ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«МЕТІНВЕСТ ПОЛІТЕХНІКА»

КОМП’ЮТЕРНІ МЕРЕЖІ:
методичні рекомендації до виконання індивідуального розрахункового завдання

Запоріжжя 2024

metinvest polytechnic

УДК 004.7(072)
К63

Рекомендовано Науково-методичною радою
ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«МЕТІНВЕСТ ПОЛІТЕХНІКА»
(протокол № 3 від 22.11.2024 р.)

Укладач:
Шматко О.В., к.т.н.
Гамаюн І.П., д.т.н.
Держевецька М.А., к.е.н.

К63 Комп'ютерні мережі : методичні рекомендації до виконання індивідуального розрахункового завдання / уклад. О. В. Шматко, І. П. Гамаюн, М. А. Держевецька. Запоріжжя : ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ «МЕТІНВЕСТ ПОЛІТЕХНІКА», 2024. 70 с.

Методичні вказівки включають тематику індивідуальних завдань, методичні пояснення щодо порядку їх виконання, критерії оцінювання виконаного індивідуального завдання, вимоги до його оформлення, включаючи зразок звіту.

Рекомендовано для студентів спеціальності 122 «Комп'ютерні науки» першого (бакалаврського) рівня освіти.

УДК 004.7(072)

ЗМІСТ

ВСТУП

Індивідуальне розрахункове завдання (надалі - ІНДРЗ) виконується з актуальних проблем пов'язаних з методами та моделями штучного інтелекту та являє собою самостійне дослідження, яке є важливою ланкою у системі опанування загальних та фахових компетенцій здобувачами ОПП «Комп'ютерні науки» спеціальності 122 Комп'ютерні науки усіх форм навчання.

Методичні вказівки укладено на підставі Стандарту вищої освіти за спеціальністю 122 Комп'ютерні науки галузі знань 12 Інформаційні технології для першого (бакалаврського) рівня вищої освіти, затвердженого Наказом Міністерства освіти і науки України від 28.04.2022 р. № 393.

В процесі виконання ІНДРЗ передбачається поєднання теоретичних знань і практичних умінь, набутих здобувачами освіти в результаті вивчення дисципліни професійної підготовки бакалавра, а саме: Операційні системи та основи системного програмування.

ІНДРЗ – це індивідуальне завдання, яке є творчим та практичним рішенням конкретних завдань , виконане здобувачем вищої освіти самостійно під керівництвом викладача згідно із поставленими завданнями.

Виконання ІНДРЗ сприяє розширенню та поглибленню теоретичних та практичних знань з основ побудови, принципів проектування, конфігурування й застосування різних сучасних комп'ютерних мереж, від домашніх локальних мереж, або офісних мереж, до масового і глобального Інтернету, розвитку навичок їх практичного використання, формує вміння самостійного розв'язання конкретних професійних завдань, створює наукове підґрунтя для виконання кваліфікаційної роботи бакалавра.

Мета індивідуального розрахункового завдання – поглиблення теоретичних знань та закріплення практичних навичок використання можливостей комп'ютерів для обміну інформацією та спілкування один з одним.

Для досягнення цієї мети необхідно поставити та вирішити такі завдання:

– сформулювати постановку задачі з дослідження проблемної ситуації (практичного завдання) відповідно до обраного варіанту ІНДРЗ;

– побудувати топологію мережі згідно з обраним варіантом ІНДРЗ;

– налаштувати параметрі мережі згідно з обраним варіантом ІНДРЗ;

– застосовувати знання засобів імітаційного моделювання для перевірки працездатності побудованої мережі;

– представити керівнику у встановлений термін результати індивідуального розрахункового завдання, у якому у логічній послідовності відобразити основні етапи і результати дослідження, обґрунтувати методи, засоби, інструменти вирішення проблемної ситуації (практичного завдання), а також очікувані результати і рекомендації і пропозиції вирішення проблемної ситуації (практичного завдання) із застосуванням методів штучного інтелекту;

– підготувати презентацію результатів виконання індивідуального розрахункового завдання у вигляді проєкту і продемонструвати вміння обґрунтовано і коректно викладати та відстоювати власну позицію перед професійною аудиторією та експертами з інших галузей знань під час захисту.

Дисципліна спрямована на отримання здобувачами наступних загальних та спеціальних (фахових) компетентностей:

– СК12. Здатність забезпечити організацію обчислювальних процесів в інформаційних системах різного призначення з урахуванням архітектури, конфігурування, показників результативності функціонування операційних систем і системного програмного забезпечення.

– СК13. Здатність до розробки мережевого програмного забезпечення, що функціонує на основі різних топологій структурованих кабельних систем, використовує комп’ютерні системи і мережі передачі даних та аналізує якість роботи комп’ютерних мереж.

– СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об’єктів критичної інформаційної інфраструктури.

У результаті виконання ІНДРЗ вищої освіти повинен продемонструвати достатній рівень сформованості наступних програмних результатів навчання:

– ПР13. Володіти мовами системного програмування та методами розробки програм, що взаємодіють з компонентами комп’ютерних систем, знати мережні технології, архітектури комп’ютерних мереж, мати практичні навички технології адміністрування комп’ютерних мереж та їх програмного забезпечення.

1. МЕТОДИЧНІ РЕКОМЕНДАЦІЇ З ВИКОНАННЯ ІНДИВІДУАЛЬНОГО РОЗРАХУНКОВОГО ЗАВДАННЯ СТУДЕНТА

Самостійна робота студентів (СРС) займає провідне місце у системі сучасної вищої освіти. З усіх видів навчальної діяльності СРС значною мірою забезпечує формування самостійності як провідної риси особистості студента.

Самостійна робота завершує завдання усіх інших видів навчальної діяльності. Адже знання, що не стали об'єктом власної діяльності, не можуть вважатися дійсним надбанням людини. Тому СРС має навчальне, особисте та суспільне значення.

СРС – це багатоаспектне та поліфункціональне явище з двоєдиністю цілей:

- формування самостійності студента;
- розвиток здібностей, вмінь, знань та навичок студентів.

Завдяки СРС відбувається перехід від переважно виконавчої репродуктивної діяльності студентів до пошукового, творчого начала на всіх етапах навчання у ВНЗ.

Індивідуальне розрахункове завдання (ІНДРЗ) з дисципліни «Комп'ютерні мережі» припускає її здійснення в наступних видах: самостійне вивчення теоретичного матеріалу, самостійне виконання практичних завдань для більш глибокого засвоєння матеріалу.

Метою виконання ІНДРЗ є більше глибоке вивчення сфери застосування та можливостей комп'ютерних мереж, ознайомлення з концепцією шарів, які складають основу, навколо якої будуються мережі, знайомство з концепцією протоколів прикладного рівня, транспортного рівня, включаючи протокол управління передачею (TCP), протокол призначених для користувача дейтаграмм (UDP) і Інтернет-протокол мережевого рівня (IP) і протоколи маршрутизації пакетів, знання мережевих технології, архітектури комп'ютерних мереж, отримання практичних навичок технології адміністрування комп'ютерних мереж.

Правильна організація самостійної роботи необхідна для більш повного оволодіння дисципліною та визначає успішність здачі заліку й наступної практичної діяльності.

Самостійна робота виконується студентами під керівництвом викладача, який здійснює аудиторну роботу в навчальній групі.

Самостійна робота студентів повинна мати такі головні ознаки:

- бути виконаною особисто студентом;

– бути закінченою розробкою, де розкриваються й аналізуються актуальні проблеми з певної теми або її окремих аспектів;

– демонструвати достатню компетентність автора в розкритті питань, що досліджуються;

– мати навчальну, наукову, й/або практичну спрямованість і значимість;

– містити певні елементи новизни;

– самостійна індивідуальна розрахункова робота оформляється відповідно до вимог кафедри.

1.1 Основні вимоги до виконання індивідуального розрахункового завдання

Перед виконанням самостійної роботи потрібно повністю ознайомитися зі змістом завдання, підібрати потрібну літературу, визначити усі параметри виконання індивідуального завдання.

Результатом виконання самостійної роботи є звіт, який виконується з використанням комп'ютерної техніки та надрукований на папері формату А4. Оформлення звіту: шрифт − Arial; розмір шрифту − 14 кегель; інтервал між рядками − півтора; абзац − 12,5 мм, поля: верхнє і нижнє – 20 мм, ліве – 25 мм, праве – 15 мм; нумерація сторінок − по центру нижнього поля. Зразок оформлення звіту наведено у додатку А.

Після перевірки кожного завдання викладачем студент зобов'язаний усунути допущені помилки, інакше він не допускається до виконання наступного завдання.

Усі види самостійної роботи повинні бути здані у встановлений графіком термін. Викладач фіксує факт здачі кожної роботи та виставляє оцінку в журнал.

Поради із планування й організації часу, необхідного для виконання самостійної роботи

Раціональне планування і організація самостійної роботи студентів є найважливішою умовою її ефективності.

Планування самостійної роботи направлено на формування логічно вибудуваної, прозорої, зрозумілої, доступної і ефективної системи організації самостійної роботи та її оцінки.

При цьому необхідно пам'ятати, що самостійна робота студентів виконує в навчальному процесі кілька функцій:

− розвиваючу (підвищення культури розумової праці, привчання до творчих видів діяльності, вдосконалення інтелектуальних здібностей студентів);

− інформаційно-навчальну (навчальна діяльність на аудиторних заняттях, непідкріплена самостійною роботою, стає мало результативною);

− орієнтуючу і стимулюючу (процесу навчання надається прискорення і мотивація);

− виховну (формуються і розвиваються професійні якості фахівця);

− дослідницьку (новий рівень професійно-творчого мислення).

В основі самостійної роботи студентів лежать наступні принципи: розвиток творчої діяльності, цільове планування, особистісно-діяльнісний підхід.

Самостійну роботу можна назвати ефективною тільки в тому випадку, якщо вона організована і реалізується в освітньому процесі як цілісна система на всіх етапах навчання.

Можна виділити кілька об’єктивних закономірностей організації самостійної роботи студентів:

− творча складова самостійної роботи зростає в міру навчання;

− в процесі організації самостійної роботи виникає потреба в методичному забезпеченні;

− застосування інформаційних технологій стає частиною організації і моніторингу самостійної роботи студентів на всіх її етапах.

У процесі самостійної роботи студент набуває навиків самоорганізації, самоконтролю, самоврядування, саморефлексії і стає активним самостійним суб’єктом навчальної діяльності.

Самостійна робота повинна давати важливий вплив на формування особистості майбутнього фахівця. Кожен, хто навчається самостійно планує режим своєї роботи з урахуванням часу роботи бібліотеки, профільних лабораторій, комп’ютерних класів і т.п. Він виконує самостійну роботу за особистим індивідуальним планом, в залежності від його підготовки, часу та інших умов.

Першим завданням в організації позааудиторної самостійної роботи є складання розкладу, що відображає час занять і їх характер, перерви на обід, вечеря, відпочинок, сон, проїзд і т.п. Із самого початку студенту не потрібно прагнути робити відразу найважчу її частину. Доцільно вибрати щось середнє за складністю. Після цього, перейти до

більш важкої роботи, легке залишивши наостанок. Розумову працю необхідно не тільки правильно організувати, а й стимулювати. Важливо вміти підтримувати стійку увагу до досліджуваного матеріалу. Вироблення уваги вимагає значних вольових зусиль від студента. Стійка увага з'являється тоді, коли людина ставиться до справи з інтересом.

Слід правильно організувати свої заняття за часом: 50 хвилин − робота, 5-10 хвилин − перерва, після 3 годин роботи перерва − 20-25 хвилин. Інакше наростаюча втома спричинить нестійкість уваги. Організація активного відпочинку передбачає чергування розумової та фізичної діяльності, що відновлює працездатність людини.

1.2 Опис послідовності дій студента при виконанні самостійної роботи

Організацію самостійної роботи можна умовно розділити на три етапи:

- планування навчальної діяльності та її методична підготовка;
- здійснення цієї діяльності та її супровід;
- контроль, аналіз результатів (з можливими змінами в плануванні самостійної роботи).

Рекомендації щодо використання матеріалів навчально-методичного комплексу навчальної дисципліни

Зміст вивчення дисципліни "Комп`ютерні мережі" визначено її робочою програмою.

Інформативну частину навчання складають навчальні посібники, конспекти лекцій у паперовій та електронній формі, план, зміст та методичні рекомендації до проведення лабораторних занять, методичні рекомендації до виконання самостійної роботи, перелік рекомендованої до вивчення літератури, ресурси мережі Інтернет.

У рекомендаціях до виконання індивідуального розрахункового завдання з дисципліни "Комп'ютерні мережі" містяться варіанти індивідуальних завдань та перелік питань для самостійного опрацювання матеріалу. Також зазначається короткий теоретичний коментар до кожної теми, що допомагає студентові ознайомитися із сутністю питань, на основі яких базується виконання завдань.

1.3 Рекомендації щодо роботи з літературою

Найважливішим інформаційним джерелом вивчення навчальної дисципліни «Операційні системи та основи системного програмування» є ресурси мережі Інтернет. Основна частина матеріалу в Інтернеті розрахована на професіоналів, тому при вивченні навчальної дисципліни спочатку необхідно користуватися літературою навчального характеру.

При опрацюванні матеріалу потрібно дотримуватись таких правил:

1. Зосередитися на тому, що читаєш.
2. Виділити головну думку автора.
3. Виділити основні питання тексту від другорядних.
4. Зрозуміти думку автора чітко і ясно, що допоможе виробити власну думку.
5. Уявити ясно те, що читаєш.

У процесі роботи над темою тлумачення незнайомих слів і спеціальних термінів слід знаходити у фаховій літературі, термінологічних словниках. Незрозумілі місця, фрази, вирази доречно перечитувати декілька разів, щоб зрозуміти їх зміст.

Після прочитання тексту необхідно:

1. Усвідомити зв’язок між теоретичними положеннями і практикою.
2. Закріпити прочитане у свідомості.
3. Пов’язати нові знання з попередніми у даній галузі.
4. Перейти до заключного етапу засвоєння і опрацювання – записам.

Записи необхідно починати з назви теми та посібника, прізвища автора, року видання та назви видавництва. Якщо це журнал, то рік і номер видання, заголовок статті. Після чого скласти план, тобто короткий перелік основних питань тексту в логічній послідовності теми.

Складання плану, або тез логічно закінченого за змістом уривка тексту, сприяє кращому його розумінню. План може бути простий або розгорнутий, тобто більш поглиблений, особливо при опрацюванні додаткової літератури за даною темою. Записи необхідно вести розбірливо і чітко. Вони можуть бути короткі або розгорнуті залежно від рівня знань студента, багатства його літературної і професійної лексики, навичок самостійної роботи з книгою.

Для зручності користування записами необхідно залишати поля для заміток і вільні рядки для доповнень. Записи не повинні бути

одноманітними. В них необхідно виділяти важливі місця, головні слова, які акцентуються різним шрифтом або різним кольором шрифтів, підкреслюванням, замітками на полях, рамками, стовпчиками тощо. Записи можуть бути у вигляді конспекту, простих або розгорнутих тез, цитат, виписок, систематизованих таблиць, графіків, діаграм, схем.

1.4 Поради із підготовки до поточного, проміжного та підсумкового контролю

Контрольні заходи включають поточний і підсумковий контроль знань студентів. Поточний контроль є органічною частиною навчального процесу і проводиться під час лекцій та лабораторних занять.

Форми поточного контролю:

- усна співбесіда за матеріалами розглянутої теми на початку лабораторного заняття з оцінкою відповідей студентів (5-10 хв.);
- письмове фронтальне опитування студентів на початку чи в кінці лабораторного заняття (5-10 хв.). Відповіді перевіряються і оцінюються викладачем у поза аудиторний час;
- перевірка виконання завдань лабораторних робіт;
- тестова перевірка знань студентів;
- модульний контроль;
- інші форми.

При кредитно-модульній системі навчання теми самостійної роботи входять у модуль, який контролюються після закінчення логічно завершеної частини лекцій та інших видів занять з дисципліни та їх результати враховуються при виставленні підсумкової оцінки.

2. ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ ЩОДО ВИКОНАННЯ ІНДИВІДУАЛЬНОГО РОЗРАХУНКОВОГО ЗАВДАННЯ №1

2.1 Теоретичні відомості. Налаштування мережевих сервісів DNS, DHCP і Web

Мета роботи: вивчення принципів роботи та налаштування протоколу **DHCP (Dynamic Host Configuration Protocol)** для автоматичного призначення мережевих параметрів вузлам у комп'ютерній мережі [1,2]. У ході роботи студенти набудуть навичок налаштування **DHCP**-сервера на мережевому обладнанні, а також конфігурації **DHCP**-клієнтів. Крім того, ця робота спрямована на оволодіння методами моніторингу та діагностування роботи **DHCP** для забезпечення стабільного функціонування мережі.

Призначення параметрів вузлу в IP-мережі є ключовим процесом, що забезпечує коректне функціонування мережевого обладнання та обмін даними між пристроями. Для ефективної роботи кожен вузол (комп'ютер, смартфон, принтер тощо) повинен отримати унікальну IP-адресу та інші мережеві параметри, які дозволяють ідентифікувати його у мережі й забезпечити доступ до інших ресурсів.

Основні параметри, що призначаються вузлу в IP-мережі [3]:

1. IP-адреса - Унікальний числовий ідентифікатор вузла в мережі, який дозволяє іншим пристроям визначати його місцезнаходження для маршрутизації трафіку. IP-адреси можуть бути статичними (призначаються вручну) або динамічними (призначаються автоматично через **DHCP**).

2. Маска підмережі - Визначає діапазон адрес, які належать до тієї ж мережі, і допомагає маршрутизаторам правильно обробляти пакети даних, визначаючи, чи знаходиться призначений пристрій у локальній чи зовнішній мережі.

3. Шлюз за замовчуванням (**Default Gateway**) - IP-адреса маршрутизатора, що з’єднує локальну мережу з іншими мережами. Шлюз за замовчуванням забезпечує передачу даних між вузлом і зовнішніми мережами, зокрема Інтернетом.

4. **DNS**-сервери (**Domain Name System**) - Сервери, які дозволяють вузлам перетворювати доменні імена (наприклад, www.example.com) на IP-адреси. Вузли звертаються до **DNS**-серверів для визначення IP-

адреси веб-сайтів та інших ресурсів, до яких вони хочуть отримати доступ.

5. Додаткові параметри (опціонально) - Інші мережеві налаштування, такі як **WINS**-сервери, домен для пошуку (search domain), опції маршрутизації тощо, які можуть додатково оптимізувати мережеві з'єднання.

Протокол **DHCP** (**Dynamic Host Configuration Protocol**) є стандартним механізмом автоматичного призначення IP-адрес та інших мережевих параметрів вузлам у мережі. **DHCP**-сервер керує пулом доступних IP-адрес і автоматично розподіляє їх між клієнтами (вузлами), забезпечуючи динамічну конфігурацію мережі та зменшуючи потребу в ручному налаштуванні [4].

Міжмережний обмін забезпечує передачу даних між різними локальними мережами та підключення до глобальної мережі, зокрема Інтернету. Це є основою сучасної мережевої інфраструктури, що дозволяє пристроям з різних мереж взаємодіяти між собою і отримувати доступ до зовнішніх ресурсів. Основним пристроєм для реалізації міжмережного обміну є маршрутизатор, який аналізує IP-адреси пакетів і визначає оптимальний шлях для їх передачі. Маршрутизатор також виконує функцію шлюзу за замовчуванням, забезпечуючи вихід з локальної мережі до зовнішніх мереж.

Оптимальний обмін даними між мережами підтримується за допомогою протоколів маршрутизації, таких як **OSPF, EIGRP, RIP та BGP** [5], які дозволяють маршрутизаторам обмінюватися інформацією про топологію мережі і вибирати найкращі шляхи для передачі даних. Для підключення приватних мереж до Інтернету часто застосовується протокол NAT (Network Address Translation) [6], який транслює внутрішні IP-адреси у зовнішні, дозволяючи всім пристроям у локальній мережі мати доступ до Інтернету, а також приховує внутрішню структуру мережі від зовнішніх користувачів, підвищуючи рівень безпеки.

Ще одним важливим елементом міжмережного обміну є **VPN (Virtual Private Network)** [7], яка створює захищені канали для обміну даними між віддаленими мережами або пристроями через Інтернет. Це особливо корисно для організацій, які потребують безпечного зв'язку між офісами чи доступу до корпоративної мережі з віддалених локацій. Захист міжмережного обміну додатково забезпечується за допомогою фаєрволів, які контролюють доступ і фільтрують трафік між локальними та зовнішніми мережами, блокуючи небажані з'єднання та захищаючи мережу від потенційних загроз.

Загалом, міжмережний обмін виконує важливі функції, включаючи об’єднання окремих мереж у єдину комунікаційну мережу, підключення пристроїв у приватних мережах до Інтернету, а також забезпечення безпеки обміну даними. Використання маршрутизаторів, **NAT, VPN** і фаєрволів [8] сприяє побудові оптимальної, захищеної та надійної інфраструктури для міжмережної взаємодії.

Для забезпечення доступу до ресурсів серверів за допомогою символьних доменних імен необхідно налаштувати використання DNS-сервера, який відповідає за перетворення доменних імен на відповідні IP-адреси. Коли користувач або пристрій у мережі звертається до певного ресурсу за доменним ім’ям, DNS-сервер виконує запит і повертає відповідну IP-адресу, що дозволяє здійснити підключення до потрібного сервера.

Щоб мережевий пристрій міг користуватися **DNS**, необхідно вказати IP-адресу **DNS**-сервера у налаштуваннях мережі. Це можна зробити як вручну, так і автоматично, якщо мережа використовує **DHCP**-сервер, який надає параметри підключення, включаючи IP-адресу **DNS**-сервера. Налаштування **DNS** є важливим елементом для забезпечення зручного та швидкого доступу до мережевих ресурсів, оскільки користувачам не потрібно запам’ятовувати числові IP-адреси; вони можуть просто вводити символьні доменні імена, які зрозумілі та легкі для використання.

Призначення параметрів IP-адресації може здійснюватися як статично, так і динамічно, залежно від потреб і налаштувань мережі. У разі статичного призначення адміністратор вручну конфігурує IP-адреси для кожного пристрою, що дозволяє точно контролювати розподіл адрес і забезпечувати стабільність мережевих налаштувань. Цей метод особливо ефективний для серверів та інших важливих мережевих ресурсів, де необхідно забезпечити постійне з'єднання та стабільний IP.

Динамічне призначення, навпаки, здійснюється автоматично за допомогою спеціальних технологій та протоколів, зокрема протоколу **DHCP (Dynamic Host Configuration Protocol). DHCP** дозволяє автоматично надавати пристроям у мережі IP-адреси, маску підмережі, шлюз за замовчуванням і **DNS**-сервери, що спрощує адміністрування, особливо в мережах з великою кількістю пристроїв. Такий підхід дозволяє оптимально використовувати пул IP-адрес та знижує ризик конфліктів адрес, автоматично вивільняючи IP після закінчення терміну оренди.

Таким чином, статичне призначення IP використовується для фіксованих пристроїв, які вимагають стабільного доступу, тоді як динамічне призначення IP значно полегшує управління адресацією у великих і динамічних мережах.

Наприклад, в операційних системах Unix/Linux для налаштування мережевих параметрів застосовується команда **ifconfig**. Ця команда дозволяє адміністратору вручну конфігурувати IP-адресу, маску підмережі, шлюз та інші параметри інтерфейсу, необхідні для підключення до мережі. Команда **ifconfig** є важливим інструментом для статичного призначення параметрів IP-адресації.

Серед засобів динамічного призначення параметрів IP-адресації в першу чергу слід згадати такі технології та протоколи, як **DHCP (Dynamic Host Configuration Protocol)**. **DHCP** є основним стандартом для автоматичного призначення IP-адрес та інших мережевих параметрів (наприклад, маски підмережі, шлюзу за замовчуванням, **DNS**-серверів). Використання **DHCP** значно спрощує управління мережевими налаштуваннями, особливо в великих мережах, оскільки адміністратору не потрібно вручну конфігурувати кожен пристрій.

Ще однією важливою технологією для динамічного призначення мережевих параметрів є **APIPA (Automatic Private IP Addressing** [9].

APIPA (Automatic Private IP Addressing) — це функція автоматичного призначення IP-адрес у локальних мережах, яка дозволяє пристроям самостійно отримувати IP-адресу у випадку, якщо **DHCP**-сервер недоступний. **APIPA** розроблена для забезпечення базового підключення між пристроями у межах однієї мережі, навіть без централізованого **DHCP**-сервера.

APIPA активується, коли пристрій намагається отримати IP-адресу через **DHCP**, але не отримує відповіді від **DHCP**-сервера. У такому випадку пристрій автоматично призначає собі IP-адресу з резервного пулу **169.254.0.0/16**, тобто з діапазону від **169.254.0.1** до **169.254.255.254**. Після цього пристрій періодично продовжує запити до DHCP-сервера, і якщо сервер стає доступним, APIPA-адреса автоматично замінюється на адресу, отриману від DHCP.

APIPA дозволяє пристроям спілкуватися між собою в межах локальної мережі без необхідності в DHCP-сервері, забезпечуючи мінімальну мережеву доступність.

APIPA використовує спеціально зарезервований діапазон IP-адрес (169.254.0.0/16), який не маршрутизується за межі локальної

мережі. Це означає, що пристрої з **APIPA**-адресами не можуть підключатися до зовнішніх мереж, зокрема Інтернету.

Коли пристрій генерує **APIPA**-адресу, він перевіряє її унікальність, щоб уникнути конфліктів у мережі. Якщо адреса вже використовується іншим пристроєм, система обирає нову адресу з того ж діапазону.

APIPA забезпечує тимчасове підключення, дозволяючи пристроям обмінюватися даними в локальній мережі, поки DHCP-сервер знову не стане доступним. Як тільки DHCP-сервер починає відповідати на запити, пристрій автоматично отримує нову IP-адресу з DHCP.

APIPA корисна у невеликих локальних мережах або в мережевих середовищах, де тимчасово недоступний **DHCP**-сервер, оскільки вона дозволяє пристроям залишатися підключеними один до одного. Проте основним обмеженням **APIPA** є те, що вона не забезпечує підключення до Інтернету або зовнішніх мереж. APIPA призначена для локального використання і не може бути маршрутизована за межі локальної мережі.

Протокол віддаленого завантаження **BOOTP (Bootstrap Protocol)**— це мережевий протокол, розроблений для автоматичного призначення IP-адрес та передачі конфігураційних даних пристроям у мережі під час їхнього завантаження [10]. **BOOTP** використовується в середовищах, де клієнтські пристрої не мають постійного зберігання налаштувань мережі, таких як дисковіless робочі станції або мережеві пристрої, що потребують динамічної конфігурації.

BOOTP працює за схемою клієнт-сервер і дозволяє клієнтам запитувати у **BOOTP**-сервера мережеві параметри під час завантаження. Основні функції цього протоколу включають:

1. Призначення IP-адреси. Клієнтський пристрій надсилає запит **BOOTP**-серверу, який у відповідь призначає йому IP-адресу. Ця адреса зазвичай надається з заздалегідь визначеного пулу адрес.

2. Передача конфігураційних параметрів. Крім IP-адреси, **BOOTP** може передавати інші мережеві параметри, такі як маска підмережі, шлюз за замовчуванням і IP-адреса сервера **DNS**, що забезпечує належну інтеграцію пристрою в мережу.

3. Завантаження операційної системи. **BOOTP** може вказувати клієнту на сервер, де зберігається операційна система або інше програмне забезпечення, необхідне для завантаження пристрою. Завантаження здійснюється через **TFTP** (Trivial File Transfer Protocol), який передає файли безпосередньо клієнту.

BOOTP широко застосовувався в ранніх мережах, де було необхідне віддалене завантаження пристроїв. Проте з часом BOOTP був частково замінений більш сучасним протоколом **DHCP (Dynamic Host Configuration Protocol),** який розширив функціональні можливості **BOOTP** та додав динамічне управління IP-адресами. Однак, у деяких системах **BOOTP** досі використовується, особливо в середовищах, де важлива простота та статичність конфігурації.

BOOTP залишається важливим протоколом для віддаленого завантаження і автоматичної конфігурації пристроїв у мережах з обмеженими вимогами до динамічності. Він забезпечує автоматичне призначення IP-адрес, передачу конфігураційних даних і завантаження операційної системи, що є важливим для дисковless станцій та інших мережевих пристроїв.

Призначення параметрів IP-адресації за допомогою засобів протоколу **DHCP** (надалі призначення IP-адрес) може бути виконано одним з трьох способів [11]:

1. Динамічне призначення IP-адреси — найпоширеніший метод, при якому **DHCP**-сервер автоматично виділяє IP-адресу з пулу доступних адрес на обмежений термін (так званий "лізинг"). Після закінчення цього часу адреса або оновлюється, або повертається в пул для повторного використання іншими пристроями. Динамічне призначення дозволяє ефективно використовувати IP-адреси, особливо в мережах з великою кількістю пристроїв.

2. Автоматичне призначення IP-адреси — метод, за якого DHCP-сервер постійно закріплює виділену IP-адресу за певним пристроєм після першого підключення. У випадку автоматичного призначення пристрою буде надана та ж IP-адреса, яку він отримав спочатку, що забезпечує постійність адреси без необхідності ручного налаштування.

3. Статичне призначення IP-адреси — метод, при якому адміністратор вручну прив'язує IP-адресу до конкретного пристрою на основі його MAC-адреси. Цей метод часто використовується для серверів, принтерів та інших пристроїв, що потребують стабільного мережевого з’єднання з фіксованою IP-адресою. Статичне призначення забезпечує стабільність та прогнозованість у використанні IP-адрес.

Протокол **DHCP** дозволяє гнучко управляти IP-адресацією в мережі, використовуючи динамічний, автоматичний або статичний методи призначення адрес залежно від потреб конкретного пристрою або мережевого середовища.

Динамічне призначення IP-адрес є найпоширенішим методом, оскільки воно забезпечує ефективне використання адресного простору. У цьому випадку адреса надається пристрою на обмежений час (лізинг), після закінчення якого вона може бути повернута в пул для використання іншими пристроями. Цей підхід спрощує управління мережею, знижуючи потребу в ручному налаштуванні адрес для кожного нового пристрою. Проте динамічне призначення не забезпечує стабільності IP-адреси, яка може змінюватися після кожного перезавантаження чи закінчення терміну лізингу. Така непостійність ускладнює використання для пристроїв, що потребують стабільного з'єднання, як-от сервери.

Автоматичне призначення IP-адрес передбачає закріплення певної IP-адреси за пристроєм після його першого підключення до мережі, що забезпечує постійність адреси без необхідності ручного налаштування. Це дозволяє пристрою завжди отримувати ту ж саму адресу при підключенні, що є зручним з точки зору користувачів і знижує навантаження на адміністрування. Водночас автоматичне призначення IP-адрес може знижувати ефективність використання адресного простору, оскільки зарезервовані IP-адреси не повертаються до загального пулу, а нові пристрої можуть не отримати доступу до мережі за відсутності DHCP-сервера.

Статичне призначення IP-адрес передбачає ручне закріплення адреси за пристроєм, що забезпечує стабільність та передбачуваність з'єднання. Цей метод є особливо доцільним для серверів, принтерів та інших мережевих пристроїв, які потребують постійного доступу за фіксованою адресою. Проте цей метод потребує значних адміністративних зусиль, оскільки IP-адреси повинні налаштовуватися вручну для кожного пристрою, що може ускладнити управління в масштабних мережах. Також можливі конфлікти IP-адрес при помилковому дублюванні адрес, що може призвести до збоїв у роботі мережі. Крім того, статичне призначення може обмежувати наявність адрес для нових пристроїв, оскільки IP-адреси залишаються зарезервованими навіть за відсутності активного використання.

Кожен із способів призначення IP-адрес має свої особливості й обмеження, і вибір методу залежить від специфіки та вимог мережевого середовища. Динамічне призначення оптимальне для мереж із великою кількістю тимчасових підключень, автоматичне забезпечує стабільність адреси без додаткових зусиль, а статичне ідеально підходить для пристроїв, які потребують фіксованого і постійного підключення.

Більшість сучасних виробників маршрутизаторів (зокрема Cisco, Huawei, Juniper) реалізовуються підтримку функціонування як **DHCP**-серверів, так і **DHCP**-клієнтів та зв'язних агентів на своїх пристроях.

Порядок налагодження DHCP-сервера на базі маршрутизатора Cisco.

Налагодження **DHCP**-сервера на базі маршрутизатора Cisco включає кілька основних етапів, що забезпечують коректне функціонування протоколу **DHCP** для автоматичного призначення IP-адрес і мережевих параметрів клієнтам у мережі [12]. Першим кроком є перехід у режим глобальної конфігурації маршрутизатора для виконання налаштувань.

На початку налаштовується пул адрес, який **DHCP**-сервер буде розподіляти серед клієнтів. Для цього створюється пул **DHCP** за допомогою команди `*ip dhcp pool <name>*`, де `*<name>*` — це унікальне ім'я пулу. У межах пулу потрібно визначити діапазон IP-адрес, які будуть надані клієнтам, використовуючи команду `*network <IP-адреса мережі> <маска підмережі>*`.

Далі вказуються додаткові параметри мережі, які клієнти отримають разом із IP-адресою. Зазвичай це адреса шлюзу за замовчуванням, яку можна налаштувати командою `*default-router <IP-адреса шлюзу>*`, а також IP-адреси **DNS**-серверів, задані командою `*dns-server <IP-адреса DNS-сервера>*`. Це забезпечує коректний доступ клієнтів до Інтернету та можливість виконання DNS-запитів.

За необхідності можна налаштувати тривалість оренди адреси для клієнтів за допомогою команди `*lease <тривалість оренди>*`, яка задає час, на який клієнту надається IP-адреса. Після закінчення цього терміну клієнт може отримати нову адресу або продовжити оренду існуючої.

Якщо в мережі є адреси або пристрої, для яких не потрібно призначати IP-адресу через **DHCP**, їх можна виключити з пулу, використовуючи команду `*ip dhcp excluded-address <початкова IP-адреса> <кінцева IP-адреса>*`. Це дозволяє зарезервувати певні адреси для конкретних пристроїв або налаштувань, таких як сервери чи статичні IP-адреси.

Завершивши налаштування, можна перевірити коректність роботи DHCP-сервера на маршрутизаторі Cisco за допомогою команд діагностики, таких як `*show ip dhcp pool*` для перевірки конфігурації пулу, `*show ip dhcp binding*` для перегляду виділених IP-адрес і `*show ip dhcp conflict*` для виявлення конфліктів адрес.

Порядок налаштування **DHCP**-сервера на маршрутизаторі Cisco включає налаштування пулу адрес, конфігурацію шлюзу, **DNS**-серверів, виключення певних адрес з пулу, а також перевірку функціонування **DHCP**-сервера для забезпечення надійного розподілу IP-адрес у мережі.

Команди налагодження DHCP-сервера на базі маршрутизатора Cisco.

Для налаштування **DHCP**-сервера на маршрутизаторі Cisco використовується набір команд, які дозволяють створити пул IP-адрес, задати мережеві параметри, визначити додаткові опції та перевірити правильність налаштування. Нижче наведено основні команди для конфігурації **DHCP**-сервера на маршрутизаторі **Cisco**.

Основні команди для налагодження **DHCP**-сервера

1. Вхід у режим глобальної конфігурації

```
enable
configure terminal
```

Ці команди дозволяють перейти в режим глобальної конфігурації маршрутизатора.

2. Визначення пулу DHCP

```
ip dhcp pool <ім'я пулу>
```

Створює DHCP-пул із заданим ім'ям, у якому будуть налаштовані основні параметри для клієнтів.

3. Задання діапазону IP-адрес для пулу

```
network <IP-адреса мережі> <маска підмережі>
```

Ця команда вказує діапазон IP-адрес, які DHCP-сервер буде виділяти клієнтам.

4. Встановлення адреси шлюзу за замовчуванням

```
default-router <IP-адреса шлюзу>
```

Визначає IP-адресу шлюзу за замовчуванням, який буде наданий клієнтам.

5. Налаштування DNS-сервера

```
dns-server <IP-адреса DNS-сервера>
```

Задає IP-адресу DNS-сервера, який буде використовуватися для перетворення доменних імен на IP-адреси.

6. Встановлення тривалості оренди IP-адрес

```
lease <дні> <години> <хвилини>
```

Визначає період оренди IP-адреси, наданої клієнту. Якщо час оренди не заданий, використовується значення за замовчуванням.

7. Виключення IP-адрес із пулу

```
ip dhcp excluded-address <початкова IP-адреса> <кінцева IP-адреса>
```

Виключає певний діапазон адрес з пулу, запобігаючи їхньому автоматичному призначенню клієнтам. Це корисно для статичних адрес або зарезервованих пристроїв.

Команди перевірки роботи DHCP-сервера

1. Перевірка налаштувань пулу DHCP

```
show ip dhcp pool
```

Виводить інформацію про створений пул DHCP, включаючи кількість доступних та виділених IP-адрес.

2. Перегляд виділених IP-адрес (зв'язування)

```
show ip dhcp binding
```

Показує IP-адреси, які були виділені клієнтам, а також їхні MAC-адреси.

3. Виявлення конфліктів IP-адрес

```
show ip dhcp conflict
```

Відображає список конфліктів IP-адрес у мережі. Конфлікти можуть виникати, якщо декілька пристроїв намагаються використовувати ту саму IP-адресу.

Після налаштування DHCP-сервера на маршрутизаторі Cisco слід зберегти конфігурацію для забезпечення її збереження після перезавантаження:

```
write memory
```

Цей набір команд дозволяє повністю налаштувати **DHCP**-сервер на маршрутизаторі Cisco, включаючи створення пулу IP-адрес, налаштування мережевих параметрів, виключення певних адрес з пулу, а також діагностику та перевірку коректності роботи DHCP-сервера.

Типи серверів. Cisco Server.

Сервери – це потужні обчислювальні системи, призначені для зберігання, обробки та розподілу даних, а також для надання ресурсів і послуг іншим комп'ютерам у мережі. Залежно від функцій та ролей у мережі, сервери можуть бути різних типів:

1. **Файлові сервери** – зберігають файли та дозволяють користувачам у мережі доступ до них. Вони використовуються для централізованого зберігання та управління файлами.
2. **Веб-сервери** – обробляють HTTP-запити від клієнтів і надають доступ до веб-сторінок та веб-додатків через Інтернет або внутрішню мережу.

3. **Бази даних (сервери баз даних)** – використовуються для зберігання, управління та доступу до баз даних, надаючи клієнтам структуровану інформацію.

4. **DHCP-сервери** – автоматично призначають IP-адреси пристроям у мережі, що спрощує налаштування мережевих з'єднань.

5. **DNS-сервери** – відповідають за перетворення доменних імен на IP-адреси, що забезпечує доступ до ресурсів за символьними іменами.

6. **Проксі-сервери** – виступають посередниками між клієнтами та Інтернетом, забезпечуючи додатковий рівень безпеки та оптимізуючи трафік.

7. **Поштові сервери** – використовуються для відправлення, отримання та зберігання електронної пошти.

8. **Віртуальні сервери** – розділяють фізичний сервер на декілька віртуальних екземплярів, кожен з яких працює як незалежний сервер. Це дозволяє оптимізувати ресурси та знижувати витрати на обладнання.

Cisco Server – це апаратне або програмне забезпечення, яке надає мережеві послуги та рішення для організації корпоративних мереж та центрів обробки даних. Компанія Cisco Systems є провідним виробником мережевого обладнання та серверів, розробляючи різноманітні рішення для різних потреб у мережах.

Основні типи серверів Cisco [12]:

1. **Cisco UCS (Unified Computing System)** – інтегрована обчислювальна інфраструктура, що об'єднує сервери, сховища та мережеві ресурси. UCS дозволяє централізовано керувати інфраструктурою, підвищувати продуктивність і масштабованість.

2. **Cisco UCS C-Series** – це сервери в форматі стоякових серверів (rack servers), призначені для високопродуктивних додатків і корпоративних центрів обробки даних. C-Series забезпечують баланс між продуктивністю, ємністю та ефективністю.

3. **Cisco UCS B-Series** – це сервери у форматі блейд-серверів, що дозволяють компактно розміщувати обчислювальні ресурси у шасі. Блейд-сервери забезпечують високу щільність розміщення серверів, що дозволяє знижувати витрати на охолодження та електроенергію.

4. **Cisco HyperFlex** – інтегроване рішення для гіперконвергентної інфраструктури, яке об'єднує обчислювальні ресурси, сховища даних і мережеві функції в одному рішенні. HyperFlex оптимізований для

роботи з віртуальними машинами та хмарними сервісами, що підвищує гнучкість і спрощує керування інфраструктурою.

5. **Cisco Cloud Servers** – надають інфраструктуру для побудови приватних і гібридних хмар, що дозволяє компаніям використовувати хмарні сервіси та оптимізувати управління даними. Рішення Cisco для хмарного середовища підтримують масштабованість і автоматизацію, що є важливим для сучасних хмарних додатків.

Cisco Server та їх різновиди забезпечують широкий спектр послуг для побудови, керування та оптимізації мережевої інфраструктури. Відмінні риси серверів Cisco – це висока надійність, продуктивність і інтегровані рішення для різноманітних потреб, включаючи хмарні, корпоративні й центрів обробки даних.

Cisco Packet Tracer – це потужний інструмент симуляції мереж, який дозволяє проводити налаштування різних мережевих сервісів і технологій. Він надає можливість створювати, тестувати та налагоджувати мережі, дозволяючи студентам, інженерам і адміністраторам експериментувати з мережевими конфігураціями в безпечному середовищі.

Cisco Packet Tracer підтримує налаштування таких мережевих сервісів [12]:

1. **DHCP (Dynamic Host Configuration Protocol)** – забезпечує автоматичне призначення IP-адрес та інших параметрів мережі (шлюз, DNS-сервери) клієнтам у мережі, що спрощує управління IP-адресами.

2. **DNS (Domain Name System)** – дозволяє налаштовувати сервери для перетворення доменних імен на IP-адреси, що забезпечує доступ до ресурсів за символьними іменами.

3. **HTTP і HTTPS (Hypertext Transfer Protocol Secure)** – моделює роботу веб-серверів і клієнтів, дозволяючи тестувати доступ до веб-сторінок через HTTP і HTTPS.

4. **FTP (File Transfer Protocol)** – дозволяє налаштувати сервери та клієнтів для передачі файлів у мережі. Це корисно для тестування доступу та передачі даних між пристроями.

5. **SMTP і POP3 (Simple Mail Transfer Protocol, Post Office Protocol 3)** – підтримує налаштування поштових серверів і клієнтів, що дозволяє моделювати процес надсилання та отримання електронної пошти.

6. **NAT (Network Address Translation)** – дозволяє налаштовувати трансляцію IP-адрес, що забезпечує зв’язок між приватними та

глобальними мережами та дозволяє використовувати одну IP-адресу для доступу багатьох пристроїв до Інтернету.

7. **VPN (Virtual Private Network)** – дозволяє налаштовувати віртуальні приватні мережі для створення захищених тунелів між пристроями в мережі, забезпечуючи безпеку та конфіденційність даних.

8. **ACL (Access Control Lists)** – дозволяє конфігурувати списки контролю доступу для управління потоком трафіку, визначаючи, які пакети можуть проходити через мережеві пристрої, що допомагає забезпечити безпеку.

9. **VoIP (Voice over IP)** – підтримує моделювання послуг для передачі голосу через IP-мережі, дозволяючи налаштувати телефони IP та інші VoIP-пристрої.

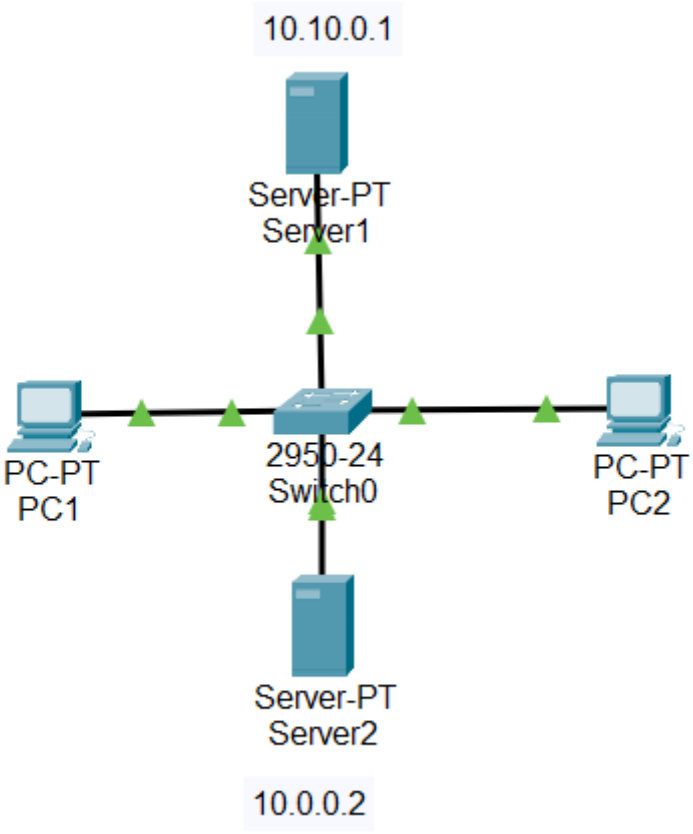
10. **Статична та динамічна маршрутизація (RIP, OSPF, EIGRP)** – Packet Tracer дозволяє налаштовувати протоколи маршрутизації, такі як RIP, OSPF і EIGRP, для ефективного керування маршрутизацією трафіку між мережами.

11. **SNMP (Simple Network Management Protocol)** – дозволяє налаштувати моніторинг та управління мережевими пристроями за допомогою SNMP, що допомагає здійснювати управління мережею.

Cisco Packet Tracer дозволяє працювати з різними мережевими сервісами, імітуючи їхню роботу в реальному середовищі. Це робить його ефективним інструментом для навчання та тестування мережевих технологій.

2.2 Порядок налаштування мережевих сервісів **DNS, DHCP і Web** у мережі на базі обладнання **Cisco**

Завдання полягає у налаштуванні мережевих служб на двох серверах в локальній мережі, топологія якої зображено на рисунку 2.1. Метою є забезпечення доступності основних мережевих сервісів: DNS, веб-сервера та DHCP для клієнтських пристроїв у мережі.



Рисуонок 2.1 – Топологія мережі

Опис завдання:

1. Налаштувати **Server1** як **DNS** та веб-сервер

- **DNS-сервер**: **Server1** повинен виконувати роль **DNS**-сервера для надання послуг доменних імен. Це означає, що він буде зберігати записи, які перетворюють доменні імена на IP-адреси, що дозволяє клієнтським пристроям у мережі звертатися до ресурсів за доменними іменами, а не за IP-адресами.

- **Веб-сервер**: Крім того, **Server1** буде налаштований як веб-сервер для обробки **HTTP**-запитів від клієнтів. Веб-сервер повинен відповідати на запити до домену (наприклад, `www.example.com`), надаючи веб-сторінки або веб-додатки, розміщені на сервері.

2. Налаштувати **Server2** як **DHCP-сервер**

- **DHCP-сервер**: **Server2** буде виконувати роль **DHCP-сервера**, який автоматично призначатиме IP-адреси клієнтським пристроям у мережі. **DHCP-сервер** дозволить уникнути необхідності ручного налаштування IP-адрес для кожного пристрою, що спрощує управління мережею та запобігає можливим конфліктам IP-адрес.

Для розробки топології мережі, показаної на рисунку 2.1, у Cisco Packet Tracer необхідно виконати наступні кроки:

1. Додавання пристроїв

- Додайте комутатор **Cisco Switch 2950-24** у робочу область.
- Додайте два сервери (**Server-PT**) та назвіть їх **Server1** і **Server2**.
- Додайте два комп’ютери (**PC-PT**) та назвіть їх **PC1** і **PC2**.

2. Підключення пристроїв

- Використовуйте інструмент **Copper Straight-Through** (прямий Ethernet-кабель) для підключення пристроїв до комутатора.
- Підключіть **Server1** до одного з портів комутатора (наприклад, Fa0/1).
- Підключіть **Server2** до іншого порту комутатора (наприклад, Fa0/2).
- Підключіть **PC1** та **PC2** до комутатора, під'єднавши їх до портів Fa0/3 і Fa0/4 відповідно.

Налаштовуємо IP адреси серверів і DHCP на ПК

Увійдемо в налаштування клієнтського комп’ютеру. На рисунку 2.2 зображено налаштування параметрів мережевого інтерфейсу для клієнтського пристрою (в даному випадку PC1) в Cisco Packet Tracer. Вибір опції DHCP вказує на те, що пристрій буде використовувати протокол DHCP для автоматичного отримання мережевих налаштувань.

Опис налаштувань:

- Виберіть інтерфейс FastEthernet0, що підключає пристрій до локальної мережі через Ethernet.
- Встановість режим отримання IP-адреси та інших параметрів мережі. Увімкніть радіокнопку DHCP, що означає, що комп'ютер буде автоматично запитувати IP-адресу, маску підмережі, шлюз за замовчуванням і DNS-сервер у DHCP-сервера. У цьому режимі користувачеві не потрібно вручну вводити IP-адресу, шлюз та DNS-сервер. Ці параметри будуть автоматично надані, як тільки DHCP-сервер відповість на запит пристрою..

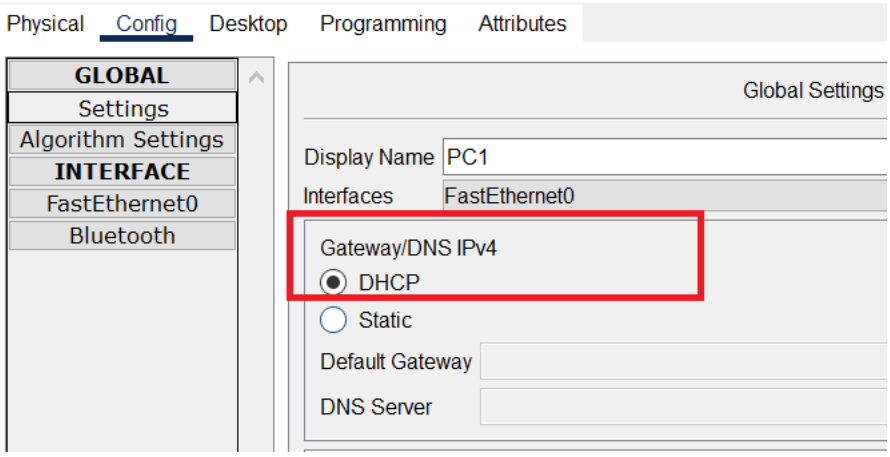


Рисунок 2.2 – Налаштування DHCP

Коли вибрано **DHCP**:

- Пристрій **PC1** відправляє запит DHCP-серверу для отримання IP-адреси та інших необхідних параметрів мережі.
- Якщо в мережі налаштований DHCP-сервер (наприклад, на іншому сервері або маршрутизаторі), то він надасть **IP-адресу**, **маску підмережі**, **шлюз за замовчуванням**, а також **DNS-сервер**.
- Це налаштування спрощує управління мережею, оскільки зменшує потребу в ручному налаштуванні кожного пристрою.

Таким чином, завдяки використанню DHCP, **PC1** зможе автоматично отримувати всі необхідні мережеві параметри для роботи в локальній мережі без потреби ручного налаштування.

Задаємо в конфігурації серверів настройки IP: Server1 – **10.0.0.1**, Server2 – **10.0.0.2**. Маска підмережі встановиться автоматично як **255.0.0.0.**

На рисунку 2.3 показано налаштування IPv4-адреси для інтерфейсу **FastEthernet0** сервера1 в Cisco Packet Tracer. Нижче наведені кроки для налаштування статичної IP-адреси **10.0.0.1** з маскою підмережі **255.0.0.0**.

Кроки налаштування IP-адреси для Server1:

1. **Виберіть інтерфейс FastEthernet0:**

- Увійдіть в режим налаштування пристрою.
- Перейдіть на вкладку **Config** (Конфігурація) і оберіть інтерфейс **FastEthernet0** з лівого меню.

2. **Вибір методу конфігурації IP-адреси:**

- У розділі **IP Configuration** виберіть опцію **Static**. Це означає, що IP-адреса буде введена вручну, а не отримуватиметься через DHCP.

3. **Введення IP-адреси та маски підмережі:**

- У полі **IPv4 Address** введіть IP-адресу **10.0.0.1**.

- У полі **Subnet Mask** введіть маску підмережі **255.0.0.0**. Ця маска вказує на те, що IP-адреса належить до класу A з великою підмережею.

4. **Завершення налаштування**:

- Переконайтесь, що інтерфейс **FastEthernet0** увімкнений (прапорець **On** вгорі праворуч повинен бути відмічений).

- Перевірте правильність введених даних, щоб уникнути помилок у мережевій конфігурації.

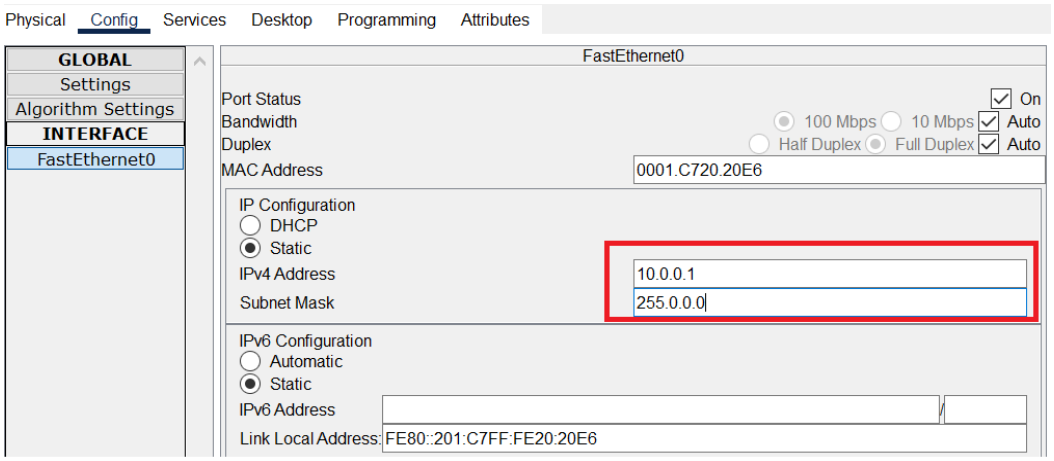


Рисунок 2.3 – IP-адреса для серевера 1

Після налаштування статичної IP-адреси можна протестувати з'єднання сервера з іншими пристроями в мережі. Для цього використовуйте команду `*ping*` на іншому пристрої, щоб перевірити доступність сервера за IP-адресою **10.0.0.1**. Аналогічним способом налаштуйте IP-адресу для сервера 2, як показано на рисунку 2.4.

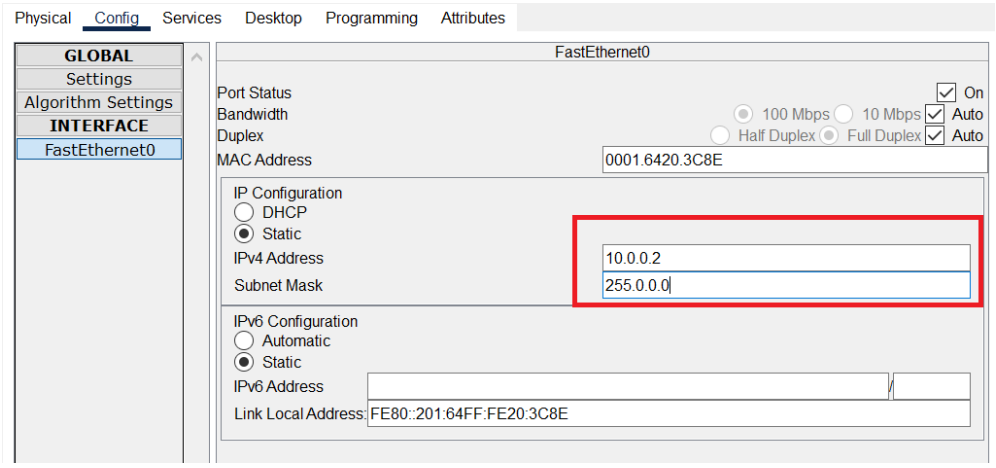


Рисунок 2.4 – IP-адреса для серевера 2

Налаштування служб DNS і HTTP на Server1

Для налаштування служб DNS на **Сервері 2** у Cisco Packet Tracer необхідно виконати кілька кроків, щоб сервер міг обробляти DNS-запити і виконувати перетворення доменних імен у відповідні IP-адреси. Нижче наведено інструкцію з налаштування DNS-сервісу на Server2.

Кроки налаштування DNS на Server2

1. Виберіть Server2:
   - У робочій області Cisco Packet Tracer клацніть на **Server2**, щоб відкрити його налаштування.
2. Перейдіть на вкладку Services:
   - У вікні налаштувань сервера відкрийте вкладку **Services** (Сервіси) у верхньому меню.
3. Активуйте DNS-сервіс (рис.2.5):
   - У лівому меню сервісів знайдіть і виберіть **DNS**.
   - У розділі **DNS Service** оберіть опцію **On**, щоб увімкнути службу DNS на сервері. Це дозволить серверу обробляти DNS-запити від клієнтів у мережі.

Для створення ресурсного запису **A Record** в Cisco Packet Tracer, як показано на рисунку 2.5, виконайте наступні кроки:

4. Додайте ресурсний запис (Resource Record):

- У розділі **Resource Records** введіть ім'я домену, який потрібно зіставити з IP-адресою. У полі **Name** введіть: **server1.example.net**.

- Переконайтеся, що тип запису встановлено як **A Record** (цей запис використовується для зіставлення доменного імені з IP-адресою).

- У полі **Address** введіть IP-адресу, яка відповідає доменному імені. У нашому випадку це **10.0.0.1**.

5. Збережіть ресурсний запис:

- Натисніть кнопку **Add** або **Save** (залежно від версії Cisco Packet Tracer) для збереження запису в таблиці ресурсних записів DNS-сервера.

6. Перевірте запис:

- Після додавання запису він з'явиться в таблиці нижче. Переконайтеся, що доменне ім'я **server1.example.net** зіставлено з IP-адресою 10.0.0.1.

Ці кроки дозволяють створити DNS-запис типу **A Record** на сервері, який зіставляє доменне ім’я з відповідною IP-адресою. Цей запис дозволяє клієнтам у мережі звертатися до сервера за доменним ім'ям замість IP-адреси, що полегшує навігацію та доступ до ресурсів.

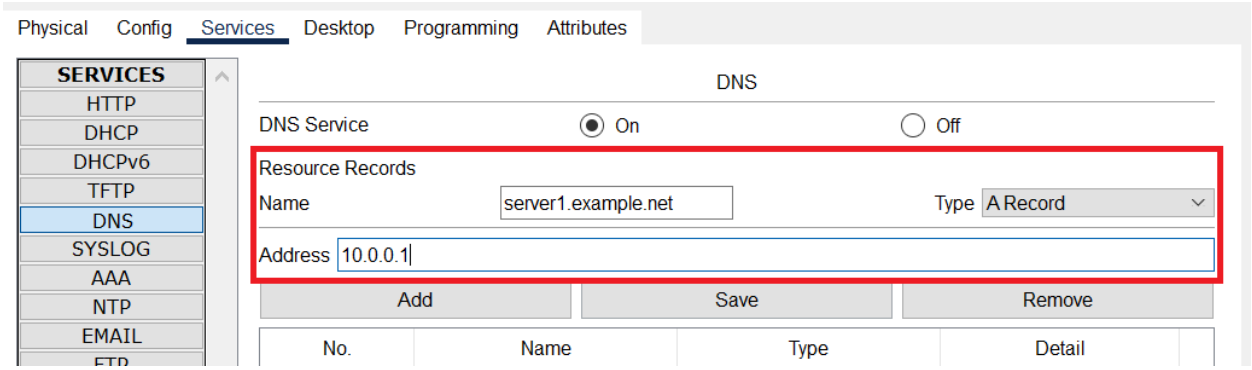


Рисунок 2.5 – Введення ресурсного запису типу A Record

Для внесення ресурсного запису **CNAME** у Cisco Packet Tracer, як показано на рисунку 2.6, необхідно виконати наступні кроки. Запис типу **CNAME** (Canonical Name) використовується для створення псевдоніма (альтернативного імені) для існуючого доменного імені.

Кроки для створення CNAME-запису на DNS-сервері:

1. Введення інформації для CNAME-запису:
   - У полі **Name** введіть псевдонім (альтернативне ім'я), який ви хочете створити. На рисунку вказано **example.net**.
   - У випадаючому меню **Type** оберіть **CNAME** для створення запису типу CNAME.
   - У полі **Host Name** введіть ім'я оригінального домену, на який буде посилатися псевдонім. У цьому випадку, це **server1.example.net**.
2. Збереження CNAME-запису:

– Натисніть кнопку **Add** або **Save** для збереження запису. Після цього запис з'явиться в таблиці ресурсних записів DNS-сервера (рис.2.7).

3. Перевірка CNAME-запису:
   – Щоб перевірити роботу CNAME-запису, ви можете перейти на інший пристрій у мережі та використовувати команду nslookup або звернутися до псевдоніма **example.net**. DNS-сервер повинен перенаправити запит на оригінальний запис **server1.example.net**.

Ресурсний запис **CNAME** дозволяє створити псевдонім для вже існуючого домену, що спрощує доступ до ресурсу через альтернативне ім'я. Наприклад, замість того, щоб звертатися до **server1.example.net**, користувачі можуть використовувати більш коротке ім'я **example.net**.

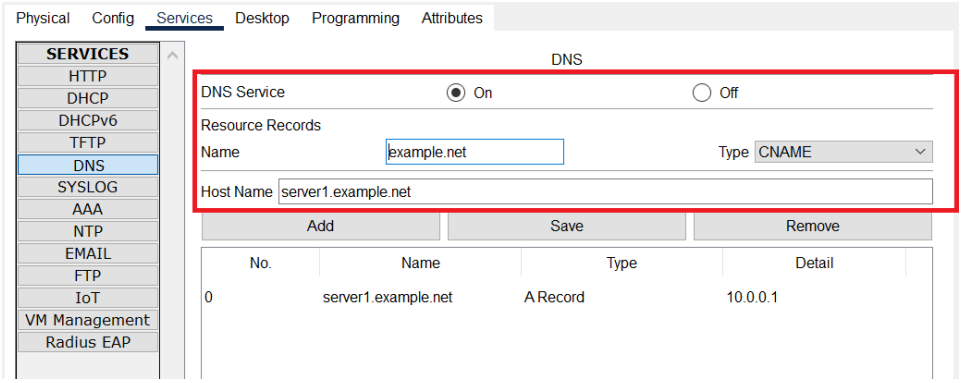


Рисунок 2.6 – Введення ресурсної записи типу **CNAME**

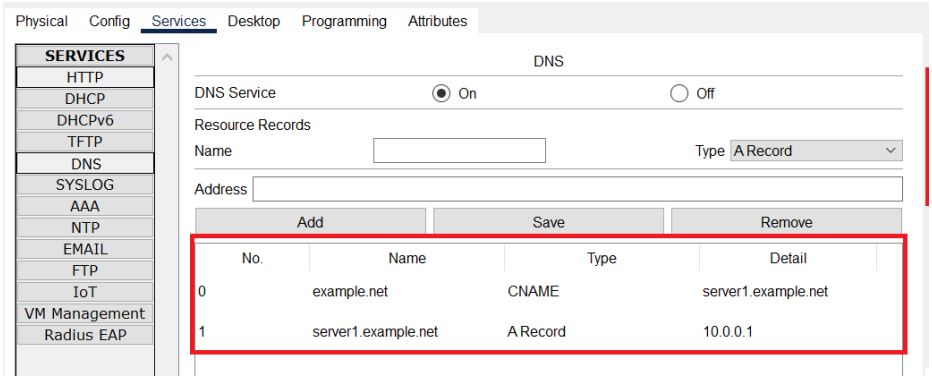


Рисунок 2.7 – Служба DNS в прямій зоні

Служба HTTP дозволяє клієнтам отримувати доступ до веб-сторінок, розміщених на сервері, через веб-браузери. Для налаштування служби HTTP на **Server1** у Cisco Packet Tracer, виконайте такі кроки**:**

1. Виберіть Server1:

- На робочій області Cisco Packet Tracer клацніть на **Server1**, щоб відкрити його налаштування.

2. Перейдіть на вкладку Services:
   - У вікні налаштувань сервера виберіть вкладку **Services** у верхньому меню.
3. Виберіть HTTP-сервіс:
   - У лівому меню перейдіть до розділу **HTTP** (інколи він може бути відображений як HTTP/HTTPS).
4. Увімкніть HTTP-сервіс:
   - Переконайтеся, що опція **HTTP Service** встановлена в положення **On**. Це активує веб-сервер на Server1, що дозволить йому відповідати на запити HTTP-клієнтів.
5. Додавання веб-контенту (за потреби):
   - У деяких версіях Cisco Packet Tracer можна редагувати або додавати веб-сторінки.
   - Перейдіть до розділу **Web Pages** та введіть HTML-код або текст, який ви хочете бачити на веб-сторінці, що буде доступною за запитом HTTP (рис.2.8).

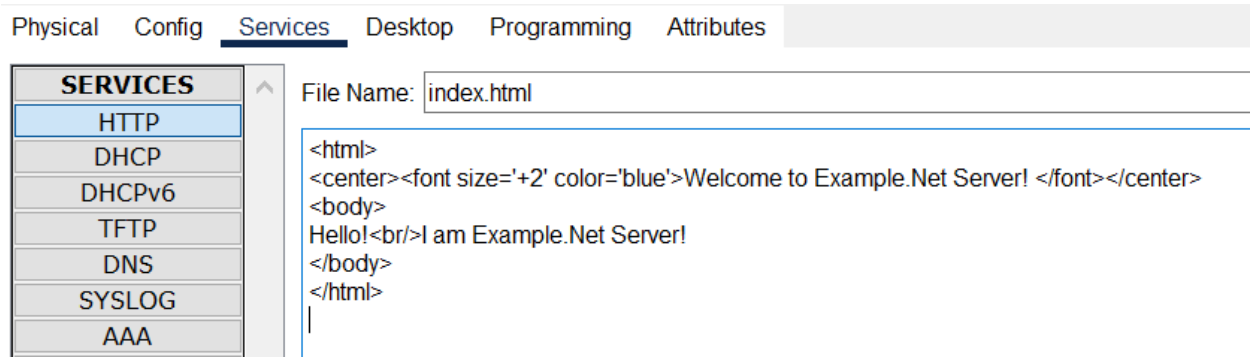


Рисунок 2.8 – Створення сторніки index.html

Виконання команди **nslookup** дозволяє перевірити, чи правильно працює DNS-сервер і чи повертає він IP-адресу, відповідну зазначеному доменному імені. Це корисний інструмент для діагностики та налагодження роботи DNS у локальній мережі.

Для перевірки роботи служби DNS на **Server1** (або іншому сервері, налаштованому як DNS-сервер) у Cisco Packet Tracer за допомогою команди **nslookup**, виконайте наступні кроки:

1. Відкрийте командний рядок на сервері або клієнтському пристрої:
   - У Cisco Packet Tracer виберіть пристрій, з якого ви хочете виконати команду **nslookup**. Це може бути сервер, на якому

налаштовано DNS, або будь-який інший пристрій у тій же мережі.

- Перейдіть на вкладку **Desktop** (якщо ви на комп'ютері) або **Command Line Interface (CLI)** (якщо ви на сервері).

2. Введіть команду nslookup:
   - У командному рядку введіть команду, як вказано на рисунку 2.9:
   - **example.net** – це доменне ім’я, яке ви хочете перевірити. Ви можете ввести інше доменне ім'я, яке є в конфігурації вашого DNS-сервера.
3. Проаналізуйте результат:
   - Якщо DNS-сервер налаштований правильно, команда **nslookup** поверне IP-адресу, пов’язану з доменним іменем **example.net**.
   - У цьому випадку **10.0.0.1** – це IP-адреса, призначена для **example.net** на вашому DNS-сервері.

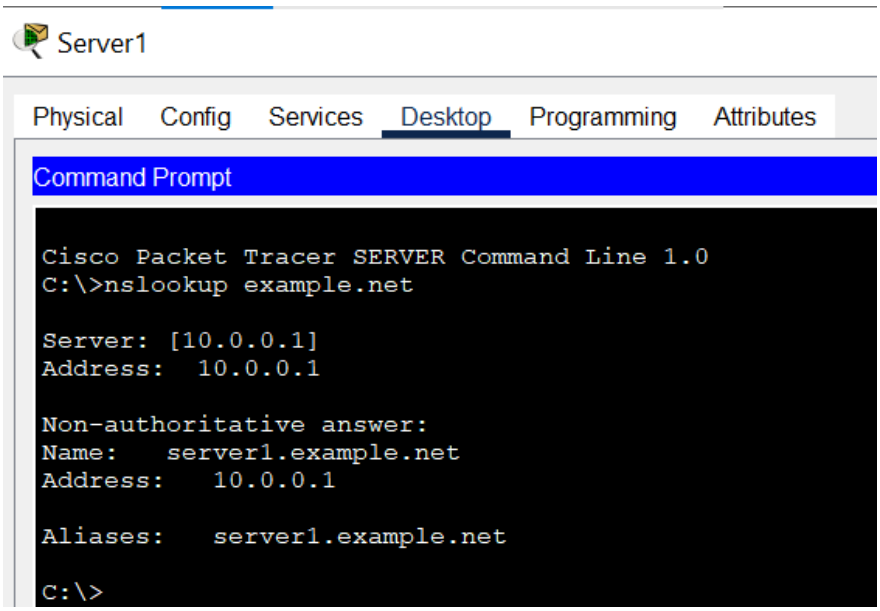


Рисунок 2.9 – Перевірка служби за допомогою команди **nslookup example.net**

Налаштування служби DHCP на Server2

Налаштування DHCP-сервера дозволить автоматично призначати IP-адреси та інші мережеві параметри клієнтам у локальній мережі, зменшуючи потребу в ручному налаштуванні кожного пристрою.

Для налаштування служби **DHCP** на **Server2** у Cisco Packet Tracer, виконайте наступні кроки:

1. Виберіть Server2:

- У робочій області Cisco Packet Tracer клацніть на **Server2**, щоб відкрити його налаштування.

2. Перейдіть на вкладку Services:
   - У вікні налаштувань сервера виберіть вкладку **Services** (Сервіси) у верхньому меню.
3. Виберіть DHCP-сервіс:
   - У лівому меню виберіть **DHCP**. Це відкриє налаштування для служби DHCP.
4. Увімкніть DHCP-сервіс:
   - У розділі **DHCP Service** оберіть опцію **On** для активації DHCP-сервера на Server2. Це дозволить серверу відповідати на запити DHCP-клієнтів.
5. Налаштування DHCP-пулу (діапазону адрес) (рис.2.10):
   - У розділі **Pool Name** введіть ім'я пулу, яке описує цю конфігурацію DHCP. Наприклад, **serverPool**.
   - У полі **Default Gateway** введіть IP-адресу шлюзу за замовчуванням, яку клієнти використовуватимуть для виходу з локальної мережі (наприклад, **0.0.0.0**).
   - У полі **DNS Server** введіть IP-адресу DNS-сервера, який буде використовуватися клієнтами. Якщо **Server1** налаштований як DNS-сервер, введіть його IP-адресу (наприклад, **10.0.0.1**).
   - У полі **Start IP Address** введіть початкову IP-адресу діапазону, який буде розподілятися DHCP-сервером. Наприклад, **10.0.0.10**.
   - У полі **Subnet Mask** введіть маску підмережі (наприклад, **255.0.0.0**).
   - У полі **Maximum Number of Users** вкажіть максимальну кількість клієнтів, які можуть отримати IP-адреси з цього пулу (наприклад, **5**).
6. Збережіть налаштування:
   - Натисніть кнопку **Add** або **Save** (залежно від версії Cisco Packet Tracer) для збереження конфігурації DHCP-пулу. Після цього пул з’явиться у таблиці налаштувань DHCP-сервера.

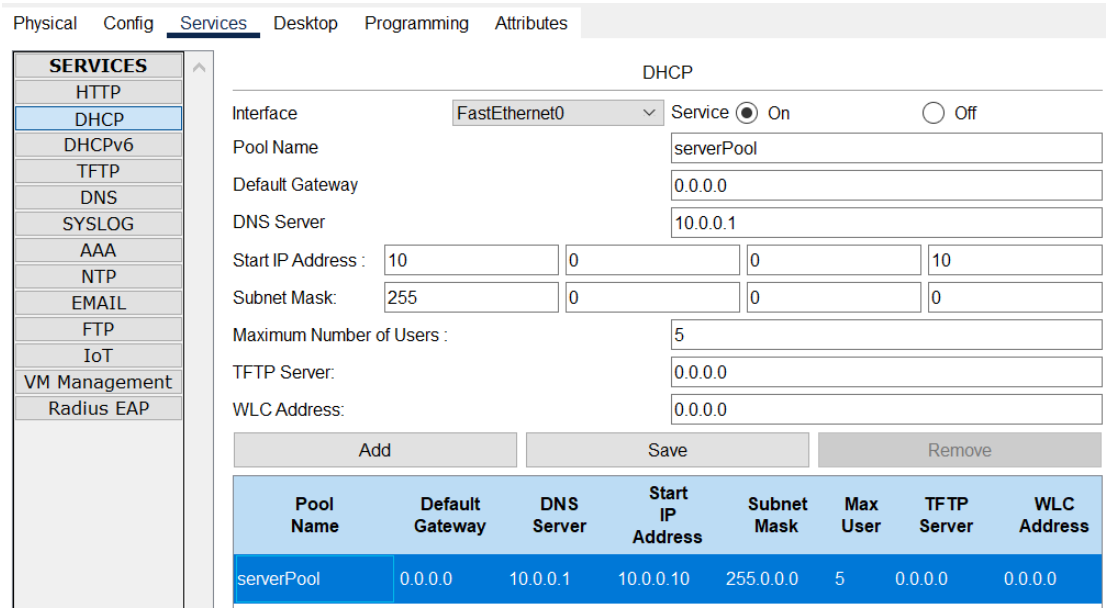


Рисунок 2.10 – Налаштування DHCP сервера.

Після налаштування DHCP-сервісу на Server2, клієнти мережі автоматично отримуватимуть IP-адреси та інші мережеві параметри, що спрощує процес конфігурації і знижує ймовірність виникнення конфліктів IP-адрес. Це дозволяє легко управляти мережею, особливо якщо до неї підключено велику кількість пристроїв.

Перевірка роботи клієнтів

Для перевірки роботи клієнтів **PC1** та **PC2** після налаштування DHCP-сервера на **Server2** можна використовувати команди **ipconfig /release** та **ipconfig /renew**. Ці команди дозволяють скинути існуючу IP-адресу та оновити її через DHCP-сервер.

1. Команда ipconfig /release:
   - **Призначення**: команда **ipconfig /release** скидає (звільняє) поточну IP-адресу, яку отримав клієнт від DHCP-сервера. Це корисно, якщо потрібно скинути існуючі налаштування IP-адреси або підготувати пристрій для отримання нової адреси.
   - **Коли використовується**: зазвичай використовується перед виконанням **ipconfig /renew** для оновлення IP-адреси. Ця команда відключає поточне мережеве підключення, видаляючи призначену IP-адресу.
2. Команда ipconfig /renew:
   - **Призначення**: команда **ipconfig /renew** надсилає запит до DHCP-сервера на отримання нової IP-адреси. Пристрій

зв'язується з DHCP-сервером, щоб отримати IP-адресу, маску підмережі, шлюз за замовчуванням та DNS-сервер.

- **Коли використовується**: після **ipconfig /release** або для оновлення IP-адреси, коли DHCP-сервер вже налаштований і потрібно отримати нові мережеві параметри.

Кроки виконання команд на клієнтах PC1 та PC2

1. Відкрийте командний рядок на PC1 або PC2:
   - У Cisco Packet Tracer виберіть клієнтський комп'ютер **PC1** або **PC2**.
   - Перейдіть на вкладку **Desktop** і виберіть **Command Prompt** (Командний рядок).
2. Виконайте команду ipconfig /release:
   - У командному рядку введіть код, як вказано на рисунку 2.11.
   - Натисніть **Enter**.
   - Ця команда звільнить поточну IP-адресу клієнта. Після виконання команда покаже, що IP-адреса відсутня, оскільки мережеве підключення тимчасово припинено.
3. Виконайте команду ipconfig /renew:
   - Після звільнення IP-адреси введіть команду, як показано на риснку 2.12.
   - Натисніть **Enter**.
   - Клієнтський комп'ютер надішле запит на отримання IP-адреси від DHCP-сервера. Якщо DHCP-сервер (Server2) налаштований правильно, клієнт отримає нову IP-адресу, маску підмережі, шлюз за замовчуванням та DNS-сервер.

Команди **ipconfig /release** та **ipconfig /renew** дозволяють скинути і повторно отримати IP-адресу через DHCP. Вони корисні для тестування і налагодження роботи DHCP-сервера, а також для перевірки, чи клієнт отримує правильні мережеві параметри.

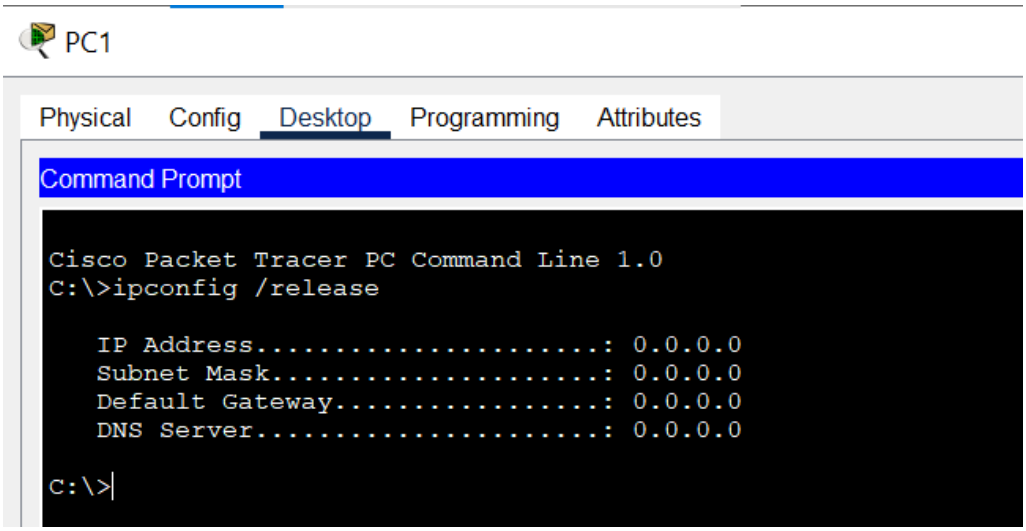


Рисунок 2.11 – Видалення конфігурації IP-адрес для всіх адаптерів

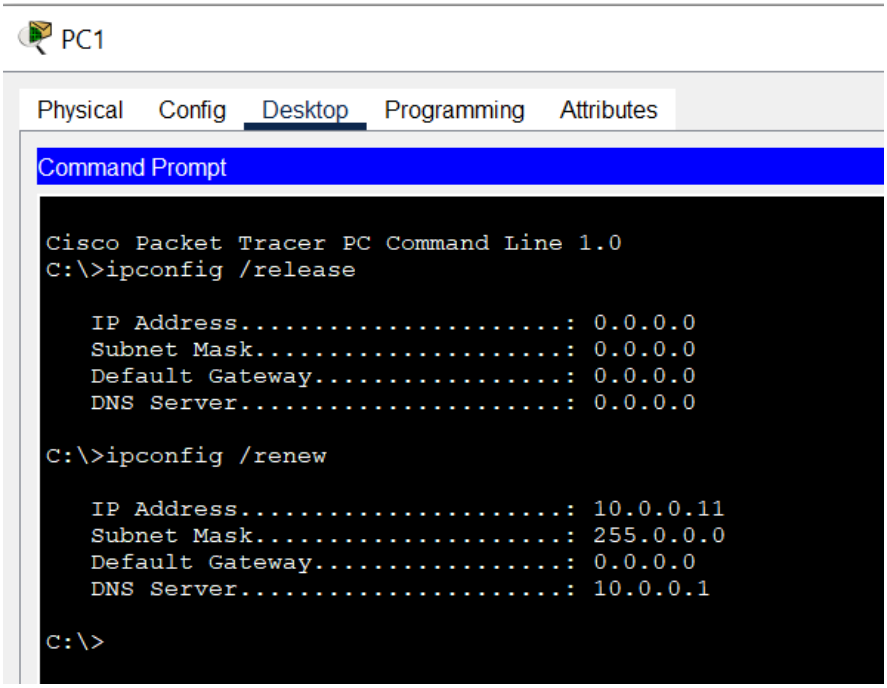


Рисунок 2.12 - Конфігурація протокол TCP/IP клієнта від DHCP сервера

Аналогічно необхідно скинути і повторно отримати IP-адресу через DHCP для PC2 (рис. 2.13).

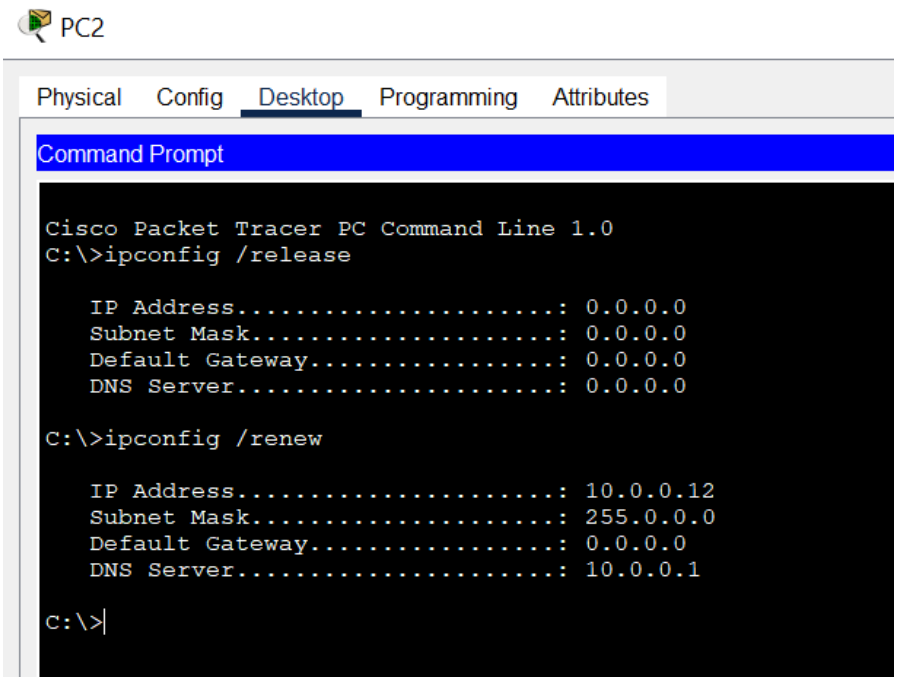


Рисунок 2.13 - PC2 отримав IP адрес від DHCP сервера Server2

Переконайтеся, що Server1 налаштований як веб-сервер (HTTP-сервіс увімкнений), і він має IP-адресу, яку клієнт зможе використовувати для доступу до веб-контенту. Для перевірки роботи веб-сервера на **Server1** і доступу до сайту через веб-браузер на клієнтському комп'ютері **PC1** виконайте наступні кроки:

1. **Переконайтеся, що HTTP-сервіс увімкнений на Server1**:
   - Виберіть **Server1** у Cisco Packet Tracer.
   - Перейдіть на вкладку **Services** та виберіть **HTTP** у лівому меню.
   - Переконайтеся, що **HTTP Service** встановлено на **On**. Це означає, що веб-сервер активний і готовий обробляти запити клієнтів.
2. **Перевірте IP-адресу Server1**:
   - На вкладці **Config** або **Desktop** (Command Prompt) перевірте, яка IP-адреса призначена Server1. Наприклад, IP-адреса сервера — **10.0.0.1**.
3. **Відкрийте веб-браузер на PC1**:
   - Виберіть клієнтський комп'ютер **PC1**.
   - Перейдіть на вкладку **Desktop** і виберіть **Web Browser** (веб-браузер) з доступних додатків.
4. **Введіть IP-адресу Server1 в адресний рядок веб-браузера**:
   - У адресному рядку браузера введіть IP-адресу Server1 у форматі http://<IP-адреса> або доменне ім'я, як показано на рисунку 2.14.
   - Натисніть **Enter** для завантаження веб-сторінки.

5. **Перевірте результат**:
   - Якщо Server1 налаштований правильно як веб-сервер, браузер на PC1 повинен відобразити веб-сторінку, розміщену на Server1 (рис.2.14).
   - Якщо сторінка відображається, це означає, що веб-сервер працює належним чином і клієнт може до нього підключатися.

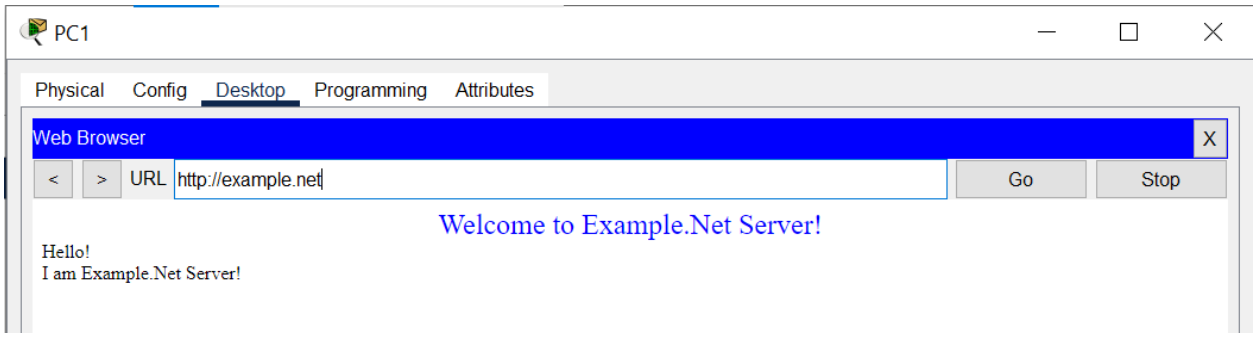


Рисунок 2.14 - Перевірка роботи служби HTTP на Server1

Після виконання цих кроків ви зможете підтвердити, що веб-сервер на Server1 працює правильно, і клієнтський комп'ютер PC1 може отримати доступ до веб-сторінки, розміщеної на сервері.

2.3 Варіанти індивідуального завдання №1

1. У середовищі програмного симулятора/емулятора створити проект мережі (рис. 2.1).

2. Розробити узагальнену схему адресації пристроїв мережі. Для цього скористатися даними, наведеними нижче:

Варіант 1: Корпоративна мережа "example.local"

- Server1 (DNS + Web): 192.168.1.10
- Server2 (DHCP): 192.168.1.11
- DHCP пул: 192.168.1.50-192.168.1.100
- Доменне ім'я: www.example.local
- Web-сторінка: "Корпоративний портал Example Company"
- Кількість клієнтів: 3 PC

Варіант 2: Освітня мережа "edu.net"

- Server1 (DNS + Web): 172.16.0.10
- Server2 (DHCP): 172.16.0.11
- DHCP пул: 172.16.0.50-172.16.0.150
- Доменне ім'я: portal.edu.net

- Web-сторінка: "Освітній портал"
- Кількість клієнтів: 4 PC

Варіант 3: Мережа малого бізнесу "shop.local"
- Server1 (DNS + Web): 10.0.1.10
- Server2 (DHCP): 10.0.1.11
- DHCP пул: 10.0.1.100-10.0.1.200
- Доменне ім'я: store.shop.local
- Web-сторінка: "Онлайн магазин"
- Кількість клієнтів: 2 PC

Варіант 4: Готельна мережа "hotel.net"
- Server1 (DNS + Web): 192.168.10.10
- Server2 (DHCP): 192.168.10.11
- DHCP пул: 192.168.10.50-192.168.10.250
- Доменне ім'я: booking.hotel.net
- Web-сторінка: "Система бронювання готелю"
- Кількість клієнтів: 5 PC

Варіант 5: Медична мережа "hospital.local"
- Server1 (DNS + Web): 172.20.0.10
- Server2 (DHCP): 172.20.0.11
- DHCP пул: 172.20.0.100-172.20.0.200
- Доменне ім'я: med.hospital.local
- Web-сторінка: "Медичний портал"
- Кількість клієнтів: 3 PC

Варіант 6: Бібліотечна мережа "library.net"
- Server1 (DNS + Web): 10.1.0.10
- Server2 (DHCP): 10.1.0.11
- DHCP пул: 10.1.0.50-10.1.0.150
- Доменне ім'я: catalog.library.net
- Web-сторінка: "Бібліотечний каталог"
- Кількість клієнтів: 4 PC

Варіант 7: Спортивний центр "sport.local"
- Server1 (DNS + Web): 192.168.20.10

- Server2 (DHCP): 192.168.20.11
- DHCP пул: 192.168.20.100-192.168.20.200
- Доменне ім'я: fitness.sport.local
- Web-сторінка: "Спортивний центр розкладу"
- Кількість клієнтів: 3 PC

Варіант 8: Ресторанна мережа "restaurant.net"
- Server1 (DNS + Web): 172.30.0.10
- Server2 (DHCP): 172.30.0.11
- DHCP пул: 172.30.0.50-172.30.0.150
- Доменне ім'я: menu.restaurant.net
- Web-сторінка: "Меню ресторану"
- Кількість клієнтів: 2 PC

Варіант 9: Музейна мережа "museum.local"
- Server1 (DNS + Web): 10.2.0.10
- Server2 (DHCP): 10.2.0.11
- DHCP пул: 10.2.0.100-10.2.0.200
- Доменне ім'я: expo.museum.local
- Web-сторінка: "Віртуальна виставка"
- Кількість клієнтів: 4 PC

Варіант 10: Транспортна компанія "transport.net"
- Server1 (DNS + Web): 192.168.30.10
- Server2 (DHCP): 192.168.30.11
- DHCP пул: 192.168.30.50-192.168.30.150
- Доменне ім'я: track.transport.net
- Web-сторінка: "Система відстеження"
- Кількість клієнтів: 3 PC

4. Провести базове налагодження пристроїв, інтерфейсів та каналів зв’язку побудованої мережі.

5. Провести налагодження функціонування DHCP-серверів.

6. Дослідити особливості отримання службової та діагностичної інформації протоколу DHCP за допомогою відповідних команд.

7. Дослідити процеси передачі даних між DHCP-клієнтами та DHCP-сервером. У разі появи конфліктів визначити та усунути їх джерела.

3. ОСНОВНІ ТЕОРЕТИЧНІ ВІДОМОСТІ ЩОДО ВИКОНАННЯ ІНДИВІДУАЛЬНОГО РОЗРАХУНКОВОГО ЗАВДАННЯ №1

3.1 Теоретичні відомості. Створення списків доступу ACL

Мета роботи: вивчити принципи побудови списків доступу, застосувати отримані знання при виконанні практичних завдань.

ACL (Access Control List) - це набір текстових виразів, які щось дозволяють, або щось забороняють.

Списки керування доступом (Access Control Lists, ACL) є важливим інструментом для забезпечення мережевої безпеки та управління трафіком у комп'ютерних мережах. ACL дозволяють адміністраторам встановлювати правила, які визначають, які пакети даних можуть або не можуть проходити через мережеві пристрої, такі як маршрутизатори і комутатори. За допомогою ACL можна контролювати доступ до мережевих ресурсів, обмежувати небажаний трафік та підвищувати рівень безпеки мережі.

Access Control List (ACL) — це набір правил, які визначають, як обробляти вхідний та вихідний трафік на мережевих пристроях. ACL можуть застосовуватися на маршрутизаторах, комутаторах рівня 3 та інших пристроях, які підтримують фільтрацію трафіку. Кожне правило в ACL визначає конкретний критерій, за яким пристрій приймає або відхиляє мережевий пакет. Критерії можуть включати IP-адреси відправника та одержувача, порти, протоколи, типи пакетів і інші атрибути.

Уявімо, що в організації є приватна мережа, підключена до Інтернету через маршрутизатор. У цій мережі містяться два сегменти: один сегмент з адресами в діапазоні 192.168.1.0/24, який використовується для робочих станцій співробітників, а інший – у діапазоні 192.168.2.0/24, який використовується для серверів. З міркувань безпеки компанія вирішує обмежити доступ співробітників до певних зовнішніх ресурсів, зокрема, дозволити лише вихідний трафік на порти, пов'язані з переглядом веб-сторінок (HTTP та HTTPS). Крім того, співробітники не повинні мати доступу до серверного сегмента 192.168.2.0/24, але доступ між серверами і Інтернетом має бути дозволений.

Для реалізації таких обмежень адміністратор налаштовує розширений список контролю доступу на маршрутизаторі. ACL фільтрує трафік на основі IP-адрес, протоколів і портів, що дозволяє більш гнучко

керувати доступом. Спочатку ACL пропускає HTTP- та HTTPS-трафік (порти 80 і 443) з мережі робочих станцій (192.168.1.0/24) до будь-якої зовнішньої адреси, забезпечуючи співробітникам доступ до веб-ресурсів. Водночас ACL блокує всі інші види вихідного трафіку з цього сегмента, включаючи доступ до FTP-сервісів, SSH і будь-яких інших служб, що працюють на нестандартних портах. Таким чином, співробітники можуть користуватися лише дозволеними веб-ресурсами, що відповідає політиці компанії.

Далі, ACL забороняє весь трафік між сегментами мережі. Правило блокує будь-які спроби доступу з сегмента 192.168.1.0/24 до мережі серверів 192.168.2.0/24, обмежуючи прямий доступ співробітників до критично важливих серверів компанії. Водночас ACL дозволяє вихідний трафік із серверного сегмента до Інтернету, що дозволяє серверам отримувати оновлення або обмінюватися даними з зовнішніми ресурсами.

Таким чином, налаштування ACL забезпечує дотримання політики безпеки, створюючи багаторівневий доступ до мережевих ресурсів. Завдяки використанню ACL можна точно контролювати, які пристрої мають доступ до певних ресурсів, визначати дозволені та заборонені порти, а також блокувати небажані мережеві з’єднання, що значно підвищує рівень захисту мережі організації. На цьому прикладі видно, як списки керування доступом дозволяють тонко налаштувати правила безпеки та забезпечити ізоляцію між різними сегментами мережі, знижуючи ймовірність несанкціонованого доступу та зловживань.

Існує два основних типи ACL: **стандартні** та **розширені**.

1. **Стандартні ACL**:
   - Стандартні ACL є базовим типом списку контролю доступу, що фільтрує трафік лише за IP-адресою відправника.
   - Стандартні ACL застосовуються до всього трафіку, незалежно від порту чи протоколу, і можуть або дозволити, або відхилити весь трафік від певного джерела.
   - Вони мають обмежену гнучкість і здебільшого застосовуються у простих мережах, де потрібно контролювати доступ за IP-адресою.
2. **Розширені ACL**:
   - Розширені ACL забезпечують більшу гнучкість і дозволяють фільтрувати трафік за багатьма параметрами, включаючи

IP-адреси відправника та одержувача, порти, протоколи (TCP, UDP, ICMP тощо) і навіть конкретні типи пакетів.

- Завдяки цим можливостям розширені ACL є ефективним інструментом для тонкого налаштування правил безпеки та управління доступом у великих і складних мережах.
- Вони дозволяють налаштувати більш детальні правила, наприклад, блокування певного порту або протоколу для конкретного IP-адреси.

Числові ACL (Access Control Lists) – це списки керування доступом, яким призначаються унікальні числові ідентифікатори замість імен. Числові ACL використовуються для ідентифікації списків контролю доступу в мережевих пристроях, таких як маршрутизатори і комутатори, та дозволяють фільтрувати мережевий трафік на основі певних критеріїв. Числові ACL бувають двох основних типів: **стандартні** та **розширені**, кожен з яких має свій діапазон числових ідентифікаторів.

Діапазони числових ACL:

- **Стандартні числові ACL**: використовують числові ідентифікатори від **1 до 99** та **1300 до 1999**.
- **Розширені числові ACL**: використовують числові ідентифікатори від **100 до 199** та **2000 до 2699**.

Призначення стандартних і розширених числових ACL

- **Стандартні ACL** фільтрують трафік на основі IP-адреси відправника. Вони дозволяють або забороняють трафік, але не надають можливості вказувати конкретні порти чи протоколи.
- **Розширені ACL** забезпечують більшу гнучкість, дозволяючи вказувати IP-адреси відправника та одержувача, протоколи (TCP, UDP, ICMP тощо), порти і навіть конкретні параметри для певних типів трафіку.

Припустимо, ми хочемо дозволити доступ тільки для трафіку з мережі 192.168.1.0/24 і заблокувати весь інший трафік. Це можна зробити за допомогою стандартного ACL із числовим ідентифікатором.

```
access-list 10 permit 192.168.1.0 0.0.0.255
```

Цей ACL з ідентифікатором 10 дозволяє весь трафік, який надходить від IP-адрес у діапазоні 192.168.1.0 – 192.168.1.255. Усі інші

IP-адреси будуть заблоковані, якщо цей ACL застосувати до інтерфейсу.

Припустимо, адміністратор мережі хоче дозволити доступ до веб-сервера тільки для трафіку HTTP (порт 80) з певної мережі, наприклад, 192.168.10.0/24, і заблокувати інші протоколи та порти.

```
access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq 80
```

Тут ACL з ідентифікатором 101 дозволяє трафік TCP, що надходить від мережі 192.168.10.0/24 до будь-якої IP-адреси (any) тільки на порт 80 (HTTP). Усі інші типи трафіку, які не відповідають цим критеріям, будуть заблоковані, якщо ACL застосувати до відповідного інтерфейсу.

Розглянемо ситуацію, коли адміністратор хоче заборонити всі ICMP-запити з мережі 10.0.0.0/24 до певного сервера.

```
access-list 110 deny icmp 10.0.0.0 0.0.0.255 host 192.168.1.10
access-list 110 permit ip any any
```

Цей ACL з ідентифікатором 110 блокує ICMP-запити (наприклад, ping) з мережі 10.0.0.0/24 до IP-адреси 192.168.1.10. Друга команда permit ip any any дозволяє весь інший трафік, оскільки за замовчуванням будь-який трафік, що не відповідає жодному правилу, буде заблокований.

Символьні ACL (Access Control Lists), подібно до числових ACL, поділяються на стандартні та розширені. Вони надають адміністраторам можливість використовувати символьні імена замість числових ідентифікаторів для легшого розпізнавання та керування списками доступу. Це особливо корисно в складних мережах, де необхідно створити велику кількість ACL для різних цілей, оскільки символьні імена можуть відображати призначення списку, роблячи конфігурацію більш зрозумілою і зручною для підтримки.

Символьні стандартні ACL працюють аналогічно числовим стандартним ACL, зокрема фільтрують трафік лише за IP-адресою відправника. Стандартні символьні ACL дозволяють або дозволити, або

заблокувати весь трафік з певного джерела незалежно від порту чи протоколу. Наприклад, символьний ACL з іменем "BLOCK_OFFICE" може бути налаштований на блокування доступу до певної мережі з конкретної підмережі. Це дає можливість адміністраторам швидко визначити, що цей список контролює трафік з офісної підмережі.

Символьні розширені ACL, на відміну від стандартних, дозволяють значно більш гнучке налаштування. Вони можуть фільтрувати трафік на основі декількох параметрів, таких як IP-адреси відправника та одержувача, протоколи (TCP, UDP, ICMP тощо), порти та навіть певні типи пакетів. Завдяки цьому символьні розширені ACL є ефективним інструментом для управління доступом і безпекою у великих мережах, де потрібно контролювати доступ до специфічних ресурсів. Наприклад, розширений ACL із символьним ім'ям "WEB_ACCESS" може дозволяти HTTP та HTTPS-трафік до веб-серверів у мережі, блокуючи водночас доступ до інших протоколів.

Символьні стандартні ACL використовуються для основного фільтрування за IP-адресою відправника, тоді як символьні розширені ACL забезпечують тонке налаштування доступу за допомогою додаткових критеріїв, таких як протоколи і порти. Обидва типи символьних ACL значно підвищують зручність управління мережевою конфігурацією, дозволяючи адміністраторам створювати чітко структуровані та легко підтримувані правила доступу..

У списках керування доступом (ACL) для фільтрації IP-адрес використовується **WildCard-маска**. Вона визначає, які біти в IP-адресі враховуються для фільтрації, а які ігноруються. На відміну від звичайної маски підмережі (де 1 вказує на важливий біт), у WildCard-масці 0 означає, що біт є значущим і враховується при фільтрації, а 1 вказує на біт, який ігнорується.

WildCard-маска дозволяє гнучко налаштовувати ACL, зокрема визначати окремі IP-адреси, мережі, підмережі або певні діапазони адрес. Наприклад:

- **0.0.0.0** — означає, що всі біти IP-адреси є важливими, тобто вказує на одну конкретну IP-адресу.
- **0.0.0.255** — означає, що перші три октети значущі, а останній ігнорується, що дозволяє фільтрувати адреси в межах мережі з 256 адресами.
- **0.0.255.255** — означає, що перші два октети значущі, а останні два ігноруються, що дозволяє фільтрувати адреси в межах мережі з 65,536 адресами.

Приклади використання WildCard-маски в ACL

Приклад 1: Фільтрація однієї IP-адреси

Припустимо, ми хочемо дозволити доступ тільки з конкретної IP-адреси, наприклад, **192.168.1.10**. Для цього використовується WildCard-маска **0.0.0.0**, яка вказує на точну відповідність усіх бітів.

```
access-list 10 permit 192.168.1.10 0.0.0.0
```

У цьому прикладі ACL з номером 10 дозволяє доступ тільки з IP-адреси **192.168.1.10**.

Приклад 2: Фільтрація підмережі з 256 адресами

Щоб дозволити доступ для всієї підмережі **192.168.1.0/24**, використовуємо WildCard-маску **0.0.0.255**. Ця маска ігнорує останній октет, дозволяючи доступ для всіх адрес у діапазоні від **192.168.1.0** до **192.168.1.255**.

```
access-list 10 permit 192.168.1.0 0.0.0.255
```

Така конфігурація дозволяє трафік для всіх IP-адрес у підмережі 192.168.1.0/24.

Приклад 3: Фільтрація мережі з 65,536 адресами

Для дозволу доступу до більшої мережі, наприклад, **192.168.0.0/16**, використовується WildCard-маска **0.0.255.255**. Це означає, що враховуються тільки перші два октети, а інші можуть бути будь-якими.

```
access-list 10 permit 192.168.0.0 0.0.255.255
```

Це дозволяє трафік для всіх IP-адрес у діапазоні **192.168.0.0** – **192.168.255.255**.

Приклад 4: Фільтрація певного діапазону адрес

Уявімо, що потрібно дозволити доступ для IP-адрес з діапазону **192.168.1.0** до **192.168.1.15**. Використовуємо IP-адресу **192.168.1.0** з WildCard-маскою **0.0.0.15**. Така маска дозволяє відповідність адресам з будь-яким останнім чотирьохбітним значенням від 0000 до 1111, що відповідає 16 адресам.

```
access-list 10 permit 192.168.1.0 0.0.0.15
```

Цей запис дозволяє доступ для IP-адрес від **192.168.1.0** до **192.168.1.15**.

Приклад 5: Блокування окремого адресного діапазону

Якщо потрібно заблокувати доступ з адрес **192.168.2.64** – **192.168.2.127**, можна використати адресу **192.168.2.64** з WildCard-маскою **0.0.0.63**.

```
access-list 20 deny 192.168.2.64 0.0.0.63
```

Це правило блокує доступ для IP-адрес у вказаному діапазоні, оскільки маска **0.0.0.63** дозволяє відповідність адресам від 192.168.2.64 до 192.168.2.127.

WildCard-маски є потужним інструментом для точного налаштування ACL, дозволяючи задавати як конкретні IP-адреси, так і великі діапазони адрес. Вони забезпечують гнучкість у керуванні доступом і фільтрації трафіку, підвищуючи ефективність контролю в складних мережах.

Списки керування доступом (Access Control Lists, ACL) поділяються на кілька основних видів, кожен з яких призначений для вирішення конкретних завдань з фільтрації та контролю трафіку в мережі. Нижче наведено основні види ACL.

1. Стандартні ACL (Standard ACL)

Стандартні ACL — це базовий тип ACL, який фільтрує мережевий трафік лише за IP-адресою відправника. Стандартні ACL обмежуються тільки дозволом або забороною доступу на основі IP-адрес, і не можуть фільтрувати трафік за іншими параметрами, такими як порти чи протоколи.

2. Розширені ACL (Extended ACL)

Розширені ACL забезпечують гнучкіші можливості для фільтрації, дозволяючи задавати IP-адреси відправника та одержувача, а також вказувати протоколи (TCP, UDP, ICMP тощо) і порти. Це робить розширені ACL ефективним інструментом для детального контролю доступу і безпеки в мережах з високими вимогами до фільтрації.

3. Іменовані ACL (Named ACL)

Іменовані ACL дозволяють використовувати символьні імена замість числових ідентифікаторів, що робить їх більш зручними для великих мереж, де налаштовано багато ACL. Іменовані ACL можуть бути як стандартними, так і розширеними, а їх конфігурація легша для

розуміння і супроводу, оскільки імена ACL можуть вказувати на їхнє призначення.

4. Динамічні ACL (Dynamic ACL, також відомі як Lock-and-Key ACL)

Динамічні ACL — це розширений тип ACL, який дозволяє надавати доступ користувачам на основі аутентифікації. Користувачі повинні виконати вхід у мережу (зазвичай через Telnet), і після успішної аутентифікації їм надається тимчасовий доступ на основі динамічного ACL. Це підвищує безпеку, оскільки доступ надається лише після ідентифікації користувача.

5. Зворотні ACL (Reflexive ACL)

Зворотні ACL фільтрують трафік на основі його стану. Вони дозволяють вихідний трафік і автоматично створюють тимчасові ACL для дозволу вхідного трафіку у відповідь. Зворотні ACL зазвичай використовуються в мережах, де необхідно контролювати з'єднання між внутрішньою та зовнішньою мережею на основі сесій.

ACL є потужним інструментом для управління доступом і підвищення безпеки в комп'ютерних мережах. Вони забезпечують адміністраторам можливість фільтрувати трафік за IP-адресами, протоколами, номерами портів та іншими параметрами. Правильне використання ACL може значно підвищити рівень безпеки та захистити мережу від небажаного трафіку, але водночас вимагає уважного налаштування та періодичного моніторингу. Завдяки своїм можливостям ACL залишаються важливим інструментом мережевих адміністраторів для забезпечення надійності та стабільності мережевих систем.

3.2 Приклад налагодження параметрів списків доступу ACL в мережі, побудованій на базі комутаторів та маршрутизаторів Cisco

При виконанні другого індивідуального завдання потрібно створити списки контролю доступу (ACL) для управління трафіком у мережі, зображеній на рисунку 3.1. Мережа складається з маршрутизатора **Router0**, двох клієнтських комп'ютерів **PC0** та **PC1**, комутатора **Switch0** і сервера **Server0**. Основна мета завдання – налаштувати ACL на маршрутизаторі, щоб реалізувати наступні політики доступу (рис.3.2):

1. Заборонити комп'ютеру **PC0** (з IP-адресою 192.168.0.11) доступ до сервера **Server0** (з IP-адресою 10.10.0.100).

2. Дозволити комп'ютеру **PC1** (з IP-адресою 192.168.0.12) доступ до сервера **Server0**.

Мета завдання:

- Розробити і застосувати ACL для реалізації політики безпеки в локальній мережі.
- Використати ACL для контролю доступу між сегментами мережі, базуючись на IP-адресах і напрямку трафіку.
- Ознайомитися з принципами роботи стандартних і розширених ACL, а також навчитися застосовувати їх для вирішення реальних задач мережевої безпеки.

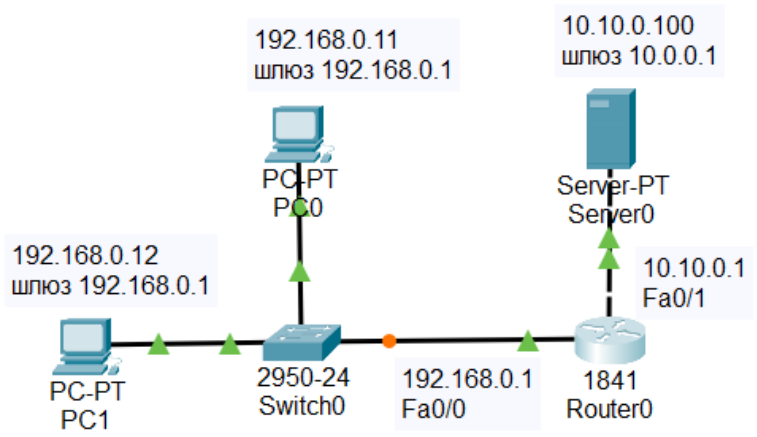


Рисунок 3.1 – Топологія мережі

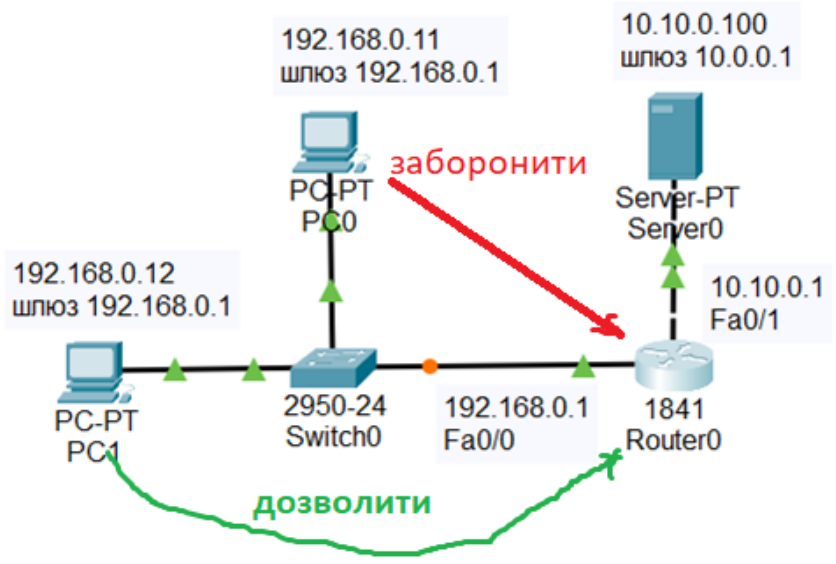


Рисунок 3.2 – Настройки прав доступу

Зберемо дану схему і налаштуємо її. Налаштування PC0 і PC1 виконайте самостійно.

Налаштування R0

Маршрутизатор **R0** у цьому прикладі потрібно налаштувати з використанням розширеного списку контролю доступу (ACL) для реалізації певних політик доступу в мережі. Мета налаштування полягає у тому, щоб заборонити комп'ютеру **PC0** доступ до сервера **Server0**, водночас дозволити доступ до цього сервера з комп'ютера **PC1**.

1. Підключення до маршрутизатора R0

Спочатку необхідно підключитися до **Router0** і перейти в режим глобальної конфігурації. Це можна зробити через CLI маршрутизатора або за допомогою терміналу в Cisco Packet Tracer.

```
enable
configure terminal
```

2. Налаштування інтерфейсів на маршрутизаторі

Переконайтеся, що інтерфейси **Fa0/0** і **Fa0/1** на маршрутизаторі налаштовані з правильними IP-адресами, щоб пристрої в мережі могли передавати пакети.

- **Fa0/0** (інтерфейс, підключений до мережі 192.168.0.0/24, де розташовані PC0 та PC1):

```
interface FastEthernet0/0
ip address 192.168.0.1 255.255.255.0
no shutdown
```

- **Fa0/1** (інтерфейс, підключений до мережі 10.10.0.0/24, де знаходиться сервер Server0):

```
interface FastEthernet0/1
ip address 10.10.0.1 255.255.255.0
no shutdown
```

Налаштування сервера

Для налаштування сервера **Server0** відповідно до рисунка 3.3, виконайте наступні кроки:

1. Відкрийте налаштування сервера:
   - На робочому столі Cisco Packet Tracer клацніть на **Server0**. Це відкриє вікно з налаштуваннями сервера.

2. Перейдіть на вкладку Desktop:
   - У верхньому меню виберіть вкладку **Desktop**. Це дозволить налаштувати IP-адресу сервера.
3. Виберіть розділ IP Configuration:
   - На вкладці Desktop відкрийте розділ **IP Configuration** (Конфігурація IP).
4. Налаштування статичної IP-адреси (рис.3.3):
   - Виберіть опцію **Static** для призначення серверу постійної IP-адреси.
   - В полі **IPv4 Address** введіть IP-адресу сервера. Згідно з рисунком, введіть **10.0.0.100**.
   - В полі **Subnet Mask** введіть маску підмережі. На рисунку вказана маска **255.0.0.0**, що відповідає мережі класу A.
   - В полі **Default Gateway** введіть адресу шлюзу за замовчуванням. Відповідно до рисунка, це **10.0.0.1**.
5. Завершення налаштування:
   - Після введення IP-адреси, маски підмережі та шлюзу за замовчуванням, закрийте вікно налаштувань.

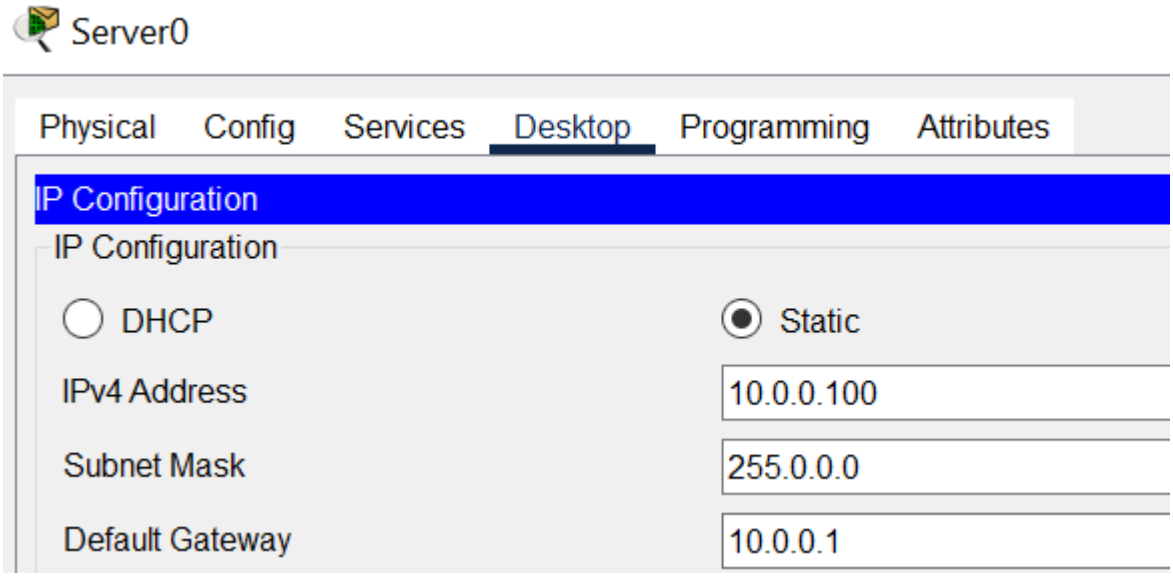


Рисунок 3.3 – Налаштування сервера

Після виконання цих кроків сервер **Server0** буде мати такі налаштування:

- **IP-адреса**: 10.0.0.100
- Маска підмережі: 255.0.0.0
- Шлюз за замовчуванням: 10.0.0.1

Це налаштування дозволяє серверу спілкуватися з іншими пристроями в мережі, використовуючи вказані IP-параметри, і передавати трафік через маршрутизатор, вказаний як шлюз.

Діагностика мережі

На рисунку 3.4 наведено результат виконання команди ping для діагностики мережевого з'єднання. Операції проводяться для перевірки доступності двох IP-адрес: **10.0.0.100** (сервер) і **192.168.0.11** (іншого комп'ютера в локальній мережі). (рис. 3.4).

```
C:\>ping 10.0.0.100

Pinging 10.0.0.100 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.100: bytes=32 time<1ms TTL=127
Reply from 10.0.0.100: bytes=32 time<1ms TTL=127
Reply from 10.0.0.100: bytes=32 time=1ms TTL=127

Ping statistics for 10.0.0.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.0.11

Pinging 192.168.0.11 with 32 bytes of data:

Reply from 192.168.0.11: bytes=32 time<1ms TTL=128
Reply from 192.168.0.11: bytes=32 time=16ms TTL=128
Reply from 192.168.0.11: bytes=32 time<1ms TTL=128
Reply from 192.168.0.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 4ms

C:\>
```

Рисунок 3.4. - ПК з різних мереж можуть спілкуватися

Налаштування списку контролю доступу (ACL) на маршрутизаторі **R0**, що дозволяє пакети з IP-адреси **192.168.0.12** (вузол) до сервера з IP-адресою **10.0.0.100** дозволить трафік лише для цього з'єднання, тоді як інші підключення можуть бути заблоковані залежно від політики безпеки. Для налаштування, виконайте наступні кроки:

1. Увійдіть у режим конфігурації маршрутизатора R0:

- Підключіться до маршрутизатора **R0** (наприклад, через консоль або Telnet) і перейдіть у привілейований режим, ввівши команду:

```
Enable
```

- Перейдіть в глобальний режим конфігурації:

```
configure terminal
```

2. Створіть розширений ACL для дозволу трафіку з IP-адреси 192.168.0.12 до сервера 10.0.0.100:
   - Введіть команду для створення ACL з ідентифікатором, наприклад, **1** (стандартний ACL):

```
access-list 1 permit ip host 192.168.0.12 host 10.0.0.100
```

   - Ця команда створює ACL з номером 1, який дозволяє IP-трафік лише від конкретного вузла з IP-адресою **192.168.0.12** до сервера **10.0.0.100**. Використання ключового слова host вказує на точну IP-адресу без маски.
3. Додайте правило для дозволу іншого трафіку (опціонально):
   - Якщо потрібно дозволити весь інший трафік, додайте правило, яке дозволяє всі інші пакети:

```
access-list 1 permit ip any any
```

   - Це правило дозволяє всім іншим пакетам проходити через інтерфейс, до якого застосовано ACL. Однак, якщо ви хочете блокувати інший трафік, це правило не додавайте, щоб за замовчуванням решта пакетів блокувалася.
4. Застосуйте ACL до відповідного інтерфейсу на R0:
   - Перейдіть до інтерфейсу **FastEthernet0/0** (інтерфейс, до якого підключені пристрої з IP-адресами 192.168.0.0/24):

```
interface FastEthernet0/0
```

   - Застосуйте створений ACL для вхідного трафіку (inbound):

```
ip access-group 1 in
```

- Ця команда застосовує ACL до інтерфейсу **Fa0/0**, обмежуючи вхідний трафік на основі створених правил ACL.

5. Завершення конфігурації:
   - Вийдіть з режиму конфігурації інтерфейсу і збережіть конфігурацію:

```
exit
write memory
```

- Команда write memory (або copy running-config startup-config) зберігає зміни в конфігурації, щоб вони збереглися після перезапуску маршрутизатора.

Після виконання цих кроків маршрутизатор **R0** буде налаштований так, що трафік від **192.168.0.12** до **10.0.0.100** дозволений, тоді як інші з'єднання (якщо відсутнє загальне правило permit ip any any) можуть блокуватися. Це налаштування допомагає контролювати доступ до сервера з конкретного клієнта в мережі. На рисунках 3.5-3.6 показано код для налаштування списку контролю доступа на R0

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 1 permit host 192.168.0.12
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```

Рисунок 3.5 – .Створюємо на R0 ACL, що дозволяє пакети з PC на Server1

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int fa0/0
Router(config-if)#ip access-group 1 in
Router(config-if)#exit
Router(config)#
```

Рисунок 3.6 – Застосовуємо правило до порту Fa0/0

Перевіримо як працюють спсики контролю доступу на на маршрутизаторі **R0**. Мета перевірки – підтвердити, що ACL коректно дозволяє або блокує трафік відповідно до заданих правил, зокрема дозволяє трафік від **PC2** до сервера і блокує трафік від **PC1**. Щоб перевірити правильність роботи списку контролю доступу (ACL) на маршрутизаторі **R0** для клієнтів **PC1** (IP-адреса 192.168.0.11) та **PC2** (IP-адреса 192.168.0.12), виконайте наступні кроки:

1. Підключіться до маршрутизатора R0:
   - За допомогою консолі або Telnet підключіться до маршрутизатора **R0**.
   - Перейдіть у привілейований режим:

```
enable
```

2. Перевірка правил ACL на маршрутизаторі:
   - Переконайтеся, що ACL налаштований правильно. Виведіть список правил ACL, щоб підтвердити, що потрібні правила дозволу або блокування встановлені (рис.3.7):

```
show access-lists
```

   - Перевірте, що ACL містить правило, яке дозволяє трафік від **192.168.0.12** (PC2) до сервера **10.0.0.100** і блокує або не має правила для **192.168.0.11** (PC1).

```
Router>en
Router#sh access-list
Standard IP access list 1
    10 permit host 192.168.0.12 (4 match(es))

Router#
```

Рисунок 3.7 – Перевірка списку доступу

3. Використовуючи команду ping на клієнтах перевіремо доступ до серверу:
   - **На PC2 (192.168.0.12)**: відкрийте командний рядок і виконайте команду ping для перевірки доступу до сервера **10.0.0.100**:

```
ping 10.0.0.100
```

   - **Очікуваний результат**: пакети повинні досягти сервера, і ви повинні отримати відповіді. Це підтверджує, що ACL дозволяє трафік від **PC2** до сервера (рис.3.8).
   - **На PC1 (192.168.0.11)**: відкрийте командний рядок і виконайте ту ж команду ping для перевірки доступу до сервера **10.0.0.100**:

```
ping 10.0.0.100
```

   - **Очікуваний результат**: пакети повинні бути заблоковані, і команда ping не повинна отримувати відповіді від сервера. Це підтверджує, що ACL блокує трафік від **PC1** до сервера (рис.3.9).
4. Перевірка лічильників пакетів у ACL (опціонально):
   - Щоб побачити, скільки разів спрацювали правила ACL, використовуйте команду:

```
show access-lists 1
```

   - Ця команда виведе детальну інформацію про кількість пакетів, які відповідають кожному правилу ACL. Наприклад, якщо правило для **PC2** (permit) має лічильник пакетів, це

підтверджує, що трафік від **PC2** проходить. Якщо ж правило для **PC1** (імпліцитне deny) має лічильник або інші правила блокують цей трафік, це підтвердить, що пакети від **PC1** були заблоковані (рис.3.7).

```
C:\>ping 10.0.0.100

Pinging 10.0.0.100 with 32 bytes of data:

Reply from 10.0.0.100: bytes=32 time<1ms TTL=127
Reply from 10.0.0.100: bytes=32 time=1ms TTL=127
Reply from 10.0.0.100: bytes=32 time<1ms TTL=127
Reply from 10.0.0.100: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Рисунок 3.8 – Перевірка зв'язку з сервером PC1

```
C:\>ping 10.0.0.100

Pinging 10.0.0.100 with 32 bytes of data:

Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.

Ping statistics for 10.0.0.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Рисунок 3.8 – Перевірка зв'язку з сервером PC0

За допомогою цих кроків ви можете перевірити роботу списків контролю доступу на маршрутизаторі **R0** і переконатися, що ACL виконує свою функцію, дозволяючи трафік від **PC2** і блокуючи його для **PC1**.

3.3 Варіанти індивідуального завдання 2

Для кожного варіанту студенти повинні:

1. Створити схему мережі (рис.3.1)

2. Провести налаштування параметрів IP-адресації пристроїв мережі у відповідності до індивідуальних варіантів (таблиця 3.1). Перевірити наявність зв'язку між усіма пристроями мережі.

Таблиця 3.1 – Варіанти індивідуальних завдань

Варіант	IP адреси підмереж	Налаштування дозволу	
		Дозволити	Заборонити
1	Підмережі: 172.16.0.0 та 192.168.1.0	PC1 (172.16.0.15)	PC0 (172.16.0.10)
2.	Підмережі: 10.10.0.0 та 192.168.2.0	PC1 (10.10.0.20)	PC0 (10.10.0.25)
3.	Підмережі: 192.168.3.0 та 172.20.0.0	PC1 (192.168.3.30)	PC0 (192.168.3.35)
4.	Підмережі: 10.20.0.0 та 192.168.4.0	PC1 (10.20.0.40)	PC0 (10.20.0.45)
5.	Підмережі: 172.30.0.0 та 192.168.5.0	PC1 (172.30.0.50)	PC0 (172.30.0.55)
6.	Підмережі: 10.30.0.0 та 192.168.6.0	PC1 (10.30.0.60)	PC0 (10.30.0.65)
7.	Підмережі: 172.40.0.0 та 192.168.7.0	PC1 (172.40.0.70)	PC0 (172.40.0.75)
8.	Підмережі: 10.40.0.0 та 192.168.8.0	PC1 (10.40.0.80)	PC0 (10.40.0.85)
9.	Підмережі: 172.50.0.0 та 192.168.9.0	PC1 (172.50.0.90)	PC0 (172.50.0.95)

10.	Підмережі: 10.50.0.0 та 192.168.10.0	PC1 (10.50.0.100)	PC0 (10.50.0.105)

3. Створити та застосувати стандартний ACL.

4. Дослідити особливості роботу ACL за допомогою відповідних команд ping-тестів.

5. Задокументувати всі налаштування та результати тестів

4. КОНТРОЛЬНІ ПИТАННЯ

4.1 Контрольні питання до індивідуальної роботи №1

1. Які кроки необхідно виконати для налаштування DHCP-сервісу на сервері в Cisco Packet Tracer?
2. Як перевірити, чи клієнт отримав IP-адресу від DHCP-сервера? Які команди для цього використовуються?
3. Яка різниця між ресурсними записами типів A та CNAME на DNS-сервері, і як їх створити в Cisco Packet Tracer?
4. Опишіть процес налаштування веб-сервера на Cisco Packet Tracer. Які параметри необхідно ввімкнути, щоб сервер почав відповідати на HTTP-запити?
5. Які налаштування потрібно вказати в DHCP-пулі, щоб клієнти отримували IP-адресу, шлюз за замовчуванням і DNS-сервер?
6. Як за допомогою команди nslookup перевірити роботу DNS-сервера в Cisco Packet Tracer? Наведіть приклад команди.
7. Як налаштувати клієнтський комп'ютер на автоматичне отримання IP-адреси від DHCP-сервера в Cisco Packet Tracer?
8. Які команди можна використовувати на клієнті для звільнення та повторного отримання IP-адреси від DHCP-сервера? Опишіть їхнє призначення.
9. Як налаштувати DNS-сервер в Cisco Packet Tracer, щоб він правильно перетворював доменне ім’я (наприклад, example.net) у відповідну IP-адресу?
10. Як перевірити доступність веб-сервера з клієнтського комп’ютера в Cisco Packet Tracer? Що потрібно вказати в адресному рядку браузера?

4.2 Контрольні питання до індивідуальної роботи №2

1. Що таке список контролю доступу (ACL) і яке його основне призначення в мережах?
2. Які основні типи ACL існують, і чим вони відрізняються один від одного?
3. Яка різниця між стандартними та розширеними ACL? У яких випадках застосовуються кожен із цих типів?

4. Що таке WildCard-маска і як вона використовується в ACL для фільтрації трафіку? Наведіть приклади.
5. Як працює імпліцитне правило deny any any в ACL, і чому воно важливе для безпеки мережі?
6. Яка різниця між вхідним (inbound) та вихідним (outbound) ACL? Коли доцільно застосовувати кожен з них?
7. Яка роль іменованих ACL, і в чому їхня перевага порівняно з числовими ACL?
8. Що таке динамічні ACL (Dynamic ACL) та зворотні ACL (Reflexive ACL)? У яких ситуаціях вони використовуються?
9. Як впливає порядок правил у списку ACL на його роботу? Чому важливо правильно розміщувати правила в ACL?
10. Які команди використовуються для перевірки налаштувань ACL на маршрутизаторах Cisco і для моніторингу їхньої роботи?

5. КРИТЕРІЇ ОЦІНЮВАННЯ

Підготовлений звіт у вигляді файлу *pdf розміщується у відповідному розділі дисципліни в Moodle і перевіряється протягом тижня після завершення терміну подачі. Оскарження оцінки може бути здійснене на останньому практичному занятті модуля.

Max 15 балів:

– студент підготував звіт за індивідуальним завданням, в якому: правильно визначив мету, описав комп’ютерну мережу, відповів на контрольні запитання, представив висновок, матеріали звіту викладено діловим, науковим або публіцистичним стилем української (10 балів);

– студент під час захисту індивідуального завдання демонструє володіння термінологічним апаратом, відповідає на запитання, здатний продемонструвати робочу мережу (5 балів).

6. ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТРИ

1. Технологія Ethernet : лабораторний практикум / М. О. Білова, С. П. Євсеєв, О. С. Жученко, І. С. Іванченко, О. В. Шматко. Харків : НТУ «ХПІ», 2019. 194 .
2. Computer Networks Title: Computer Networking: A Top-Down Approach / A. Tanenbaum et al. Instructor. 2019. Т. 201901.
3. Проектування комп'ютерних систем та мереж : навч. посіб. / О. А. Смірнов. Кропивницький : Видавець Лисенко В. Ф., 2019. 264 с.
4. Вибрані питання комп'ютерних систем та мереж : навчальний посібник / укладач Г. В. Ткачук. Умань : Візваві, 2018. 130 с.
5. Технології проектування комп'ютерних систем (частина 1) / В. А. Лахно. Київ : НУБіП України, 2019. 205 с.
6. Comer D. E. The Internet book: everything you need to know about computer networking and how the Internet works. Chapman and Hall/CRC, 2018.
7. Cisco packet tracer simulation as effective pedagogy in Computer Networking course / N. A. Rashid et al. *International Journal of Interactive Mobile Technologies (iJIM)*. 2019. №*13*(10). P. 4–18. DOI: https://doi.org/10.3991/ijim.v13i10.11283.
8. Open educational resources for computer networking / O. Bonaventure et al. *ACM SIGCOMM Computer Communication Review*. 2020. Т. 50. №. 3. С. 38-45.
9. Gould C. C. The information web: Ethical and social implications of computer networking. Routledge, 2019.
10. Ryan N. G. Basic Computer Networking. XP Solution Surabaya, 2018. Т. 3.
11. Blokdyk G. Computer Network A Complete Guide - 2024 Edition. 5STARCooks, 2023. 252 p. URL: https://read.kortext.com/inventory/search/2498876.
12. Cisco Academy : веб-сайт. URL:https://www.netacad.com/ (дата звернення: 27.09.2024).

ДОДАТОК А

ТОВ «ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«МЕТІНВЕСТ ПОЛІТЕХНІКА»
Факультет автоматизації виробництва
та цифрових технологій
Кафедра цифрових технологій
та проєктно-аналітичних рішень

ЗВІТ
З ІНДИВІДУАЛЬНОГО ЗАВДАННЯ №1

з дисципліни: «КОМП'ЮТЕРНІ МЕРЕЖІ»

на тему
«Технології та протоколи
логічної адресації в IP-мережах»

Роботу виконав Іван ФЕЩЕНКО

Роботу перевірив Олександр ШМАТКО

ЗАПОРІЖЖЯ 2024

ЗМІСТ

1. Мета роботи

Чітке формулювання мети індивідуального завдання та очікуваних результатів.

2. Вихідні дані

- Номер та опис варіанту завдання
- Топологія мережі
- Вимоги до налаштування
- Обмеження та додаткові умови

3. Хід виконання роботи

3.1. Проектування мережі

- Схема мережі з позначенням всіх пристроїв

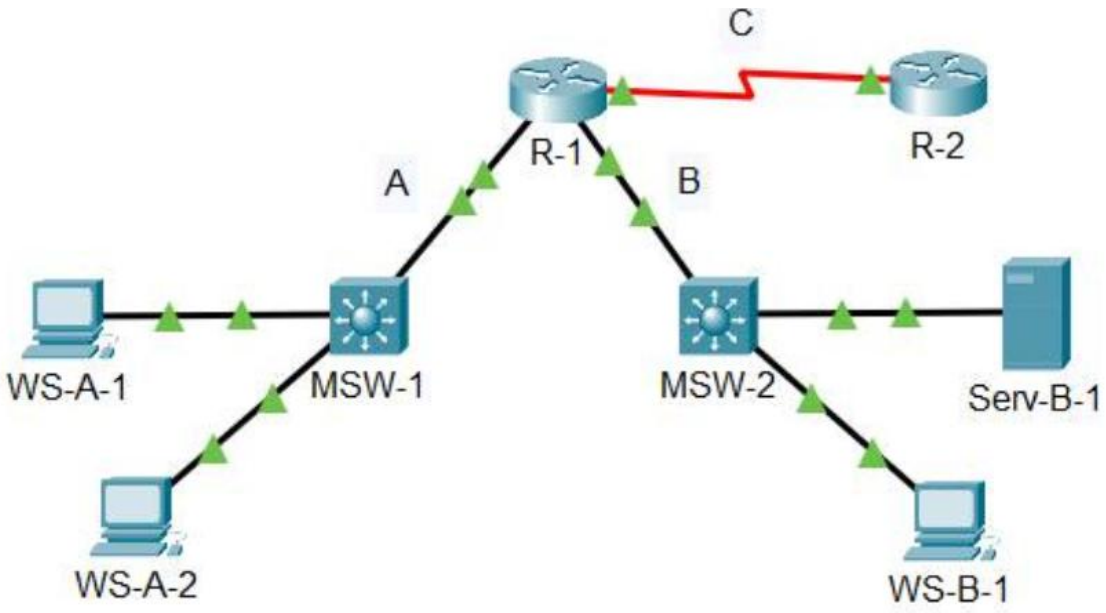


Рисунок 1 – Приклад топології мережі

Оформлення рисунків:

- Послідовна нумерація
- Підписи під рисунками
- Посилання на рисунки в тексті
- Якісні та інформативні зображення
- Таблиця IP-адресації

Таблиця 1 - Параметри IP-адресації підмереж

Мережа	Адреса мережі	Префікс
A	2001:G:N:A::	/64
B	2001:G:N:B::	/64
C	2001:G:N:C::	/64
D	2001:G:N:D::	/64
E	2001:G:N:E::	/64

Оформлення таблиць:

– Послідовна нумерація
– Заголовки таблиць виділяються напівжирним
– Посилання на таблиці в тексті
– Опис логічної структури мережі

3.2. Налаштування обладнання

– Базова конфігурація пристроїв
– Налаштування протоколів маршрутизації
– Конфігурація додаткових параметрів
– Повні конфігурації всіх пристроїв

3.3. Тестування мережі

– Результати перевірки зв'язності
– Таблиці маршрутизації
– Результати налагодження (debugging)
– Скріншоти виконання команд перевірки

4. Відповідь на контрольні запитання

Відповіді на контрольні запитання

ВИСНОВКИ

Підсумок виконаної роботи та отриманих практичних навичок.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.
2.
3.

Навчально-методичне видання

Шматко Олександр Віталійович
Гамаюн Ігор Петрович
Держевець Марина Анатоліївна

КОМП’ЮТЕРНІ МЕРЕЖІ

методичні рекомендації до виконання індивідуального розрахункового завдання

Самостійне електронне мережеве видання

Публікується в авторський редакції