

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

**Інститут КНІТ
Кафедра ПЗ**

ЗВІТ

До лабораторної роботи № 1

З дисципліни: “Організація комп’ютерних мереж”

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

Лектор:

викл. каф. ПЗ
Задорожний І. М.

Виконав:

ст. гр. ПЗ-22
Чаус Олег

Прийняв:

викл. каф. ПЗ
Задорожний І. М.

« ____ » _____ 2023 р.

Σ= ____ .

Львів – 2023

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.

ТЕОРЕТИЧНІ ВІДОМОСТІ

1. Яке основне призначення Wireshark?

Основним призначенням Wireshark є збір і аналіз мережевих пакетів, що передаються через мережу. Він дозволяє користувачам переглядати і аналізувати дані, які передаються між комп'ютерами в режимі реального часу або з використанням збережених файлів.

2. Як відобразити лише дані про пакети, передані за протоколом http або tcp або udp?

Потрібно ввести фільтр “http or tcp or udp”.

3. Який принцип роботи протоколу ARP?

Система-відправник запитує фізичну адресу системи-одержувача через ARP-запит. Але спочатку мережевий стек “пробує пошукати” потрібну йому адресу у кеші ARP. Якщо потрібні дані відсутні у кеші ARP, то формується широкомовний (broadcast) запит ARP. Це означає, що усім вузлам в мережі надсилають запитання про те, яку фізичну адресу має вузол із даною IP-адресою. Коли одержувач з цією IP-адресою отримає цей запит, він зобов'язаний відповісти, що це його адреса, і повідомити свою фізичну адресу. Після цього буде оновлений ARP-кеш відправника і надіслана потрібна інформація одержувачу.

ЗАВДАННЯ

1. Ознайомтеся з теоретичними відомостями.
2. Використовуючи алгоритм, для тестування з'єднання з віддаленим сервером, протестуйте з'єднання з іншим ПК в локальній мережі і перехопіть ICMP- запити і відгуки в програмі Wireshark. Перевірте, чи правильно Ви визначили власну MAC-адресу та MAC-адресу іншого студента (знайдіть необхідну інформацію в зібраних кадрах).
3. Відправте ехо-запити на віддалені вузли (варіант відповідає номеру студента в журналі), проаналізуйте дані сформовані цими запитами в програмі Wireshark. Визначте відмінності між цими даними і даними отриманими для локальної мережі.

13	www.president.gov.ua	www.intel.com
----	----------------------	---------------

4. Випробуйте всі параметри команди ping (в яких комбінаціях перевіряти параметри – це залишається на розсуд виконавця). Прочитайте інформацію про IP-пакети, перехоплені аналізатором протоколів Wireshark і

переконайтеся в розумінні значень всіх полів IP-пакета. Для кожної випробуваної комбінації параметрів дослідіть структуру перехопленого IP-пакета. У звіті відобразіть екранні знімки всіх спроб виконати ping та вміст IP—пакетів, відповідних цим спробам. Якщо команда ping була неуспішною (не було відповіді на запит), з'ясуйте причину цього.

5. З використанням параметра -l утиліт ping дослідити фрагментацію IP-пакетів шляхом вказання в полі size розміру більшого за MTU даної мережі (для Ethernet більше 1600 байт).
6. Перевірте можливість з'єднання (згідно варіанту) до віддаленого серверу двома засобами для трасування маршруту: утилітою tracert та програмою VisualRoute. Порівняйте та поясніть результати трасування. Випробуйте всі параметри команди tracert і проаналізуйте дані IP-пакета у Wireshark, відобразивши результати у звіті.
7. Визначте адреси інтерфейсів проміжних маршрутизаторів за допомогою опцій IP-протоколу (використайте утиліту ping з параметром -r). Порівняйте результат з даними, отриманими за допомогою утиліти tracert.
8. Самостійно знайдіть детальну інформацію про всі типи ICMP-пакетів (підказка: документ RFC), дослідіть структуру перехоплених аналізатором протоколів пакетів і визначте тип кожного з досліджених пакетів.
9. Самостійно знайдіть відповідь на одне з наступних запитань (варіант запитання відповідає номеру студента в журналі) та представте цю відповідь звіті:

13) Які операційні системи належать до мережевих?

10. Сформууйте звіт зі структурою, аналогічною до звіту з лабораторної роботи No1. У теоретичних відомостях слід дати відповіді на 3 вибрані викладачем запитання з числа контрольних запитань. У висновку слід подати результати осмислення одержаних результатів, опис неуспішних спроб виконання команд ping і tracert та пояснення причин.

ХІД ВИКОНАННЯ

Спочатку протестував з'єднання з іншим ПК у локальній мережі використовуючи алгоритм для тестування з'єднання з віддаленим сервером.

```
Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::a44f:493:70e5:4cf1%19
IPv4 Address. . . . . : 192.168.88.20
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.88.1
```

Рис. 1. Результат виконання команди ipconfig.

```

C:\Users\Oleh>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

Рис. 2. Результат з'єднання зі собою ж.

```

C:\Users\Oleh>ping 192.168.88.20

Pinging 192.168.88.20 with 32 bytes of data:
Reply from 192.168.88.20: bytes=32 time<1ms TTL=128
Reply from 192.168.88.20: bytes=32 time<1ms TTL=128
Reply from 192.168.88.20: bytes=32 time<1ms TTL=128
Reply from 192.168.88.20: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.88.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

Рис. 3. Результат з'єднання зі своєю IP-адресою.

```

C:\Users\Oleh>ping 192.168.88.1

Pinging 192.168.88.1 with 32 bytes of data:
Reply from 192.168.88.1: bytes=32 time<1ms TTL=64
Reply from 192.168.88.1: bytes=32 time<1ms TTL=64
Reply from 192.168.88.1: bytes=32 time<1ms TTL=64
Reply from 192.168.88.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.88.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

Рис. 4. Результат з'єднання зі шлюзом.

```

C:\Users\Oleh>ping 192.168.88.19

Pinging 192.168.88.19 with 32 bytes of data:
Reply from 192.168.88.19: bytes=32 time=20ms TTL=64
Reply from 192.168.88.19: bytes=32 time=48ms TTL=64
Reply from 192.168.88.19: bytes=32 time=299ms TTL=64
Reply from 192.168.88.19: bytes=32 time=135ms TTL=64

Ping statistics for 192.168.88.19:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 299ms, Average = 125ms

```

Рис. 5. Результат з'єднання з віддаленим вузлом.

62200	124.186338	192.168.88.20	192.168.88.19	ICMP	74 Echo (ping) request	id=0x0001, seq=70/17920, ttl=128 (reply in 62224)
62224	124.206854	192.168.88.19	192.168.88.20	ICMP	74 Echo (ping) reply	id=0x0001, seq=70/17920, ttl=64 (request in 62200)
63219	125.189084	192.168.88.20	192.168.88.19	ICMP	74 Echo (ping) request	id=0x0001, seq=71/18176, ttl=128 (reply in 63365)
63365	125.237098	192.168.88.19	192.168.88.20	ICMP	74 Echo (ping) reply	id=0x0001, seq=71/18176, ttl=64 (request in 63219)
63904	126.190982	192.168.88.20	192.168.88.19	ICMP	74 Echo (ping) request	id=0x0001, seq=72/18432, ttl=128 (reply in 64086)
64086	126.490432	192.168.88.19	192.168.88.20	ICMP	74 Echo (ping) reply	id=0x0001, seq=72/18432, ttl=64 (request in 63904)
64543	127.193893	192.168.88.20	192.168.88.19	ICMP	74 Echo (ping) request	id=0x0001, seq=73/18688, ttl=128 (reply in 64632)
64632	127.329180	192.168.88.19	192.168.88.20	ICMP	74 Echo (ping) reply	id=0x0001, seq=73/18688, ttl=64 (request in 64543)

Рис. 6. Перехоплені пакети у Wireshark.

```

DNS Servers . . . . . : 192.168.88.1
                        193.104.85.10
                        193.104.85.11
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\0leh>ping 192.168.88.1

Pinging 192.168.88.1 with 32 bytes of data:
Reply from 192.168.88.1: bytes=32 time=1ms TTL=64
Reply from 192.168.88.1: bytes=32 time<1ms TTL=64
Reply from 192.168.88.1: bytes=32 time<1ms TTL=64
Reply from 192.168.88.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.88.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

Рис. 7. Результат з'єднання з DNS-сервером.

Відправив ехо-запити на віддалені вузли згідно зі своїм варіантом.

```

C:\Users\0leh>ping www.president.gov.ua

Pinging e132601.a.akamaiedge.net [96.16.54.113] with 32 bytes of data:
Reply from 96.16.54.113: bytes=32 time=24ms TTL=57
Reply from 96.16.54.113: bytes=32 time=24ms TTL=57
Reply from 96.16.54.113: bytes=32 time=24ms TTL=57
Reply from 96.16.54.113: bytes=32 time=24ms TTL=57

Ping statistics for 96.16.54.113:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 24ms, Maximum = 24ms, Average = 24ms

```

Рис. 8. Результат з'єднання з сервером www.president.gov.ua

4720...	611.878531	192.168.88.20	96.16.54.113	ICMP	74 Echo (ping) request	id=0x0001, seq=78/19968, ttl=128 (reply in 472138)
4721...	611.902800	96.16.54.113	192.168.88.20	ICMP	74 Echo (ping) reply	id=0x0001, seq=78/19968, ttl=57 (request in 472017)
4749...	612.880685	192.168.88.20	96.16.54.113	ICMP	74 Echo (ping) request	id=0x0001, seq=79/20224, ttl=128 (reply in 475051)
4750...	612.904823	96.16.54.113	192.168.88.20	ICMP	74 Echo (ping) reply	id=0x0001, seq=79/20224, ttl=57 (request in 474936)
4777...	613.882592	192.168.88.20	96.16.54.113	ICMP	74 Echo (ping) request	id=0x0001, seq=80/20480, ttl=128 (reply in 477745)
4777...	613.906565	96.16.54.113	192.168.88.20	ICMP	74 Echo (ping) reply	id=0x0001, seq=80/20480, ttl=57 (request in 477744)
4798...	614.884512	192.168.88.20	96.16.54.113	ICMP	74 Echo (ping) request	id=0x0001, seq=81/20736, ttl=128 (reply in 479875)
4798...	614.909424	96.16.54.113	192.168.88.20	ICMP	74 Echo (ping) reply	id=0x0001, seq=81/20736, ttl=57 (request in 479800)

Рис. 9. Перехоплені пакети у Wireshark.

```

c4 ad 34 4d 41 3f 04 7c 16 19 ab cb 08 00 45 00  ..4MA?..|.....E.
00 3c 83 5a 00 00 80 01 08 29 c0 a8 58 14 60 10  <..Z....)....X..
36 71 08 00 4d 0d 00 01 00 4e 61 62 63 64 65 66  6q..M....Nabcdf
67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
77 61 62 63 64 65 66 67 68 69                    wabcdfgh hi

```

Рис. 10. Вміст ехо-запиту.

Вміст ехо запитів та запитів до www.president.gov.ua є однаковим, якщо не брати до уваги гедери, які різні у різних запитах.

```
C:\Users\Oleh>ping www.intel.com

Pinging e7842.dsca.akamaiedge.net [104.87.182.18] with 32 bytes of data:
Reply from 104.87.182.18: bytes=32 time=24ms TTL=57
Reply from 104.87.182.18: bytes=32 time=23ms TTL=57
Reply from 104.87.182.18: bytes=32 time=24ms TTL=57
Reply from 104.87.182.18: bytes=32 time=24ms TTL=57

Ping statistics for 104.87.182.18:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 24ms, Average = 23ms
```

Рис. 11. Результат з'єднання зі сервером www.intel.com

8641...	1047.035209	192.168.88.20	104.87.182.18	ICMP	74 Echo (ping) request	id=0x0001, seq=82/20992, ttl=128 (reply in 864118)
8641...	1047.059225	104.87.182.18	192.168.88.20	ICMP	74 Echo (ping) reply	id=0x0001, seq=82/20992, ttl=57 (request in 864108)
8646...	1048.037026	192.168.88.20	104.87.182.18	ICMP	74 Echo (ping) request	id=0x0001, seq=83/21248, ttl=128 (reply in 864631)
8646...	1048.060883	104.87.182.18	192.168.88.20	ICMP	74 Echo (ping) reply	id=0x0001, seq=83/21248, ttl=57 (request in 864630)
8646...	1048.142327	83.99.235.23	192.168.88.20	ICMP	176 Destination unreachable (Port unreachable)	
8646...	1048.177819	109.252.158.196	192.168.88.20	ICMP	176 Destination unreachable (Port unreachable)	
8648...	1048.372862	109.252.136.69	192.168.88.20	ICMP	90 Destination unreachable (Port unreachable)	
8652...	1049.039919	192.168.88.20	104.87.182.18	ICMP	74 Echo (ping) request	id=0x0001, seq=84/21504, ttl=128 (reply in 865205)
8652...	1049.064097	104.87.182.18	192.168.88.20	ICMP	74 Echo (ping) reply	id=0x0001, seq=84/21504, ttl=57 (request in 865203)
8654...	1049.330725	116.73.125.71	192.168.88.20	ICMP	90 Destination unreachable (Port unreachable)	
8654...	1049.405528	27.5.164.39	192.168.88.20	ICMP	90 Destination unreachable (Port unreachable)	
8657...	1050.041838	192.168.88.20	104.87.182.18	ICMP	74 Echo (ping) request	id=0x0001, seq=85/21760, ttl=128 (reply in 865851)
8658...	1050.065821	104.87.182.18	192.168.88.20	ICMP	74 Echo (ping) reply	id=0x0001, seq=85/21760, ttl=57 (request in 865798)

Рис. 12. Перехоплені пакети у Wireshark.

З'єднання з віддаленими комп'ютерами було швидше, ніж з комп'ютером у локальній мережі.

РЕЗУЛЬТАТИ

// Якщо ви реалізуєте щось програмно тут повинні бути скріншоти виконання вашої програми. Якщо ні (наприклад, у 1 лабі) – цей розділ у звіт не додаєте.

ВИСНОВКИ

// Мінімум 3-4 речення, які описують, що було вивчено на лабораторній роботі (опис, переваги, недоліки, тощо) + виконано, які отримані результати, особливості виконання і т.д.