

Serviço de Nomes (DNS)

Consulta simples ao DNS gerada a partir de um comando ping

1. Quem são os servidores DNS da sua máquina?

181.213.132.4

181.213.132.5

2804:14d:1:0:181:213:132:4 (IPv6)

2804:14d:1:0:181:213:132:5 (IPv6)

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ resolvectl status
Global
  Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  resolv.conf mode: stub

Link 2 (wlo1)
  Current Scopes: DNS
  Protocols: +DefaultRoute -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
  Current DNS Server: 181.213.132.5
  DNS Servers: 181.213.132.4 181.213.132.5 2804:14d:1:0:181:213:132:4 2804:14d:1:0:181:213:132:5
  DNS Domain: home

Link 3 (docker0)
  Current Scopes: none
  Protocols: -DefaultRoute -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported

Link 4 (br-c7577b95616b)
  Current Scopes: none
  Protocols: -DefaultRoute -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported

Link 5 (br-f15b30ebf387)
  Current Scopes: none
  Protocols: -DefaultRoute -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported
```

2. O ping gerou pergunta para cada um deles?

Não, o ping foi enviado diretamente ao IP **150.162.2.10**. O tráfego ICMP não interage diretamente com os servidores DNS, e sim resolve os nomes de domínio (caso necessário) antes de enviar os pacotes ICMP.

icmp dns						
Packet list						
Narrow & Wide						
Case sensitive						
Display filter						
No.	Time	Source	Destination	Protocol	Length	Info
6	2.814405084	192.168.0.4	181.213.132.4	DNS	82	Standard query 0x7e3d A www.ufsc.br OPT
7	2.814563329	192.168.0.4	181.213.132.4	DNS	82	Standard query 0xdd4 AAAA www.ufsc.br OPT
8	2.832927853	181.213.132.4	192.168.0.4	DNS	98	Standard query response 0x7e3d A www.ufsc.br A 150.162.2.10 OPT
9	2.838562828	181.213.132.4	192.168.0.4	DNS	110	Standard query response 0xdd4 AAAA www.ufsc.br AAAA 2801:84:0:2::10 OPT
10	2.839297779	192.168.0.4	150.162.2.10	ICMP	98	Echo (ping) request id=0x35be, seq=1/256, ttl=64 (reply in 11)
11	2.852102403	150.162.2.10	192.168.0.4	ICMP	98	Echo (ping) reply id=0x35be, seq=1/256, ttl=58 (request in 10)
12	2.852696886	192.168.0.4	181.213.132.4	DNS	96	Standard query 0xb997 PTR 10.2.162.150.in-addr.arpa OPT
13	2.864311676	181.213.132.4	192.168.0.4	DNS	125	Standard query response 0xb997 PTR 10.2.162.150.in-addr.arpa PTR paginas.ufsc.br OPT
14	3.840040892	192.168.0.4	150.162.2.10	ICMP	98	Echo (ping) request id=0x35be, seq=2/512, ttl=64 (reply in 15)
15	3.854891610	150.162.2.10	192.168.0.4	ICMP	98	Echo (ping) reply id=0x35be, seq=2/512, ttl=58 (request in 14)

3. Qual o tipo da RR associada a pergunta (*Queries*). O que significa?

Tipos A, AAAA e PTR.

A: Retorna o endereço IPv4 associado a um domínio.

AAAA: Retorna o endereço IPv6 associado a um domínio.

PTR: Faz o mapeamento reverso de um endereço IP para um nome de domínio.

4. Qual endereço IP retornado da solicitação da resolução de www.ufsc.br?

No pacote 9, a resposta à consulta AAAA retorna o endereço **2801:84:0:2::10** e no pacote 8, a resposta à consulta A é o endereço **150.162.2.10**.

8	2.832927853	181.213.132.4	192.168.0.4	DNS	98	Standard query response 0x7e3d A www.ufsc.br A 150.162.2.10 OPT
9	2.838562828	181.213.132.4	192.168.0.4	DNS	110	Standard query response 0xdd4 AAAA www.ufsc.br AAAA 2801:84:0:2::10 OPT

5. Qual endereço IP usado no ping (ver pacote REQUEST ICMP)?

O endereço IP de destino usado no ping é **150.162.2.10**.

6. Qual protocolo de transporte, camada 4, que foi usado para transportar as mensagens de aplicação DNS?

O protocolo de transporte utilizado foi o **UDP**.

No.	Time	Source	Destination	Protocol	Length	Info
6	2.814405084	192.168.0.4	181.213.132.4	DNS	82	Standard query
7	2.814563329	192.168.0.4	181.213.132.4	DNS	82	Standard query
8	2.832927853	181.213.132.4	192.168.0.4	DNS	98	Standard query
9	2.838562828	181.213.132.4	192.168.0.4	DNS	110	Standard query
10	2.839297779	192.168.0.4	150.162.2.10	ICMP	98	Echo (ping) request
11	2.852102403	150.162.2.10	192.168.0.4	ICMP	98	Echo (ping) response
12	2.852696886	192.168.0.4	181.213.132.4	DNS	96	Standard query
13	2.864311676	181.213.132.4	192.168.0.4	DNS	125	Standard query
14	3.840040892	192.168.0.4	150.162.2.10	ICMP	98	Echo (ping) request
15	3.854891610	150.162.2.10	192.168.0.4	ICMP	98	Echo (ping) response

Frame 6: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface wlo1, id 0

Ethernet II, Src: Intel_7d:3b:f1 (ec:63:d7:7d:3b:f1), Dst: SagemcomBroa_01:87:c5 (cc:58:00:01:87:c5)

Internet Protocol Version 4, Src: 192.168.0.4, Dst: 181.213.132.4

User Datagram Protocol, Src Port: 33647, Dst Port: 53

Source Port: 33647

Destination Port: 53

Length: 48

Checksum: 0xfac7 [unverified]

[Checksum Status: Unverified]

[Stream index: 0]

[Timestamps]

UDP payload (40 bytes)

Domain Name System (query)

7. No QUERY realizado foi solicitado consulta recursiva. O servidor aceitou esta solicitação? (ver a resposta do servidor)

Sim, pois houve uma resposta correspondente.

No.	Time	Source	Destination	Protocol	Length	Info
6	2.814405084	192.168.0.4	181.213.132.4	DNS	82	Standard query 0x7e3d A
7	2.814563329	192.168.0.4	181.213.132.4	DNS	82	Standard query 0xdd4 AA
8	2.832927853	181.213.132.4	192.168.0.4	DNS	98	Standard query response
9	2.838562828	181.213.132.4	192.168.0.4	DNS	110	Standard query response
10	2.839297779	192.168.0.4	150.162.2.10	ICMP	98	Echo (ping) request id=
11	2.852102403	150.162.2.10	192.168.0.4	ICMP	98	Echo (ping) reply id=
12	2.852696886	192.168.0.4	181.213.132.4	DNS	96	Standard query 0xb997 PTR
13	2.864311676	181.213.132.4	192.168.0.4	DNS	125	Standard query response
14	3.840040892	192.168.0.4	150.162.2.10	ICMP	98	Echo (ping) request id=
15	3.854891610	150.162.2.10	192.168.0.4	ICMP	98	Echo (ping) reply id=

▶ Frame 9: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface wlo1, ▶ Ethernet II, Src: SagemcomBroa_01:87:c5 (cc:58:30:01:87:c5), Dst: Intel_7d:3b:f1 (ec:63: ▶ Internet Protocol Version 4, Src: 181.213.132.4, Dst: 192.168.0.4 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 56946 ▶ Domain Name System (response) Transaction ID: 0xdd4 Flags: 0x8180 Standard query response, No error Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 1 Queries Answers ▶ www.ufsc.br: type AAAA, class IN, addr 2801:84:0:2::10 Additional records ▶ <Root>: type OPT	0000 ec 63 0010 00 60 0020 00 04 0030 00 01 0040 62 72 0050 10 00 0060 00 00
--	--

8. Qual o IP que se pretende resolver?

O IP que se pretende resolver é 10.2.162.150, conforme a consulta PTR vista no pacote 12.

10	2.839297779	192.168.0.4	150.162.2.10	ICMP	98	Echo (ping) request id=0x350e, seq=1/250, ttl=64 (reply in 11)
11	2.852102403	150.162.2.10	192.168.0.4	ICMP	98	Echo (ping) reply id=0x35be, seq=1/256, ttl=58 (request in 10)
12	2.852696886	192.168.0.4	181.213.132.4	DNS	96	Standard query 0xb997 PTR 10.2.162.150.in-addr.arpa OPT
13	2.864311676	181.213.132.4	192.168.0.4	DNS	125	Standard query response 0xb997 PTR 10.2.162.150.in-addr.arpa PTR pag

9. Qual o nome retornado?

“paginas.ufsc.br”, conforme a resposta do servidor DNS no pacote 13.

10	2.839297779	192.168.0.4	150.162.2.10	ICMP	98	Echo (ping) r
11	2.852102403	150.162.2.10	192.168.0.4	ICMP	98	Echo (ping) r
12	2.852696886	192.168.0.4	181.213.132.4	DNS	96	Standard quer
13	2.864311676	181.213.132.4	192.168.0.4	DNS	125	Standard quer
14	3.840040892	192.168.0.4	150.162.2.10	ICMP	98	Echo (ping) r
15	3.854891610	150.162.2.10	192.168.0.4	ICMP	98	Echo (ping) r

▶ Frame 13: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface wlo ▶ Ethernet II, Src: SagemcomBroa_01:87:c5 (cc:58:30:01:87:c5), Dst: Intel_7d:3b:f1 (ec:63: ▶ Internet Protocol Version 4, Src: 181.213.132.4, Dst: 192.168.0.4 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 37200 ▶ Domain Name System (response) Transaction ID: 0xb997 Flags: 0x8180 Standard query response, No error 1... .. = Response: Message is a response .000 0... .. = Opcode: Standard query (0)0... .. = Authoritative: Server is not an authority for domain0... .. = Truncated: Message is not truncated1... .. = Recursion desired: Do query recursively1... .. = Recursion available: Server can do recursive queries0... .. = Z: reserved (0)0... .. = Answer authenticated: Answer/authority portion was not authent0... .. = Non-authenticated data: Unacceptable0000 = Reply code: No error (0) Questions: 1 Answer RRs: 1 Authority RRs: 0 Additional RRs: 1 Queries ▶ 10.2.162.150.in-addr.arpa: type PTR, class IN Answers ▶ 10.2.162.150.in-addr.arpa: type PTR, class IN, paginas.ufsc.br Additional records [Request In: 12] [Time: 0.011614790 seconds]
--

10. O nome retornado é **www.ufsc.br**? Sim ou não? Explique.

Não Isso acontece porque a consulta PTR resolve o nome do domínio associado diretamente ao IP fornecido, e o IP 10.2.162.150 está associado ao subdomínio **paginas.ufsc.br**, que pode ser uma parte diferente da infraestrutura de servidores da UFSC.

Consultas DNS por meio de ferramentas especializadas

1. Usando o programa **host** ou **dig**, que são executados no terminal, descubra e anote no relatório os endereços IP associados aos seguintes nomes de hosts (máquinas):

- mail.ifsc.edu.br:
 - o Endereço IPv4 de hermes.ifsc.edu.br: 200.135.190.2
- www.google.com:
 - o Endereço IPv4: 142.250.218.196
 - o Endereço IPv6: 2800:3f0:4001:835::2004
- www.gmail.com:
 - o Endereço IPv4: 142.250.219.229
 - o Endereço IPv6: 2800:3f0:4001:809::2005

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ host mail.ifsc.edu.br
host www.google.com
host www.gmail.com
mail.ifsc.edu.br is an alias for hermes.ifsc.edu.br.
hermes.ifsc.edu.br has address 200.135.190.2
www.google.com has address 142.250.218.196
www.google.com has IPv6 address 2800:3f0:4001:835::2004
www.gmail.com has address 142.250.219.229
www.gmail.com has IPv6 address 2800:3f0:4001:809::2005
```

2. Agora descubra e anote no relatório quem é o servidor DNS responsável por cada um dos domínios (p.e.: ifsc.edu.br) dos nomes acima. Para isso consulte o valor do registro NS associado a esses domínios. Por exemplo, com o programa **host** ou **dig** isso pode ser feito assim: **host -t ns ifsc.edu.br**

- ifsc.edu.br
 - o ns2.ifsc.edu.br
 - o adns1.pop-sc.rnp.br
 - o ns1.ifsc.edu.br
 - o adns2.pop-sc.rnp.br
- google.com

- ns4.google.com
- ns3.google.com
- ns2.google.com
- ns1.google.com
- gmail.com
 - ns1.google.com
 - ns4.google.com
 - ns3.google.com
 - ns2.google.com

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ host -t ns ifsc.edu.br
host -t ns google.com
host -t ns gmail.com
ifsc.edu.br name server ns2.ifsc.edu.br.
ifsc.edu.br name server adns1.pop-sc.rnp.br.
ifsc.edu.br name server ns1.ifsc.edu.br.
ifsc.edu.br name server adns2.pop-sc.rnp.br.
google.com name server ns4.google.com.
google.com name server ns3.google.com.
google.com name server ns2.google.com.
google.com name server ns1.google.com.
gmail.com name server ns2.google.com.
gmail.com name server ns1.google.com.
gmail.com name server ns4.google.com.
gmail.com name server ns3.google.com.
lulu@lulu-ZenBook-UX435EA-UX435EA:~$
```

3. Descubra e anote no relatório quem é o servidor de emails nos seguintes domínios:

- gmail.com
- hotmail.com
- ifsc.edu.br

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ host -t mx gmail.com
gmail.com mail is handled by 40 alt4.gmail-smtp-in.l.google.com.
gmail.com mail is handled by 10 alt1.gmail-smtp-in.l.google.com.
gmail.com mail is handled by 20 alt2.gmail-smtp-in.l.google.com.
gmail.com mail is handled by 5 gmail-smtp-in.l.google.com.
gmail.com mail is handled by 30 alt3.gmail-smtp-in.l.google.com.
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ host -t mx hotmail.com
hotmail.com mail is handled by 2 hotmail-com.olc.protection.outlook.com.
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ host -t mx ifsc.edu.br
ifsc.edu.br mail is handled by 10 alt4.aspmx.l.google.com.
ifsc.edu.br mail is handled by 5 alt2.aspmx.l.google.com.
ifsc.edu.br mail is handled by 1 aspmx.l.google.com.
ifsc.edu.br mail is handled by 10 alt3.aspmx.l.google.com.
ifsc.edu.br mail is handled by 5 alt1.aspmx.l.google.com.
lulu@lulu-ZenBook-UX435EA-UX435EA:~$
```

3. Faça uma consulta iterativa com *dig* e responda:

3.1. Qual foi o RLD (*Root Level Domain*) consultado?

Representado pelos servidores root-servers.net.

3.2. Qual o TLD (*Top Level Domain*) consultado?

Foi .ru.

3.3. Qual o SLD (*Second Level Domain*) consultado?

Foi o mail.

3.4.. Como você sabe que foram esses os LDs consultados?

A partir das respostas mostradas no comando dig +trace, ele mostra cada etapa da consulta DNS.

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ dig +trace mail.ru.

; <<>> DiG 9.18.28-0ubuntu0.24.04.1-Ubuntu <<>> +trace mail.ru.
;; global options: +cmd
.                489227 IN      NS      a.root-servers.net.
.                489227 IN      NS      h.root-servers.net.
.                489227 IN      NS      i.root-servers.net.
.                489227 IN      NS      j.root-servers.net.
.                489227 IN      NS      l.root-servers.net.
.                489227 IN      NS      f.root-servers.net.
.                489227 IN      NS      k.root-servers.net.
.                489227 IN      NS      g.root-servers.net.
.                489227 IN      NS      c.root-servers.net.
.                489227 IN      NS      b.root-servers.net.
.                489227 IN      NS      m.root-servers.net.
.                489227 IN      NS      d.root-servers.net.
.                489227 IN      NS      e.root-servers.net.
;; Received 239 bytes from 127.0.0.53#53(127.0.0.53) in 59 ms

ru.              172800 IN      NS      a.dns.ripn.net.
ru.              172800 IN      NS      b.dns.ripn.net.
ru.              172800 IN      NS      d.dns.ripn.net.
ru.              172800 IN      NS      e.dns.ripn.net.
ru.              172800 IN      NS      f.dns.ripn.net.
ru.              86400 IN      DS      43786 8 2 3C59747544090BC74419D5F69E32D8C9E
ru.              86400 IN      RRSIG   DS 8 1 86400 20241020210000 20241007200000
C6KCF3koXmpPa8DktQ1NyupTLbhuIF2 rRQ37hCdNRFZUH5osh5SGqxWyb3mzpd7Wsb5Cfvh6evyNe0jU0aCcsbC uN
;; Received 683 bytes from 2801:1b8:10::b#53(b.root-servers.net) in 182 ms

MAIL.RU.         345600 IN      NS      ns2.mail.RU.
MAIL.RU.         345600 IN      NS      ns1.mail.RU.
J20C0QKDHUA3CUMNKST289FF06U2S091.ru. 3600 IN NSEC3 1 1 0 - J21LULR2UNPA28SERE28OVNJNI67QP7V
J20C0QKDHUA3CUMNKST289FF06U2S091.ru. 3600 IN RRSIG NSEC3 8 2 3600 20241110155306 2024093012
Evwr59QnOp3G/HeUJGnLAr/xNfHBggJJdoG3qJ QvA=
UI68RDB76N8TRSIHGPGCK981SK28G1U8.ru. 3600 IN NSEC3 1 1 0 - UI8S9USHP4V1P4E3SJCv9QALB7C04K2V
UI68RDB76N8TRSIHGPGCK981SK28G1U8.ru. 3600 IN RRSIG NSEC3 8 2 3600 20241109111608 2024093012
J13GkMiC8ba+9dZ5kGHYwHFWU36YfZmMO/Z74k Xvw=
;; Received 601 bytes from 2001:678:15:0:193:232:142:17#53(e.dns.ripn.net) in 242 ms

mail.ru.         60      IN      A       217.69.139.202
mail.ru.         60      IN      A       217.69.139.200
mail.ru.         60      IN      A       94.100.180.201
mail.ru.         60      IN      A       94.100.180.200
mail.ru.         600     IN      NS      ns1.mail.ru.
mail.ru.         600     IN      NS      ns2.mail.ru.
;; Received 224 bytes from 217.69.139.112#53(ns1.mail.RU) in 308 ms
```

Algumas Consultas AAAA

1. No terminal de sua máquina faça uma consulta e responda: qual o endereço IPv6 dos hosts? Por exemplo: `host -t AAAA google.com`
 1. `www.ufsc.br`
 2. `ipv6.br`

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ host -t AAAA www.ufsc.br
www.ufsc.br has IPv6 address 2801:84:0:2::10
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ host -t AAAA ipv6.br
ipv6.br has IPv6 address 2001:12ff:0:4::9
lulu@lulu-ZenBook-UX435EA-UX435EA:~$
```

2. Agora vamos fazer a consulta reversa. Qual é o nome de host dos seguintes endereços? Por exemplo: `host 2600:1419:1e00:38e::356e`
 1. `2801:84:0:2::10`
 2. `2001:12d0:0:126::183:244`

```
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ host 2801:84:0:2::10
0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.0.0.0.4.8.0.0.1.0.8.2.ip6.arpa domain name pointer www.ufsc.br.
lulu@lulu-ZenBook-UX435EA-UX435EA:~$ host 2001:12ff:0:4::9
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer seminarioprivacidade.cgi.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer icannsaopaulo.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer pttforum.nic.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer ipv6.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer igfbrazil2007.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer antispam.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer internetsegura.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer www.xn--icannsopaulo-7bb.br.
9.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.f.f.2.1.1.0.0.2.ip6.arpa domain name pointer cetic.br.
lulu@lulu-ZenBook-UX435EA-UX435EA:~$
```