# МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**Національний університет “Львівська політехніка”**



**Інститут післядипломної освіти**

**ЗВІТ**

**Про виконання лабораторної роботи №4**

**«Дослідження роботи DNS сервера та протоколу DHCP»**

**з дисципліни «Організація комп'ютерних мереж»**

Виконав:

слухач групи ПЗС-11

Гринчук Тарас

Прийняв:

ст. викл. Тушницький Р.Б.

« »\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2014 р.

∑ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

ЛЬВІВ – 2014

**Тема роботи**: Дослідження роботи DNS сервера та протоколу DHCP.

## 1. Теоретичні відомості

Служба **DNS** **(англ. Domain Name System, DNS)** організовує імена вузлів в ієрархію доменів. Домен - це набір вузлів , в деякому розумінні пов'язаних між собою. Всі ці вузли можуть належати до однієї мережі (наприклад, всі машини, що входять до складу локальної мережі університету , або всі машини мережі BITNET), всі вони також можуть належати до однієї організації (наприклад, всі комп'ютери, що належать уряду США), нарешті, все вони можуть бути просто близько розташовані один від одного в географічному сенсі. Наприклад, всі навчальні заклади входять до складу домену edu, a кожному університету або коледжу відповідає свій субдомен (subdomain), до складу якого входять всі його комп'ютери. Університетові Гручо Маркс відповідає домен groucho.edu, а департаменту математики цього університету - math.groucho.edu. Всі комп'ютери , що входять до складу локальної мережі цього департаменту, повинні містити у своїй назві ім'я цього домену . Наприклад, повне ім'я комп'ютера erdos буде erdos.math.groucho.edu . Це ім'я називається повним доменним ім'ям (fully qualified domain name , FQDN). Воно точно ідентифікує мережний вузол в рамках всесвітньої мережі.

Залежно від розташування на дереві доменів , домен може бути доменом верхнього рівня , другого рівня або третього рівня. Іноді зустрічаються домени більш низького рівня , однак це буває рідко. Нижче ми наводимо список найбільш часто зустрічаються доменів верхнього рівня.

* edu - Освітні установи (в основному , в США ) . Наприклад , університети і т. д.;
* com - Комерційні організації і компанії;
* org - Некомерційні організації . Приватні мережі UUCP часто належать до таких доменів;
* net - Шлюзи та інші адміністративні мережеві вузли;
* mil - Військові установи;
* gov-Урядові установи;
* uucp - Всі вузли . раніше іменувалися в стандарті імен UUCP та не належать ніяким доменам , включаються до складу цього домену.

Домен (англ.domain - область**)** - частина простору ієрархічних імен мережі Інтернет, що обслуговується групою серверів доменних імен (DNS-серверів) та централізовано адмініструється. DNS-сервери зберігають інформацію про вузли, імена яких належать домену і виконують трансляцію їх імен в адреси. Кожний домен має унікальне ім'я, а кожен комп'ютер, підключений до Інтернету, має, як правило, доменне ім'я. Домени мають між собою ієрархічні відношення. Два домени, що розташовані на сусідніх рівнях ієрархії, називаються відповідно доменом вищого та нижчого рівнів. Домени найвищого (верхнього) рівня можуть бути сформовані за організаційним або географічним ознаками. Домени, сформовані за географічним ознаками, об'єднують вузли, що належать конкретній державі. За географічними ознаками об'єднуються в основному комп'ютери, що містяться на території США.

DNS-сервер - програма, призначена для відповідей на DNS-запити за відповідним протоколом. Також DNS-сервером можуть називати хост, на якому запущено відповідну програму. DNS-клієнт (від англ. Domain Name System-client — доменних імен система — клієнт) - програма або модуль в програмі, що забезпечує з'єднання із DNS-сервером для визначення IP-адреси по його доменному імені.

## 2. Хід роботи

1. За допомогою аналізатора протоколів Wireshark дослідити формат повідомлень запиту і відповіді DNS сервера.

nslookup — утиліта, що надає користувачеві інтерфейс командного рядка для звернення до системи DNS. Дозволяє задавати різні типи запитів і запрошувати довільно вказані сервери. З її допомогою відішлемо dns-запит на адресу ya.ru. Результат зображено на рис. 2.1.

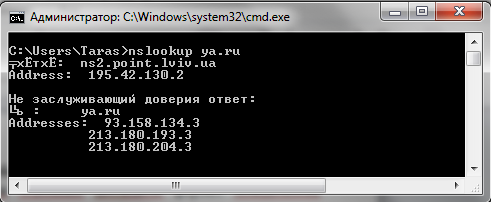


Рис. 2.1. nslookup ya.ru

Розглянемо детально пакети цих dns-запитів у аналізаторі протоколів Wireshark (рис. 2.2):

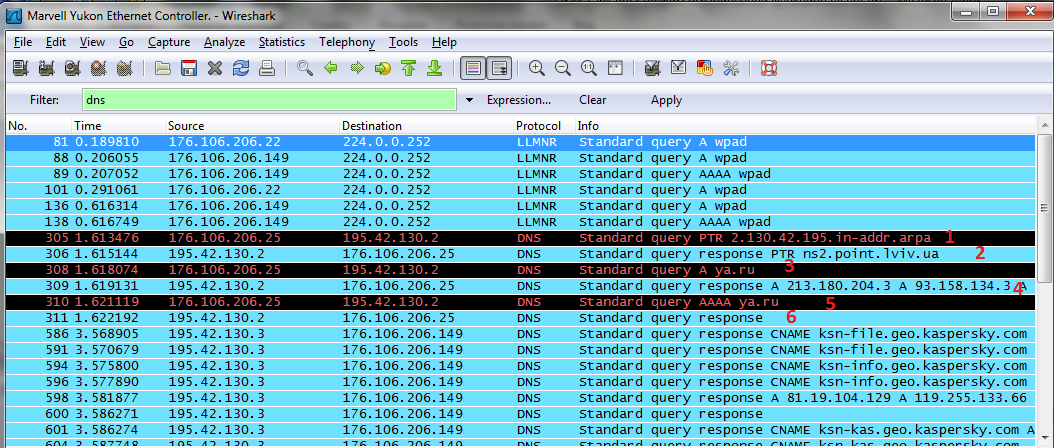
****

Рис. 2.2. вигляд dns-запитів у Wireshark

1. Запит, з ресурсним записом PTR (Domain name pointer) код 12, що реалізує механізм переадресації.
2. Відповідь DNS-сервера з записом PTR.
3. Запит у DNS-сервера з записом A ip-адреси ya.ru, тобто чи сервер "знає" щось про даний домен ya.ru.
4. У відповідь DNS-сервер надає список ip-адрес запис А домена ya.ru, з власної талиці DNS-записів.
5. Запит у DNS-сервера з записом AAAA ip-адреси ya.ru, тобто чи сервер знає щось про даний домен ya.ru в дресації IPv6.
6. Відповідь DNS-сервера на запит (5).

Розглянемо dns-запит більш детально (рис. 2.3):

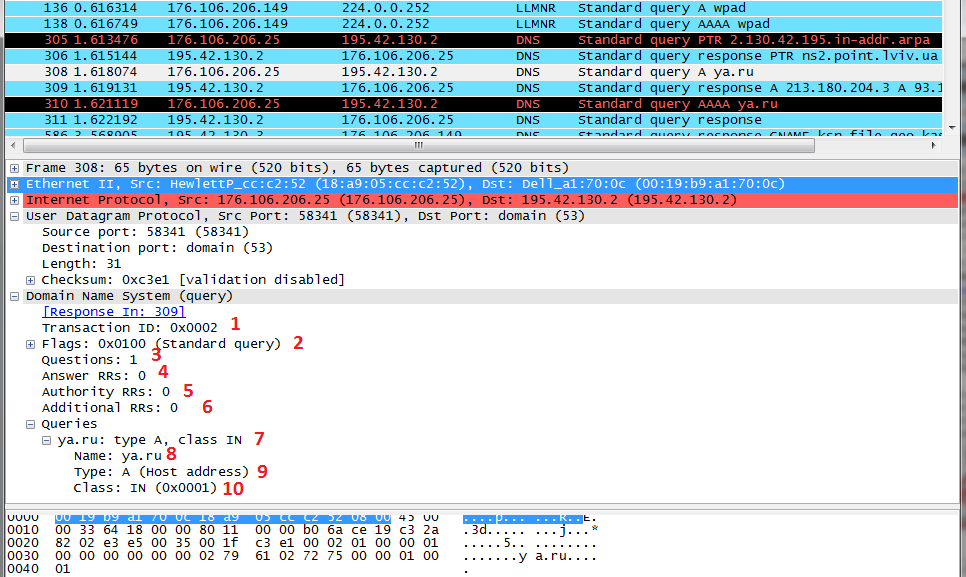


Рис. 2.3. dns-запит, докладно

1. Кожне повідомлення починається з повідомлення Індентифікація / Transaction ID, яке дозволяє зв'язати пару запит і відклик. Значення поля рівне: 0х0002 (бо це 2-й по порядку запит у DNS-сервера).
2. Прапори / Flags – це поле оприділяє поле запитуваної процедури, а також кодування відклику. Значення поля рівне: 0х0100.
3. Запити / Questions – задає число запитів в секції запитів, де записані запити на які необхідні відповіді. Значення поля рівне: 1.
4. Відповідь РРС / Answer RRs — це поля яким відповідають Тип і Клас. Якщо, будь-який з співпадаючих записів містить запис CNAME, що веде до інших записів, тоді цільові адреси також слід включати у відповідь. Значення поля рівне: 0.
5. Сервери імен / Authority Rrs – є записами NS типу, що вказують на сервери імен ближче до цільового імені в ієрархії імен. Це поле не являється обов'язковим проте клієнтам пропонується кешувати цю інформацію, якщо подальші спроби будуть направлятись в однойменній ієрархії. Значення поля рівне: 0x0000.
6. Додаткові записи / Additional RRs – це записи імені сервера які вважається можуть стати корисними клієнту. Найпоширенішим використанням для цього поля є А (адрес) запису для серверу імен, перерахованих в розділі адміністрації. Значення поля рівне: 0x0000.
7. Секція DNS-запиту.
8. Символьне ім'я домену / Name – це поле має змінну довжину, містить одне або більше субполів, що починаються з байта довжини (0-63). Поле завершується 0. Значення поля рівне: ya.ru.
9. Тип і код запиту / Type - поле тип запиту характеризує різновид запиту: Наприклад A – ір-адрес(1), NS-сервер імен(2), CNAME- канонічне ім'я (5), MX - запис про поштовий сервер (15). Значення поля рівне: А.
10. Клас запиту / Class - Поле клас запиту дозволяє використовувати імена доменів для довільних об'єктів (всі офіційні імена Інтернет відносяться до одного класу [IN] - 1). Значення поля рівне: 0x0001.

Розглянемо dns-відповідь (рис. 2.4):

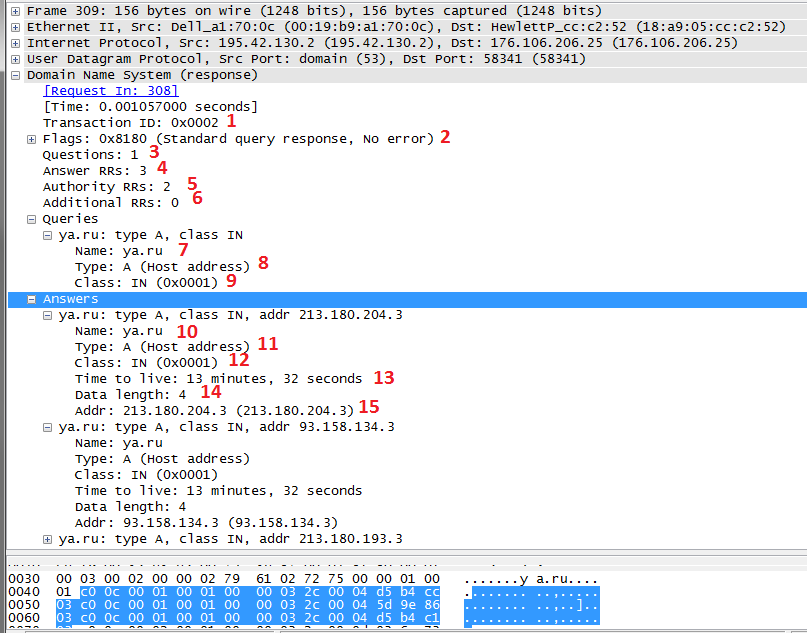


Рис. 2.4. dns-відповідь, докладно

1. Індентифікатор/ Transaction ID. Значення поля рівне:0x0002.
2. Прапори / Flags. Значення поля рівне: 0x8180.
3. Запити / Questions. Значення поля рівне: 1.
4. Відповідь РРС / Answer RRs. Значення поля рівне: 3.
5. Сервери імен / Authority Rrs. Значення поля рівне: 2.
6. Додаткові записи / Additional RRs. Значення поля рівне: 0.
7. Символьне ім'я запиту домену / Name. Значення поля рівне: ya.ru.
8. Тип і код запиту / Type. Значення поля рівне: А.
9. Клас запиту / Class. Значення поля рівне: 1.
10. Символьне ім'я відповіді домену / Name. Значення поля рівне: ya.ru.
11. Тип і код відповіді / Type. Значення поля рівне: A.
12. Клас відповіді / Class. Значення поля рівне: 1.
13. Час життя (TTL) — кількість маршрутизаторів, які може пройти даний пакет.Значення поля рівне: 13 хвилин 32 секунди.
14. Довжина запису про ресурси / Data length. Значення поля рівне: 4.
15. Адреса / Addr — символьний адрес запитуваного ресурсу. Значення поля рівне: 213.180.204.3.
16. Ознайомитись з основними функціями та можливостями утиліти nslookup.

Розглянемо з якими додатковими параметрами можна запускати утиліту nslookup.

Для цього виконаємо команду: nslookup /?. Результат зображено на рис. 2.5.

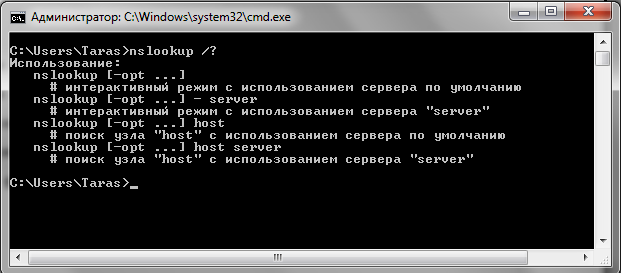


Рис. 2.5. nslookup /?.

Спробуємо запустити утиліту з опцією вказання сервера, так і без неї (рис. 2.6):

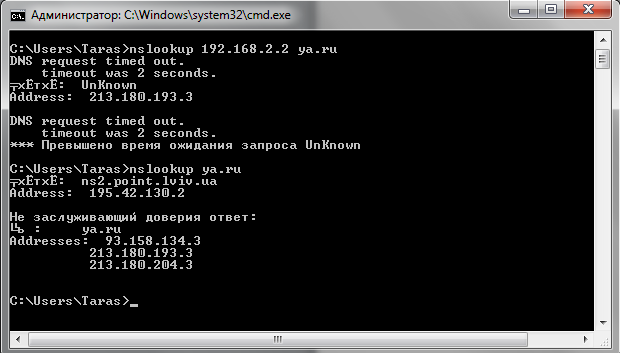


Рис. 2.6. nslookup /? з опцією сервер та без неї.

1. За допомогою аналізатора протоколів дослідити обмін повідомленнями при отриманні динамічної ІР-адреси від DHCP-сервера, розглянути роботу утиліти ipconfig з ключами /release та /renew.

**ipconfig** - утиліта командного рядка для управління мережевими інтерфейсами.

В операційних системах Microsoft Windows ipconfig - це утиліта командного рядка для виводу деталей поточного з'єднання та управління клієнтськими сервісами DHCP і DNS. Також є подібні графічні утиліти з назвами winipcfg і wntipcfg (остання передувала ipconfig). Утиліта ipconfig дозволяє визначати, які значення конфігурації були отримані за допомогою DHCP, APIPA або іншої служби IP-конфігурування або задані адміністратором вручну.

Утиліту ipconfig можна запускати з такими параметрами:

* **/all** - Відображення повної інформації по всіх адаптерам.
* **/release [адаптер]** - Відправка повідомлення DHCPRELEASE сервера DHCP для звільнення поточної конфігурації DHCP і видалення конфігурації IP-адрес для всіх адаптерів (якщо адаптер не заданий) або для заданого адаптера. Цей ключ відключає протокол TCP / IP для адаптерів, налаштованих для автоматичного отримання IP-адресу.
* **/renew [адаптер]** - Оновлення IP-адреси для певного адаптера або якщо адаптер не заданий, то для всіх. Доступно тільки при налаштованому автоматичному отриманні IP-адреси.
* **/flushdns** - Очищение DNS кешу.
* **/registerdns** - Оновлення всіх зарезервованих адрес DHCP та перереєстрація імен DNS.
* **/displaydns** - Відображення вмісту кешу DNS.
* **/showclassid адаптер** - Відображення коду класу DHCP для зазначеного адаптера. Доступно тільки при налаштованому автоматичним отриманням IP-адрес.
* **/setclassid адаптер** - Зміна коду класу DHCP. Доступно тільки при налаштованому динамічному отримуванні IP-адреси.
* **/?** - Довідка.

Запустимо утиліту ipconfig з ключом /renew та /release (рис. 2.7):

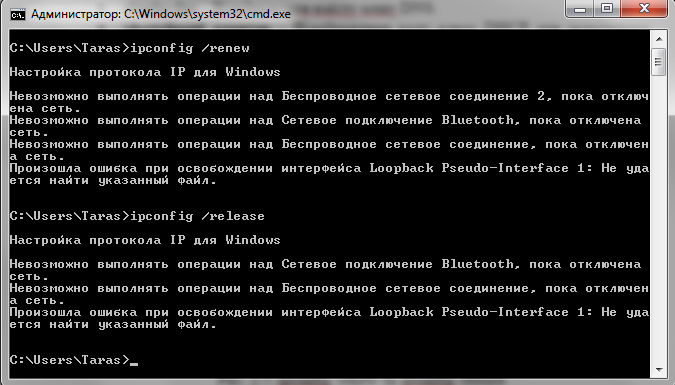


Рис. 2.7. ipconfig /renew та ipconfig /release

Запит а отримання динамічної ІР-адреси від DHCP-сервера у Wireshark має вигляд (рис. 2.8):

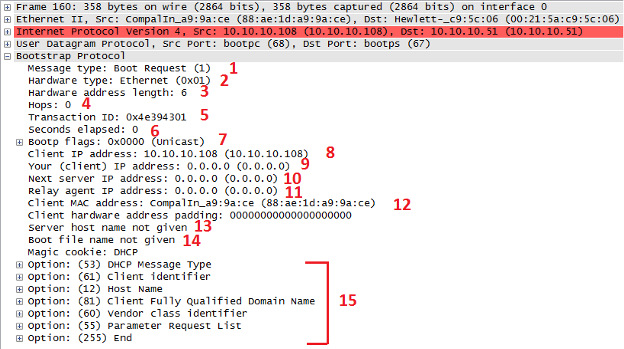


Рис. 2.8. Запит ipconfig /renew

1. Тип повідомлення / Message type - Наприклад може приймати значення: BOOTREQUEST (1, запит від клієнта до сервера) і BOOTREPLY (2, відповідь від сервера до клієнта). Значення поля рівне: Boot Request 0x01.
2. Тип апаратної адреси / Hardware type. Допустимі значення цього поля визначені в RFC1700 «Assigned Numbers». Наприклад, для [MAC-адреси](http://uk.wikipedia.org/wiki/MAC-адреса) Ethernet 10 Мбіт/с це поле приймає значення 1. Значення поля рівне: Ethernet 0x01.
3. Довжина апаратної адреси в байтах. Для MAC-адреси Ethernet - 6. Значення поля рівне: 6.
4. Кількість проміжних маршрутизаторів / Hops (так званих агентів ретрансляції DHCP), через які пройшло повідомлення. Клієнт встановлює це поле в 0. Значення поля рівне: 0.
5. Унікальний ідентифікатор транзакції / Transaction ID, що генерується клієнтом на початку процесу отримання адреси. Значення поля рівне: 0x4e394301.
6. Час в секундах з моменту початку процесу отримання адреси. Може не використовуватися (в цьому випадку воно встановлюється в 0). Значення поля рівне: 0.
7. Поле для прапорів / Flags – перелік спеціальних параметрів протоколу DHCP. Значення поля рівне: 0х0000 (unicast).
8. [IP-адреса](http://uk.wikipedia.org/wiki/IP-адреса) клієнта. Заповнюється тільки в тому випадку, якщо клієнт вже має власний IP-адресу і здатний відповідати на запити ARP (це можливо, якщо клієнт виконує процедуру поновлення адреси після закінчення терміну оренди). Значення поля рівне: 10.10.10.108.
9. Новий IP-адрес клієнта, запропонований сервером. Значення поля рівне: 0.0.0.0.
10. IP-адреса сервера. Повертається в реченні DHCP. Значення поля рівне: 0.0.0.0.
11. IP-адреса агента ретрансляції, якщо такий брав участь в процесі доставки повідомлення DHCP до сервера. Значення поля рівне: 0.0.0.0.
12. Апаратний адрес (зазвичай MAC-адрес) клієнта. Значення поля рівне: 88:ae:1d:a9:9a:ce.
13. Необов'язкове ім'я сервера у вигляді нуль-термінованого рядка. Значення поля рівне: 0.
14. Необов'язкове ім'я [файлу](http://uk.wikipedia.org/wiki/Файл) на сервері, що використовується бездисковими робочими станціями при віддаленому завантаженні. Як і sname, представлено у вигляді нуль-термінованого рядка. Значення поля рівне: 0.
15. Поле опцій DHCP. Тут вказуються різні додаткові параметри конфігурації. На початку цього поля вказуються чотири особливих байта зі значеннями 99, 130, 83, 99 («чарівні числа»), що дозволяють серверу визначити наявність цього поля. Поле має змінну довжину, проте DHCP-клієнт повинен бути готовий прийняти DHCP-повідомлення завдовжки 576 байт (в цьому повідомленні поле options має довжину 340 байт).

Відповідь на хапит отримання динамічної ІР-адреси від DHCP-сервера у Wireshark має вигляд (рис. 2.9-2.10):

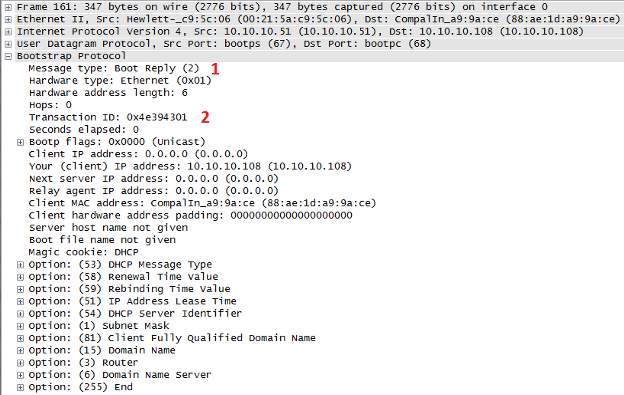


Рис. 2.9. Відповідь на запит ipconfig /renew

1. Тип повідомлення / Message type. Значення поля рівне: Boot replay (2).
2. Унікальний ідентифікатор транзакції / Transaction ID. Значення поля рівне: 0х4e394301.

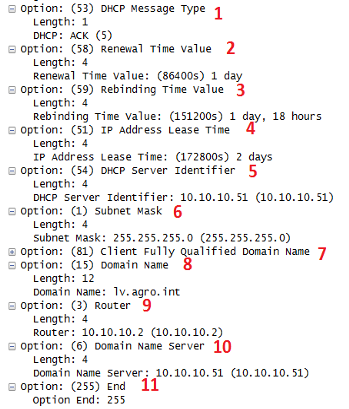


Рис. 2.10. Відповідь на запит ipconfig /renew

1. Тип повідомлення / Message type - Наприклад може приймати значення: BOOTREQUEST (1, запит від клієнта до сервера) і BOOTREPLY (2, відповідь від сервера до клієнта).
2. Значення поля рівне: Boot Request 0x01.
3. Тип апаратної адреси / Hardware type. Допустимі значення цього поля визначені в RFC1700 «Assigned Numbers». Наприклад, для [MAC-адреси](http://uk.wikipedia.org/wiki/MAC-адреса) Ethernet 10 Мбіт/с це поле приймає значення 1.
4. Значення поля рівне: Ethernet 0x01.
5. Довжина апаратної адреси в байтах. Для MAC-адреси Ethernet - 6.
6. Значення поля рівне: 6.
7. Кількість проміжних маршрутизаторів / Hops (так званих агентів ретрансляції DHCP), через які пройшло повідомлення. Клієнт встановлює це поле в 0.
8. Значення поля рівне: 0.
9. Унікальний ідентифікатор транзакції / Transaction ID, що генерується клієнтом на початку процесу отримання адреси.
10. Значення поля рівне: 0x4e394301.
11. Час в секундах з моменту початку процесу отримання адреси. Може не використовуватися (в цьому випадку воно встановлюється в 0).
12. Значення поля рівне: 0.
13. Поле для прапорів / Flags – перелік спеціальних параметрів протоколу DHCP.
14. Значення поля рівне: 0х0000 (unicast).
15. [IP-адреса](http://uk.wikipedia.org/wiki/IP-адреса) клієнта. Заповнюється тільки в тому випадку, якщо клієнт вже має власний IP-адресу і здатний відповідати на запити ARP (це можливо, якщо клієнт виконує процедуру поновлення адреси після закінчення терміну оренди).
16. Значення поля рівне: 10.10.10.108.
17. Новий IP-адрес клієнта, запропонований сервером.
18. Значення поля рівне: 0.0.0.0.
19. IP-адреса сервера. Повертається в реченні DHCP.
20. Значення поля рівне: 0.0.0.0.
21. IP-адреса агента ретрансляції, якщо такий брав участь в процесі доставки повідомлення DHCP до сервера.

## ВИСНОВКИ

На даній лабораторній роботі я дослідив роботу протоколів DHCP та DNS, дізнався про роботу утиліти nslookup. З допомогою з програми wireshark перехопив та відфільтрував потік даних що містив запити по протоколу DNS та DHCP, та дослідив структуру пакетів DNS та DHCP.