

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ  
УНІВЕРСИТЕТ "ЛЬВІВСЬКА ПОЛІТЕХНІКА"**

**ІКНІ**  
Кафедра ПЗ



**ЗВІТ**

До лабораторної роботи №9

**на тему:** “Налаштування протоколу IP в Windows XP, дослідження роботи протоколу ARP.”

**з дисципліни:** “Організація комп’ютерних мереж”

**Лектор:**  
доцент кафедри ПЗ  
Крук О.Г.

**Виконав:**  
студент групи ПЗ-24  
Губик А. С.

**Прийняв:**  
доцент кафедри ПЗ  
Задорожний І. М.

**Тема роботи:** Налаштування протоколу IP в Windows XP, дослідження роботи протоколу ARP.

**Мета роботи:** Ознайомитися із засобами перевірки та налаштування протоколів TCP/IP та ARP.

### Індивідуальне завдання

1. Відвідати сторінку [whatismyip.com](http://whatismyip.com), за допомогою якої дізнатися свою IP-адресу. З командного рядка виконати команду `ipconfig` (яка виводить IP-адресу). Зіставити IP-адреси, одержані зазначеними двома способами. У висновку дати пояснення результату зіставлення.
2. Відвідати сторінку [speedtest.net](http://speedtest.net). Вибрати на карті точку світу для встановлення з'єднання з одним з серверів у ній. У звіті відобразити фрагмент екранного знімка сторінки, де містяться дані про швидкість виконання процедури `ping` та передавання і прийому даних.
3. З командного рядка виконати команду `ipconfig` з параметром `/all`. Результати подати у звіті.
4. З командного рядка виконати спочатку команду `ipconfig` з параметром `/displaydns`, а тоді – з параметром `/flushdns`. Результати подати у звіті. У висновку пояснити одержані результати.
5. З командного рядка виконати команду `ipconfig` з параметром `/flushdns`. Результати подати у звіті.
6. Виконати команду `ipconfig` з параметрами `/renew` та `/release`. Результати прокоментувати у висновку.
7. З командного рядка виконати команду `arp`.
8. З сайту Wireshark завантажити версію цього програмного продукту, що не потребує інсталяції.
9. Налаштувавши необхідний мінімум параметрів, запустити процес перехоплення мережевого трафіка. Поспостерігати за процесом протягом декількох хвилин. Відфільтрувати пакети, передані за протоколом ARP. Виписати у звіт декілька рядків таблиці з описом перехоплених пакетів.
10. Відмінити попередній фільтр. Знаючи свою IP-адресу, відфільтрувати дані лише про пакети, передані з цієї адреси або ж прийняті на цю адресу.
11. Знайти HTTP-запит і детально розглянути його.

## Теоретичні відомості

Wireshark є вільно поширюваним аналізатором протоколів – програмним продуктом, що дозволяє дізнатися, які пакети «подорожують» мережним кабелем. Wireshark може використовуватися спеціалістами для ряду задач, зокрема, дослідження проблем безпеки в мережі, відлагодження реалізацій протоколів, усунення проблем з мережею тощо. Пересічні користувачі можуть застосовувати WireShark для вивчення мережевих протоколів. Слід зазначити, що Wireshark лише «вловлює» пакети, що надходять з мережі, однак сам пакетів в мережу не надсилає. Крім того, Wireshark не сигналізує про втручання в систему, хоча може допомогти помітити підозрілі речі. Щоб почати “відловлювати” пакети, потрібно виконати наступне: 1. Вибрати необхідне зі списку активних мережевих адаптерів (Interface List); 2. Налаштувати необхідні параметри перехоплення пакетів (Capture Options для виклику відповідного діалогу); 3. Власне, запустити процес перехоплення (Start capture on interface). Слід у діалоговому вікні “Capture Options” відмітити прапорець “Capture packets in promiscuous mode” – для захоплення пакетів в режимі прийому всіх мережевих пакетів. Для оновлення списку захоплених пакетів у реальному часі слід відмітити прапорець Update list in real time. Для відображення лише тих пакетів, що відповідають певній умові, застосовують фільтри. Наприклад, щоб вибрати лише пакети, передані за протоколом ARP, слід у полі Filter набрати `arp` (малими латинськими літерами, див. рис. 1). Для відміни дії фільтра слід натиснути кнопку Clear. Кожне поле в таблиці опису пакетів може брати участь у фільтруванні. Для побудови складніших фільтрів використовують вирази. Вирази утворюють за допомогою операторів порівняння та логічних операторів. Оператори порівняння: `==` (eq), `!=` (ne), `>` (gt), `<` (lt), `>=` (ge), `<=` (le). Наприклад, `ip.src != 10.0.0.5` означає умову, при якій IP-адреса відправника повідомлення не повинна бути 10.0.0.5. Логічні оператори: `(and)`, `||` (or), `'(xor)`, `!` (not). Для задавання фільтрів зручно користуватися діалогом, що появляється при натисненні Expression. Рис. 1

1.2. Команда `ipconfig` Команда `ipconfig` служить для відображення всіх поточних параметрів мережі TCP/IP та оновлення параметрів DNS і DHCP. Для застосування `ipconfig` необхідно з командного рядка (виклик якого здійснюємо так: Start => Run => cmd) задати слово `ipconfig` і (опційно) один з розглянутих нижче параметрів. 1. `ipconfig` без жодних параметрів дозволяє дізнатися IP-адресу, маску підмережі та основний шлюз для кожного адаптера (рис. 2). 2. `ipconfig /all` виводить повну конфігурацію TCP/IP для всіх адаптерів. 3. `ipconfig /displaydns` відображає вміст кеша зіставлення імен DNS, що включає записи, завантажені з локального файлу `hosts`, та останні записи ресурсів для запитів на зіставлення імен (цю інформацію служба DNS застосовує для швидкого зіставлення часто запитуваних імен без звертання до DNS-серверів); приклад команди показаний на рис 3. 4. `ipconfig /flushdns` очищає кеш зіставлення імен DNS клієнта. 5. `ipconfig /registerdns` служить для динамічної реєстрації вручну DNS і IP-адрес, налаштованих на комп'ютері. 6. `ipconfig /renew [адаптер]` служить для оновлення конфігурації DHCP для конкретного адаптера, якщо він заданий, а інакше – для всіх адаптерів. Цей параметр доступний лише для комп'ютерів з адаптерами, налаштованими для автоматичного одержання IP-адрес. 7. `ipconfig /release [адаптер]` служить для відправлення повідомлення DHCPRELEASE серверу DHCP для очищення поточної конфігурації DHCP та видалення конфігурації IP-адрес для всіх адаптерів або ж конкретного заданого адаптера.

## Хід роботи

### 1. Перша програма

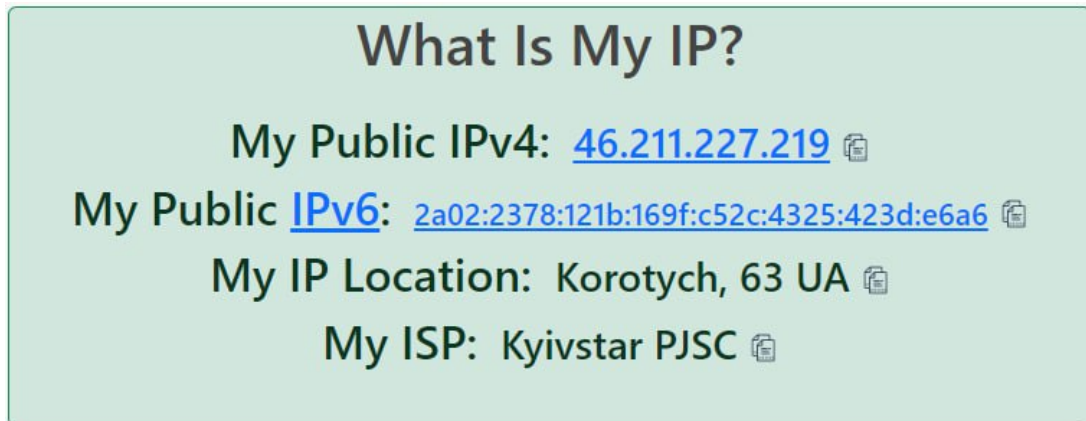


Рис. 1: Публічний IP

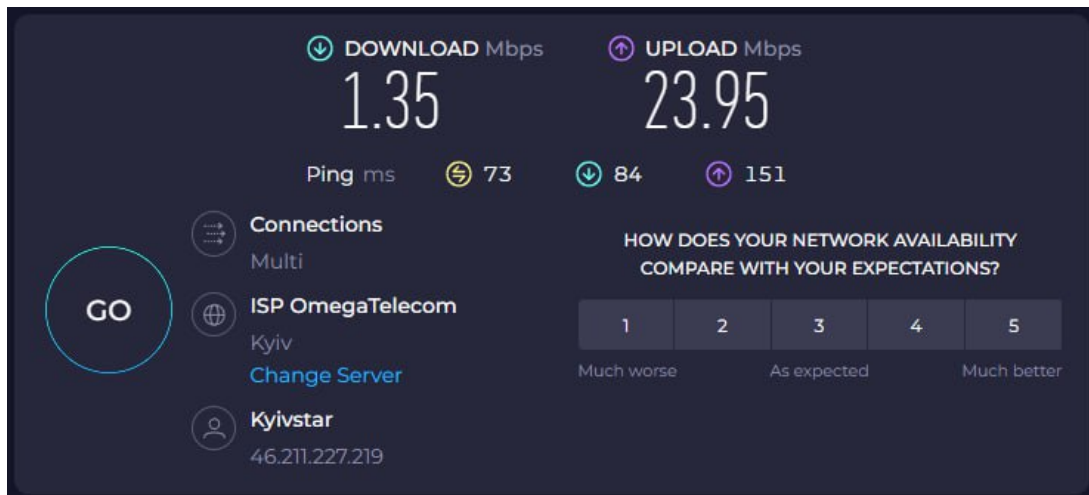


Рис. 2: Швидкість мобільного інтернету в лекційній аудиторії

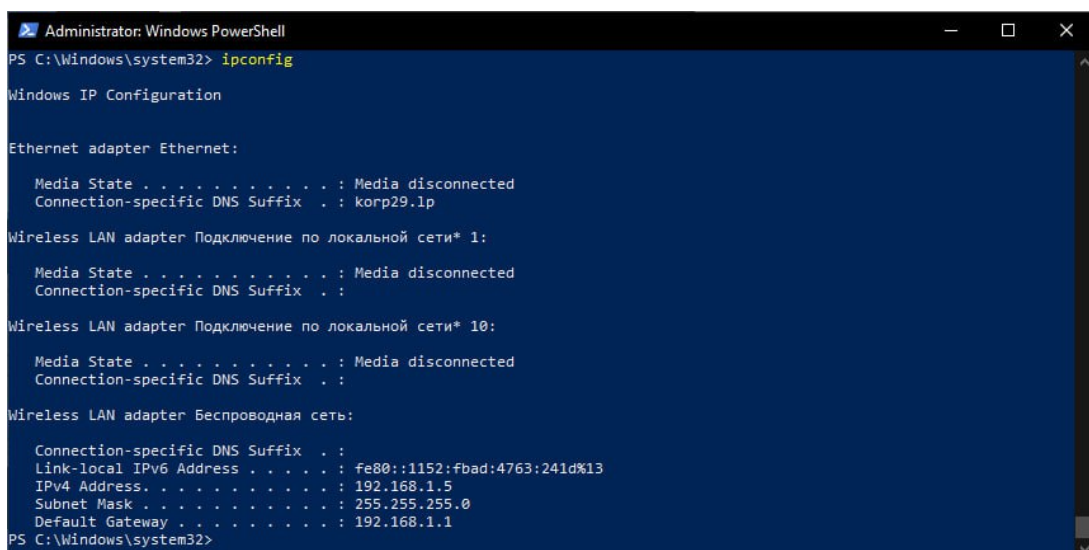


Рис. 3:

```
Administrator: Windows PowerShell
PS C:\Windows\system32> ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-UHR0B21
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : korp29.lp
Description . . . . . : Realtek PCIe GbE Family Controller
Physical Address. . . . . : C0-18-50-6B-C9-45
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Подключение по локальной сети* 1:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 7C-70-DB-5D-C9-84
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Подключение по локальной сети* 10:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
Physical Address. . . . . : 7E-70-DB-5D-C9-83
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Беспроводная сеть:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) Wi-Fi 6 AX200 160MHz
Physical Address. . . . . : 7C-70-DB-5D-C9-83
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::1152:fbad:4763:241d%13(Preferred)
IPv4 Address. . . . . : 192.168.1.5(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, November 20, 2023 6:35:59 PM
Lease Expires . . . . . : Monday, November 20, 2023 8:36:00 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 108818651
DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-D4-45-DF-C0-18-50-6B-C9-45
DNS Servers . . . . . : 192.168.0.27
                        8.8.8.8
                        192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
PS C:\Windows\system32>
```

Рис. 4:

```
Administrator: Windows PowerShell
PS C:\Windows\system32> ipconfig /displaydns

Windows IP Configuration

edged1.me.gvt1.com
-----
Record Name . . . . . : edged1.me.gvt1.com
Record Type . . . . . : 1
Time To Live . . . . . : 674
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 34.104.35.123

www.wireshark.org
-----
Record Name . . . . . : www.wireshark.org
Record Type . . . . . : 1
Time To Live . . . . . : 1007
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 104.26.11.240

Record Name . . . . . : www.wireshark.org
Record Type . . . . . : 1
Time To Live . . . . . : 1007
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 104.26.10.240

Record Name . . . . . : www.wireshark.org
Record Type . . . . . : 1
Time To Live . . . . . : 1007
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 172.67.75.39

account-public-service-prod03.ol.epicgames.com
-----
Record Name . . . . . : account-public-service-prod03.ol.epicgames.com
Record Type . . . . . : 1
Time To Live . . . . . : 1121
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 3.227.155.128

Record Name . . . . . : account-public-service-prod03.ol.epicgames.com
Record Type . . . . . : 1
Time To Live . . . . . : 1121
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . . : 3.234.8.69
```

Рис. 5:

```
Administrator: Windows PowerShell
PS C:\Windows\system32> ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
PS C:\Windows\system32> ipconfig /displaydns

Windows IP Configuration

PS C:\Windows\system32>
```

Рис. 6:

```
Administrator: Windows PowerShell
PS C:\Windows\system32> ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Подключение по локальной сети* 1 while it has its media disconnected.
No operation can be performed on Подключение по локальной сети* 10 while it has its media disconnected.

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : korp29.lp

Wireless LAN adapter Подключение по локальной сети* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Подключение по локальной сети* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Беспроводная сеть:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::1152:fbad:4763:241d%13
    IPv4 Address. . . . . : 192.168.1.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
PS C:\Windows\system32>
```

Рис. 7:

```
Administrator: Windows PowerShell
PS C:\Windows\system32> ipconfig /release

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Подключение по локальной сети* 1 while it has its media disconnected.
No operation can be performed on Подключение по локальной сети* 10 while it has its media disconnected.

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : korp29.lp

Wireless LAN adapter Подключение по локальной сети* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Подключение по локальной сети* 10:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Беспроводная сеть:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::1152:fbad:4763:241d%13
    Default Gateway . . . . . :
PS C:\Windows\system32>
```

Рис. 8:



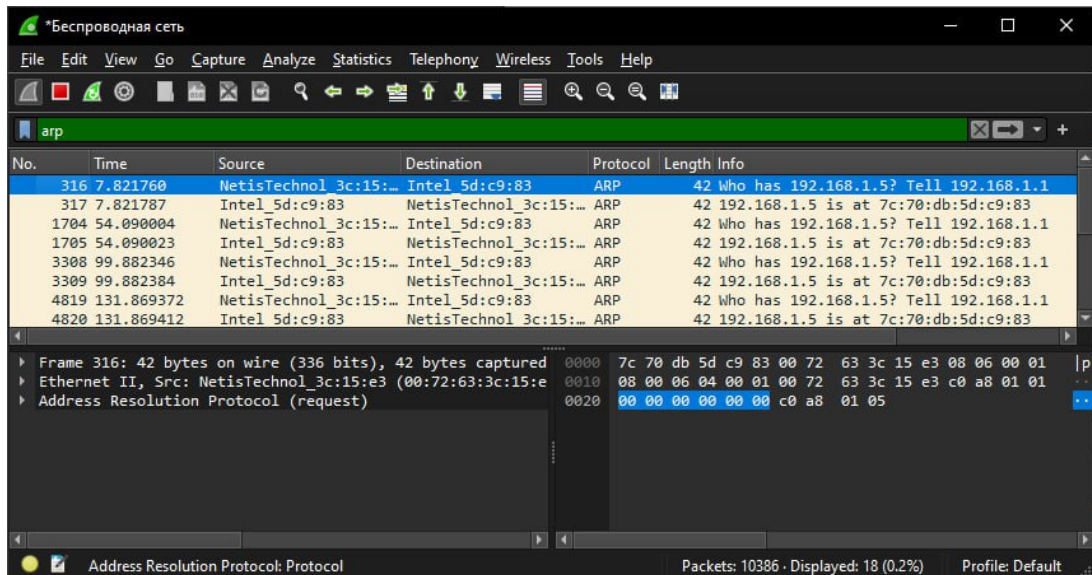


Рис. 9:

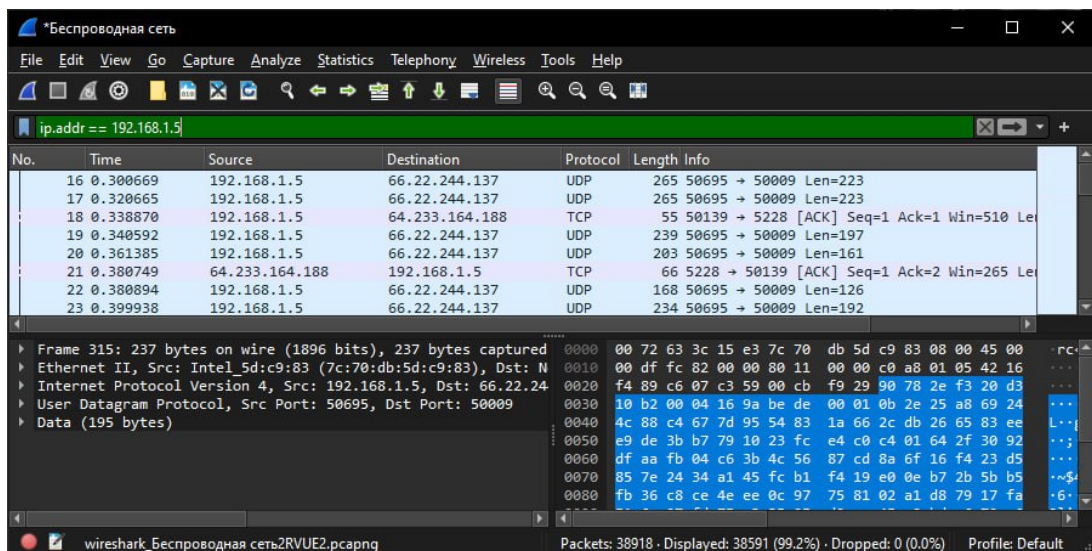


Рис. 10:

## Висновок

Я навчився як можна дізнатись свою публічну і локальну IP-адресу, що таке ARP протокол і як подивитись ARP-таблицю, як користуватись Wireshark і фільтрувати пакети за допомогою нього.