Instituto de Informática - UFRGS

Redes de Computadores

Domain Name System (DNS)

Aula 25

Introdução

- Máquinas na Internet são identificadas por endereços IP
- Nomes simbólicos são atribuídos a máquinas para facilitar seu uso
  - e-mail: asc@inf.ufrgs.br
  - Servidor web: www.inf.ufrgs.br
- Necessidade de conversão nomes simbólicos para endereços IP
  - Resolução de nomes feito por um serviço de nomes
- *Domain Name System* é
  - o sistema de nomes usado na Internet
  - um protocolo Internet usado para resolver nomes

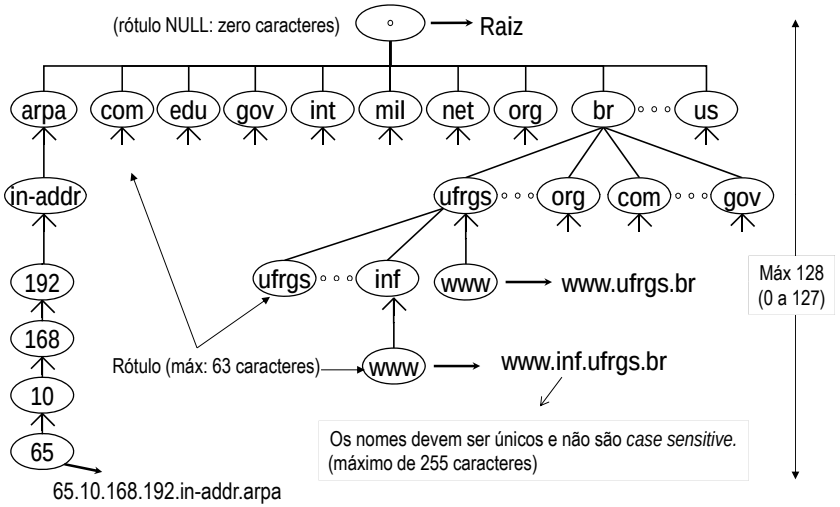
Sistema de nomes

- Maneira de referenciar simbolicamente objetos de um sistema
  - Possuem uma sintaxe e uma semântica
  - Conjunto de nomes válidos: espaço de nomes
- Espaço de nomes designa um nome único a um "objeto"
  - Plano: um nome é um conjunto de caracteres sem estrutura alguma
    - Quantidade finita de nomes
    - Normalmente um controle centralizado para evitar duplicação
      - e.g.: placas de automóveis (ABC1234), endereços IP, etc
  - Hierárquico: nome é dividido em porções
    - Quantidade infinita de nomes
    - Controle pode ser distribuído: cada organização cuida de sua porção
      - e.g.: sistemas de arquivos (arquivos em um diretório)

Espaço de nomes DNS

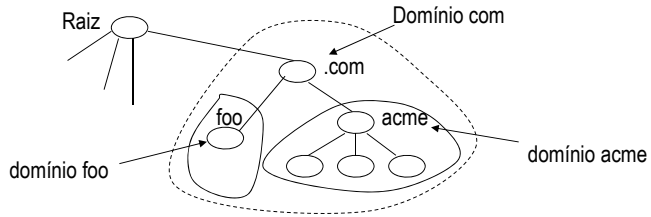
- Espaço de nomes é hierárquico (em árvore)
  - A raiz da árvore é notada como "." (*root*)
  - Os nós intermediários representam domínios
  - Os nós-folha representam objetos nomeados (máquinas)
- Cada nó possui um rótulo
  - O nome do nó é uma sequência de rótulos separados por ponto
  - O s nós podem ser referenciados por seus nomes absolutos ou relativos
    - *Fully Qualified Domain Name* (FQDN): descreve a hierarquia de nós
      - e.g: asterix.inf.ufrgs.br. (atenção ao "." final)
    - *Partial Qualified Domain Name* (PQDN): nome que não atinge a raiz
      - E.g.: asterix (supõe que se está no domínio *inf.ufrgs.br*)

Espaço de nomes DNS



Domínios e subdomínios

- Domínio é uma subárvore do espaço de nomes DNS
  - O nome de um domínio é o nome do nó de sua subárvore
  - Um domínio pode ser dividido em subdomínios
- Os domínios de mais alto nível (*Top Level Domain*) são de três tipos:
  - Organizacionais: áreas de atuação de instituições e indivíduos
  - Geográficos: códigos de países (duas letras)
  - Arpa: domínio especial usado para mapeamento reverso

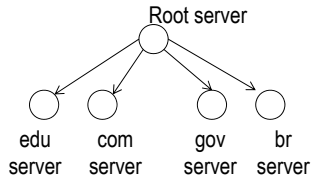


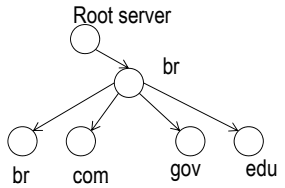
Registros DNS: *resource record* (RR)

- Nomes DNS estão associados a atributos definidos em um registro
  - Pode ser de um domínio ou de uma máquina
- Registro de recurso formam a base de dados do DNS
  - Quando se pesquisa por um nome, se obtém os registros de recursos associados àquele nome
- Registros de recursos (RR) é uma tupla (*nome, valor, tipo e TTL*)
  - Interpretação do *nome* e do *valor* dependem do *tipo,* exemplos:
    - A ou AAAA: associa nome simbólico a um endereço IPv4/IPv6
    - CNAME: define um "apelido" (alias) para um nome simbólico
    - NS: define os servidores de nome do domínio
    - MX: servidor de correio eletrônico
    - SOA: definição do servidor primário

Distribuição do espaço de nomes

- Necessário armazenar o espaço de nomes
  - Não pode ser centralizado (ineficiente → gargalo, tolerância a falhas)
- Solução:
  - Distribuir o espaço de nomes entre diferentes máquinas →Servidores de DNS
- Subdivisão pode continuar grande
  - Subdivide a subdivisão, criando uma hierarquia de servidores

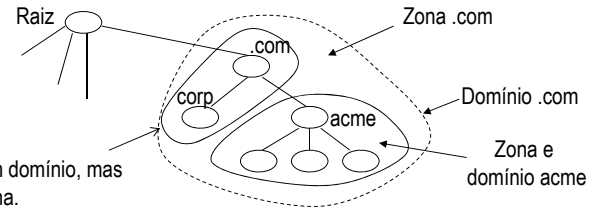




Pode ser responsável por um domínio grande ou pequeno (responsável=autoridade)

Conceito de zona

- Porção administrativa de um (sub)domínio DNS
  - Subárvore do espaço de nomes que contém um servidor responsável por ela
  - Pode ser composta por domínios, (sub)zonas e máquinas
- Zona é composta por:
  - Um arquivo mestre que contém os RRs de um domínio
  - Armazenado em um servidor (autoridade dos dados)



Delegação de autoridade

- Autoridade é a entidade responsável pelo arquivo mestre
  - Cada zona é administrada por uma autoridade (servidor)
    - Se um servidor é responsável por um domínio e não delega responsabilidade a noção de domínio e zona se confundem
- Delegação de autoridade
  - Autoridade pode ser distribuída entre zonas e uma zona pode subdividi-la em zonas menores (sub-zonas)
    - Compõe uma hierarquia de servidores
- Arquivos de zona ou mestre (*zone files*)
  - Base de dados mantida pelo servidor com informações dos nós do domínio
    - Inclui, se o domínio foi subdividido em zonas, quem são os responsáveis pelas sub-zonas

Definição da hierarquia de servidores DNS

- Os servidores raiz apontam para servidores TLD que por sua vez apontam para servidores autoridade do nível inferior
- Inserção nos servidores TLD é feito por uma entidade de registro
- Entidade de registro
  - Organismo (comercial) que verifica se um nome de domínio é exclusivo
  - Registra nome de domínio em sua base de dados (pagamento anuidade)
    - Cadastra os servidores DNS (primário e secundário) da organização que solicita seu registro → são os servidores autoridade
  - No Brasil é o http://www.registro.br
- Um servidor autoridade pode servir como "entidade de registro" para subdomínios abaixo dele

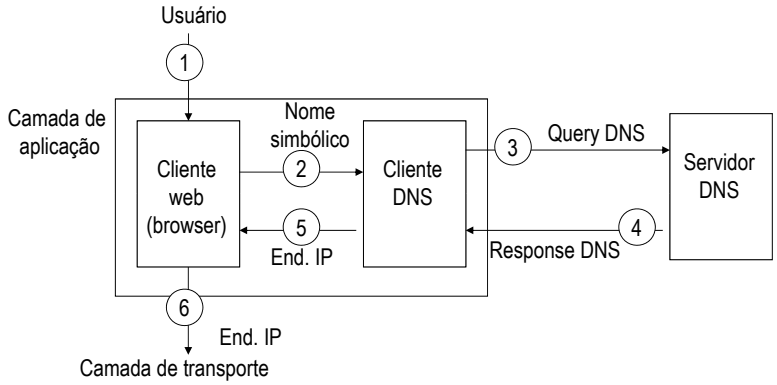
Servidores raiz, TLD e autoridade

- Servidores raiz
  - Sua zona é formada por toda a árvore do DNS
  - Delega autoridade a outros outros servidores fazendo referência a eles
  - Existem 13 servidores raiz (A, B, C, D, E, F, G, H, I, J ,K , L e M)
    - Distribuídos no mundo
- Servidores Top Level Domain (TLD)
  - Responsáveis pelos domínios de alto nível: com, org, mil, net, br, fr, it etc
- Servidores autoridade
  - Responsável por abrigar registros de uma organização
    - e.g.: servidor DNS responsável pelas máquinas na UFRGS (ufrgs.br)
  - Podem "delegar" autoridade a sub-níveis

Tipos de servidores DNS: primário e secundário

- Servidor primário
  - Servidor que mantém um arquivo de zona para a subárvore que é autoridade
  - Responsável por criar, manter e atualizar o arquivo de zona
    - Arquivo de zona é um arquivo no sistema de arquivos do servidor
- Servidor secundário
  - Servidor que obtém a informação do arquivo de zona de outro servidor (primário ou secundário) e armazena em seu sistema de arquivos
    - Denominado "transferência de zona"
  - Não cria, nem atualiza o arquivo de zona, seu objetivo é redundância (disponibilidade do serviço de DNS)
- Em uma zona:
  - Existe um servidor primário e um ou mais secundários
  - Servidor primário e secundário são autoridades para a zona que servem

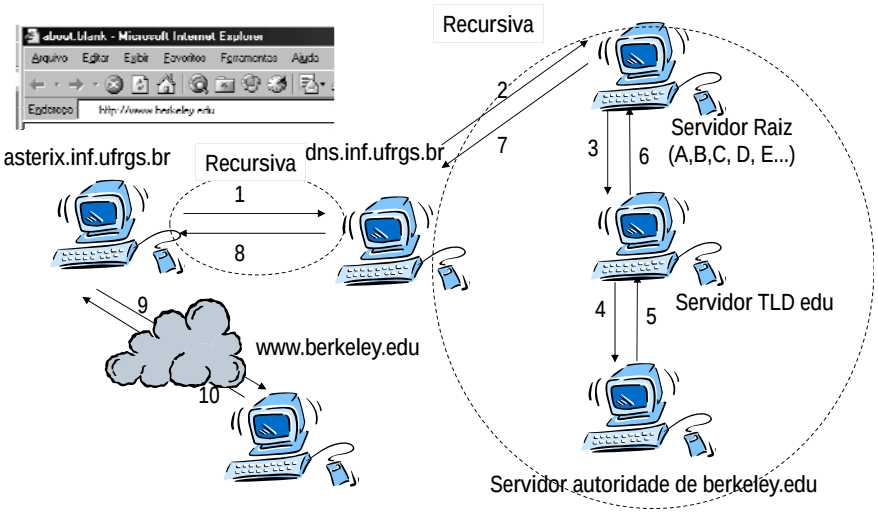
Resolução de nomes



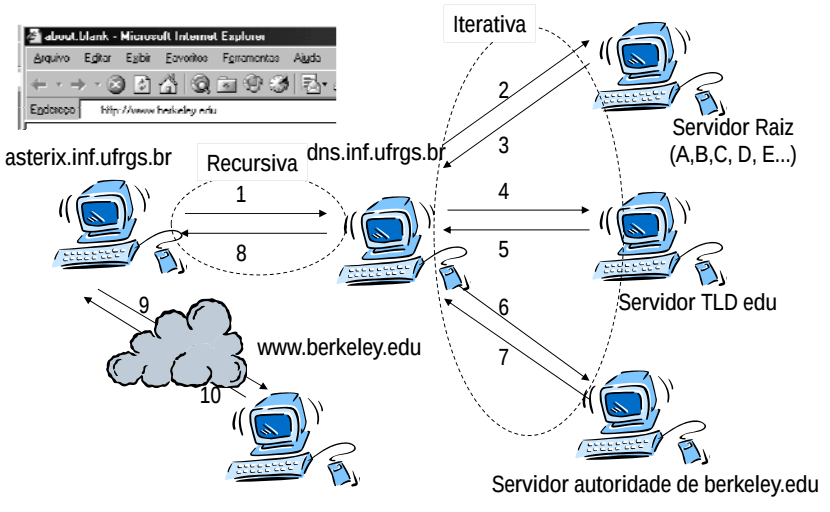
Consulta iterativa e recursiva

- Iterativa (não recursiva)
  - Servidor emprega apenas informações locais para atender a requisição
  - Resposta contém:
    - as informações requisitadas OU
    - informações auxiliares que identificam servidores com autoridade no domínio de nível mais inferior
- Recursiva
  - Servidor emprega informações locais e, na ausência, encaminha requisição para outros servidores para obter a resposta
  - Resposta contém as informações requisitadas

O Processo de consulta DNS: recursiva



O Processo de consulta DNS: iterativa



Problema com a resolução de nomes

- Esquema original é penalizante para o servidor raiz, então se faz algumas otimizações
  - Replicação:
    - Várias cópias dos servidores raizes e dos servidores TLD geograficamente dispersos
  - Cache:
    - Armazenamento local das resoluções recentes

Mecanismo de cache DNS

- Cada servidor mantém uma cache de resolução de nomes
  - Novas consultas a um nome armazenado são resolvidos com essa cópia local
    - Reduz o tráfego DNS
    - Alivia consulta a servidores de hierarquia mais alta
  - Resposta é assinalada como non-authoritative
- Respostas armazenadas na cache possuem um tempo de vida
  - Configurado pela entidade com autoridade do respectivo domínio ou definida pelo servidor non-authoritative
  - Entrada é automaticamente removida na expiração do seu tempo de vida
- Problema:
  - Resposta fornecida por uma informação na cache pode não ser válida

Respostas DNS

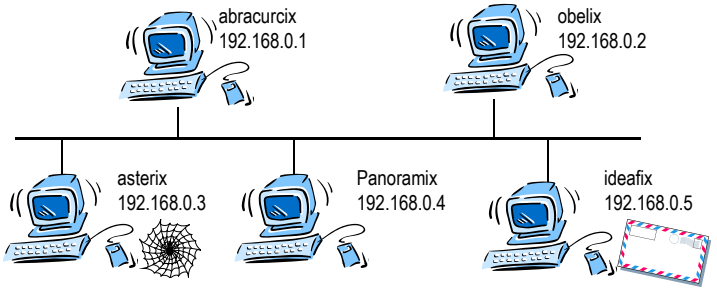
- *Authoritative* (registro oficial)
  - Gerada por um servidor que possui autoridade para o domínio do nome a ser resolvido
  - Resposta representa o que está nos arquivos de configuração de zona
- *Non-authoritative* (registro em cache)
  - Gerada por servidores que não possuem autoridade no domínio do nome a ser resolvido
  - Resposta não é confiável pois as informações podem ter sido modificadas nos arquivos de configuração de zona, mas ainda não foram propagadas
- Respostas de cache são sempre *non-authoritative*
  - Indicam os servidores com autoridade no respectivo domínio

DNS Reverso

- Dado um endereço IP obter o nome simbólico da máquina
  - Alguns serviços tem uma lista com o nome simbólico das máquinas autorizadas a executá-lo
- Baseado na consulta a um domínio especial: *in-addr.arpa*
- Cada endereço IP possui uma representação nesse domínio
  - e.g.: IP 212.198.253.142 ⇔ 142.253.198.212.in-addr.arpa

Exemplo: Criando um pequeno domínio

- Supondo uma rede composta por 5 máquinas no domínio village.net
- Funcionalidades das máquinas:
  - abracurcix.village.net: servidor DNS
  - ideafix.village.net: servidor mail (smtp e pop)



Zona village.net

```
village.net. IN SOA abracurcix.village.net. root .village.net. (
                1       ;serial  -> indicação de versão
                3600    ;refresh -> freq. de verificação escravos
                600     ;retry   -> tempo entre tentativas de atualz.
                60480   ;expire  -> tempo escravo responde p/ mestre
                86400)  ;minimum -> tempo de vida dos dados em cache

                IN NS   abracurcix.village.net.

abracurcix      IN      A       192.168.0.1
obelix          IN      A       192.168.0.2
asterix         IN      A       192.168.0.3
panoramix       IN      A       192.168.0.4
ideafix         IN      A       192.168.0.5
localhost       IN      A       127.0.0.0
```

Aliases e Registro MX

```
abracurcix      IN      A       192.168.0.1
obelix          IN      A       192.168.0.2
asterix         IN      A       192.168.0.3
panoramix       IN      A       192.168.0.4
ideafix         IN      A       192.168.0.5
localhost       IN      A       127.0.0.0

; Aliases

smtp            CNAME           ideafix
pop             CNAME           ideafix
ftp             CNAME           asterix
www             CNAME           asterix

; E-mail

village.net     IN      MX      10      ideafix
```


Zona 0.168.192.in-addr.arpa

```
0.168.192.in-addr.arpa IN SOA abracurcix.village.net.
        root.village.net. (
                        1;
                        3600;
                        600;
                        60480;
                        86400)

    IN   NS      abracurcix.village.net.

1   IN   PTR      abracurcix.village.net.
2   IN   PTR      obelix.village.net.
3   IN   PTR      asterix.village.net.
4   IN   PTR      panoramix.village.net.
5   IN   PTR      ideafix.village.net.
```


Protocolo DNS

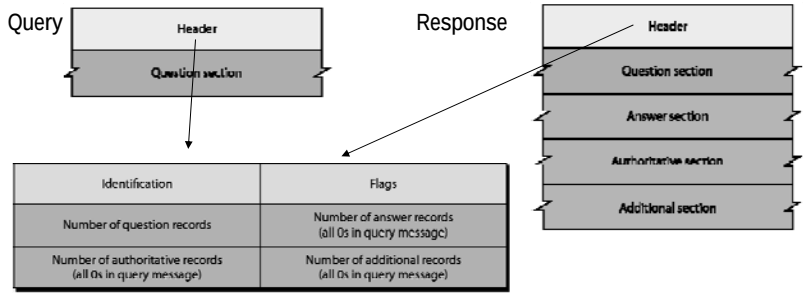
- Modelo cliente-servidor
- Servidor emprega a porta 53 (UDP/TCP)
  - TCP é usado em transferência de zonas ou para respostas que são superiores a 512 bytes (truncamento se UDP)
- Implementa as consultas DNS na Internet
  - Baseado em duas mensagens: requisição e resposta
  - Mensagens possuem um cabeçalho comum

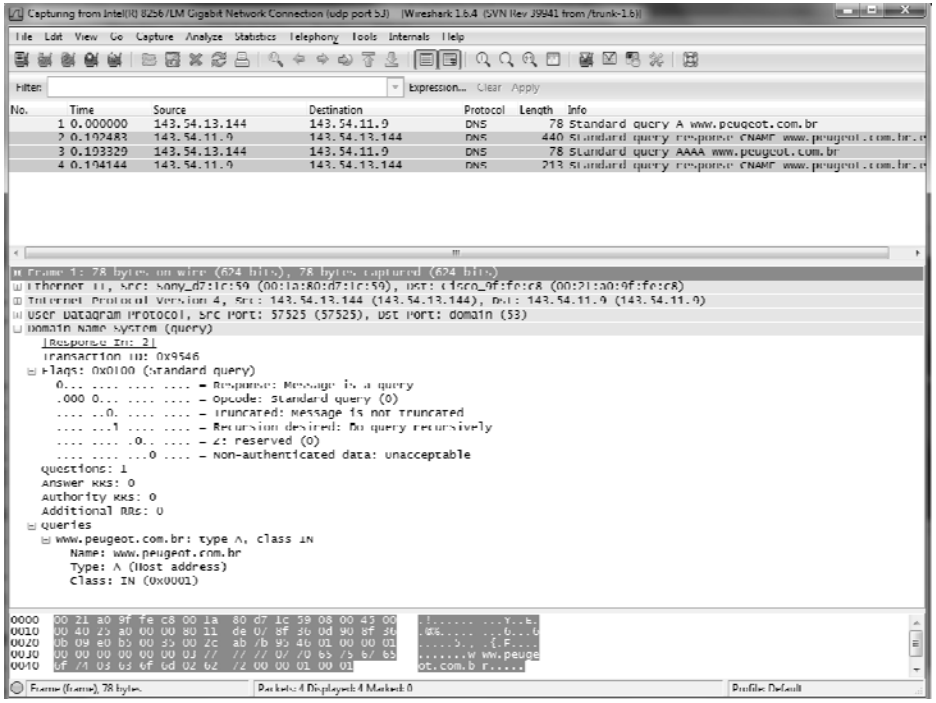
Modelo cliente-servidor

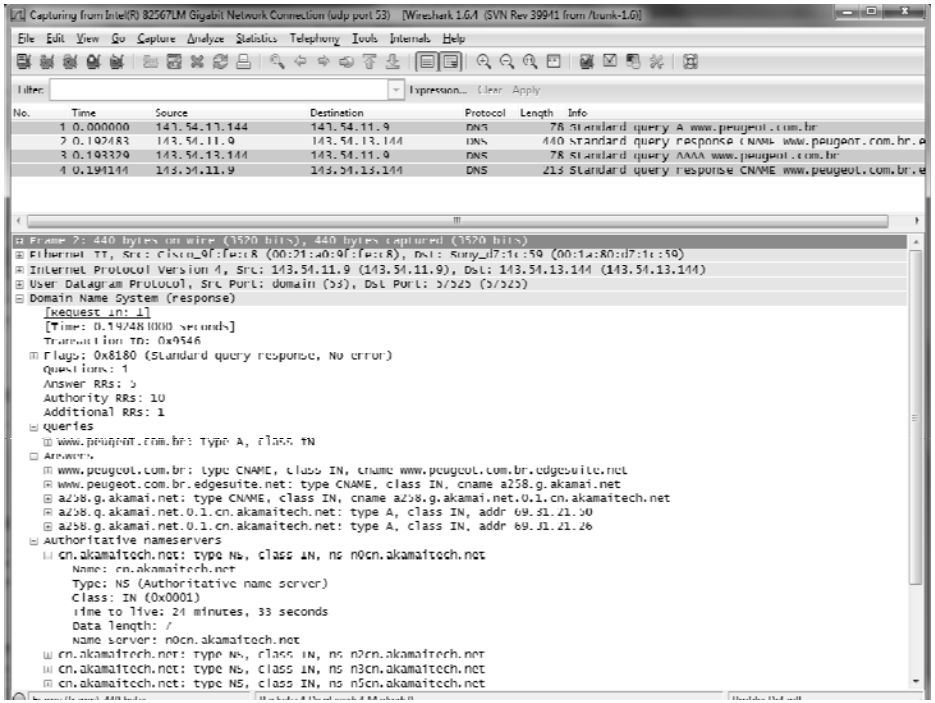
- Cliente
  - Processo de aplicação que acessa servidores de nome
  - Normalmente implementado por chamadas de funções disponibilizadas pelo sistema operacional
  - Em Unix é comumente denominado de *resolver*
    - Configuração em */etc/resolv.conf* (servidores a consultar e domínio)
- Servidor
  - Processo de aplicação que trata as requisições DNS
  - Em Unix, o servidor mais comum é o BIND (*Berkeley Internet Name Domain*)

Mensagens DNS: consultas e respostas

- Mensagem organizada em seções
  - Pergunta: informações sobre a consulta (nome/tipo)
  - Resposta: Resource Records (RR) que satisfazem a consulta
  - Autoridade: registros relativos a outros servidores com autoridade
  - Adicional: RR com informações que podem ser úteis a futuras consultas DNS





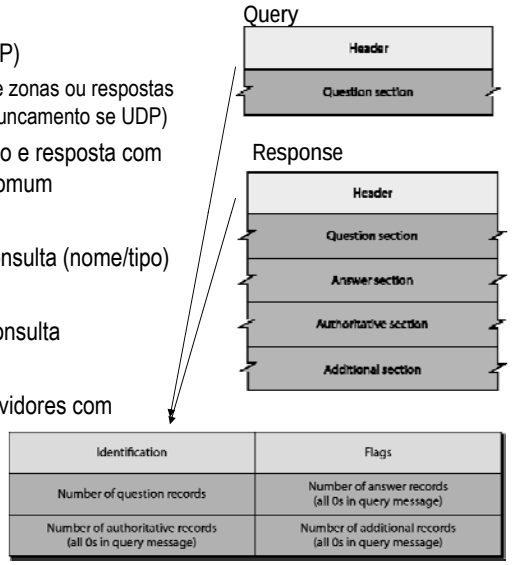


Leituras complementares

- Tanenbaum, A. *Redes de Computadores* (4ª edição), Campus, 2000.
  - Capítulo 7, seção 7.1
- Carissimi, A.; Rochol, J; Granville, L.Z; *Redes de Computadores*. Série Livros Didáticos. Bookman 2009.
  - Capítulo 7, seção 7.1

Mensagens DNS

- DNS usa porta 53 (UDP/TCP)
  - TCP para transferência de zonas ou respostas superiores a 512 bytes (truncamento se UDP)
- Duas mensagens: requisição e resposta com um cabeçalho de formato comum
- Seção pergunta
  - Informações sobre a consulta (nome/tipo)
- Seção resposta
  - RR que satisfazem a consulta
- Seção autoridade
  - Registros de outros servidores com autoridade
- Seção adicional
  - RR úteis



Servidores primário e secundário

- Servidor primário (mestre)
  - Mantém os arquivos de configuração local com as informações da zona que possui autoridade
  - Um único servidor por zona
    - Mas um servidor pode atender mais de uma zona simultaneamente
- Servidor secundário (escravo)
  - Objetivo é oferecer disponibilidade ao serviço de DNS
    - Deve ser independente do primário e estar situado em um local diferente
  - Mantém uma cópia das informações da zona que possui autoridade
  - Recebe essas informações diretamente do servidor primário
    - Procedimento denominado de transferência de zona

Outros serviços importantes do DNS

- Aliases para máquinas: sinônimos para o nome canônico
  - Nome canônico: nome "oficial" da máquina (e.g. relay1.west-coast.acme.com)
  - Alias: nome de mais fácil memorização (e.g. www.acme.com)
- Resolução de alias (para servidores)
  - Dado um alias descobre o nome canônico
    - e.g.: quem é o MX do acme.com? (Mail eXchanger)
- Distribuição de carga
  - Comum para resolução de nomes de servidores muito acessados
  - Conjunto de endereços IP associados a um nome canônico
    - Na resolução entrega esse conjunto de forma a fazer um rodízio

Detalhes, curiosidades, etc

- Exemplos de consultas DNS
  - dnspeugeot.dump
  - dns-www.fiat.com.br (consulta recursiva)
  - dns.dump (consulta forçada ao raízes)
- Lista dos operadores dos 13 servidores raiz
  - http://www.root-servers.org
- Servidor *f.root-server.br* no Brasil
  - Fisicamente instalado em São Paulo (registro.br – fapesp)
  - Existem 46 réplicas no mundo do servidor f.root-server.br
    - http://www.isc.org/community/f-root/sites

Resolução de nomes

- Modelo cliente-servidor
- Cliente (*resolver*)
  - Parte da instalação padrão de qualquer sistema operacional
  - Conjunto de funções de bibliotecas
  - Qualquer aplicativo pode realizar acessos a essas rotinas
- Servidor de nome (*name server*)
  - *Daemon* (processo) que recebe requisições (consultas)
  - Distribuídos geograficamente e interagem para resolver nomes
  - Servidor de domínio mantém informações locais sobre subdomínios e máquinas
  - Servidor de domínio conhece todos servidores dos subdomínios
  - Exemplo:
    - Berkeley Internet Name Domain (*bind*) implementado pelo *daemon named*

Servidores primário e secundário

- Servidor primário (mestre)
  - Mantém os arquivos de configuração local com as informações da zona que possui autoridade
  - Um único servidor por zona
    - Mas um servidor pode atender mais de uma zona simultaneamente
- Servidor secundário (escravo)
  - Objetivo é oferecer disponibilidade ao serviço de DNS
    - Deve ser independente do primário e estar situado em um local diferente
  - Mantém uma cópia das informações da zona que possui autoridade
  - Recebe essas informações diretamente do servidor primário
    - Procedimento denominado de transferência de zona

Tipos de servidores DNS

- Recursivo
  - Recebe requisições recursivas e usa requisições iterativas para obter a resposta
    - Cenário típico: máquinas de usuários e servidor DNS configurado
- Encaminhador (forwarder)
  - Recebe requisição recursiva e as repassa a um servidor recursivo