

Міністерство освіти і науки України  
НТУУ «КПІ ім. Ігоря Сікорського»  
Навчально-науковий інститут атомної та теплової енергетики  
Кафедра цифрових технологій в енергетиці

Лабораторна робота №2  
з дисципліни  
«Інформаційне забезпечення комп'ютерних систем»  
Тема «Основи побудови комп'ютерної мережі»  
Варіант №18

Студента 4-го курсу НН ІАТЕ гр. ТР-12

Ковальова Олександра

Перевірив: доцент, Онисько А. І.

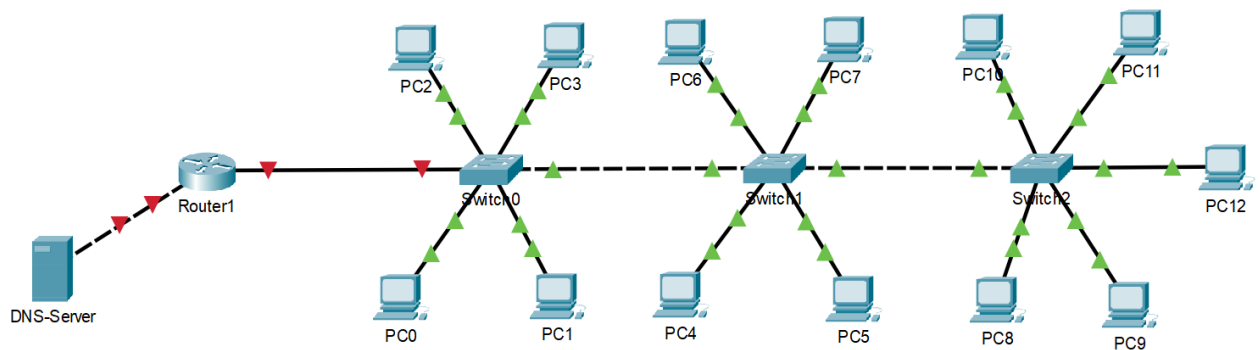
**Мета роботи.** Ознайомитися з основними поняттями комп'ютерних мереж, з видами топологій, класифікацією по області дії, за призначенням, типом комп'ютерів, які входять до складу комп'ютерної мережі, за територіальним розташуванням, за типом функціональної взаємодії та набуття навиків у побудові мережі та її налаштуванні.

**Індивідуальне завдання:**

1. Побудувати мережу за такими даними:
  - *Кількість робочих станцій:* 13;
  - *Кількість мережевих пристроїв:* 3;
  - *Топологія мережі:* Шина;
  - *Клас мережі:* В.
2. IP-адресу шлюзу вибирати виходячи з першої адреси вузла обраної мережі.  
IP-адреса DNS сервера – 172.20.0.149.  
Присвоїти IP-адресу усім комп'ютерам мережі із врахуванням класу мережі.  
IP-адресу, маску мережі, адресу шлюзу, DNS сервера мережі відобразити на схемі мережі.
3. У відповідності до побудованої мережі представити наступні теоретичні матеріали:
  1. Характеристику використаної кабельної системи.
  2. Описати переваги і недоліки використаної топології мережі.
  3. Пояснити поняття класів IP-адрес: А, В, С.
  4. Призначення маски мережі, як проводиться розрахунок кількості вузлів відповідно неї, як маска використовується в умовах дефіциту IP-адрес.
4. Замість висновку відповісти на теоретичні питання.

**Хід роботи**

Для початку, треба побудувати мережу з 13 робочих станцій, з трьома мережевими пристроями, топологія мережі – шина. Клас мережі – В.



Побудована мережа представлена на скріншоті. Вона схожа на топологію «Зірка», але попри це, потрібно звернути увагу на «кістяк» – підключення йде однією

лінією через всі комутатори до маршрутизатора. Маємо 13 робочих станцій, 3 мережеві пристрої (комутатори – свічі) та один маршрутизатор (роутер).

В якості комутаторів обрана модель Cisco 2960. Такий вибір був зроблений через те, що ця модель максимально підходить для умов лабораторної роботи, є популярною для загального користування.

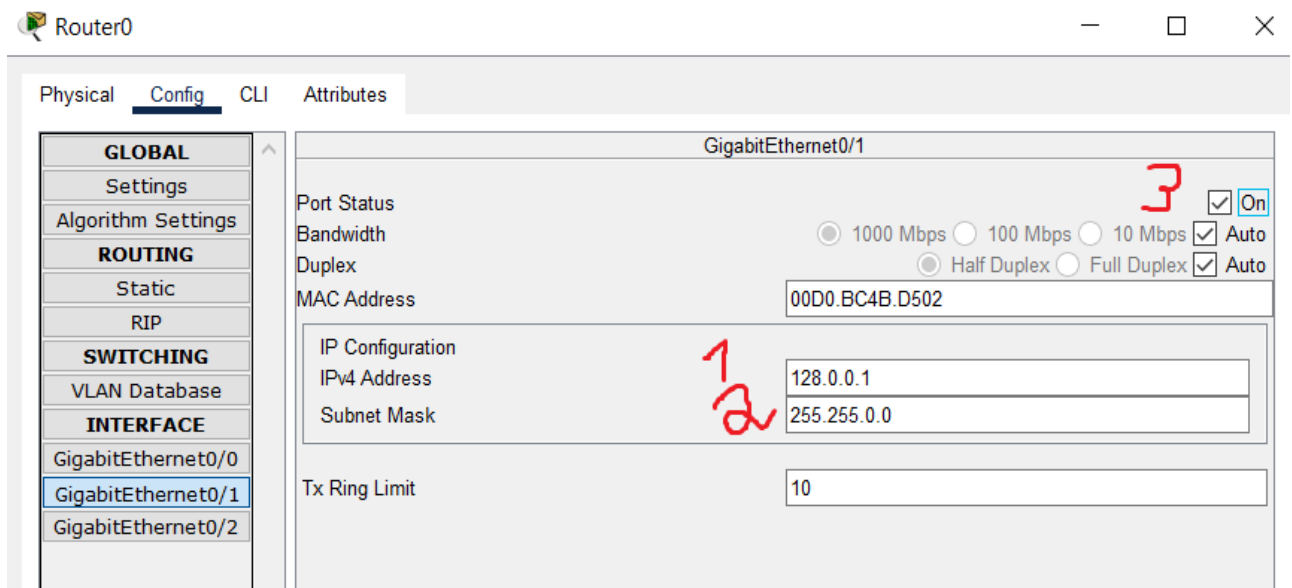
Щодо роутеру – був обраний Cisco Router 2911. Ця модель є оптимальною для середніх мереж, підтримує Layer 3 Switching.

Для встановлення зв'язку між персональними комп'ютерами, треба призначити IP-адреси.

Так як маємо клас мережі B, то перші два біти адреси – 10. Перший октет – 128-196. Маска підмережі – 255.255.0.0. Число можливих адрес мережі – 16384. Число можливих адрес хостів – 65536.

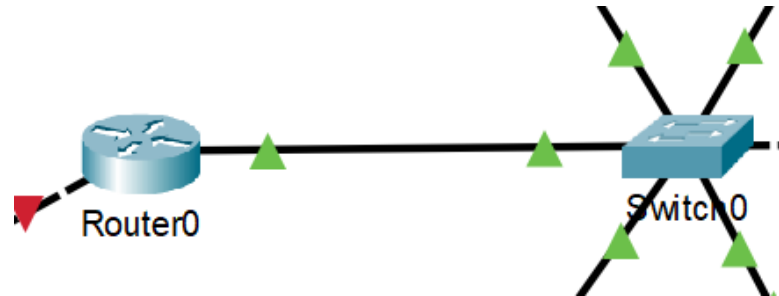
Насправді, ця система є дуже застарілою [1][2][3], нею зовсім незручно користуватись. В 1993 році з'явилась система CIDR (Classless Inter-Domain Routing), яка ввела систему масок (так, в класовій системі такого не існувало, але навіть в даному прикладі для зручності маска була приведена як приклад, що свідчить про факт – про класову систему можна забути, вивчати її наразі не варто *[хоча це й моя особиста думка, для обґрунтування посилаюсь на 2]*). Ця система повністю замінила класову, так як розподіл IP-адрес став набагато ефективнішим, без зайвих втрат хостів (наприклад, потрібна мережа на 16 хостів, але адміністратор повинен розраховувати на більшу кількість), та й загалом вона є простою для розуміння.

Оберемо мережу 128.0.0.0. Так як за «мережеву частину» відповідають два октети (128.0), то за «хостову» частину відповідають інші 2 (0.0). Адресою мережі буде 128.0.0.0. Broadcast – 128.0.255.255. Зазвичай, першим хостом є роутер. Призначаємо роутеру IP адресу 128.0.0.1:



Окрім цього, звичайно, потрібно вказати маску (255.255.0.0), та увімкнути порт (зазвичай, в Cisco Packet Tracer порти роутерів вимкнені за замовчуванням).

Можемо бачити, що підключення між комутатором та маршрутизатором з'явилося:



Призначаємо адреси всім ПК: від 128.0.0.2 до 128.0.0.14. Також, відразу призначаємо Default Gateway – адресу роутера (128.0.0.1) та адресу DNS-серверу (172.20.0.149):

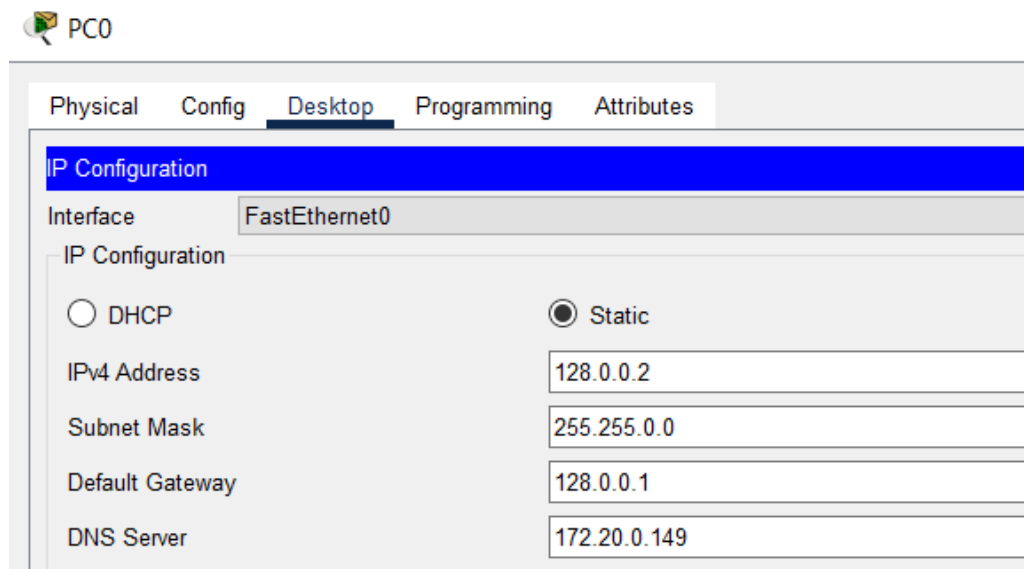
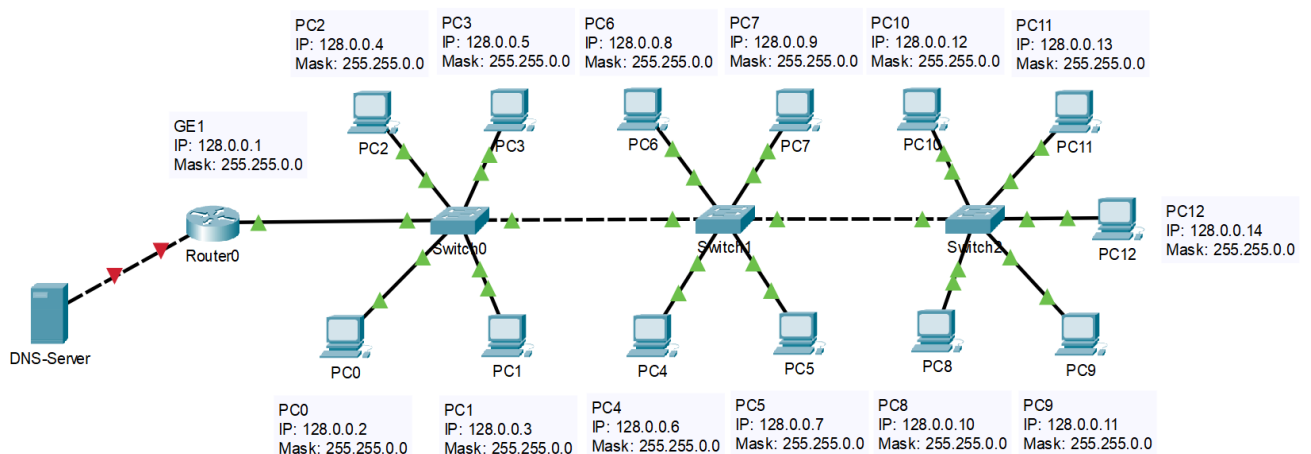
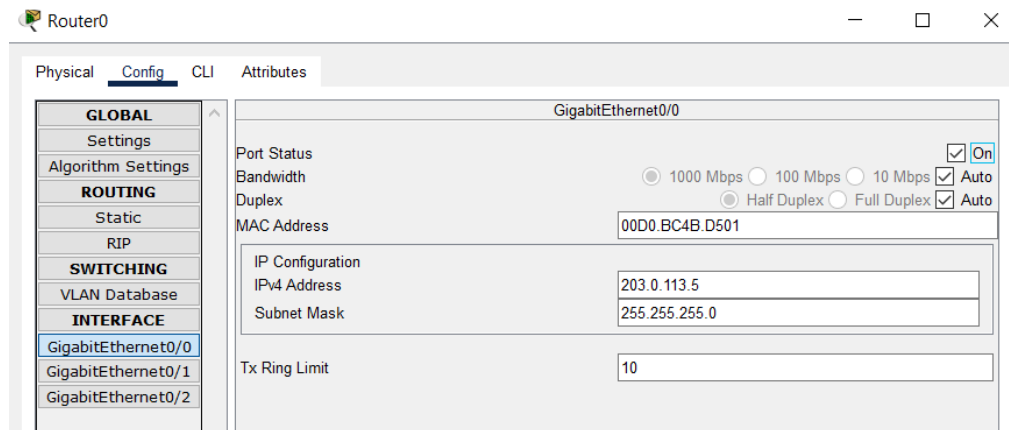


Схема:



Для того, щоб був наявний доступ до «глобальної мережі» (WAN) потрібно ще призначити IP-адресу роутеру на його перший порт, GE0. Адреса повинна бути «білою», зазвичай внутрішня мережа має «сірі» адреси, та на роутері працює технологія NAT.

Оберемо адресу 203.0.113.5 (просимулюємо NAT). Ця адреса належить зарезервованому блоку адрес, призначених для документації та тестування [4].



Також встановимо IP-адреси на DNS сервері і додатковому сервері Google (для тестування DNS) – 8.8.8.8. Окрім цього, встановимо «глобальний роутер», до якого буде звертатись наш. Можемо вважати, що це роутер провайдера.

IP-адреса на інтерфейсі GE0 (вихід до DNS-серверу): 172.20.0.1

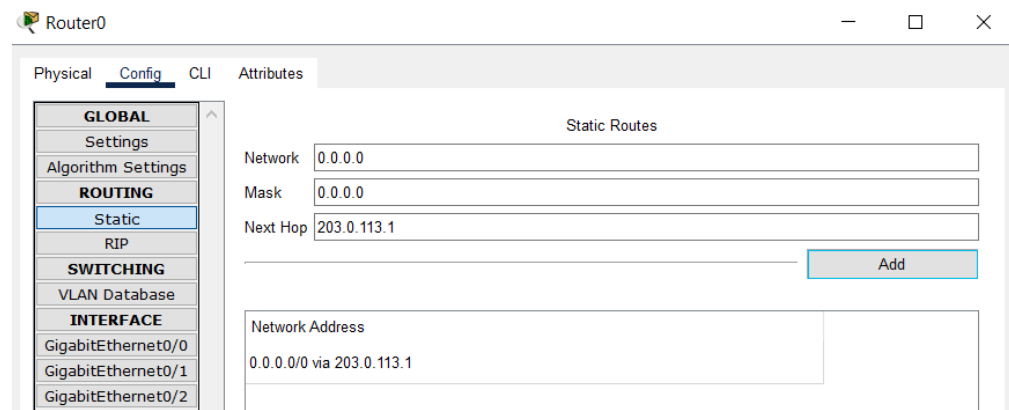
IP-адреса на інтерфейсі GE1 (вихід до «серверу Google»): 8.0.0.1

IP-адреса на інтерфейсі GE2 (вихід до нашого роутера): 203.0.113.1

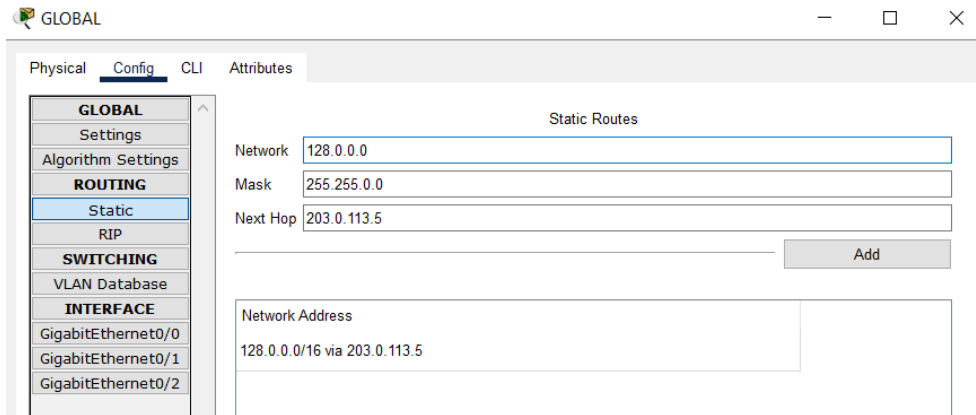
При спробі пропінгувати DNS з серверу нас чекає помилка: сервер недоступний.

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 172.20.0.149, timeout is 2 seconds:  
.....  
Success rate is 0 percent (0/5)  
Router>
```

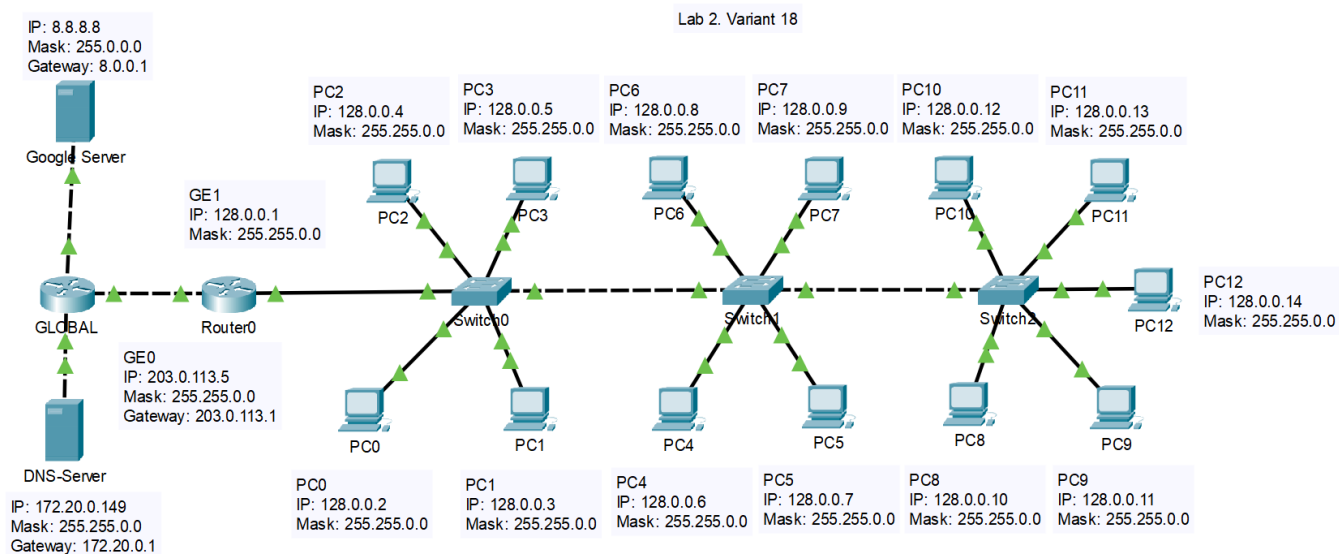
Проблема полягає в тому, що роутер не знає як дістатись до серверу. Потрібно прописати шляг в роутінгу. Так як це вихід в глобальний інтернет, то потрібно вказувати «шлях останньої надії» – мережа 0.0.0.0 з маскою 0.0.0.0:



Для того щоб глобальний роутер дізнався про нашу внутрішню мережу, заради симуляції, можна вказати шлях до нашого роутера:



Загальний вигляд схеми:



Спробуємо пропінгувати DNS-сервер з певного ПК. Наприклад, з ПК4:

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...: 
    Link-local IPv6 Address . . . . .: FE80::201:42FF:FEA0:C18E
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 128.0.0.6
    Subnet Mask . . . . .: 255.255.0.0
    Default Gateway . . . . .: ::
                                   128.0.0.1

Bluetooth Connection:

    Connection-specific DNS Suffix...: 
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                   0.0.0.0

C:\>ping 172.20.0.149

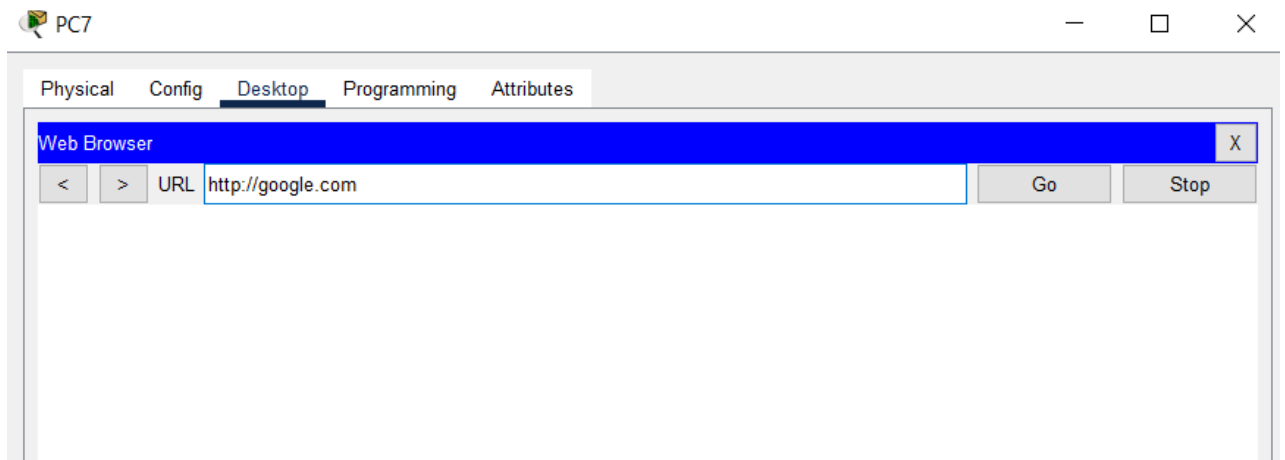
Pinging 172.20.0.149 with 32 bytes of data:

Reply from 172.20.0.149: bytes=32 time<1ms TTL=126
Reply from 172.20.0.149: bytes=32 time<1ms TTL=126
Reply from 172.20.0.149: bytes=32 time<1ms TTL=126
Reply from 172.20.0.149: bytes=32 time<1ms TTL=126

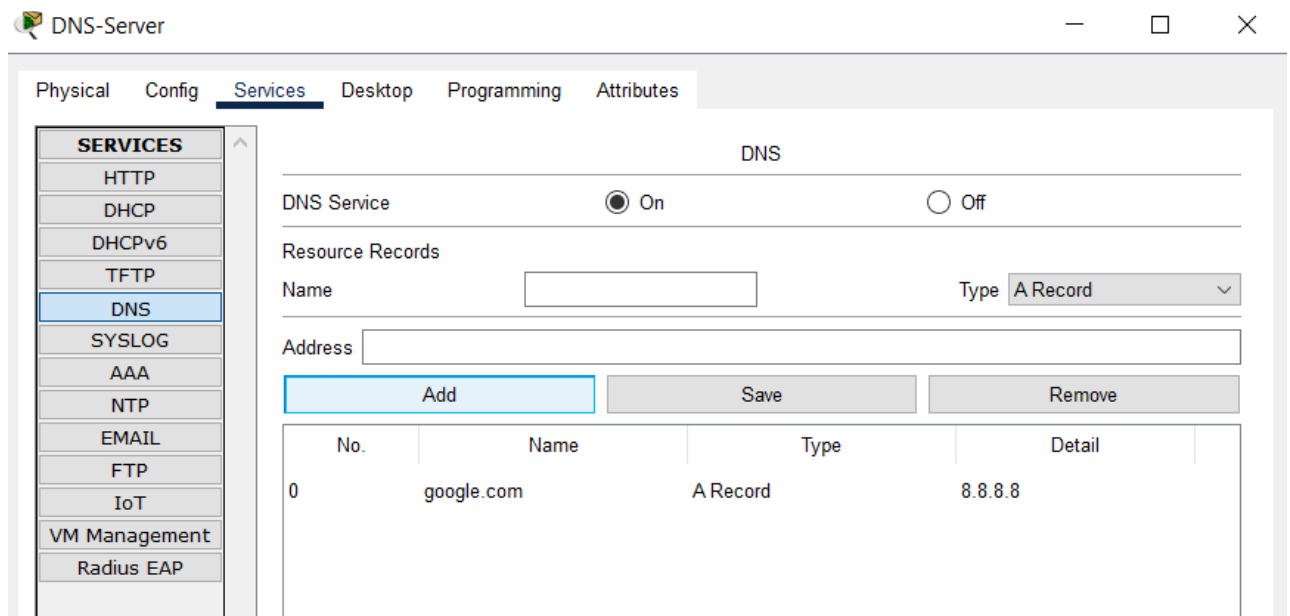
Ping statistics for 172.20.0.149:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

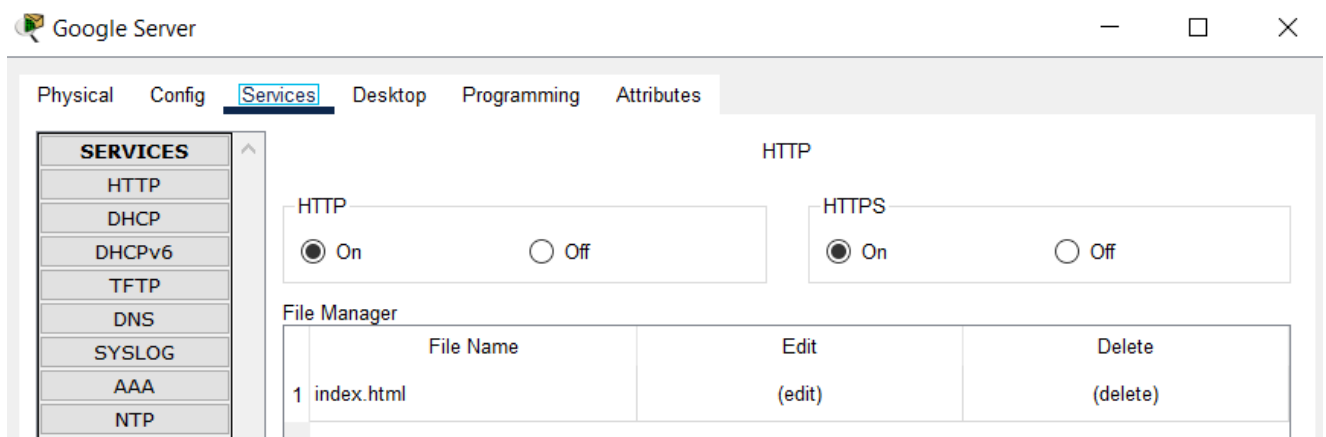
Зв'язок наявний, все працює. Спробуємо зайти на google.com:



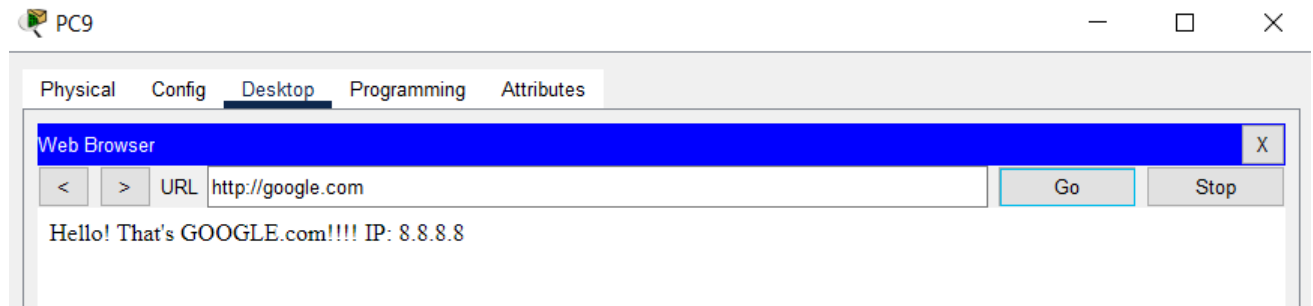
Нічого не отримуємо. Помилка в тому, що не наявний запис DNS на сервері. Вмикаємо сервер, додаємо запис з типом «A Record» (пряме зв'язування доменного імені з адресою):



Вмикаємо HTTP сервер на google.com:



Спробуємо зайти на сайт, наприклад, з PC9:



Все працює. Завдання виконане.

### **Пункт 3 – Теоретичні матеріали.**

*Характеристика використаної кабельної системи.*

В системі використовувались кабелі Copper Straight-Through та Copper Cross-Over, в перекладі на українську прямий мідний кабель та перехресний мідний кабель. Перехресний використовується щоб з'єднувати пристрої одного типу, прямий – різного (наприклад, комутатор та персональний комп'ютер).

*Описати переваги і недоліки використаної топології мережі.*

Топологія «шина» є однією з найпростіших і найстаріших мережевих структур. Вона передбачає використання одного центрального кабелю, до якого підключаються всі пристрої мережі. Однією з головних переваг такої топології є простота реалізації. Використання одного кабелю зменшує витрати на матеріали та прокладання, а також полегшує налаштування. Крім того, шина є зручним варіантом для невеликих мереж із обмеженою кількістю пристроїв, де немає потреби в складних конфігураціях.

Однак топологія шина має і свої недоліки. Основним недоліком є залежність всієї мережі від одного кабелю. Якщо цей кабель зазнає пошкодження, то вся мережа перестає працювати. Також з часом можуть виникати проблеми із затримкою сигналу, особливо якщо кількість підключених пристроїв збільшується, оскільки всі вони ділять один канал для передачі даних. Крім того, виявлення й усунення несправностей у такій мережі може бути складним процесом, оскільки всі пристрої підключені до одного й того самого кабелю, і важко точно визначити місце збою.

Топологія шина також має обмежену масштабованість, оскільки додавання нових пристроїв може ускладнити передачу даних, збільшуючи трафік у мережі. Хоча ця топологія була популярною на ранніх етапах розвитку комп'ютерних мереж, сьогодні її рідко використовують у сучасних великих і складних мережах через перелічені обмеження.

*Пояснити поняття класів IP-адрес: A, B, C.*

IP-адреси поділялись на класи для полегшення їх використання та організації мереж (до появи CIDR). Класи A, B і C визначають різні діапазони IP-адрес, які використовуються для різних масштабів мереж.



Клас А призначений для дуже великих мереж і охоплює адреси, де перший октет (перша частина IP-адреси) варіюється від 1 до 126. У таких мережах перший октет використовується для ідентифікації мережі, а решта три октети – для ідентифікації окремих пристроїв. Це дозволяє створювати мережі з великою кількістю пристроїв.

Клас В підходить для середніх мереж і включає IP-адреси, де перший октет знаходиться в діапазоні від 128 до 191. У мережах класу В перші два октети використовуються для ідентифікації мережі, а два інші – для адресації пристроїв всередині цієї мережі. Це дає можливість мати більше мереж, але з меншою кількістю пристроїв у кожній, порівняно з класом А.

Клас С призначений для невеликих мереж і охоплює адреси з першим октетом від 192 до 223. У цьому класі перші три октети ідентифікують мережу, а останній октет призначений для ідентифікації пристроїв. Мережі класу С мають обмежену кількість пристроїв, але таких мереж може бути набагато більше, ніж у класах А і В.

Таким чином, кожен клас IP-адрес має своє призначення та масштаб використання, залежно від розміру мережі та кількості пристроїв, які потрібно адресувати.

Також, є класи D і E. Клас D використовується для мультикастингу, де дані надсилаються групам пристроїв, і охоплює адреси від 224 до 239. Клас E зарезервований для експериментальних цілей, з адресами від 240 до 255, і не використовується в звичайних мережах.

*Призначення маски мережі, як проводиться розрахунок кількості вузлів відповідно неї, як маска використовується в умовах дефіциту IP-адрес.*

Маска мережі визначає, яка частина IP-адреси відповідає мережі, а яка – вузлам у цій мережі. Вона допомагає розділити IP-адресу на дві частини: мережеву і ту, що ідентифікує конкретний пристрій (вузол) у мережі. Маска складається з 32 бітів, де всі біти, що відповідають мережевій частині, встановлені в 1, а біти, що відповідають вузлам, – у 0. Наприклад, маска 255.255.255.0 показує, що перші три октети відповідають мережевій частині, а останній – вузлам.

Розрахунок кількості вузлів у мережі проводиться за допомогою маски. Для цього визначають кількість бітів, відведених під вузли (біти, що дорівнюють 0). Якщо в масці мережі 8 бітів відведено під вузли, то кількість можливих адрес для вузлів дорівнює  $2^8$  (256), але треба відняти дві адреси: одну для самої мережі і одну для широкомовної адреси, отже, доступно 254 вузли.

У разі дефіциту IP-адрес маска використовується для «сабнеттінгу», тобто поділу однієї великої мережі на менші підмережі. Це дозволяє ефективніше використовувати доступні адреси, оскільки кожна підмережа матиме свою мережеву частину та власний набір вузлів, навіть якщо загальна кількість IP-адрес обмежена.

#### **Пункт 4 – Відповіді на теоретичні питання.**

*Описати основні положення LAN, PAN, WAN.*

LAN, або локальна мережа, є системою, що охоплює невелику географічну область, зазвичай одну будівлю або групу сусідніх будівель. Вона забезпечує високошвидкісний обмін даними між пристроями, такими як комп'ютери, принтери та

сервери, через Ethernet або Wi-Fi. LAN зазвичай використовується в офісах, школах або домах, де кількість підключених пристроїв не перевищує кількох десятків.

PAN, або персональна мережа, є ще меншою за масштабом і призначена для з'єднання особистих пристроїв на відстані до кількох метрів. Зазвичай у PAN підключаються мобільні телефони, ноутбуки, планшети та інші гаджети за допомогою технологій Bluetooth або Wi-Fi. PAN дозволяє користувачам швидко та зручно обмінюватися даними між особистими пристроями.

WAN, або глобальна мережа, охоплює великі території, такі як міста, країни або навіть континенти. WAN складається з багатьох мереж, які з'єднуються через різні типи комунікаційних ліній, такі як оптоволокно або супутникові з'єднання. WAN забезпечує зв'язок між LAN та PAN на великих відстанях. До речі, мережа Internet теж є WAN.

*Які ви знаєте види комп'ютерних мереж? Поясніть, чим вони різняться.*

Існує кілька видів комп'ютерних мереж, які розрізняються за масштабом, архітектурою і призначенням. LAN, як уже згадувалося, є локальною мережею, яка з'єднує пристрої на невеликій території. WAN охоплює великі відстані та з'єднує різні LAN, забезпечуючи зв'язок між ними. Ще одним видом є MAN (Metropolitan Area Network), яка об'єднує кілька LAN у межах одного міста або великої території.

Крім того, існують також спеціалізовані мережі, такі як VPN (Virtual Private Network), які використовуються для безпечного підключення до мережі через Інтернет. Інші приклади включають SAN (Storage Area Network), призначену для зберігання даних, і WLAN (Wireless Local Area Network), яка є бездротовою версією LAN. Кожен вид мережі має свої особливості, завдання і технології, які використовуються для їх реалізації.

*Назвіть характеристики каналів зв'язку.*

Канали зв'язку мають кілька ключових характеристик, які визначають їх ефективність і можливості. По-перше, це пропускна спроможність, яка вимірюється в біт/с і визначає, скільки даних може передаватися через канал за одиницю часу. Чим вища пропускна спроможність, тим більше даних можна передати, що особливо важливо для швидкісного інтернет-з'єднання.

Другою важливою характеристикою є затримка, яка визначає, скільки часу потрібно, щоб дані досягли своєї цілі. Затримка може впливати на якість зв'язку, особливо в реальному часі, наприклад, під час відеоконференцій. Також слід враховувати надійність каналу, яка вказує на ймовірність успішної передачі даних без втрат або спотворень.

Крім того, важливими є також типи передачі (аналогова чи цифрова), фізичні засоби передачі (оптоволокно, мідь, радіохвилі) і можливість масштабування каналу в міру зростання потреб. Ці характеристики разом визначають, наскільки ефективно і якісно канал може виконувати свої функції у мережі.

*Поясніть різницю між повторювачем та концентратором.*

Повторювач і концентратор – це два різних мережевих пристрої, які використовуються для з'єднання та розширення мережі, але їх функції суттєво відрізняються. Повторювач, як правило, використовується для підсилення та

відновлення сигналу, щоб подовжити довжину кабелю в мережі. Він приймає слабкий сигнал, підсилює його і передає далі, що дозволяє зберігати якість передачі даних на великих відстанях.

Концентратор, з іншого боку, є більш складним пристроєм, який діє як центральна точка для з'єднання декількох пристроїв у мережі. Він отримує дані від одного пристрою і розподіляє їх на всі інші підключені пристрої. Однак концентратор не має можливості аналізувати дані або визначати, куди їх слід надіслати, тому всі пристрої отримують один і той же сигнал, що може призводити до конфліктів у передачі даних. Таким чином, повторювач забезпечує підсилення сигналу, тоді як концентратор є розподільником для з'єднання кількох пристроїв у мережі.

#### **Додаткові джерела:**

1. Is classful networking still relevant? URL: <https://eitca.org/cybersecurity/eitc-is-cnf-computer-networking-fundamentals/internet-protocols/introduction-to-ip-addresses/is-classful-networking-still-relevant/>
2. Classful Routing Has Little Meaning In Modern Networking. URL: <https://packetpushers.net/blog/classful-addressing-has-little-meaning-in-modern-networking/>
3. Difference Between Classful Routing and Classless Routing. URL: <https://www.geeksforgeeks.org/difference-between-classful-routing-and-classless-routing/>
4. Reserved IP addresses. URL: [https://en.wikipedia.org/wiki/Reserved\\_IP\\_addresses](https://en.wikipedia.org/wiki/Reserved_IP_addresses)