налаштування ACL.

Реалізація запропонованої веб-орієнтованої системи дозволить автоматизувати процес створення розширених списків контролю доступу, спростити адміністрування мережевого обладнання Cisco та підвищити якість налаштування механізмів мережевої безпеки.

РОЗДІЛ 2. МОДЕЛЮВАННЯ МЕРЕЖІ З ВИКОРИСТАННЯМ ЕМУЛЯТОРА CISCO PACKET TRACER

2.1 Емулятор Cisco Packet Tracer

Cisco Packet Tracer є одним із найпоширеніших програмних засобів для моделювання та візуалізації комп'ютерних мереж, розробленим компанією Cisco Systems у межах освітньої програми Cisco Networking Academy. Програмний продукт призначений для проєктування мережевих топологій, налаштування мережевого обладнання та дослідження принципів функціонування сучасних комп'ютерних мереж без необхідності використання фізичних пристроїв .

Сучасні версії Cisco Packet Tracer підтримують роботу на операційних системах Microsoft Windows, Linux та macOS. Крім того, користувачам доступні мобільні версії застосунку для платформ Android та iOS, що забезпечує можливість навчання та виконання лабораторних робіт на різних типах пристроїв. Завдяки регулярним оновленням програмне забезпечення підтримує нові мережеві технології, протоколи та сценарії автоматизації мереж.

На рис. 2.1 можна побачити стартове вікно програми.

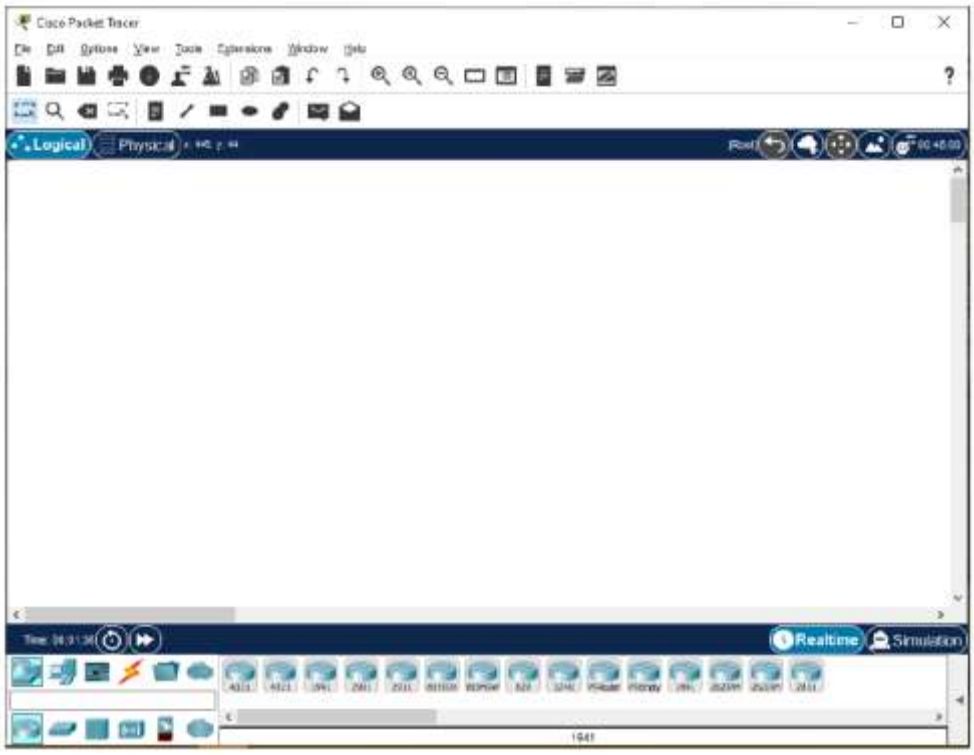


Рис. 2.1 Інтерфейс Cisco Packet Tracer

Інтерфейс Cisco Packet Tracer побудований за принципом графічного конструктора мереж, що дозволяє користувачеві легко створювати, редагувати та аналізувати мережеві топології. У робочій області можна додавати різноманітні мережеві пристрої, встановлювати між ними логічні та фізичні з'єднання, налаштовувати параметри роботи обладнання та відстежувати процес передавання даних у мережі. Фізичні канали зв'язку між пристроями відображаються за допомогою різних типів кабелів, що відповідають реальним способам підключення обладнання.

У нижній частині головного вікна програми розташована панель вибору мережевих компонентів. До складу бібліотеки входять маршрутизатори, комутатори, сервери, персональні комп'ютери, ноутбуки, бездротові точки доступу, міжмережеві екрани та інші пристрої, які використовуються в корпоративних мережах. Крім традиційного мережевого обладнання, Packet Tracer підтримує моделювання компонентів Інтернету речей (IoT), серед яких датчики руху, системи освітлення, камери відеоспостереження, контролери «розумного будинку», датчики температури та диму, що дозволяє створювати комплексні моделі кіберфізичних систем.

Однією з важливих переваг Packet Tracer є підтримка великої кількості мережевих протоколів і технологій, зокрема IPv4 та IPv6, VLAN, STP, EtherChannel, OSPF, EIGRP, RIP, DHCP, DNS, NAT, ACL, бездротових мереж та засобів мережевої безпеки. Також у сучасних версіях реалізовано підтримку програмованих мереж і засобів автоматизації, що дає можливість моделювати сценарії централізованого керування мережею та використовувати елементи мережевого програмування.

Програма має два основні режими роботи: Realtime та Simulation. У режимі Realtime користувач може спостерігати за функціонуванням мережі в реальному часі, тоді як режим Simulation дозволяє детально аналізувати проходження пакетів через мережу, досліджувати процеси маршрутизації, комутації та роботу окремих мережевих протоколів на різних рівнях моделі OSI.

Додатковою перевагою Packet Tracer є можливість організації спільної роботи користувачів над мережевими проєктами. Засоби багатокористувацької взаємодії дозволяють об’єднувати декілька мережевих топологій та виконувати колективне моделювання складних мережевих інфраструктур. Саме тому програмний продукт широко використовується у закладах вищої освіти та центрах професійної підготовки як ефективний інструмент для проведення лабораторних занять і практичного вивчення мережевих технологій.

Слід зазначити, що Cisco Packet Tracer не є повноцінним емулятором реального мережевого обладнання. Програма реалізує спрощене моделювання роботи операційної системи Cisco IOS та мережевих сервісів, забезпечуючи достатній рівень деталізації для навчальних і дослідницьких цілей. Використання Packet Tracer дозволяє перевіряти працездатність мережевих рішень, тестувати конфігурації маршрутизаторів і комутаторів, зокрема списки контролю доступу (Access Control Lists, ACL), оцінювати вплив змін на функціонування мережі та мінімізувати ризики, пов’язані з впровадженням нових налаштувань на реальному обладнанні. Це робить програму важливим інструментом для мережевих адміністраторів, інженерів та студентів, які займаються проєктуванням і супроводом комп’ютерних мереж.

2.2 Створення топології мережі на базі емулятора Packet Tracer

Першим етапом розроблення програмного засобу для автоматизації конфігурування списків контролю доступу (Access Control Lists, ACL) є створення тестового мережевого середовища, яке дозволяє перевіряти коректність роботи майбутньої системи та моделювати різні сценарії взаємодії між мережевими сегментами. Для цього було використано середовище Cisco Packet Tracer, яке надає можливість проєктувати мережеву інфраструктуру, налаштовувати мережеві пристрої та аналізувати результати застосування конфігурацій Cisco IOS у безпечному віртуальному середовищі.

З метою дослідження механізмів керування доступом було побудовано модель корпоративної мережі умовної IT-компанії (рис. 2.2). Створена топологія відображає типову структуру сучасного підприємства, у якому різні підрозділи мають власні сегменти мережі та різні рівні доступу до інформаційних ресурсів. Такий підхід дозволяє максимально наблизити процес тестування до реальних умов експлуатації мережевої інфраструктури.

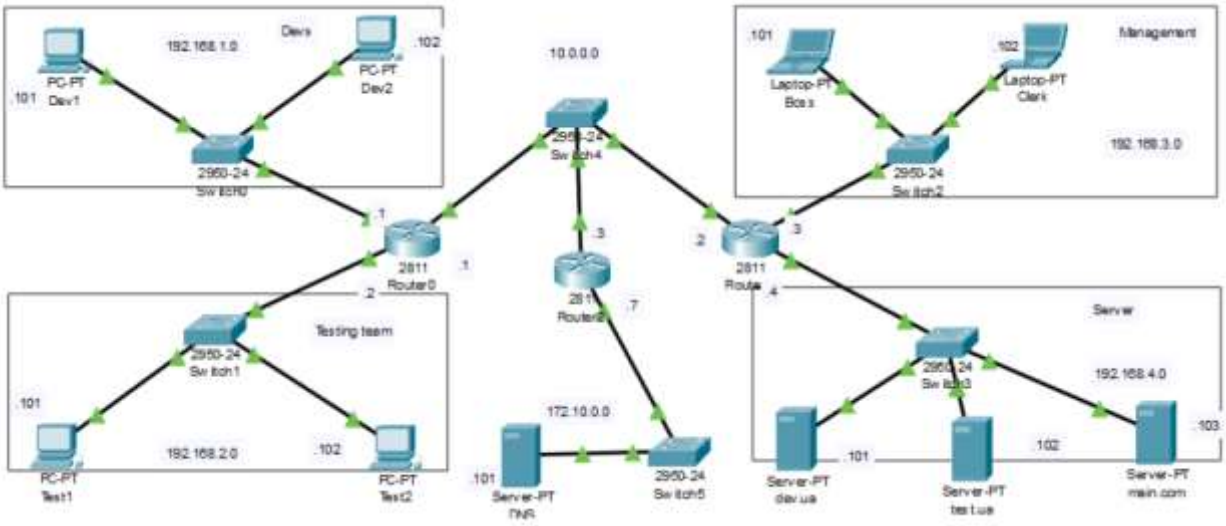


Рис. 2.2 Сконфігурована в емуляторі мережа

Модель містить п’ять логічно відокремлених підмереж, які представляють основні структурні підрозділи організації. До них належать мережа відділу розробки програмного забезпечення, мережа тестування, мережа адміністративного персоналу, сегмент серверної інфраструктури та окрема мережа сервера доменних імен (DNS). Використання декількох підмереж дає можливість досліджувати міжмережеву взаємодію та реалізовувати політики контролю доступу між окремими групами користувачів.

Відділ розробки використовує підмережу 192.168.1.0/24 та включає два робочі комп’ютери розробників. Відділ тестування розміщений у підмережі 192.168.2.0/24 і також містить два робочі місця тестувальників. Адміністративний сегмент підприємства функціонує в межах підмережі 192.168.3.0/24 та складається з двох ноутбуків, які належать керівнику компанії та його помічнику. Серверна інфраструктура розташована в підмережі

192.168.4.0/24 і містить декілька серверів, що забезпечують роботу внутрішніх сервісів підприємства. Окремо виділено DNS-сервер, який знаходиться в підмережі 172.16.0.0/24 та відповідає за перетворення доменних імен на IP-адреси, забезпечуючи зручний доступ користувачів до мережевих ресурсів.

Кожному мережевому пристрою та кінцевому вузлу призначено унікальну IP-адресу відповідно до обраної схеми адресації. Це дозволяє організувати коректний обмін даними між сегментами мережі та створює основу для реалізації правил фільтрації трафіку за допомогою ACL.

Для забезпечення зв’язку між окремими підмережами використано комутатори другого рівня та маршрутизатори Cisco. Комутатори виконують функції комутації кадрів усередині локальних сегментів, тоді як маршрутизатори забезпечують передавання пакетів між різними мережами. На маршрутизаторах налаштовано статичну маршрутизацію, що дозволяє визначити оптимальні шляхи проходження трафіку між усіма підмережами та спрощує аналіз результатів застосування списків контролю доступу.

Побудована мережева модель використовується як експериментальний полігон для перевірки алгоритмів автоматичного створення та застосування ACL. У межах дослідження на ній можуть відпрацьовуватися сценарії обмеження доступу до серверних ресурсів, контролю взаємодії між підрозділами підприємства, фільтрації мережевого трафіку за IP-адресами та протоколами, а також оцінювання впливу політик безпеки на функціонування корпоративної мережі. Завдяки цьому створене середовище є ефективною платформою для тестування та валідації розробленого програмного забезпечення до його впровадження на реальному мережевому обладнанні Cisco.

2.3. Конфігурація розширених списків доступу в емуляторі Cisco Packet Tracer

Для детального дослідження принципів функціонування списків контролю доступу та подальшого порівняння результатів ручного налаштування ACL із

роботою розробленого програмного засобу було виконано моделювання типових сценаріїв використання розширених списків контролю доступу (Extended Access Control Lists). Такі сценарії відображають найбільш поширені завдання, які виникають під час адміністрування корпоративних мереж і забезпечення інформаційної безпеки.

Розширені ACL є одним із ключових механізмів керування мережевим трафіком на обладнанні Cisco. На відміну від стандартних списків доступу, вони дозволяють здійснювати фільтрацію пакетів не лише за IP-адресою джерела, а й за адресою призначення, типом протоколу та номерами портів. Завдяки цьому адміністратор може реалізовувати більш гнучкі та детальні політики доступу до мережевих ресурсів.

У рамках дослідження було розглянуто найбільш поширені варіанти використання розширених ACL, а саме:

- обмеження доступу між окремими вузлами мережі (host-to-host);
- заборона доступу від конкретного вузла до цілої мережі (host-to-network);
- обмеження доступу від мережі до окремого вузла (network-to-host);
- блокування взаємодії між двома мережевими сегментами (network-to-network);
- заборона використання протоколу ICMP (ping) за збереження доступу до мережевих сервісів;
- дозвіл або блокування FTP-з’єднань для керування передаванням файлів між вузлами мережі.

Першим розглянемо сценарій обмеження доступу між двома окремими вузлами мережі. Подібний механізм часто застосовується в корпоративному середовищі для реалізації принципу мінімально необхідних привілеїв (Principle of Least Privilege), відповідно до якого користувач повинен мати доступ лише до тих ресурсів, які необхідні для виконання його службових обов’язків.

Наприклад, під час прийняття нового співробітника до компанії адміністрація може тимчасово обмежити його доступ до критично важливих

інформаційних ресурсів, баз даних або внутрішніх сервісів до завершення процесу адаптації та перевірки рівня повноважень. У створеній тестовій мережі можна змоделювати ситуацію, коли за кожним розробником закріплений окремий тестувальник, а доступ до певних ресурсів повинен надаватися лише визначеним користувачам. Для реалізації такого сценарію використовується ACL типу host-to-host, який дозволяє точно контролювати обмін даними між конкретними пристроями мережі (рис. 2.3).

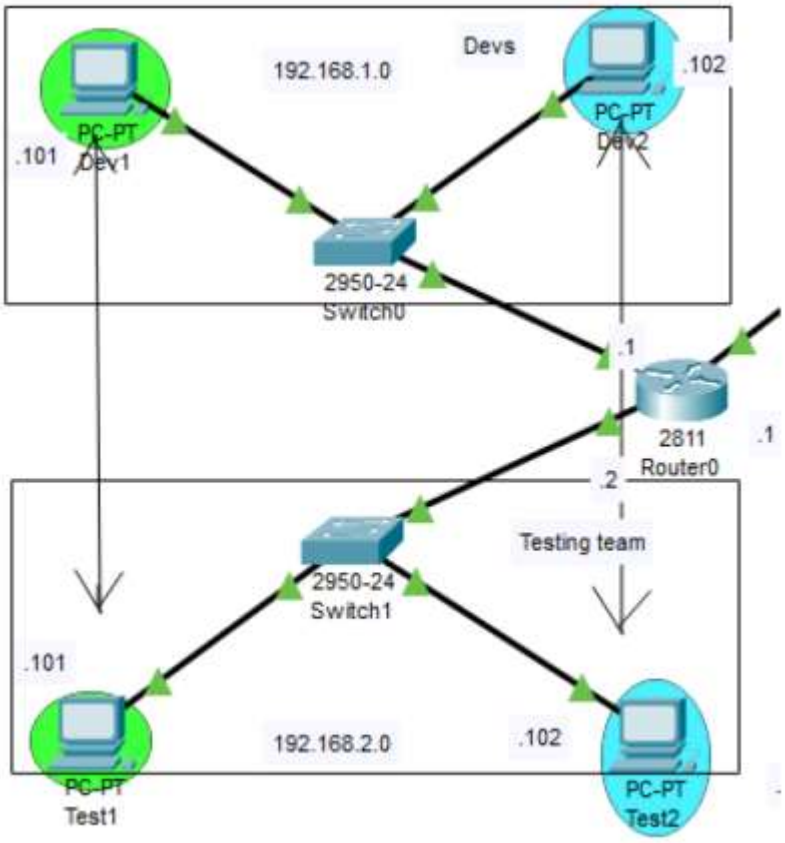


Рис. 2.3 Схема взаємозв'язку між розробниками та тестувальниками

Дослідження даного типу правил є важливим етапом розробки системи автоматизованого конфігурування ACL, оскільки саме такі налаштування найчастіше використовуються в корпоративних мережах для сегментації доступу, підвищення рівня безпеки та запобігання несанкціонованому доступу до інформаційних ресурсів організації.

Налаштування списку, який не дозволятиме розробникам мати доступ до вузла «чужого» тестувальника може допомогти керувати трафіком у системі. Додаємо наступний код на маршрутизатор 0.

```
Router>en
Router#conf t
Router(config)#access-list 101 deny icmp host 192.168.1.101 192.168.2.102 0.0.0.0
Router(config)#access-list 101 deny icmp host 192.168.1.102 192.168.2.101 0.0.0.0
Router(config)#access-list 101 permit icmp any any
Router(config)#int fa0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#ex
```

Після розміщення списку контролю доступу 101 на інтерфейсі fa0/0 маршрутизатора 0 на вхідному трафіку, Dev1 має доступ лише до Test1, а Dev2 в свою чергу лише до Test2. Результат можна побачити використавши командну строку комп’ютера і команду ping в Packet Tracer (рис. 2.4, 2.5)

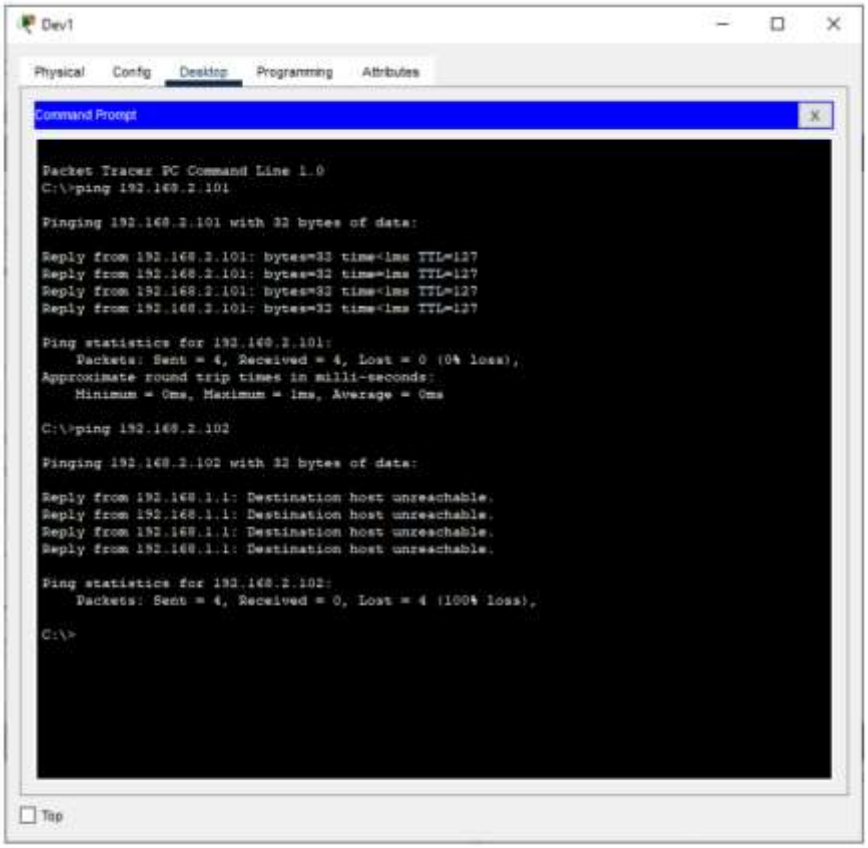


Рисунок 2.4 – Пінг з вузла Dev1 після налаштування

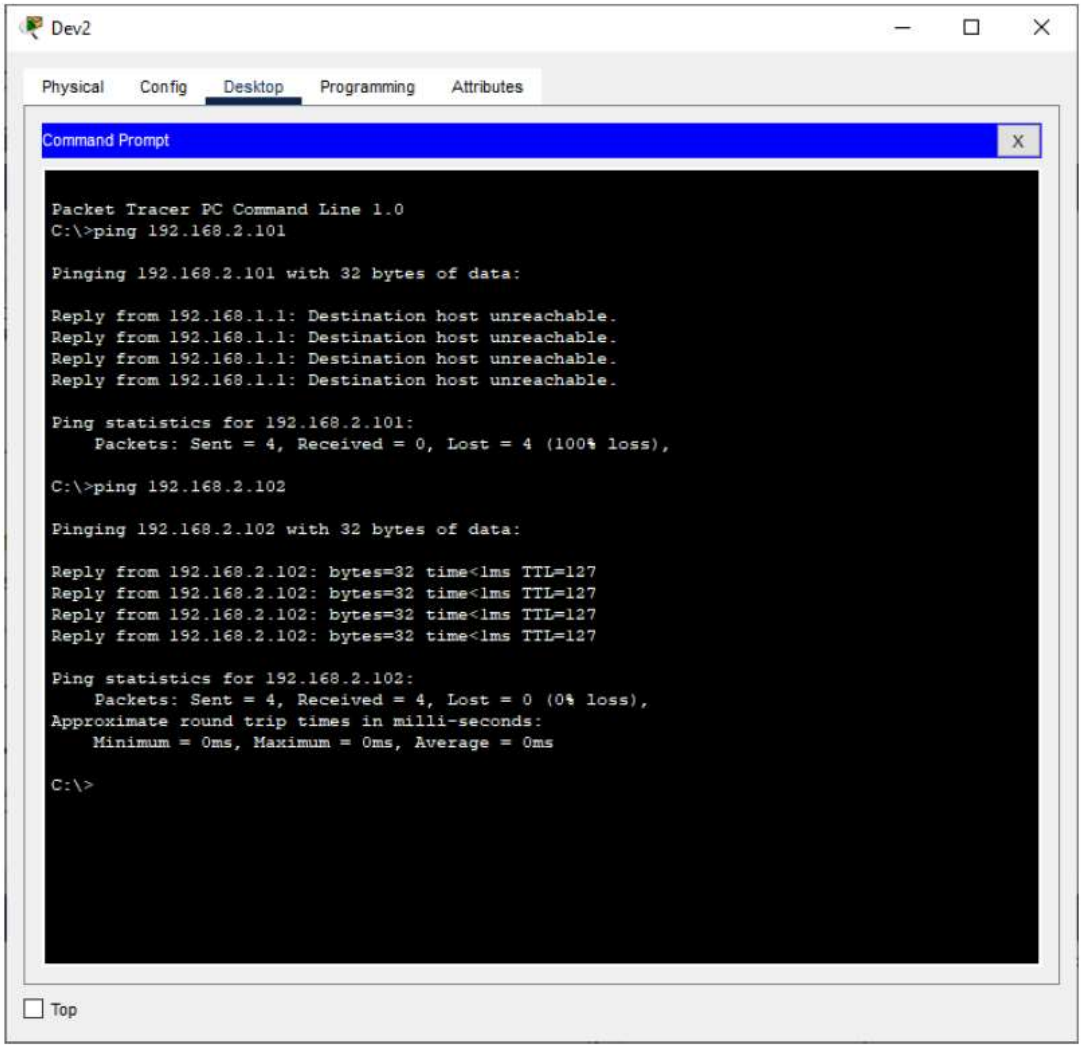


Рис. 2.5 Пінг з вузла Dev2 після налаштування

Наступним сценарієм використання розширених списків контролю доступу є обмеження доступу окремого вузла до цілої мережі (host-to-network). Подібний механізм широко застосовується в корпоративних інформаційних системах для реалізації політик безпеки, розмежування прав доступу та захисту критично важливих ресурсів від несанкціонованих підключень.

Для демонстрації роботи такого типу ACL розглянемо мережеву топологію, зображену на рисунку 2.6. У даному сценарії моделюється взаємодія між адміністративним персоналом компанії та відділом розробки програмного забезпечення.

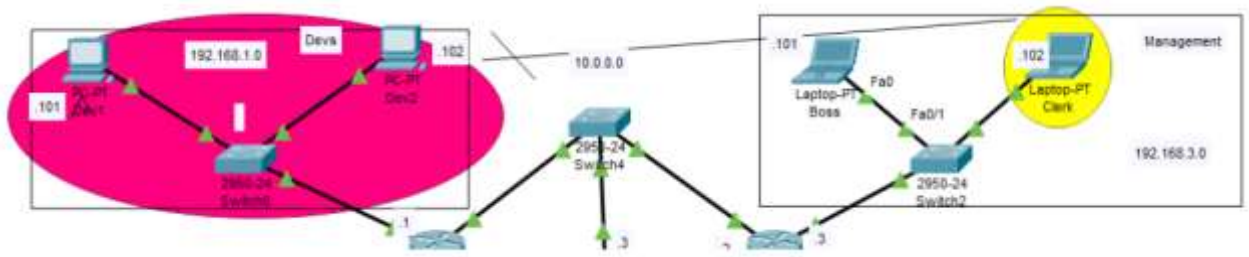


Рис. 2.6 Схема взаємозв’язку між секретарем та розробниками

Відповідно до прийнятої політики безпеки підприємства, секретар керівника компанії не потребує прямого доступу до робочих станцій розробників, оскільки інформація про стан виконання проєктів та результати роботи може надаватися через співробітників відділу тестування або керівників відповідних команд. Такий підхід дозволяє зменшити кількість зайвих мережевих взаємодій та підвищити рівень захисту внутрішніх ресурсів організації.

Для реалізації зазначеної політики на першому маршрутизаторі буде налаштовано розширений список контролю доступу, який блокуватиме весь трафік від вузла секретаря до мережі відділу розробки. При цьому доступ до інших сегментів мережі, необхідних для виконання службових обов’язків, залишатиметься дозволеним. Таким чином, ACL забезпечуватиме вибіркову фільтрацію пакетів, обмежуючи лише ті з’єднання, які суперечать встановленим правилам безпеки.

Використання такого підходу відповідає сучасним принципам сегментації мережі та концепції мінімально необхідного доступу (Least Privilege), згідно з якою кожен користувач повинен мати доступ лише до тих інформаційних ресурсів, які необхідні для виконання його посадових функцій. Це дозволяє знизити ризик несанкціонованого доступу до конфіденційних даних, зменшити потенційну площу атаки та спростити адміністрування корпоративної мережі.

```
Router>en
Router#conf t
Router(config)#access-list 102 deny icmp host 192.168.3.102 192.168.1.0 0.0.0.255
```

```
Router(config)#access-list 102 permit icmp any any
Router(config)#int fa0/0
Router(config-if)#ip access-group 102 in
Router(config-if)#ex
```

Список доступу номер 102 забороняє вузлу 192.168.3.102 направляти свій трафік до мережи 192.168.1.0. Використавши команду ping, бачимо успіш-ний результат (рис. 2.7)

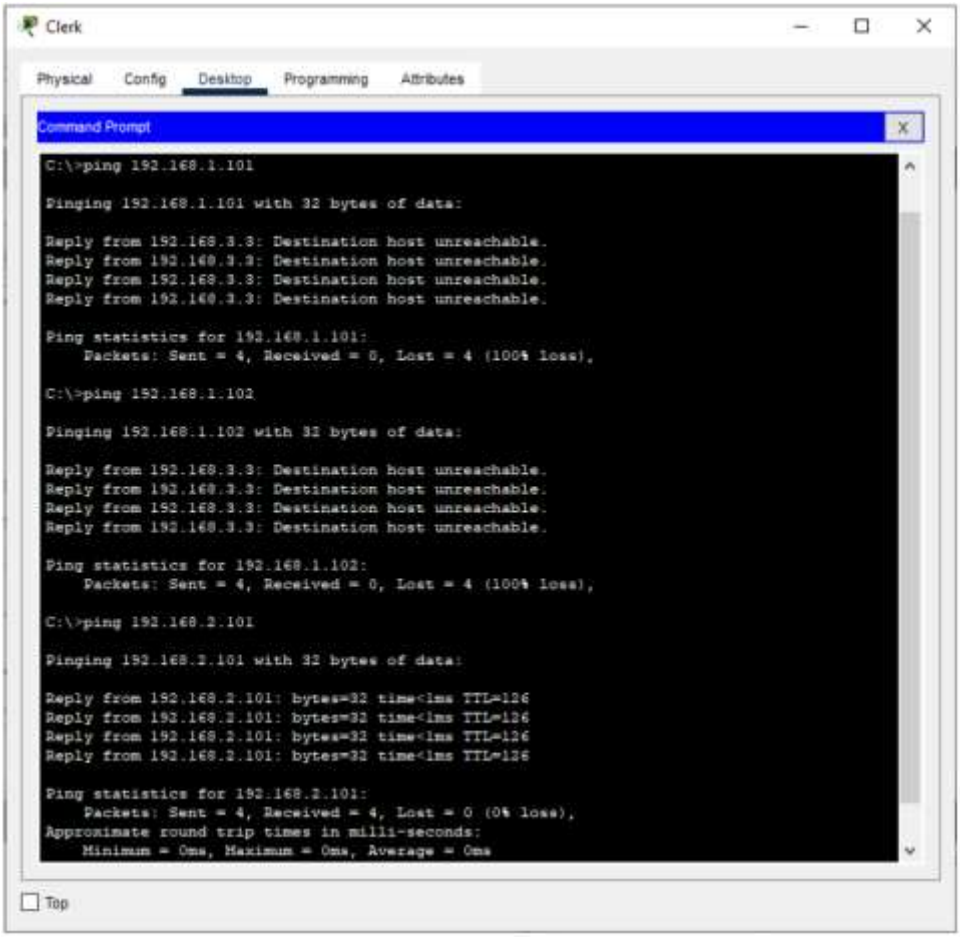


Рис. 2.7 Пінг з вузла Clerk у мережі розробників та тестувальників

Далі йде блокування від мережі до вузла. Мережі тестувальників не має сенсу мати доступ до серверів розробки та менеджменту. Проконтролювати це можна використовуючи третій вид розширених списків контролю доступу, суть якого полягає в блокуванні трафіку від мережі до вузла. Нехай відділ тес-тувальників має доступ лише до серверу test.ua.

```
Router>en
Router#conf t
Router(config)#access-list 103 deny icmp 192.168.2.0 0.0.0.255 192.168.4.101 0.0.0.0
Router(config)#access-list 103 deny icmp 192.168.2.0 0.0.0.255 192.168.4.103 0.0.0.0
Router(config)#access-list 103 permit icmp any any
Router(config)#int fa 0/1
Router(config-if)#ip access-group 103 in
Router(config-if)#ex
```

Завдяки розміщенню даного списку доступу на маршрутизаторі 0 мере-жа 192.168.2.0 матиме доступ лише до одного сервера, який знаходиться у ме-режі 192.168.4.0, до власного (рис. 2.8).

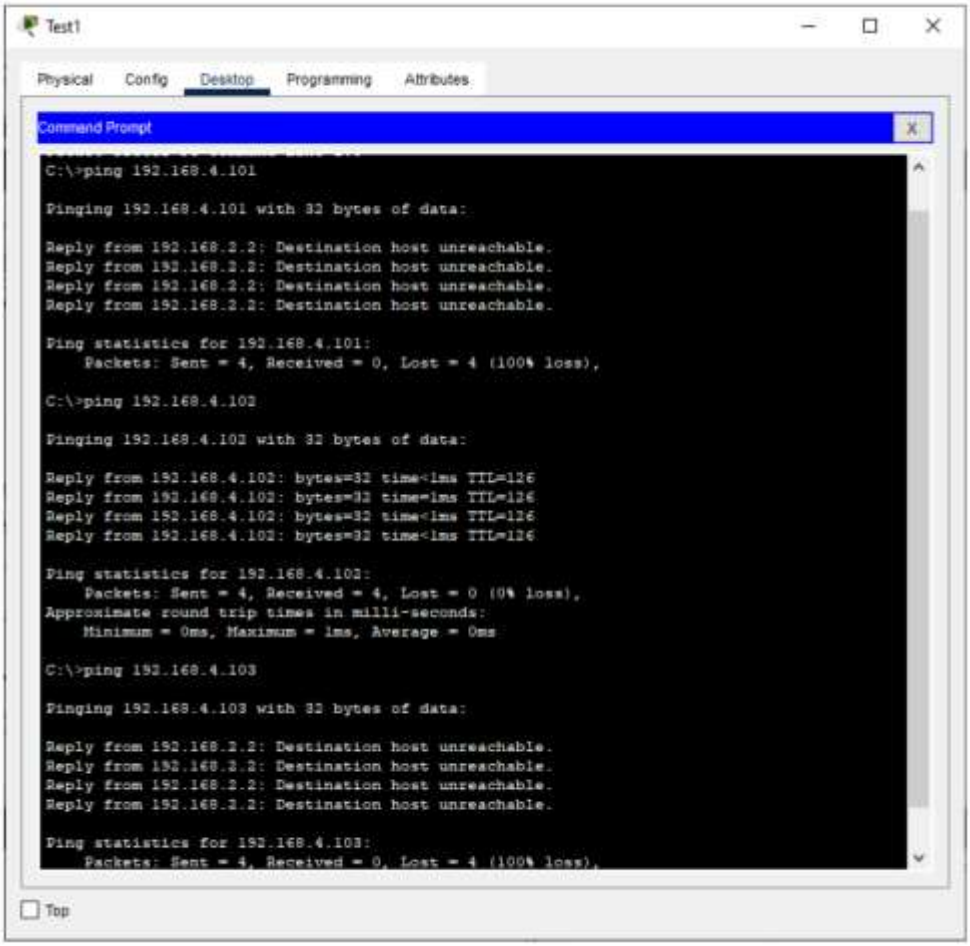


Рис. 2.8 З мережі тестувальників є доступ лише до власного сервера

Наступним важливим етапом налаштування політик мережевої безпеки є реалізація обмеження доступу між цілими мережевими сегментами, тобто сценарію типу network-to-network. Такий підхід широко застосовується в

корпоративних мережах для забезпечення ізоляції окремих підрозділів та захисту конфіденційної інформації від несанкціонованого доступу.

У межах розробленої мережевої моделі передбачається заборона доступу користувачів мереж відділу тестування до мережі менеджменту компанії. Подібне обмеження обумовлене необхідністю захисту службової, фінансової та управлінської інформації, яка використовується керівництвом підприємства в процесі прийняття рішень.

Оскільки склад співробітників технічних підрозділів може регулярно змінюватися внаслідок розширення штату, ротації персоналу або залучення тимчасових працівників, надання прямого доступу до мережі керівництва створює додаткові ризики для інформаційної безпеки організації. Саме тому доцільно застосувати політику сегментації мережі, яка передбачає повне блокування мережевого трафіку між зазначеними підмережами.

Для реалізації такого сценарію на маршрутизаторі налаштовується розширений список контролю доступу, який забороняє передавання пакетів від мережі відділу тестування до мережі менеджменту. При цьому взаємодія користувачів з іншими дозволеними ресурсами мережі зберігається без змін. Використання ACL у даному випадку забезпечує централізоване керування доступом, підвищує рівень захисту корпоративних даних та відповідає сучасним принципам побудови безпечних мережевих інфраструктур, зокрема концепціям сегментації мережі та мінімально необхідних привілеїв.

```
Router>en
Router#conf t
Router(config)#access-list 109 deny icmp 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
Router(config)#access-list 109 permit icmp any any
Router(config)#int fa0/0
Router(config-if)#ip access-group 109 in
```

Перевіряємо, доступ до мережі менеджменту, використовуючи ping. Як результат – пакети були знищені.

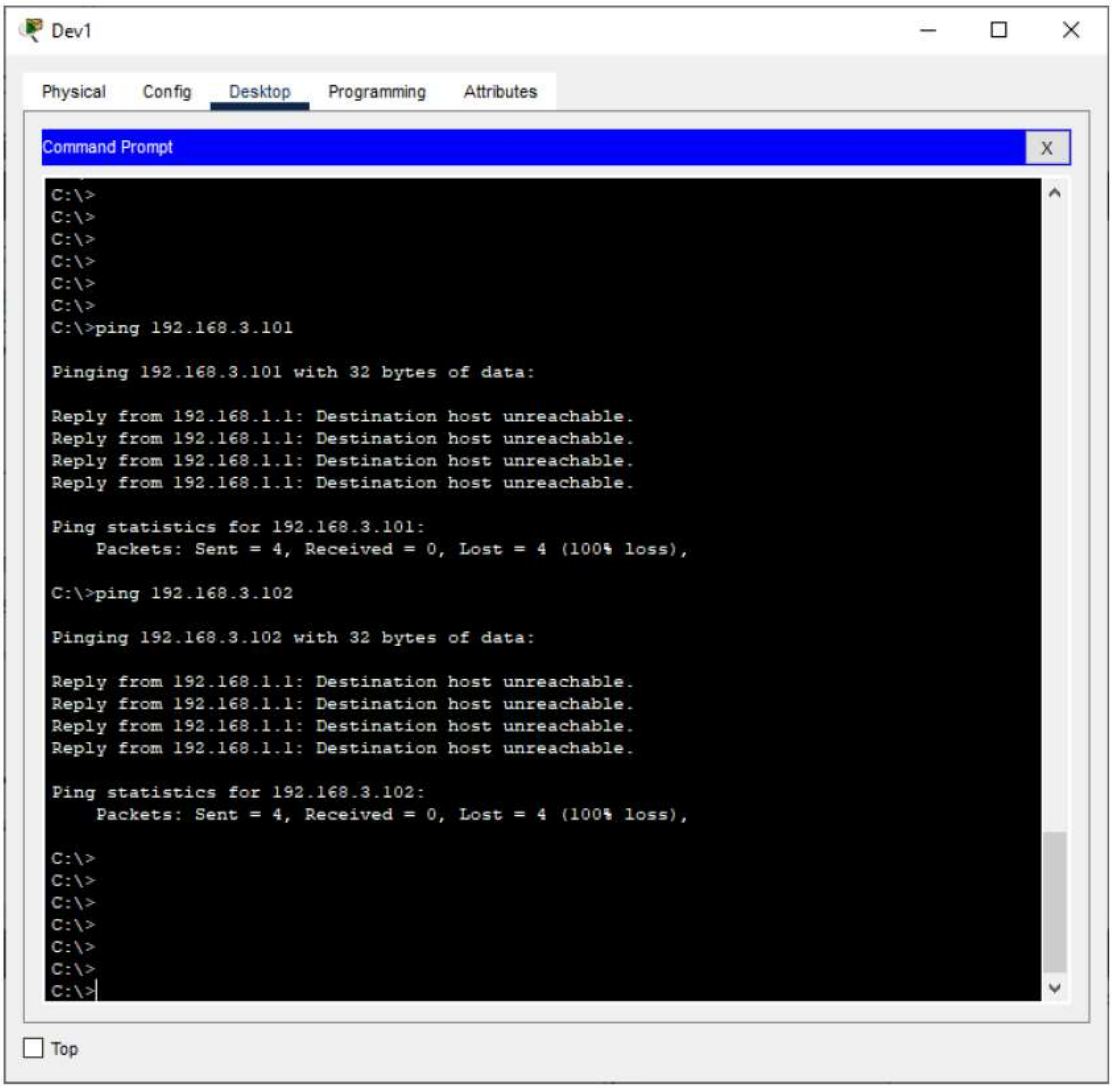


Рис. 2.9 Пінг з Dev до мережі менеджменту неможливий

Для того, щоб запобігти перевантаженню серверів необхідно заборонити можливість надсилання на них ping-запитів, але залишити співробітникам доступ до серверів. Це можна виконати, налаштувавши наступний список контролю доступу на роутері 1.

```
Router>en
Router#conf t
Router(config)#access-list 107 deny icmp any any echo
Router(config)#access-list 107 permit ip any any
Router(config)#int fa0/1
Router(config-if)#ip access-group 107 out
```

Як можна побачити, при спробі пінгування пакети були знищені, але доступ до серверу залишився (рис. 2.10, 2.11).

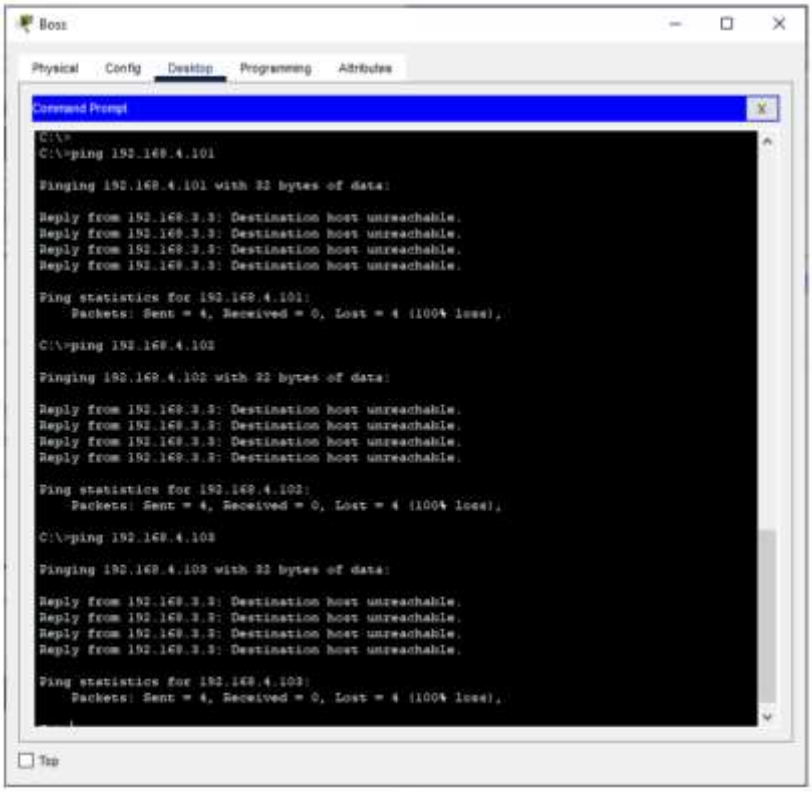


Рис. 2.10 Boss не може надсилати пінг-запити до серверів



Рис. 2.11 Boss все ще має доступ до серверу main.com

Останнім, але не менш важливим і поширеним варіантом контролю трафіку у мережі є регулювання ftp-трафіку. Наступним налаштуванням можна заборонити передачу даного трафіку від відділу розробки до тестувальників, аби не перевантажувати мережу.

```
Router>en
Router#conf t
Router(config)#access-list 106 deny tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
eq 21
Router(config)#int fa0/0
Router(config-if)#ip access-group 106 in
```

Необхідно створити пакет трафіку типу ftp. Для цього у Packet Tracer ic-нує спеціальна функція (рис. 2.12).

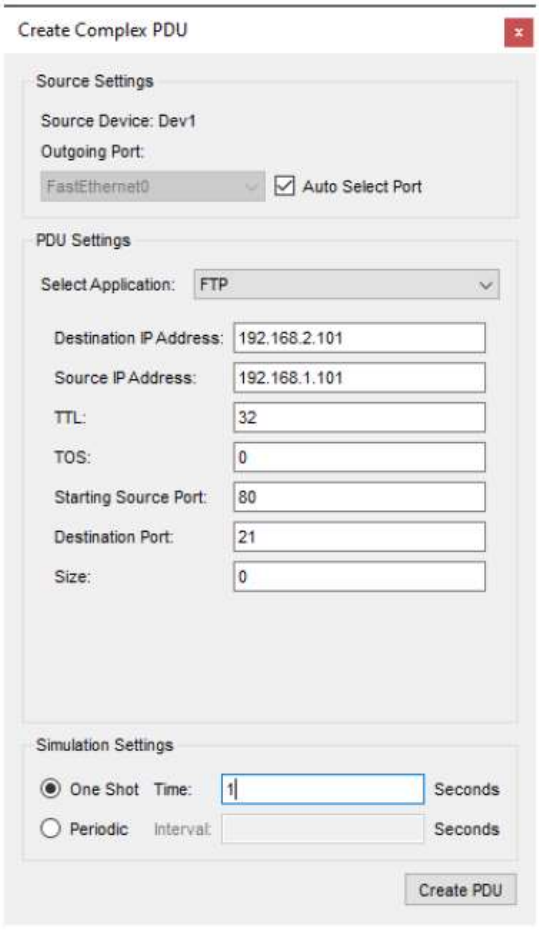


Рис. 2.12 Створення та відправка ftp-пакетів

Після надсилання створеного пакету, бачимо, що він не зміг досягнути пункту призначення, як і планувалося (рис. 2.13)



Рис.2.13 Знищення пакетів, як заборонених

Хоча усі виконані налаштування не виглядають складними, але вони потребують часу та знань конфігурації мережі. Необхідно розробити інтерфейс, який допоможе спростити цю задачу.

РОЗДІЛ 3. ІНФОРМАЦІЙНЕ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ГРАФІЧНОГО ІНТЕРФЕЙСУ НАЛАШТУВАННЯ РОЗШИРЕНИХ СПИСКІВ КОНТРОЛЮ ДОСТУПУ

3.1. Розробка графічного інтерфейсу з використанням мови програмування JavaScript та технологій HTML і CSS

Для реалізації програмного засобу автоматизації конфігурування списків контролю доступу на мережевому обладнанні Cisco найбільш доцільним є використання веборієнтованого графічного інтерфейсу. Такий підхід забезпечує універсальність, простоту використання та доступність системи для широкого кола користувачів, зокрема для початківців, які не мають значного досвіду роботи з мережевим обладнанням або спеціалізованим програмним забезпеченням.

На відміну від традиційних настільних застосунків, вебінтерфейс не потребує встановлення додаткового програмного забезпечення на комп’ютер користувача. Для роботи із системою достатньо сучасного веббраузера, що значно спрощує процес розгортання та використання програмного продукту. Крім того, веборієнтовані рішення є кросплатформними та можуть використовуватися на різних операційних системах, зокрема Microsoft Windows, Linux та macOS, а також на мобільних пристроях.

Розробка графічного інтерфейсу передбачає використання сучасного стеку вебтехнологій, який складається з мови гіпертекстової розмітки HTML, каскадних таблиць стилів CSS та мови програмування JavaScript. Поєднання цих технологій дозволяє створювати функціональні, інтерактивні та зручні у використанні вебзастосунки.

Основою будь-якої вебсторінки є мова гіпертекстової розмітки HTML (HyperText Markup Language). Вона використовується для формування структури документа та визначення розташування елементів інтерфейсу. HTML не є мовою програмування, оскільки не містить механізмів реалізації алгоритмів

або логічних операцій. Її основне призначення полягає у створенні структури вебсторінки, яка надалі може бути стилізована за допомогою CSS та доповнена функціональністю за допомогою JavaScript.

Сучасним стандартом є HTML5, який продовжує активно розвиватися в межах специфікацій WHATWG та підтримується всіма сучасними браузерами. HTML5 надає широкий набір семантичних елементів, засобів роботи з мультимедійним контентом, графікою, формами введення даних та вебсервісами. Завдяки цьому розробники можуть створювати складні вебзастосунки без використання додаткових плагінів або зовнішніх компонентів.

Важливою особливістю HTML є ієрархічна структура документа, побудована за принципом вкладеності елементів. Коректна організація структури сторінки покращує її читабельність, спрощує підтримку коду та позитивно впливає на швидкодію браузера. Крім того, семантична розмітка сприяє підвищенню доступності вебресурсів та покращує їх індексацію пошуковими системами.

За візуальне оформлення вебінтерфейсу відповідають каскадні таблиці стилів CSS (Cascading Style Sheets). Дана технологія дозволяє визначати зовнішній вигляд елементів сторінки, включаючи кольорову схему, шрифти, відступи, розташування блоків, анімації та адаптивне відображення на різних пристроях. Сучасні можливості CSS дають змогу створювати складні макети без використання сторонніх бібліотек, застосовуючи технології Flexbox та Grid Layout.

Однією з ключових переваг CSS є відокремлення логіки відображення від структури документа. Це спрощує супровід проєкту, підвищує повторне використання коду та дозволяє централізовано керувати зовнішнім виглядом усіх сторінок вебзастосунку. Завдяки підтримці адаптивного дизайну інтерфейс автоматично підлаштовується під різні розміри екранів, що є важливою вимогою до сучасних інформаційних систем.

Для реалізації логіки роботи системи використовується мова програмування JavaScript. На сьогодні JavaScript є однією з найпоширеніших мов програмування

у сфері веброзробки та підтримується всіма сучасними браузерами. Саме вона забезпечує інтерактивність вебсторінки, обробку дій користувача, перевірку введених даних, динамічне оновлення інтерфейсу та взаємодію із серверною частиною застосунку.

Сучасний JavaScript значно відрізняється від своїх ранніх версій. Завдяки стандарту ECMAScript 2024 він підтримує модульну архітектуру, асинхронне програмування, класи, сучасні структури даних та ефективні механізми взаємодії з вебсервісами через API. Крім того, JavaScript використовується не лише на стороні клієнта, але й на сервері за допомогою платформи Node.js, що дозволяє створювати повноцінні вебзастосунки з використанням єдиної мови програмування.

У розроблюваній системі JavaScript забезпечує автоматизацію процесів налаштування ACL, взаємодію користувача з графічним інтерфейсом, перевірку правильності введених параметрів, формування конфігураційних команд Cisco IOS та передачу необхідних даних між компонентами системи.

Таким чином, використання технологій HTML5, CSS3 та JavaScript дозволяє створити сучасний вебінтерфейс для автоматизації конфігурування списків контролю доступу на мережевому обладнанні Cisco. Після виконання моделювання корпоративної мережі в Cisco Packet Tracer та дослідження принципів роботи розширених ACL можна перейти безпосередньо до проєктування та реалізації графічного інтерфейсу, який стане основним інструментом взаємодії користувача із системою.

3.2 Огляд функціоналу розробленої веборієнтованої системи

Розроблена веборієнтована система призначена для автоматизації процесу створення та налаштування розширених списків контролю доступу (Extended Access Control Lists, ACL) на мережевому обладнанні Cisco. Основною метою системи є спрощення процесу конфігурування ACL для користувачів, які не мають достатнього досвіду роботи з командним рядком Cisco IOS, а також

зменшення ймовірності виникнення помилок під час ручного введення конфігураційних команд.

Інтерфейс вебзастосунку побудований за принципами сучасного UX/UI-дизайну та складається з трьох основних функціональних блоків (рис. 3.1). У лівій верхній частині сторінки розташована схема мережевої топології, створена на основі моделі корпоративної мережі, розробленої в середовищі Cisco Packet Tracer. Візуальне відображення структури мережі дозволяє користувачу швидко орієнтуватися у взаємозв'язках між окремими сегментами та коректно визначати напрямки мережевого трафіку, для яких необхідно створити правила фільтрації.

У правій частині інтерфейсу розміщено покрокову інструкцію щодо використання системи. Наявність алгоритму дій дозволяє користувачам швидше освоїти функціональні можливості застосунку та мінімізує кількість помилок під час формування конфігурації ACL.

Нижню частину сторінки займає блок налаштування параметрів списку контролю доступу. Саме в цьому розділі користувач задає характеристики майбутніх правил фільтрації трафіку та параметри застосування ACL до мережевого обладнання.

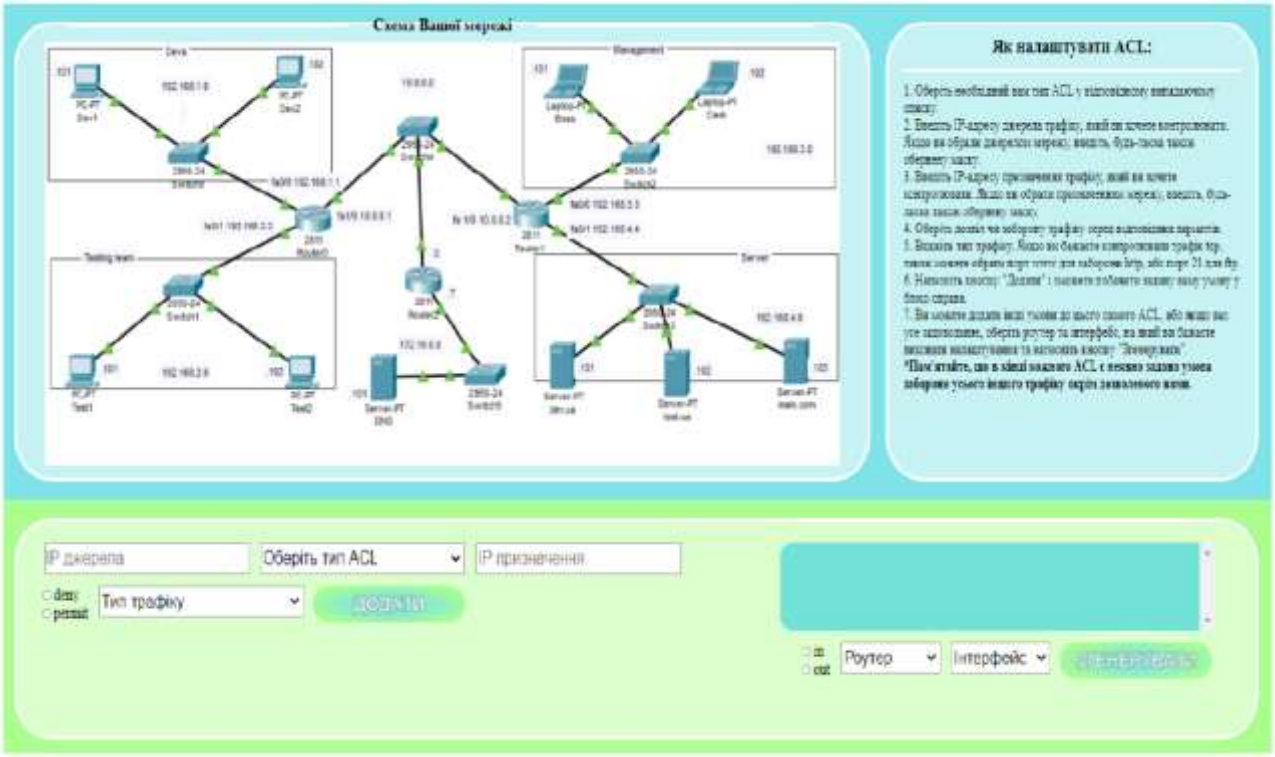


Рис. 3.1 Інтерфейс розробленої веборієнтованої системи

Основними елементами блоку налаштування є випадаючі списки, текстові поля введення, перемикачі вибору режиму роботи та кнопки керування (рис. 3.2).

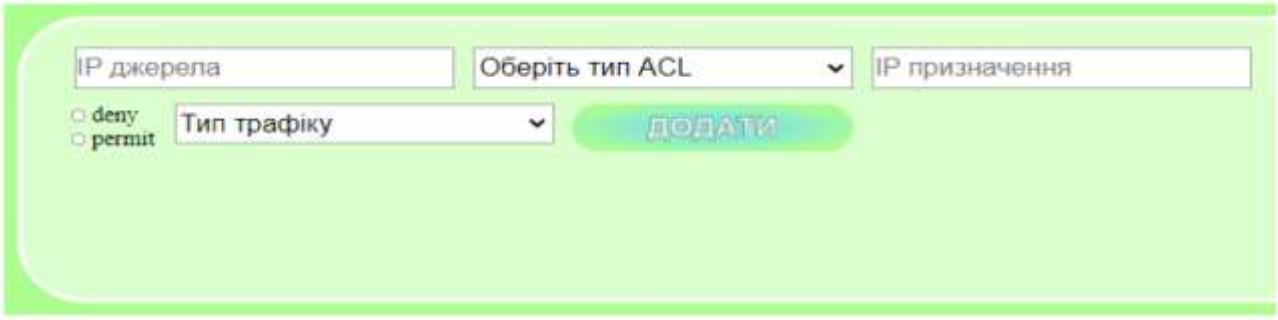


Рис. 3.2 Блок налаштування параметрів ACL

Першим елементом інтерфейсу є список вибору типу ACL. Користувачу доступні чотири найбільш поширені варіанти застосування розширених списків контролю доступу:

- Host-to-Host;
- Host-to-Network;
- Network-to-Host;
- Network-to-Network.

Вибір певного типу ACL безпосередньо впливає на набір доступних параметрів. Система динамічно змінює форму введення, приховуючи або відображаючи поля для введення IP-адрес та wildcard-масок залежно від обраного сценарію. Такий підхід дозволяє спростити роботу користувача та уникнути введення зайвих параметрів.



Рис. 3.3 Динамічне відображення полів введення залежно від типу ACL

Для забезпечення коректності конфігурації всі поля введення оснащені механізмами валідації. Під час введення IP-адрес або масок система автоматично

перевіряє правильність формату введених даних. У разі виявлення помилки відповідне поле підсвічується, а користувачу відображається пояснення щодо характеру помилки та рекомендації щодо її виправлення.

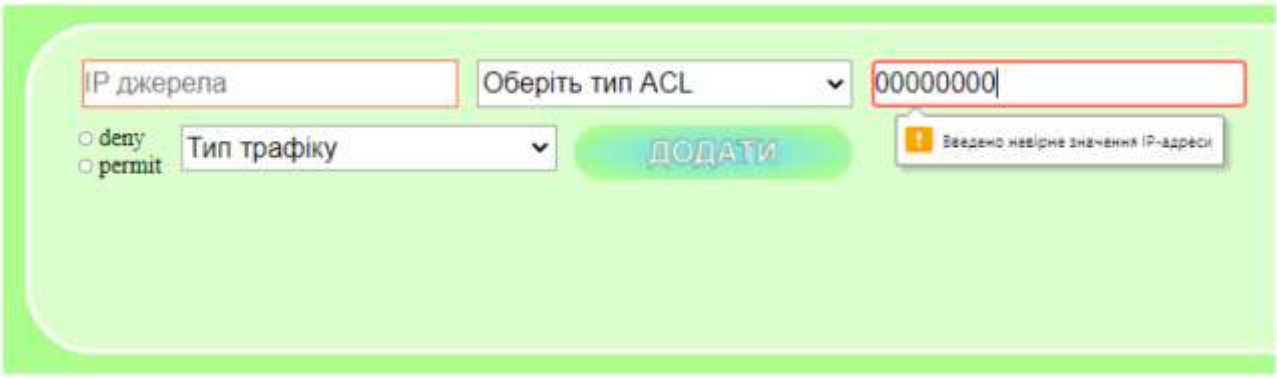
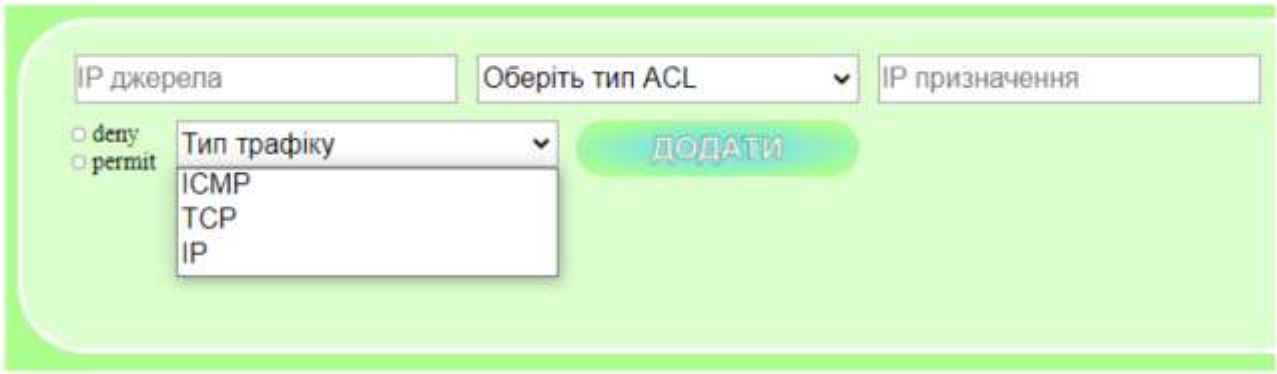


Рис.3.4 Перевірка коректності введених параметрів

Важливою частиною налаштування ACL є визначення дії над мережевим трафіком. Для цього в інтерфейсі реалізовано перемикачі permit та deny, які відповідають за дозвіл або заборону проходження пакетів через мережевий пристрій. Додатково користувач може обрати тип трафіку, до якого буде застосовуватися правило.

На поточному етапі реалізації підтримуються найбільш поширені протоколи:

- IP - фільтрація всього IP-трафіку;
- TCP - контроль передачі даних через транспортний протокол TCP;
- ICMP - керування службовими повідомленнями та запитами ping.



Рису. 3.5 Вибір типу мережевого трафіку

У разі вибору протоколу TCP система автоматично відкриває додаткові параметри для роботи з портами. Це дозволяє налаштовувати доступ до окремих сервісів, наприклад вебсерверів або FTP-серверів. Користувач може обрати стандартні порти або вказати необхідний номер порту вручну.

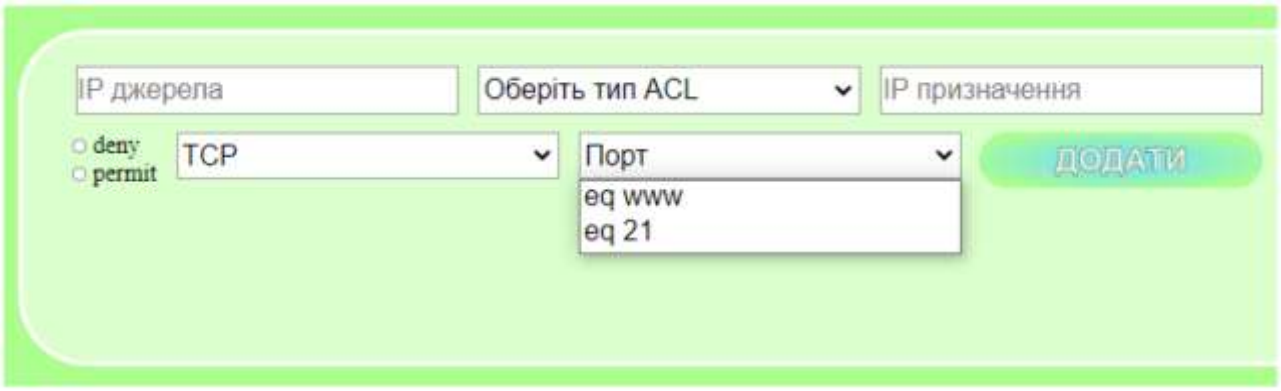


Рис. 3.6 Налаштування TCP-портів

Після заповнення необхідних параметрів користувач натискає кнопку «Додати», після чого сформоване правило відображається у спеціальному списку активних правил. Такий механізм дозволяє створювати багаторядкові ACL, які можуть містити декілька умов фільтрації трафіку. Користувач має можливість переглядати, редагувати або видаляти створені правила до моменту генерації фінальної конфігурації.



Рис.3.7 Формування списку правил ACL

Після завершення створення правил користувач переходить до етапу прив’язки ACL до мережевого обладнання. Для цього необхідно вибрати маршрутизатор, інтерфейс та напрямок застосування списку доступу (inbound або outbound). Такий підхід відповідає рекомендаціям Cisco щодо впровадження механізмів контролю доступу та дозволяє точно визначати місце застосування політики безпеки.

Після натискання кнопки «Згенерувати» система автоматично формує готовий набір команд Cisco IOS, який може бути використаний для налаштування реального маршрутизатора або тестування в середовищі Cisco Packet Tracer.

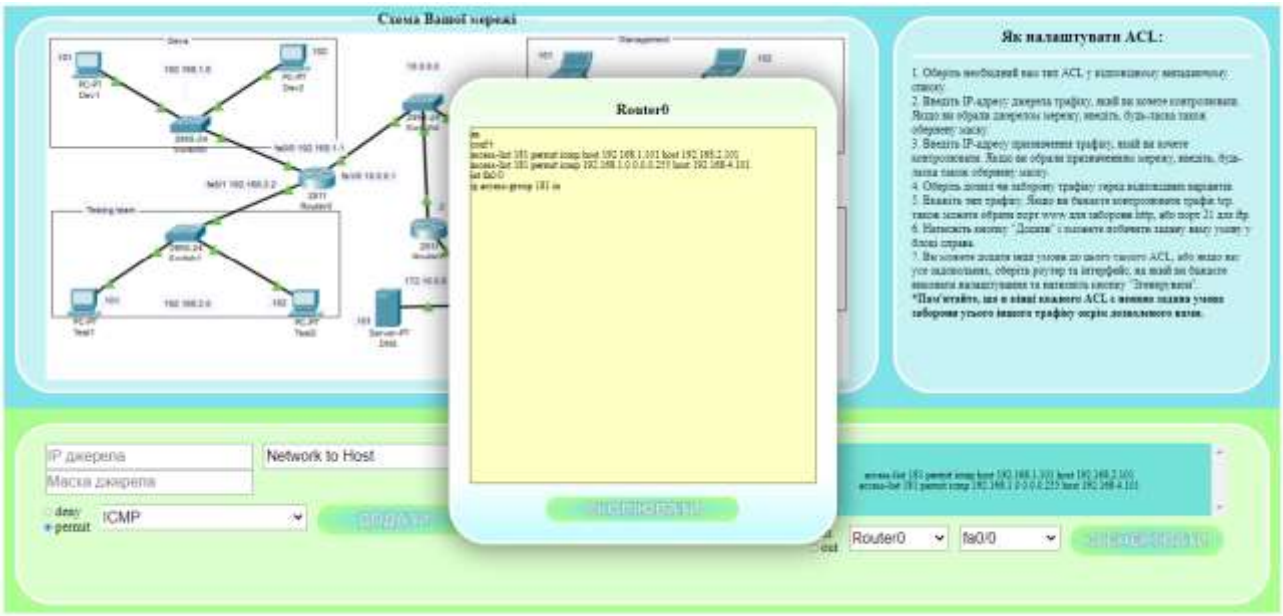


Рис.3.8 Генерація конфігураційного коду

Згенерований код відображається у спливаючому вікні та доступний для копіювання в буфер обміну за допомогою спеціальної кнопки. Це значно прискорює процес розгортання конфігурації та усуває ризик виникнення помилок, пов’язаних із ручним введенням команд.



Рис.3.9 Вигляд згенерованої конфігурації ACL

Після копіювання користувач може безпосередньо вставити отримані команди до консолі Cisco Packet Tracer або на реальне мережеве обладнання Cisco. Таким чином розроблена система забезпечує повний цикл автоматизованого створення ACL — від вибору параметрів фільтрації до отримання готової конфігурації Cisco IOS. Це суттєво спрощує роботу мережевих адміністраторів, зменшує кількість конфігураційних помилок та підвищує ефективність управління мережевою інфраструктурою.

3.3 Тестування графічного інтерфейсу в емуляторі Cisco Packet Tracer

Для оцінювання ефективності та коректності роботи розробленого веборієнтованого графічного інтерфейсу було проведено серію експериментів у середовищі Cisco Packet Tracer. Як тестове середовище використовувалась раніше створена модель корпоративної мережі, у якій налаштовано IP-адресацію, статичну маршрутизацію та забезпечено повну мережеву зв’язність між усіма сегментами. На початковому етапі жодних стандартних або розширених списків

контролю доступу на маршрутизаторах не було налаштовано, тому всі вузли мережі могли безперешкодно обмінюватися даними.

Основною метою тестування було підтвердження правильності генерації конфігурацій Cisco IOS та перевірка відповідності фактичної поведінки мережі очікуваним результатам після застосування автоматично створених ACL.

Першим етапом перевірки стало тестування сценарію типу Network-to-Network. Відповідно до політики безпеки підприємства необхідно було обмежити доступ користувачів мережі розробки до мережі менеджменту. Для цього за допомогою вебінтерфейсу було сформовано відповідне правило ACL та згенеровано набір команд Cisco IOS для маршрутизатора №0 (рис. 3.10).

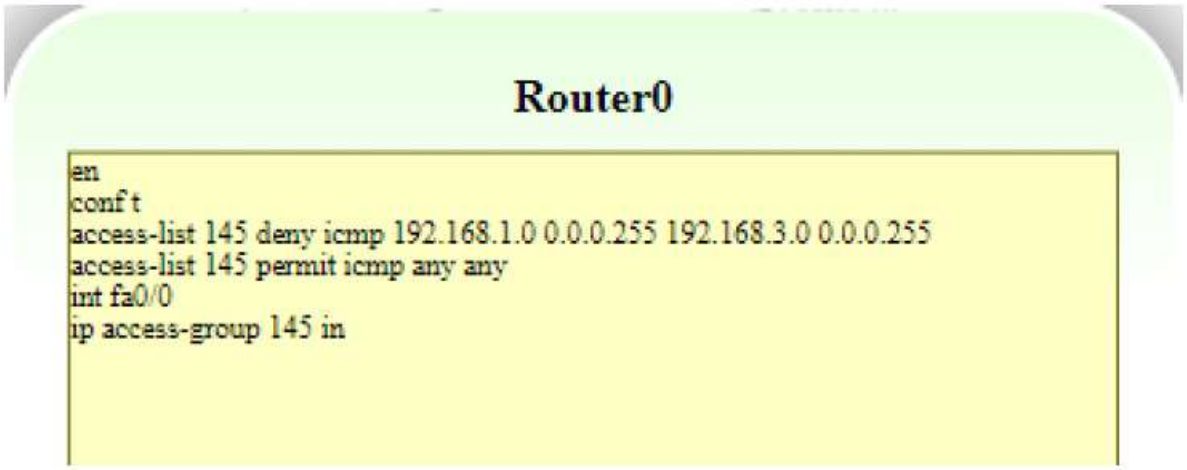


Рис. 3.10 Генерація конфігурації ACL типу Network-to-Network

Після завершення генерації конфігураційний код було скопійовано за допомогою вбудованої функції інтерфейсу та застосовано на відповідному маршрутизаторі в середовищі Cisco Packet Tracer (рис. 3.11).

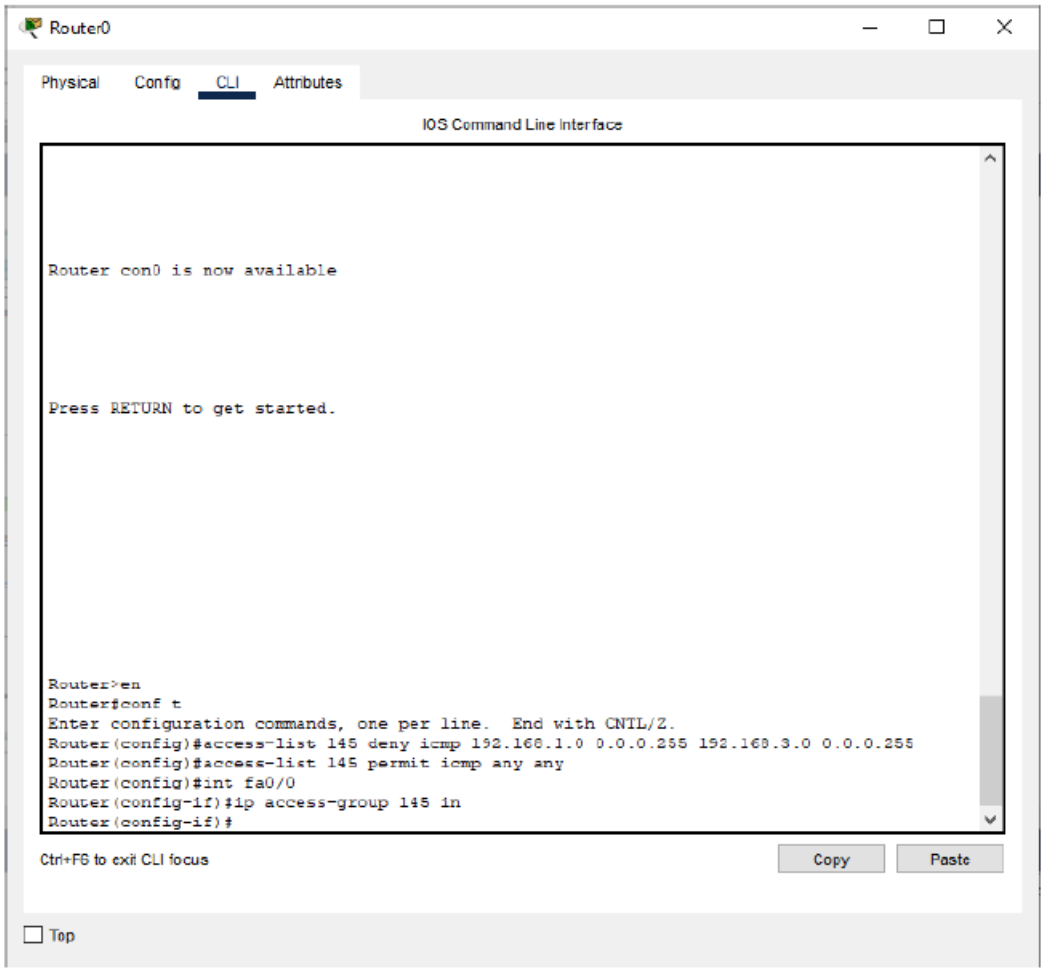


Рис. 3.11 Застосування згенерованої конфігурації на маршрутизаторі

Для перевірки працездатності створеного правила було виконано передавання тестових пакетів між вузлами зазначених мереж. Аналіз результатів симуляції показав, що пакети, які підпадали під умови забороняючого правила ACL, успішно блокувалися маршрутизатором та не передавалися до мережі призначення (рис. 3.12).

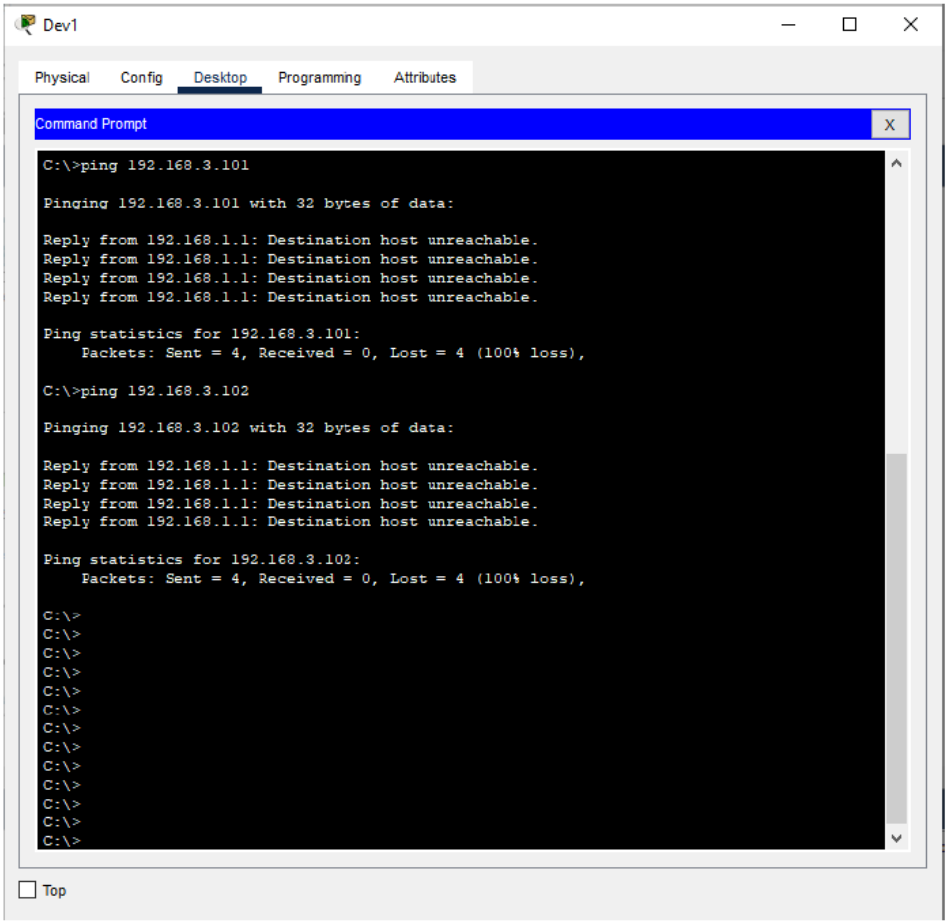


Рис. 3.12 Блокування мережевого трафіку відповідно до правил ACL

Отримані результати підтвердили правильність роботи механізму генерації ACL та коректне застосування створених правил до мережевого обладнання. Заборонений трафік не досягає кінцевого вузла, що відповідає встановленій політиці безпеки та запобігає небажаному навантаженню мережевої інфраструктури.

Наступним етапом тестування стала перевірка можливості формування більш складних правил, що враховують тип транспортного протоколу та номер порту. У сучасних корпоративних мережах подібні механізми широко використовуються для контролю доступу до окремих сервісів та реалізації принципів мережевої сегментації.

У рамках експерименту було змодельовано ситуацію, коли користувачам мережі менеджменту необхідно надати доступ до вебсервера, але водночас заборонити використання FTP-сервісу. Для реалізації такого сценарію за

допомогою вебінтерфейсу було створено ACL, що містить правило блокування FTP-трафіку (TCP-порт 21) та правило дозволу HTTP-трафіку (TCP-порт 80) (рис. 3.13).

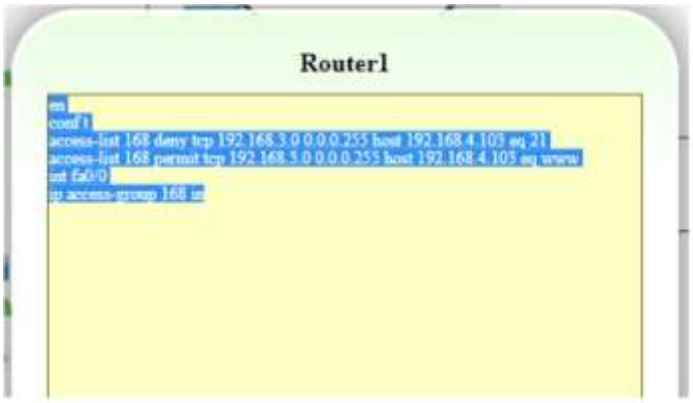


Рис. 3.13 Генерація ACL для контролю FTP та HTTP-трафіку

Після формування конфігурації отриманий код було застосовано до маршрутизатора №1 у середовищі Cisco Packet Tracer (рис. 3.14).

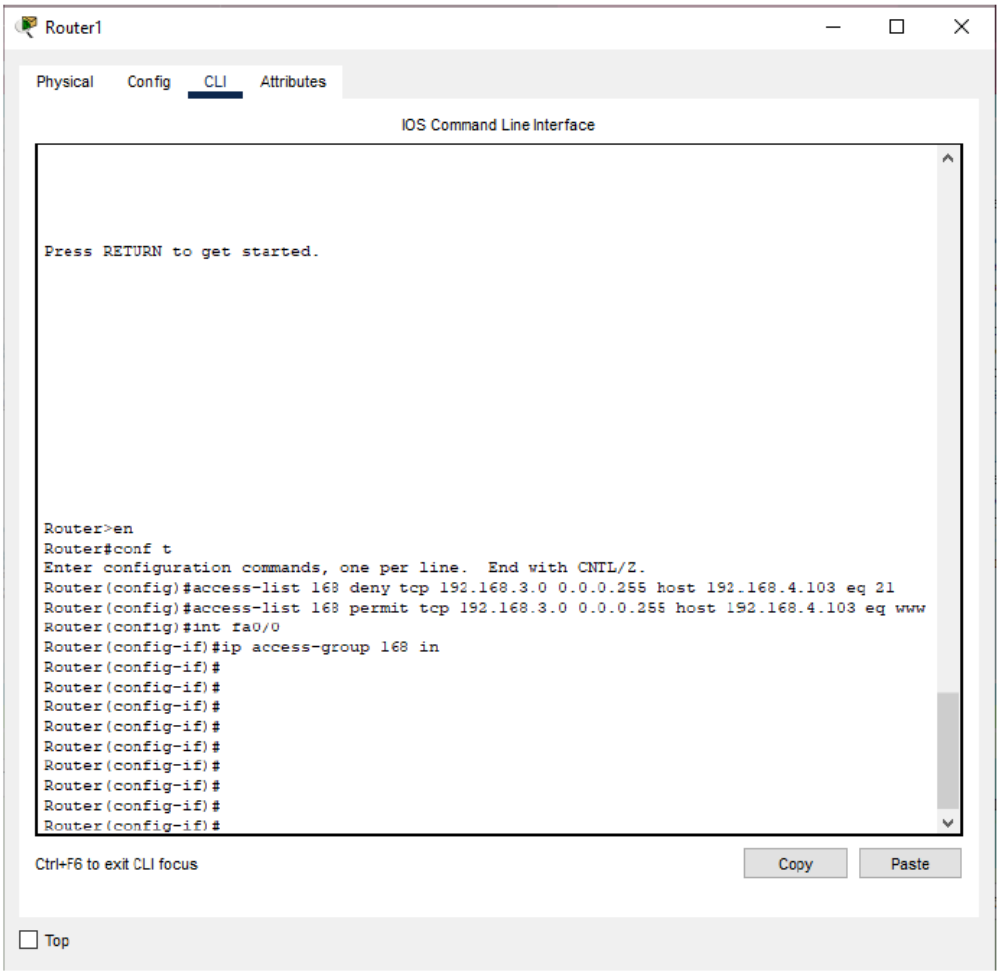


Рис. 3.14 Конфігурування маршрутизатора з використанням згенерованих команд

Для перевірки результатів було створено два типи тестового трафіку: FTP та HTTP. Передавання пакетів виконувалося між вузлами мережі менеджменту та серверним сегментом (рис. 3.15–3.16).

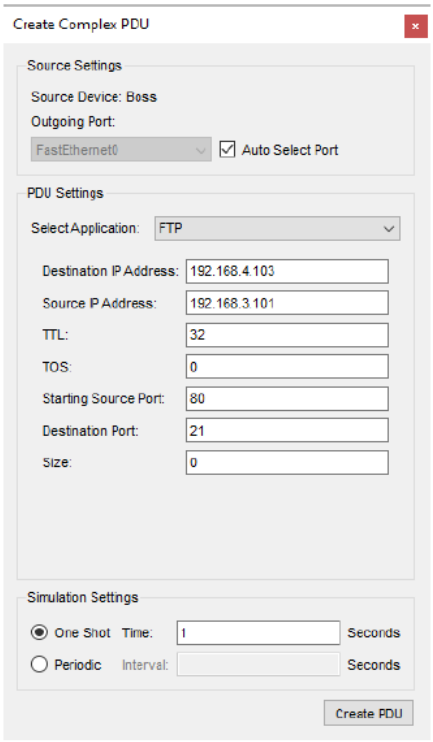


Рис.3.15 Формування FTP-запиту

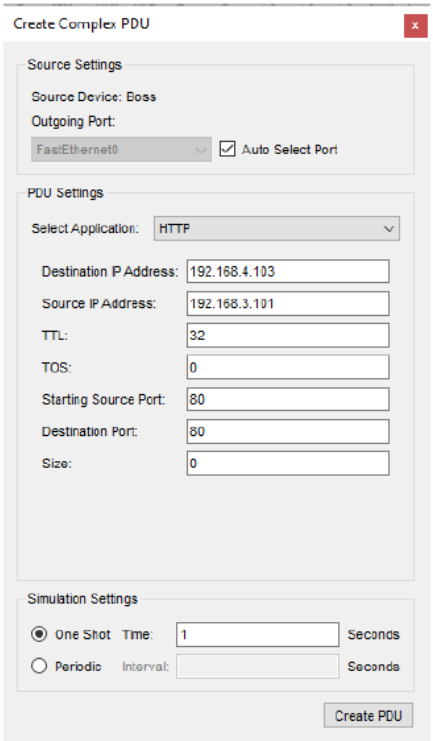


Рис. 3.16 Формування HTTP-запиту

Результати симуляції підтвердили правильність роботи створеного списку контролю доступу. FTP-пакети були заблоковані відповідно до налаштованого правила, тоді як HTTP-трафік успішно досяг сервера та отримав відповідь (рис. 3.17).

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Failed	Boss	192.168.4....	TCP		1.000	N	0
	Successful	Boss	192.168.4....	TCP		1.000	N	1

Рис.3.17 Результат роботи ACL: блокування FTP та дозвіл HTTP-трафіку

Проведене тестування продемонструвало, що розроблений веборієнтований інтерфейс коректно генерує конфігураційні команди Cisco IOS для різних типів розширених списків контролю доступу. Усі створені правила були успішно застосовані до маршрутизаторів та забезпечили очікувану поведінку мережі.

Крім перевірки функціональної правильності роботи системи, було відзначено суттєве спрощення процесу налаштування ACL порівняно з ручним введенням команд через консоль Cisco IOS. Використання графічного інтерфейсу дозволяє скоротити час створення конфігурації, мінімізувати кількість синтаксичних помилок та зробити процес налаштування більш зрозумілим для користувачів із початковим рівнем підготовки.

Таким чином, результати тестування підтверджують доцільність використання розробленої системи як інструмента автоматизації процесу створення та впровадження розширених списків контролю доступу на мережевому обладнанні Cisco. Використання такого підходу сприяє підвищенню ефективності адміністрування мереж, зменшенню кількості конфігураційних помилок та прискоренню впровадження політик мережевої безпеки.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було досліджено принципи функціонування списків контролю доступу (Access Control Lists, ACL) на мережевому обладнанні Cisco та розроблено веборієнтований програмний засіб для автоматизації процесу їх конфігурування.

Під час виконання роботи було проаналізовано сучасні підходи до забезпечення мережевої безпеки в корпоративних комп'ютерних мережах. Встановлено, що списки контролю доступу є одним із найефективніших механізмів фільтрації мережевого трафіку та реалізації політик інформаційної безпеки. Водночас процес їх ручного налаштування потребує спеціальних знань синтаксису Cisco IOS та супроводжується ризиком виникнення конфігураційних помилок.

У межах дослідження було розглянуто особливості стандартних та розширених ACL, визначено їхні переваги, недоліки та сфери застосування. Особливу увагу приділено розширеним спискам контролю доступу, які дозволяють здійснювати фільтрацію трафіку за IP-адресами джерела та призначення, типами протоколів і номерами портів.

Для перевірки працездатності майбутньої системи було створено модель корпоративної мережі в середовищі Cisco Packet Tracer. Розроблена топологія включала декілька логічно відокремлених підмереж, що моделюють роботу різних підрозділів підприємства. На створеній мережі було досліджено роботу найбільш поширених типів розширених ACL, зокрема сценаріїв Host-to-Host, Host-to-Network, Network-to-Host та Network-to-Network, а також фільтрацію трафіку за транспортними протоколами та портами.

На основі проведеного аналізу було спроєктовано та реалізовано веборієнтований графічний інтерфейс, призначений для автоматизованого формування конфігурацій ACL. Для розробки програмного засобу використано сучасні вебтехнології HTML5, CSS3 та JavaScript, що забезпечило

кросплатформність, простоту використання та відсутність необхідності встановлення додаткового програмного забезпечення на стороні користувача.

Розроблений застосунок надає можливість вибору типу ACL, налаштування параметрів джерела та призначення трафіку, визначення протоколів і портів, а також автоматичного генерування готових команд Cisco IOS. Для підвищення надійності роботи системи реалізовано механізми перевірки введених даних та динамічної адаптації інтерфейсу залежно від обраного типу правила.

Експериментальна перевірка працездатності програмного засобу була проведена шляхом застосування згенерованих конфігурацій до маршрутизаторів у середовищі Cisco Packet Tracer. Результати тестування підтвердили коректність роботи системи та відповідність отриманих конфігурацій очікуваним результатам. Згенеровані ACL успішно забезпечували блокування або дозвіл мережевого трафіку відповідно до встановлених правил безпеки.

Практичне значення отриманих результатів полягає у спрощенні процесу налаштування мережевого обладнання Cisco, скороченні часу створення конфігурацій та зменшенні ймовірності помилок під час адміністрування мереж. Розроблена система може використовуватися як навчальний інструмент для вивчення технологій Cisco, а також як допоміжний засіб для мережевих адміністраторів під час налаштування політик контролю доступу.

Перспективами подальшого розвитку роботи є розширення підтримки додаткових типів ACL, реалізація автоматичного підключення до мережевого обладнання через SSH, інтеграція з сучасними платформами мережевої автоматизації, такими як Ansible та Netmiko, підтримка IPv6, а також впровадження механізмів централізованого управління політиками мережевої безпеки.

Таким чином, поставлену мету роботи досягнуто, а всі визначені завдання виконано в повному обсязі. Розроблений програмний засіб підтвердив свою працездатність та ефективність під час моделювання процесу автоматизованого конфігурування списків контролю доступу на мережевому обладнанні Cisco.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Odom W. Cisco CCNA 200-301 Official Cert Guide. Volume 1. Indianapolis : Cisco Press, 2024. 1008 p.

2. Odom W. Cisco CCNA 200-301 Official Cert Guide. Volume 2. Indianapolis : Cisco Press, 2024. 1104 p.

3. Edgeworth B., Hucaby D., Dooley J. CCNP and CCIE Enterprise Core ENCOR 350-401 Official Cert Guide. Indianapolis : Cisco Press, 2023. 1200 p.

4. Hucaby D. Cisco LAN Switching Configuration Handbook. 2nd ed. Indianapolis : Cisco Press, 2022. 700 p.

5. Hucaby D. CCNP Enterprise Advanced Routing ENARSI 300-410 Official Cert Guide. Cisco Press, 2023. 960 p.

6. Stallings W. Network Security Essentials: Applications and Standards. 7th ed. Pearson, 2020. 816 p.

7. Stallings W. Data and Computer Communications. 11th ed. Pearson, 2023. 896 p.

8. Kurose J., Ross K. Computer Networking: A Top-Down Approach. 8th ed. Pearson, 2021. 864 p.

9. Tanenbaum A., Wetherall D. Computer Networks. 6th ed. Pearson, 2021. 960 p.

10. Forouzan B. A. Data Communications and Networking. 6th ed. McGraw-Hill Education, 2022. 1264 p.

11. Edelman J., Lowe S., Oswalt M. Network Programmability and Automation. Sebastopol : O'Reilly Media, 2018. 584 p.

12. Lowe S. Python Network Programming Cookbook. 3rd ed. Birmingham : Packt Publishing, 2022. 670 p.

13. Oswalt M. Network Automation with Go. O'Reilly Media, 2023. 420 p.

14. Limoncelli T., Hogan C., Chalup S. The Practice of System and Network Administration. 3rd ed. Addison-Wesley, 2016. 1232 p.

15. Al-Shaer E., Hamed H. Modeling and Management of Firewall Policies. IEEE Transactions on Network and Service Management. 2021. Vol. 18, No. 3. P. 2581–2595.

16. Szigeti T., Hattingh C. End-to-End QoS Network Design. 2nd ed. Cisco Press, 2021. 1056 p.

17. Mozilla Foundation. HTML Living Standard. URL: https://developer.mozilla.org (дата звернення: 15.06.2026).

18. Duckett J. HTML and CSS: Design and Build Websites. Indianapolis : Wiley, 2021. 490 p.

19. Freeman E., Robson E. Head First HTML and CSS. 3rd ed. Sebastopol : O'Reilly Media, 2024. 800 p.

20. Duckett J. JavaScript and JQuery: Interactive Front-End Web Development. Wiley, 2022. 640 p.

21. Flanagan D. JavaScript: The Definitive Guide. 8th ed. Sebastopol : O'Reilly Media, 2025. 720 p.

22. Simpson K. You Don't Know JS Yet. 2nd ed. O'Reilly Media, 2023. 350 p.

23. Keith J. HTML5 for Web Designers. 2nd ed. A Book Apart, 2021. 160 p.

24. Keith J. CSS in Depth. Manning Publications, 2023. 640 p.

25. Osmani A. Learning JavaScript Design Patterns. O'Reilly Media, 2022. 254 p.

26. Hall B. Pro CSS3 Animation. Apress, 2022. 450 p.

27. Cisco Systems. Cisco IOS Security Configuration Guide. URL: https://www.cisco.com (дата звернення: 15.06.2026).

28. Cisco Systems. Cisco Secure Firewall Configuration Guide. URL: https://www.cisco.com (дата звернення: 15.06.2026).

29. Cisco Systems. Access Control Lists Configuration Guide. URL: https://www.cisco.com (дата звернення: 15.06.2026).

30. Cisco Systems. Cisco Packet Tracer User Guide. URL: https://www.netacad.com (дата звернення: 15.06.2026).

31. Cisco Networking Academy. Introduction to Networks Companion Guide. Cisco Press, 2023. 800 p.

32. Cisco Networking Academy. Switching, Routing, and Wireless Essentials Companion Guide. Cisco Press, 2023. 720 p.

33. Cisco Networking Academy. Enterprise Networking, Security, and Automation Companion Guide. Cisco Press, 2023. 720 p.

34. Byers K. Netmiko Documentation. URL: https://ktbyers.github.io/netmiko (дата звернення: 15.06.2026).

35. NAPALM Developers. Network Automation and Programmability Abstraction Layer with Multivendor Support. URL: https://napalm.readthedocs.io (дата звернення: 15.06.2026).

36. Red Hat. Ansible Documentation. URL: https://docs.ansible.com (дата звернення: 15.06.2026).

37. OpenJS Foundation. Node.js Documentation. URL: https://nodejs.org (дата звернення: 15.06.2026).

38. Python Software Foundation. Python Documentation. URL: https://www.python.org/doc (дата звернення: 15.06.2026).

39. RFC 791. Internet Protocol. URL: https://www.rfc-editor.org/rfc/rfc791 (дата звернення: 15.06.2026).

40. RFC 793. Transmission Control Protocol. URL: https://www.rfc-editor.org/rfc/rfc793 (дата звернення: 15.06.2026).

41. RFC 8200. Internet Protocol, Version 6 (IPv6) Specification. URL: https://www.rfc-editor.org/rfc/rfc8200 (дата звернення: 15.06.2026).

42. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII.

43. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи управління інформаційною безпекою. Вимоги. Київ : ДП «УкрНДНЦ», 2023.

44. Буров Є. В. Комп'ютерні мережі : підручник. Львів : Видавництво Львівської політехніки, 2020. 584 с.