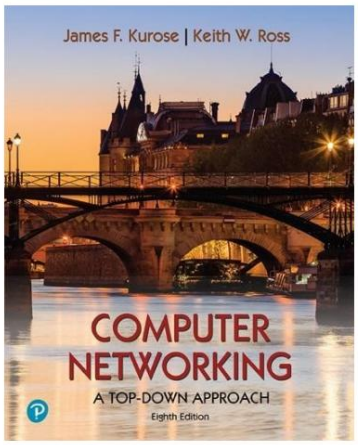
Laboratório Wireshark: DNS v8.1



Suplemento para *Redes de Computadores: Uma Abordagem de Cima para Baixo, 8ª ed.,* JF Kurose e KW Ross

"Diga-me e eu esqueço. Mostre-me e eu lembro. Envolva-me e eu entendo." Provérbio chinês

---

Conforme descrito na Seção 2.4 do texto, o Sistema de Nomes de Domínio (DNS) traduz nomes de host para endereços IP, cumprindo uma função crítica na infraestrutura da Internet. Neste laboratório, daremos uma olhada mais de perto no lado do cliente do DNS. Lembre-se de que a função do cliente no DNS é relativamente simples – um cliente envia uma *consulta* para seu servidor DNS local e recebe uma *resposta* de volta. Conforme mostrado nas Figuras 2.19 e 2.20 no livro didático, muita coisa pode acontecer "por baixo dos panos", invisível para um cliente DNS, pois os servidores DNS hierárquicos se comunicam entre si para resolver recursivamente ou iterativamente a consulta DNS do cliente. Do ponto de vista do cliente DNS, no entanto, o protocolo é bem simples – uma consulta é formulada para o servidor DNS local e uma resposta é recebida desse servidor.

Antes de começar este laboratório, você provavelmente vai querer revisar o DNS lendo a Seção 2.4 do texto. Em particular, você pode querer revisar o material sobre **servidores DNS locais, cache DNS, registros e mensagens DNS** e o **campo TYPE** no registro DNS.

1. nslookup

Vamos começar nossa investigação do DNS examinando o comando nslookup , que invocará os serviços DNS subjacentes para implementar sua funcionalidade. O comando nslookup está disponível na maioria dos sistemas operacionais Microsoft, Apple IOS e Linux. Para executar o nslookup , basta digitar o comando nslookup na linha de comando em uma janela DOS, janela de terminal Mac IOS ou shell Linux.

Em sua operação mais básica, o nslookup permite que o host que executa o nslookup consulte qualquer servidor DNS especificado para um registro DNS. O servidor DNS consultado pode ser um servidor DNS raiz, um servidor DNS de domínio de nível superior (TLD), um servidor DNS autoritativo ou um servidor DNS intermediário (consulte o livro-texto para obter as definições desses termos). Por exemplo, o nslookup pode ser usado para recuperar um registro DNS “Tipo=A” que mapeia um nome de host (por exemplo, www.nyu.edu) para seu endereço IP. Para realizar essa tarefa, o nslookup envia uma consulta DNS para o servidor DNS especificado (ou o servidor DNS local padrão para o host no qual o nslookup é executado, se nenhum servidor DNS específico for especificado), recebe uma resposta DNS desse servidor DNS e exibe o resultado.

Vamos dar uma volta no nslookup ! Primeiro, executaremos o nslookup na linha de comando do Linux no host newworld.cs.umass.edu localizado no Departamento de Ciência da Computação do campus da Universidade de Massachusetts (UMass), onde o servidor de nomes local é chamado primo.cs.umass.edu (que tem um endereço IP 128.119.240.1). Vamos tentar o nslookup em sua forma mais simples:

```
newworld.cs.umass.edu> nslookup www.nyu.edu
Server:         128.119.240.1
Address:        128.119.240.1#53

Non-authoritative answer:
www.nyu.edu     canonical name = WEB.GSLB.nyu.edu.
Name:   WEB.GSLB.nyu.edu
Address: 216.165.47.12
Name:   WEB.GSLB.nyu.edu
Address: 2607:f600:1002:6113::100
```

Figura 1: o comando básico nslookup

Neste exemplo, o comando nslookup recebe um argumento, um nome de host (www.nyu.edu). Em palavras, este comando está dizendo “por favor, envie-me o endereço IP do host www.nyu.edu.” Conforme mostrado na captura de tela, a resposta deste comando fornece duas informações: (1) o nome e o endereço IP do servidor DNS que fornece a resposta – neste caso, o servidor DNS local na UMass; e (2) a resposta em si, que é o nome do host canônico e o endereço IP de www.nyu.edu. Você deve ter notado que há dois pares nome/endereço fornecidos para www.nyu.edu. O primeiro (216.165.47.12) é um endereço IPv4 na notação decimal pontilhada de aparência familiar; o segundo (2607:f600:1002:6113::100) é um endereço IPv6 mais longo e de aparência mais complicada. Aprenderemos sobre IPv4 e IPv6 e seus dois esquemas de endereçamento diferentes mais adiante no Capítulo 4. Por enquanto, vamos nos concentrar apenas em nosso mundo IPv4 mais confortável (e comum)1 .

[1] Para Mac OS, se você quiser trabalhar apenas no mundo IPv4: Preferências do sistema -> Rede. Em seguida, selecione sua interface ativa (por exemplo, Wi-Fi) e Avançado->TCP/IP. Em seguida, selecione o menu suspenso Configurar IPv6

Embora a resposta tenha vindo do servidor DNS local (com endereço IP 128.119.240.1) na UMass, é bem possível que esse servidor DNS local tenha contatado iterativamente vários outros servidores DNS para obter a resposta, conforme descrito na Seção 2.4 do livro didático.

Além de usar o nslookup para consultar um registro DNS “Tipo=A”, também podemos usar o nslookup para consultar um registro “TIPO=NS”, que retorna o nome do host (e seu endereço IP) de um servidor DNS autoritativo que sabe como obter os endereços IP para hosts no domínio do servidor autoritativo.

Figura 2: usando nslookup para encontrar os servidores de nomes autorizados para o domínio nyu.edu

No exemplo da Figura 2, invocamos o nslookup com a opção “-type=NS” e o domínio “nyu.edu”. Isso faz com que o nslookup envie uma consulta para um registro do tipo NS para o servidor DNS local padrão. Em palavras, a consulta está dizendo, “por favor, envie-me os nomes de host do DNS autoritativo para nyu.edu”. (Quando a opção –type não é usada, *o nslookup* usa o padrão, que é consultar registros do tipo A.) A resposta, exibida na captura de tela acima, primeiro indica o servidor DNS que está fornecendo a resposta (que é o servidor DNS local padrão da UMass com endereço 128.119.240.1) junto com três servidores de nomes DNS da NYU. Cada um desses servidores é de fato um servidor DNS autoritativo para os hosts no campus da NYU. No entanto, o nslookup também indica que a resposta é “não autoritativa”, o que significa que essa resposta veio do cache de algum servidor em vez de um servidor DNS autoritativo da NYU. Por fim, a resposta também inclui os endereços IP dos servidores DNS autoritativos da NYU. (Embora a consulta do tipo NS gerada pelo nslookup não tenha solicitado explicitamente os endereços IP, o servidor DNS local retornou esses “de graça” e *o nslookup* exibe o resultado.)

O nslookup tem uma série de opções adicionais além de “-type=NS” que você pode querer explorar. Aqui está um site com capturas de tela de dez usos populares do nslookup : https://www.cloudns.net/blog/10-most-used-nslookup-commands/ e aqui estão as “páginas de manual” do nslookup: https://linux.die.net/man/1/nslookup.

menu e defina-o como “Link-local only” ou “Off”.

Por fim, às vezes podemos estar interessados em descobrir o nome do host associado a um determinado endereço IP, ou seja, o inverso da pesquisa mostrada na Figura 1 (onde o nome do host era conhecido/especificado e o endereço IP do host era retornado). O nslookup também pode ser usado para executar essa chamada "pesquisa reversa de DNS". Na Figura 3, por exemplo, especificamos um endereço IP como o argumento nslookup (128.119.245.12 neste exemplo) e o nslookup retorna o nome do host com esse endereço (gaia.cs.umass.edu neste exemplo)

Figura 3: usando nslookup para executar uma “pesquisa reversa de DNS”

Agora que fornecemos uma visão geral do nslookup, é hora de você testá-lo você mesmo. Faça o seguinte (e anote os resultados).

Figura 4: usando nslookup para encontrar o endereço IP de www.iitb.ac.in e os nomes dos servidores de nomes autorizados para o domínio iitb.ac.in

Sobre essa parte, execute e responda as questões de 1 a 4 na Atividade 4.

2. O cache DNS no seu computador

A partir da descrição da resolução de consulta DNS iterativa e recursiva (Figuras 2.19 e 2.20) em nosso livro, você pode pensar que o servidor DNS local deve ser contatado *toda* vez que um aplicativo precisa traduzir de um nome de host para um endereço IP. Isso nem sempre é verdade na prática!

A maioria dos hosts (por exemplo, seu computador pessoal) mantém um *cache* de registros DNS recuperados recentemente (às vezes chamado de *cache de resolução de DNS),* assim como muitos navegadores da Web mantêm um cache de

objetos recuperados recentemente por HTTP. Quando serviços DNS precisam ser invocados por um host, esse host primeiro verificará se o registro DNS necessário é residente no cache DNS desse host; se o registro for encontrado, o host nem se incomodará em contatar o servidor DNS local e, em vez disso, usará esse registro DNS em cache. Um registro DNS em um cache de resolução acabará expirando e será removido do cache de resolução, assim como os registros em cache em um servidor DNS local (veja Figuras 2.19, 2.20) expirarão.

Você também pode limpar explicitamente os registros no seu cache DNS. Não há mal nenhum em fazer isso – isso significa apenas que seu computador precisará invocar o serviço DNS distribuído na próxima vez que precisar usar o serviço de resolução de nomes DNS, já que não encontrará registros no cache. Em um computador Mac, você pode digitar o seguinte comando em uma janela de terminal para limpar o cache do seu resolvedor DNS:

```
sudo killall -HUP mDNSResponder
```

No computador Windows, você pode digitar o seguinte comando no prompt de comando:

```
ipconfig /flushdns
```

e em um computador Linux, digite:

```
sudo systemd-resolve --flush-caches
```

3. Rastreando DNS com Wireshark

Agora que estamos familiarizados com o nslookup e a limpeza do cache do resolvedor DNS, estamos prontos para começar a trabalhar seriamente. Vamos primeiro capturar as mensagens DNS que são geradas pela atividade comum de navegação na Web.

- Limpe o cache DNS no seu host, conforme descrito acima.
- Abra seu navegador da Web e limpe o cache do navegador.
- Abra o Wireshark e digite ip.addr == <seu_endereço_IP> no filtro de exibição, onde <seu_endereço_IP> é o endereço IPv4 do seu computador[2] . Com esse filtro, o Wireshark exibirá apenas pacotes originados ou destinados ao seu host.
- Inicie a captura de pacotes no Wireshark.
- Com seu navegador, visite a página da Web: http://gaia.cs.umass.edu/kurose_ross/
- Pare a captura de pacotes.

---

2 Se não tiver certeza de como encontrar o endereço IP do seu computador, você pode pesquisar na Web por artigos sobre seu sistema operacional. As informações do Windows 10 estão aqui; Informações sobre Mac estão aqui: Informações sobre Linux estão aqui

Se você não conseguir executar o Wireshark em uma conexão de rede ativa, você pode baixar um arquivo de rastreamento de pacotes que foi capturado ao seguir as etapas acima em um dos computadores do autor.

Sobre essa parte, execute e responda as questões de 5 a 11 na Atividade 4.

Agora vamos brincar com o nslookup.

- Iniciar captura de pacotes.
- Faça uma pesquisa nslookup em www.cs.umass.edu
- Pare a captura de pacotes.

Você deve obter um rastreamento que se parece com o seguinte na sua janela do Wireshark. Vamos dar uma olhada na primeira consulta do tipo A (que é o pacote número 19 na figura abaixo, e indicado pelo “A” na coluna *Info* para esse pacote.

Sobre essa parte, execute e responda as questões de 12 a 15 na Atividade 4.

Por último, vamos usar o nslookup para emitir um comando que retornará um registro DNS do tipo NS, Digite o seguinte comando:

nslookup –type=NS umass.edu

Sobre essa parte, execute e responda as questões de 16 a 18 na Atividade 4.

Agora repita o experimento anterior, mas em vez disso emita o comando:

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

Sobre essa parte, execute e responda as questões de 19 a 21 na Atividade 4.