

Redes de Computadores

Camada de Aplicação

DNS

DNS – Como Funciona

- Os motivos do DNS não ser centralizado:
 - **Um único ponto**, se o mesmo falhar a internet para;
 - **Volume de tráfego**, um servidor para atender milhares de requisições;
 - **Banco de Dados distante**, um BD centralizado beneficiaria os *hosts* que estão próximos, mas prejudicaria os distantes;
 - **Manutenção**, problemas para atualizar e manter funcionando o enorme BD;
 - **Escalonamento**, um único servidor não é escalável.

DNS – Como Funciona

- O DNS é distribuído por conceito de projeto;
- Usa um grande número de servidores, organizados de maneira hierárquica e distribuídos por todo mundo;
- As informações estão distribuídas por todos os servidores;

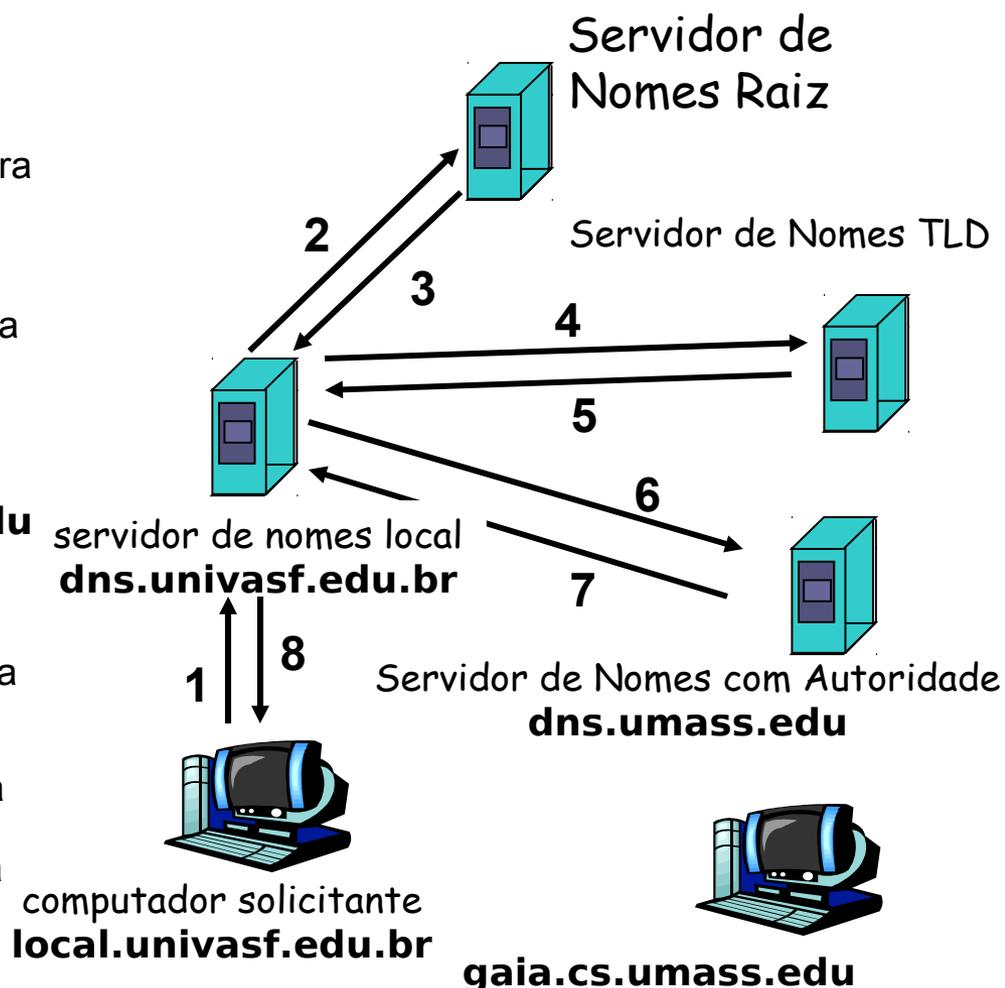
DNS – Tipos de Servidores

- Servidores de Nomes Raiz
 - Existem 13 servidores de nomes raiz no mundo;
 - Cada servidor, na verdade, é um conglomerado de servidores replicados;
- Servidores de Nomes de Domínio de Alto Nível (TLD – *Top-Level Domain*)
 - Servidores responsáveis por domínios de alto nível, como com, org, net, edu e gov;
 - Responsáveis pelos domínios de países, como br, uk, fr;
- Servidores de Nomes com Autoridade
 - Toda organização com *hosts* que possam ser acessados publicamente pela internet, deve fornecer registros que mapeiem os nomes dos seus *hosts* para endereço IP;
 - Geralmente grandes empresas e grandes universidades possuem servidores DNS primários e secundários (*backup*);
- Servidor DNS Local
 - Não pertence propriamente a hierarquia de servidores DNS;
 - Mantidos por ISP's;
 - Funciona como um proxy DNS;

Rede de Computadores

Exemplo Simples

1. O *host* requisita o endereço de **gaia.cs.umass.edu**, que é repassado para o DNS local **dns.univasf.edu.br**;
2. O servidor local repassa a consulta para um servidor DNS raiz;
3. O servidor raiz verifica o sufixo **edu** e retorna uma lista de endereços IP de servidores de nomes TLD responsáveis por **edu**;
4. O servidor de nomes local retransmite a mensagem para um dos servidores da lista;
5. O servidor TLD observa o sufixo **umass.edu** e retorna o endereço IP para o servidor DNS com autoridade para a *University of Massachusetts*;
6. O servidor DNS local envia a mensagem para o servidor de nomes com autoridade para o endereço **dns.umass.edu**;
7. O servidor responde com o endereço IP para **gaia.cs.umass.edu**;
8. O Servidor de nomes local repassa o IP para o computador solicitante.



Tipos de Consulta

● Consulta Recursiva

- É passada uma consulta a um servidor para que o mesmo obtenha e retorne o mapeamento em nome do solicitante;

● Consulta Iterativa

- A consulta é feita a um determinado servidor e o mesmo responde diretamente ao solicitante (ou a resolução do nome ou o endereço do próximo servidor a ser consultado).

Cache DNS

- Utilizado para melhorar o desempenho da resolução de nomes (diminuição do tempo de resposta);
- Quando um servidor DNS recebe uma resposta de uma consulta feita, ele pode armazenar temporariamente esses dados em sua memória local;
- Um servidor de nomes local pode armazenar e responder a consultas, mesmo sem ter autoridade para tanto;

Registros DNS

- O DNS possui uma base de dados distribuída que armazena registro de recursos (RR);
- O RR's fornecem mapeamentos para nomes de hospedeiros para endereços IP;
- Uma mensagem de resposta pode carregar um ou mais RR's;

Registros DNS

- Um RR é uma tupla (conjunto de objetos que compartilham as mesmas características ou possuem a mesma propriedade) de quatro elementos:
 - (*Name, Value, Type, TTL*)
- Os significados de *Name* e *Value* dependem de *Type*.

Rede de Computadores

Registros DNS

● *Type=A*

- *Name* é um nome de hospedeiro e *Value* é o endereço IP para o nome do hospedeiro;
- Ex: (relay.jaca.arvore.com, 200.145.10.1, A);

● *Type=NS*

- *Name* é um domínio (arvore.com) e *Value* é o nome do servidor de nomes com autoridade que sabe resolver os endereços IP para o domínio;
- Ex: (arvore.com, dns.arvore.com, NS);

● *Type=CNAME*

- *Value* é um nome canônico do hospedeiro, cujo nome está em *Name*;
- Ex: (arvore.com, relay.jaca.arvore.com, CNAME);

● *Type=MX*

- *Value* é o nome canônico de um servidor de correio cujo apelido de hospedeiro está contido em *Name*;
- Ex: (arvore.com, mail.jaca.arvore.com, MX);

Registros DNS

- Um apelido pode ser o mesmo para um servidor de correio e para outros servidores, com uma consulta ao registro MX ou ao registro CNAME;
- Um servidor com autoridade para um determinado *host* terá um registro *Type=A*;
- Um servidor sem autoridade para um determinado *host* terá um registro do tipo NS para o domínio que tem o registro *Type=A*.

Rede de Computadores

Mensagens DNS

- *identification*, campo de 16bits, que é o mesmo, tanto para a consulta quanto para a resposta;
- Os *flags* informam: se a mensagem é de consulta ou resposta, *flag* de autoridade, recursão desejada e recursão disponível;
- Os campos *number*, informam a quantidade que virá abaixo;

identification	flags
number of questions	number of answer RRs
number of authority RRs	number of additional RRs
questions (variable number of questions)	
answers (variable number of resource records)	
authority (variable number of resource records)	
additional information (variable number of resource records)	



Mensagens DNS

- *questions*, contêm informações sobre a consulta que está sendo feita;
 - possui um campo com o nome que está sendo consultado e um campo com o tipo da consulta;
- *answers*, é usado nas respostas. Contém os RR's para o nome que foi consultado;
- *authority*, possui registros de outros servidores com autoridade;
- *additional information*, contém outros registros úteis, como o registro *Type=A* para uma consulta *Type=MX*.

Inserção de Dados DNS

● Entidade Registradora

- Entidade comercial que verifica se o nome do domínio é exclusivo, registra-o no banco de dados do DNS e cobra uma taxa por isso.
- No registro é colocado registros *Type A* e *Type NS* nos servidores TLD do domínio para cada servidor existente;
- É feita a inserção de registros *Type A* para os servidores e *Type MX* para os servidores de e-mail;

Rede de Computadores

Brincar com “nslookup”

nslookup www.hotmail.com

Server: 10.87.10.14

Address: 10.87.10.14#53

Non-authoritative answer:

www.hotmail.com canonical name = toplevel.mail.live.com.akadns.net.

toplevel.mail.live.com.akadns.net canonical name = origin.mail.live.com.

Name: origin.mail.live.com

Address: 64.4.20.184

Name: origin.mail.live.com

Address: 64.4.20.186

Name: origin.mail.live.com

Address: 64.4.20.169

Name: origin.mail.live.com

Address: 64.4.20.174