Міністерство освіти і науки України
Сумський державний університет

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт
з дисципліни «Телекомунікаційні та інформаційні мережі»
для студентів спеціальності
172 "Телекомунікації та радіотехніка"
усіх форм навчання

Суми
Сумський державний університет
2017

Методичні вказівки до виконання лабораторних робіт з дисципліни «Телекомунікаційні та інформаційні мережі» / укладачі: О. В. Д’яченко, О. Є. Горячев, Т. О. Протасова, К. О. Д’яченко. – Суми: Сумський державний університет, 2017. – 33 с.

Кафедра електроніки і комп’ютерної техніки

Лабораторна робота №5

Протоколи ARP і ICMP (програми ping і tracert)

Мета роботи: вивчити режим симуляції Cisco Packet Tracer, протоколи ARP і ICMP на прикладі програм ping і tracert.

Програма роботи:

1. Побудова топології мережі, настройка кінцевих вузлів;
2. Налаштування маршрутизатора;
3. Перевірка роботи мережі в режимі симуляції;
4. Здійснення ping-запиту всередині мережі;
5. Здійснення ping-запиту в зовнішню мережу;
6. Здійснення ping-запиту на неіснуючий IP-адреса вузла;
7. Виконання індивідуального завдання.

Теоретичні відомості: протокол ARP Для визначення фізичної адреси по IP-адресою використовується протокол дозволу адреси Address Resolution Protocol (ARP). Протокол ARP працює по-різному залежно від того, який протокол канального рівня працює в даній мережі з можливістю широкомовного доступу одночасно до всіх вузлів мережі. [1] Протокол ARP дозволяє динамічно визначити MAC-адреса по IP-адресою. MAC-адреса - це унікальний серійний номер, який присвоюється кожному мережевому пристрою для ідентифікації його в мережі, так само називається фізичним або апаратним адресою. Протокол локальної мережі, підтримуваний в лабораторній роботі - Ethernet. У Ethernet мережах, що використовують стек TCP / IP, мережевий інтерфейс має фізичну адресу довжиною в 48 біт. Кадри, якими обмінюються на канальному рівні, повинні містити апаратну адресу мережевого інтерфейсу. Однак TCP / IP використовує власну схему адресації: 32-бітові IP-адреси. Значення IP-адреси приймача недостатньо, щоб відправити дейтаграмму цього хосту. Драйвер Ethernet повинен знати MAC-адреса інтерфейсу призначення, щоб послати туди дані. У завдання ARP входить забезпечення динамічного відповідності між 32-бітними IP-адресами і 48-бітними MAC-адресами, використо-

вуваними різними мережевими технологіями. Протокол ARP працює в межах однієї підмережі і автоматично запускається, коли виникає необхідність перетворення IP-адреси в апаратну адресу.[2]

Робота протоколу ARP пояснюється на рис. 4.25.

Рис. 4.25 ARP-запит і ARP-відповідь

Вузол, якому потрібно виконати відображення IP-адреси на локальний адресу, формує ARP-запит, вкладає його в кадр протоколу канального рівня, вказуючи в ньому відомий IP-адреса, і розсилає запит широкомовно. Всі вузли локальної мережі отримують ARP запит і порівнюють зазначений там IP-адресу з власним. У разі їх збігу вузол формує ARP-відповідь, в якому вказує свій IP-адресу і свій локальний адресу і відправляє його вже направлено, так як в ARP запиті відправник вказує свою локальну адресу. Для того щоб зменшити кількість посилаються запитів ARP, кожен пристрій в мережі, що використовує протокол ARP, має мати спеціальну буферну пам'ять. У ній зберігаються пари адрес (IP-адреса, фізичну адресу) пристроїв в мережі. Всякий раз, коли пристрій отримує ARP-відповідь, воно зберігає в буферній пам'яті відповідну пару. Якщо адреса є в списку пар, то немає необхідності надсилати ARP-запит. Ця буферна пам'ять називається ARP-таблицею. У ARP-таблиці можуть міститися як статичні, так і динамічні записи. Динамічні записи додаються і видаляються автоматично, статичні заносяться вручну. Так як більшість пристроїв в мережі підтримує динамічне дозвіл адрес, то адміністратору, як правило, немає

необхідності вручну вказувати записи протоколу ARP в таблиці адрес.

Кожен запис в ARP-таблиці має свій час життя. Політики очищення ARP-таблиці продиктовані використовуваною операційною системою. При додаванні запису для неї активується таймер. Повідомлення протоколу ARP при передачі по мережі инкапсулируются в поле даних кадру. Вони не містять IP-заголовка. На відміну від повідомлень більшості протоколів, повідомлення ARP не мають фіксованого формату заголовка. Це пояснюється тим, що протокол був розроблений таким чином, щоб він був застосуємо для дозволу адрес в різних мережах. [3] ARP-запити і відповіді використовують один і той же формат пакета. Так як локальні адреси можуть у різних типах мереж мати різну довжину, то формат пакета протоколу ARP залежить від типу мережі. На рис. 4.26 показана структура пакету запитів і відповідей. [4]

Рис. 4.26 Формат пакета ARP

- Network Type - тип канального протоколу для Ethernet - 1.
- Protocol - протокол мережевого рівня
- HAL - довжина канального адреси
- PAL - довжина мережевого адреси
- Operation - тип операції (1 - запит, 2 - відповідь) вузол, що відправляє ARP-запит, заповнює в пакеті всі поля, крім поля шуканого локальної адреси. Значення цього поля заповнюється вузлом, упізнав свою IP-адресу.

Протокол ICMP

Протокол ICMP призначений для передачі керуючих і діагностичних повідомлень. З його допомогою передаються повідомлення про помилки, а також про виникнення ситуацій, що вимагають підвищеної уваги. Протокол відноситься до мережевого рівня моделі TCP / IP. Повідомлення ICMP генеруються і обробляються протоколами мережевого (IP) і більш високих рівнів (TCP або UDP). При появі деяких ICMP-повідомлень генеруються повідомлення про помилки, які передаються призначеним для користувача процесів. ICMP-повідомлення передаються всередині IP-дейтаграм (рис. 4.27). [2]

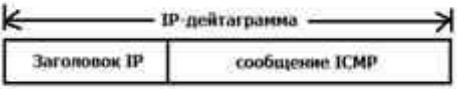

Рис. 5.27 Інкапсуляція ICMP-повідомлень в IP-дейтаграми

Формат ICMP-повідомлення показаний на Рис. 5.28. Тема ICMP включає 8 байт, але тільки перші 4 байта однакові для всіх повідомлень, інші поля заголовка і тіла повідомлення визначаються типом повідомлення.

Рис. 5.28 Формат ICMP-повідомлень

Поле контрольної суми охоплює ICMP-повідомлення цілком.

Тип повідомлення визначається значенням поля "Тип" заголовка. Деякі типи ICMP-повідомлень мають внутрішню деталізацію (код), при цьому конкретний вид повідомлення визначається як типом, так і кодом повідомлення. Детальніше з видами типів і кодів ICMP-повідомлень можна ознайомитися в спе-

цифікації протоколу ICMP RFC 792. [Електронний ресурс]. URL: http://tools.ietf.org/html/rfc792.

Програма ping

Програма ping була розроблена для перевірки доступності віддаленого вузла. Програма посилає ICMP-ехо-запит на вузол і очікує повернення ICMP-луна-відгуку. Програма ping є зазвичай першим діагностичним засобом, за допомогою якого починається ідентифікація будь-якої проблеми в мережах. Крім доступності, за допомогою ping можна оцінити час повернення пакета від вузла, що дає уявлення про те, "наскільки далеко" знаходиться вузол. Крім цього, Ping має опції запису маршруту і тимчасової мітки. Повідомлення луна-запиту і луна-відгуку мають один формат (рис 4.29). [2]

Рис. 5.29 Формат пакета ICMP-повідомлення

• Тип - тип пакета 8 - запит луни 0 - відповідь на запит луни

• Код - розшифровка призначення пакета всередині типу (в даному випадку 0) • Контрольна сума обчислюється для всього пакета

• Ідентифікатор - ідентифікатор гілки повідомлень

• Послідовний номер - номер пакета в потоці [3]

Так само, як у випадку інших ICMP-запитів, в луна-відгуку повинні міститися поля ідентифікатора і номера послідовності. Крім того, будь-які додаткові дані, надіслані комп'ютером, повинні бути відображені луною. В поле ідентифікатора ICMP повідомлення встановлюється ідентифікатор процесу, що відправляє запит. Це дозволяє програмі ping ідентифікувати повернувся відповідь, якщо на одному і тому ж хості в один і той же час запущено кілька програм ping.

Номер послідовності починається з 0 і инкрементируется кожен раз, коли посилається наступний ехо-запит. Висновок програми показаний на Рис. 5.30. Перший рядок виводу містить

IP-адресу хоста призначення, навіть якщо було вказано ім'я. Тому програма ping часто використовується для визначення IP-адреси віддаленого вузла. [2]

```
C:\>ping yandex.ru

Обмен пакетами с yandex.ru [93.158.134.11] с 32 байтами данных:
Ответ от 93.158.134.11: число байт=32 время=48мс TTL=52
Ответ от 93.158.134.11: число байт=32 время=27мс TTL=52
Ответ от 93.158.134.11: число байт=32 время=29мс TTL=52
Ответ от 93.158.134.11: число байт=32 время=29мс TTL=51

Статистика Ping для 93.158.134.11:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 27мсек, Максимальное = 48 мсек, Среднее = 33 мсек
```

Рис. 5.30 Висновок програми ping програма tracert

Програма tracert

Дозволяє подивитися маршрут, по якому рухаються IP-дейтаграми від одного хоста до іншого. Програма tracert не вимагає ніяких спеціальних серверних додатків. В її роботі використовуються стандартні функції протоколів ICMP і IP. Для розуміння роботи програми слід згадати порядок обробки поля TTL в заголовку IP-дейтаграми.

Кожен маршрутизатор, що обробляє дейтаграму, зменшує значення поля TTL в її заголовку на одиницю. При отриманні дейтаграми з TTL рівним 1, маршрутизатор знищує її і посилає хосту, який її відправив, ICMP-повідомлення "час минув". При цьому дейтаграмма, що містить це ICMP-повідомлення, має в якості адреси джерела IP-адреса маршрутизатора. Це і використовується в програмі tracert. На хост призначення відправляється IP-дейтаграмма, в якій поле TTL, встановлено в одиницю. Перший маршрутизатор на шляху дейтаграми, знищує її (так як TTL дорівнює 1) і відправляє ICMP-повідомлення про закінчення часу.

Таким чином, визначається перший маршрутизатор в маршруті. Потім tracert відправляє дейтаграмму з полем TTL рівним 2, що дозволяє отримати IP-адресу другого маршрутизатора. Аналогічні дії тривають до тих пір, поки дейтаграмма не

досягне хоста призначення. При отриманні відповіді від цього вузла процес трасування вважається завершеним.

Приклад виведення програми показаний на Рис. 5.31.

Рис. 5.31 Висновок програми tracert

Перший рядок, без номера містить ім'я і IP адреса пункту призначення і вказує на те, що величина TTL не може бути більше 30. Наступні рядки виведення починаються з роздруківки значення TTL (1, 2, 3 і т.д.) і містять ім'я (IP-адреса) хоста або маршрутизатора і час повернення ICMP-повідомлення. Для кожного значення TTL відправляється 3 дейтаграми. Для кожного повернутого ICMP-повідомлення розраховується і друкується час повернення. Якщо відповідь на дейтаграмму ми отримали протягом п'яти секунд, друкується зірочка, після чого вирушає наступна дейтаграмма. [2] Виконання роботи: 1. Побудова топології мережі В кінці вступної лабораторної роботи ми створили таку топологію мережі, що складається з кінцевих вузлів (PC), комутаторів і маршрутизатора (Рис. 5.32):

Виконання роботи:

1. Побудова топології мережі В кінці вступної лабораторної роботи ми створили таку топологію мережі, що складається з кінцевих вузлів (PC), комутаторів і маршрутизатора (Рис. 5.32):

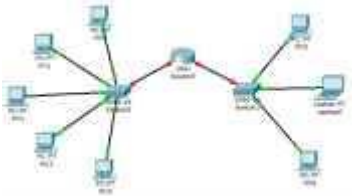

Рис. 5.32 Тестова топологія мережі

Маршрутизатор Router0 має два інтерфейси і з'єднує дві підмережі. Зробимо налаштування кінцевих вузлів. 2. Налаштування кінцевих вузлів На пристроях PC0-PC4 встановимо задані IP-адреси і маски підмережі (таблиця 4.2). IP-адреса шлюзу для всіх вузлів - 192.168.3.1. IP-адреса DNS-сервера вказувати необов'язково, тому що в даній роботі він використовуватися не буде.

Таблиця 4.2

Хост	IP-адрес	Маска підмережі
PC0	192.168.3.3	255.255.255.0
PC1	192.168.3.4	255.255.255.0
PC2	192.168.3.5	255.255.255.0
PC3	192.168.3.6	255.255.255.0
PC4	192.168.3.7	255.255.255.0

На пристроях PC5, Laptop0, PC6 встановимо задані IP-адреси і маски підмережі (таблиця 4.3). IP-адреса шлюзу для всіх вузлів - 192.168.5.1. IP-адреса DNS-сервера вказувати необов'язково.

Таблиця 4.3

Хост	IP-адрес	Маска підмережі
PC5	192.168.5.3	255.255.255.0
Laptop0	192.168.5.4	255.255.255.0
PC6	192.168.5.5	255.255.255.0

Кожен вузол перейменуємо його ж IP-адресою, вийде наступне (Рис. 5.33):

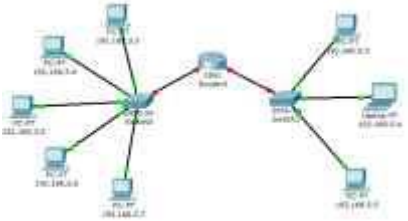

Рис. 5.33 Вид робочої області

3. Налаштування маршрутизатора

Під час налаштування кінцевих вузлів вже згадувалося про те, що маршрутизатор в даній топології мережі має два інтерфейси. Зробимо налаштування інтерфейсу FastEthernet0 / 0:

1) Один клік по влаштуванню (маршрутизатора);

2) Вибираємо вкладку "Config";

3) Знаходимо інтерфейс FastEthernet0 / 0, задаємо потрібний IP-адреса і маску підмережі (Рис. 5.34).

Важливо: інтерфейс маршрутизатора, за замовчуванням, відключений; необхідно його включити, клікнувши мишкою поруч з "On".

Рис. 5.34 Налаштування інтерфейсу маршрутизатора

4) Закриваємо вікно, дивимося на всю топологію мережі. Зелені індикатори стану на лінії зв'язку між Router0 і Switch0 сигналізують, що інтерфейс підключений правильно (Рис. 5.35).

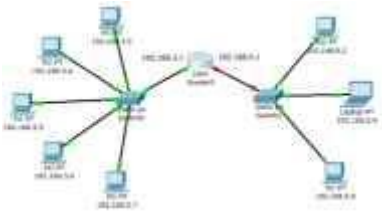

Рис. 5.35 Вид робочої області

Аналогічно проводимо настройку інтерфейсу FastEthernet0/1 (Рис. 5.36).

Рис. 5.36 Налаштування інтерфейсу маршрутизатора

Зробити написи до інтерфейсів маршрутизатора, можна за допомогою інструменту Place Note на панелі Common Tools Небхідно клікнути на інструмент, потім зробити клік в потрібному місці на робочій області

4. Режим симуляції Cisco Packet Tracer

Переконайтеся, що ви перебуваєте в режимі симуляції. Для цього клікніть на іконку симуляції в правому нижньому кутку робочої області симулятора.

Відкриється вікно подій, в якому ви побачите список подій, керуючі кнопки, задані фільтри (Рис. 5.37). За замовчуванням, фільтруються, тобто будуть відображатися, пакети всіх можливих протоколів, необхідно поправити і обмежити цей список до досліджуваних протоколів.

Кнопки:• Back – назад

• Auto Capture / Play - автоматичний захват пакетів від джерела до приймача і назад

• Capture / Forward - захоплення пакетів тільки від одного пристрою до іншого

Рис. 5.37 Вікно подій режиму симуляції

У даній лабораторній роботі нас цікавлять пакети двох типів ARP і ICMP.

Отже, потрібно поставити фільтр тільки на повідомлення заданого типу (Рис. 5.38):

1) Натискаємо на кнопку "Edit Filters"

2) Знімаємо мітку з "Show All / None"

3) Вибираємо ARP і ICMP

Рис. 5.38 Додавання фільтрів на протоколи ARP і ICMP

4) Переконаємося, що задані протоколи для фільтрації призначені (Рис. 5.39)

Рис. 5.39 Вікно подій режиму симуляції

1. Перевірка роботи мережі в режимі симуляції

Відправимо тестовий ping-запит з кінцевого вузла с IP-адресою 192.168.3.3 на хост з IP-адресою 192.168.3.5.

Важливо: обидва вузла знаходяться в межах одного сегмента мережі

1) Один клік по вибраному пристрою (Рис. 5.40)

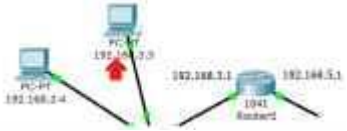

Рис. 5.40 Вибір вузла 192.168.3.3

1) Вибираємо вкладку Desktop, в якій містяться симулятори деяких програм, доступних на комп'ютері (див. Рис. 3.4).

2) Вибираємо "Command Prompt", програму, яка імітує командний рядок комп'ютера.

3) За допомогою утиліти ping відправляємо ping-запит (Рис. 5.41). (Не забудьте натиснути Enter).

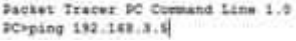

Рис. 5.41 Командний рядок вузла 192.168.3.3

На пристрої-джерелі формуються два пакети протоколу ARP і ICMP (Рис. 5.42). ARP-запит виникає завжди, коли хост намагається зв'язатися з іншим хостом.

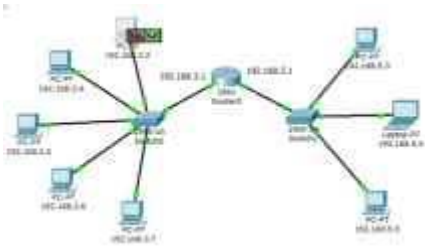

Рис. 5.42 Вид робочої області

Натискаємо на кнопку "Auto Capture / play" або "Capture / Forward", остання дозволить вам управляти рухом пакетів від пристрою до пристрою самим. Бачимо, що першим вирушає пакет протоколу ARP, так як ARP-таблиця хоста 192.168.3.3 порожня, і він ще «не знає», кому відправляти ping-запит. Зробіть один клік по самому пакету (конверту), ознайомтеся, які рівні моделі OSI задіяні. Перейдіть до вкладки "Inbound PDU Details", яка містить структуру пакета (Рис. 5.43).

Рис. 5.43 Формат пакету ARP-запиту

Вузол 192.168.3.3 побудував запит і посилає його широкомовним повідомленням всім хостам підмережі. Крім IP-адреси призначення, запит містить IP-адресу і MAC-адреса відправника, щоб прийомна сторона могла відповісти.

При перегляді проходження пакетів переконайтеся, що на ARP-запит відповість тільки хост 192.168.3.5. Кожен хост в підмережі отримує запит і перевіряє на відповідність свій IP-

адресу. Якщо він не співпадає з адресою в запиті, то запит ігнорується (Рис. 5.44).

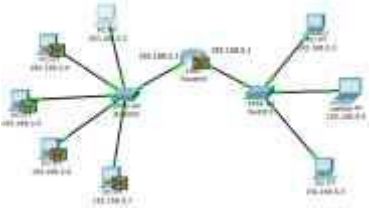

Рис. 5.44 Вид робочої області

Подивіться вміст пакета ARP-відповіді, який прийшов на хост 192.168.3.3 (Рис. 5.45).

Рис. 5.45 Формат пакету ARP-відповіді

Вузол 192.168.3.5. послав ARP-відповідь безпосередньо відправнику, використовуючи його MAC-адресу, із зазначенням власного MAC-адреси в поле "Target MAC".

Далі вирушає ICMP-повідомлення ping-запиту. Подивіться вміст пакету, зробивши клік по пакету (конверту) (Рис. 5.46).

Рис. 5.46 Формат пакету ICMP-exo-запиту

Фізичні адреси вузлів відомі. IP-адреса джерела - 192.168.3.3. IP-адреса призначення - 192.168.3.5. Тип ICMP-повідомлення - 8 (луна-запит).

Запит оформлюється на хост 192.168.3.5 через комутатор (Рис. 5.47).

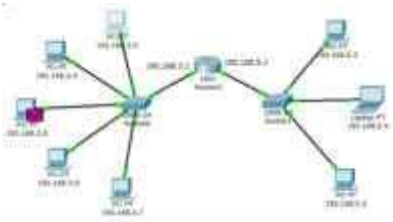

Рис. 5.47 Вид робочої області

Подивіться вміст пакета ping-відповіді, який прийшов на хост 192.168.3.3 (Рис. 5.48).

Рис. 5.48 Формат пакету ICMP-exo-відповіді

IP-адреса джерела - 192.168.3.5. IP-адреса призначення - 192.168.3.3. Тип ICMP-повідомлення - 0 (луна-відповідь).

Подивіться ping-відповідь в командному рядку хоста 192.168.3.3 (Рис. 5.49).

Рис. 5.49 Висновок програми ping

У вікні подій так само вказані маршрути запиту ARP і ICMP: через які пристрої пройшли пакети (Рис. 5.50).

Рис. 5.50 Вікно подій режиму симуляції

Видалити сценарій симуляції можна за допомогою кнопки "Reset Simulation" або скористатися кнопкою "Delete" в області User Created Packet Window.

Тепер ARP-таблиці хостів 192.168.3.3 і 192.168.3.5 не пустили, в них міститься одна запис. Щоб переглянути вміст ARP-таблиці, потрібно виконати команду

"Arp -a" в командному рядку.

Вміст ARP-таблиці вузла 192.168.3.3 (Рис. 5.51):

```
PC>arp -a
  Internet Address      Physical Address      Type
  192.168.3.5           0002.1790.c065        dynamic
```

Рис. 5.51 ARP-таблиця вузла 192.168.3.3 в командному рядку

Можна скористатися іншим способом: натиснути на кнопку «Inspect»  , натиснути на вибраний пристрій, вибрати «ARP table» і переглянути записи ARP-таблиці вузла (Рис. 5.52).

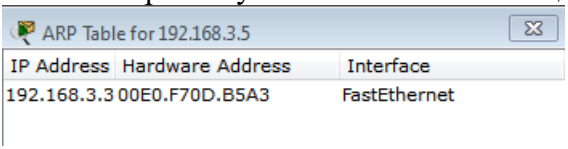

Рис. 5.52 ARP-таблиця вузла 192.168.3.3, показана за допомогою інструменту «Inspect»

Якщо знову поставити ping-запит на хост 192.168.3.5, то відразу буде сформований тільки один пакет ICMP-повідомлення, тому що в ARP-таблиці комп'ютера-джерела вже зберігається відповідний локальний адресу.

Спробуйте відправити ping-запит знову.

Щоб видалити всі записи ARP-таблиці, слід скористатися командою "arp -d".

1. Здійснення ping-запиту в зовнішню мережу

Відправимо тестовий ping-запит з кінцевого вузла с IP-адресою 192.168.3.4 на хост з IP-адресою 192.168.5.5.

Важливо: один вузол намагається передати пакет іншому вузлу, що знаходиться з ним в різних мережах.

У пункті 5 лабораторної роботи було розглянуто випадок посилки ARP-запиту всередині локальної мережі. Протокол ARP в цьому випадку визначав безпосередньо MAC-адреса вузла-приймача запиту. Тепер розглянемо ситуацію, коли вузол-джерело і вузол-приймач знаходяться в різних мережах. Протокол ARP працює в межах сегмента мережі, тому в даному випадку він буде використовуватися для визначення MAC-адреси маршрутизатора. Таким чином, пакет буде переданий маршрутизатора для подальшої ретрансляції.

Відкриваємо "Command Promt", що імітує командний рядок, на комп'ютері 192.168.3.4 і посилаємо на хост 192.168.5.5. ping-запит (Рис. 5.53).

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.5.5
```

Рис. 5.53 Командний рядок вузла 192.168.3.4

В цьому випадку ініціюється ARP-запит маршрутизатора, який пересилає пакети в мережу призначення. На вузлі-джерелі формуються два пакети протоколу ARP і ICMP (Рис. 5.54).

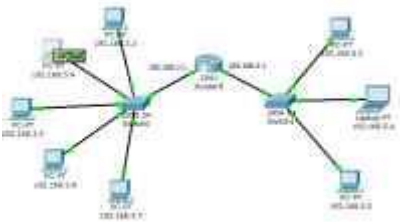

Рис. 5.54 Вид робочої області

Формат пакета ARP-запиту містить ті ж відомості, що і для вирішення локальної адреси пристрою, і розсилається широкомовно всіх вузлів підмережі (Рис. 5.55)

Рис. 5.55 Формат пакету ARP-запиту

Всі вузли ігнорують пакет, крім маршрутизатора, якому цей пакет призначався (Рис. 5.56).

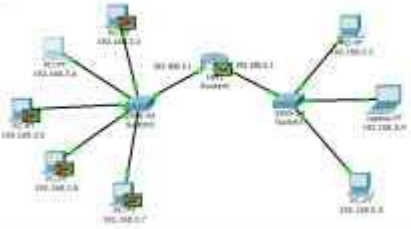

Рис. 5.56 Вид робочої області

Маршрутизатор формує ARP-відповідь, вказуючи свою фізичну адресу, і відправляє його вузлу 192.168.3.4 (Рис. 5.57).

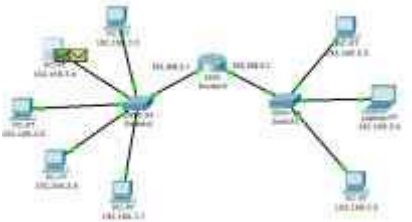

Рис. 5.57 Вид робочої області

Після отримання ARP-відповіді хост 192.168.3.4 посилає ICMP-повідомлення ping-запиту через маршрутизатор в мережу призначення.

Подивіться вміст пакету, зробивши клік по пакету (конверту) (Рис. 5.58).

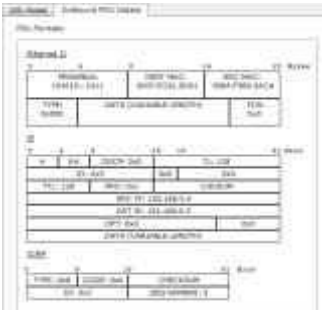

Рис. 5.58 Формат пакета ICMP-луна-запиту

IP-адреса джерела - 192.168.3.4. IP-адреса призначення - 192.168.5.5. Тип ICMP-повідомлення - 8 (луна-запит).

Коли запит приходить в мережу призначення, то маршрутизатор визначає MAC-адресу одержувача, якщо такого немає в ARP-таблиці маршрутизатора. Таким чином, знову вирішується завдання дозволу локального адреси (Рис. 5.59).

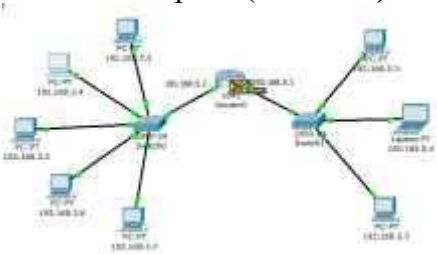

Рис. 5.59 Вид робочої області

Маршрутизатор змушений спершу дізнатися фізичну адресу одержувача, перш ніж він зможе відправити ping-запит за призначенням, тому пакет з ping-запитом, що прийшов на маршрутизатор, відхилений.

Новий ARP-запит відправляється широкомовним повідомленням від маршрутизатора, містить його IP-адресу і MAC-адреса (Рис. 5.60). IP-адреса призначення - вузол 192.168.5.5.

Рис. 5.60 Формат пакета ARP-запиту

Вузли підмережі, яким пакет не призначений, його ігнорують (Рис. 5.61).

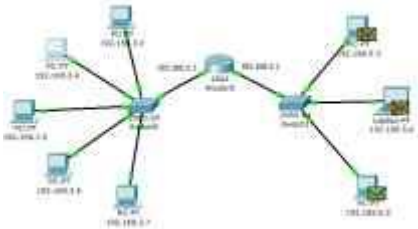

Рис. 5.61 Вид робочої області

Вузол 192.168.5.5. формує ARP-відповідь і відправляє його назад маршрутизатора (Рис. 5.62), вказавши свій MAC-адреса, про що свідчить вміст пакету (Рис. 5.63).

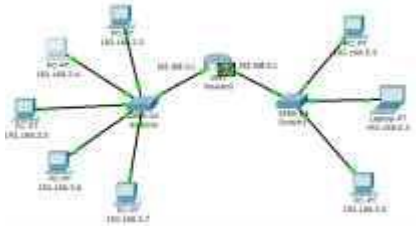

Рис. 5.62 Вид робочої області

Після того, як маршрутизатор визначив MAC-адреса одержувача входить ping-запиту, він посилає ICMP-відповідь маршрутизатора хоста відправника. (В даному випадку це той же маршрутизатор Router0).

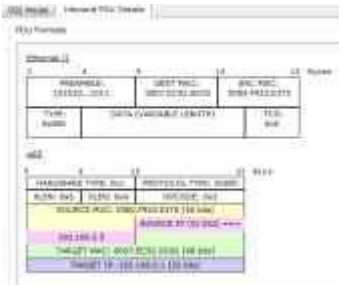

Рис. 5.63 Формат пакета ARP-відповіді

Вузол 192.168.3.4. знову намагається відправити ping-запит в зовнішню мережу вузла 192.168.5.5. Його маршрут повинен лежати через комутатор Switch0, маршрутизатор Router0, комутатор Switch1 і досягти вузла призначення (Рис. 5.64). Прослідкуйте маршрут пакета самостійно.

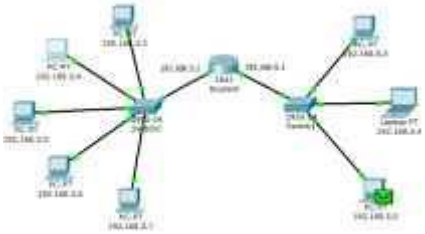

Рис. 5.64 Вид робочої області

Вузол формує ping-відповідь, який відправляється назад вузлу 192.168.3.4 (Рис. 5.65).

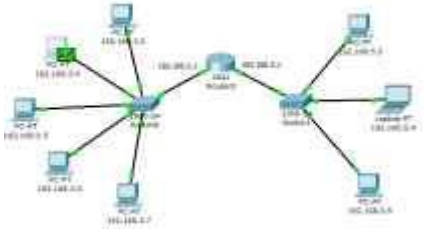

Рис. 5.65 Вид робочої області

Подивіться вміст пакета ping-відповіді, який прийшов на хост 192.168.3.4 (Рис. 5.66).

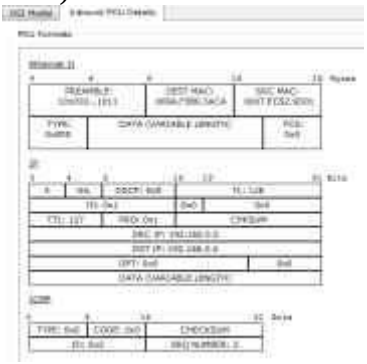

Рис. 5.66 Формат пакета ICMP-exo-відповіді

IP-адреса джерела - 192.168.5.5. IP-адреса призначення - 192.168.3.4. Тип ICMP-повідомлення - 0 (луна-відповідь).

Подивіться ping-відповідь в командному рядку хоста 192.168.3.4 (Рис. 5.67).

```
PC>ping 192.168.5.5

Pinging 192.168.5.5 with 32 bytes of data:

Reply from 192.168.5.5: bytes=32 time=8ms TTL=127
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127
Reply from 192.168.5.5: bytes=32 time=8ms TTL=127

Ping statistics for 192.168.5.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 8ms, Average = 8ms
```

Рис. 5.67 Висновок програми ping

Маршрут пакета можна подивитися за допомогою команди tracert. Виконаємо цю команду, наприклад, в командному рядку комп'ютера 192.168.3.5 (Рис. 5.68):

```
PC>tracert 192.168.5.4

Tracing route to 192.168.5.4 over a maximum of 30 hops:

  1    40 ms     40 ms     40 ms     192.168.3.1
  2    80 ms     70 ms     50 ms     192.168.5.4

Trace complete.
```

Рис. 5.68 Висновок програми tracert

На шляху пакета до хоста 192.168.5.4 один проміжний маршрутизатор.

1. Здійснення ping-запиту на неіснуючий хост

Відправимо ping-запит на неіснуючу адресу в мережу 192.168.5.0/24.

Відкриємо програму "Command Promt" на вузлі 192.168.3.7 і спробуємо відправити ping-запит на неіснуючий хост з IP-адресою 192.168.5.6 (Рис. 5.69).

```
PC>ping 192.168.5.6

Pinging 192.168.5.6 with 32 bytes of data:
```

Рис. 5.69 Командний рядок вузла 192.168.3.7

ARP-таблиця на вузлі-джерелі не містить відповідного запису про MAC-адресу вузла 192.168.5.6, тому формується ARP-запит (Рис. 5.70).

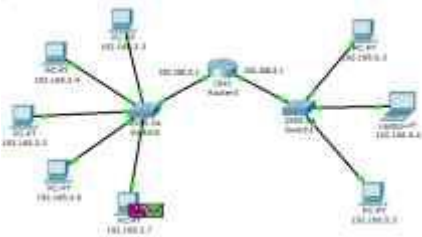

Рис. 5.70 Вид робочої області

Всі вузли ігнорують пакет, крім маршрутизатора, якому цей пакет призначався (Рис. 5.71).

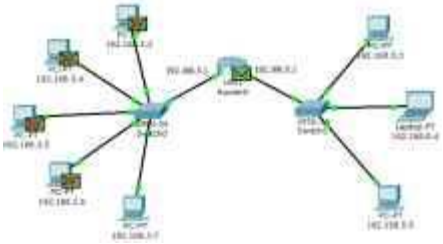

Рис. 5.71 Вид робочої області

Вузол 192.168.3.7 отримує ARP-відповідь з MAC-адресою маршрутизатора. Тепер, знаючи його апаратну адресу, хост відправляє ping-запит на вузол 192.168.5.6 (Рис. 5.72).

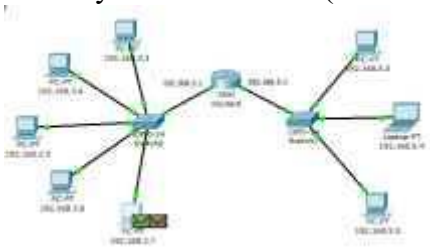

Рис. 5.72 Вид робочої області

Маршрутизатор прийшов пакет знищує, тому що не може його перенаправити на вказану адресу, тому що відповідного MAC-адреси він «не знає». У зв'язку з цим маршрутизатор формує ARP-запит за адресою 192.168.5.6 (Рис. 5.73).

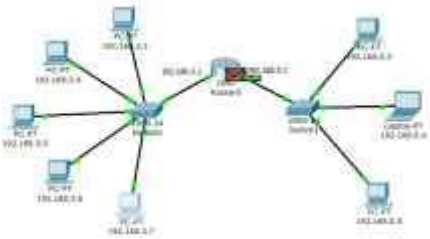

Рис. 5.73 Вид робочої області

Всі вузли підмережі ігнорують пакет, тому що IP-адреса в запиті не відповідає їх власним (Рис. 5.74). Маршрутизатор жодного відповіді ні від кого не отримуєлабораторный компьютерный сеть

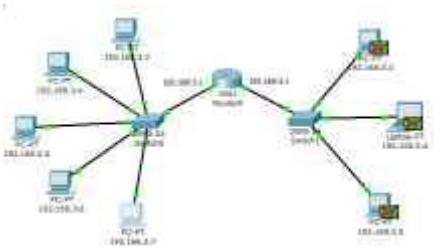

Рис. 5.74 Вид робочої області

Процедура проходження пакетів повторюється протягом всього сценарію симуляції: маршрутизатор як і раніше «не знає» MAC-адреса зазначеного в ping-запиті IP-адреси 192.168.5.6 і продовжує розсилати ARP-запити. Жоден з вузлів підмережі на ці запити не реагує. Не отримавши відповіді, маршрутизатор і сам «мовчить», ніяк не повідомляючи про помилку хост-джерело ping-запиту.

Примітка: насправді в даному випадку маршрутизатора слід відправити ICMP-повідомлення «хост недосяжний»: повідомлення типу 3 з кодом 1. Однак проведений експеримент з теорією розійшовся.

Подивимося відповідь на ping-запит в командному рядку вузла-джерела 192.168.3.7: «перевищено час очікування» (Рис. 5.75).

```
PC>ping 192.168.5.6

Pinging 192.168.5.6 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.5.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рис. 5.75 Висновок програми ping

Спробуємо відправити ping-запит, який містить IP-адресу вузла, в мережу, на яку немає маршруту.

Відкриємо програму "Command Promt" на вузлі 192.168.3.6 і спробуємо відправити ping-запит на неіснуючий хост з IP-адресою 192.168.6.6 (Рис. 5.76).

```
PC>ping 192.168.6.6

Pinging 192.168.6.6 with 32 bytes of data:
```

Рис. 5.76 Командний рядок вузла 192.168.3.6

Так як ARP-таблиця вузла-джерела відповідного запису не має, формується ARP-запит на заданий вузол з IP-адресою 192.168.6.6 (Рис. 5.77).

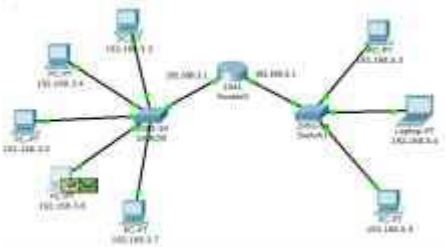

Рис. 5.77 Вид робочої області

Всі вузли ігнорують пакет, крім маршрутизатора, якому цей пакет призначався (Рис. 5.78).

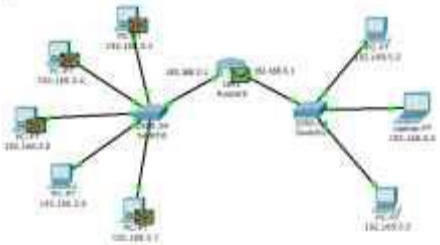

Рис. 5.78 Вид робочої області

Вузол 192.168.3.6 отримує ARP-відповідь з MAC-адресою маршрутизатора. Тепер, знаючи його апаратну адресу, хост відправляє ping-запит (Рис. 5.79).

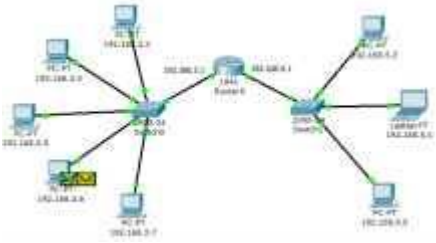

Рис. 5.79 Вид робочої області

Коли ping-запит потрапляє на маршрутизатор, той не може його перенаправити не на якийсь зі своїх інтерфейсів, тому що IP-адреси його інтерфейсів не збігаються з тим адресою, яка вказана в ping-запиті. Відповідно, цей пакет знищується і формується нове ICMP-повідомлення (Рис. 5.80).

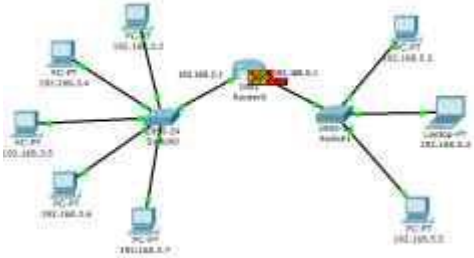

Рис. 5.80 Вид робочої області

Подивимося вміст пакета, сформованого маршрутизатором (Рис. 5.81).

Рис. 5.81 Формат пакета ICMP «хост недосяжний»

IP-адреса джерела - 192.168.3.1. IP-адреса призначення - 192.168.3.6. Тип ICMP-повідомлення - 3 з кодом 1, що означає «хост недосяжний». Цей пакет приходить на вузол 192.168.3.6.

Результат ping-запиту в командному рядку вузла 192.168.3.6: «хост призначення недосяжний» (Рис. 5.82).

```
PC>ping 192.168.6.6

Pinging 192.168.6.6 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 192.168.6.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Рис. 5.82 Висновок програми ping

Таким чином, маршрутизатор «відповів» на ping-запит, для якого у нього не було відповідного маршруту, новим ICMP-повідомленням «хост недосяжний».

Примітка: чи коректно відреагував маршрутизатор в даній ситуації, відправивши на хост-джерело ping-запиту ICMP-повідомлення «хост недосяжний»? Щоб відповісти на це питання, необхідно звернутися до специфікації протоколу ICMP RFC 792 і ознайомиться з іншими типами ICMP-повідомлень.

СПИСОК ЛІТЕРАТУРИ

1. М.А.Плоткін. Лекції з курсу «Мережі зв'язку та системи комутації». Тема 1 Комп'ютерні мережі. Основні визначення. Розділ «Комунікаційні пристрої і структуризація комп'ютерних мереж».
2. В.Г.Оліфер і ін. Комп'ютерні мережі. 4-е видання, ПІТЕР, 2010р. Глава 2 Загальні принципи побудови мереж.
3. Cisco Network Academy (netacad.com)
4. Джо Хабракена. Як працювати з маршрутизаторами Cisco. Пер. з англ. - М .: ДМК Пресс. 2005.
5. Пакет Cisco Packet Tracer, Tutorials (Getting Started, Logical Workspace, Configuring Devices, Realtime and Simulation Modes).

Навчальне видання

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт
з дисципліни «Телекомунікаційні та інформаційні мережі»
для студентів спеціальності
172 " Телекомунікації та радіотехніка"
усіх форм навчання

Відповідальний за випуск А.С. Опанасюк
Редактор Н.З. Клочко
Комп'ютерне верстання К О. Д'яченко

Підп. до друку 11.06.2017, поз.
Формат 60х84/16. Ум. друк. арк. 2,09. Обл.-вид.арк. 1,62. Тираж 60 пр. Зам. №
Собівартість вид. грн.. к.

Видавець і виготовлювач
Сумський державний університет,
Вул. Римського – Корсакова, 2, м. Суми, 40007
Свідоцтво суб'єкта видавничої справи ДК № 3062 від 17.12.2007.