

Universidade Estadual da Paraíba
Departamento de Matemática, Estatística e Computação
Disciplina: Redes de Computadores
Professor: Edmar José do Nascimento

3º Exercício Prático: DNS

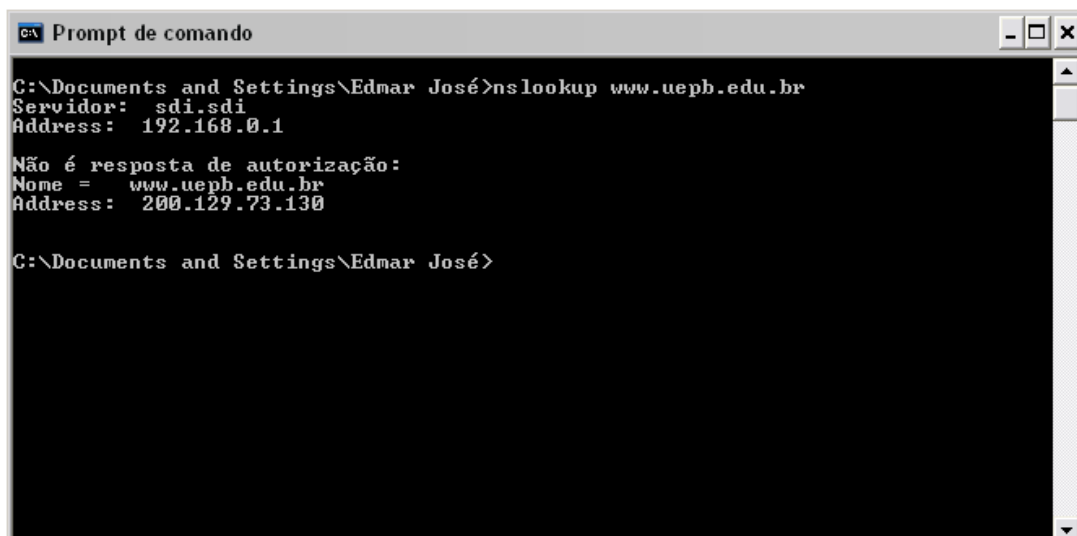
Introdução

O Sistema de Nome de Domínios (DNS, *Domain Name System*) traduz nomes de hospedeiros para endereços IP, tendo assim um papel crucial no funcionamento da Internet. Neste exercício prático vamos observar o funcionamento do DNS pelo lado do cliente. Relembre que o lado cliente do DNS tem uma função relativamente simples, ele pergunta ao seu DNS local e recebe a resposta. Muito do trabalho feito pelo DNS é invisível pelo cliente.

nslookup

Neste exercício usaremos extensivamente a ferramenta *nslookup*, que está disponível em muitas plataformas Linux/Unix e Microsoft Windows. Para executar o *nslookup* no Linux/Unix, você deve digitar o comando *nslookup*. Para executar no Windows, abra um Prompt de Comando e digite *nslookup*.

Na sua operação mais básica, *nslookup* permite que o host que roda a ferramenta faça perguntas a um servidor DNS específico. O DNS perguntado pode ser um servidor DNS raiz, um DNS de alto nível, um DNS com autoridade ou um servidor DNS intermediário. Para fazer essa tarefa, *nslookup* envia uma pergunta (*query*) DNS para o servidor DNS específico, recebe a resposta (*response*) desse DNS e mostra o resultado, veja o resultado de uma execução do *nslookup* na Figura 1.



```

C:\Documents and Settings\Edmar José>nslookup www.uepb.edu.br
Servidor:  sdi.sdi
Address:  192.168.0.1

Não é resposta de autorização:
Nome =  www.uepb.edu.br
Address:  200.129.73.130

C:\Documents and Settings\Edmar José>
```

Figura 1 - Utilização do nslookup para encontrar www.uepb.edu.br

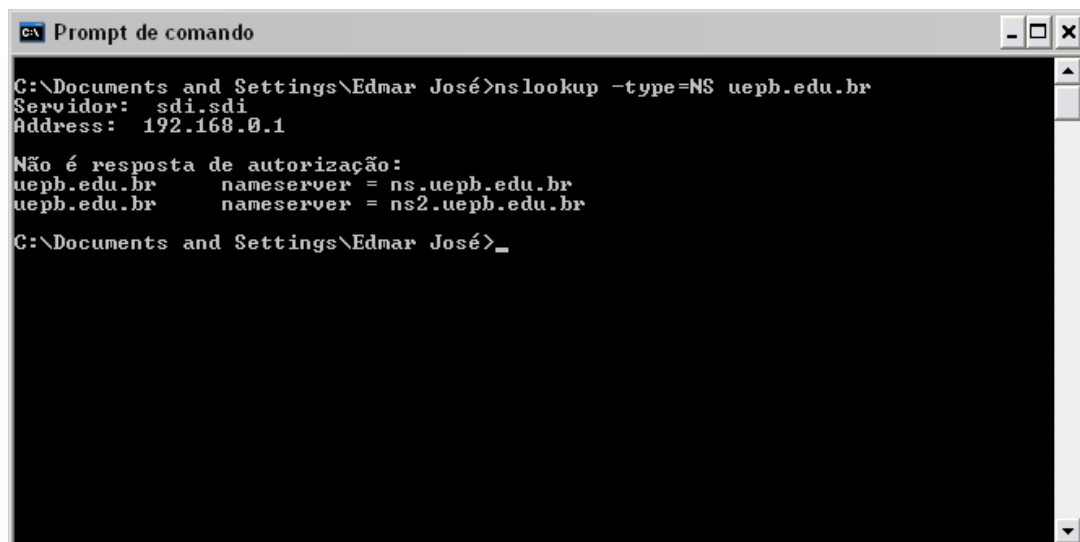
A Figura 1 mostra o resultado da execução do *nslookup* para determinar o endereço de *www.uepb.edu.br*. Neste exemplo, a máquina onde a busca foi iniciada está na rede do prédio em que o professor mora, a qual possui um servidor DNS local na máquina *sdi.sdi* cujo endereço é 192.168.0.1. Quando *nslookup* é executado, se nenhum servidor for especificado a busca é enviada para o servidor *default*, que neste caso foi informado ao sistema operacional nas configurações de rede.

Quando o comando: *nslookup www.uepb.edu.br* é executado, a resposta fornece duas informações (1) o nome e o IP do servidor DNS que respondeu à pergunta e (2) a resposta em si, que consiste no nome e o IP do site *www.uepb.edu.br*.

Agora seja o seguinte comando:

```
nslookup -type=NS uepb.edu.br
```

Neste exemplo, nós fornecemos a opção “-type=NS” e o domínio “uepb.edu.br”. Isto faz com que o *nslookup* envie uma pergunta para o registro do tipo “NS” para o servidor DNS local. Em outras palavras, a pergunta está dizendo: “por favor, envie-me o nome das máquinas do DNS com autoridade para uepb.edu.br”. Quando a opção -type não é usada, *nslookup* usa o *default* que é a busca por registros do tipo A. O resultado, mostrado na Figura 2, indica inicialmente o servidor DNS que está provendo a resposta (que é o DNS local), junto com os nomes dos servidores DNS responsáveis pelo domínio uepb.edu.br. Outro dado mostrado na Figura 2 é que a resposta não é de autorização, significando que ele veio do *cache* de algum servidor que não tem autoridade sobre uepb.edu.br. A resposta pode também incluir opcionalmente os endereços IP dos servidores de nomes, apesar da pergunta feita pelo *nslookup* não ser exatamente pelos IPs, mas sim pelos nomes dos servidores.



```
CA Prompt de comando
C:\Documents and Settings\Edmar José>nslookup -type=NS uepb.edu.br
Servidor: sdi.sdi
Address: 192.168.0.1

Não é resposta de autorização:
uepb.edu.br      nameserver = ns.uepb.edu.br
uepb.edu.br      nameserver = ns2.uepb.edu.br
C:\Documents and Settings\Edmar José>
```

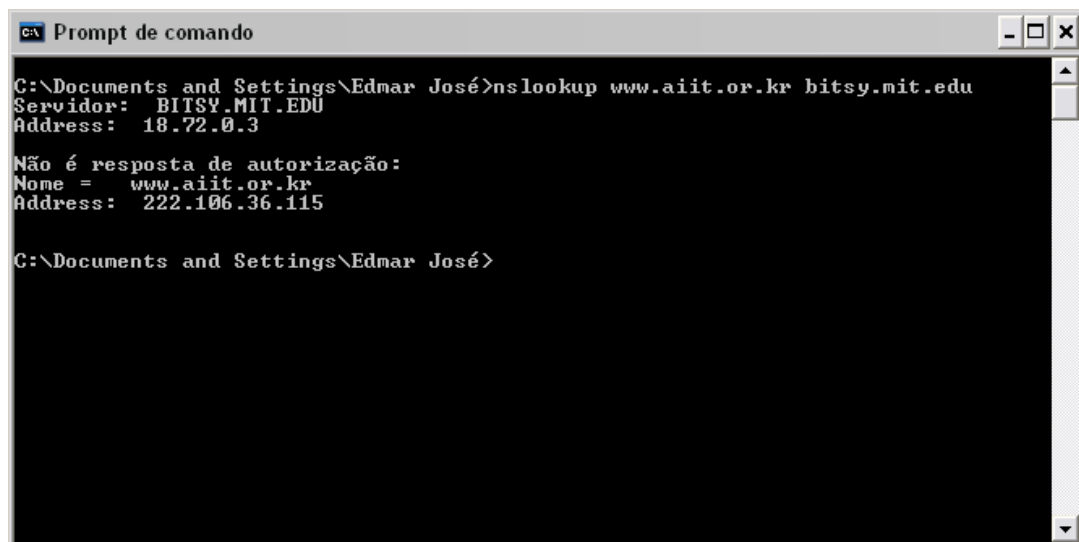
Figura 2 - Utilização do *nslookup* com a opção -type=NS

Agora finalmente seja o seguinte comando:

```
nslookup www.aiit.or.kr bitsy.mit.edu
```

Neste exemplo mostrado na Figura 3, indicamos que queremos enviar uma pergunta ao servidor DNS bitsy.mit.edu ao invés do servidor DNS local. Assim, a transação da

pergunta e da resposta são realizadas diretamente em bitsy.mit.edu. No exemplo, o servidor bitsy.mit.edu fornece o endereço IP do host www.aiit.or.kr, que é um servidor web do *Advanced Institute of Information Technology* (na Coreia do Sul).



```
C:\Documents and Settings\Edmar José>nslookup www.aiit.or.kr bitsy.mit.edu
Servidor:  BITSY.MIT.EDU
Address:  18.72.0.3

Não é resposta de autorização:
Nome =     www.aiit.or.kr
Address:  222.106.36.115

C:\Documents and Settings\Edmar José>
```

Figura 3 - Utilização do nslookup.

Agora que já observamos alguns exemplos ilustrativos, veja a sintaxe geral do comando nslookup:

```
nslookup -opção1 -opção2 hospedeiro-procurado servidor-dns
```

Em geral, *nslookup* pode rodar com nenhuma, uma, duas ou mais opções. E como vimos nos exemplos acima, o nome do servidor DNS é opcional, e caso ele não seja fornecido, a busca é enviada ao servidor DNS local.

Faça as seguintes tarefas:

1. Execute nslookup para obter o endereço IP de um servidor WEB nos Estados Unidos. Anote a resposta obtida.
2. Execute nslookup para determinar um servidor com autoridade para uma universidade na Europa. Anote a resposta obtida.
3. Execute nslookup para que um dos servidores DNS obtidos na questão 2 forneça o endereço do servidor de e-mails do GMAIL. Anote a resposta obtida.

ipconfig

ipconfig (para Windows) e *ifconfig* (para Linux/Unix) são comandos bastante úteis na sua máquina, especialmente para depurar uma rede. Aqui iremos descrever ipconfig, apesar do ifconfig ser bastante similar. ipconfig pode ser usado para mostrar as suas configurações TCP/IP atuais, incluindo seu endereço IP, servidor DNS, tipo do adaptador de rede e assim por diante. Por exemplo, se você quiser visualizar todas essas informações, basta fazer:

```
ipconfig /all
```

no prompt de comando, como mostrado na Figura 4.

```
C:\Documents and Settings\Edmar José>ipconfig /all

Configuração de IP do Windows

Nome do host . . . . . : Edmar
Sufixo DNS primário. . . . . :
Tipo de nó . . . . . : misto
Roteamento de IP ativado . . . . . : sim
Proxy WINS ativado . . . . . : não
Lista de pesquisa de sufixo DNS. . . . . : sdi

Adaptador Ethernet Conexão local:

Sufixo DNS específico de conexão . . : sdi
Descrição . . . . . : Broadcom 440x 10/100 Integrated Co
ntroller
Endereço físico . . . . . : 00-14-22-98-6A-7D
DHCP ativado. . . . . : Sim
Configuração automática ativada . . : Sim
Endereço IP . . . . . : 192.168.0.14
Máscara de sub-rede . . . . . : 255.255.255.0
Gateway padrão. . . . . : 192.168.0.1
Servidor DHCP . . . . . : 192.168.0.1
Servidores DNS . . . . . : 192.168.0.1
                          200.165.132.147
                          200.165.132.154
Concessão obtida. . . . . : sábado, 4 de outubro de 2008 08:52
:07
Concessão expira. . . . . : terça-feira, 19 de janeiro de 2038
00:14:07

Adaptador Ethernet Conexão de rede sem fio 2:

Estado da mídia . . . . . : mídia desconectada
Descrição . . . . . : Intel(R) PRO/Wireless 2200BG Netwo
rk Connection
Endereço físico . . . . . : 00-16-6F-40-B6-74

Adaptador Ethernet Conexão local 2:

Estado da mídia . . . . . : mídia desconectada
Descrição . . . . . : Bluetooth PAN Network Adapter
Endereço físico . . . . . : 10-11-11-11-11-11

C:\Documents and Settings\Edmar José>
```

Figura 4 - Utilização do ipconfig.

Ipconfig também é muito útil para gerenciar informações do DNS armazenadas no seu computador. Vimos que uma máquina faz um cachê das últimas respostas do DNS, para ver o que está no *cache*, basta executar:

```
ipconfig /displaydns
```

Cada entrada mostra o *Time to Live* (TTL) em segundos restantes. Para limpar o cache, faça:

```
ipconfig /flushdns
```

Analizando o DNS com o Wireshark

Agora que já estamos familiarizados com nslookup e ipconfig podemos fazer algo mais sério. Vamos inicialmente capturar pacotes DNS gerados pela navegação WEB comum.

- Use ipconfig para esvaziar o *cache* do DNS da sua máquina.
- Abra seu navegador e limpe o *cache* (você já fez isso no exercício passado).

- Abra o Ethereal e entre com “ip.addr == seu_endereço_IP” no filtro de pacotes. Você pode obter o seu endereço IP com ipconfig. Este filtro remove todos os pacotes que não foram gerados e nem são destinados a sua máquina.
- Inicie a captura de pacotes no Wireshark.
- Com o seu navegador visite: <http://www.ietf.org>
- Pare a captura de pacotes.

Responda as seguintes questões;

4. Localize as mensagens DNS de pergunta e resposta. Elas são enviadas por TCP ou por UDP?
5. Qual é a porta de destino da mensagem DNS query? Qual a porta fonte da resposta DNS?
6. Para qual endereço IP a mensagem DNS query foi enviada? Use ipconfig para determinar o endereço IP do servidor DNS local. Esses dois endereços IPs são os mesmos?
7. Examine a mensagem DNS query. Que tipo de consulta é essa mensagem? A mensagem query contém qualquer resposta?
8. Examine a mensagem DNS de resposta. Quantas respostas são fornecidas? O que cada resposta contém?
9. Considere os pacotes TCP SYN enviados pelo seu host. O endereço IP destino dos pacotes SYN correspondem ao IP fornecido na mensagem DNS de resposta?
10. O web site que você visitou possui imagens? Antes de receber as imagens foram necessárias novas mensagens de consulta ao DNS?

Vamos trabalhar com nslookup.

- Inicie a captura de pacotes.
- Faça um *nslookup* em www.mit.edu
- Pare a captura de pacotes

Observando a saída, responda as seguintes questões:

11. Qual é a porta destino das mensagens de consulta ao DNS? Qual é a porta fonte da mensagem DNS de resposta?
12. Para qual endereço IP o DNS enviou a mensagem de consulta ao DNS? Este IP é o seu ou do seu servidor DNS local?
13. Examine as mensagens de consulta ao DNS. Qual é o “Type” da consulta ao DNS?
14. Examine a mensagem de resposta ao DNS. Quantas respostas são fornecidas? O que cada uma dessas respostas contém?

Agora repita o experimento com o seguinte comando:
 nslookup -type=NS mit.edu

Responda as seguintes questões:

15. Para qual endereço IP a mensagem de consulta ao DNS foi enviada? É o IP da sua máquina ou do DNS local?
16. Examine as mensagens de consulta ao DNS. Qual é o “Type” da consulta ao DNS?

17. Examine a mensagem de resposta ao DNS. Quantas respostas são fornecidas? O que cada uma dessas respostas contém?

Agora repita o experimento anterior, mas com o seguinte comando:
nslookup www.aiit.or.kr bitsy.mit.edu

Responda as seguintes questões:

18. Para qual endereço IP a mensagem de consulta ao DNS foi enviada? É o IP da sua máquina ou do DNS local?
19. Examine as mensagens de consulta ao DNS. Qual é o “Type” da consulta ao DNS?
20. Examine a mensagem de resposta ao DNS. Quantas respostas são fornecidas? O que cada uma dessas respostas contém?