



Лабораториска вежба бр. 2

DNS протокол

Како што е опишано во Дел 2.4 од текстот¹, Domain Name system (DNS) преведува од име на домаќин во IP адреса, исполнувајќи ја клучна улога во инфраструктурата на Интернет. Во оваа лабораториска вежба, ќе ја погледнеме одблизу клиентската страна на DNS. Потсетете се дека улогата на клиентот во DNS е релативно едноставна - клиентот испраќа барање (query) до својот локален DNS сервер и добива одговор. Како што е прикажано на сликите 2.19 и 2.20 во учебникот, многу работи се случуваат во позадина, без да забележат DNS клиентите, бидејќи хиерархиските DNS сервери комуницираат едни со други за да рекурзивно или итеративно го решат барањето на DNS клиентот. Од гледна точка на DNS клиент, сепак, протоколот е прилично едноставен - барањето е формулирано до локалниот DNS сервер и од него се добива одговор.

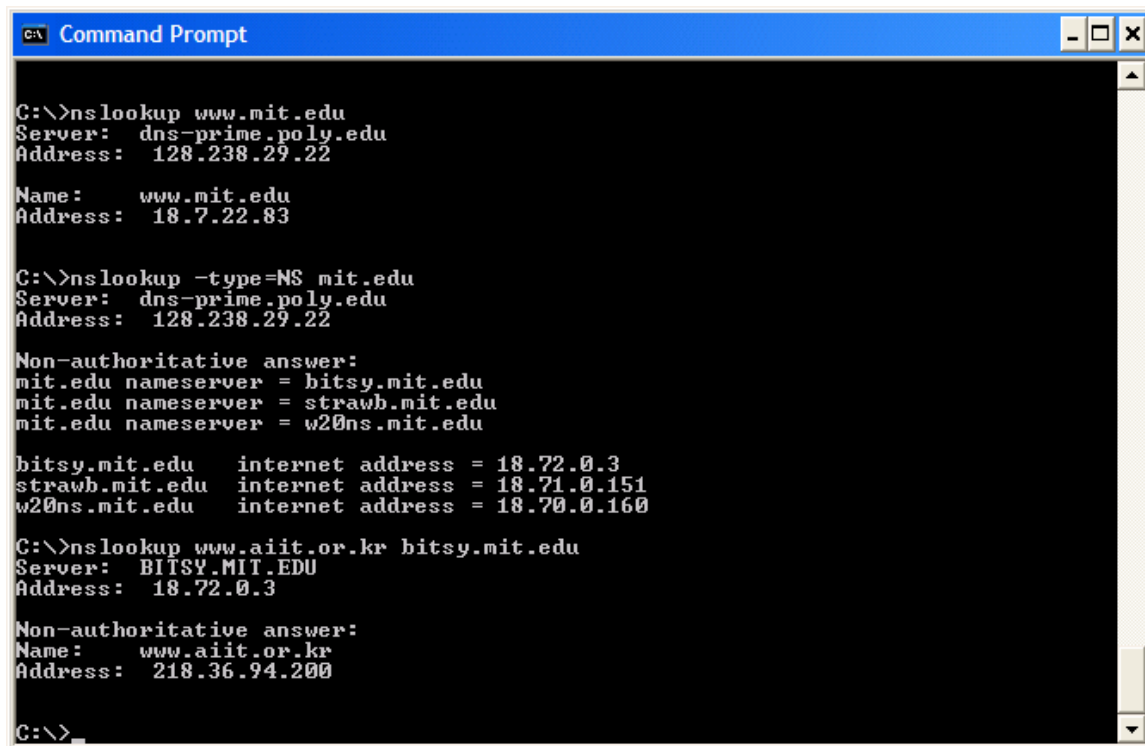
Пред да започнете со оваа лабораториска вежба, веројатно ќе сакате да го проучите DNS со читање на Дел 2.4 од текстот. Особено, можеби ќе сакате да го прегледате материјалот за локалните DNS сервери, DNS кеширањето, записите и пораките на DNS и полето TYPE во DNS записот.

1. nslookup

Во оваа лабораториска вежба, ќе ја искористиме алатката *nslookup*, која е достапна денес во повеќето Linux/Unix и Microsoft платформи. За да извршите *nslookup* во Linux/Unix, само внесете ја командата *nslookup* на командната линија. За да ја стартувате во Windows, отворете Command Prompt и извршете *nslookup* на командната линија.

nslookup му овозможува на домаќинот да ја активира алатката за да побара кој било одреден DNS сервер за даден DNS запис. Пребаруваниот DNS сервер може да биде root DNS-сервер, top-level-domain DNS, авторитативен DNS или локален DNS сервер (видете во учебникот за дефиниции на овие поими). За да ја постигнете оваа задача, *nslookup* испраќа DNS барање до наведениот сервер, добива одговор од истиот DNS сервер и го прикажува резултатот.

¹ References to figures and sections are for the 7th edition of our text, *Computer Networks, A Top-down Approach*, 7th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2016.



```
C:\>nslookup www.mit.edu
Server:  dns-prime.poly.edu
Address: 128.238.29.22

Name:    www.mit.edu
Address: 18.7.22.83

C:\>nslookup -type=NS mit.edu
Server:  dns-prime.poly.edu
Address: 128.238.29.22

Non-authoritative answer:
mit.edu nameserver = bitsy.mit.edu
mit.edu nameserver = strawb.mit.edu
mit.edu nameserver = w20ns.mit.edu

bitsy.mit.edu    internet address = 18.72.0.3
strawb.mit.edu   internet address = 18.71.0.151
w20ns.mit.edu    internet address = 18.70.0.160

C:\>nslookup www.aait.or.kr bitsy.mit.edu
Server:  BITSY.MIT.EDU
Address: 18.72.0.3

Non-authoritative answer:
Name:    www.aait.or.kr
Address: 218.36.94.200

C:\>
```

Горната слика ги прикажува резултатите од три независни команди *nslookup* (прикажани во Command Prompt на Windows). Во овој пример, домаќинот-клиент се наоѓа на кампусот на Политехничкиот универзитет во Бруклин, каде што е основниот локален DNS сервер - dns-prime.poly.edu. Кога се извршува командата *nslookup*, ако не е наведен DNS сервер, тогаш *nslookup* го испраќа прашањето до стандардниот DNS сервер, кој во овој случај е dns-prime.poly.edu. Разгледајте ја првата команда:

```
nslookup www.mit.edu
```

Со зборови, оваа команда вели „те молам, испратете ми ја IP адресата за домаќинот *www.mit.edu*“. Како што е прикажано на екранот, одговорот од оваа команда дава два вида информации: (1) името и IP адресата на DNS серверот што го дава одговорот; и (2) самиот одговор, односно име на домаќин и IP адреса на *www.mit.edu*. Иако одговорот дојде од локалниот DNS сервер на Политехничкиот универзитет, сосема е можно овој локален DNS сервер итеративно да контактирал со неколку други DNS сервери за да го добие одговорот, како што е опишано во Дел 2.4 од учебникот.

Сега да ја разгледаме втората команда:

```
nslookup -type=NS mit.edu
```

Во овој пример, ја дадовме опцијата „-type=NS“ и доменот „mit.edu“. Ова предизвикува *nslookup* да испрати барање за запис од типот NS до стандардниот



локален сервер DNS. Со зборови, прашањето вели: „Ве молам, испратете ми ги имињата на домаќините на авторитативните DNS за mit.edu“. (Кога опцијата `-type` не се користи, *nslookup* ја користи стандардната, што е за пребарување за записите од типот A.) Одговорот, прикажан во горната слика, најпрво го означува DNS серверот што го дава одговорот (стандардниот локален DNS сервер) заедно со три сервери за имиња на MIT. Секој од овие сервери е навистина овластен DNS сервер за домаќините во кампусот MIT. Како и да е, *nslookup* исто така означува дека одговорот е „неовластен“, што значи дека овој одговор потекнува од кешот на некој сервер, а не од овластен MIT DNS сервер. Конечно, одговорот вклучува и IP адреси на авторитативните DNS сервери на MIT. (И покрај тоа што барањето од тип-NS генерирано од *nslookup* не ги бараше експлицитно и IP адресите, локалниот DNS сервер ги врати овие „бесплатно“ и *nslookup* го прикажува резултатот.)

На крај, да ја разгледаме третата команда:

```
nslookup www.aiit.or.kr dns.google
```

Во овој пример, посочуваме дека сакаме да го испратиме прашањето до DNS серверот на Google кој е достапен на IP адресата `dns.google`, а не до стандардниот сервер DNS (`dns-prime.poly.edu`). Така, барањето и одговорот се одвиваат директно помеѓу нашиот домаќин за пребарување и `dns.google`. Во овој пример, DNS серверот `dns.google` ја обезбедува IP адресата на домаќинот `www.aiit.or.kr`, кој е Веб сервер во Напредниот институт за информатичка технологија (во Кореја).

Сега, кога поминавме низ неколку илустративни примери, можеби се прашувате за општата синтакса на командите *nslookup*. Синтаксата е:

```
nslookup -option1 -option2 host-to-find dns-server
```

Во принцип, *nslookup* може да се изврши со нула, една, две или повеќе опции. И, како што видовме во горенаведените примери, DNS серверот е опционален; ако не е даден, барањето е испратено до стандардниот локален DNS сервер.

Сега, кога го поминавте прегледот на *nslookup*, време е да го тестирате сами. Направете го следново (и запишете ги резултатите):

1. Извршете ја *nslookup* командата за да добиете IP адреса на веб-сервер во Азија. Која е IP адресата на тој сервер?
2. Извршете ја *nslookup* командата за да ги одредите авторитетните DNS сервери за универзитет во Европа.
3. Извршете ја *nslookup* командата така што на еден од DNS серверите добиен од Прашањето 2 се испрати барање за mail серверите на Yahoo! mail. Која е неговата IP адреса?

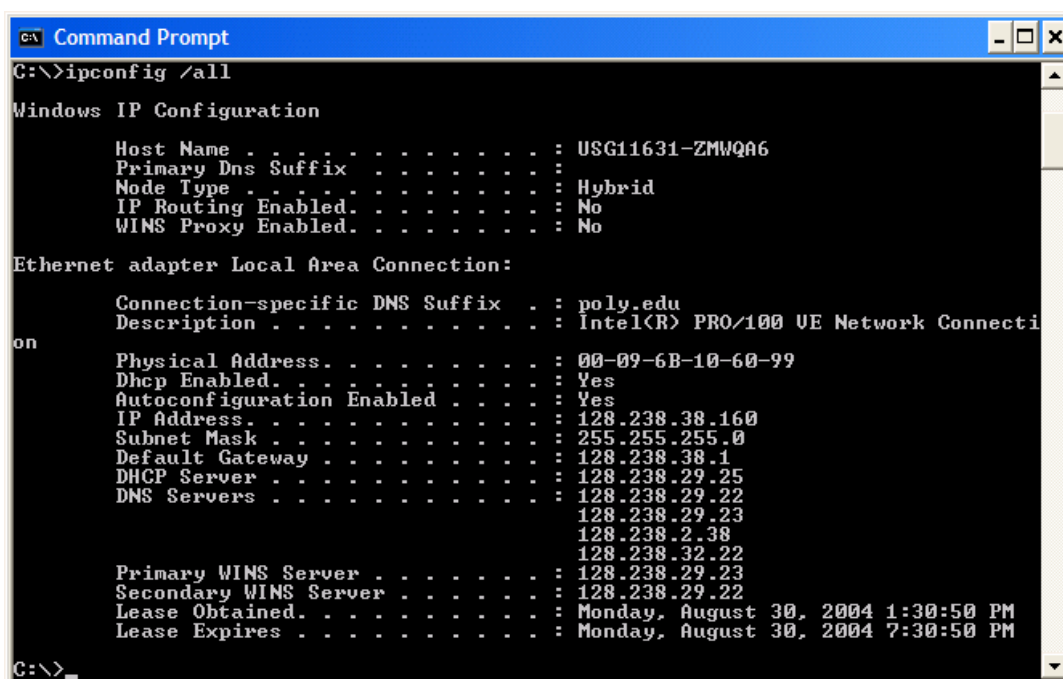


2. ipconfig

ipconfig (за Windows) и *ifconfig* (за Linux/Unix) се меѓу најкорисните услуги во вашиот домаќин, особено за дебагирање мрежни проблеми. Овде ќе ги опишеме само *ipconfig*, иако *ifconfig* на Linux / Unix е многу сличен. *ipconfig* може да се користи за прикажување на тековните TCP/IP информации, вклучувајќи ја и вашата адреса, адресите на DNS серверот, типот на адаптерот и така натаму. На пример, ќе ги добиете сите овие информации за вашиот домаќин едноставно со внесување:

```
ipconfig \all
```

во Command Prompt, како што е прикажано на сликата подолу.



ipconfig е исто така многу корисно за управување со DNS информациите зачувани во вашиот домаќин. Во делот 2.5 научивме дека домаќинот може да зачува DNS запис што неодамна ги добил. За да ги видите овие зачувани записи, по C: \> внесете ја следнава команда:

```
ipconfig /displaydns
```

Секој запис прикажува и останатото “време на живот” (Time to Live - TTL) во секунди. За да се исчисти кешот, внесете:

```
ipconfig /flushdns
```

Оваа команда ги брише сите записи од DNS кешот и повторно ги вчитува записите од датотеката на домаќинот.



3. DNS со Wireshark

Сега кога сте запознаени со *nslookup* и *ipconfig*, подготвени сте за посериозна работа. Прво, да ги фатиме DNS пакетите што се создаваат со обично Веб сурфање.

- Користете *ipconfig* за да го испразните DNS кешот во вашиот домаќин.
- Отворете го прелистувачот и испразнете го кешот на прелистувачот.
- Отворете Wireshark и внесете „ip.addr == вашата_IP_адреса“ во филтерот (каде што вашата_IP_адреса ја дознавате со *ipconfig*). Овој филтер ги отстранува сите пакети што ниту потекнуваат, ниту се наменети за вашиот домаќин.
- Започнете со снимање на пакети во Wireshark.
- Со прелистувачот, посетете ја Веб страницата: <http://www.ietf.org>
- Прекинете со снимање во Wireshark.

Одговорете на следните прашања. Секогаш кога е можно, кога одговарате на прашањата, треба да прикажете `print` на пакетот што сте го користеле за да одговорите на поставеното прашање. Означете го `print`-от за да го објасните вашиот одговор². За да отпечатите пакет, користете *File-> Print*, изберете само *Selected packet only*, изберете *Packet summary line* и изберете ја минималната количина детали за пакетот што ви е потребна за да одговорите на прашањето.

4. Пронајдете ги DNS пораките за барањето и одговорите. Дали се испраќаат преку UDP или TCP?
5. Која е дестинациската порта на пораката за DNS барање? Која е изворната порта на пораката за DNS одговор?
6. На која IP адреса се испраќа пораката за DNS барање? Користете *ipconfig* за да ја одредите IP адресата на вашиот локален DNS сервер. Дали се овие две IP адреси исти?
7. Разгледајте ја пораката за DNS барање. Кој "Type" на DNS барањето е тоа? Дали пораката за барање содржи некои „одговори“?
8. Разгледајте ја пораката за DNS одговор. Колку „одговори“ се дадени? Што содржат секој од овие одговори?
9. Разгледајте го последователниот TCP SYN пакет испратен од вашиот домаќин. Дали IP адресата за дестинација на SYN пакетот одговара на која било IP адреса дадена во пораката за DNS одговор?
10. Оваа Веб страница содржи слики. Пред да ја прегледате секоја слика, дали вашиот домаќин издава нови DNS барања?

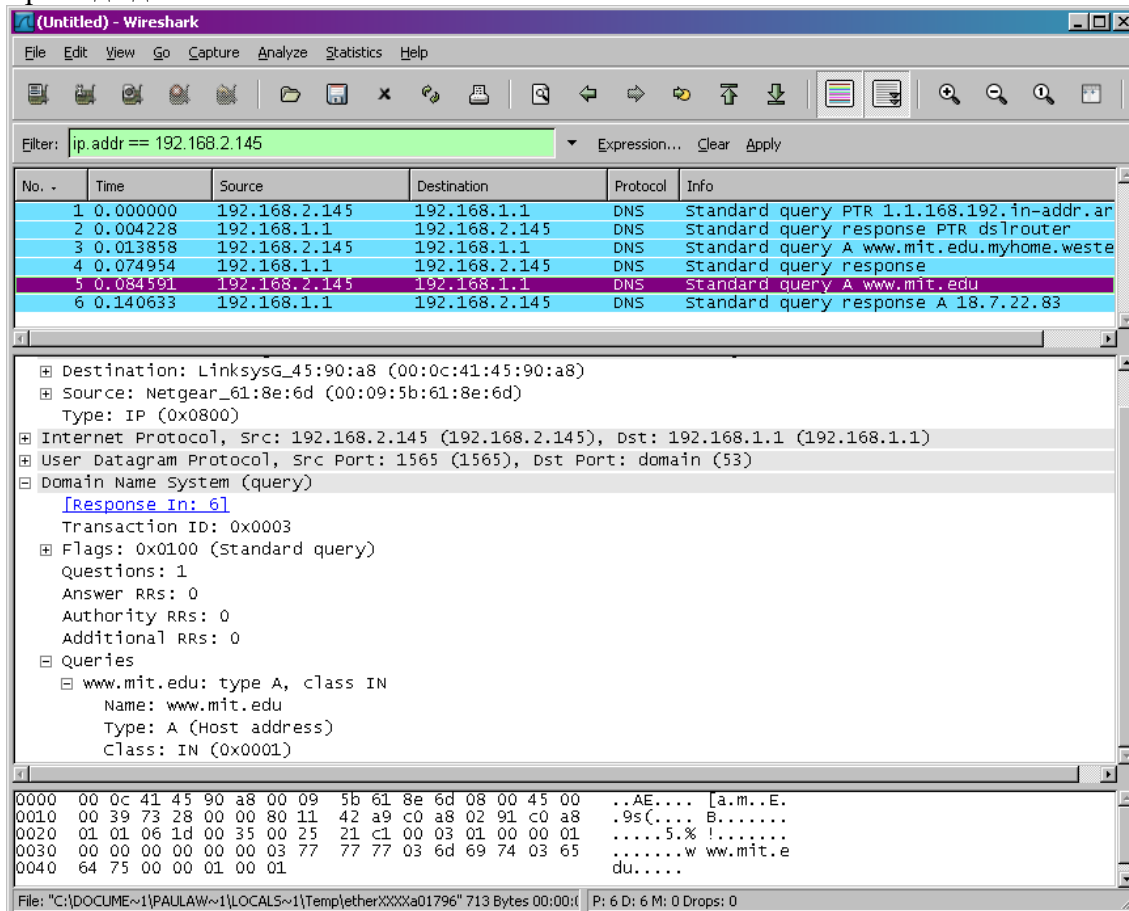
Сега да го видиме *nslookup*.

² What do we mean by “annotate”? If you hand in a paper copy, please highlight where in the printout you’ve found the answer and add some text (preferably with a colored pen) noting what you found in what you’ve highlight. If you hand in an electronic copy, it would be great if you could also highlight and annotate.



- Започнете со снимање на пакети.
- Направете *nslookup* на www.mit.edu
- Прекинете со снимање на пакети.

Треба да добиете нешто слично на:



Погоре гледаме дека *nslookup* испратил три DNS барања и добил три DNS одговори. За оваа задача, треба да се игнорираат останатите DNS барања, а треба да се земе во предвид само барањето кое во Info делот има "Standard query A www.mit.edu". Овие три барања се специфични за *nslookup* и не се вообичаено генерирани од стандардни Интернет апликации. Одговорете на следните прашања:

11. Која е дестинациската порта на пораката за DNS барање? Која е изворната порта на пораката за DNS одговор?
12. На која IP адреса се испраќа пораката за DNS барање? Дали е ова IP адресата на вашиот основен локален DNS сервер?
13. Разгледајте ја пораката за DNS барање. Кој "Type" на DNS барање е тоа? Дали пораката за DNS барање содржи „одговори“?
14. Разгледајте ја пораката за DNS одговор. Колку „одговори“ се дадени? Што содржи секој од овие одговори?
15. Поставете screenshot.



Сега повторете го претходниот експеримент, но наместо тоа, внесете ја командата:

```
nslookup -type=NS mit.edu
```

Одговорете ги следните прашања (и во овој случај игнорирајте го првото DNS барање – од тип PTR):

16. На која IP адреса се испраќа пораката за DNS барање? Дали е ова IP адресата на вашиот основен локален DNS сервер?
17. Разгледајте ја пораката за DNS барање. Кој "Type" на DNS барање е тоа? Дали пораката за DNS барање содржи „одговори“?
18. Разгледајте ја пораката за DNS одговор. Кои паметни сервери на MIT се дадени во порака за одговор? Дали оваа порака за одговор дава и IP адреси на паметните сервери на MIT?
19. Поставете screenshot.

Сега повторете го претходниот експеримент, но наместо тоа, внесете ја командата:

```
nslookup www.aiit.or.kr dns.google
```

Одговорете ги следните прашања:

20. На која IP адреса е пратено DNS барањето? Дали е ова IP адресата на вашиот основен локален DNS сервер? Ако не, на што одговара оваа IP адреса?
21. Разгледајте ја пораката за DNS барање. Кој "Type" на DNS барање е тоа? Дали пораката за DNS барање содржи „одговори“?
22. Разгледајте ја пораката за DNS одговор. Колку „одговори“ се дадени? Што содржи секој од овие одговори?
23. Поставете screenshot.