Wireshark Lab: DNS

Versão 1.1

Como descrito na seção 2.5 do livro, o *Domain Name System* (DNS) traduz nomes de *hosts* em endereços Internet *Protocol* (IP), preenchendo uma lacuna crítica na infra-estrutura da Internet. Neste laboratório, observaremos de mais perto o lado cliente do DNS. Lembre-se de que o papel do cliente no DNS é relativamente simples - um cliente envia uma consulta ao seu DNS, e obtém uma resposta. Como exibido na figura 2.26 e 2.18 no livro, muito pode acontecer “por baixo dos panos”, de forma invisível aos clientes DNS, enquanto os servidores DNS, organizados hierarquicamente, comunicam-se entre si para, ou recursivamente ou iterativamente, resolver uma consulta DNS de um cliente. Do ponto de vista do cliente DNS, contudo, o protocolo é bastante simples - uma consulta é feita ao seu servidor DNS e uma resposta é recebida deste servidor.
Antes de iniciar este laboratório, você provavelmente desejará revisar DNS lendo a seção 2.5 no livro. Em particular, você deve revisar os materiais: servidores DNS locais, cache DNS, mensagens e registros DNS e o campo TYPE no registro DNS.

1. nslookup

Neste laboratório, faremos um uso extensivo da ferramenta nslookup, que está disponível na maioria dos sistemas operacionais atuais, sejam Windows, Linux ou Unix. Para executar nslookup no Linux ou Unix, basta digitar nslookup em uma linha de comando. Para executá-lo no Windows, abra o Prompt de Comando e digite nslookup na linha de comando.
No seu modo de operação mais básico, nslookup permite que o *host* que o execute consulte qualquer servidor DNS para obter um registro. O servidor DNS consultado pode ser um servidor raiz, um servidor DNS responsável por um domínio, um servidor DNS autoritário, ou um servidor DNS intermediário (veja o livro para as definições destes termos). Para realizar esta tarefa, o nslookup envia uma consulta DNS ao servidor especificado e recebe uma resposta do mesmo servidor, exibindo o resultado no vídeo.
As figuras 1, 2 e 3 mostram o resultado de três comandos nslookup independentes (na linha de comando do Linux). Nestas figuras, o host cliente é o laptop do Prof. Othon em casa, sendo o servidor DNS padrão o endereço IP 200.225.157.105 (ns2.ig.com.br).

Quando executa-se nslookup sem um servidor DNS especificado, ele consulta o servidor DNS padrão, que neste caso é ns2.ig.com.br.

```
[othon@hplaptop ~]$ nslookup www.mit.edu
Server:         200.225.157.105
Address:        200.225.157.105#53

Non-authoritative answer:
Name:   www.mit.edu
Address: 18.7.22.83
```

Figura 1. Primeiro exemplo de uso do nslookup.

O comando da figura 1, em palavras, diz “por favor, envie-me o endereço IP para o host www.mit.edu”. A resposta exibida na mesma figura para este comando fornece duas informações:

- o nome e endereço IP do servidor DNS que foi consultado;
- a resposta em si, que é o nome do *host* e o endereço IP.

Embora a resposta venha do servidor ns2.ig.com.br, é bem possível que este servidor DNS tenha contactado diversos outros servidores DNS para obter a resposta, como descrito na seção 2.5 do livro.

```
[othon@hplaptop ~]$ nslookup -type=NS mit.edu
Server:         200.225.157.105
Address:        200.225.157.105#53

Non-authoritative answer:
mit.edu nameserver = STRAWB.mit.edu.
mit.edu nameserver = BITSY.mit.edu.
mit.edu nameserver = W20NS.mit.edu.

Authoritative answers can be found from:
BITSY.mit.edu   internet address = 18.72.0.3
STRAWB.mit.edu  internet address = 18.71.0.151
```

Figura 2. Segundo exemplo do uso do nslookup.

Na figura 2, foi passada como parâmetro a opção “-type=NS” e o domínio “mit.edu”. Isto faz com que o nslookup envie uma consulta ao servidor DNS local para um registro do tipo NS. Em palavras, a consulta diz, “por favor envie-me os nomes dos *hosts* dos servidores DNS autoritários para mit.edu”. Quando a opção -type não é utilizada, o nslookup usa o padrão, que é consultar por registros do tipo A. A resposta inicialmente

indica o servidor DNS que está respondendo (que é o servidor DNS local) juntamente com três nomes de servidores do *Massachussets Institute of Technology* (MIT). Cada um destes servidores é de fato um servidor DNS autoritário para os *hosts* no campus do MIT. Entretanto, o nslookup também indica que a resposta é “não autoritária”, o que significa que ela veio do cache de algum servidor ao invés de algum dos servidores DNS autoritários do MIT. Finalmente, a resposta também inclui o endereço IP dos servidores DNS autoritários do MIT. Mesmo que a consulta pelo registro de tipo NS não tenha pedido explicitamente os endereços IP, o servidor DNS local os retornou e o nslookup os apresentou no resultado.

```
[othon@hplaptop ~]$ nslookup www.aiit.or.kr bitsy.mit.edu
Server:         bitsy.mit.edu
Address:        18.72.0.3#53

Non-authoritative answer:
Name:   www.aiit.or.kr
Address: 222.106.36.115
```

Figura 3.Terceiro exemplo de uso do nslookup.

Na figura 3, indicamos que desejamos que a consulta seja enviada ao servidor DNS bitys.mit.edu ao invés do servidor DNS local (ns2.ig.com.br). Assim, a consulta e resposta ocorrem diretamente entre o nosso *host* e o servidor DNS bitsy.mit.edu. Neste exemplo, o servidor DNS bitsy.mit.edu fornece o endereço IP do *host* www.aiit.or.kr, que é o servidor *web* do *Advanced Institute of Information Technology*, na Coréia.

Agora que já passamos por alguns exemplos ilustrados, talvez você esteja se perguntando sobre a sintaxe genérica do comando nslookup. A sintaxe é:

nslookup -opção1 -opção2 host-a-encontrar servidor-dns

Geralmente, o nslookup pode ser executado com nenhuma, uma, duas ou mais opções. A como vimos nos exemplos das figuras 1, 2 e 3, o parâmetro servidor-dns é opcional; se ele não é informado, a consulta é enviada ao servidor DNS local.

Agora que revisamos o comando nslookup, está na hora de você testá-lo sozinho. Execute o nslookup para cada uma das questões, e escreva os resultados:

1. obtenha o endereço IP de um servidor *web* na Ásia;
2. determine os servidores DNS autoritários para uma universidade na Europa;
3. utilize um dos servidores DNS obtidos na questão 2 e consulte pelo endereço IP do

Yahoo! Mail.

2. ipconfig ou ifconfig

ipconfig, no Windows, e ifconfig, no Linux ou Unix, estão entre as mais úteis ferramentas de rede no seu host, especialmente para depuração. Esta seção está dividida em duas partes, uma que explica o ipconfig no Windows, e outra que esplica o ifconfig no Linux.

2.1. ipconfig

O comando ipconfig pode ser utilizado para mostrar a informação TCP/IP atual, incluindo: endereço IP, endereço de servidores DNS locais, tipo de adaptador de rede, entre outras. Por exemplo, todas as informações de um host podem ser obtidas através da digitação no prompt de comando de ipconfig /all (figura 4).

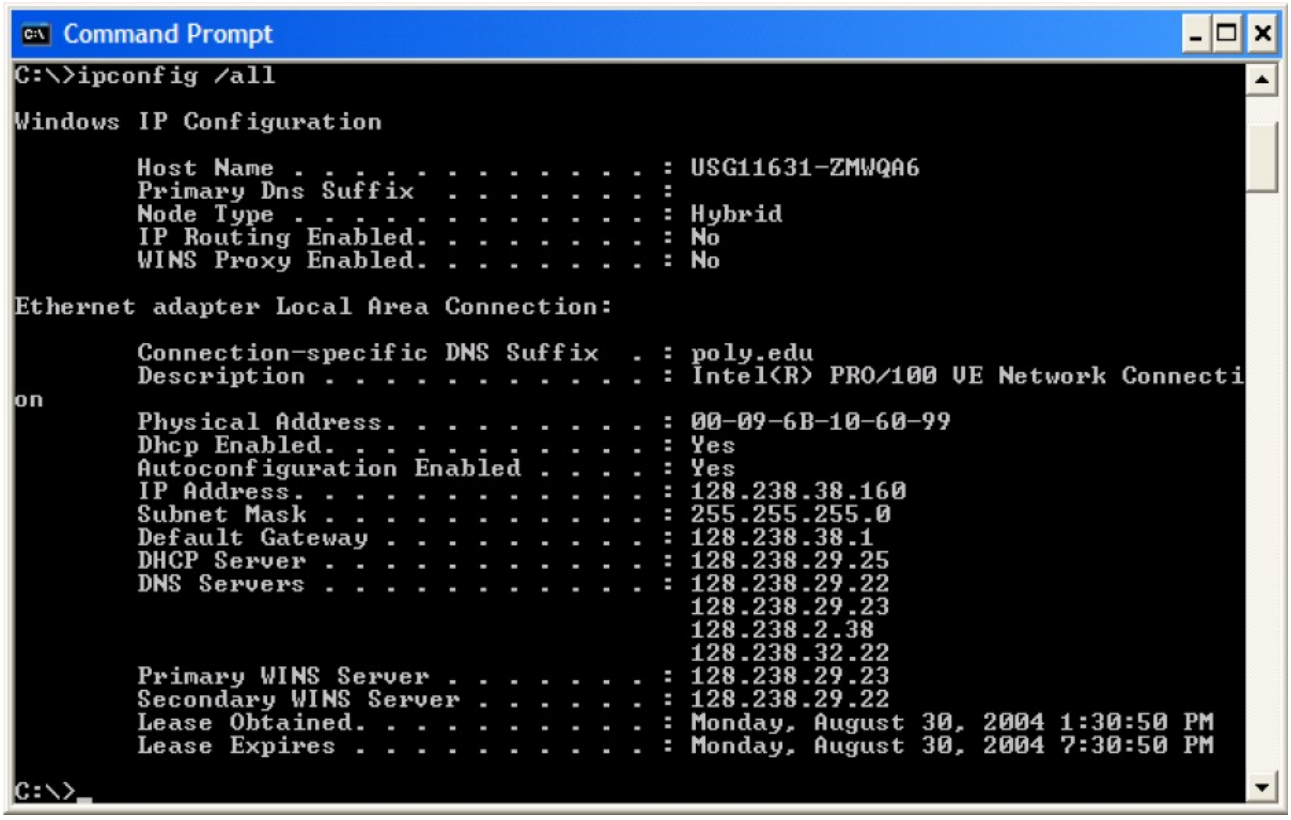

Figura 4. Informação obtida do ipconfig /all.

O comando ipconfig também é bastante útil para exibir as informações do DNS armazenadas no *host*. Na seção 2.5, aprendemos que um *host* pode gravar em *cache* os registros DNS obtidos recentemente. Para ver os registros gravados em *cache*, basta

digitar na linha de comando “ipconfig /displaydns”, sem as aspas. Cada entrada mostra o tempo de vida (TTL) restante em segundos. Para limpar o *cache*, digita-se “ipconfig /flushdns”, sem as aspas. Limpar o *cache* faz com que todas as entradas sejam apagadas e recarrega as entradas do arquivo *hosts*. Estes comandos funcionam no Windows porque ele executa automaticamente um servidor DNS cache no *host*.

2.2. ifconfig

O comando ifconfig funciona no Linux e serve para exibir as configurações das *interfaces* de rede conectadas ao *host*. A figura 5 mostra uma saída típica do comando ifconfig no sistema operacional Linux.

```
[root@hplaptop ~]# ifconfig
eth0      Link encap:Ethernet  Endereço de HW 00:0B:CD:34:D9:FC
          inet end.: 192.168.1.10  Bcast:192.168.1.255  Masc:255.255.255.0
          endereço inet6: fe80::20b:cdff:fe34:d9fc/64 Escopo:Link
          UP BROADCASTRUNNING MULTICAST  MTU:1500  Métrica:1
          RX packets:523 errors:0 dropped:0 overruns:0 frame:0
          TX packets:93 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:1000
          RX bytes:184362 (180.0 KiB)  TX bytes:9042 (8.8 KiB)
          IRQ:11 Endereço de E/S:0xa000

lo        Link encap:Loopback Local
          inet end.: 127.0.0.1  Masc:255.0.0.0
          endereço inet6: ::1/128 Escopo:Máquina
          UP LOOPBACKRUNNING  MTU:16436  Métrica:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          colisões:0 txqueuelen:0
          RX bytes:660 (660.0 b)  TX bytes:660 (660.0 b)
```

Figura 5. Saída típica do comando ifconfig.

Na figura 5 estão as configurações de duas *interfaces* de rede: eth0 e lo. O nome eth0 é uma sigla para a primeira interface *ethernet* e lo para *loopback*. A *interface* lo serve para utilizar aplicações TCP/IP mesmo que o *host* não esteja conectado fisicamente a uma rede. O endereço 127.0.0.1 é atribuído como padrão a esta *interface*. A interface eth0 é uma abstração do sistema operacional para uma placa de rede *ethernet*. O endereço IP exibido na figura 5 é 192.168.1.10.

Em Linux, os endereços dos servidores DNS locais estão em uma arquivo texto

denominado resolv.conf no diretório /etc. Cada linha deste arquivo que inicia com nameserver é finalizada pelo endereço IP de um servidor DNS local (figura 6). Vale lembrar que este arquivo só pode ser editado pelo administrador do sistema (usuário root).

```
[othon@hplaptop ~]$ cat /etc/resolv.conf
# generated by NetworkManager, do not edit!

domain mrgluhome

search mrgluhome

nameserver 200.225.157.105
nameserver 192.168.1.13
```

Figura 6. Conteúdo do arquivo /etc/resolv.conf.

Os comandos “ipconfig /displaydns” e “ipconfig /flushdns” só tem similares no Linux quando é executado um servidor DNS cache no *host*, como o nscd.

3. Rastreando DNS com o Wireshark

Agora que nos familiarizamos com o nslookup e ipconfig, estamos prontos para botar as mãos na massa. Inicialmente vamos capturar as mensagens DNS que são geradas por uma navegação na *web*. Para isso, siga os passos:

- utilize ipconfig para limpar o cache DNS do host;
- abra o navegador *web* e limpe o *cache* do mesmo;
- abra o Wireshark e digite “ip.addr == seu_endereço_IP” no filtro (sem as aspas). Este filtro só mostra os pacotes que ou são originados ou destinados ao seu *host*;
- inicie a captura de pacotes no Wireshark;
- no navegador *web*, visite a página http://www.ietf.org;
- pare a captura de pacotes.

Se você não conseguir executar o Wireshark em uma conexão de rede, baixe o arquivo de rastreamento de pacotes[1] que foi capturado quando os passos indicados foram executados no computador do autor do livro. Responda às questões:

1. localize as mensagens de solicitação e resposta DNS. Foram enviadas com TCP ou UDP?

1 Baixe o arquivo compactado http://gaia.cs.umass.edu/ethereal-labs/ethereal-traces.zip e extraia o arquivo dns-ethereal-trace-1.

2. qual é a porta destino para a mensagem de consulta DNS? Qual é a porta fonte da mensagem de resposta DNS?
3. a qual endereço IP a mensagem de consulta DNS é enviada? Utilize ipconfig para determinar o endereço IP do seu servidor DNS local. Estes endereços são os mesmos?
4. examine a mensagem de consulta DNS. Qual o campo "*type*" desta mensagem? A mensagem de consulta contém algum campo "*answer*"?
5. examine a mensagem de resposta DNS. Quantos campos com "*answer*" existem? O que há em cada uma destas mensagens?
6. considere o segmento TCP SYN subseqüente enviado pelo seu *host*. O endereço IP de destino do pacote SYN corresponde a algum dos endereços IP fornecidos na mensagem de resposta DNS?
7. a página *web* visitada contém imagens. Antes de recuperar cada imagem, o *host* realiza novas consultas DNS?

Agora vamos brincar com o nslookup[2]. Siga os passos:

- adicione ao filtro " && dns", sem as aspas;
- inicie a captura de pacotes;
- execute o comando "nslookup www.mit.edu", sem as aspas;
- pare a captura de pacotes.

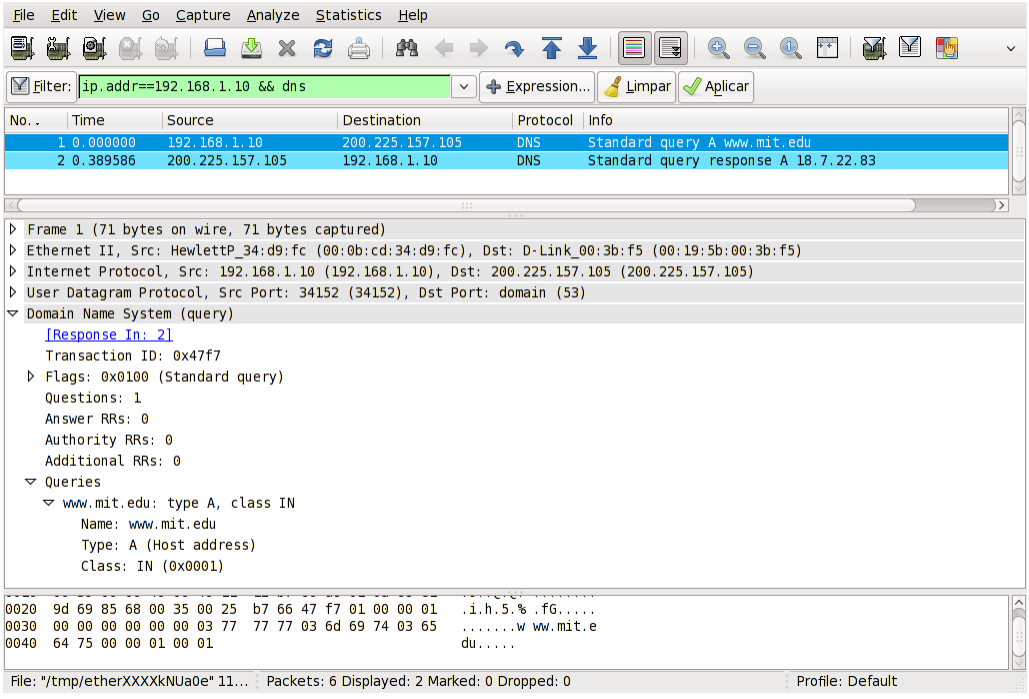

Figura 7. Captura dos pacotes para "nslookup www.mit.edu".

2 Caso não possa executar o Wireshark, utilize o arquivo dns-ethereal-trace-2 extraído do arquivo comapctado http://gaia.cs.umass.edu/ethereal-labs/ethereal-traces.zip.

A figura 7 mostra o resultado da captura dos pacotes. Nela estão a mensagem de consulta e a resposta DNS. Responda às questões:

1. qual é a porta destino para a mensagem de consulta DNS? Qual é a porta fonte para a mensagem de resposta DNS?
2. a qual endereço IP a mensagem de consulta DNS está endereçada? Este endereço é o de algum dos seus servidores DNS locais?
3. examine a mensagem de consulta DNS. Qual o campo "*type*" que há nela? A mensagem de consulta contém algum campo "*answer*"?
4. examine a mensagem de resposta DNS. Quantos campos com "answer" existem? O que há em cada uma destas respostas?
5. grave a tela de captura de pacotes.

Repita o experimento anterior para o comando: "nslookup -type=NS mit.edu", sem as aspas. Depois responda às questões:

1. a qual endereço IP a mensagem de consulta DNS está endereçada? Este endereço é o de algum dos seus servidores DNS locais?
2. examine a mensagem de consulta DNS. Qual o campo "type" que há nela? A mensagem de consulta contém algum campo "answer"?
3. examine a mensagem de resposta DNS. Quais servidores DNS do MIT são fornecidos na resposta? Esta mensagem de resposta também fornece os endereços IP dos servidores DNS do MIT?
4. grave a tela de captura de pacotes.

Repita o experimento anterior para o comando: "nslookup www.aiit.or.kr bitsy.mit.edu", sem as aspas. Depois responda às questões:

1. a qual endereço IP a mensagem de consulta DNS está endereçada? Este endereço é o de algum dos seus servidores DNS locais? Caso contrário, qual o *host* para este endereço IP?
2. examine a mensagem de consulta DNS. Qual o campo "type" que há nela? A mensagem de consulta contém algum campo "answer"?
3. examine a mensagem de resposta DNS. Quantos campos com "answer" existem? O que há em cada uma destas respostas?
4. grave a tela de captura de pacotes.