UNIVERSIDADE ESTADUAL DO OESTE DO PARANÁ
CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS
COLEGIADO DE CIÊNCIA DA COMPUTAÇÃO

Relatório de Aula Prática – Redes de Computadores

Título: DNS
Aluno: Vitor Mayorca Camargo Data: 11/09/2024

---

1. INTRODUÇÃO

A internet surgiu por volta de 1960 com o nome de ARPANET, e era um projeto do Departamento de Defesa norte-americano, que procurava criar uma rede de computadores descentralizada e capaz de operar mesmo em casos de ataques. Por muitos anos, a ARPANET foi usada exclusivamente nos Estados Unidos como meio de comunicação interno militar e acadêmico (LEINER, et al. 2009).

Originalmente, a internet possuía um número limitado de hospedeiros. Logo, para facilitar a comunicação entre eles, era usada uma tabela que relacionava cada hospedeiro com seu nome e endereço. Porém, o aumento da escala da internet fez com que essa metodologia se tornasse cada vez mais difícil de gerenciar. Logo, em 1983 Paul Mockapetris criou o protocolo Domain Name System (RFC 1035), ou DNS, que permitia a criação de mecanismos distribuídos escaláveis, capazes de converter nomes de hospedeiros hierárquicos (domínio) em um endereço de internet (endereço IP) (LEINER *et al.* 2009).

Os domínios da internet são organizados numa hierarquia, que identifica e categoriza servidores web. Segundo Tanenbaum (2003), os domínios têm 3 camadas: Nível Superior, Segundo Nível, e Terceiro Nível. Existem mais de 200 domínios de nível superior, onde cada domínio cobre vários hosts. Os dois tipos de domínios de nível superior são: genéricos (.com, .gov, .org, .net, …); e de países (.us, .br, .io, .fr, .jp, …). O Domínio de Segundo Nível geralmente é escolhido livremente pelo dono do domínio, e geralmente é um nome de uma empresa, pessoa, ou organização. Por fim, temos o Domínio de Terceiro Nível (ou Subdomínio), que é opcional, e separa um servidor em diferentes seções/serviços. No final, o nome do domínio é visualizado como:

$$Subdomínio + '.' + Segundo\,Nível + '.' + Nível\,Superior$$

Sendo assim, o protocolo DNS também irá funcionar por meio de uma hierarquia de 3 camadas de servidores DNS. São eles: Servidores DNS Raiz, Servidores DNS de domínio de alto nível (**TLD**); e Servidores DNS autoritativos. Também existe o Servidor DNS local, que não pertence à hierarquia DNS, mas é essencial para o processo como um todo (KUROSE, ROSS. 2021).

Segundo Kurose e Ross (2021), o protocolo DNS funciona da seguinte maneira: inicialmente, um usuário faz uma requisição ao servidor de DNS local, enviando o nome do hospedeiro a ser traduzido para um endereço IP. O servidor DNS local consulta um servidor DNS raiz, que identifica o domínio de nível superior, e retorna uma lista de endereços IP contendo servidores TLD responsáveis pelo domínio identificado. Então, o servidor DNS local consulta um desses servidores TLD, que identifica o domínio de segundo nível, e retorna o servidor que o hospeda. Por fim, o servidor DNS local envia uma mensagem a esse hospedeiro, que identifica o subdomínio (se existir), e por fim retorna o endereço IP da URL enviada pelo cliente. Toda essa comutação de

pacotes ocorre utilizando protocolo UDP.

Junto com o endereço de IP, todo domínio possui diversos recursos associados a ele, armazenados no registro de recursos. Cada registro é uma tupla de 5 valores, contendo Domain_name, Time_to_Live (TTL), Class, Type, e Value. Domain_name é o nome do domínio ao qual se associa; TTL é o tempo de vida útil do registro; Class indica o tipo de rede ao qual o registro se aplica, geralmente sendo “IN” (internet); Type indica o tipo do recurso ao qual o registro se refere; e Value é o valor associado ao tipo informado. Conforme Tanenbaum (2003), os principais tipos são:

- **A:** Endereço de IPv4 associado, com 32 bits;
- **AAAA:** Endereço IPv6 associado, com 128 bits;
- **SOA:** Start of Authority. Contém informações administrativas sobre uma zona DNS;
- **MX:** Define os servidores de e-mail responsáveis por receber e-mails para um domínio;
- **NS:** Indica os servidores DNS responsáveis por um domínio;
- **CNAME:** Indica o nome canônico de um domínio;
- **PTR:** Associa um endereço IP a um nome de domínio, permitindo uma espécie de busca por “DNS Reverso”;
- **HINFO:** Mostra informações sobre o hardware do hospedeiro;
- **TXT:** Armazena informações de texto.

Os pacotes de requisição DNS são divididos em 5 seções: O *cabeçalho*, de 12 bytes, que contém diversas informações básicas sobre o pacote; a *seção de questão*, com informações sobre a consulta sendo feita; a *seção de resposta*, presente apenas na resposta de um servidor DNS, e contém o valor dos registros consultados anteriormente; a *seção de autoridade*, que contém registros de outros servidores autoritativos; e a *seção adicional*, que contém informações extras, caso necessário (KUROSE, ROSS. 2021).

Normalmente, os pacotes do protocolo DNS são invisíveis ao usuário. Porém, eles podem ser visualizados usando ferramentas conhecidas como sniffers de rede. Essas ferramentas capturam e analisam o tráfego de rede, permitindo a visualização dos pacotes em tempo real. As duas ferramentas de sniffing de redes mais populares são o Wireshark e o Tcpdump (GOYAL, GOYAL. 2017). Além disso, a ferramenta *nslookup* também pode ser utilizada para requisitar e verificar todas as informações dos pacotes DNS (KUROSE, ROSS. 2021).

2. OBJETIVOS

A atividade prática realizada no dia 29/08/2024 teve como objetivo entender o funcionamento do protocolo DNS, com o uso da ferramenta “*nslookup*", junto com o sniffer de rede *wireshark*. Os testes foram feitos com diversos servidores web distribuídos ao redor do mundo.

3. MATERIAL UTILIZADO

Os testes foram realizados numa máquina virtual, executando num notebook da marca DELL, modelo Vostro 3520, com um CPU Intel Core i7-1255U 1.70 GHz, 16Gb de memória RAM DDR4, placa de vídeo integrada Intel Iris Xe Graphics, placa de video dedicada NVIDIA GeForce MX550, adaptador de rede modelo Intel(R) Wi-Fi 6 AX201 160MHz, unidade de disco SSD NVMe ADATA 512Gb, com o sistema operacional Windows 11 Home versão 23H2.

A máquina virtual foi criada com o software Oracle VM Virtualbox, versão 7.0.12. Dentro dela, foi executado o sistema operacional MX Linux versão 6.1.0-21-amd64, uma distro baseada em Debian. O ambiente virtual foi conectado à placa de rede do notebook por meio do modo Bridge. Mais especificações da máquina virtual estão explícitas na figura 1.

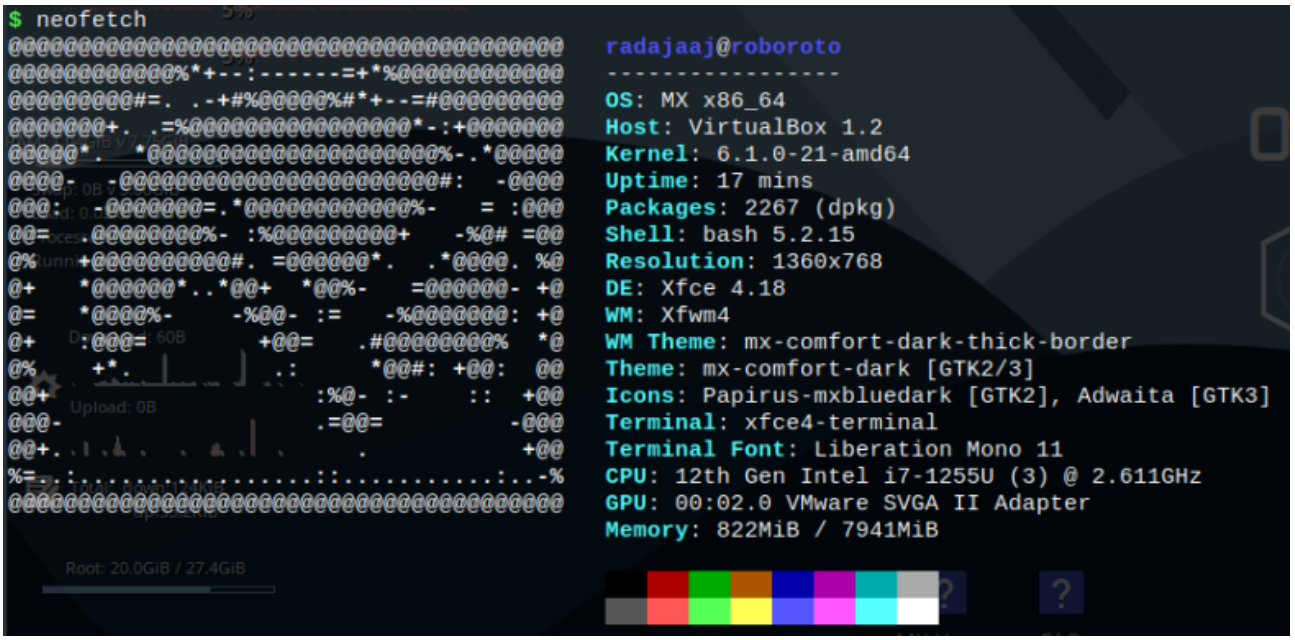

Figura 1: Ambiente virtual após a execução do comando *neofetch*.

No ambiente virtual Linux, foram instalados os pacotes wireshark e nslookup. Os testes foram feitos na UNIOESTE, durante a aula prática do dia 29/08/2024.

4. METODOLOGIA

4.1 Nslookup - Comandos Básicos:

Inicialmente, foram testados os comandos básicos da ferramenta nslookup. Para isso, foi digitado no terminal o comando "nslookup" seguido da URL de um servidor. Nesse caso, as URL escolhidas foram "www.unioeste.br" e "code.visualstudio.com". Depois, foram testados outros tipos de requisição DNS, com modificador -type=[código da requisição]. Foram executados os comandos: "nslookup -type=[x] www.unioeste.br", com x sendo: A, AAAA, mx, ns, CNAME, e PTR.

4.2 Nslookup + Sniffer de Rede:

Depois dos primeiros testes, a ferramenta nslookup foi executada mais 4 vezes, junto com a captura de rede da ferramenta wireshark. Primeiro, iniciou-se a captura de rede dentro do wireshark, aberto com "sudo wireshark". Depois, em outro terminal, com a ferramenta nslookup, foram feitos: uma consulta padrão IPv4 e IPv6 (nslookup -type=A|AAAA www.google.com.br); uma consulta ao nome canônico (nslookup -type=cname www.google.com.br), uma consulta ao domínio de e-mail (nslookup -type=mx gmail.com); e uma consulta de DNS reverso (nslookup -type=ptr 8.8.8.8). Por fim, a captura dos pacotes de rede foi finalizada, e os resultados foram interpretados.

5. RESULTADOS E DISCUSSÃO

5.1 Nslookup - Comandos Básicos:

Os testes iniciais da ferramenta nslookup foram executados com sucesso. Nas figuras 1 e 2, podemos ver os resultados dos primeiros testes. Podemos ver que o servidor "code.visualstudio.com" mostrou muito mais informações que o servidor de "www.unioeste.br".

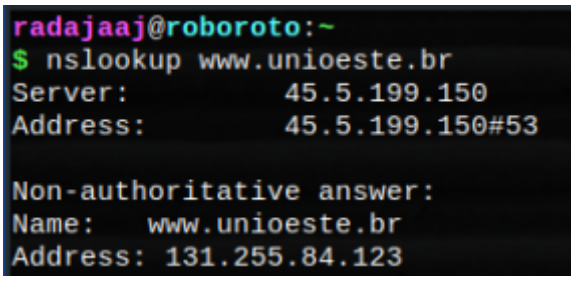

Figura 2: Resultados da execução do comando "nslookup www.unioeste.br".

Figura 3: Resultados da execução do comando "nslookup code.visualstudio.com".

A execução do comando "nslookup -type=A" obteve o mesmo resultado que a figura 1. Já a execução do mesmo comando com o tipo "AAAA" obteve um resultado um pouco diferente, com um erro: "Can't find www.unioeste.br" (Figura 4). O mesmo erro esteve presente na execução dos tipos "mx", mas com alguns erros a mais (Figura 5). A resposta da execução dos tipos "ns", "CNAME", e "PTR" foi idêntica à resposta apresentada na figura 5.

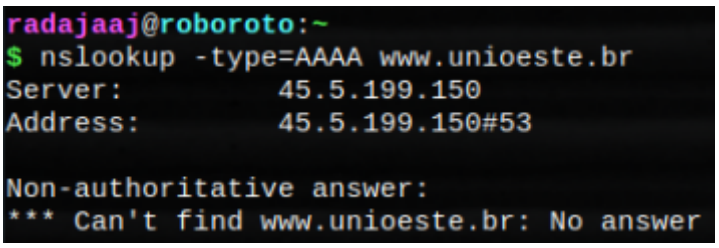

Figura 4: Resultados da execução do comando "nslookup -type =A www.unioeste.br".

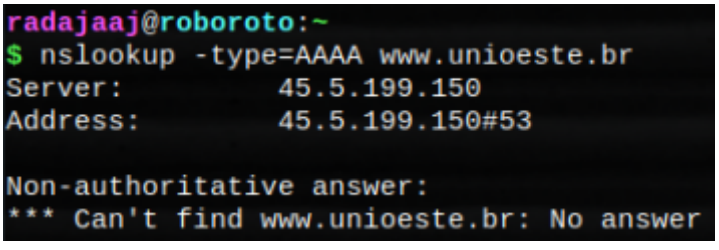

Figura 5: Resultados da execução do comando "nslookup -type =mx www.unioeste.br".

5.2 Nslookup + Sniffer de Rede:

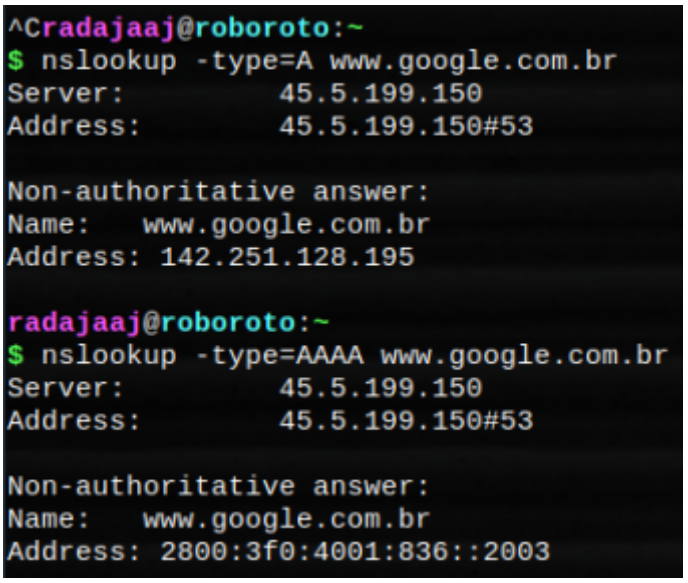

Figura 6: Resultados da execução do comando “nslookup -type =A|AAAA www.google.com.br”.

Os resultados das duas primeiras execuções da ferramenta nslookup (tipo A e AAAA) podem ser visualizados na Figura 6. Podemos ver que, na primeira execução, foi retornado um endereço IPv4 de 32 bits, enquanto a segunda retornou um endereço IPv6 de 128 bits, em hexadecimal. As execuções com o tipo cname e mx resultaram no erro “Can’t find www.google.com.br : No answer”, e foram idênticas. Isso pode ser visualizado na Figura 7. Porém, mesmo assim foi possível obter o endereço de e-mail do servidor: “dns-admin.google.com”.

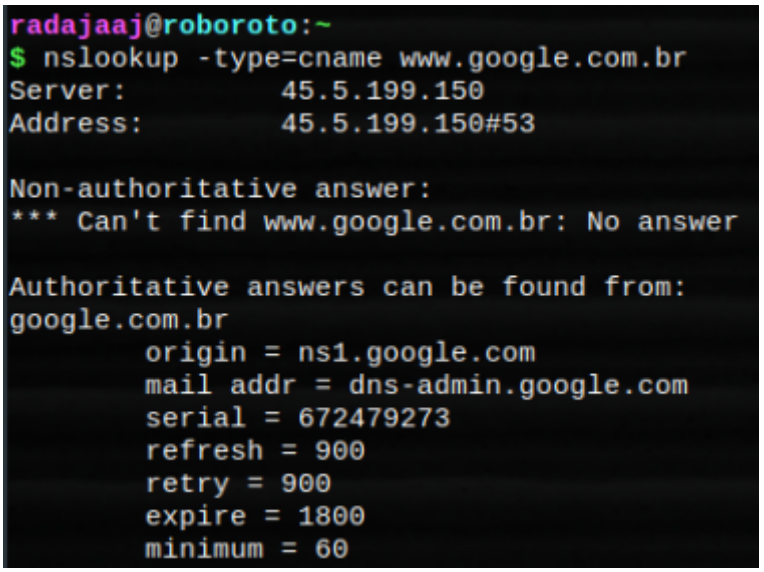

Figura 7: Resultados da execução do comando “nslookup -type =cname www.google.com.br”.

Por fim, a consulta de DNS reversa revelou que o endereço 8.8.8.8 está associado à URL “dns.google” (Figura 8).

```
radajaaj@roboroto:~
$ nslookup -type=ptr 8.8.8.8
Server:         45.5.199.150
Address:        45.5.199.150#53

Non-authoritative answer:
8.8.8.8.in-addr.arpa    name = dns.google.

Authoritative answers can be found from:
```

Figura 8: Resultados da execução do comando “nslookup -type =ptr 8.8.8.8”.

Por fim, a captura do wireshark foi interrompida. Ao aplicar o filtro “dns”, podemos ver na Figura 9 que é possível visualizar claramente o tipo de cada requisição DNS na coluna “info” (A, AAAA, CNAME, MX, e PTR). Também podemos ver que cada comutação de pacotes é simples: cada requisição (de qualquer tipo), é seguida imediatamente por uma resposta. Ao expandir um desses pacotes DNS, também podemos ver que a transação foi feita seguindo o protocolo UDP (User Datagram Protocol) (Figura 10).

Source	Destination	Protocol	Length	Info
10.0.2.15	45.5.199.150	DNS	77	Standard query 0x40ff A www.google.com.br
45.5.199.150	10.0.2.15	DNS	93	Standard query response 0x40ff A www.google.com.br A 142.251.128.195
10.0.2.15	45.5.199.150	DNS	77	Standard query 0xa10c AAAA www.google.com.br
45.5.199.150	10.0.2.15	DNS	105	Standard query response 0xa10c AAAA www.google.com.br AAAA 2800:3f0:4001:836::2003
10.0.2.15	45.5.199.150	DNS	77	Standard query 0xda1b CNAME www.google.com.br
45.5.199.150	10.0.2.15	DNS	137	Standard query response 0xda1b CNAME www.google.com.br SOA ns1.google.com
10.0.2.15	45.5.199.150	DNS	77	Standard query 0x79ec MX www.google.com.br
45.5.199.150	10.0.2.15	DNS	137	Standard query response 0x79ec MX www.google.com.br SOA ns1.google.com
10.0.2.15	45.5.199.150	DNS	80	Standard query 0xfa26 PTR 8.8.8.8.in-addr.arpa
45.5.199.150	10.0.2.15	DNS	104	Standard query response 0xfa26 PTR 8.8.8.8.in-addr.arpa PTR dns.google

Figura 9: Resultados da captura de pacotes de rede do wireshark.

```
▸ Frame 1: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_9c:47:92 (08:00:27:9c:47:92), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
▸ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 45.5.199.150
▸ User Datagram Protocol, Src Port: 51929, Dst Port: 53
▾ Domain Name System (query)
    Transaction ID: 0x40ff
  ▾ Flags: 0x0100 Standard query
      0... .... .... .... = Response: Message is a query
      .000 0... .... .... = Opcode: Standard query (0)
      .... ..0. .... .... = Truncated: Message is not truncated
      .... ...1 .... .... = Recursion desired: Do query recursively
      .... .... .0.. .... = Z: reserved (0)
      .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▸ Queries
    [Response In: 2]
```

Figura 10: Expansão da primeira requisição DNS feita (Standard query 0x40FF).

6. CONCLUSÕES

A aula prática teve como objetivo clarificar alguns dos conceitos básicos relacionados ao funcionamento do protocolo DNS, bem como ter uma melhor visão do conteúdo interno dos pacotes enviados e recebidos por uma máquina que segue esse protocolo. Nesse sentido, conclui-se que o trabalho foi um sucesso, pois foi possível completar todas as atividades propostas, bem como obter um conhecimento básico sobre o funcionamento da ferramenta nslookup.

A ferramenta nslookup permitiu uma boa visualização dos conteúdos de um pacote DNS, dos mais variados tipos. Esses conteúdos também foram bem visualizados com a ajuda do sniffer de rede wireshark. Infelizmente, não foi possível visualizar a comunicação entre as diferentes camadas hierárquicas do processo de tradução de uma URL por meio do protocolo DNS. Isso provavelmente ocorreu pois esse processo é intermediado por um servidor DNS local, que apenas recebe requisições e retorna a resposta final.

BIBLIOGRAFIA

GOYAL, Piyush; GOYAL, Anurag. Comparative study of two most popular packet sniffing tools-Tcpdump and Wireshark. In: **2017 9th International Conference on Computational Intelligence and Communication Networks (CICN)**. IEEE, 2017. p. 77-81.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet: Uma abordagem top-down**. Trad. 8 ed. São Paulo: Francisco Araújo da Costa, 2021.

LEINER, Barry M. et al. **A brief history of the Internet**. ACM SIGCOMM computer communication review, v. 39, n. 5, p. 22-31, 2009.

TANENBAUM, Andrew S. **Redes de Computadores**, 7ª Edição, Editora Campus, Rio de Janeiro – RJ, 2003.