



03 AULA PRÁTICA – Domain Name System: DNS (WIRESHARK) (Baseada nas Práticas do livro de James Kurose – 4Edição)

Nesta terceira aula prática usando o Wireshark, exploraremos os aspectos simples do lado cliente do protocolo DNS.

nslookup

Usaremos a ferramenta nslookup nesta aula de laboratório. O nslookup é um comando que funciona tanto no prompt do Windows como no Linux. Ele permite obter informações sobre registros de DNS sobre um determinado domínio, host ou IP. Em uma busca nslookup padrão, o servidor DNS do provedor de acesso é consultado, e retorna as informações sobre o domínio ou host pesquisado. A Figura 1 ilustra exemplos de sua utilização.

No exemplo da Figura 1, o host cliente é localizado no Campus da Polytechnic University no Brooklyn, onde o servidor local padrão DNS é dns-prime.poly.edu. Quando executado o nslookup, se nenhum servidor DNS é especificado, então nslookup envia a requisição para o servidor default DNS, que neste caso é dnsprime.poly.edu.

```
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.aiit.or.kr bitsy.mit.edu
Server: BITSY.MIT.EDU
Address: 18.72.0.3

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

C:\>
```

Figura 1. Exemplo da execução do nslookup

Considere o comando: ***nslookup www.mit.edu.***

Em palavras, este comando está dizendo “Por favor, envie-me o endereço IP para o host www.mit.edu”. A resposta para este comando tem duas informações: (1) o nome e o endereço IP do servidor DNS que provê a resposta; (2) a resposta em si, que é o nome do host e o endereço IP do www.mit.edu. Embora a resposta venha do servidor local DNS da

Polytechnic University, é bastante possível que este servidor local DNS interativamente contactou vários outros servidores DNS para obter a resposta.

Nota1: Em uma busca nslookup padrão, o servidor DNS do provedor de acesso é consultado, e retorna as informações sobre o domínio ou host pesquisado.

Nota2: Se a informação "Não é resposta de autorização" apareceu, significa que o servidor DNS do provedor de acesso não responde por este domínio, ou seja, isto significa que uma consulta externa foi realizada, aos servidores DNS do domínio pesquisado (neste caso, mit.edu). Em outras palavras, indica apenas que o servidor não é responsável pelo domínio consultado.

Agora, considere o segundo comando: **nslookup -type=NS mit.edu**

Neste exemplo, nós temos providenciado a opção "-type=NS" e o domínio "mit.edu". Isto causa o nslookup enviar uma requisição para um registro type-NS para o servidor padrão local DNS. Em palavras, a requisição está dizendo: "Por favor, envie-me os nomes do host do servidor de autoridade para mit.edu." (Quando a opção -type não é usada, nslookup usa o padrão que é a busca por registros do tipo A).

A resposta dada indica o servidor DNS que está providenciando a resposta (que é o servidor local padrão DNS) e com três servidores de nomes MIT. Cada um destes servidores é um servidor de autoridade DNS para os hosts no Campus MIT. Entretanto, nslookup também indica que a resposta veio do cache de algum servidor ao invés de um servidor DNS do MIT. Finalmente, a resposta também inclui os endereços IP dos servidores de autoridade DNS no MIT.

Finalmente considere o terceiro comando: **nslookup www.aiit.or.kr bitsy.mit.edu.**

Neste exemplo, nós indicamos que desejamos a requisição enviada para o servidor DNS bitsy.mit.edu ao invés do servidor padrão DNS (dns-prime.poly.edu). Assim, a transação de requisição e resposta toma lugar diretamente entre o host que solicita e o servidor bitsy.mit.edu. Neste exemplo, o servidor DNS bitsy.mit.edu provê o endereço IP do host www.aiit.or.kr, que é um servidor no Advanced Institute of Information Technology (na Korea).

Finalizando, a sintaxe geral do comando nslookup. A sintaxe é:

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

Em geral, nslookup pode ser executado com zero, uma, duas ou mais opções. Agora, teste o comando nslookup. Faça o seguinte:

1. Execute nslookup para obter o endereço IP de um servidor Web no Brasil.
2. Execute nslookup para determinar o servidor de autoridade DNS para um endereço IP qualquer.
3. Execute nslookup para os servidores de e-mail para o Yahoo! mail.

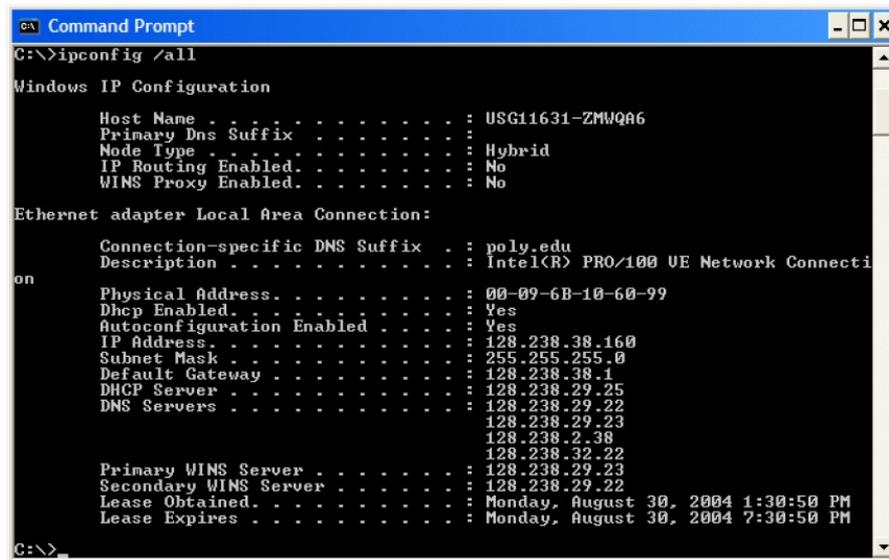
ipconfig

Ipconfig (para Windows) e ifconfig (para Linux/Unix) estão entre as mais úteis ferramentas, especialmente para "debugar" questões da rede. Vamos descrever somente o ipconfig (muito parecido com o ifconfig) nesta aula prática.

Ipconfig pode ser usado para mostrar a informação atual TCP/IP, incluindo seu endereço IP, endereço de servidor DNS, tipo de adaptador e etc. Por exemplo, se você deseja

ver as informações sobre seu host, simplesmente digite no prompt do Windows (como mostrado na Figura 2): **ipconfig /all**

ipconfig é também muito útil para gerenciar a informação DNS armazenada no host. Para ver os registros armazenados em cache, digite o seguinte comando: **ipconfig /displaydns**



```
C:\>ipconfig /all

Windows IP Configuration

Host Name . . . . . : USG11631-ZMWQ06
Primary Dns Suffix . . . . . : poly.edu
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . : poly.edu
Description . . . . . : Intel(R) PRO/100 UE Network Connecti
on
Physical Address. . . . . : 00-09-6B-10-60-99
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IP Address. . . . . : 128.238.38.160
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 128.238.38.1
DHCP Server . . . . . : 128.238.29.25
DNS Servers . . . . . : 128.238.29.22
                        128.238.29.23
                        128.238.2.38
                        128.238.32.22
Primary WINS Server . . . . . : 128.238.29.23
Secondary WINS Server . . . . . : 128.238.29.22
Lease Obtained. . . . . : Monday, August 30, 2004 1:30:50 PM
Lease Expires . . . . . : Monday, August 30, 2004 7:30:50 PM

C:\>
```

Figura 2. Exemplo de ipconfig

Cada entrada mostra o restante Tempo de Vida (Time to Live - TTL) em segundos.

Nota: Se desejar, você pode popular entradas de DNS no arquivo `\WINDOWS\system32\drivers\etc\hosts` que armazena as informações sobre DNS. As entradas registradas neste arquivo tem prioridade sobre as entradas pesquisas em servidores DNS.

Para limpar o cache, digite **ipconfig /flushdns**

Este commando limpa o cache DNS com todas as suas entradas.

Nota: Se a resposta for “A operação solicitada requer elevação”, significa que você não possui permissão de administrador para executar a tarefa. Vá em Iniciar>Programas>Acessórios>Prompt. Clique com o botão direito do mouse e selecione “Execute como administrador”.

DNS com Wireshark

Vamos capturar os pacotes DNS que são gerados.

- Use ipconfig para esvaziar o cache DNS em seu host.
- Inicie seu navegador e esvazie o cache do navegador.
- Execute Wireshark e digite “ip.addr == seu_endereço_IP” no campo de filtro, onde você obtém o endereço do computador que está executando Wireshark com ipconfig. Este filtro remove todos os pacotes que não foram originados ou destinados para seu host.
- Inicie captura de pacotes no Wireshark.

- Com seu navegador, visite o site <http://www.ietf.org>
- Finalize a captura de pacotes.

Responda às seguintes questões:

4. Localize as mensagens de requisição e resposta DNS. Elas são enviadas sobre o UDP ou TCP?
5. Qual a porta destino para a mensagem de requisição DNS? Qual é a porta fonte da mensagem DNS?
6. Para qual endereço IP a mensagem de requisição DNS é enviada? Use ipconfig para determinar o endereço IP de seu servidor local DNS. Esses dois endereços IP são os mesmos?
7. Examine a mensagem de requisição DNS. Qual o tipo de requisição DNS? A mensagem de requisição contém quais “respostas”?
8. Examine a mensagem DNS response. Quantas “respostas” são providas? O que cada resposta contém?
9. Considere o pacote subsequente TCP SYN enviado pelo seu host. O endereço IP destino do pacote SYN corresponde ao endereços IP fornecido pela mensagem response DNS?
10. Este site contém imagens. Antes de recuperar cada imagem, seu host requer novas requisições DNS?

Agora vamos usar novamente o nslookup.

- Inicie captura de pacotes.
- Faça um nslookup no www.mit.edu
- Finalize a captura de pacotes.

Você deve obter um trace que seja parecido com o da Figura 3 abaixo.

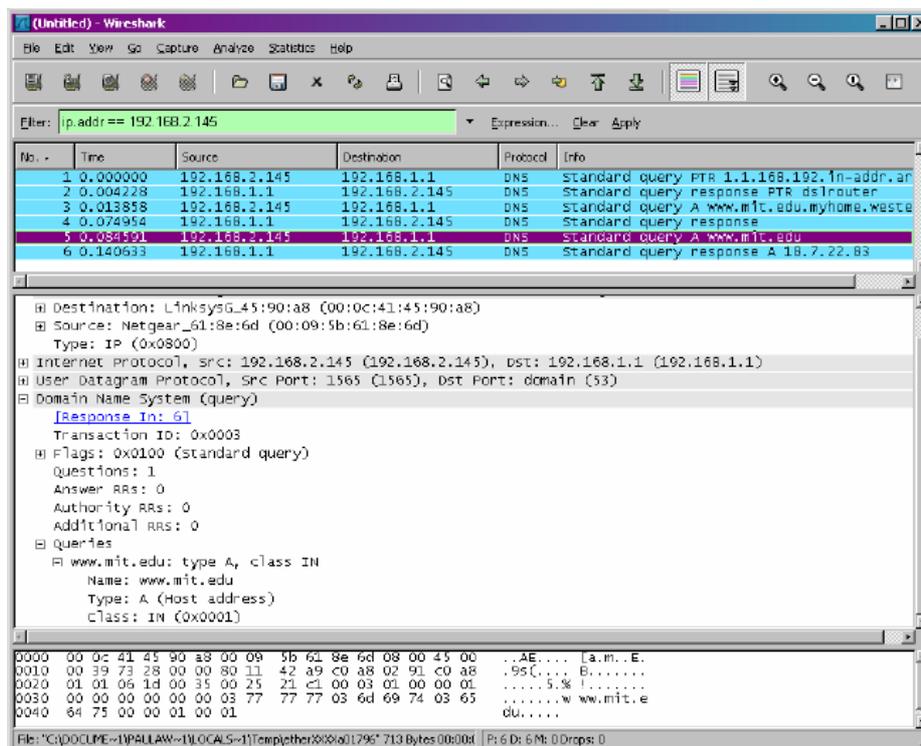


Figura 3. Nslookup – Outro exemplo

Nota-se na Figura 3 que o nslookup atualmente enviou três requisições DNS e recebeu três DNS response. Para responder às questões seguintes, ignore os dois primeiros conjuntos de requisições/responses (como eles são específicos do nslookup e não são normalmente

gerados pela aplicações padrões. Você deve ao invés disso, focar nas últimas mensagens de requisições e respostas).

11. Qual a porta destino para a mensagem de requisição DNS? Qual é porta fonte da mensagem DNS response?
12. Para qual endereço IP a mensagem de requisição DNS é enviada? Este é o endereço IP de seu servidor default local DNS?
13. Examine a mensagem de requisição DNS. Qual é o tipo mensagem de requisição DNS? A mensagem de requisição contém quais “respostas”?
14. Examine a mensagem DNS response. Quantas “respostas” são providas? O que cada uma dessas mensagens contém?

Agora repita o experimento anterior, mas com o comando:

nslookup -type=NS mit.edu

Responda as seguintes questões:

16. Para qual endereço IP a mensagem de requisição DNS é enviada? Este é o endereço IP de seu servidor default local DNS?
17. Examine a mensagem de requisição DNS. Qual é o tipo da mensagem de requisição DNS? A mensagem de requisição contém quais “respostas”?
18. Examine a mensagem DNS response. Quantos nomes de servidores MIT a mensagem response provê? Esta mensagem response também prove endereços IP dos servidores de nome MIT?

Agora repita o experimento anterior, mas execute o comando:

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

Responda as seguintes questões:

20. Para qual endereço a mensagem de requisição DNS é enviada? Este é o endereço IP de seu servidor default local DNS? Se não, qual é o endereço IP correspondente?
21. Examine a mensagem de requisição DNS. Qual o tipo de requisição de DNS? A mensagem de requisição contém alguma “resposta”?
22. Examine a mensagem response DNS. Quantas “respostas” são dadas? O que cada resposta contém?

“Conte-me e eu esquecerei. Mostre-me e eu lembrarei. Envolve-me e eu compreenderei.”
Provérbio Chinês