Redes de Computadores

Camada de Aplicação

Agenda

DNS

1

DNS

Visão Geral, Serviços, Tipos de Servidores, Interações, Formato de Mensagem

Visão Geral do DNS

- Visão pessoal: Muitas identificações
  - RG
  - CPF
  - Passaporte
  - Nome
- Roteadores e Hosts
  - Endereços IP (32b) - endereçamento dos datagramas
  - “Nome” - endereçamento para as pessoas

Visão Geral do DNS

- Enorme banco de dados distribuído:
  - Em torno de bilhões de registros, cada um simples
- Lida com muitos trilhões de consultas/dia:
  - Muito mais leituras do que gravações
  - O desempenho é importante: quase todas as transações da Internet interagem com o DNS - contagem de milisegundos!

Visão Geral do DNS

- Banco de dados distribuído implementado na hierarquia de muitos servidores de nomes
- Protocolo de camada de aplicação: hosts, servidores DNS se comunicam para resolver nomes (tradução de endereço/nome)
    - Nota: função central da Internet, implementada como protocolo de camada de aplicação
    - Complexidade na “borda” da rede

Visão Geral do DNS

- Organizacionalmente, fisicamente descentralizado:
  - Milhões de organizações diferentes responsáveis por seus registros
  - “à prova de balas”: confiabilidade, segurança

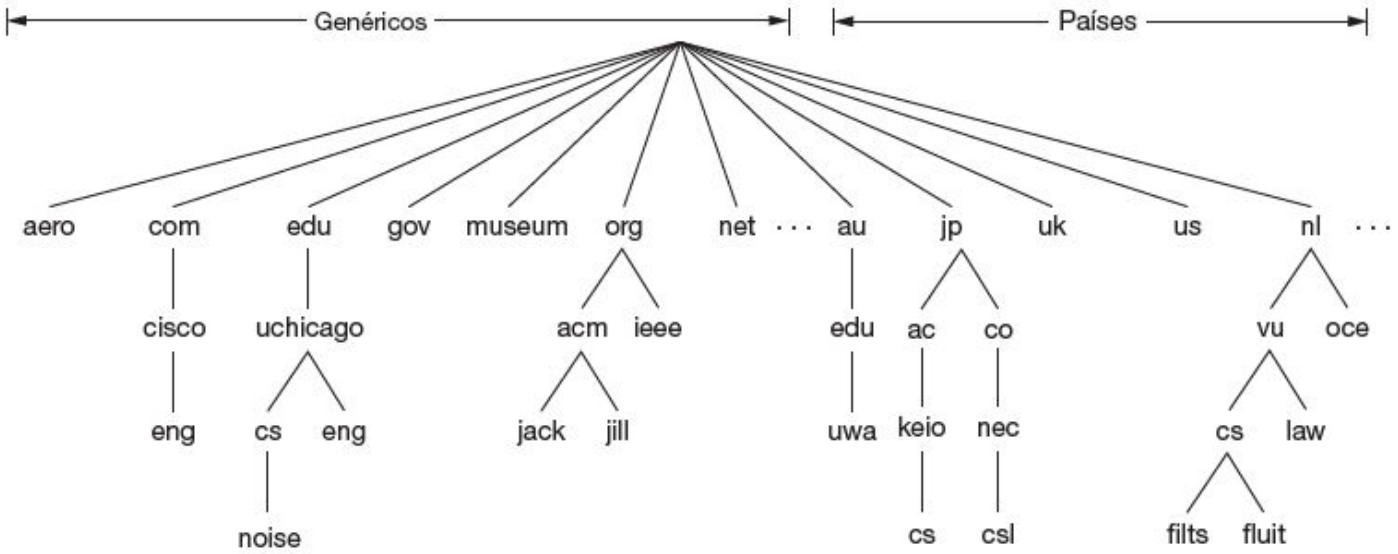
Serviços DNS

- Tradução de nome de host para endereço IP
- Alias (apelido) de host e de servidor de correio
- Distribuição de carga
- Servidores Web replicados: muitos endereços IP correspondem a um nome

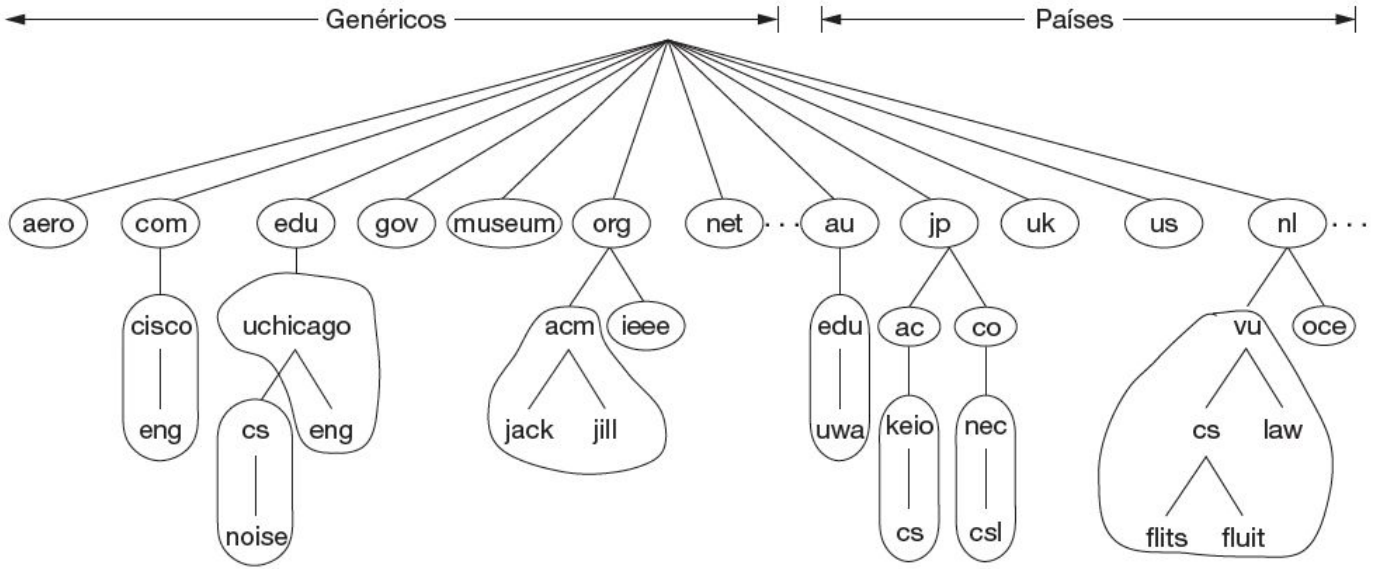
Serviços DNS

- Por que não centralizar o DNS?
  - Ponto único de falha
  - Volume de trafego
  - Banco de dados centralizado distante
  - Manutenção
  - Não é escalável!
    - Servidores DNS Comcast sozinhos: 600B de consultas DNS/dia
    - Servidores DNS da Akamai sozinhos: 2,2T de consultas DNS/dia

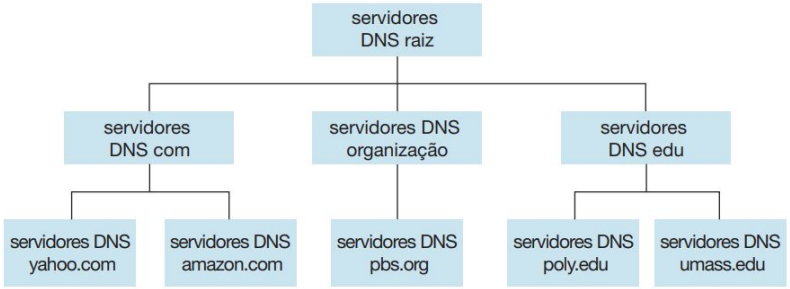
Visualização do DNS



Visualização do DNS



Visualização do DNS



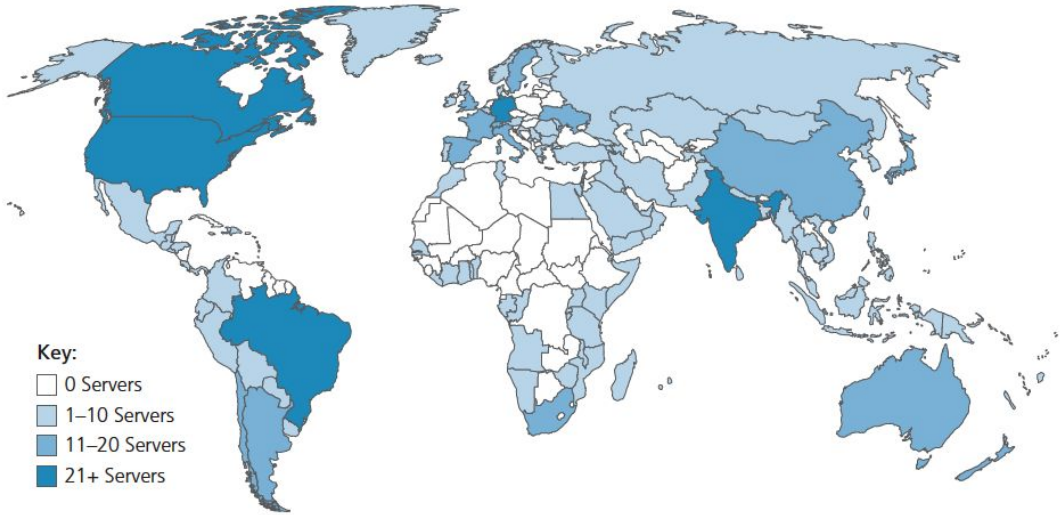
- Cliente quer o IP para www.amazon.com; 1ª aprox.:
  - Cliente consulta um servidor de raiz para encontrar o servidor DNS .com
  - Cliente consulta o servidor DNS com para obter o servidor DNS amazon.com
  - Cliente consulta o servidor DNS amazon.com para obter o endereço IP para www.amazon.com

Tipos de Servidores DNS

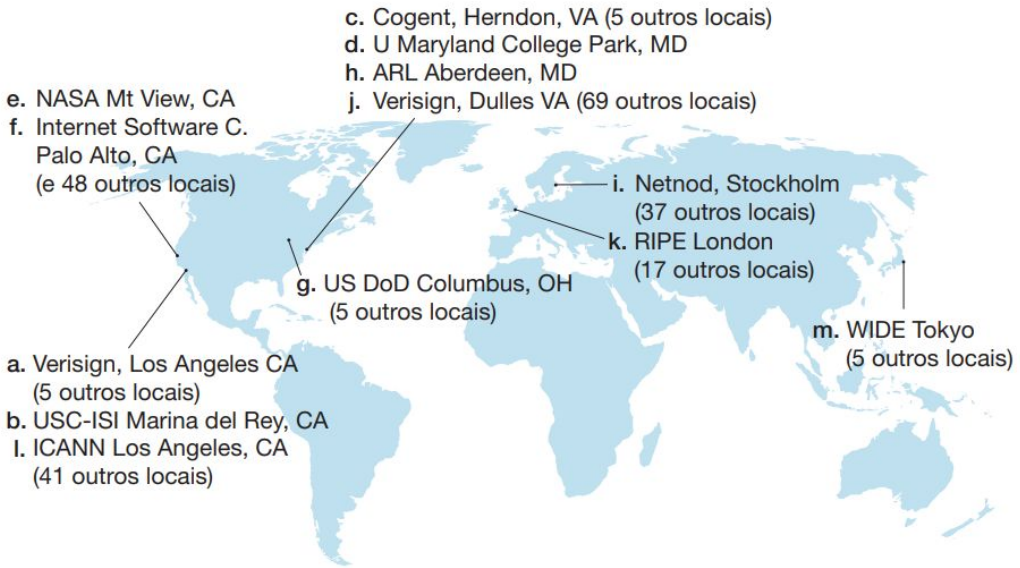
- Servidores de Nomes Raiz
  - São contatados pelos servidores de nomes locais que não podem resolver um nome
  - Buscam servidores de nomes autorizados se o mapeamento do nome não for conhecido
    - Conseguem o mapeamento
    - Retornam o mapeamento para o servidor de nomes local

Tipos de Servidores DNS

- Servidores de nomes raiz pelo mundo (USA: ~200)



Tipos de Servidores DNS



Tipos de Servidores DNS

- Servidores Top-Level Domain (TLD): responsáveis pelos domínios com, org, net, edu etc e todos os domínios top-level nacionais uk, fr, ca, jp, br
  - Soluções de rede mantém servidores para o TLD “com”
  - Educause para o TLD “edu”

Tipos de Servidores DNS

- Servidores DNS autorizados: servidores DNS de organizações
  - Provêem nome de hospedeiro autorizado para mapeamentos IP para servidores de organizações (ex.: Web e mail)
  - Podem ser mantidos por uma organização ou provedor de serviços

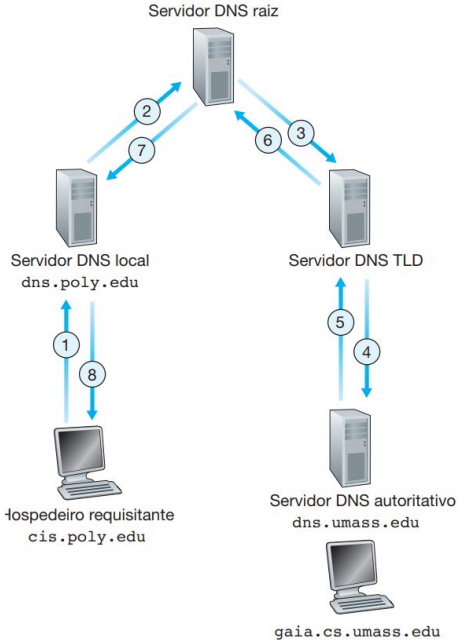
Tipos de Servidores DNS

- Servidor Local
  - Não pertence estritamente a uma hierarquia
  - Cada ISP (ISP residencial, companhia, universidade) possui um
    - Também chamado de “servidor de nomes default”
  - Quando um hospedeiro faz uma pergunta a um DNS, a pergunta é enviada para seu servidor DNS local
    - Age como um procurador (proxy), encaminhando as perguntas para dentro da hierarquia

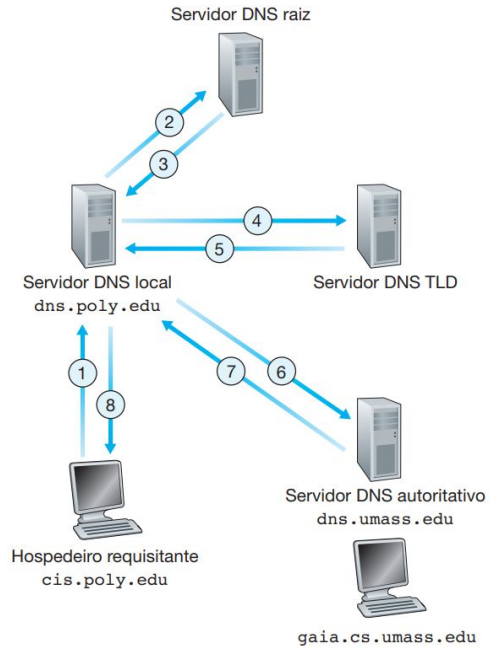
Exemplo de Consulta DNS

- Consulta recursiva: Transfere a tarefa de resolução do nome para o servidor de nomes consultado
- Consulta encadeada: Servidor contatado responde com o nome de outro servidor de nomes para contato
    - “eu não sei isto, mas pergunte a este servidor”

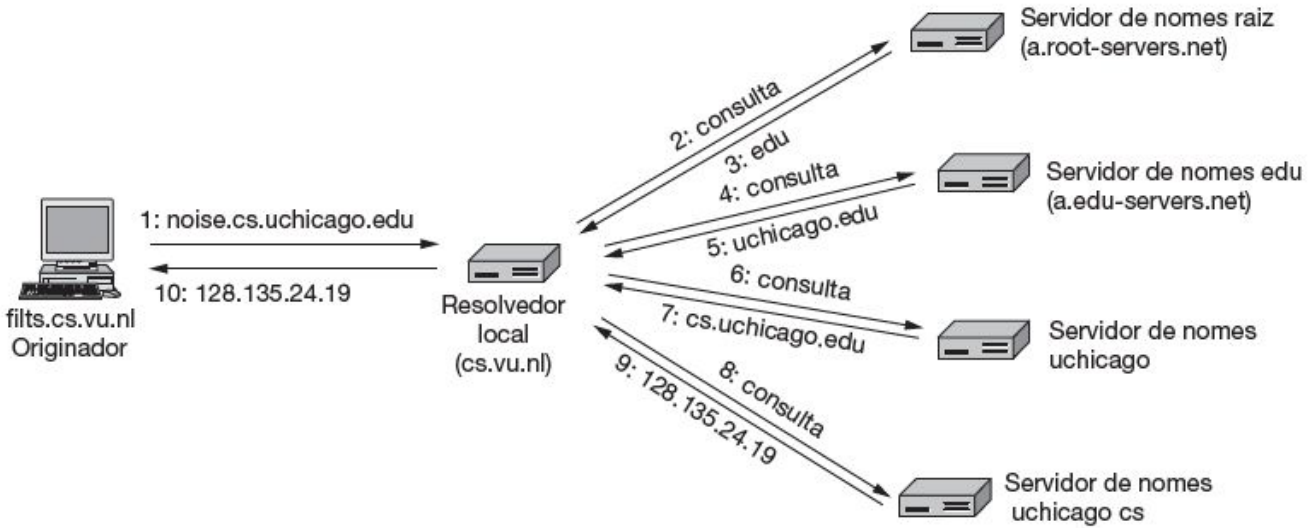
Exemplo de Consulta DNS



Interação de Servidores DNS



Interação de Servidores DNS



Atualizações DNS

- Uma vez que um servidor de nomes aprende um mapeamento, ele armazena o mapeamento num registro do tipo cache
  - Registro do cache tornam-se obsoletos e desaparecem depois de um certo tempo
  - Servidores TLD são tipicamente armazenados em cache nos servidores de nome locais

Atualizações DNS

- DNS: base de dados distribuída que armazena registros de recursos (RR)
  - formato dos RR: (name, value, type,ttl)
- Type = A
  - name é o nome do computador
  - value é o endereço IP
- Type = NS
  - name é um domínio (ex.: foo.com)
  - value é o endereço IP do servidor de nomes autorizados para este domínio

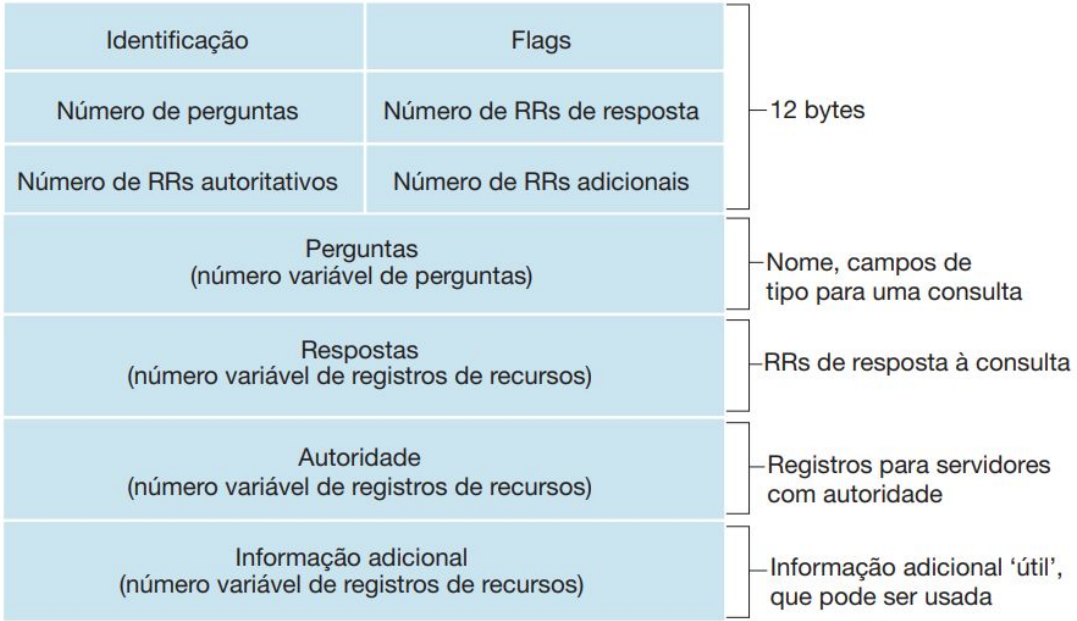
Atualizações DNS

- DNS: base de dados distribuída que armazena registros de recursos (RR)
  - formato dos RR: (name, value, type,ttl)
- Type = CNAME
  - name é um “apelido” para algum nome “canônico” (o nome real)
    - Exemplo: www.ibm.com é realmente www.ibm.com.cs186.net
  - value é o nome canônico
- Type = MX
  - value é o nome do servidor de correio associado com name

Formato de Mensagem

- Protocolo DNS: mensagem de consulta e resposta , ambas com o mesmo formato de mensagem
- Cabeçalho da mensagem
  - Identificação: 16 bits para consulta, resposta usa o mesmo número
  - Flags:
    - Consulta ou resposta
    - Recursão desejada
    - Recursão disponível
    - Resposta é autorizada

Formato de Mensagem



Segurança DNS

- Ataques DDoS
  - Bombardeio em servidores raiz com tráfego
    - Sem sucesso até hoje
    - Filtragem de tráfego
    - Servidores DNS locais armazenam IPs de servidores TLD, permitindo o desvio do servidor raiz
  - Bombardeio em servidores TLD
    - Potencialmente mais perigoso

Segurança DNS

- Ataques de falsificação
  - Interceptação de consultas DNS, retornando respostas falsas
    - Envenenamento de cache DNS
    - RFC 4033: serviços de autenticação DNSSEC

Obrigado!

Dúvidas?