

[◀ VOLTAR](#)

Sistema de Nomes: DNS

Descrição do protocolo DNS e seu funcionamento

NESTE TÓPICO



Marcar
tópico



Os serviços de DNS (*Domain Name System*) - Sistema de Nomes de Domínios) da internet são, em poucas palavras, grandes bancos de dados espalhados em servidores localizados em várias partes mundo

O DNS é um protocolo que implementa um serviço da camada de aplicação, que utiliza a porta 53, no destino, encapsulado no protocolo UDP, responsável por identificar uma estação de trabalho na internet por um nome ou por um endereço IP.

Para conciliar este serviço, é necessário um serviço de diretório que traduza nomes para endereços IP, sendo que esta é a tarefa principal do DNS da Internet. Pode-se dizer que o DNS é um banco de dados distribuído executado em uma hierarquia de servidores de DNS, é um protocolo de camada de aplicação que permite que as estações de trabalho na rede consultem este banco de dados distribuído.

O DNS provê alguns outros serviços importantes além da tradução de nomes de estações de trabalho na rede para endereços IP:

- Apelidos (*aliasing*) das estações de trabalho na rede;
- Apelidos de servidor de correio;
- Distribuição de carga.

Nenhum servidor DNS isolado tem todos os mapeamentos para todos os hospedeiros da Internet. Em vez disso, os mapeamentos são distribuídos pelos servidores DNS.

Os servidores de DNS formam uma rede com uma estrutura hierárquica onde os registros e nomes estão alocados de forma distribuída de modo que não é necessário que todos os endereços do mundo estejam alocados em um único servidor.

Esta hierarquia tem uma estrutura em forma de árvore onde são locados diversos servidores do tipo raiz e servidores do tipo TLD, como ser fossem, servidores de segundo nível como um .com, .edu ou de organizações conforme figura 1.

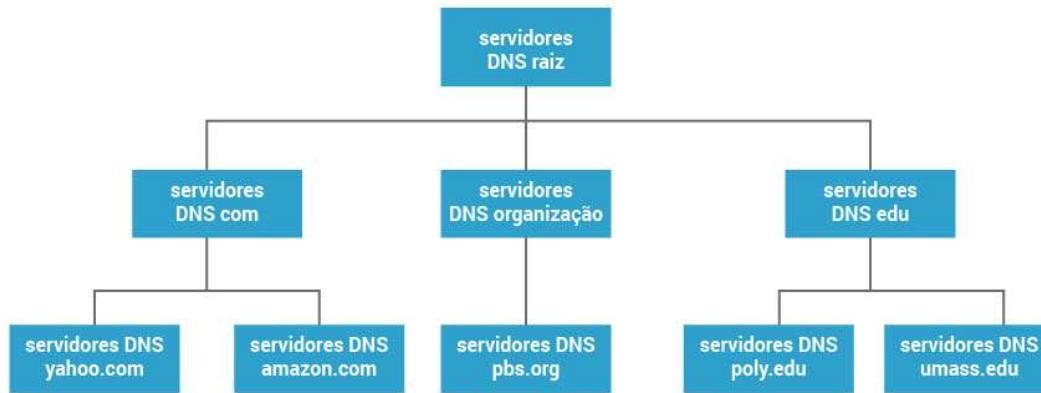


Figura 1 - Estrutura em árvore do serviço de DNS

Fonte: TANENBAUM, Andrew S. Redes de computadores . 2011

Em 2012, os servidores do tipo raiz estavam assim distribuídos pelo mundo.

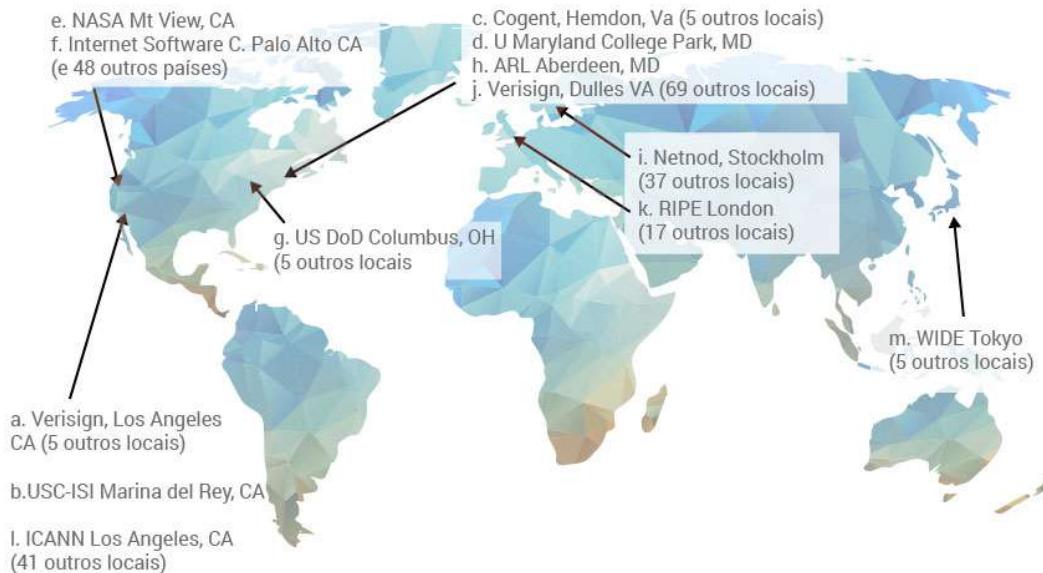


Figura 2 - Distribuição de servidores raiz DNS pelo mundo

Fonte: TANENBAUM, Andrew S. Redes de computadores . 2011

Apresentando uma estrutura de árvore um pouco mais completa, pode-se observar a figura 3 onde se dividem como genérico ou relativo aos países como é o caso do .br (Brasil), .us (Estados Unidos), .uk (reino unido), entre outros, ou seja, cada país criou sua estrutura em árvore e é responsável pela sua distribuição.

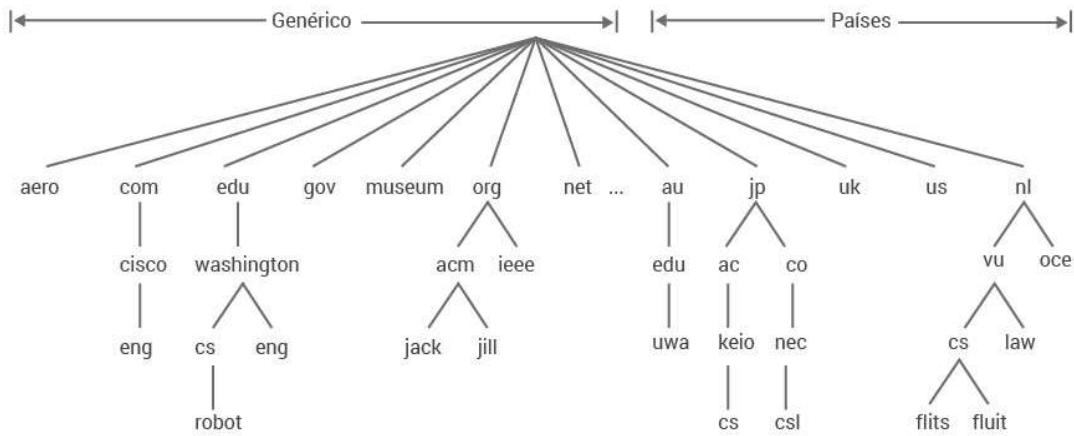


Figura 3 - Estrutura da árvore de DNS com nomes genéricos e atrelado a países

Fonte: TANENBAUM, Andrew S. Redes de computadores . 2011

A tabela 1 apresenta alguns domínios (extensões) que já são bastante comuns na estrutura do DNS

Domínio	Uso intencionado	Data de início	Restrito?
com	comercial	1985	não
edu	instituições educacionais	1985	sim
gov	governo	1985	sim
int	organizações internacionais	1988	sim
mil	militares	1985	sim
net	provedores de rede	1985	não
org	organizações não lucrativas	1985	não
aero	transporte aéreo	2001	sim
biz	empresas	2001	não
coop	cooperativas	2001	sim
info	informativos	2002	não

museum	museus	2002	sim
name	pessoas	2002	sim
pro	profissionais	2002	sim
cat	catalão	2005	sim
jobs	empregos	2005	sim
mobi	dispositivos móveis	2005	sim
tel	detalhes de contato	2005	sim
travel	indústria de viagens	2005	sim
xxx	indústria do sexo	2010	não

O protocolo DNS funciona em uma arquitetura tipo cliente-servidor onde a estação de trabalho cliente, solicita uma resolução de endereço (nome para IP ou IP para nome) para um servidor de DNS por meio de um tipo de solicitação, conforme tabela 2, sendo os mais comuns o do tipo A ou NS, ou seja, a tradução de endereço IPv4 de um host e o tipo servidor de nome

Tipo	Significado	Valor
SOA	início da autoridade	parâmetros para essa zona
A	endereço de IPv4 de um host	inteiro de 32 bits
AAAA	endereço de IPv6 de um host	inteiro de 128 bits
MX	troca de mensagens de correio	prioridade, domínio disposto a aceitar correio eletrônico
NS	servidor de nomes	nome de um servidor de domínio
CNAME	nome canônico	nome de domínio
PTR	ponteiro	nome alternativo de um endereço IP
SPF	estrutura de política do transmissor	codificação de texto da política de envio de mensagens ao correio
SRV	serviço	host que o oferece
TXT	texto	texto ASCII descritivo

- **Registros A:** basicamente, associam um ou mais endereços IP a um ou mais domínios. Pode-se utilizar AAAA para endereços IPv6;
- **Registros CNAME (Canonical Name):** servem para criar redirecionamentos para domínios ou subdomínios. É este parâmetro que deve ser utilizado, por exemplo, para criar um endereço do tipo *blog.seusite.com.br*;
- **Registros MX (Mail Exchanger):** são os parâmetros que devem ser configurados para contas de e-mail no domínio (*@seusite.com.br*);
- **Registros NS (Name Server):** indicam quais servidores atuam como serviço de DNS do site. São os endereços mencionados no tópico sobre registros de domínios;
- **Registros PTR (Pointer):** informam quais domínios estão associados a determinados IPs, quase se fosse o reverso dos registros A;
- **Registros SRV** (abreviação de *Service*): indicam a localização de determinados serviços dentro do domínio;
- **Registros SOA (Start of Authority):** indicam o início de uma zona, isto é, de um conjunto de registros localizado dentro de um espaço de nomes de DNS. Cada zona deve ter um registro SOA;
- **Registros TXT** (abreviação de *Text*): servem para a inserção de comentários ou orientações.

Servidores de nome raiz

Na internet existem 13 servidores raiz que na verdade são um conglomerado de servidores replicados para fins de segurança e confiabilidade.

Servidores de nome de Domínio de Alto Nível (TLD)

Esses são responsáveis por domínio de alto nível como com, edu, net e gov e também por domínio de países com br, fr, ru.

Servidores de nomes com autoridade

São servidores gerenciados por universidades e grandes empresas que por opção pode preferir montar seu próprio servidor DNS para abrigar seus registros e utilizar registros de algum servidor de autoridade de algum servidor de serviço.

Servidor de Nome Local

O servidor de nome local não pertence a hierarquia de servidores DNS mas é central para o seu funcionamento. Cada ISP (Provedor de Internet) como universidades e grandes empresas possui um ou mais servidores DNS locais, quando uma estação de trabalho se conecta a um ISP este fornece um ou mais IPs de servidores DNS locais normalmente por DHCP).

Consultas ao servidor DNS de forma interativa

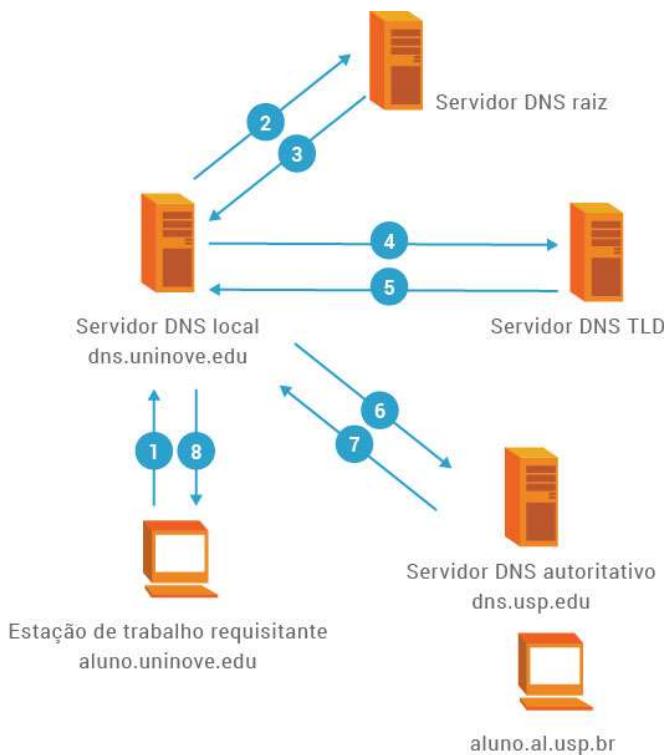


Figura 5 - Solicitação de mensagem interativa

Fonte: Kurose, James F - Redes de computadores, 2013

1 - A estação de trabalho solicita uma pesquisa ao DNS local sobre o endereço IP de um determinado nome;

2 - Caso o nome não faça parte do cache do servidor local, este repassa a pergunta a um servidor do tipo raiz;

3 - Como se trata de uma pesquisa hierárquica, o servidor raiz irá indicar o próximo servidor ou servidor TLD (Top Level Domain)

4 - O servidor TLD recebe a requisição

5 - O servidor TLD indicará o caminho para chegar ao destino

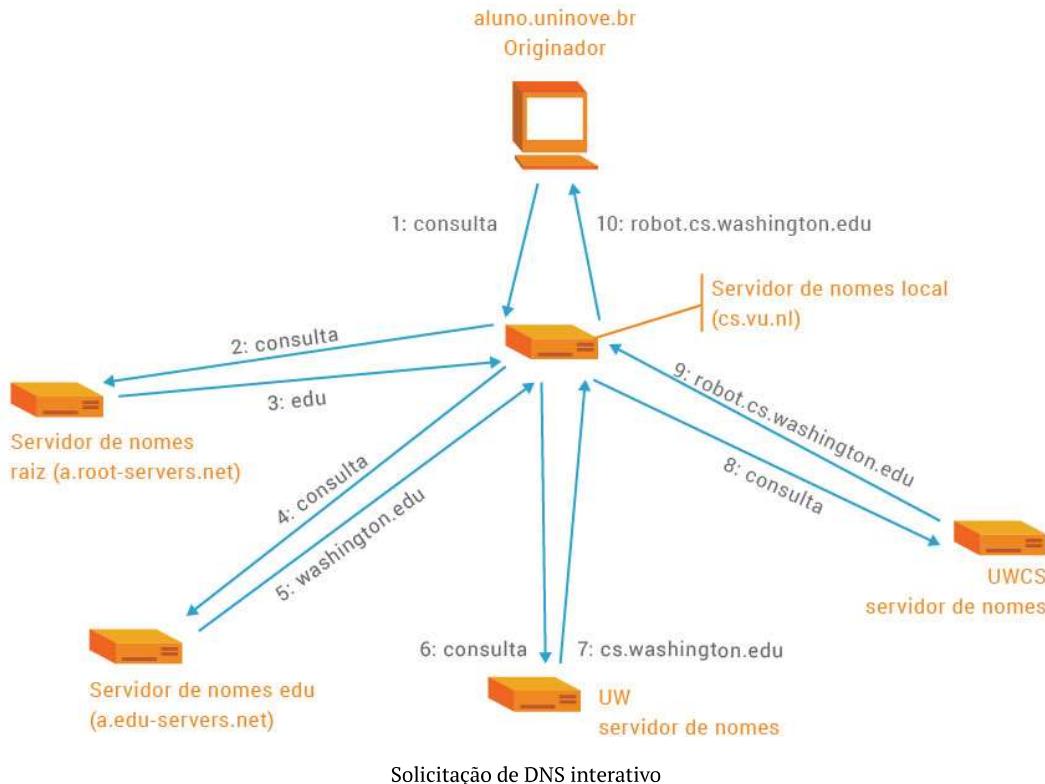
6 - O encaminhamento, agora, é apontado para o servidor de DNS autoritativo

7 - O DNS autoritativo devolve a resposta para o DNS local

8 - O DNS local devolve a resposta a estação de trabalho requisitante

Exemplo 2 - consulta interativo

A estação de trabalho originador aluno.uninove.br solicita uma consulta para robot.cs.washington.edu:



Fonte: Kurose, James F - Redes de computadores, 2013

Consulta o DNS local – **cs.vu.nl** o endereço para **robot.cs.washington.edu** e não encontra o nome no cache local;

2- A consulta é repassada para o servidor de raiz.

3 - O servidor raiz, não conhece o caminho final mas conhece o **.edu** e indica onde encontra-se o servidor **.edu** (estrutura hierárquica)

4 – O servidor local novamente faz interação solicitando o endereço ao servidor de nomes **.edu** que agora já é conhecido

5- O servidor **.edu** não sabe o caminho final mas conhece o caminho para o servidor **washington.edu**

6 – O servidor local novamente faz interação solicitando o endereço ao servidor de nomes **washington.edu** que agora já é conhecido.

7 - O servidor **.washington.edu** não sabe o caminho final mas conhece o caminho para o servidor **cs.washington.edu**

8 - O servidor local novamente faz interação solicitando o endereço **robot.cs.washington.edu** ao servidor de nomes **.cs.washington.edu** que agora já é conhecido

9 - O servidor **.cs.washington.edu** conhece e devolve o caminho para o servidor **robot.cs. washington.edu**

1. – O servidor local **cs.vu.nl** devolve a resposta para o originador.

O DNS explora extensivamente o cache para melhorar o desempenho quanto ao atraso e reduzir o número de mensagens DNS que dispara pela Internet.

Consultas recursivas em DNS

Uma outra forma de consultar o servidor de DNS é de forma recursiva, ou seja, o servidor DNS local faz uma única interação e fica aguardando do servidor vizinho a resposta a solicitação e assim por diante, conforme figura 6.

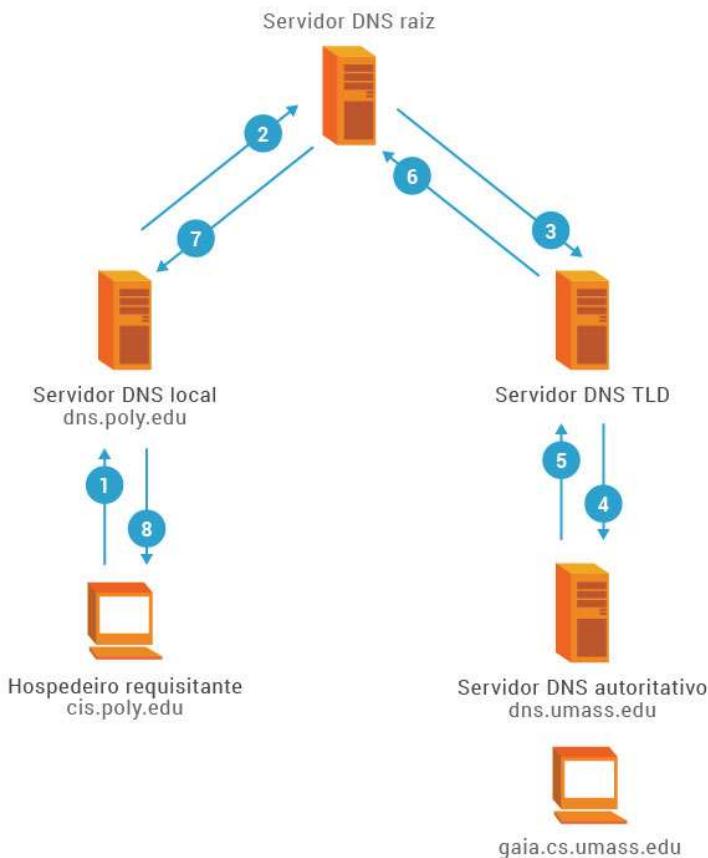


Figura 6 - Consulta recursiva

Fonte: Kurose, James F - Redes de computadores, 2013

Os Registros e mensagens DNS

Um registro de recurso é uma tupla de quatro elementos que contém os seguintes campos:

(Name, Value, Type, TTL)

Formato da mensagem DNS



Figura 7 - Formato do protocolo DNS

Fonte: Kurose, James F & Redes de computadores, 2014

A estrutura detalhada do cabeçalho da mensagem DNS é mostrada na ilustração a seguir:

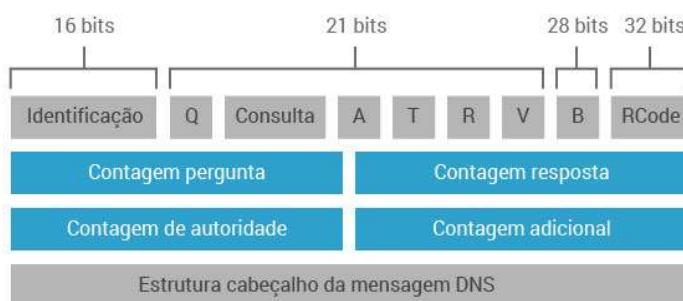


Figura 8 - Detalhamento do protocolo DNS

Fonte: o autor

- ID campo de 16 bits usado para correlacionar as consultas e respostas.
- Q campo de 1 bit que identifica a mensagem como uma consulta ou resposta.
- Consulta campo de 4 bits que descreve o tipo de mensagem:
 - 0 - Consulta padrão (nome para endereço);
 - 1 - Consulta inversa (endereço para nome);
 - 2 - Solicitação de status do servidor.
- A resposta autoritária. Campo de 1 bit. Quando definido para 1, identifica a resposta como uma feita por um servidor de nomes com autoridade.

- T truncamento. Campo de 1 bit. Quando definido para 1, indica que a mensagem foi truncada.
- R campo de 1 bit. Situado a 1 pela decisão de solicitar o serviço recursiva pelo servidor de nome.
- V campo de 1 bit. Sinaliza a disponibilidade do serviço recursiva pelo servidor de nome.
- B campo de 3 bits. Reservado para uso futuro. Deve ser definido como 0.
- RCODE Response Code. Campo de 4 bits que é definida pelo servidor de nome para identificar o estado da consulta:

- 0 Nenhuma condição de erro.
- 1 Não é possível interpretar consulta devido a um erro de formato.
- 2 Não é possível processar devido a falha do servidor.
- 3 Nome na consulta não existe.
- 4 Tipo de consulta não é suportado.
- 5 Pesquisa recusada.

- Contagem pergunta - campo de 16 bits que define o número de entradas na seção de perguntas.
- Contagem de resposta - campo de 16 bits que define o número de registros de recursos na seção resposta.
- Contagem de Autoridade - campo de 16 bits que define o número de registros de recursos do servidor de nomes na seção autoridade.
- Contagem adicional - campo de 16 bits que define o número de registros de recursos na seção de registros adicionais.

Para ilustrar os campos acima foram capturados com o software wireshark uma pergunta ao servidor DNS perguntando o IP do site www.citibank.com (<http://www.citibank.com/>) com identificador 8671, tipo A.

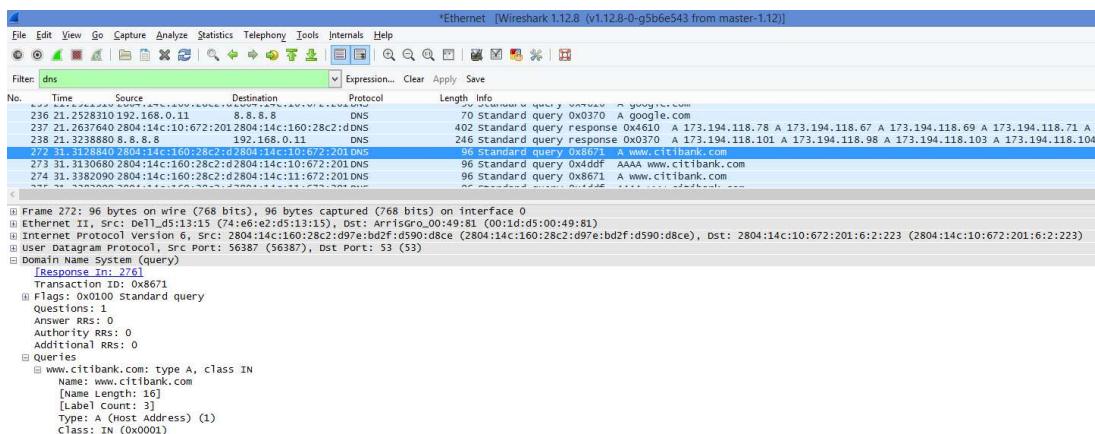


Figura 9 - Solicitação de Query

Fonte: o autor

Resposta do servidor de DNS, como forma de exercitar, verifique os campos do protocolo com wireshark e os campos do detalhe do protocolo na figura 8. O tipo AAAA retorna endereços IPv6, conforme figura 10

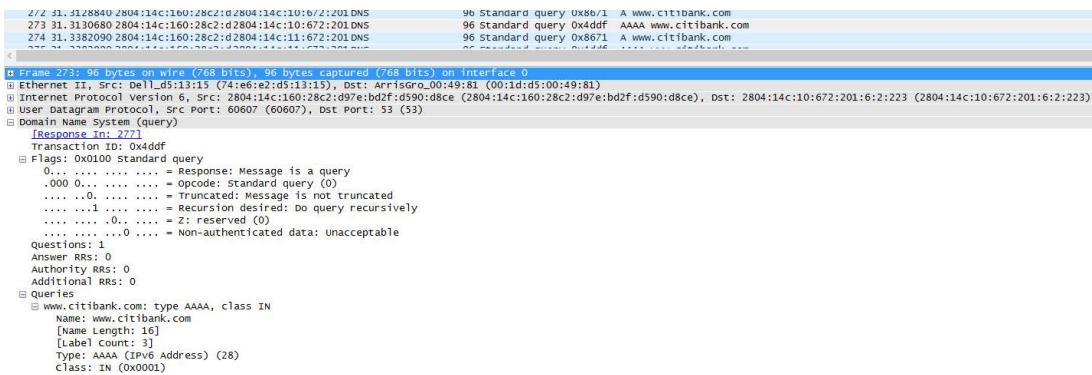


Figura 10 - Resposta de um servidor DNS

Fonte: o autor

As figuras 11 a 15 mostram partes da captura com as querys das respostas e respostas adicionais das solicitações ao servidor DNS.

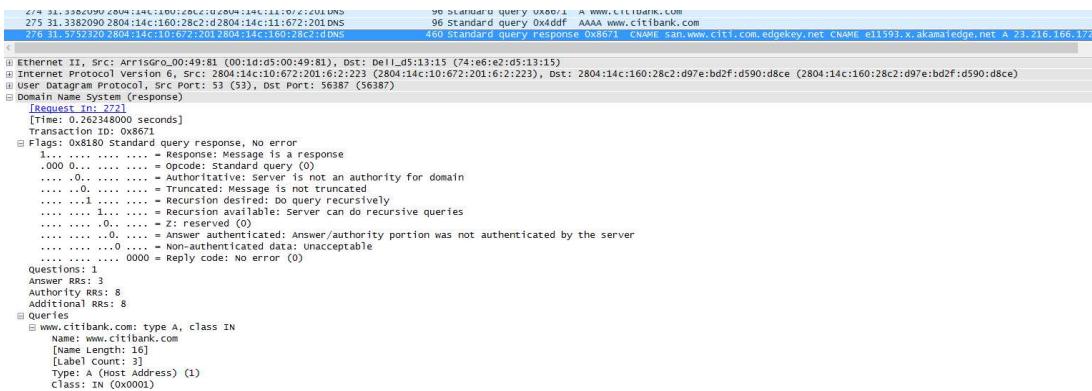


Figura 11 - Resposta com número de autoridades e flags

Fonte: o autor

Resposta com número de autoridades e flags

Figura 12 - Resposta com número de autoridades e flags

Fonte: o autor

```

Questions: 1
Answer RRs: 2
Authority RRs: 1
Additional RRs: 0
Queries
  www.citibank.com: type AAAA, class IN
    Name: www.citibank.com
    [Name Length: 16]
    [Label Count: 3]
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
Answers
  www.citibank.com: type CNAME, class IN, cname san.www.citi.com.edgekey.net
    Name: www.citibank.com
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 300
    Data length: 30
    CNAME: san.www.citi.com.edgekey.net
  san.www.citi.com.edgekey.net: type CNAME, class IN, cname e11593.x.akamaiedge.net
    Name: san.www.citi.com.edgekey.net
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 3600
    Data length: 22
    CNAME: e11593.x.akamaiedge.net
Authoritative nameservers
  x.akamaiedge.net: type SOA, class IN, mname n0x.akamaiedge.net

```

Figura 13 - Resposta com número de autoridades e flags

Fonte: o autor

```

Questions: 1
Answer RRs: 2
Authority RRs: 1
Additional RRs: 0
Queries
  www.citibank.com: type AAAA, class IN
    Name: www.citibank.com
    [Name Length: 16]
    [Label Count: 3]
    Type: AAAA (IPv6 Address) (28)
    Class: IN (0x0001)
Answers
  www.citibank.com: type CNAME, class IN, cname san.www.citi.com.edgekey.net
  san.www.citi.com.edgekey.net: type CNAME, class IN, cname e11593.x.akamaiedge.net
Authoritative nameservers
  x.akamaiedge.net: type SOA, class IN, mname n0x.akamaiedge.net
    Name: x.akamaiedge.net
    Type: SOA (start of a zone of Authority) (6)
    Class: IN (0x0001)
    Time to live: 1000
    Data length: 46
    Primary name server: n0x.akamaiedge.net
    Responsible authority's mailbox: hostmaster.akamai.com
    Serial Number: 1446837859
    Refresh Interval: 1000 (16 minutes, 40 seconds)
    Retry Interval: 1000 (16 minutes, 40 seconds)
    Expire limit: 1000 (16 minutes, 40 seconds)
    Minimum TTL: 1800 (30 minutes)

```

Figura 14 - Resposta com número de autoridades e flags

Fonte: o autor

```

Answers
www.citibank.com: type CNAME, class IN, cname san.www.citi.com.edgekey.net
  Name: www.citibank.com
  Type: CNAME (Canonical NAME for an alias) (5)
  Class: IN (0x0001)
  Time to live: 300
  Data length: 30
  CNAME: san.www.citi.com.edgekey.net
san.www.citi.com.edgekey.net: type CNAME, class IN, cname e11593.x.akamaiedge.net
  Name: san.www.citi.com.edgekey.net
  Type: CNAME (Canonical NAME for an alias) (5)
  Class: IN (0x0001)
  Time to live: 3600
  Data length: 22
  CNAME: e11593.x.akamaiedge.net
e11593.x.akamaiedge.net: type A, class IN, addr 23.216.166.172
  Name: e11593.x.akamaiedge.net
  Type: A (Host Address) (1)
  Class: IN (0x0001)
  Time to live: 20
  Data length: 4
  Address: 23.216.166.172 (23.216.166.172)

Authoritative nameservers
x.akamaiedge.net: type NS, class IN, ns n4x.akamaiedge.net
  Name: x.akamaiedge.net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 1337
  Data length: 6
  Name Server: n4x.akamaiedge.net
x.akamaiedge.net: type NS, class IN, ns n3x.akamaiedge.net
  Name: x.akamaiedge.net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 1337
  Data length: 6
  Name Server: n3x.akamaiedge.net
x.akamaiedge.net: type NS, class IN, ns n0x.akamaiedge.net
  Name: x.akamaiedge.net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 1337
  Data Length: 6
  Name Server: n0x.akamaiedge.net
x.akamaiedge.net: type NS, class IN, ns n2x.akamaiedge.net
  Name: x.akamaiedge.net
  Type: NS (authoritative Name Server) (2)
  Class: IN (0x0001)
  Time to live: 1337
  Data length: 6
  Name Server: n2x.akamaiedge.net

```

Figura 15 - Resposta com número de autoridades e flags

Fonte: o autor

```

292 31.9108940 2804:14c:160:28c2:d2804:14c:10:672:201 DNS      99 Standard query 0xa001 AAAA online.citibank.com
Frame 292: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface 0
Ethernet II, Src: dell_d5:13:15 (74:e6:e2:d5:13:15), Dst: Arrisdro.00:49:81 (00:1d:00:00:49:81)
Internet Protocol Version 6, Src: 2804:14c:160:28c2:d97e:bd2f:bd590:d8ce (2804:14c:160:28c2:d97e:bd2f:bd590:d8ce), Dst: 2804:14c:10:672:201:6:2:223 (2804:14c:10:672:201:6:2:223)
User Datagram Protocol, Src Port: 53869 (53869), Dst Port: 53 (53)
Domain Name System (query)
  Response ID: 2961
  Transaction ID: 0xa001
  Flags: 0x0100 Standard query
    0... .... .... = Response: Message is a query (0)
    .000 0.... .... = Opcode: Standard query (0)
    .... 0.... .... = Truncated: Message is not truncated
    .... 1.... .... = Recursion desired: Do query recursively
    .... 0.... .... = Z: reserved (0)
    .... 0.... 0.... = Non-authenticated data: unacceptable
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    online.citibank.com: type AAAA, class IN
      Name: online.citibank.com
      [Name Length: 19]
      [Label Count: 3]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)

```

Figura 16 - Solicitação de endereço IPv6

Fonte: o autor

Segurança no DNS - O DNSSEC

No contexto explanado pode-se verificar que os servidores de DNS têm papel importante na internet, uma vez que, sem o mesmo, fica quase impossível navegar na internet, ao menos que você conheça o endereço IP da página

que se pretende consultar. Outro problema é que o DNS também pode ser vítima de ações maliciosas.

Vamos imaginar que um indivíduo com grande conhecimento no assunto elaborou um esquema para conseguir capturar solicitações de resolução de nomes de clientes de um determinado provedor. Ao ter sucesso com isso, ele pode tentar direcionar um endereço falso no lugar de um site que um usuário queira visitar. Por exemplo, vamos supor um site de um grande banco tipo www.bradesco.com.br (<http://www.bradesco.com.br/>) que pode ser direcionado, via DNS para uma página falsa. Perceba o risco: se o usuário não perceber que foi direcionado para uma página falsa, poderá fornecer dados sigilosos, como número de cartão de crédito, senhas, etc.

Para evitar problemas como estes é que foi criado o **DNSSEC** (*DNS Security Extensions*), que consiste em uma especificação que adiciona recursos de segurança ao DNS.

O DNSSEC considera, essencialmente, os aspectos de autenticidade e integridade dos procedimentos envolvendo DNS. Basicamente, o DNSSEC utiliza um esquema que envolve chaves públicas e privadas, bem como assinaturas digitais. Com isso, é possível ter certeza de que os servidores corretos estão respondendo às pesquisas de DNS.

A implementação do DNSSEC deve ser feita pelas entidades responsáveis pela administração dos domínios, motivo pelo qual este recurso ainda não é utilizado de maneira plena. Felizmente, em relação ao Brasil, o país foi um dos primeiros a lidar com isso ao implementar o DNS em endereços .br.

Serviços gratuitos de DNS: OpenDNS e Google Public DNS

Quando se contrata um serviço de acesso à internet, por padrão, passa a utilizar os servidores de DNS da operadora. O problema é que, muitas vezes, estes servidores podem não funcionar corretamente ou pode estar fora do ar. A conexão é estabelecida, mas o navegador não consegue encontrar nenhuma página; o acesso a sites pode estar lento porque os serviços de DNS demoram para responder.

Uma solução para problemas como estes consiste em adotar serviços de DNS alternativos e especializados, que são otimizados para oferecer o melhor desempenho possível e são menos suscetíveis a falhas. Os mais conhecidos são o [OpenDNS](http://www.opendns.com/) (<http://www.opendns.com/>) e, mais recentemente, o [Google Public DNS](http://code.google.com/speed/public-dns/) (<http://code.google.com/speed/public-dns/>). Ambos os serviços são gratuitos e, quase sempre, funcionam de maneira bastante satisfatória.

OpenDNS

Utilizar o OpenDNS é muito simples: basta utilizar os dois IPs do serviço. São eles:

- **Primário:** 208.67.222.222
- **Secundário:** 208.67.220.220

O serviço secundário é uma réplica do primário; se este não puder ser acessado por algum motivo, o segundo é a alternativa imediata.

Registro de domínios

Para se ter um site próprio, do tipo *seunome.com.br ou seunome.net*, é necessário registrar o domínio. Se o domínio terminar com .br, o procedimento pode ser feito no site [Registro.br \(http://registro.br/\)](http://registro.br/). Como exercício, acesse o site e vejam as etapas para registro. Para domínios internacionais (.com, .net, .org, entre outros) há várias empresas que oferecem este serviço, sendo a [GoDaddy \(http://www.godaddy.com/\)](http://www.godaddy.com/).

O primeiro passo consiste em verificar se o domínio está disponível, isto é, se já não foi registrado por outra pessoa ou por uma empresa. Todos os serviços de registro fornecem um campo onde é possível fazer esta verificação.

Se o domínio estiver livre, pode-se efetuar o cadastro no serviço e pagar uma taxa, que varia conforme a empresa e o tipo de domínio. No entanto, vale observar que o registro somente vale para a terminação escolhida. Se você registrar um domínio *meunome.com*, por exemplo, precisará realizar outro registro para *meunome.net*.

Além do registro do domínio, é preciso também escolher uma empresa para hospedá-lo. Há várias companhias que prestam este tipo de serviço. Pode-se pesquisar por "hospedagem de sites" no Google para tentar encontrar o melhor serviço de hospedagem.

Quando se escolher o serviço de hospedagem, deverá associar a sua conta ao domínio registrado. É fácil fazer isso: o serviço de hospedagem irá fornecer pelo menos dois endereços de DNS (*name servers*) que deve-se informar no painel oferecido pela empresa onde foi feito o registro do domínio. Estes endereços geralmente tem o seguinte formato:

- ns1.empresadehospedagem.com.br
- ns2.empresadehospedagem.com.br
- ns3.empresadehospedagem.com.br

Ao realizar este procedimento, a entidade responsável por gerenciar o seu domínio saberá informar quais serviços de DNS respondem pelo servidor que hospeda o seu site, fazendo com que este consiga ser encontrado.

Quando se registra um domínio e contrata um serviço de hospedagem, este pode oferecer subdomínios baseados em seu endereço para que seja possível acessar serviços de e-mail, servidor de FTP, entre outros.

Quiz

Exercício Final

Sistema de Nomes: DNS

INICIAR ➔

Referências

Tannenbaum, Andrew S. Redes de Computadores - 5ed - 2011

Kurose, James F - Redes de Computadores e a Internet - 2014



Avalie este tópico



ANTERIOR

Aplicações e a Topologia de Redes

Biblioteca

☰
Índice

(<https://www.uninove.br/conheca-a-uninove/biblioteca/sobre-a-biblioteca/apresentacao/>)
Portal Uninove
(<http://www.uninove.br>)
Mapa do Site

Ajuda?

PRÓXIMO
(<https://ava.uninove.br/seu/AV/A/topico/topico.php>) ➔

© Todos os direitos reservados

