# Тема9. Визначення адрес

Як хости, так і маршрутизатори створюють таблиці маршрутизації для забезпечення можливості надсилати та отримувати дані через мережі. Тож як ця інформація заноситься у таблиці маршрутизації? Як адміністратор мережі, ви можете внести ці MAC- та IP-адреси вручну. Але це займе багато часу, та існує значна ймовірність зробити якісь помилки. А чи не думаєте Ви, що існує спосіб, в який хости і маршрутизатори могли б автоматично зробити це самі? Звичайно, Ви праві! Але, навіть незважаючи на автоматичне створення, Вам все одно слід розуміти, як це робиться на випадок, якщо доведеться усувати проблеми, або, що ще гірше, мережа буде атакована.

**Мета розділу**: Пояснити, як ARP і ND дозволяють спілкуватися в мережі.

| Назва теми | Мета теми |
|---|---|
| **9.1. MAC- та IP-адреси** | Порівняти ролі MAC-адрес та IP-адрес. |
| **9.2. ARP** | Описати призначення ARP (Address Resolution Protocol). |
| **9.3. Виявлення сусіда** | Описати процес виявлення сусіда в IPv6. |

## 9.1. MAC- та IP-адреси

### 9.1.1. Пункт призначення в тій же мережі

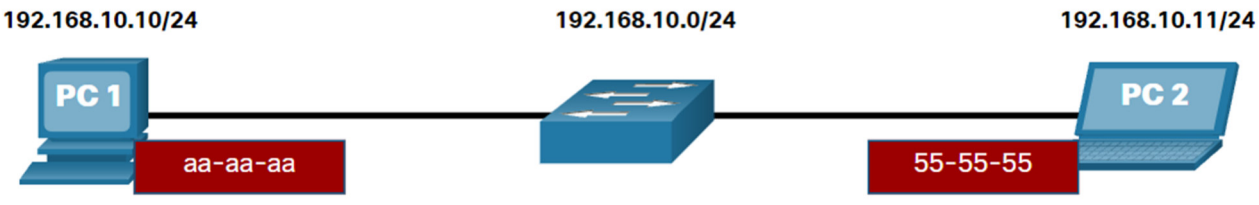
Іноді хосту потрібно відправити повідомлення, але він знає тільки IP-адресу пристрою призначення. Хосту необхідно знати MAC-адресу цього пристрою, але як її можна визначити? Саме в цьому випадку визначення адреси має вирішальне значення.

Існує дві основні адреси, призначені пристрою в локальній мережі Ethernet:

- **Фізична адреса (MAC-адреса)** – використовується для комунікації між мережними картами (NIC) в одній мережі Ethernet.
- **Логічна адреса (IP-адреса)** – використовується для відправки пакета від джерела до кінцевого пункту призначення. IP-адреса призначення може бути в тій самій IP-мережі, що й джерело, або у віддаленій мережі.

Фізичні адреси Рівня 2 (тобто, MAC-адреси Ethernet) використовуються для передачі кадра канального рівня з інкапсульованим IP-пакетом від однієї мережної карти до іншої у тій самій мережі. Якщо IP-адреса призначення знаходиться в тій самій мережі, MAC-адресою призначення буде адреса пристрою призначення.

Розглянемо приклад з використанням спрощеного подання MAC-адрес.




| MAC-адреса призначення | MAC-адреса джерела | IPv4-адреса джерела | IPv4-адреса призначення |
|---|---|---|---|
| 55-55-55 | aa-aa-aa | 192.168.10.10 | 192.168.10.11 |

У цьому прикладі PC1 хоче відправити пакет до PC2. На рисунку показано MAC-адреси призначення та джерела Рівня 2, а також IPv4-адресацію Рівня 3, яка буде включена в пакет, відправлений з PC1.

Ethernet-кадр Рівня 2 містить:

- **MAC-адресу призначення** – це спрощена MAC-адреса PC2, 55-55-55.
- **MAC-адресу джерела** – це спрощена MAC-адреса Ethernet NIC на PC1, aa-aa-aa.

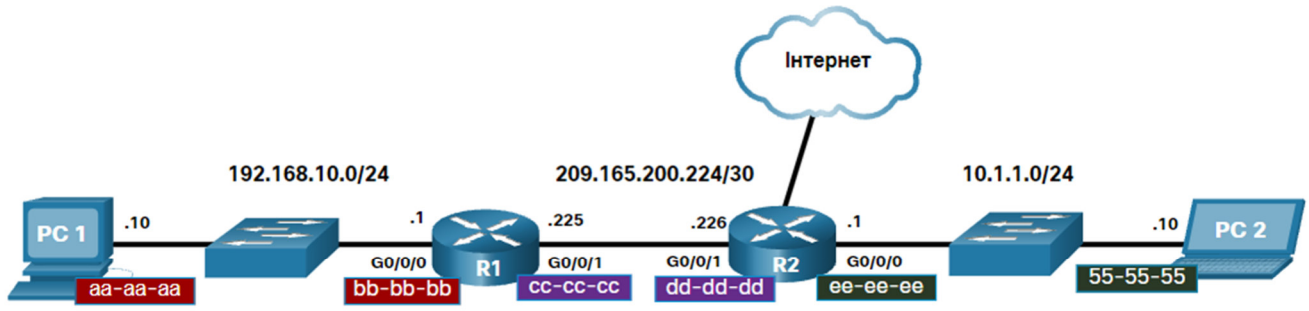
IP-пакет Рівня 3 містить:

- **IPv4-адресу джерела** – це IPv4-адреса PC1, 192.168.10.10.
- **IPv4-адресу призначення** – це IPv4-адреса PC2, 192.168.10.11.

## 9.1.2. **Пункт призначення у віддаленій мережі**

Якщо IP-адреса (IPv4 чи IPv6) призначення знаходиться у віддаленій мережі, MAC-адресою призначення буде адреса шлюзу за замовчуванням (тобто інтерфейс маршрутизатора).

Розглянемо приклад з використанням спрощеного подання MAC-адреси.

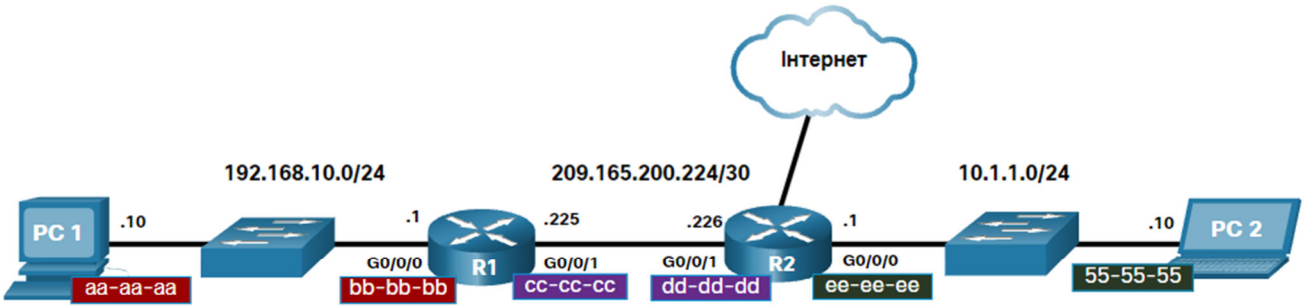



| MAC-адреса призначення | MAC-адреса джерела | IPv4-адреса джерела | IPv4-адреса призначення |
|---|---|---|---|
| bb-bb-bb | aa-aa-aa | 192.168.10.10 | 10.1.1.10 |

У цьому прикладі PC1 хоче відправити пакет до PC2. PC2 знаходиться у віддаленій мережі. Оскільки IPv4-адреса призначення не в одній локальній мережі з PC1, MAC-адресою призначення є адреса шлюзу за замовчуванням на маршрутизаторі.

Маршрутизатори досліджують IPv4-адресу призначення, щоб визначити найкращий шлях для пересилання IPv4-пакета. Коли маршрутизатор отримує кадр Ethernet, він деінкапсулює інформацію Рівня 2. Використовуючи IPv4-адресу призначення, маршрутизатор визначає пристрій наступного переходу, а потім інкапсулює IPv4-пакет у новий кадр канального рівня для вихідного інтерфейсу.

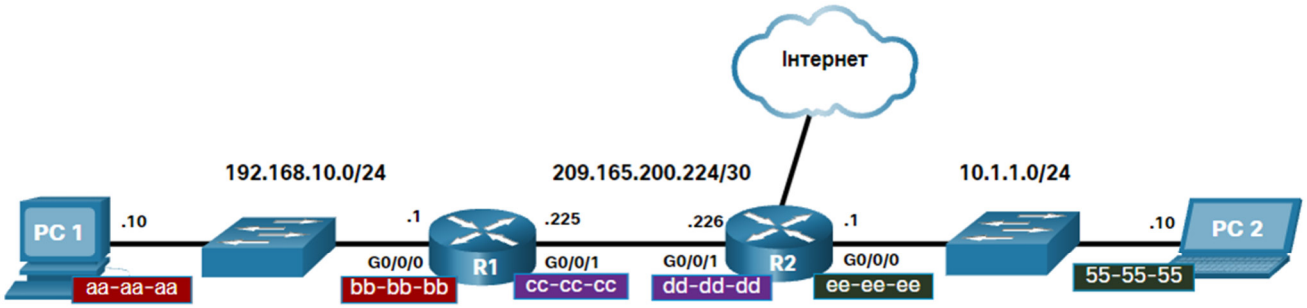
У нашому прикладі, як показано на рисунку, R1 буде інкапсулювати пакет з новою інформацією про адресу Рівня 2.




| MAC-адреса призначення | MAC-адреса джерела | IPv4-адреса джерела | IPv4-адреса призначення |
|---|---|---|---|
| dd-dd-dd | cc-cc-cc | 192.168.10.10 | 10.1.1.10 |

Новою MAC-адресою призначення буде адреса інтерфейсу G0/0/1 маршрутизатора R2, а новою MAC-адресою джерела буде адреса інтерфейсу G0/0/1 маршрутизатора R1.

Уздовж кожної ланки шляху IP-пакет інкапсулюється в кадр. Кадр є специфічним для технології канального рівня, пов'язаної з цим каналом, наприклад Ethernet. Якщо пристрій наступного переходу є кінцевим пунктом призначення, MAC-адресою призначення буде адреса мережного адаптера (NIC) Ethernet пристрою.




| MAC-адреса призначення | MAC-адреса джерела | IPv4-адреса джерела | IPv4-адреса призначення |
|---|---|---|---|
| 55-55-55 | ee-ee-ee | 192.168.10.10 | 10.1.1.10 |

Як IP-адреси IP-пакетів у потоці даних пов'язуються з MAC-адресами на кожній ділянці шляху до пункту призначення? Для пакетів IPv4 це здійснюється процесом, який називається протоколом визначення адрес (ARP, Address Resolution Protocol). Для пакетів IPv6 - це процес виявлення сусіда (ND, Neighbor Discovery) протоколу ICMPv6 .

## 9.1.3. **Packet Tracer - Визначення MAC-адрес та IP-адрес**

У цьому завданні у Packet Tracer, ви виконаєте наступні задачі:

- Збір інформації про PDU у випадку зв'язку в локальній мережі
- Збір інформації про PDU у випадку віддаленого мережного зв'язку

Це завдання оптимізоване для перегляду PDU (ping data utility). Пристрої вже налаштовані. Ви будете збирати інформацію про PDU в режимі моделювання та відповісте на ряд запитань про дані, які збираєте.

## Інструкції

## Частина 1: Збір інформації про PDU у випадку зв'язку в локальній мережі

**Примітка**: Перегляньте запитання для самоконтролю в Частині 3, перш ніж перейти до Частини 1. Це дасть вам уявлення про тип інформації, яку вам потрібно буде зібрати.

### Крок 1: Зберіть інформацію PDU під час переміщення пакету від 172.16.31.5 до 172.16.31.2.

a. Натисніть на **172.16.31.5** і відкрийте **Command Prompt**.

b. Введіть команду **ping 172.16.31.2**.

c. Перейдіть в режим моделювання і повторіть команду **ping 172.16.31.2**. Поруч із **172.16.31.5** з'явиться PDU.

d. Натисніть на PDU і перегляньте відомості на вкладках **OSI Model** і **Outbound PDU Layer**:

- MAC адреса призначення: **000C:85CC:1DA7**
- MAC-адреса джерела: **00D0:D311:C788**
- IP-адреса джерела: **172.16.31.5**
- IP адреса призначення: **172.16.31.2**
- На пристрої: **172.16.31.5**

e. Натисніть кнопку **Capture / Forward** (стрілка праворуч з вертикальною смугою), щоб перемістити PDU до наступного пристрою. Зберіть аналогічну інформацію, як описано в пункті d з Кроку 1. Повторюйте, поки PDU не досягне пункту призначення. Запишіть зібрану інформацію про PDU в електронну таблицю, використовуючи формат, подібний до таблиці нижче:

**Приклад формату електронної таблиці**

| На пристрої | MAC-адреса призначення | MAC-адреса джерела | IPv4-адреса джерела | IPv4-адреса призначення |
|---|---|---|---|---|
| 172.16.31.5 | 000C:85CC:1DA7 | 00D0:D311:C788 | 172.16.31.5 | 172.16.31.2 |
| Switch1 | 000C:85CC:1DA7 | 00D0:D311:C788 | N/A | N/A |
| Hub | N/A | N/A | N/A | N/A |
| 172.16.31.2 | 00D0:D311:C788 | 000C:85CC:1DA7 | 172.16.31.2 | 172.16.31.5 |

### Крок 2: Зберіть додаткові відомості про PDU з інших пристроїв.

Повторіть пункти Кроку 1 і зберіть інформацію для наступних тестів:

- Пропінгуйте 172.16.31.2 з вузла 172.16.31.3.
- Пропінгуйте 172.16.31.4 з вузла 172.16.31.5.

Поверніться в режим реального часу (Realtime).

## Частина 2: Збір інформації про PDU у випадку віддаленого мережного зв'язку

Для того, щоб спілкуватися з віддаленими мережами, необхідно використовувати шлюз. Вивчіть, як відбувається зв'язок з пристроями у віддаленій мережі. Приділіть особливу увагу MAC-адресам, які використовуються.

### Крок 1: Зберіть інформацію про PDU під час переміщення пакету від 172.16.31.5 до 10.10.10.2.

a. Натисніть на **172.16.31.5** і відкрийте **Command Prompt**.

b. Введіть команду **ping 10.10.10.2**.

c. Перейдіть в режим моделювання і повторно запустіть команду **ping 10.10.10.2**. Поруч із **172.16.31.5** з'явиться PDU.

d. Натисніть на PDU і перегляньте відомості на вкладці **Outbound PDU Layer**:

- MAC-адреса призначення: 00D0:BA8E:741A
- MAC-адреса джерела: 00D0:D311:C788
- IP-адреса джерела: 172.16.31.5
- IP адреса призначення: 10.10.10.2
- На пристрої: 172.16.31.5

Який пристрій має вказану MAC-адресу призначення?

e. Натисніть кнопку **Capture / Forward** (стрілка праворуч з вертикальною смугою), щоб перемістити PDU до наступного пристрою. Зберіть аналогічну інформацію, як описано в пункті d з Кроку 1. Повторюйте, поки PDU не досягне пункту призначення. Запишіть інформацію про PDU, зібрану в процесі пінгування з вузла 172.16.31.5 до 10.10.10.2 в електронну таблицю, використовуючи в якості зразка формат таблиці нижче:

| На пристрої | MAC-адреса призначення | MAC-адреса джерела | IPv4-адреса джерела | IPv4-адреса призначення |
|---|---|---|---|---|
| 172.16.31.5 | 00D0:BA8:741A | 00D0:D311:C788 | 172.16.31.5 | 10.10.10.2 |
| Switch1 | 00D0:BA8:741A | 00D0:D311:C788 | N/A | N/A |
| Router | 0060:2F84:4AB6 | 00D 0:588 C:2401 | 172.16.31.5 | 10.10.10.2 |
| Switch0 | 0060:2F84:4AB6 | 00D0:588C:2401 | N/A | N/A |
| Access Point | N/A | N/A | N/A | N/A |
| 10.10.10.2 | 00D0:588C:2401 | 0060:2F84:4AB6 | 10.10.10.2 | 172.16.31.5 |

## 9.1.4. **Питання для самоперевірки - MAC- та IP-адреси**

1. Яку MAC-адресу призначення буде включено до кадра, надісланого з вихідного пристрою на пристрій призначення в одній локальній мережі?

   - ◯ Широкомовна MAC-адреса FF-FF-FF-FF-FF-FF.
   - ◯ MAC-адреса пристрою призначення.
   - ◯ MAC-адреса інтерфейсу локального маршрутизатора.

2. Яку MAC-адресу призначення буде включено до кадра, надісланого з вихідного пристрою на пристрій призначення у віддаленій локальній мережі?

   - ◯ Широкомовна MAC-адреса FF-FF-FF-FF-FF-FF.
   - ◯ MAC-адреса пристрою призначення.
   - ◯ MAC-адреса локального інтерфейсу маршрутизатора.

3. Які два протоколи використовуються для визначення MAC-адреси відомої IP-адреси пристрою призначення (IPv4 і IPv6)?

   - ☐ DHCP
   - ☐ ARP
   - ☐ DNS
   - ☐ ND

1. Яку MAC-адресу призначення буде включено до кадра, надісланого з вихідного пристрою на пристрій призначення в одній локальній мережі?

Правильно!

- ○ Широкомовна MAC-адреса FF-FF-FF-FF-FF-FF.
- ◉ MAC-адреса пристрою призначення.
- ○ MAC-адреса інтерфейсу локального маршрутизатора.

2. Яку MAC-адресу призначення буде включено до кадра, надісланого з вихідного пристрою на пристрій призначення у віддаленій локальній мережі?

Правильно!

- ○ Широкомовна MAC-адреса FF-FF-FF-FF-FF-FF.
- ○ MAC-адреса пристрою призначення.
- ◉ MAC-адреса локального інтерфейсу маршрутизатора.

3. Які два протоколи використовуються для визначення MAC-адреси відомої IP-адреси пристрою призначення (IPv4 і IPv6)?

Правильно!

- ☐ DHCP
- ☑ ARP
- ☐ DNS
- ☑ ND

## 9.2. ARP

### 9.2.1. **Огляд ARP**

---

Якщо в мережі використовується протокол зв'язку IPv4, то потрібен протокол визначення адрес (ARP, Address Resolution Protocol), щоб поставити у відповідність IPv4-адресам MAC-адреси. У цій темі пояснюється, як працює ARP.

Кожен IP-пристрій в мережі Ethernet має унікальну MAC-адресу Ethernet. Коли пристрій надсилає кадр Ethernet Рівня 2, він містить дві адреси:

- **MAC-адреса призначення** - MAC-адреса Ethernet пристрою призначення на тому ж сегменті локальної мережі. Якщо хост призначення знаходиться в іншій мережі, то адресою призначення в кадрі буде адреса шлюзу за замовчуванням (тобто маршрутизатора).
- **MAC-адреса джерела** - MAC-адреса мережного адаптера Ethernet на хості джерела.

На рисунку показано надсилання кадра іншому хосту на тому ж сегменті в мережі IPv4.


Щоб відправити пакет на інший хост у тій же локальній мережі IPv4, хост повинен знати IPv4-адресу та MAC-адресу пристрою призначення. IPv4-адреси призначення пристрою або відомі, або визначаються за іменем пристрою. Однак MAC-адреси потрібно визначати.

Пристрій використовує протокол розпізнавання адрес (ARP) для визначення кінцевої MAC-адреси локального пристрою за відомою IPv4-адресою.

ARP забезпечує дві основні функції:

- Визначення MAC-адреси за IPv4-адресою
- Ведення таблиці відповідностей IPv4- та MAC-адрес

## 9.2.2. **Функції ARP**

Коли пакет передається на канальний рівень, де він має бути інкапсульований в кадр Ethernet, пристрій звертається до таблиці в пам'яті, щоб знайти MAC-адресу, яка пов'язана з адресою IPv4. Ця таблиця тимчасово зберігається в оперативній пам'яті і називається ARP-таблицею або ARP-кешем.

Пристрій-відправник буде шукати в ARP-таблиці для IPv4-адреси призначення відповідну MAC-адресу.

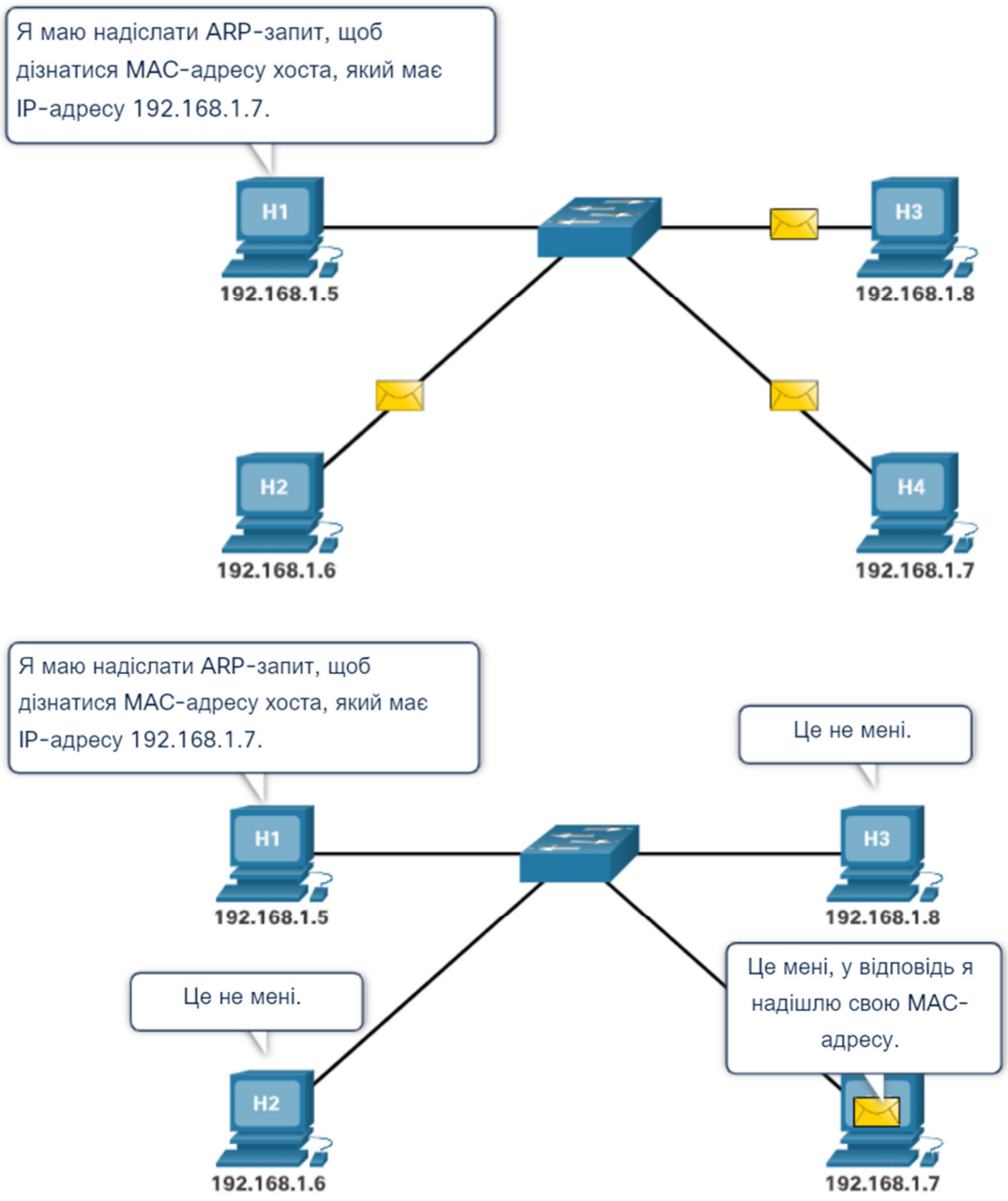
- Якщо IPv4-адреса призначення пакета знаходиться в тій самій мережі, що і IPv4-адреса джерела, пристрій буде шукати в ARP-таблиці запис для IPv4-адреси призначення.
- Якщо IPv4-адреса призначення знаходиться в іншій мережі, ніж IPv4-адреса джерела, пристрій буде шукати в ARP-таблиці IPv4-адресу шлюзу за замовчуванням.

В обох випадках для IPv4-адреси відбувається пошук відповідної MAC-адреси пристрою.

Кожен запис або рядок ARP-таблиці пов'язує IPv4-адресу з MAC-адресою. Ми називаємо встановлення відповідності між цими двома значеннями зіставленням. Це просто означає, що ви можете знайти IPv4-адресу в таблиці та дізнатися відповідну їй MAC-адресу. ARP-таблиця тимчасово зберігає (кешує) зіставлення для пристроїв локальної мережі.

Якщо пристрій знаходить IPv4-адресу, то відповідна їй MAC-адреса використовується як MAC-адреса призначення у кадрі. Якщо жодного запису не знайдено, пристрій надсилає ARP-запит.

Натисніть Відтворити на рисунку, щоб переглянути анімацію про функціонування ARP.



## 9.2.3. **ARP-запит**

ARP-запит надсилається, коли пристрою потрібно визначити MAC-адресу, асоційовану з IPv4-адресою, а в його ARP-таблиці немає відповідного запису.

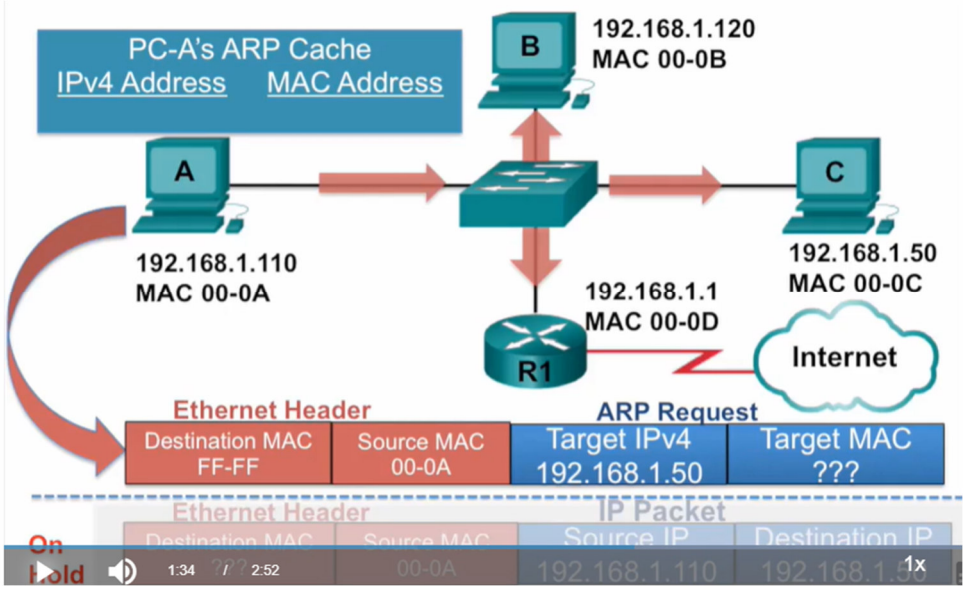
ARP-повідомлення інкапсулюються безпосередньо в кадр Ethernet. Заголовок IPv4 відсутній. ARP-запит інкапсулюється в кадр Ethernet за допомогою наступної інформації в заголовку:

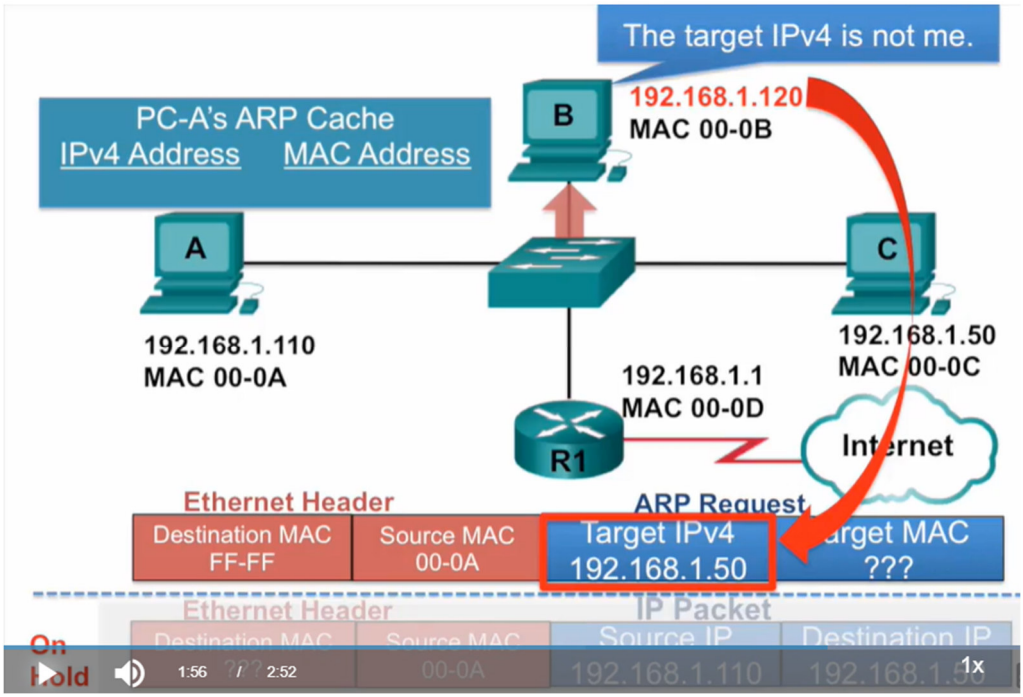
- **MAC-адреса призначення** – це адреса широкомовної розсилки FF-FF-FF-FF-FF-FF, яка вимагає, щоб всі мережні адаптери Ethernet у локальній мережі приймали та обробляли ARP-запит.
- **MAC-адреса джерела** – це MAC-адреса відправника ARP-запиту.
- **Тип** - для ARP-повідомлень це поле має значення 0x806. Воно інформує мережну плату, що інформацію з поля даних кадру потрібно передати процесу ARP.

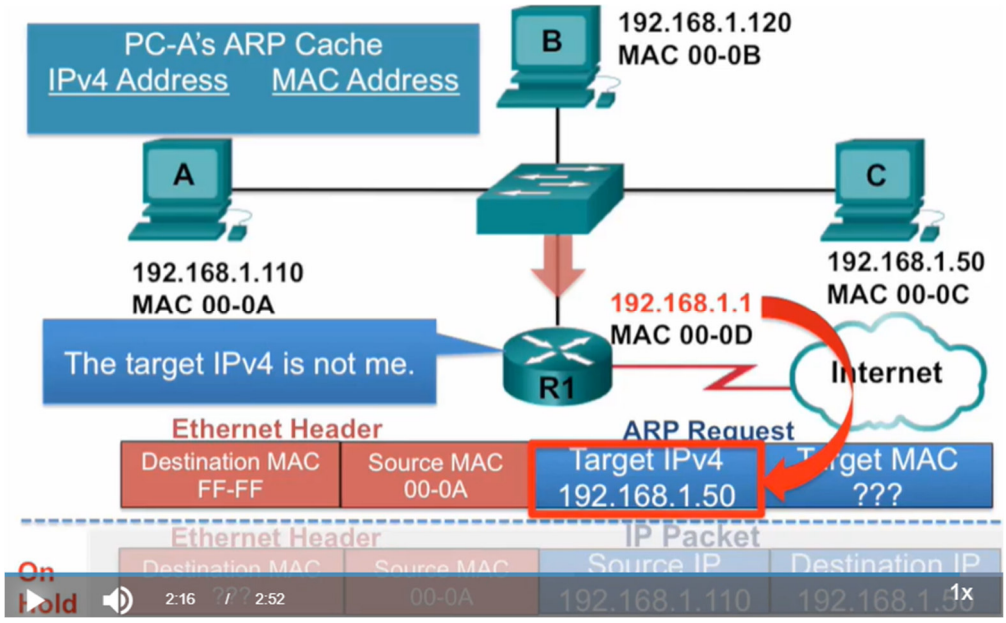
Оскільки ARP-запити є широкомовними розсилками, їх передають з усіх портів комутатора, окрім порту, на який запит було прийнято. Всі мережні адаптери Ethernet у LAN обробляють широкомовні трансляції та повинні доставити ARP-запит у свою операційну систему для обробки. Кожен пристрій повинен обробити ARP-запит, щоб перевірити, чи співпадає цільова IPv4-адреса з його власною. Маршрутизатор не пересилатиме широкомовну розсилку на інші свої інтерфейси.

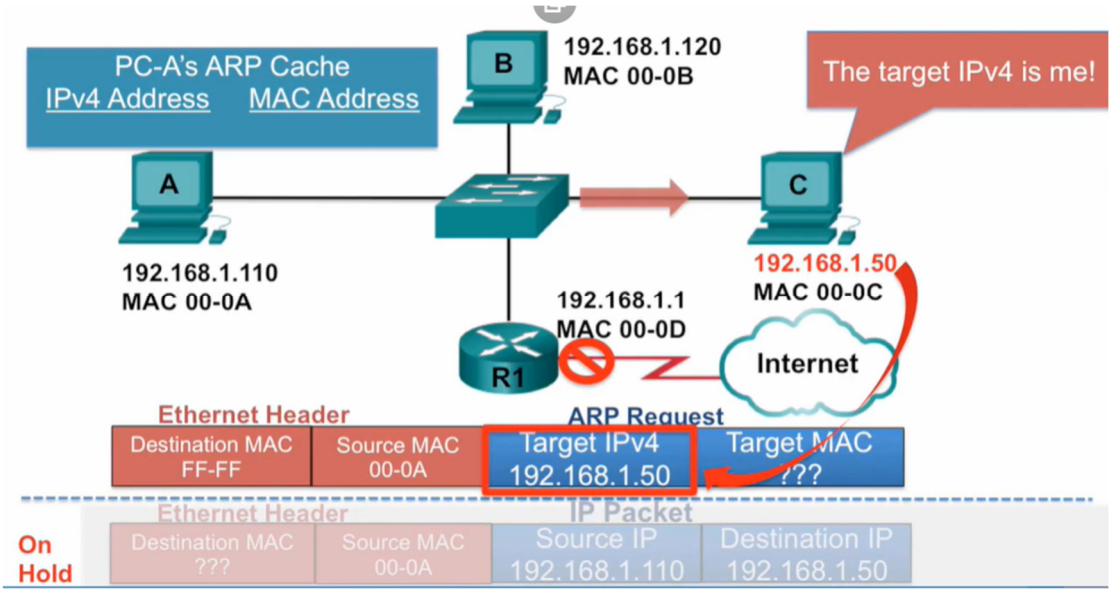
Тільки один пристрій в локальній мережі матиме IPv4-адресу, яка співпадає з цільовою IPv4-адресою у запиті ARP. Всі інші пристрої не будуть відповідати.

***На рисунку показана демонстрація ARP-запиту для IPv4-адреси призначення з PC (A) до PC (C), щоб дізнатися його*** MAC-адресу, ***які знаходиться в локальній мережі.***






***PC (C) відповідає – ARP reply.***

## *9.2.4.* Функціонування ARP - ARP-відповідь

Лише пристрій, IPv4-адреса якого пов'язана з ARP-запитом, надішле ARP-відповідь. ARP-відповідь інкапсулюється в кадр Ethernet за допомогою наступної інформації заголовку:

- **MAC-адреса призначення** – це MAC-адреса відправника ARP-запиту.
- **MAC-адреса джерела** – це MAC-адреса відправника ARP-відповіді.
- **Тип** - для ARP повідомлень це поле має значення 0x806. Воно інформує мережну плату, що інформацію з поля даних кадру потрібно передати процесу ARP.

Тільки пристрій, який відправив запит ARP, отримає ARP-відповідь на свою індивідуальну адресу (unicast ARP reply). Після отримання ARP-відповіді, пристрій додасть IPv4-адресу та відповідну MAC-адресу до своєї ARP-таблиці. Пакети, призначені для цієї IPv4-адреси, тепер можуть бути інкапсульовані в кадри за допомогою відповідної MAC-адреси.

Якщо на ARP-запит не буде відповіді, пакет буде відкинутий, оскільки неможливо створити кадр.

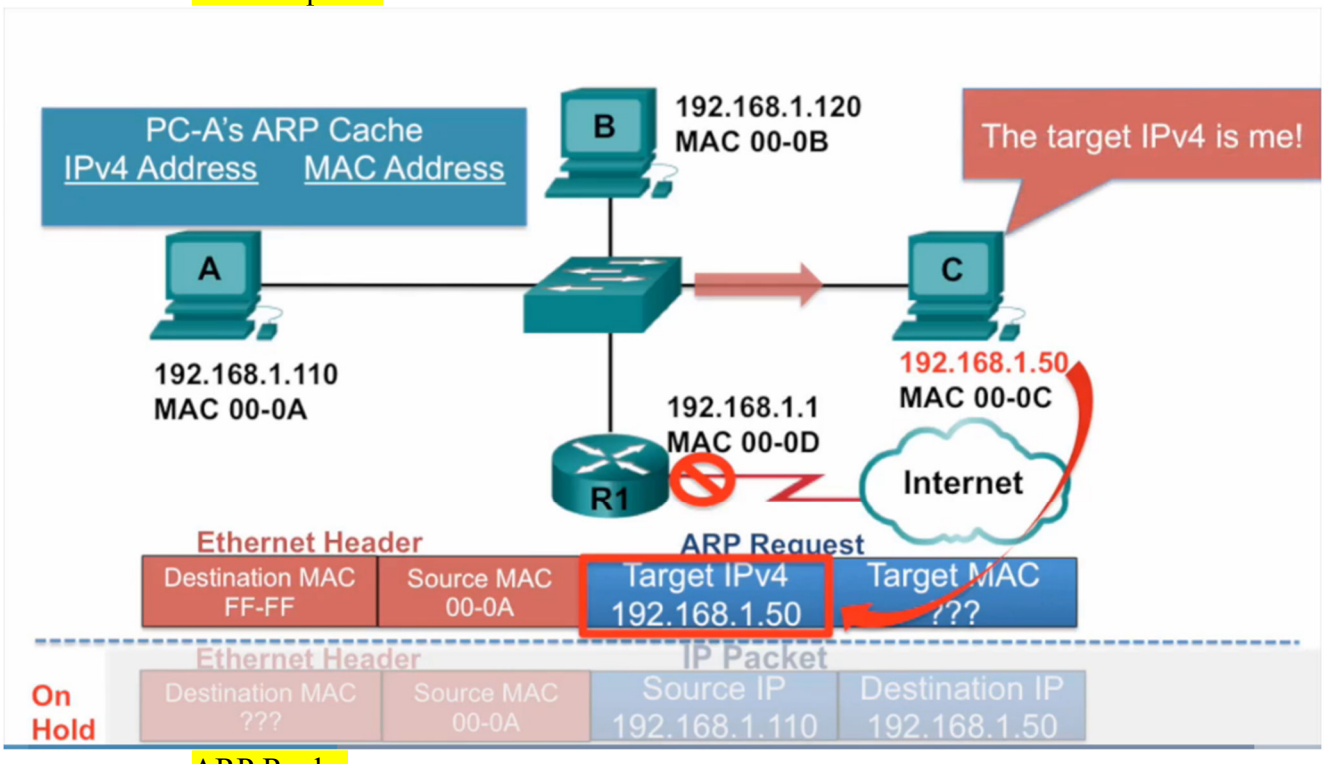
Записи в ARP-таблиці мають часову мітку. Якщо до моменту завершення дії мітки часу пристрій не отримує кадр від певного пристрою, запис для цього пристрою видаляється з ARP-таблиці.

Крім того, до таблиці ARP можна додавати статичні зіставлення, але використовується це рідко. Термін дії статичних записів в таблиці ARP не спливає з часом, тому видаляти їх потрібно вручну.

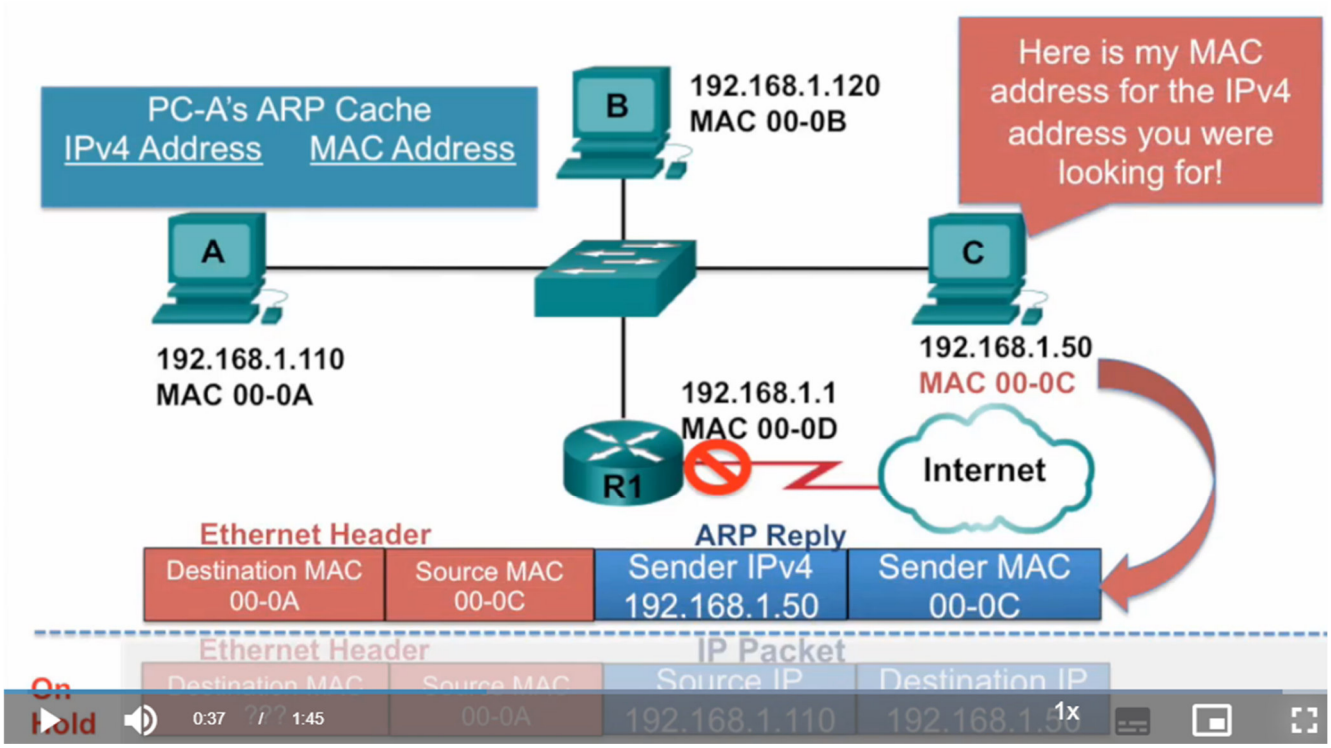
**Примітка**: IPv6 використовує процес виявлення сусіда (ND, Neighbor Discovery) протоколу ICMPv6, аналогічний до ARP-процесу для IPv4. IPv6 використовує повідомлення запиту сусідів (NS, neighbor solicitation) та анонсування сусідів (NA, neighbor advertisement), схожі на ARP-запити та ARP-відповіді IPv4.

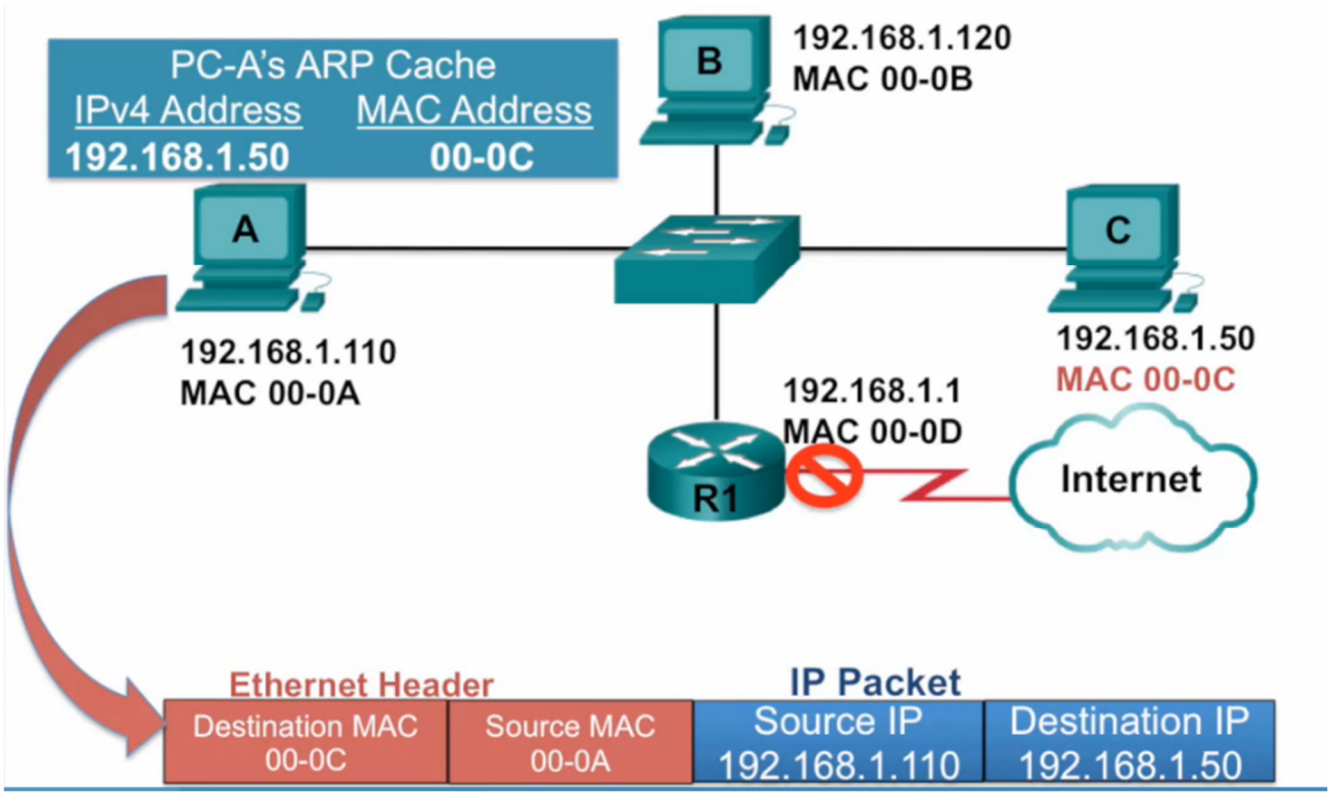
Натисніть Відтворити на рисунку, щоб переглянути демонстрацію ARP-відповіді.

ARP Request :




ARP Reply:



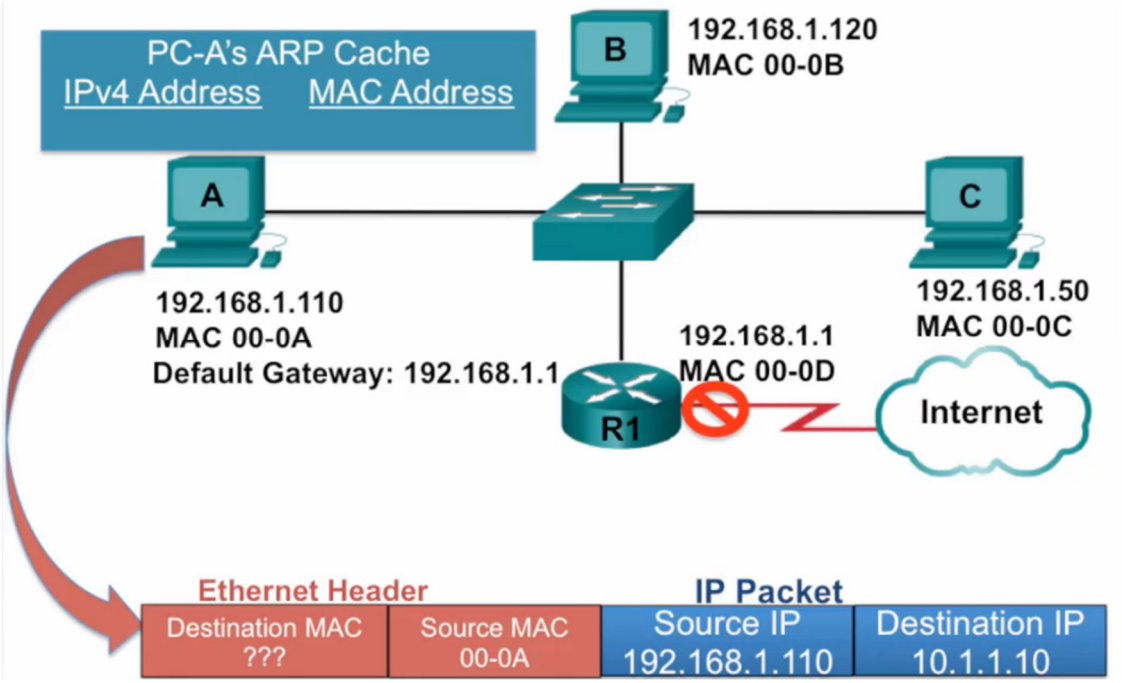



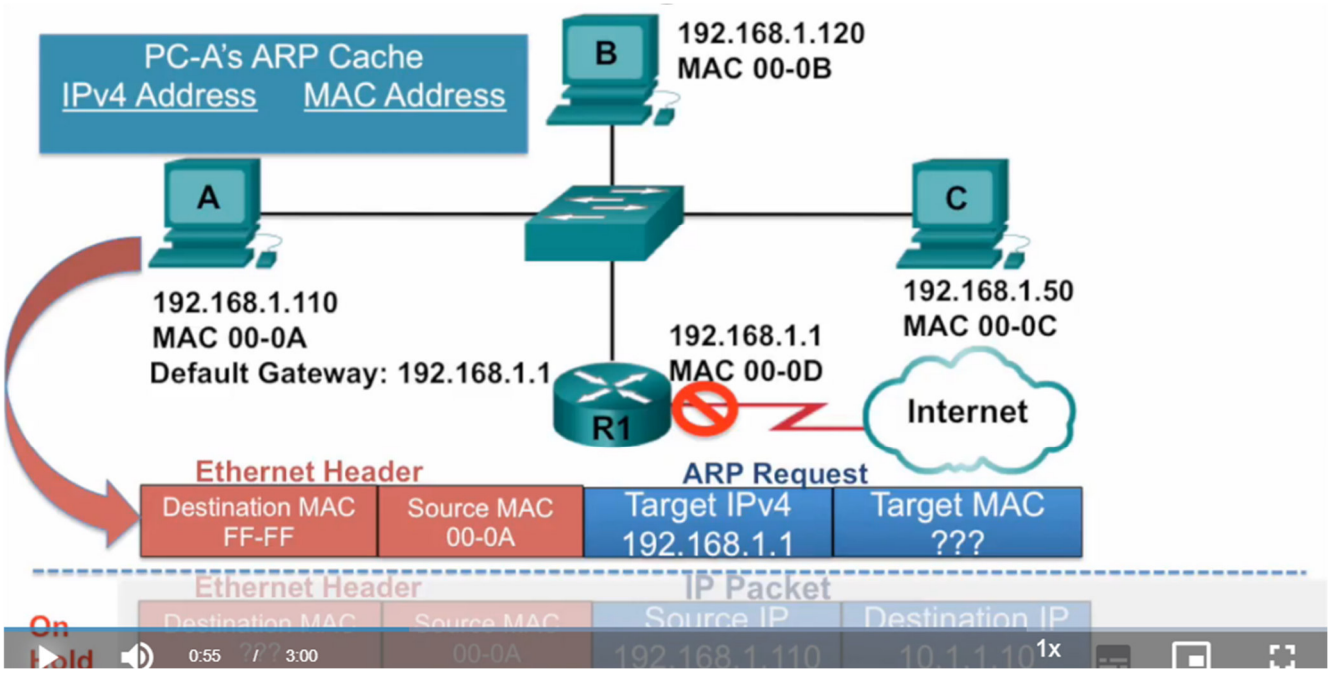

9.2.5. **Роль ARP в обміні даними з віддаленим хостом**

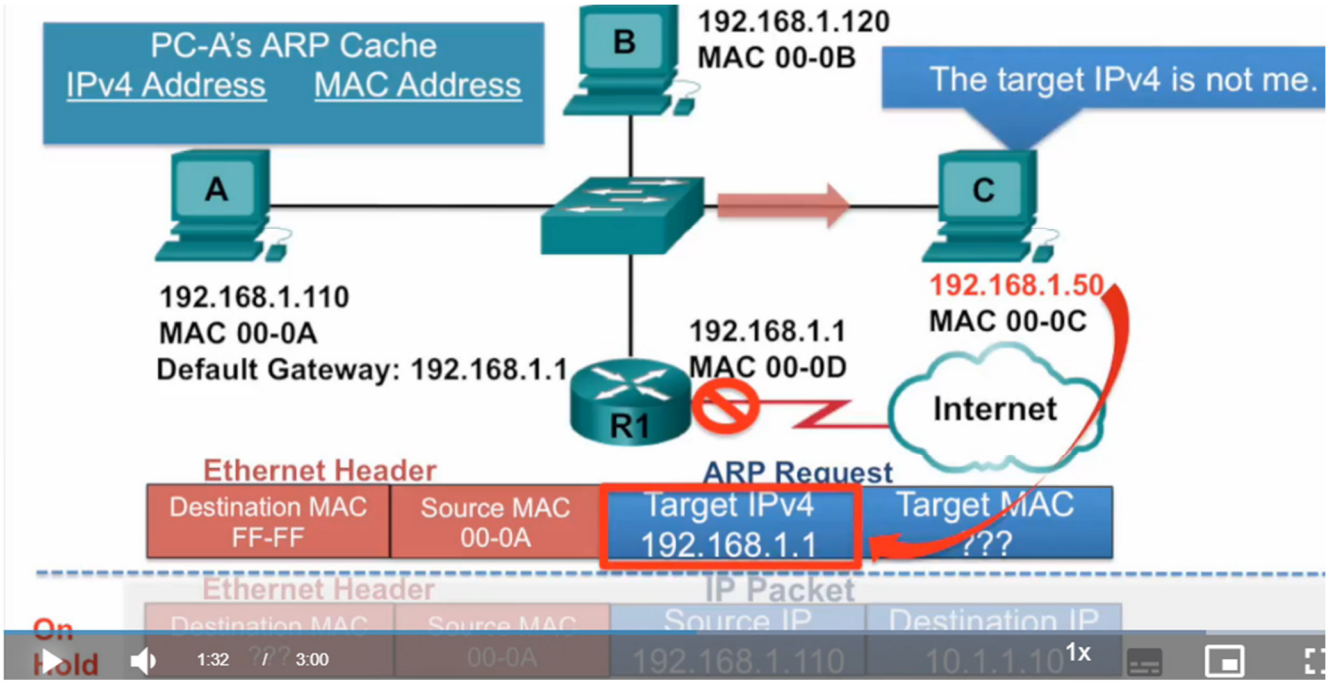
Якщо IPv4-адреса призначення знаходиться не в одній мережі з IPv4-адресою джерела, то пристрій джерела має відправити кадр до шлюзу за замовчуванням. Це інтерфейс локального маршрутизатора. Кожного разу, коли вихідний пристрій має пакет на IPv4-адресу з іншої мережі, він буде інкапсулювати цей пакет в кадр, використовуючи MAC-адресу маршрутизатора.
IPv4-адреса шлюзу за замовчуванням зберігається в конфігурації IPv4 хостів. Коли вузол створює пакет для адресата, він порівнює IPv4-адресу призначення та свою власну IPv4-адресу, щоб визначити, чи знаходяться ці дві IPv4-адреси в одній мережі Рівня 3. Якщо вузол призначення знаходиться в іншій мережі, вихідний пристрій шукає в таблиці ARP-запис з IPv4-адресою шлюзу

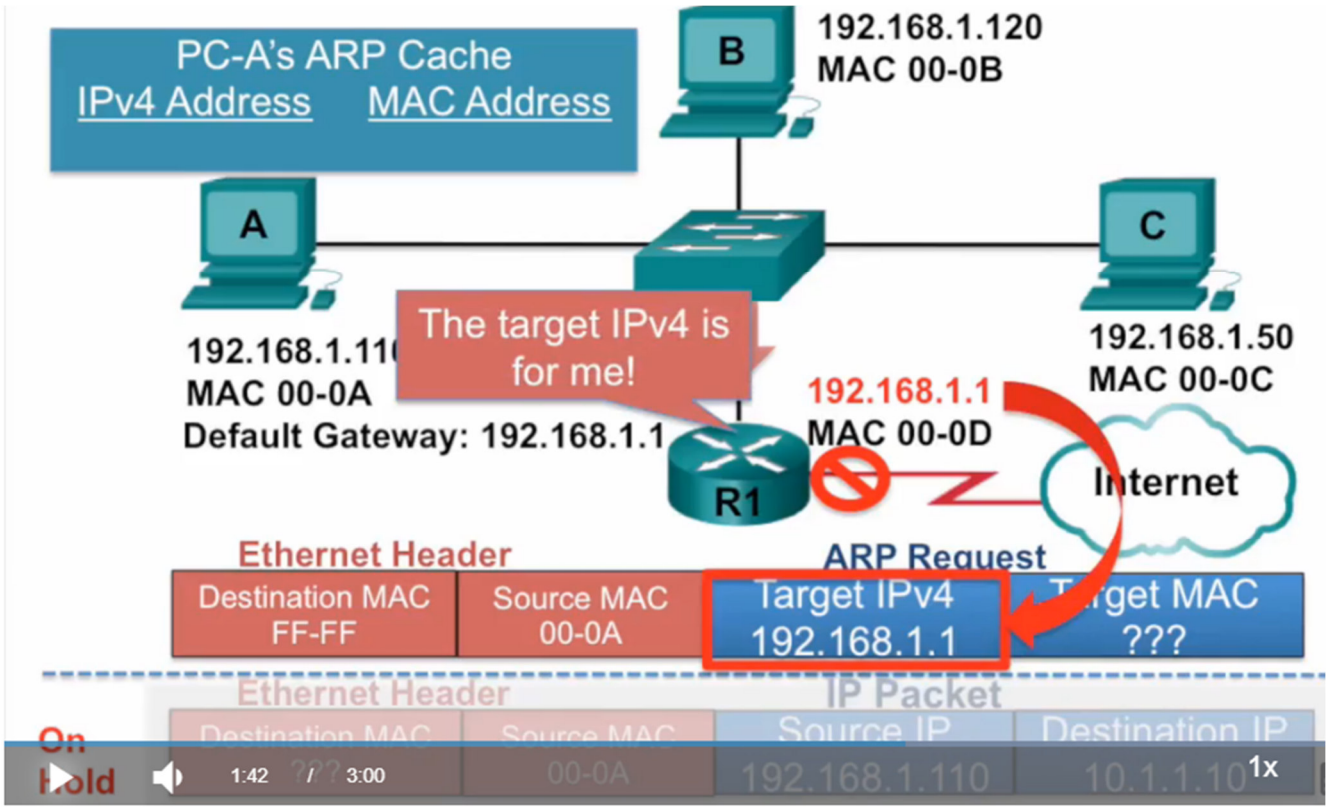
за замовчуванням. Якщо запис відсутній, то для визначення MAC-адреси шлюзу за замовчуванням використовується процесс ARP.

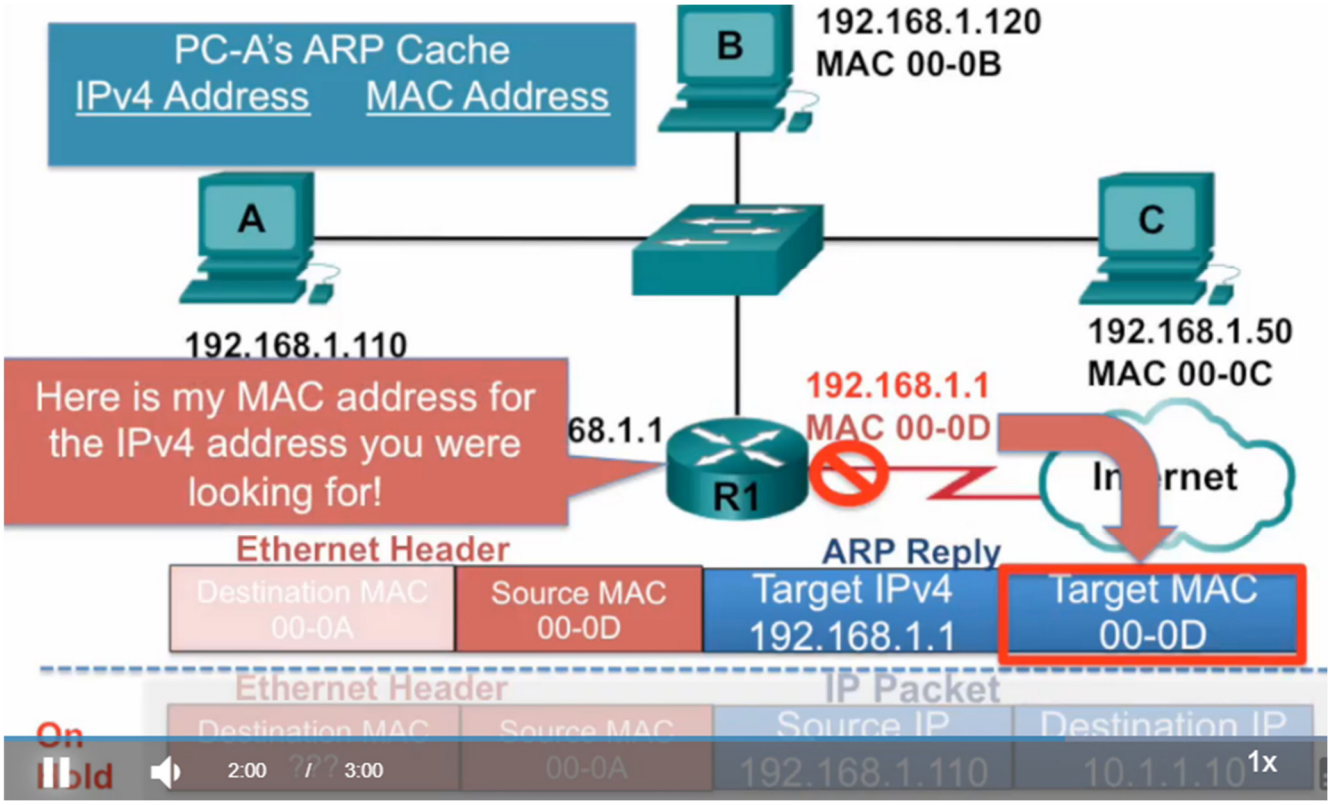
Переглянемо демонстрацію ARP-запиту та ARP-відповіді, пов'язаних зі шлюзом за замовчуванням.

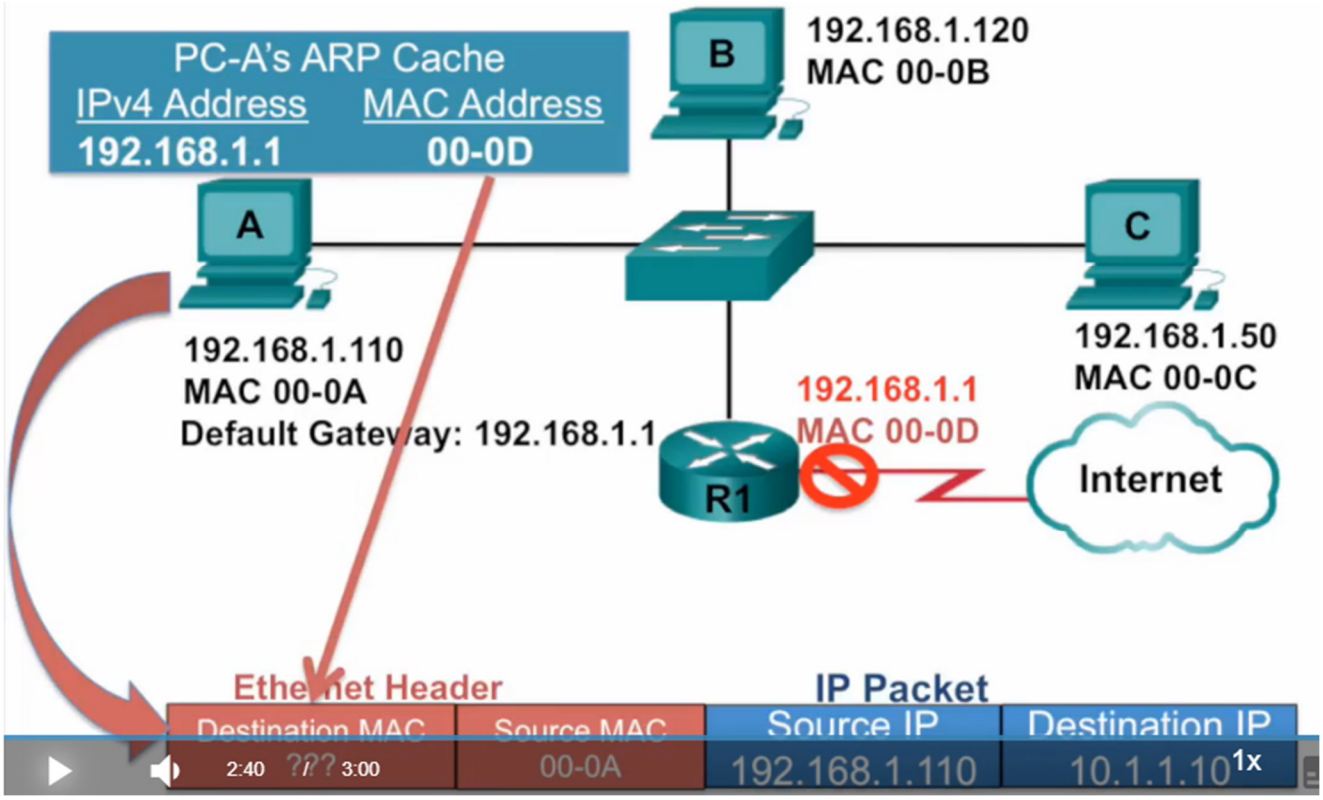



PC-A's ARP Cache
IPv4 Address MAC Address
B
192.168.1.120
MAC 00-0B
The target IPv4 is not me.
A
C
192.168.1.110
MAC 00-0A
Default Gateway: 192.168.1.1
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
ARP Request
Destination MAC
FF-FF
Source MAC
00-0A
Target IPv4
192.168.1.1
Target MAC
???
Ethernet Header
IP Packet
Source IP
Destination IP
00-0A
192.168.1.110
10.1.1.10
On Hold
1:32 / 3:00
1x

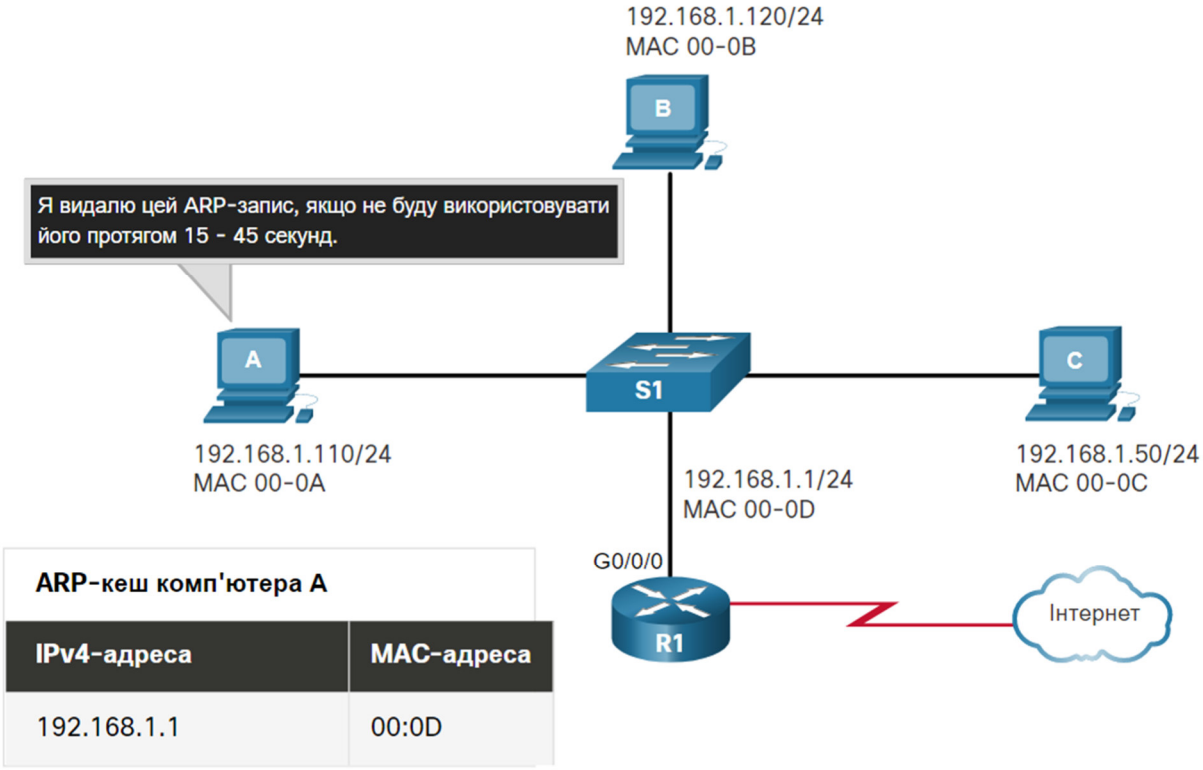

PC-A's ARP Cache
IPv4 Address MAC Address
B
192.168.1.120
MAC 00-0B
A
C
The target IPv4 is for me!
192.168.1.11
MAC 00-0A
Default Gateway: 192.168.1.1
192.168.1.50
MAC 00-0C
192.168.1.1
MAC 00-0D
R1
Internet
Ethernet Header
ARP Request
Destination MAC
FF-FF
Source MAC
00-0A
Target IPv4
192.168.1.1
Target MAC
???
Ethernet Header
IP Packet
Source IP
Destination IP
00-0A
192.168.1.110
10.1.1.10
On Hold
1:42 / 3:00
1x




## 9.2.6. **Видалення записів з ARP-таблиці**

На кожному пристрої є таймер ARP-кешу, який видаляє з ARP-таблиці записи, що не використовувались протягом зазначеного періоду часу. Цей період може бути різним і залежить від операційної системи пристрою. Наприклад, нові операційні системи Windows зберігають записи таблиці ARP від 15 до 45 секунд, як показано на рисунку.




Примітка: MAC-адреси скорочено для демонстрації.

Також можна використовувати команди для видалення деяких або всіх записів з ARP-таблиці вручну. Після видалення запису процес відправки ARP-запиту та отримання ARP-відповіді має бути задіяний повторно, щоб додати зіставлення до ARP-таблиці.

## 9.2.7. **ARP-таблиці на мережних пристроях**

На маршрутизаторі Cisco для відображення таблиці ARP використовується команда **show ip arp**, як показано на рисунку.

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1           -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
Internet  209.165.200.225        -   a0e0.af0d.e141  ARPA   GigabitEthernet0/0/1
Internet  209.165.200.226        1   a03d.6fe1.9d91  ARPA   GigabitEthernet0/0/1
R1#
```

На ПК під керуванням ОС Windows 10 для відображення таблиці ARP використовується команда **arp –a**, як показано на рисунку.

```
C:\Users\PC> arp -a
Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
  192.168.1.110         08-3e-0c-f5-f7-56     dynamic
  192.168.1.112         ac-b3-13-4a-bd-d0     dynamic
  192.168.1.117         08-3e-0c-f5-f7-5c     dynamic
  192.168.1.126         24-77-03-45-5d-c4     dynamic
  192.168.1.146         94-57-a5-0c-5b-02     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\Users\PC>
```

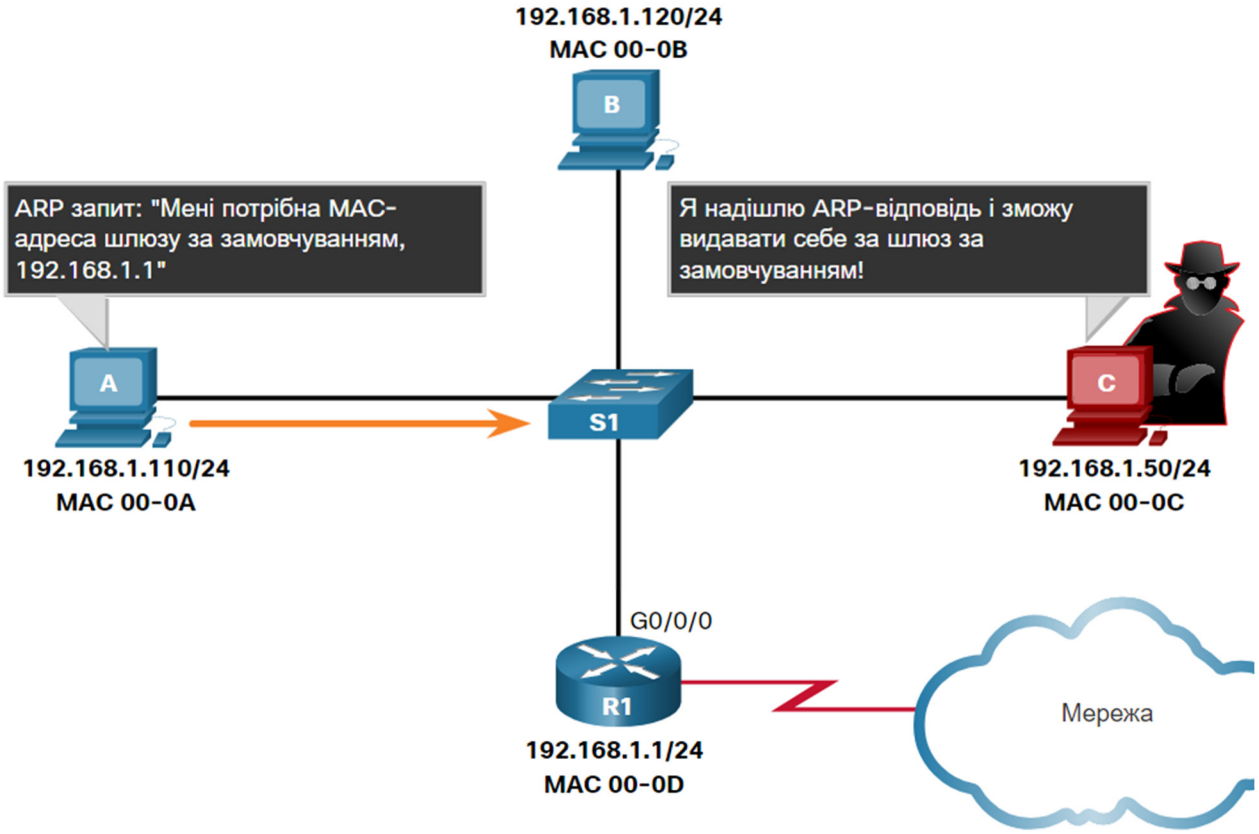
## 9.2.8. **Проблеми ARP - Широкомовні розсилки ARP та ARP-spoofing**

Оскільки ARP-запит є кадром широкомовної розсилки, то його отримують та обробляють всі пристрої в локальній мережі. В типовій корпоративній мережі такі широкомовні розсилки, скоріш за все, матимуть мінімальний вплив на продуктивність мережі. Однак, якщо велика кількість пристроїв будуть увімкнені та розпочнуть отримувати доступ до мережних послуг одночасно, це може спричинити деяке зниження продуктивності мережі на короткий проміжок часу, як показано на рисунку. Після того, як пристрої ініціюють широкомовні трансляції ARP та вивчать необхідні MAC-адреси, будь-який вплив на мережу буде мінімізовано.

**Всі пристрої було увімкнено одночасно.**


У деяких випадках використання ARP може призвести до потенційного ризику для безпеки. Зловмисник може використовувати ARP-spoofing для здійснення атаки "отруєння" ARP (підробки ARP-кешу). Під час таких атак зловмисник відповідає на ARP-запит для IPv4-адреси, яка належить іншому пристрою, наприклад шлюзу за замовчуванням, як показано на рисунку. Зловмисник надсилає ARP-відповідь з власною MAC-адресою. Отримувач ARP-відповіді додасть фальсифіковану MAC-адресу до своєї ARP-таблиці і направлятиме свої пакети зловмиснику.

Корпоративні комутатори включають методи пом'якшення наслідків, відомі як динамічна перевірка ARP (DAI, Dynamic ARP Inspection). DAI не розглядається в рамках цього курсу.




Примітка: MAC-адреси скорочено для демонстрації.

## 9.2.9. **Packet Tracer - Дослідження ARP-таблиці**

У цьому завданні у Packet Tracer, ви виконаєте наступні задачі:

- Вивчите ARP-запит
- Вивчите таблиці MAC-адрес комутатора
- Вивчите процес ARP у випадку віддаленого зв'язку

Це завдання оптимізоване для перегляду PDU. Пристрої вже налаштовані. Ви будете збирати інформацію про PDU в режимі моделювання та відповісте на ряд запитань про дані, які збираєте.

# Packet Tracer – Дослідження ARP-таблиці

## Таблиця адресації

| Пристрій | Інтерфейс | MAC-адреса | Інтерфейс комутатора |
|---|---|---|---|
| Router0 | G0/0 | 0001.6458.2501 | G0/1 |
| | S0/0/0 | N/A | N/A |
| Router1 | G0/0 | 00E0.F7B1.8901 | G0/1 |
| | S0/0/0 | N/A | N/A |
| 10.10.10.2 | Wireless (бездротове з'єднання) | 0060.2F84.4AB6 | F0/2 |
| 10.10.10.3 | Wireless (бездротове з'єднання) | 0060.4706.572B | F0/2 |
| 172.16.31.2 | F0 | 000C.85CC.1DA7 | F0/1 |
| 172.16.31.3 | F0 | 0060.7036.2849 | F0/2 |
| 172.16.31.4 | G0 | 0002.1640.8D75 | F0/3 |

## Частина 1: Вивчення ARP-запиту

### Крок 1: Генеруйте ARP-запити, надсилаючи запит ping на 172.16.31.3 з вузла 172.16.31.2.

a. Натисніть на ПК з адресою **172.16.31.2** і відкрийте **Command Prompt**.

b. Введіть команду **arp -d** для очищення ARP-таблиці.

c. Увійдіть в режим моделювання **Simulation** і введіть команду **ping 172.16.31.3**. Буде створено два PDU. Команда **ping** не може відправити ICMP-пакет, не знаючи MAC-адресу призначення. Тому комп'ютер відправляє широкомовну розсилку кадру ARP, щоб знайти MAC-адресу призначення.

d. Натисніть **Capture/Forward** один раз. PDU ARP переміщується на комутатор **Switch1**, а ICMP PDU зникає, чекаючи на ARP-відповідь. Відкрийте PDU і запишіть MAC-адресу призначення.

Чи вказана ця адреса в таблиці вище?

## 9.2.10. **Питання для самоперевірки - ARP**

1. Які дві функції забезпечує ARP? (Оберіть дві.)

- [ ] Ведення таблиці відповідностей адрес IPv4 та доменних імен
- [ ] Ведення таблиці відповідностей IPv4- та MAC-адрес
- [ ] Ведення таблиці відповідностей IPv6- та MAC-адрес
- [ ] Перетворює адреси IPv4 на доменні імена
- [ ] Перетворює адреси IPv4 на MAC-адреси
- [ ] Перетворює адреси IPv6 на MAC-адреси

2. Де зберігається таблиця ARP на пристрої?

- ◯ ПЗП (ROM)
- ◯ Флеш-пам'ять (flash)
- ◯ Енергонезалежна пам'ять (NVRAM)
- ◯ ОЗП (RAM)

3. Яке твердження правдиве стосовно ARP?

- ◯ ARP-кеш не можна видалити вручну.
- ◯ Записи ARP-таблиці кешуються остаточно.
- ◯ Записи ARP-таблиці кешуються тимчасово.

4. Яку команду можна використовувати на маршрутизаторі Cisco для перегляду таблиці ARP?

- ◯ **arp -a**
- ◯ **arp -d**
- ◯ **show arp table**
- ◯ **show ip arp**

5. Що таке атака з використанням ARP?

- ◯ Широкомовні розсилки ARP
- ◯ Атаки ARP hopping
- ◯ ARP-отруєння (ARP poisoning )
- ◯ ARP-виснаження (ARP starvation)

1. Які дві функції забезпечує ARP? (Оберіть дві.)

Правильно!

- [ ] Ведення таблиці відповідностей адрес IPv4 та доменних імен
- [x] Ведення таблиці відповідностей IPv4- та MAC-адрес
- [ ] Ведення таблиці відповідностей IPv6- та MAC-адрес
- [ ] Перетворює адреси IPv4 на доменні імена
- [x] Перетворює адреси IPv4 на MAC-адреси
- [ ] Перетворює адреси IPv6 на MAC-адреси

2. Де зберігається таблиця ARP на пристрої?

Правильно!

- ( ) ПЗП (ROM)
- ( ) Флеш-пам'ять (flash)
- ( ) Енергонезалежна пам'ять (NVRAM)
- (•) ОЗП (RAM)

3. Яке твердження правдиве стосовно ARP?

Правильно!

- ARP-кеш не можна видалити вручну.
- Записи ARP-таблиці кешуються остаточно.
- **Записи ARP-таблиці кешуються тимчасово.**

4. Яку команду можна використовувати на маршрутизаторі Cisco для перегляду таблиці ARP?

Правильно!

- **arp -a**
- **arp -d**
- **show arp table**
- **show ip arp**

5. Що таке атака з використанням ARP?

Правильно!

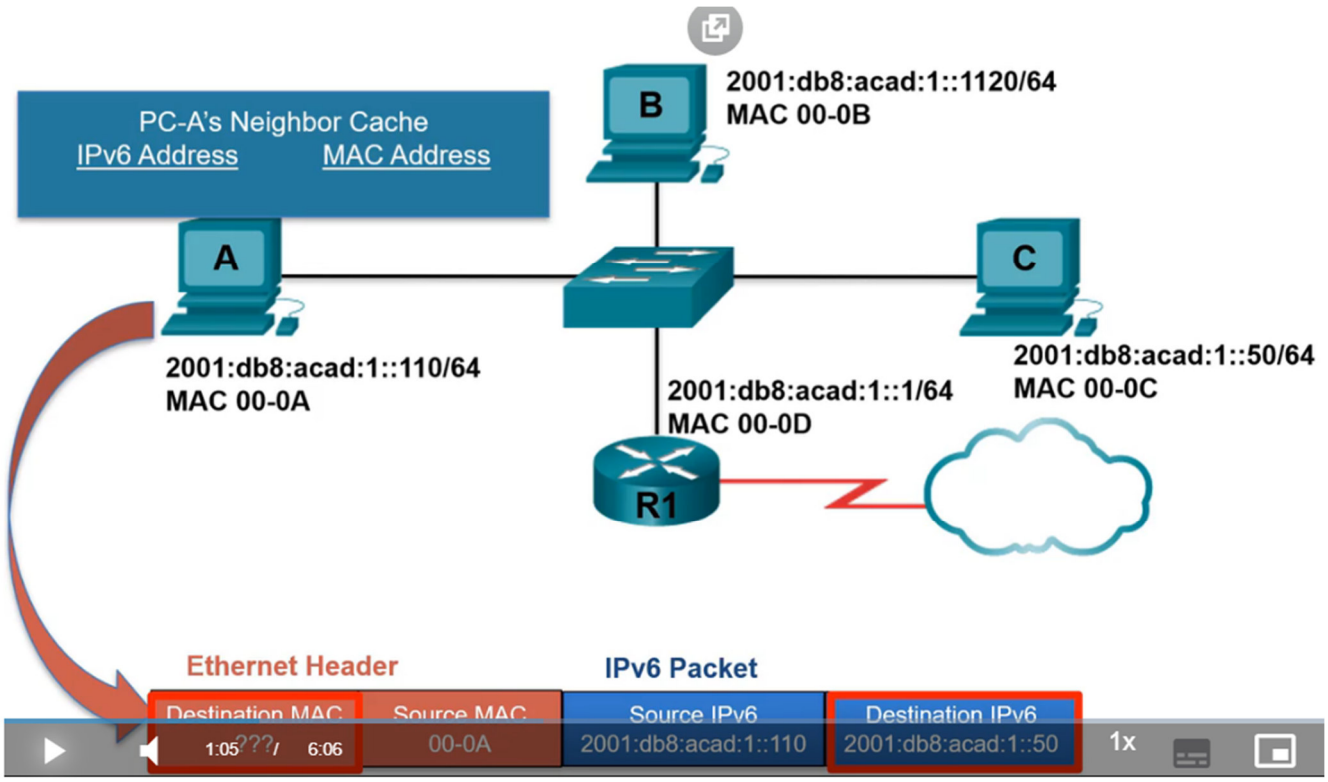
- Широкомовні розсилки ARP
- Атаки ARP hopping
- **ARP-отруєння (ARP poisoning )**
- ARP-виснаження (ARP starvation)

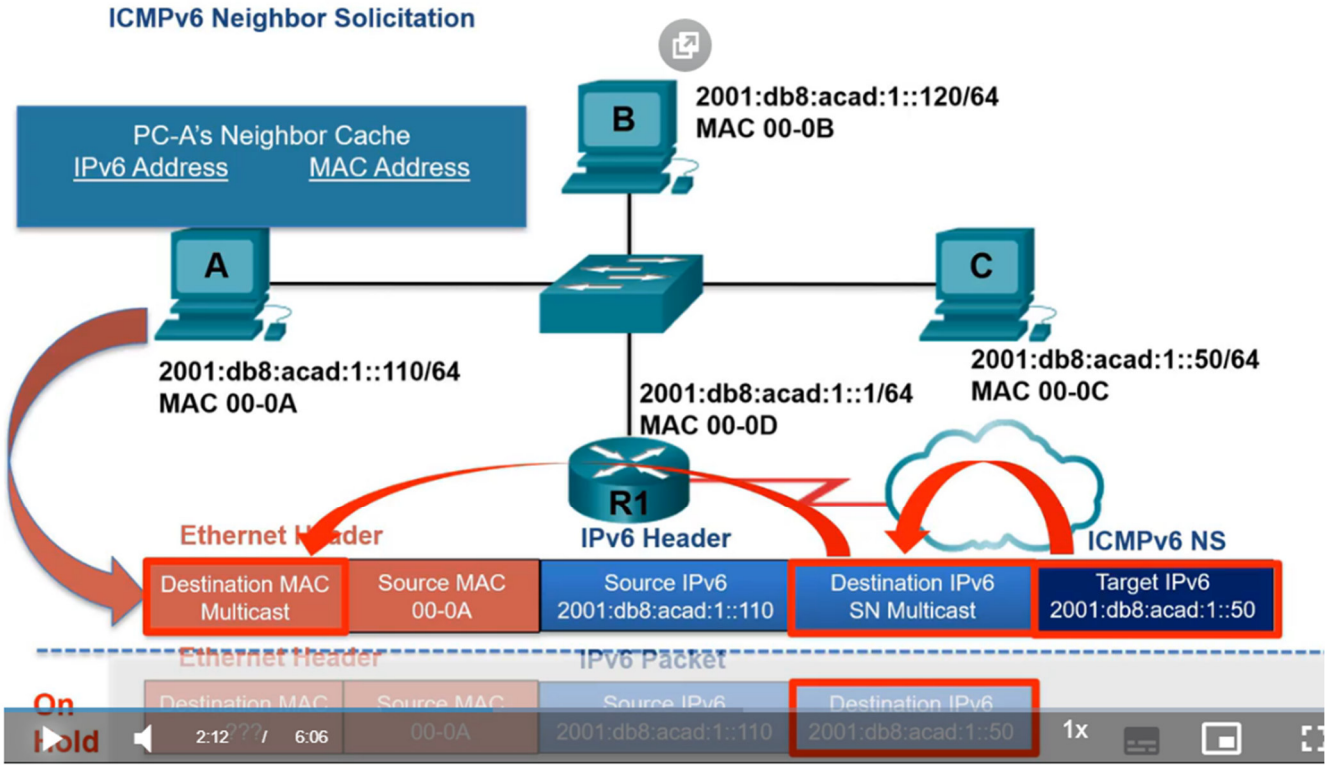
## 9.3. Виявлення сусіда

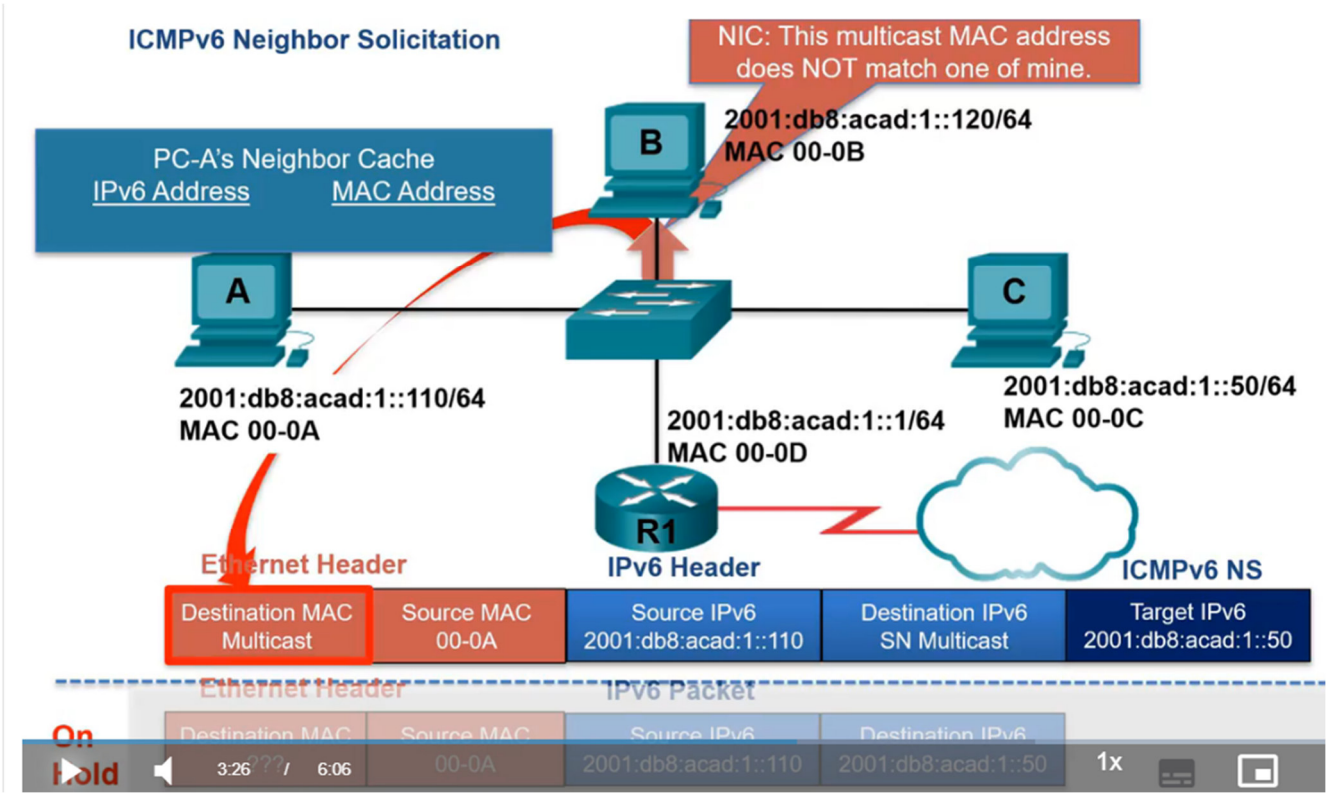
# 9.3.1. Виявлення сусіда (ND) IPv6

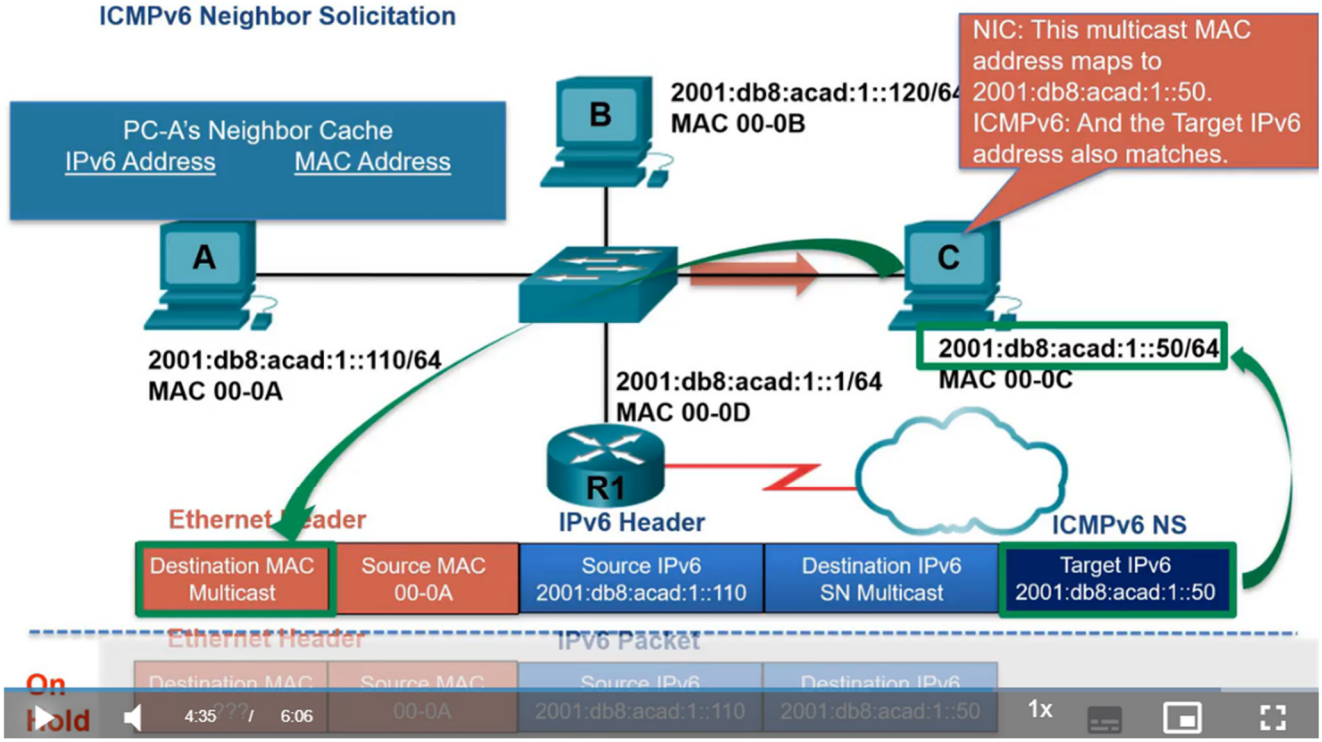
Якщо в мережі використовується протокол зв'язку IPv6, то потрібен протокол виявлення сусіда (ND, Neighbor Discovery Protocol), щоб зіставити IPv6-адреси з MAC-адресами. У цій темі пояснюється, як працює ND.

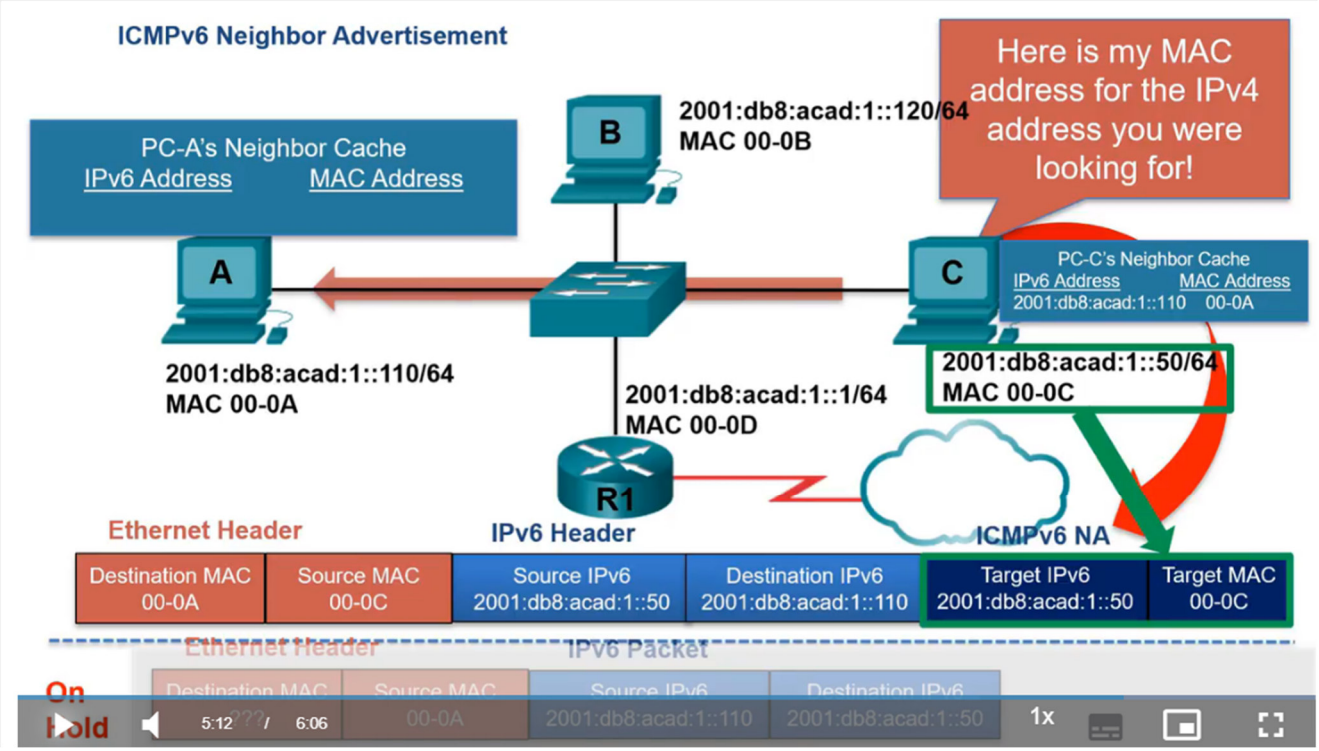
Натисніть Відтворити на рисунку, щоб переглянути демонстрацію про виявлення сусіда IPv6.

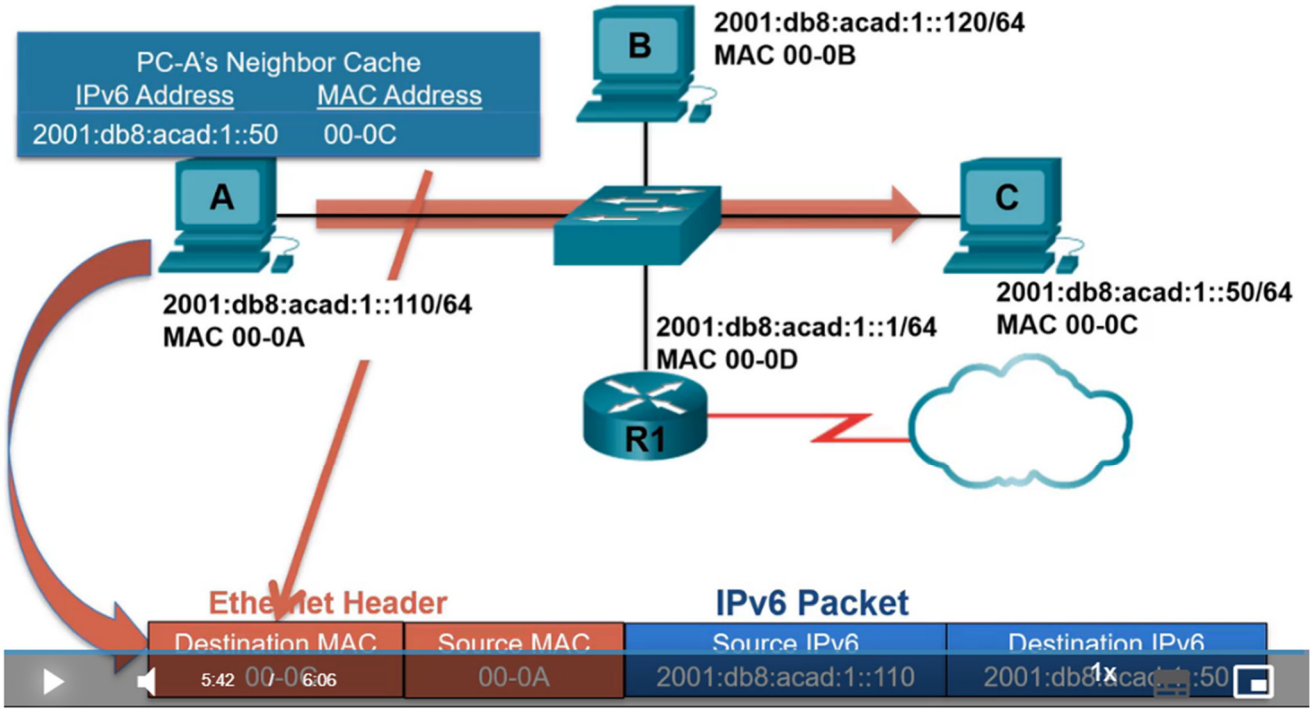



ICMPv6 Neighbor Solicitation
NIC: This multicast MAC address does NOT match one of mine.
PC-A's Neighbor Cache
IPv6 Address MAC Address
B
2001:db8:acad:1::120/64
MAC 00-0B
A
C
2001:db8:acad:1::110/64
MAC 00-0A
2001:db8:acad:1::1/64
MAC 00-0D
2001:db8:acad:1::50/64
MAC 00-0C
R1
Ethernet Header
IPv6 Header
ICMPv6 NS
Destination MAC Multicast
Source MAC 00-0A
Source IPv6 2001:db8:acad:1::110
Destination IPv6 SN Multicast
Target IPv6 2001:db8:acad:1::50
IPv6 Packet
3:26 / 6:06
1x


ICMPv6 Neighbor Solicitation
NIC: This multicast MAC address maps to 2001:db8:acad:1::50. ICMPv6: And the Target IPv6 address also matches.
PC-A's Neighbor Cache
IPv6 Address MAC Address
B
2001:db8:acad:1::120/64
MAC 00-0B
A
C
2001:db8:acad:1::110/64
MAC 00-0A
2001:db8:acad:1::1/64
MAC 00-0D
2001:db8:acad:1::50/64
MAC 00-0C
R1
IPv6 Header
ICMPv6 NS
Destination MAC Multicast
Source MAC 00-0A
Source IPv6 2001:db8:acad:1::110
Destination IPv6 SN Multicast
Target IPv6 2001:db8:acad:1::50
IPv6 Packet
4:35 / 6:06
1x




## 9.3.2. Повідомлення ND IPv6

Протокол виявлення сусіда (Neighbor Discovery protocol) IPv6 іноді називають просто ND або NDP. У цьому курсі ми будемо використовувати скорочення ND. ND забезпечує зіставлення адреси, виявлення маршрутизатора та послуги переспрямування для IPv6 за допомогою ICMPv6. ND протоколу ICMPv6 використовує п'ять повідомлень ICMPv6 для забезпечення цих сервісів:

- повідомлення запиту сусіда (Neighbor Solicitation)
- повідомлення анонсування сусіда (Neighbor Advertisement)
- повідомлення запиту маршрутизатора (Router Solicitation)
- повідомлення анонсування маршрутизатора (Router Advertisement)
- переспрямування повідомлення

Повідомлення запиту та анонсування сусіда використовуються для обміну повідомленнями між пристроями для визначення адреси (подібно до ARP у IPv4). Пристрої включають як хост-комп'ютери, так і маршрутизатори.


Повідомлення запиту та анонсування маршрутизатора призначені для обміну повідомленнями між пристроями та маршрутизаторами. Зазвичай виявлення маршрутизатора використовується для динамічного виділення адрес і автоконфігурації адрес без відстеження стану (SLAAC, StateLess Address AutoConfiguration).


**Примітка**: П'яте повідомлення ND протоколу ICMPv6 - це повідомлення для перенаправлення, яке використовується для кращого вибору наступного переходу. В рамках цього курсу воно не розглядається.

ND IPv6 визначається стандартом IETF RFC 4861.

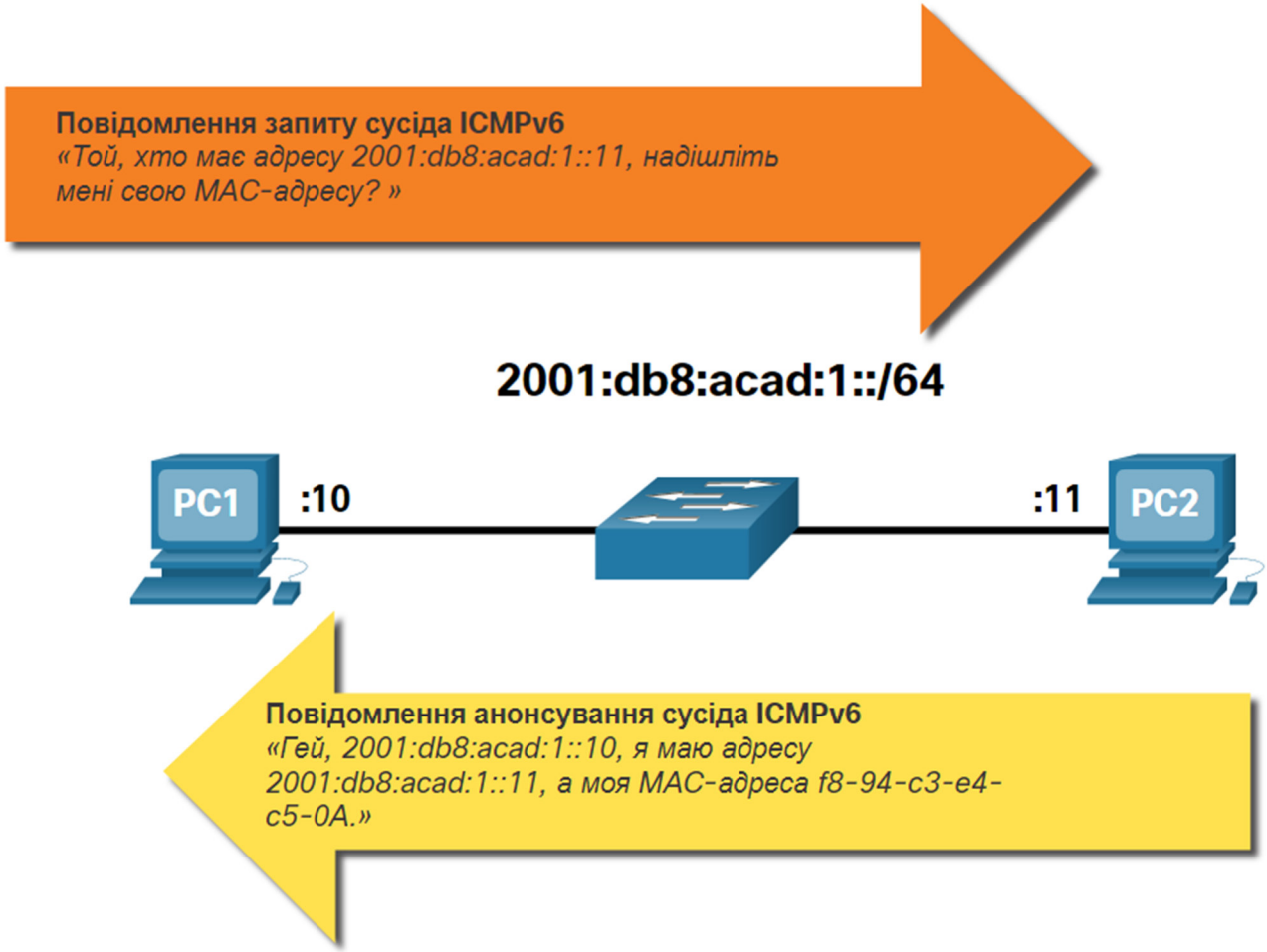
## 9.3.3. ND IPv6 - Визначення адрес

Так само, як ARP для IPv4, пристрої з IPv6 використовують ND для визначення MAC-адреси пристрою, адреса IPv6 якого відома.

Повідомлення запиту та анонсування сусіда використовуються для визначення MAC-адрес. Це схоже на ARP-запити та ARP-відповіді, що використовує ARP для IPv4. Наприклад, нехай PC1 хоче надіслати запит ping до PC2, який має IPv6-адресу 2001:db8:acad::11. Щоб визначити MAC-адресу для відомої адреси IPv6, PC1 надсилає повідомлення запиту сусіда ICMPv6, як показано на рисунку.

Повідомлення запиту сусідаICMPv6 надсилаються за допомогою спеціальних групових Ethernet- і IPv6-адрес. Це дозволяє мережному адаптеру Ethernet приймаючого пристрою визначити, чи стосується повідомлення запиту сусіда даного пристрою без необхідності відправляти його для обробки операційній системі.

PC2 відповідає на запит повідомленням анонсування сусіда ICMPv6, яке містить його MAC-адресу.




## 9.3.4. Packet Tracer - Виявлення сусіда (ND) IPv6

Для того, щоб пристрій зв'язувався з іншим пристроєм, потрібно знати MAC-адресу кінцевого пристрою. В IPv6 за визначення MAC-адреси призначення відповідає процес під назвою Виявлення сусіда (ND, Neighbor Discovery). Ви будете збирати інформацію про блок даних протоколу (PDU) в режимі моделювання, щоб краще зрозуміти процес. Це завдання у Packet Tracer не оцінюється.

### Packet Tracer – Виявлення сусіда (ND) IPv6

#### Таблиця адресації

| Пристрій | Інтерфейс | IPv6-адреса / Префікс | Шлюз за замовчуванням |
|---|---|---|---|
| RTA | G0/0/0 | 2001:db8:acad:1::1/64 | N/A |
| | G0/0/1 | 2001:db8:acad:1::1/64 | N/A |
| PCA1 | NIC | 2001:db8:acad:1::A/64 | fe80::1 |
| PCA2 | NIC | 2001:db8:acad:1::B/64 | fe80::1 |
| PCB1 | NIC | 2001:db8:acad:2::A/64 | fe80::1 |

#### Цілі та задачі

**Частина 1: Виявлення сусіда IPv6 у локальній мережі**

**Частина 2: Виявлення сусіда IPv6 у віддаленій мережі**

## Довідкова інформація

Для того, щоб пристрій міг зв'язуватися з іншим пристроєм, потрібно знати MAC-адресу кінцевого пристрою. В IPv6 за визначення MAC-адреси призначення відповідає процес Виявлення сусіда (Neighbor Discovery), що використовує NDP або протокол ND. Ви будете збирати інформацію про блок даних протоколу (PDU) в режимі моделювання, щоб краще зрозуміти цей процес. Це завдання у Packet Tracer не оцінюється.

## Інструкції

## Частина 1: Виявлення сусіда IPv6 у локальній мережі

У Частині 1 цієї практичної роботи ви одержите MAC-адресу пристрою призначення, що знаходиться у тій же мережі.

### Крок 1: Перевірте чи виявив маршрутизатор наявність будь-яких сусідів.

a. Натисніть на маршрутизатор RTA. Виберіть вкладку CLI і введіть команду **show ipv6 neighbors** у привілейованому режимі EXEC. Якщо відображаються якісь записи, видаліть їх за допомогою команди **clear ipv6 neighbors**.

b. Натисніть на **PCA1**, виберіть вкладку Desktop на натисніть на значок режиму командного рядка **Command Prompt**.

### Крок 2: Перейдіть в режим моделювання Simulation для фіксування подій.

c. Натисніть кнопку **Simulation** в правому нижньому кутку вікна топології Packet Tracer.

d. Натисніть кнопку **Show All/None** у нижній лівій частині панелі Simulation Panel. Переконайтеся у правильності налаштування: в **Event List Filters – Visible Events** відображається **None**.

e. З командного рядка на **PCA1** введіть команду **ping —n 1 2001:db8:acad:1::b**. Почнеться процес пінгування **PCA2**.




f. Натисніть кнопку **Capture/Forward,** зображену як стрілка з вертикальною смугою праворуч у полі Play Controls. В рядку стану над Play Controls відобразиться Captured to: 150. (Число може відрізнятися.)

g. Натисніть кнопку **Edit Filters**. Виберіть вкладку IPv6 вгорі і поставте галочки для **ICMPv6** та **NDP**. Натисніть на червоний хрестик у верхньому правому куті вікна Edit ACL Filters. Тепер будуть показані відстежувані події. У вікні повинно бути приблизно 12 записів.

Чому присутні PDU протоколу ND?

h. Натисніть на квадратик у стовпці Type першої події, що має бути **ICMPv6**.

Оскільки повідомлення починається з цієї події, є лише вихідний PDU. Який тип повідомлення вказано для ICMPv6 на вкладці OSI Model?

Зауважте, що немає адресації Рівня 2. Натисніть кнопку **Next Layer >>**, щоб отримати пояснення про процес ND (виявлення сусіда).

i. Натисніть на квадратик поряд з наступною подією в Simulation Panel. Вона повинна бути на пристрої PCA1 і мати тип NDP.

Що змінилося в адресації Рівня 3?

Які адреси Рівня 2 показано?

## 9.3.5. Питання для самоперевірки - Виявлення сусіда

1. Які два повідомлення ICMPv6 використовуються в SLAAC?

- [ ] Анонсування сусіда (Neighbor Advertisement)
- [ ] Запит сусіда (Neighbor Solicitation)
- [ ] Анонсування маршрутизатора (Router Advertisement)
- [ ] Запит маршрутизатора (Router Solicitation)

2. Які два повідомлення ICMPv6 використовуються для визначення MAC-адреси для відомої адреси IPv6?

- [ ] Анонсування сусіда (Neighbor Advertisement)
- [ ] Запит сусіда (Neighbor Solicitation)
- [ ] Анонсування маршрутизатора (Router Advertisement)
- [ ] Запит маршрутизатора (Router Solicitation)

3. На який тип адреси надсилаються повідомлення запиту сусіда ICMPv6?

- ◯ індивідуальна розсилка (unicast)
- ◯ групова розсилка (multicast)
- ◯ широкомовна розсилка (broadcast)

1. Які два повідомлення ICMPv6 використовуються в SLAAC?

Правильно!

- [ ] Анонсування сусіда (Neighbor Advertisement)
- [ ] Запит сусіда (Neighbor Solicitation)
- [x] Анонсування маршрутизатора (Router Advertisement)
- [x] Запит маршрутизатора (Router Solicitation)

2. Які два повідомлення ICMPv6 використовуються для визначення MAC-адреси для відомої адреси IPv6?

Правильно!

- [x] Анонсування сусіда (Neighbor Advertisement)
- [x] Запит сусіда (Neighbor Solicitation)
- [ ] Анонсування маршрутизатора (Router Advertisement)
- [ ] Запит маршрутизатора (Router Solicitation)

3. На який тип адреси надсилаються повідомлення запиту сусіда ICMPv6?

Правильно!

- ( ) індивідуальна розсилка (unicast)
- (•) групова розсилка (multicast)
- ( ) широкомовна розсилка (broadcast)

## 9.4. Контрольна

# 9.4.1. Що ми вивчили у цьому розділі?

**MAC- та IP-адреси**

Фізичні адреси Рівня 2 (тобто, MAC-адреси Ethernet) використовуються для передачі кадра канального рівня, інкапсульованого в IP-пакет, від однієї мережної карти до іншої в одній мережі. Якщо IP-адреса призначення знаходиться у тій самій мережі, тоді MAC-адресою призначення буде адреса пристрою призначення. Якщо IP-адреса (IPv4 чи IPv6) призначення знаходиться у віддаленій мережі, MAC-адресою призначення буде адреса шлюзу за замовчуванням (тобто інтерфейсу маршрутизатора). Уздовж кожного сегменту шляху IP-пакет інкапсулюється у кадр. Кадр є специфічним для технології канального рівня, пов'язаної з цим каналом, наприклад Ethernet. Якщо пристрій наступного переходу є кінцевим пунктом призначення, MAC-адресою призначення буде

адреса мережного адаптера Ethernet цього пристрою. Як IP-адреси пакетів у потоці даних пов'язуються з MAC-адресами на кожній ділянці шляху до пункту призначення? Для пакетів IPv4 це здійснюється процесом, який називається протоколом визначення адрес або ARP (Address Resolution Protocol). Для пакетів IPv6 - це процес виявлення сусіда або ND (Neighbor Discovery) протоколу ICMPv6 .

**ARP**

Кожен IP-пристрій у мережі Ethernet має унікальну MAC-адресу Ethernet. Коли пристрій надсилає кадр Ethernet Рівня 2, він містить дві адреси: MAC-адресу призначення та MAC-адресу джерела. Пристрій використовує ARP для визначення MAC-адреси призначення локального пристрою, коли відома його IPv4-адреса. ARP забезпечує дві основні функції: зіставлення IPv4-адрес до MAC-адрес і ведення таблиці відповідності IPv4-адрес до MAC-адрес. ARP-запит інкапсулюється в кадр Ethernet, використовуючи наступну інформацію заголовка: MAC-адреси джерела і призначення та тип. Лише один пристрій у локальній мережі матиме IPv4-адресу, що збігається із цільовою IPv4-адресою у запиті ARP. Всі інші пристрої не відповідатимуть. ARP-відповідь містить ті самі поля заголовка, що й запит. Лише пристрій, який надіслав ARP-запит, отримає ARP-відповідь на свою індивідуальну адресу (unicast ARP reply). Після отримання ARP-відповіді, пристрій додасть IPv4-адресу та відповідну їй MAC-адресу до своєї ARP-таблиці. Якщо IPv4-адреса призначення належить іншій мережі, пристрій джерела має надіслати кадр до шлюзу за замовчуванням. Ним є інтерфейс локального маршрутизатора. На кожному пристрої є таймер ARP-кешу, який видаляє з таблиці ARP записи, що не використовувались протягом зазначеного періоду часу. Також можна використовувати команди для видалення деяких або всіх записів з ARP-таблиці вручну. Оскільки ARP-запит є кадром широкомовної трансляції, то його отримують та обробляють всі пристрої в локальній мережі, що може призвести до сповільнення роботи мережі. Зловмисник може використовувати ARP-spoofing (підміну) для здійснення атаки "отруєння" ARP (підробки ARP-кешу).

**Виявлення сусіда**

IPv6 не використовує ARP, він використовує протокол ND для визначення MAC-адрес. ND забезпечує зіставлення адрес, виявлення маршрутизатора та послуги переспрямування для IPv6 за допомогою ICMPv6. ND протоколу ICMPv6 використовує п'ять повідомлень ICMPv6 для виконання цих послуг: запит сусіда, анонсування сусіда, запит маршрутизатора, анонсування маршрутизатора та перенаправлення. Подібно до ARP для IPv4, пристрої IPv6 використовують ND протоколу IPv6 для визначення MAC-адреси пристрою за відомою адресою IPv6.

## 9.4.2. **Контрольна робота з розділу — Визначення адрес**

1. Який компонент маршрутизатора містить таблицю маршрутизації, ARP-кеш і запущений файл конфігурації?

- ◯ Енергонезалежна пам'ять (NVRAM)
- ◯ Флеш-пам'ять (flash)
- ◯ ОЗП (RAM)
- ◯ ПЗП (ROM)

2. Який тип інформації міститься у таблиці ARP?

- ◯ порти комутатора, пов'язані з MAC-адресами призначення
- ◯ маршрути до мереж призначення
- ◯ відповідність IP-адреси до MAC-адреси
- ◯ зіставлення доменного імені та IP-адреси

3. PC налаштований на отримання IP-адреси автоматично з мережі 192.168.1.0/24. Адміністратор мережі вводить команду **arp –a** і помічає запис 192.168.1.255 ff-ff-ff-ff-ff-ff. Яке твердження описує цей запис?

- ◯ Цей запис стосується самого ПК.
- ◯ Це запис маршруту до шлюзу за замовчуванням.
- ◯ Це запис статичного маршруту.
- ◯ Це запис динамічного маршруту.

4. Аналітик з питань кібербезпеки вважає, що нападник підробляє MAC-адресу шлюзу за замовчуванням для здійснення атаки "людина посередині". Яку команду слід використати аналітику аби перевірити, яку MAC-адресу використовує хост при зверненні до шлюзу за замовчуванням?

- ◯ **ipconfig /all**
- ◯ **route print**
- ◯ **netstat -r**
- ◯ **arp -a**

5. Що робитиме комутатор Рівня 2, коли MAC-адреси призначення отриманого кадру немає в ARP-таблиці?

- ◯ Він пересилає кадр з усіх портів, крім порту, з якого було отримано кадр.
- ◯ Він сповіщає хоста-відправника, що кадр не може бути доставлений.
- ◯ Він транслює кадр з усіх портів комутатора.
- ◯ Він ініціює ARP-запит.

6. Яку з функцій виконує ARP?

- ☐ echo request
- ☐ перетворення MAC-адрес на IPv4-адреси
- ☐ перетворення IPv4-адрес  на MAC-адреси
- ☐ перетворення MAC-адрес на адреси портів
- ☐ перетворення адрес портів на MAC-адреси

7. Як процес ARP використовує IP-адресу?

- для визначення MAC-адреси віддаленого вузла призначення
- для визначення кількості часу, який займає подорож пакету від джерела до місця призначення
- для визначення MAC-адреси пристрою в одній мережі
- для визначення номера мережі на основі кількості бітів в IP-адресі

8. Яку з функцій виконує протокол ARP?

- автоматичне отримання IPv4-адреси
- перетворення IPv4-адреси на MAC-адресу
- відображає відповідність доменного імені до його IP-адреси
- ведення таблиці доменних імен з їх відповідними IP-адресами

9. Що робить комутатор Рівня 2, коли отримує кадр широкомовної розсилки Рівня 2?

- Він відправляє кадр на всі порти, які зареєстровані для широкомовних трансляцій.
- Він відкидає кадр..
- Він відправляє кадр на всі порти, окрім порту, з якого він отримав кадр.
- Він відправляє кадр на всі порти.

10. Які адреси зіставляються за допомогою ARP?

- MAC-адреса призначення з IPv4-адресою призначення
- IPv4-адреса призначення з іменем хоста призначення
- IPv4-адреса призначення з MAC-адресою джерела
- MAC-адреса призначення з IPv4-адресою джерела

11. Коли IP-пакет надсилається на хост у віддаленій мережі, яку інформацію надає ARP?

- MAC-адресу порту комутатора, який під'єднано до вузла-відправника
- IP-адресу хоста призначення
- MAC-адресу інтерфейсу маршрутизатора, найближчого до хоста-відправника
- IP-адресу шлюзу за замовчуванням

12. Відповідність яких двох типів адрес відображає ARP-таблиця комутатора?

- Адреси Рівня 3 до адреси Рівня 2
- Адреси Рівня 2 до адреси Рівня 4
- Адреси Рівня 4 до адреси Рівня 2
- Адреси Рівня 3 до адреси Рівня 4

13. Яке призначення ARP в мережі IPv4?

- подальше пересилання даних на основі IP-адреси призначення
- подальше пересилання даних на основі MAC-адреси призначення
- побудова таблиці MAC-адрес комутатора на основі інформації, яка збирається
- отримання конкретної MAC-адреси, коли відома IP-адреса

14. Яка адреса призначення використовується в кадрі ARP-запиту?

- 0.0.0.0
- 127.0.0.1
- 255.255.255.255
- FFFF.FFFF.FFFF
- 01-00-5E-00-AA-23