Laboratório de Pesquisa em Redes e Multimídia

DNS – Domain Name System

Prof. José Gonçalves
Departamento de Informática – UFES
zegonc@inf.ufes.br

Universidade Federal do Espírito Santo
Departamento de Informática

DNS - Domain Name System

- O DNS é um "sistema de nomes" cujo objetivo primário é mapear, em escala global, nomes de domínios de rede e nomes de máquinas em endereços IP, processo conhecido por "*resolução de nomes*".
- O DNS possui também a funcionalidade reversa, traduzindo endereços IP em nomes.

DNS - Domain Name System (cont.)

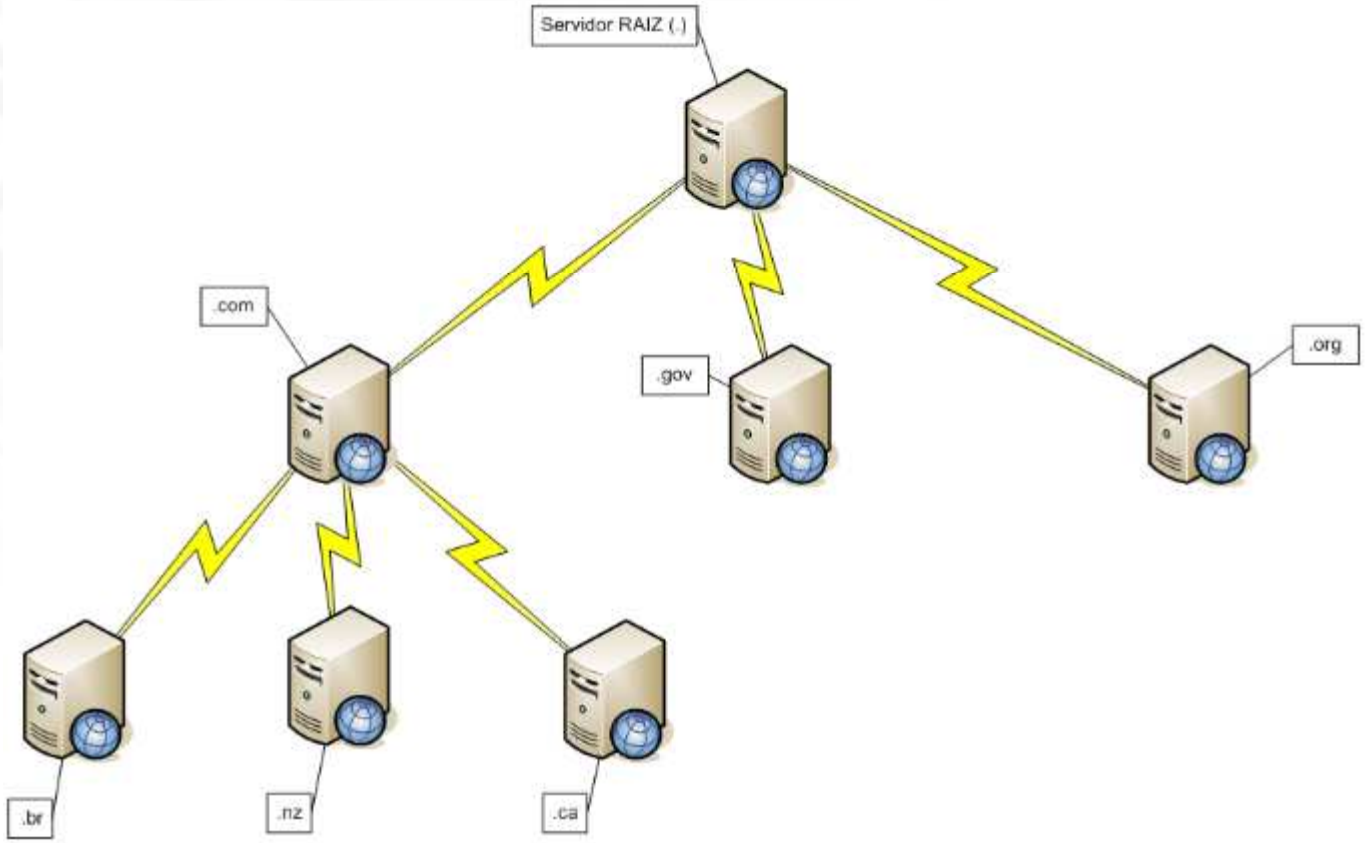
manguinhos.lprm.inf.ufes.br

200.241.16.8

DNS - Domain Name System

- O DNS é estruturado na forma de um banco de dados hierárquico distribuído, onde cada servidor é responsável por manter uma tabela com os endereços IP e nomes dos *hosts* em seu sub-domínio.

DNS - Domain Name System (cont.)



Histórico

- Antigamente, o mapeamento entre nomes de *hosts* e endereços IP era mantido em uma tabela estática, implementada como um arquivo de texto único (Unix: arquivo /etc/hosts).
- Esta tabela era gerenciada de forma centralizada e era distribuída para todos os computadores da antiga Arpanet.
- Os nomes de *hosts* não seguiam o esquema hieráquico atual. O procedimento para nomear um computador incluía verificar se já existia um outro computador com aquele nome. Como se pode deduzir, o arquivo estava constantemente desatualizado.

Histórico (cont.)

- O DNS resolveu o problema de se ter uma tabela estática administrada centralmente introduzindo dois novos conceitos:
  - Nomes de *hosts* hierárquicos; e
  - Distribuição da responsabilidade pela resolução de nomes.

Histórico (cont.)

- O DNS foi especificado formalmente por Paul Mockapetris nas RFCs 882 e 883 (1983), alterado pelas RFCs 1034 e 1035 (1987) e estendido nas RFCs 1101 e 1183 (1990).
- Em 1985, Kevin Dunlap, em Berkeley, produziu o *BIND – Berkeley Internet Name System*, uma implementação de sucesso do DNS.
- O BIND é hoje parte da maioria das implementações Unix.

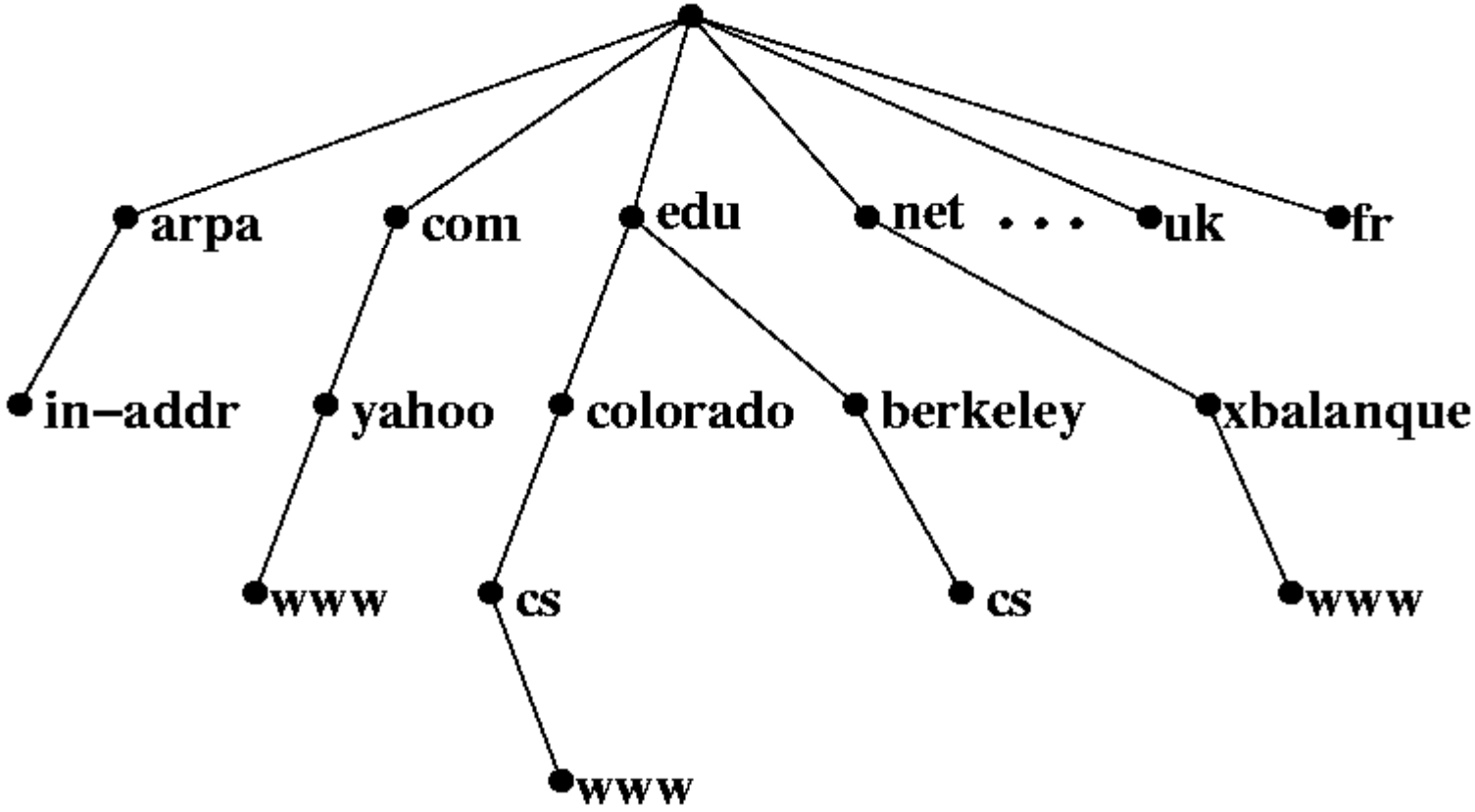
O que é definido pelo DNS?

- Um espaço de nomes hierárquico para *hosts*.
- Uma tabela de *hosts* implementada como um banco de dados distribuído.
- Rotinas de biblioteca para fazer consultas (*queries*) a este banco de dados.
- Um protocolo para trocar informações de nomes.

O Espaço de Nomes do DNS

- O espaço de nomes do DNS é representado em uma estrutura hierárquica, em forma de árvore, onde cada nó possui um *label* de até 63 caracteres.
- Não existe diferenciação entre letras maiúsculas e minúsculas, e a raiz da árvore é um nó especial, de *label* nulo.
- O espaço de nomes do DNS é, na verdade, uma árvore de nomes de domínios (*domain names*), com autoridade ascendente, cuja raiz está no Departamento de Defesa dos EUA (DoD – Department of Defense) e é chamada de "." (ponto).

O Espaço de Nomes DNS (cont.)



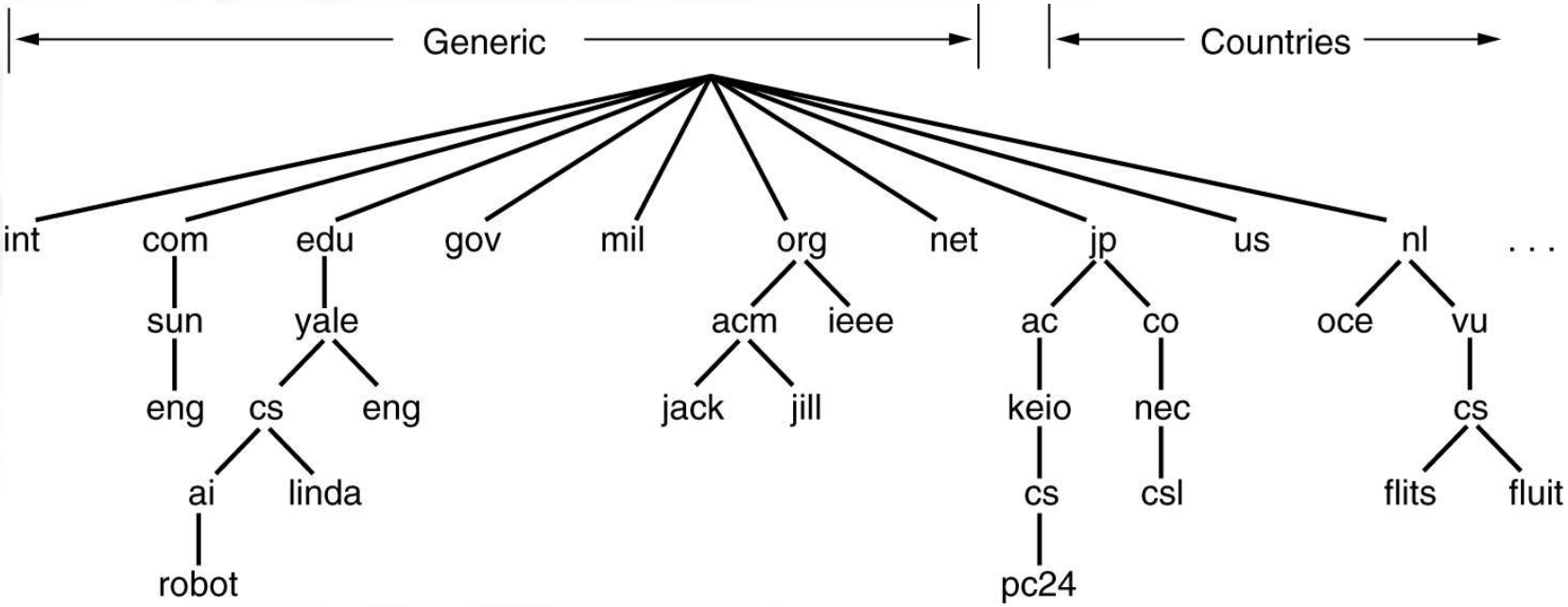
O Espaço de Nomes do DNS (cont.)

- O domínio de qualquer nó da árvore é a lista dos *labels*, começando por aquele nó, até a raiz, usando um ponto (".") como separador de *labels*.
- Cada domínio representa uma parte distinta do espaço de nomes e é mantido por uma (única) entidade administrativa.
  - Ex: inf.ufes.br amazon.com
    petrobras.com.br columbia.edu

O Espaço de Nomes do DNS (cont.)

- Debaixo da raiz estão os domínios denominados de "*top-level*" ou "*root-level*". Esses domínios são relativamente fixos.
- Por razões históricas, existem dois tipos de *top-level domain names*.
  - Nos EUA, os domínios top-level possuem usualmente 3 letras (EDU, NET, COM, etc).
  - Para domínios fora dos EUA, o código ISO de duas letras para países é usado.

O Espaço de Nomes DNS (cont.)



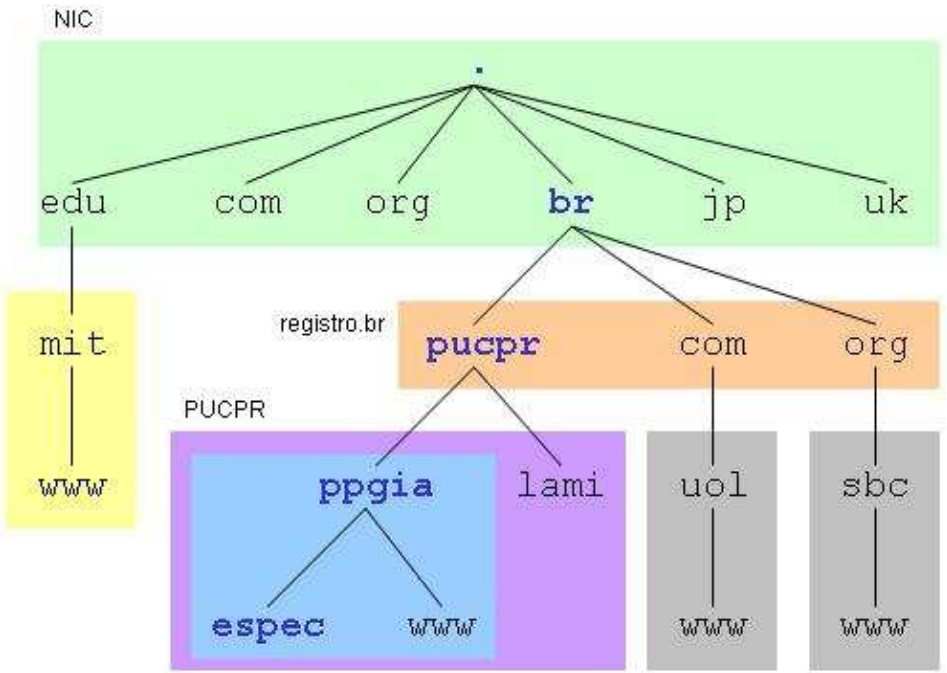
- EUA
  - EDU - instituições educacionais
  - COM - companhias comerciais
  - GOV - agências do governo
  - MIL - agências militares
  - NET - provedores de acesso à rede
  - ORG - organizações não governamentais
  - INT - organizações internacionais
- Restante do Mundo
  - BR - Brasil
  - PT - Portugal
  - FR - França
  - CA - Canadá
  - CH - Suíça
  - AU - Austrália

O Espaço de Nomes do DNS (cont.)

- Um nome de domínio que termina com um ponto é dito totalmente qualificado.
  - *FQDN – fully qualified domain name*
- Se o nome não termina com ponto, ele necessita ser completado pelo software que implementa o DNS.
  - camburi
  - camburi.lprm.inf.ufes.br.

O Espaço de Nomes do DNS (cont.)

- Cada parte da árvore de domínios pode ser gerenciada por uma organização diferente, de forma hierárquica.
- A responsabilidade pelos domínios brasileiros (nomes terminando em ".br") está a cargo do serviço Registro.BR, mantido pelo Comitê Gestor da Internet no Brasil (CGI.br).



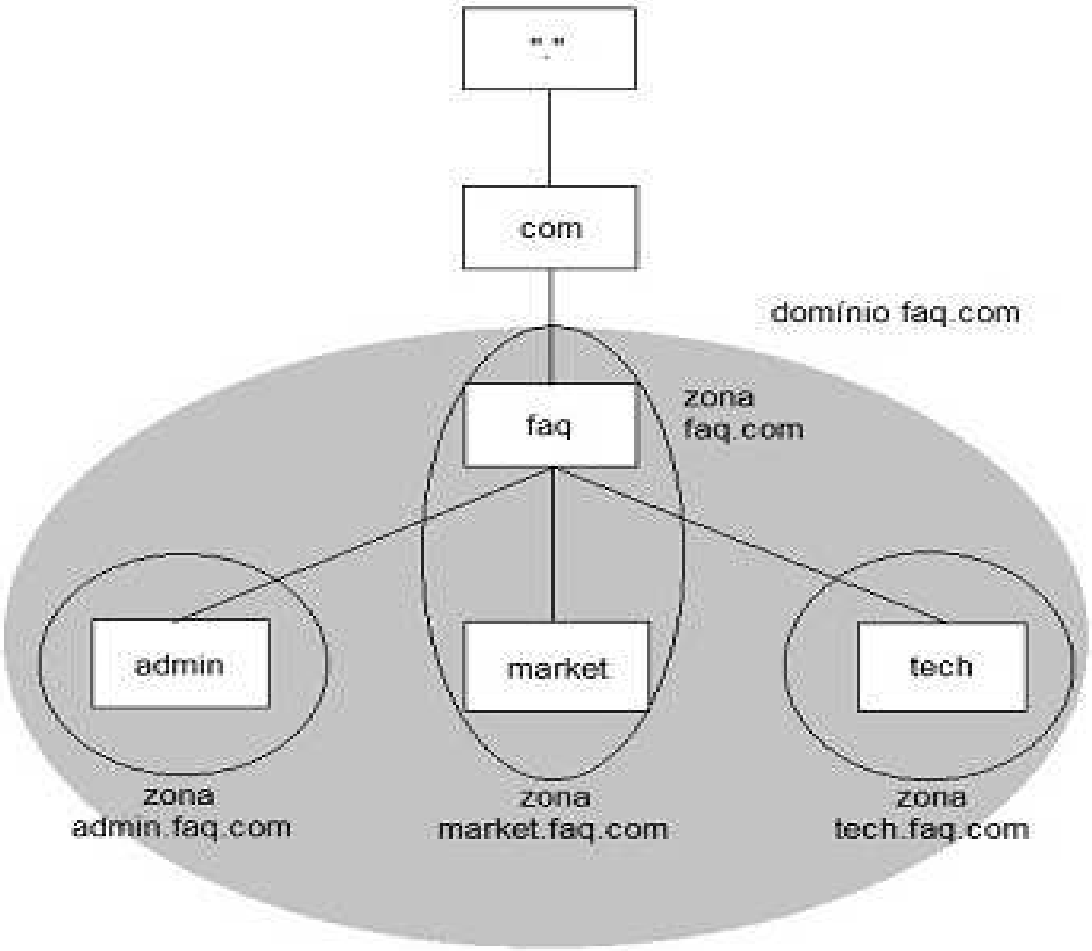
O DNS nas Organizações

- Pequena organização:
  - Pode ter o seu próprio servidor DNS ou então solicitar esse serviço do seu provedor Internet.
- Organização média, com várias sub-redes:
  - Deve ter servidores DNS em cada sub-rede para reduzir a carga da rede.
- Organização grande:
  - Deve dividir o seu domínio em sub-domínios e ter servidores para cada sub-domínio.

Zonas e Domínios

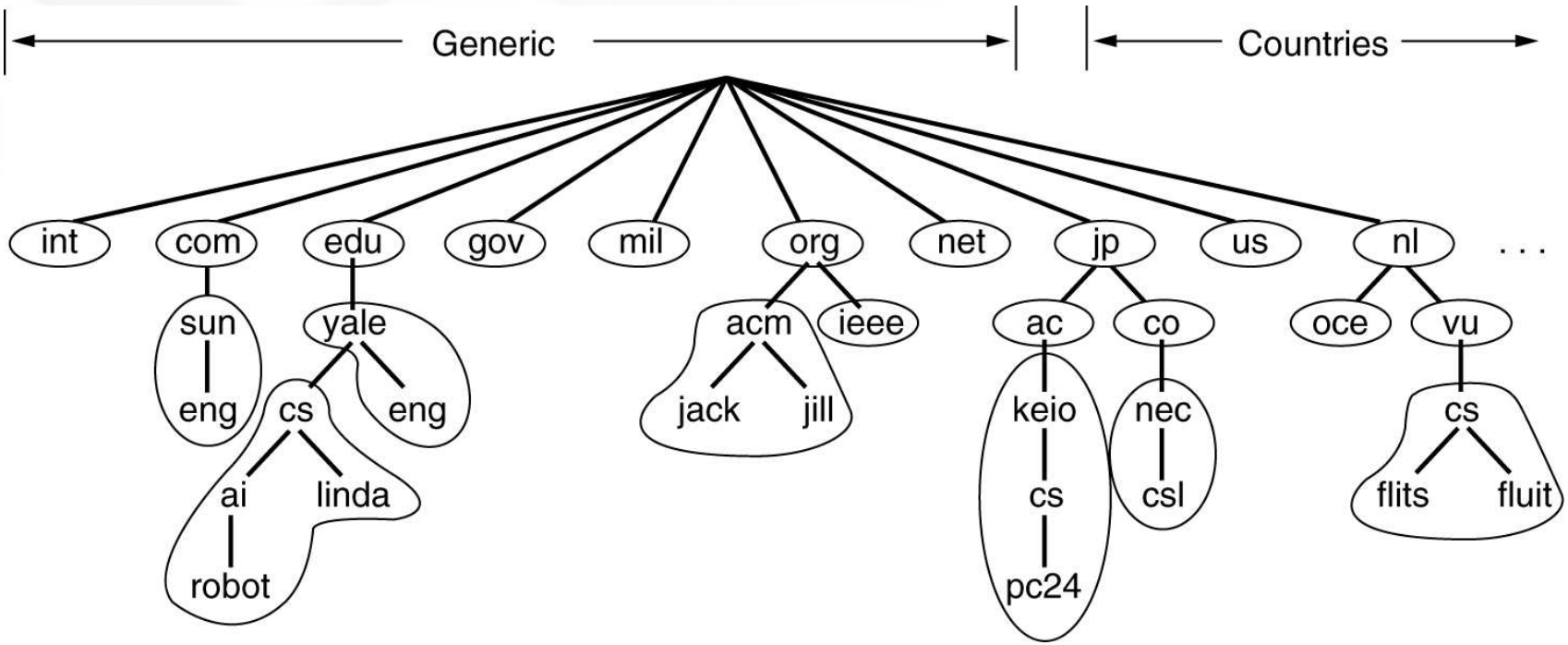
- Os nomes de domínios são chamados pelo DNS de “zonas”.
- Cada zona se relaciona com sua zona superior e registra nomes de máquinas e zero, uma ou mais zonas inferiores.
- Cada zona inferior deve ser registrada na zona superior.

Zonas e Domínios (cont.)



Zonas e Domínios (cont.)

- Um servidor pode ser responsável por mais de um domínio.



Tipos de Servidores

- Servidor Primário:
  - Mantém a cópia *master* dos dados do domínio em disco. Existe apenas um servidor de nomes primário para cada domínio ou subdomínio.
  - Deve estar localizado numa máquina estável, que não tenha muitos usuários, que seja relativamente segura e, preferencialmente, com fonte ininterrupta de energia.

Tipos de Servidores (cont.)

- Servidor Secundário:
  - Copia os dados do servidor primário através de uma operação chamada de "transferência de zona".
  - Pode haver vários servidores secundários para um domínio (tem que existir pelo menos um).
  - É recomendado existir pelo menos dois servidores secundários, um dos quais "*off-site*".
  - Secundários "*on-site*" devem ficar em diferentes redes e em diferentes circuitos de energia.

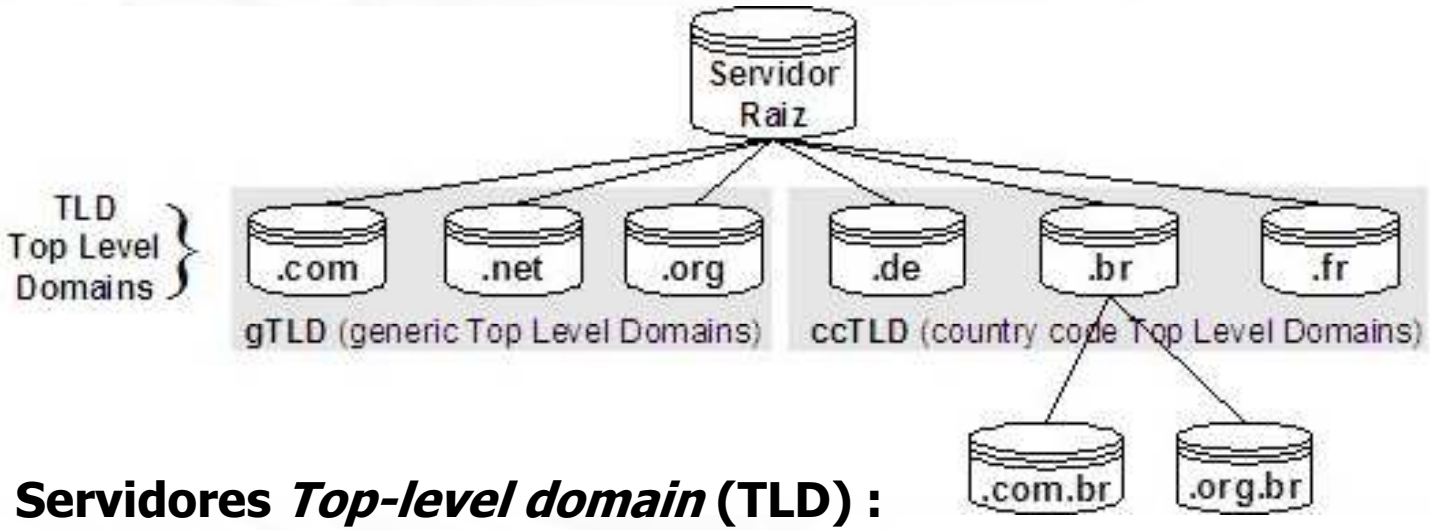
Tipos de Servidores (cont.)

- Servidor *caching-only*:
  - Carrega os endereços de um pequeno conjunto de máquinas importantes (servidores para o domínio *root*) a partir de um arquivo de *startup* e pega todo o resto dos seus dados via *caching* das respostas às consultas (*queries*) que ele resolve.
  - A maioria dos servidores primários e secundários também constroem os seus próprios *caches*.

Resumindo...

- Caching-only:
  - Possui somente dados derivados das últimas requisições + *root servers*
- Primário:
  - Servidor com autoridade sobre os dados de um domínio
- Secundário:
  - Servidor que possui autoridade sobre os dados de um domínio, mas os têm replicados, podendo atender uma requisição de um resolvedor.

TLD – Top Level Domain Servers



Servidores *Top-level domain* (TLD) :

- São os servidores DNS responsáveis por domínios como .org, .net, .com, .edu e pelos domínios de países, tais como: .br, .uk, .fr, .ca, .jp
- "Network Solutions" mantém os servidores para o domínio .com
- "NIC.br" (Registro.br) mantém servidores para o domínio .br

Servidores oficiais:

- São os servidores DNS das organizações, que provêem mapeamentos oficiais entre nomes de hosts e endereços IP da organização.
- Podem ser mantidos pelas organizações ou pelo provedor de acesso, por exemplo.

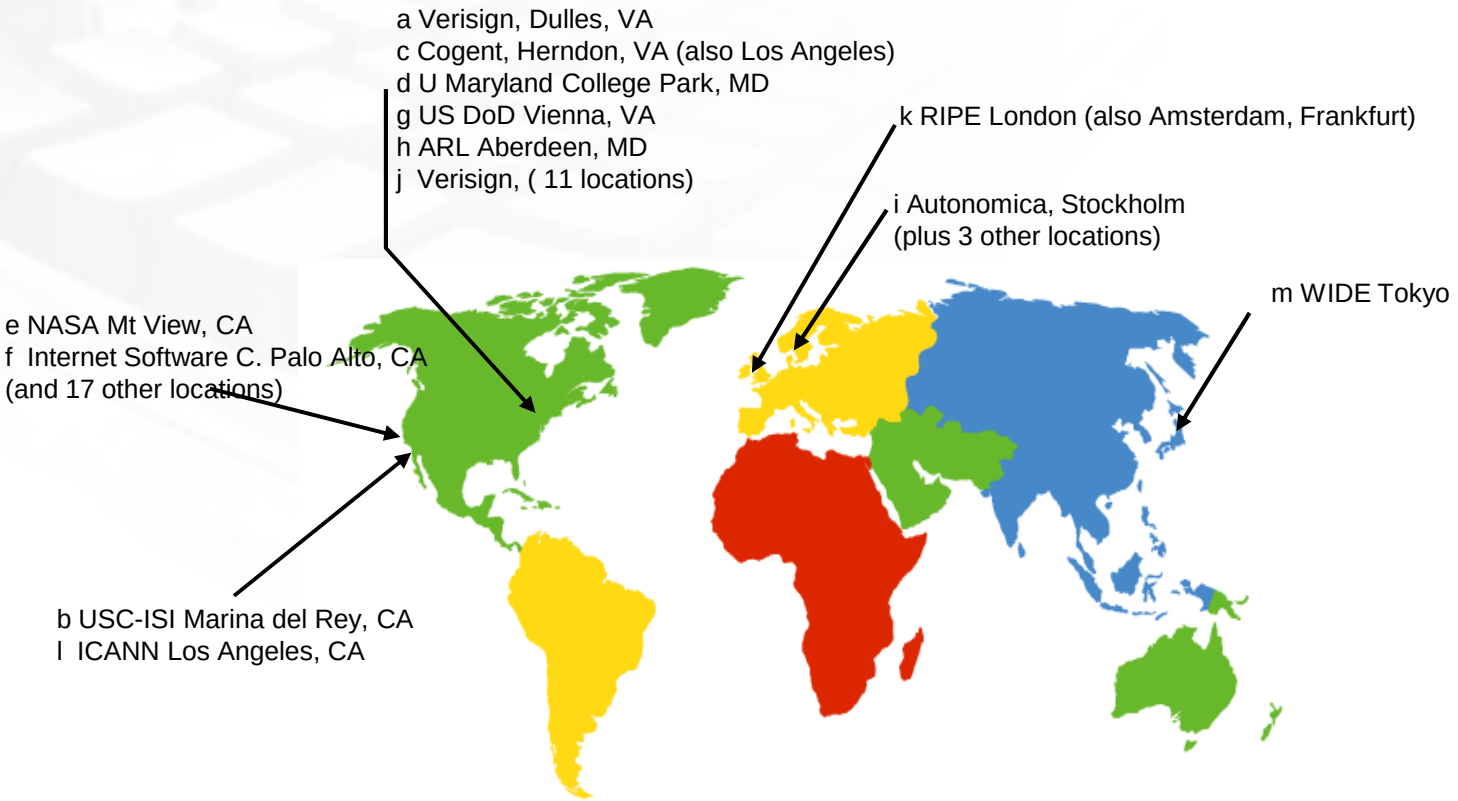
Root Name Servers

- Todo servidor DNS tem que saber, pelo menos, como contactar um dos "servidores raiz" (*root name servers*).
- Os *root servers*, por sua vez, sabem o nome e endereço IP de cada um dos servidores DNS autoritativos de cada domínio de segundo nível (.com, .edu, .br, .uk, etc.).
- O *root server* encaminha ao servidor solicitante os endereços de servidores autoritativos que podem resolver a consulta desejada (p. ex., quem são os servidores de nomes autoritativos do domínio .br).

Root Name Servers (cont.)

- Existem atualmente 13 *root name servers*, com nomes na forma *letter*.root-servers.net, onde *letter* varia de A a M.
- Isto não significa que existam apenas 13 servidores físicos; cada operador usa equipamento redundante para prover um serviço confiável mesmo na ocorrência de falha de hardware ou software.

Root Name Servers (cont.)



13 servidores de nome raiz em todo o mundo

Root Name Servers (cont.)

- Parte desses servidores operam em múltiplos locais, o que provê maior performance e tolerância a falhas.
  - Há agora servidores C, F, I, J, K, L e M localizados em diferentes continentes usando anúncios *anycast* para prover um serviço descentralizado.
- Como resultado, a maioria dos *root servers* estão hoje fora dos EUA, permitindo uma maior performance nas consultas.
- Uma relação atualizada pode ser obtida no site: *http://c.root-servers.org/*

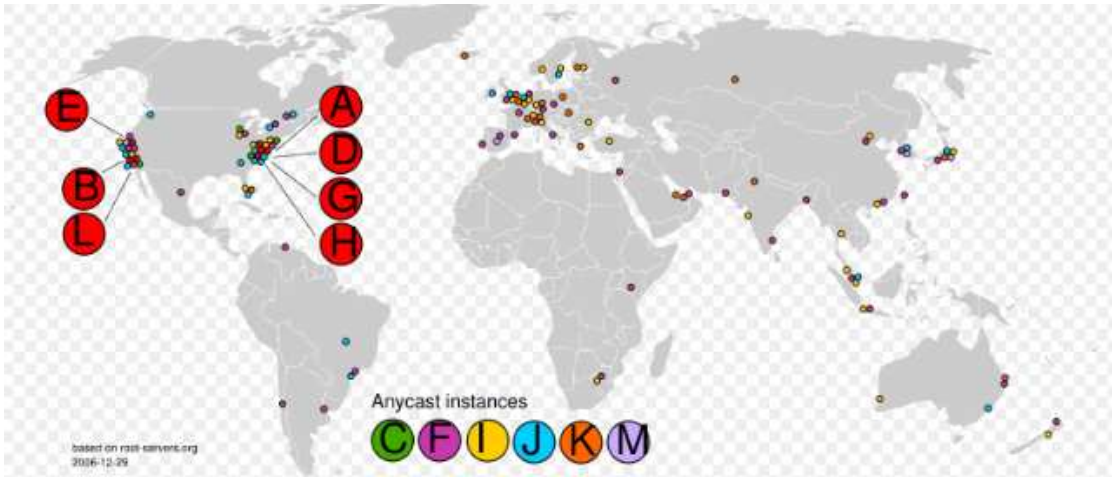
Root Name Servers (cont.)

Below is a map showing the locations of F-root nodes worldwide. Here is a list of their locations, and here are instructions for finding out which F-root is providing service to you.

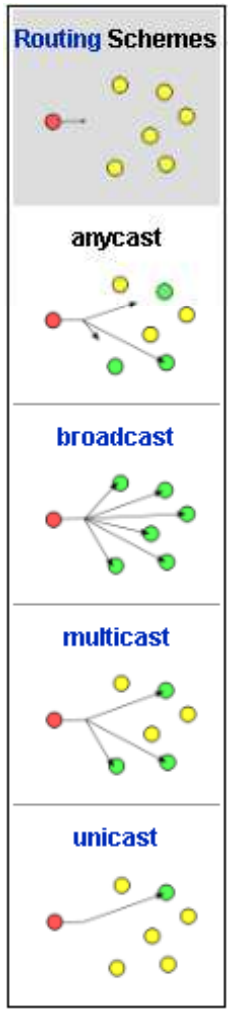
Root Name Servers (cont.)

Letter	IPv4 address	IPv6 address	Old name	Operator	Location	Software
A	198.41.0.4	2001:503:BA3E::2:30	ns.internic.net	VeriSign	distributed using anycast	BIND
B	192.228.79.201	2001:478:65::53	ns1.isi.edu	USC-ISI	Marina Del Rey, California, U.S.	BIND
C	192.33.4.12		c.psi.net	Cogent	ycast	BIND
D	128.8.10.90		terp.umd.edu	Univ	nd, U.S.	BIND
E	192.203.230.10		ns.nasa.gov	NASA	Mountain View, California, U.S.	BIND
F	192.5.5.241	2001:500:2f::f	ns.isc.org	Internet Systems Consortium	distributed using anycast	BIND 9[5]
G	192.112.36.4		ns.nic.ddn.mil	Defense Information Systems Agency	distributed using anycast	BIND
H	128.63.2.53	2001:500:1::803f:235	aos.arl.army.mil	U.S. Army Research Lab	Aberdeen Proving Ground, Maryland, U.S.	NSD
I	192.36.148.17	2001:7fe::53 (testing)	nic.nordu.net	Autonomica	distributed using anycast	BIND
J	192.58.128.30	2001:503:C27::2:30		VeriSign	distributed using anycast	BIND
K	193.0.14.129	2001:7fd::1		RIPE NCC	distributed using anycast	NSD[4]
L	199.7.83.42 (since November 2007; originally was 198.32.64.12)[5]	2001:500:3::42		ICANN	distributed using anycast	NSD[5]
M	202.12.27.33	2001:dc3::35		WIDE Project	distributed using anycast	BIND

Information Sciences Institute



- Endereçamento anycast: "one-to-one-of-many".



Número de Domínios Registrados por DPN (Domínio de Primeiro Nível) no Brasil

17/04/08

DPN	QUANTIDADE	%
Pessoas Físicas		
BLOG.BR	2450	0.19
FLOG.BR	184	0.01
NOM.BR	2714	0.21
SEC3.BR	17	0.00
VLOG.BR	97	0.01
WIKI.BR	311	0.02
	5773	**0.45**
Profissionais Liberais		
ADM.BR	1637	0.13
ADV.BR	9189	0.71
ARQ.BR	2109	0.16
ATO.BR	113	0.01
BIO.BR	351	0.03
BMD.BR	15	0.00
CIM.BR	677	0.05
CNG.BR	14	0.00
CNT.BR	1396	0.11
ECN.BR	132	0.01
ENG.BR	3691	0.29
ETI.BR	3175	0.25
FND.BR	47	0.00
FOT.BR	926	0.07
FST.BR	134	0.01
GGF.BR	18	0.00
JOR.BR	551	0.04
LEL.BR	104	0.01
MAT.BR	145	0.01
MED.BR	2748	0.21
MUS.BR	1247	0.10
NOT.BR	91	0.01
NTR.BR	89	0.01
ODO.BR	980	0.08
PPG.BR	895	0.07
PRO.BR	3095	0.24
PSC.BR	624	0.05
QSL.BR	69	0.01
SLG.BR	22	0.00
TRD.BR	132	0.01
VET.BR	344	0.03
ZLG.BR	4	0.00
	34764	**2.70**

DPN	QUANTIDADE	%
Pessoas Jurídicas		
AGR.BR	454	0.04
AM.BR	121	0.01
ART.BR	3748	0.29
COM.BR	1186411	92.01
COOP.BR	334	0.03
ESP.BR	596	0.05
ETC.BR	841	0.07
FAR.BR	208	0.02
FM.BR	227	0.02
G12.BR	601	0.05
GOV.BR	933	0.07
IMB.BR	763	0.06
IND.BR	7456	0.58
INF.BR	3165	0.25
JUS.BR	172	0.01
MIL.BR	28	0.00
NET.BR	1023	0.08
ORG.BR	32720	2.54
PSI.BR	240	0.02
REC.BR	97	0.01
SRV.BR	2706	0.21
TMP.BR	42	0.00
TUR.BR	3041	0.24
TV.BR	251	0.02
	1246178	**96.65**
Universidades		
BR	1196	0.09
EDU.BR	1523	0.12
	2719	**0.21**
Total	**1289434**	**100.00**
IDNA	**1232**	**0.10**
DNSSEC	**232**	**0.02**

Respostas Autoritativas e não-Autoritativas

- Uma "resposta autoritativa" de um servidor é garantida estar acurada (atualizada) enquanto que uma "resposta não-autoritativa" pode estar desatualizada.
- Existe um porcentual muito alto de respostas não-autoritativas que estão perfeitamente corretas.
- Servidores primários e secundários são autoritativos para os seus domínios mas não o são sobre informações a respeito de outros domínios mantidas em seus *caches*.

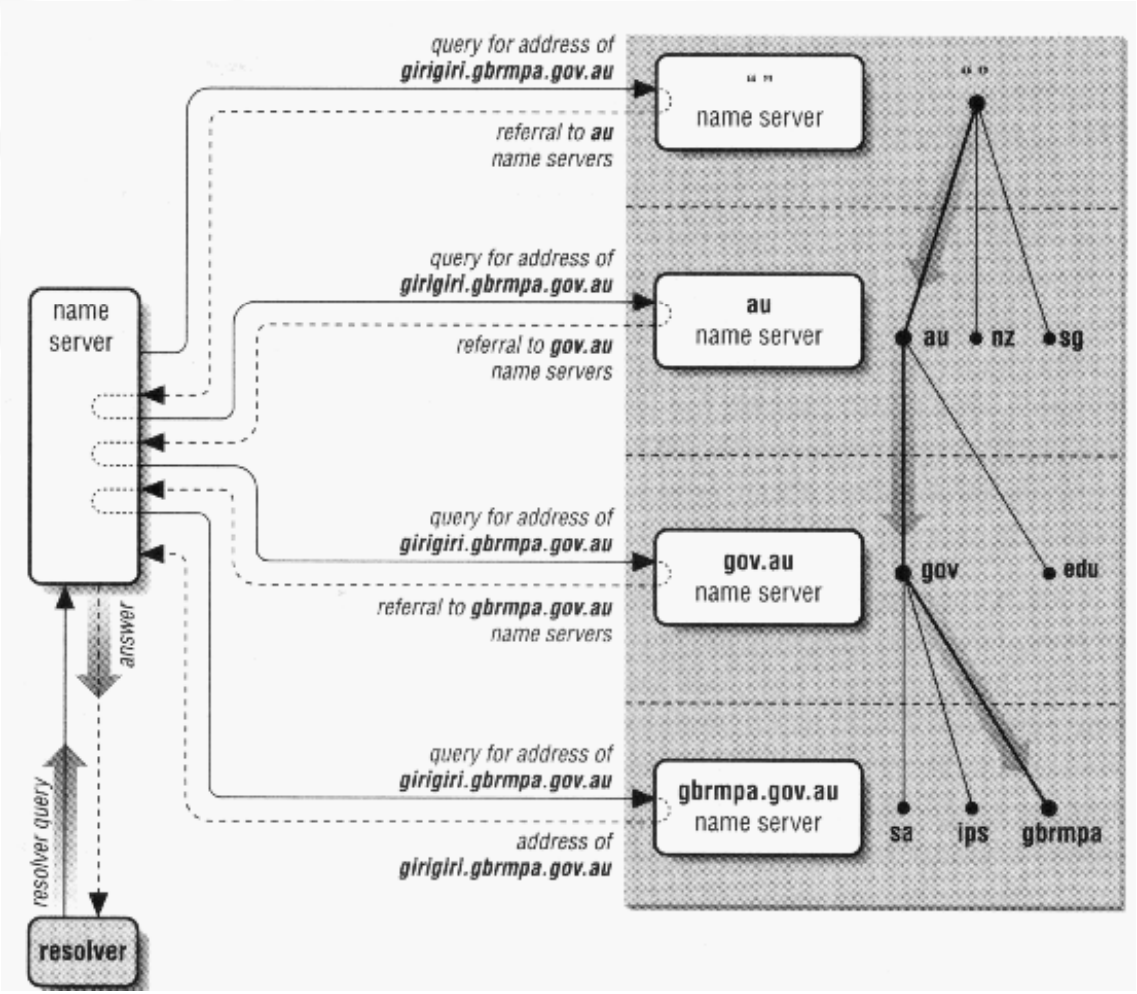
Respostas Autoritativas e não-Autoritativas (cont.)

- Servidores *caching-only* nunca são autoritativos; entretanto, podem reduzir a quantidade de tráfego DNS na rede.
- Constitui uma boa política colocar um servidor secundário ou *caching-only* em cada segmento de rede ou sub-rede.
- É perfeitamente admissível uma máquina ser servidora primária para um domínio e servidora secundária para outros domínios.

Servidor Interativo (não-Recursivo)

- É um servidor considerado com comportamento "*lazy*".
- Se ele tiver a resposta em seu *cache* proveniente de uma consulta anterior ou se ele é autoritativo para o domínio ao qual o nome consultado pertence, então ele retorna uma resposta apropriada; caso contrário, retorna uma referência a servidores autoritativos de um outro domínio que sejam mais prováveis de terem a resposta.
- O cliente de um servidor não-recursivo deve estar preparado para aceitar e saber agir ao receber as referências a outros servidores.

Servidor Interativo (não-Recursivo) (cont.)

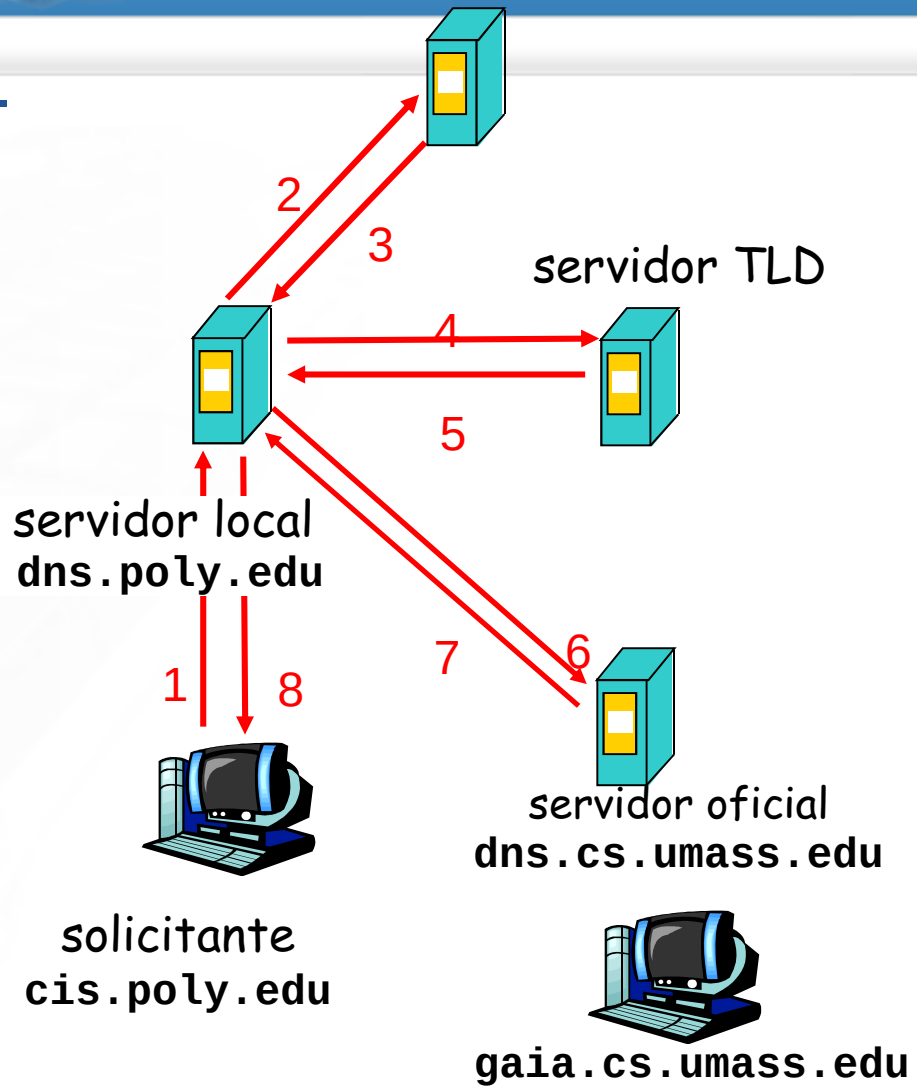


Servidor Interativo (não-Recursivo) (cont.)

- Hospedeiro em cis.poly.edu quer endereço IP para gaia.cs.umass.edu

consulta interativa:

- Servidor consultado responde com o nome de um servidor de contato
- "Não conheço este nome, mas pergunte para esse servidor"



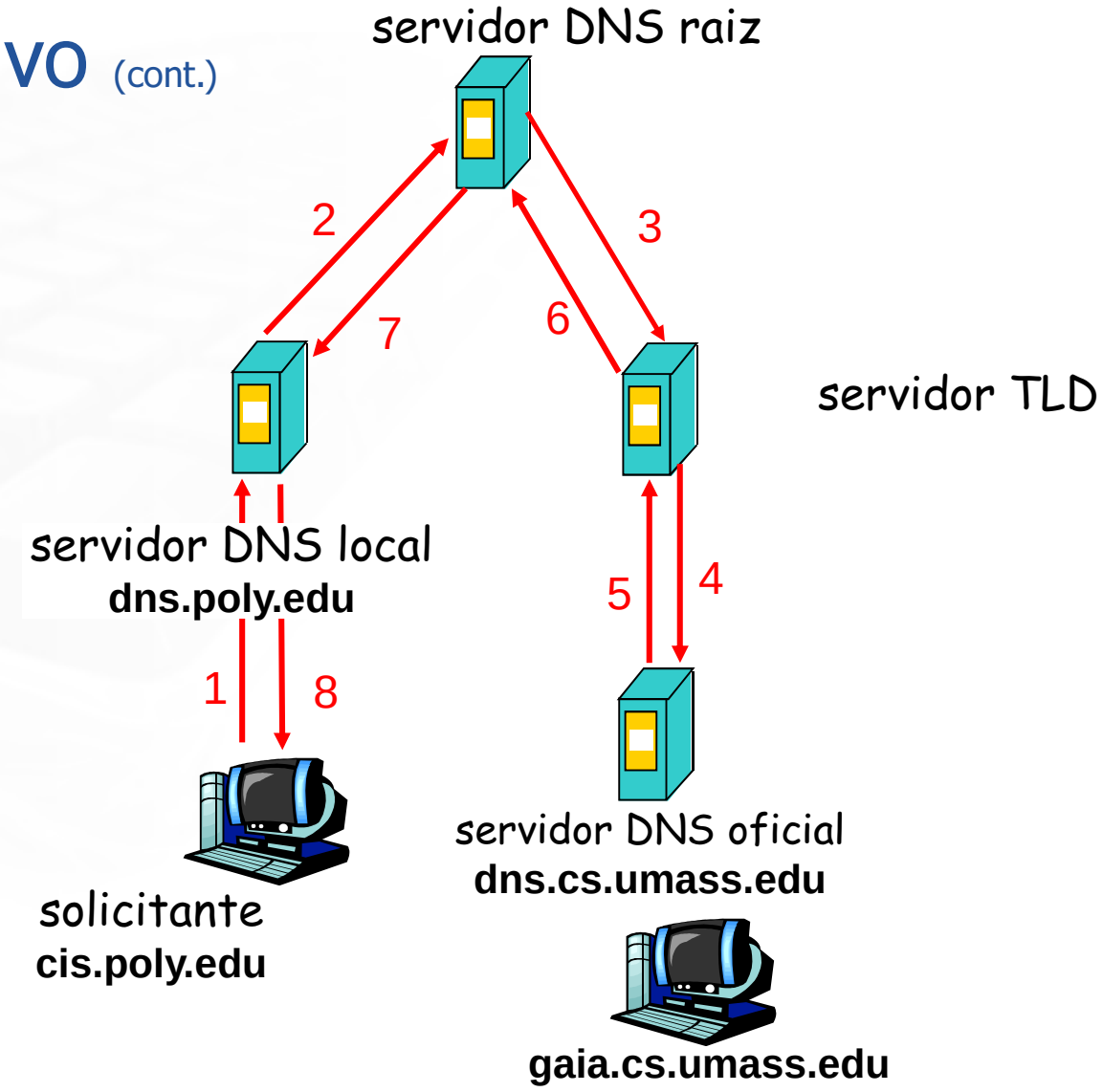
Servidor Recursivo

- Retorna somente respostas reais ou então mensagens de erro. Ele próprio segue as referências, liberando o cliente desta responsabilidade.
- O procedimento de resolver a consulta é o mesmo, o que muda é que o servidor recursivo contata ele próprio os outros servidores, ao invés de passar esta tarefa para o cliente.

Servidor Recursivo (cont.)

consulta recursiva:

- Transfere a responsabilidade de resolução do nome para o servidor de nomes contatado
- Carga pesada?



Servidores Recursivos x não-Recursivos

- Um efeito colateral de um servidor de nomes ter que seguir as referências é que seu *cache* adquire informação sobre domínios intermediários.
- Em uma LAN isso é interessante já que permite que consultas subsequentes de outros *hosts* se beneficiem do trabalho anterior do servidor.
- Já um servidor de um domínio *top-level*, como *com* ou *edu*, não deveria salvar informação requisitada por *hosts* de vários domínios abaixo, porque isso poderia encher o seu *cache* rapidamente.

Servidores Recursivos x não-Recursivos (cont.)

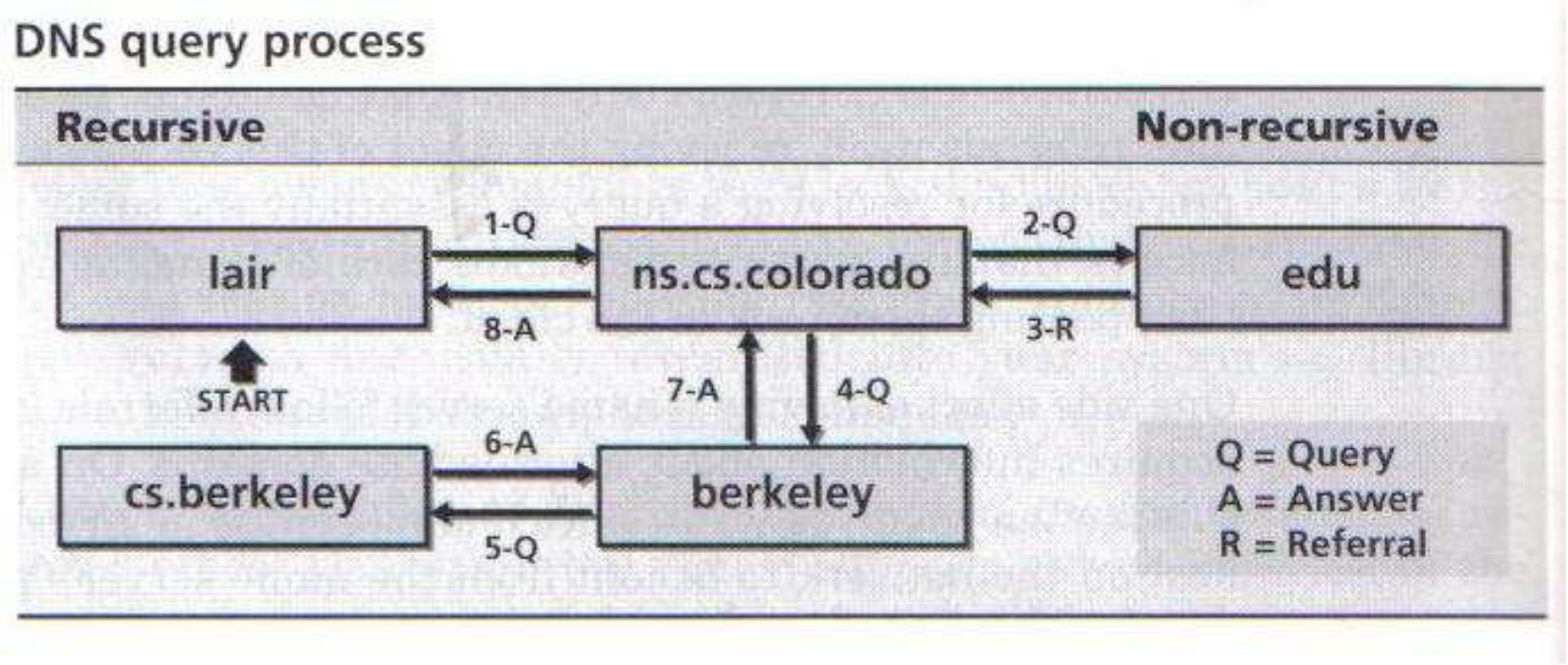
- Por esta razão, servidores de nível mais baixo na árvore de nomes são usualmente recursivos enquanto que servidores dos níveis mais altos (*top-level* ou de segundo nível) não devem sê-los.
- O lado cliente do DNS (*resolver*) que vem com a maioria das implementações Unix espera que o servidor de nomes local seja recursivo.
- Opções no BIND são providas para desligar a recursão (a partir da versão 4.9.3).

Caching

- Uma vez que um servidor qualquer aprende um mapeamento, ele o coloca num *cache* local.
  - Entradas na *cache* são sujeitas a temporização (desaparecem depois de um certo tempo)
  - Servidores TLD são tipicamente armazenados no *cache* dos servidores de nomes locais. Assim, servidores raiz acabam não sendo visitados com muita freqüência.
- Estão sendo projetados pela IETF mecanismos de atualização/notificação dos dados.
  - RFCs 2136, 3007, 4033/4/5
  - http://www.ietf.org/html.charters/dnsext-charter.html

Exemplo

- Ex: resolução do endereço mammoth.cs.berkeley.edu a partir da máquina lair.cs.colorado.edu.



Exemplo (cont.)

- Ao final da consulta:
  - ns.cs.colorado.edu tem em seu *cache* o endereço de mammoth.
  - ns.cs.colorado.edu tem em seu *cache* os endereços dos servidores de Berkeley.
  - Um servidor de Berkeley tem em seu *cache* o endereço de mamoth.

O Sistema BIND

- Escrito originalmente para o 4.3 BSD Unix, atualmente é mantido pelo Internet Software Consortium (http://www.isc.org/bind.html).
- O BIND apresenta três componentes principais:
  - *named*: *deamon* que executa as consultas. A máquina na qual ele executa é chamado de "*name server*".
  - *resolver*: rotinas de biblioteca que são usadas na resolução dos nomes. É o lado cliente do BIND.
  - *nslookup, dig* e *host*: interfaces orientadas a linhas de comando.
- Se *named* não souber a resposta é ele quem consulta outros servidores e coloca as respostas em *cache*. É ele também o responsável pela operação de "transferência de zona" (vide adiante).

A Biblioteca *Resolver*

- O serviço DNS é acessado pelos processos clientes através da biblioteca *resolver*. É através dela é que os programas que dependem da resolução de nomes requisitam operações de tradução de nomes em endereços IP e vice-versa.
- A biblioteca oferece diversas funções para resolução de nomes, das quais as mais utilizadas são: *gethostbyname()* e *gethostbyaddress().*

A Biblioteca *Resolver* (cont.)

- Na prática, a configuração do cliente se resume em definir o servidor de DNS que será usado para fazer a resolução de nomes e definir a ordem de consulta aos métodos de resolução de nomes.

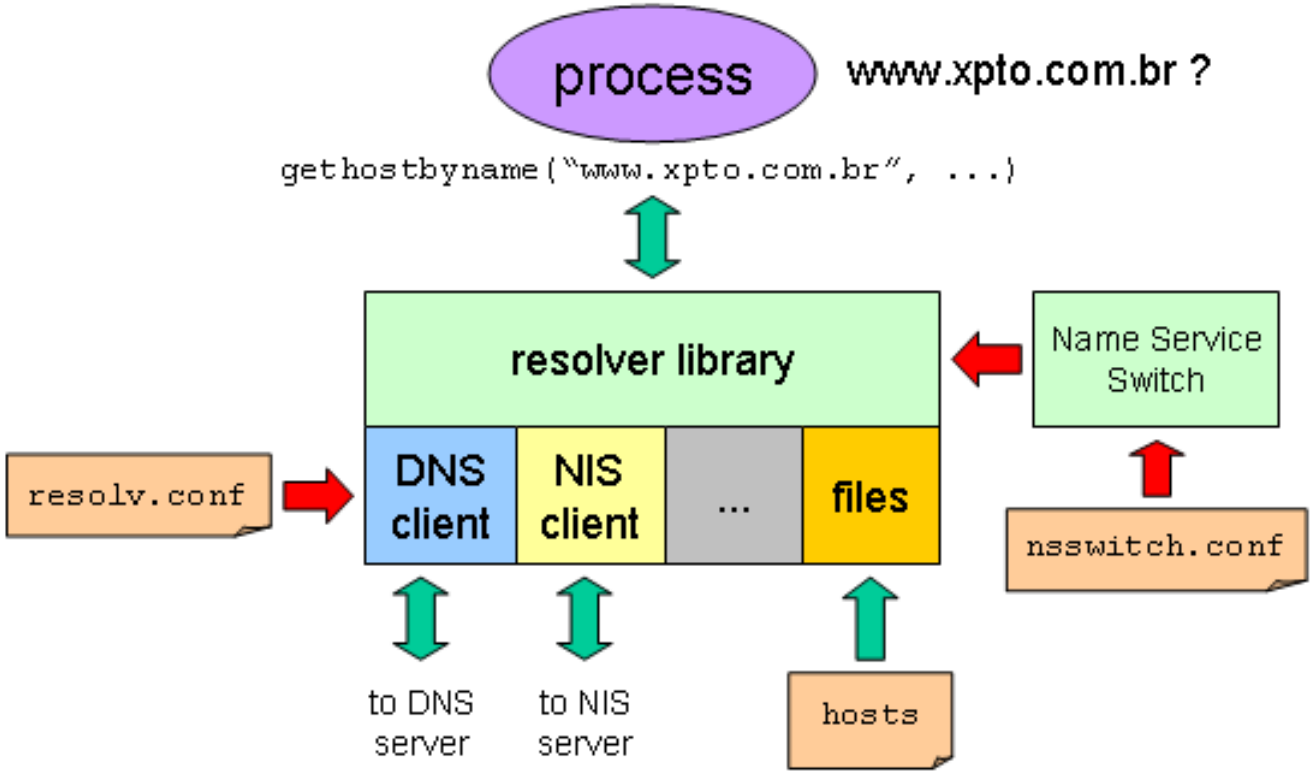
```
#cat /etc/resolv.conf
search sistemasabertos.com.br
nameserver 10.1.0.101
nameserver 10.1.0.102
```

- No UNIX, *resolver* é parte integrante do "release" de qualquer sistema. Utiliza (é preciso configurar) o arquivo */etc/resolv.conf*.

A Biblioteca Resolver (cont.)

- O *resolver* consulta a biblioteca NSS (*Name Service Switch*), que também faz parte da biblioteca Lib C, para determinar o mecanismo a ser utilizado para a resolução de um nome.
- A resolução de nomes pode fazer uso de diversos mecanismos, entre os quais os mais importantes são:
  - */etc/hosts:* arquivo do sistema local que contém uma tabela de números IP e nomes associados.
  - *DNS:* sistema de resolução de nomes da Internet.
  - *NIS: Network Information System*, um sistema criado pela Sun para difundir informações administrativas pela rede, como nomes de *hosts*, informações de usuários, etc.

A Biblioteca Resolver (cont.)



Name Server Switch

- O sistema NSS, criado inicialmente para o Solaris, permite definir a ordem de procura de serviços para a resolução de diversos tipos de nomes em um ambiente Unix.
- O arquivo Network Services Switch *(/etc/nsswitch.conf)* determina a ordem das buscas realizadas quando uma certa informação é requisitada. Exemplo:

```
passwd: files nis+ nis
shadow: files nis+ nis
group:  files nis+ nis
hosts:  files dns
ethers: files
services: files
```

- A linha "*hosts*" do exemplo indica que a resolução de nomes de computadores deverá ser feita inicialmente via arquivos locais (/etc/hosts) e depois, caso o nome não tenha sido encontrado, através do serviço DNS.

Configurando o Cliente DNS

- Deve-se configurar o arquivo *resolv.conf.* Este é o arquivo onde é indicado quem são os servidores de nome para as consultas de DNS.
- No arquivo, pode ainda ser utilizada a diretiva *search* ou *domain*, útil em consultas DNS onde é informado somente o nome do *host* ao invés do endereço completo (FQDN).
- Vários domínios podem ser adicionados, o que deve ser evitado, pois causará uma consulta DNS em cada um deles.

Configuração do Cliente DNS (cont.)

- Suponha o seguinte arquivo /etc/bind/resolv.conf:

```
(1) nameserver 200.200.20.1
(2) nameserver 200.200.30.15
(3) nameserver 148.100.1.20
(4) search  com.br  acme.com.br  com
```

- Linhas (1) – (3): lista de servidores de nomes que este cliente pode consultar, por ordem de prioridade. Podem ser especificados até três servidores.
- Linha (4): sufixos a serem adicionados pelo DNS a nomes não totalmente qualificados. Por exemplo, uma pesquisa por "obelix" pesquisará, na verdade, os seguintes nomes, nesta ordem:

  `obelix.com.br, obelix.acme.com.br e  obelix.com`
- Se for especificado o nome "obelix.com.br", sem ponto no final, serão pesquisados os seguintes nomes:

  `obelix.com.br.com.br, obelix.com.br.acme.com.br e obelix.com.br.com`

Configuração do Cliente DNS (cont.)

- Na inexistência do arquivo */etc/resolv.conf*, o comportamento normal é assumir que o servidor de nomes é o computador local e que o nome do domínio é obtido a partir do nome da máquina.
- Por exemplo, se o computador foi configurado com o nome "*obelix.unicamp.br*", o domínio é obtido a partir do resultado do comando:

```
% hostname
obelix.unicamp.br
```

Configuração do Cliente DNS (cont.)

- Configuração default
  - Não é usado o */etc/resolv.conf*
  - O servidor é o computador local
  - O domíno local é derivado de *hostname* ou *domainname*
- Configuração customizada
  - O arquivo /etc/resolv.conf é usado
  - *nameserver <ip1> <ip2> <ip3>*
  - *domainname <nomedom>*

Configuração do Servidor

- No Unix, os seguintes arquivos, no mínimo, devem ser configurados:
  - named.boot
  - named.ca
  - named.hosts
  - named.rev

Configuração do Servidor (cont.)

- Exemplo a ser usado
  - Empresa: NetRoad (provedor de acesso)
  - Domínio: netroad.com.br
  - Cliente único: empresa NetMasters
  - A NetRoad presta serviço de mestre secundário para a empresa NetWizards (netwizards.com.br)
  - Equipamentos:
    - Roteador com 16 portas assíncronas, servidor de nomes, servidor Web, servidor de FTP, servidor de Usenet News e seis microcomputadores usados pelos funcionários da empresa.

named.boot

- directory <path>
  - define que o diretório *path* conterá as demais tabelas do DNS
- primary <nomedom> <filename>
  - declara que o servidor local é primário para o domínio *nomedom* e os respectivos dados estão em *filename*
- secondary <nomedom> <listaddr> <arqdom>
  - declara que o servidor é secundário para o domínio *nomedom*. *listaddr* contém uma lista de endereços IP de, no mínimo, um servidor primário, no qual o servidor vai buscar os dados do domínio, que será armazenado no arquivo *arqdom*.

named.boot (cont.)

- cache . <filename>
  - nome do arquivo que contém os nomes e os endereços IP dos *root servers*.
- forwarders <listaddr>
  - listaddr contêm uma lista de endereços IP de servidores para os quais serão repassadas as requisições que não podem ser resolvidas localmente (que não se tem respostas autoritativas).
- slave
  - força o servidor para somente usar os servidores na lista do comando *forwarders*.

Exemplo: /etc/named.boot

```
; exemplo de named.boot
;
directory                                                    /var/named
primary        inf.ufes.br                                   named.db
primary        16.241.200.in-addr.arpa                       named.rev
primary        0.0.127.in-addr.arpa                          named.local
secondary      demac.ufu.br    200.19.153.2                  named.demac.hosts
secondary      153.19.200.in-addr.arpa   200.19.153.2        named.demac.rev
cache           .                                            named.ca
[forwarders]    ......
[slave]
```

Arquivo /etc/bind/named.boot do Servidor de Nomes da Empresa NetRoad

directory			/usr/local/named
primary	netroad.com.br		p/netroad.db
primary	netmasters.com.br		p/netmasters.db
primary	20.200.200.IN-ADDR.ARPA		p/200.200.20.0.db
secondary	netwizards.com.br	222.222.22.22	s/netwizards.db
secondary	21.200.200.IN-ADDR.ARPA	222.222.22.22	s/200.200.21.0.db
cache	.		named.root
primary	0.0.127.IN-ADDR.ARPA		127.0.0.db

A Base de Dados do DNS

- É um conjunto de arquivos texto mantido pelo administrador do sistema no servidor primário do domínio.
- Itens armazenados na base de dados são denominados *resource records* (RR).
- Os tipos e formato dos RR são definidos nas RFCs 882, 1035 e 1183.

Resource Records

- <nome> <ttl> IN <tipo> <dados>
  - nome: nome do objeto
  - ttl: tempo em segundos que a informação deve permanecer no cache
  - IN: Internet DNS resource record
  - tipo: tipo do registro
  - dados: informação específica ao tipo do registro

Resource Records (cont.)

- Start of Authority (SOA)
- Name Server (NS)
- Address (A)
- Pointer (PTR)
- Mail Exchange (MX)
- Canonical Name (CNAME)
- Host Information (HINFO)
- Well Known Service (WKS)

SOA (Start Of Authority)

```
<zone> [ttl] IN SOA <origin> <contact> {
                    serial
                    refresh
                    retry
                    expire
                    minimum }
```

- Marca o início de uma zona.
- Existe apenas um registro SOA para cada zona.

SOA (Start Of Authority) (cont.)

- *zone*: o nome da zona. O "@" referencia o domínio definido em *named.boot*.
- *origin*: nome (FQDN) do servidor primário para o domínio.
- *contact* : e-mail do gerente do domínio.
- *serial*: número seqüencial usado indicar a necessidade da atualização dos dados nos servidores secundários.
- *refresh*: tempo em segundos que o servidor secundário vai esperar para testar se precisa atualizar os dados (1 a 6 horas).

SOA (Start Of Authority) (cont.)

- *retry*: tempo em segundos que determina o intervalo de nova tentativa de um pedido de *refresh* não respondido por um servidor primário (20-60 minutos).
- *expire*: tempo em segundos que o servidor secundário poderá ficar com os dados sem um *refresh*.
- *minimum*: tempo em segundos que os registros podem ficar no *cache* de outro servidor.

Exemplo

```
netroad.com.br. IN SOA  ns.netroad.com.br.  dnsmaster.netroad.com.br. (
                        1998122103      ; Serial
                        10800           ; Refresh
                        1800            ; Retry
                        3600000         ; Expire
                        259200 )        ; Minimum
```

NS (Name Server)

- Define o(s) servidor(es) de nomes do domínio.
- Permite delegar de autoridade para sub-domínios de níveis inferiores (em outras palavras, permite definir/alterar a hierarquia de domínios).

```
<domain> [ttl] IN NS <server>
```

Onde:

domain: nome do domínio
ttl: time to live (opcional)
server: endereço da máquina servidora

NS (Name Server) (cont.)

NS (Name Server) (cont.)

```
; Definição dos servidores primário e secundário do domínio NetRoad.com.BR
;
netroad.com.br.          10800 IN NS    ns.netroad.com.br.
ns.netroad.com.br.       10800 IN A     200.200.20.1
netroad.com.br.          10800 IN NS    ns.netwizards.com.br.
```

- Obs: foi necessária a introdução de um Registro Cola (“A”) para servidor *ns.netroad.com.br.*, visto que este servidor de DNS se encontra dentro do próprio domínio *netroad.com.br*.

Delegação de Autoridade

- Suponhamos que seja feito o registro do domínio *exemplo.com.br*. na entidade responsável pela administração de nomes de domínio no Brasil, que é o Registro.br (www.registro.br).
  - OBS: O NIC.br (Núcleo de Informação e Coordenação do Ponto BR) é o braço executivo do CGI.br (Comitê Gestor da Internet no Brasil). Entre outras funções, o NIC.br responde pelo Registro.br.
- Durante o processo de registro de domínios, é necessário indicar para a entidade registradora no mínimo dois servidores DNS que estejam respondendo pelo domínio *exemplo.com.br.*
- Isto é feito inserindo registros do tipo NS nos servidores raiz do domínio BR, de modo a apontar para este novo domínio.

Delegação de Autoridade (cont.)

- Supondo que os servidores DNS do domínio *exemplo.com.br* sejam *ns1.exemplo.com.br* e *ns2.exemplo.com.br*, os registros inseridos nos servidores raiz do domínio com.BR teriam a seguinte forma:

exemplo.com.br.	IN NS	ns1.exemplo.com.br.
ns1.exemplo.com.br.	IN A	200.137.66.1
exemplo.com.br.	IN NS	ns2.exemplo.com.br.
ns2.exemplo.com.br.	IN A	200.137.66.2

Delegação de Autoridade (cont.)

- Supondo agora que o domínio *exemplo.com.br* tenha representações em todas as capitais do Brasil e cada um destes subdomínios se inicia pelo nome da capital onde está sediado, o administrador do serviço DNS do domínio *exemplo.com.br* poderá realizar a delegação de autoridade para os domínios regionais:

```
espiritosanto.exemplo.com.br.   IN NS   ns.vitoria.exemplo.com.br.
pernambuco.exemplo.com.br.      IN NS   ns.recife.exemplo.com.br.
ceara.exemplo.com.br.           IN NS   ns.fortaleza.exemplo.com.br.
maranhao.exemplo.com.br.        IN NS   ns.saoluis.exemplo.com.br.
rio.exemplo.com.br.             IN NS   ns.rio.exemplo.com.br.
minas.exemplo.com.br.           IN NS   ns.bh.exemplo.com.br.
```

Registro.Br e os *Root Servers*

- O DNS direto de uma organização começa na entidade onde ela registrou os seus domínios (registro.br, para domínios registrados no Brasil).
- Nesse registro, deve ser informado quais são os servidores de DNS da organização que respondem pelos nomes no seu domínio, e o registro.br enviará essa informação para os *root servers*.
- A partir daí, qualquer um no mundo pode acessar os domínios da organização.

A (Address Record)

- Usado para converter um nome de *host* em um endereço IP.

```
<host> [ttl] IN A <addr>
```

Onde:

host: nome do *host*, geralmente é relativo ao domínio corrente.
ttl: time to live (optional).
addr: endereço IP do *host*.

A (Address Record) (cont.)

vancouver.inf.ufes.br.	IN	A	200.137.66.5
parati.inf.ufes.br.	IN	A	200.137.66.6
camburi.inf.ufes.br.	IN	A	200.137.66.7

; Definição dos microcomputadores de trabalho de **NetRoad.com.BR**
;

pc01.netroad.com.br.	10800 IN A	200.200.20.3	
pc02.netroad.com.br.	10800 IN A	200.200.20.4	
pc03.netroad.com.br.	10800 IN A	200.200.20.5	
pc04.netroad.com.br.	10800 IN A	200.200.20.6	
pc05.netroad.com.br.	10800 IN A	200.200.20.7	
pc06.netroad.com.br.	10800 IN A	200.200.20.8	

MX (Mail eXchanger)

- Usado para o direcionamento de correio eletrônico.

```
<name> [ttl] IN MX <precedence> <host>
```

Onde:

- *name*: nome do domínio para o qual o e-mail é direcionado (*relaying*).
- *precedence*: fator usado para definir a ordem na qual os servidores de *mail* são tentados.
- *host*: o nome do servidor de *mail*.

```
; Definição dos Servidores de Email Primário e Secundário de NetRoad.br
;
netroad.com.br.     10800 IN MX 10     mail.netroad.com.br.
netroad.com.br.     10800 IN MX 20     mail.netwizards.com.br.
```

CNAME (Canonical Name)

- Permite definir um apelido (*alias*) para um nome de *host*.

```
<nickname> [ttl] IN CNAME <hostname>
```

onde:

nickname: apelido

hostname: nome já definido para o *host*

CNAME (Canonical Name) (cont.)

www.inf.ufes.br. CNAME camburi.inf.ufes.br.

Apelido

Tradução do apelido

```
; Definição dos servidores Web, FTP e News de NetRoad.br
;
www.netroad.com.br.    10800 IN CNAME    ns.netroad.com.br.
ftp.netroad.com.br.    10800 IN CNAME    ns.netroad.com.br.
news.netroad.com.br.   10800 IN A        200.200.20.2
```

Arquivo netroad.db de NetRoad.br

```
netroad.com.br. IN SOA ns.netroad.com.br. dnsmaster.netroad.com.br. (
                       1998122103  ; Serial
                       10800       ; Refresh
                       1800        ; Retry
                       3600000     ; Expire
                       259200 )    ; Minimum
;
; Definição dos Servidores Primário e Secundário do Domínio NetRoad.com.BR
;
netroad.com.br.         10800 IN NS             ns.netroad.com.br.
ns.netroad.com.br.      10800 IN A              200.200.20.1
netroad.com.br.         10800 IN NS             ns.netwizards.com.br.
;
; Definição dos Servidores de Email Primário e Secundário
;
netroad.com.br.         10800 IN MX 10          mail.netroad.com.br.
netroad.com.br.         10800 IN MX 20          mail.netwizards.com.br.
;
; Definição dos servidores Web, FTP, News
;
www.netroad.com.br.     10800 IN CNAME          ns.netroad.com.br.
ftp.netroad.com.br.     10800 IN CNAME          ns.netroad.com.br.
news.netroad.com.br.    10800 IN A              200.200.20.2
;
; Definição dos microcomputadores de trabalho do provedor
;
pc01.netroad.com.br.    10800 IN A  200.200.20.3
pc02.netroad.com.br.    10800 IN A  200.200.20.4
pc03.netroad.com.br.    10800 IN A  200.200.20.5
pc04.netroad.com.br.    10800 IN A  200.200.20.6
pc05.netroad.com.br.    10800 IN A  200.200.20.7
pc06.netroad.com.br.    10800 IN A  200.200.20.8
;
; Definição do Roteador e de suas oito portas assíncronas
;
async01.netroad.com.br. 10800 IN A  200.200.20.65
async02.netroad.com.br. 10800 IN A  200.200.20.66
async03.netroad.com.br. 10800 IN A  200.200.20.67
async04.netroad.com.br. 10800 IN A  200.200.20.68
async05.netroad.com.br. 10800 IN A  200.200.20.69
async06.netroad.com.br. 10800 IN A  200.200.20.70
async07.netroad.com.br. 10800 IN A  200.200.20.71
async08.netroad.com.br. 10800 IN A  200.200.20.72
```

DNS Reverso

- O DNS reverso resolve um endereço IP para um nome de *host*, por exemplo: 200.137.66.134 para ns1.inf.ufes.br.
- O DNS reverso funciona de forma parecida ao DNS direto: ele começa no seu provedor de acesso (ou com quem quer que lhe diga qual é o seu endereço IP).
- Você deve informar ao seu "provedor" quais servidores de DNS respondem pelos apontamentos de DNS reverso para os seus IPs (ou, o seu "provedor" pode configurar esses apontamentos em seus próprios servidores de DNS).

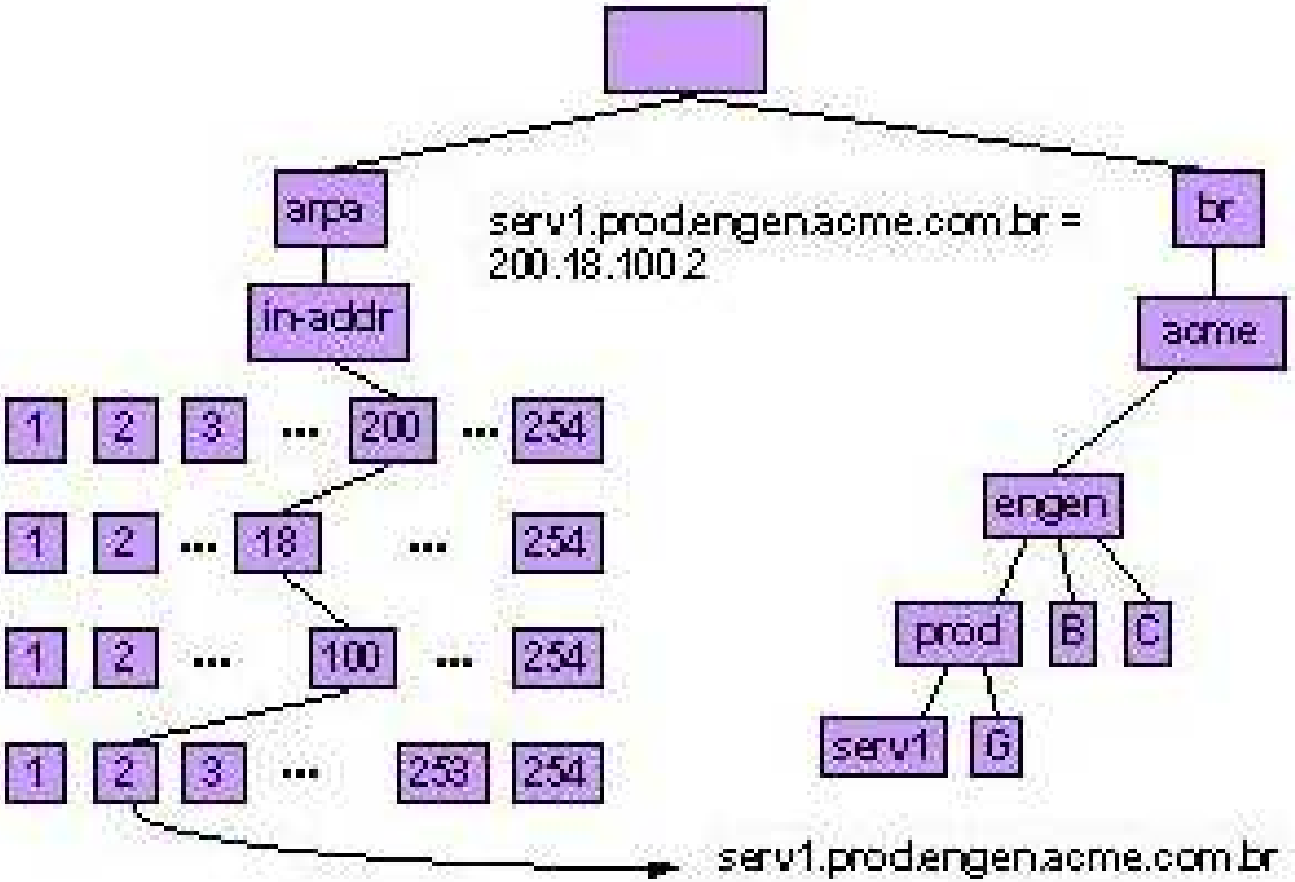
DNS Reverso (cont.)

- O seu "provedor" passará então esta informação adiante quando os servidores de DNS deles forem consultados sobre os seus apontamentos de DNS reverso.
- A partir daí, qualquer um no mundo pode consultar os apontamentos de DNS reverso dos seus IPs, e você pode responder com qualquer nome que quiser (tendo ou não controle sobre os domínios desses nomes, embora você não deva apontá-los para nomes que não são dos seus domínios, sem permissão).
- Se o seu "provedor" não sabe que você tem servidores de DNS para responder pelo DNS reverso dos seus IPs, ele não vai propagar essa informação para os *root servers*, e ninguém vai nem mesmo chegar aos seus servidores de DNS para consultar o DNS reverso.

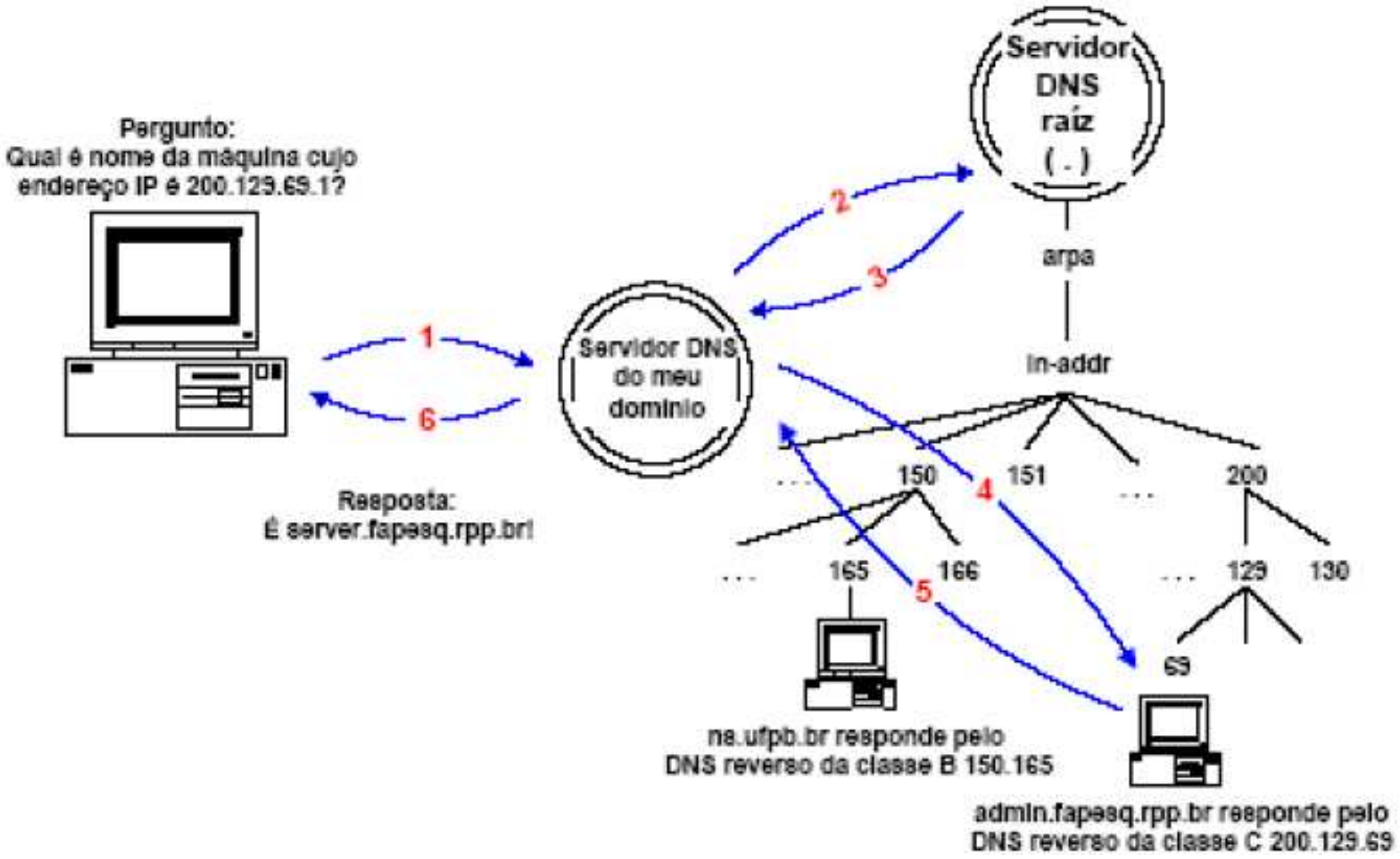
DNS Reverso (cont.)

```
0.20.200.200.IN-ADDR.ARPA. IN SOA ns.netroad.com.br. dnsmaster.netroad.com.br. (
                        1998122103  ; Serial
                        10800       ; Refresh
                        1800        ; Retry
                        3600000     ; Expire
                        259200 )    ; Minimum
;
; Definição dos Servidores Primário e Secundário do Domínio NetRoad.com.BR
;
netroad.com.br.                     10800 IN NS             ns.netroad.com.br.
ns.netroad.com.br.                  10800 IN A              200.200.20.1
netroad.com.br.                     10800 IN NS             ns.netwizards.com.br.
;
; Definição dos microcomputadores de trabalho do provedor
;
3.20.200.200.IN-ADDR.ARPA.          10800 IN PTR            pc01.netroad.com.br.
4.20.200.200.IN-ADDR.ARPA.          10800 IN PTR            pc02.netroad.com.br.
5.20.200.200.IN-ADDR.ARPA.          10800 IN PTR            pc03.netroad.com.br.
6.20.200.200.IN-ADDR.ARPA.          10800 IN PTR            pc04.netroad.com.br.
7.20.200.200.IN-ADDR.ARPA.          10800 IN PTR            pc05.netroad.com.br.
8.20.200.200.IN-ADDR.ARPA.          10800 IN PTR            pc06.netroad.com.br.
;
; Definição do Roteador e de suas oito portas assíncronas
;
65.20.200.200.IN-ADDR.ARPA.         10800 IN PTR            async01.netroad.com.br.
66.20.200.200.IN-ADDR.ARPA.         10800 IN PTR            async02.netroad.com.br.
67.20.200.200.IN-ADDR.ARPA.         10800 IN PTR            async03.netroad.com.br.
68.20.200.200.IN-ADDR.ARPA.         10800 IN PTR            async04.netroad.com.br.
69.20.200.200.IN-ADDR.ARPA.         10800 IN PTR            async05.netroad.com.br.
70.20.200.200.IN-ADDR.ARPA.         10800 IN PTR            async06.netroad.com.br.
71.20.200.200.IN-ADDR.ARPA.         10800 IN PTR            async07.netroad.com.br.
72.20.200.200.IN-ADDR.ARPA.         10800 IN PTR            async08.netroad.com.br.
```

DNS Reverso (cont.)



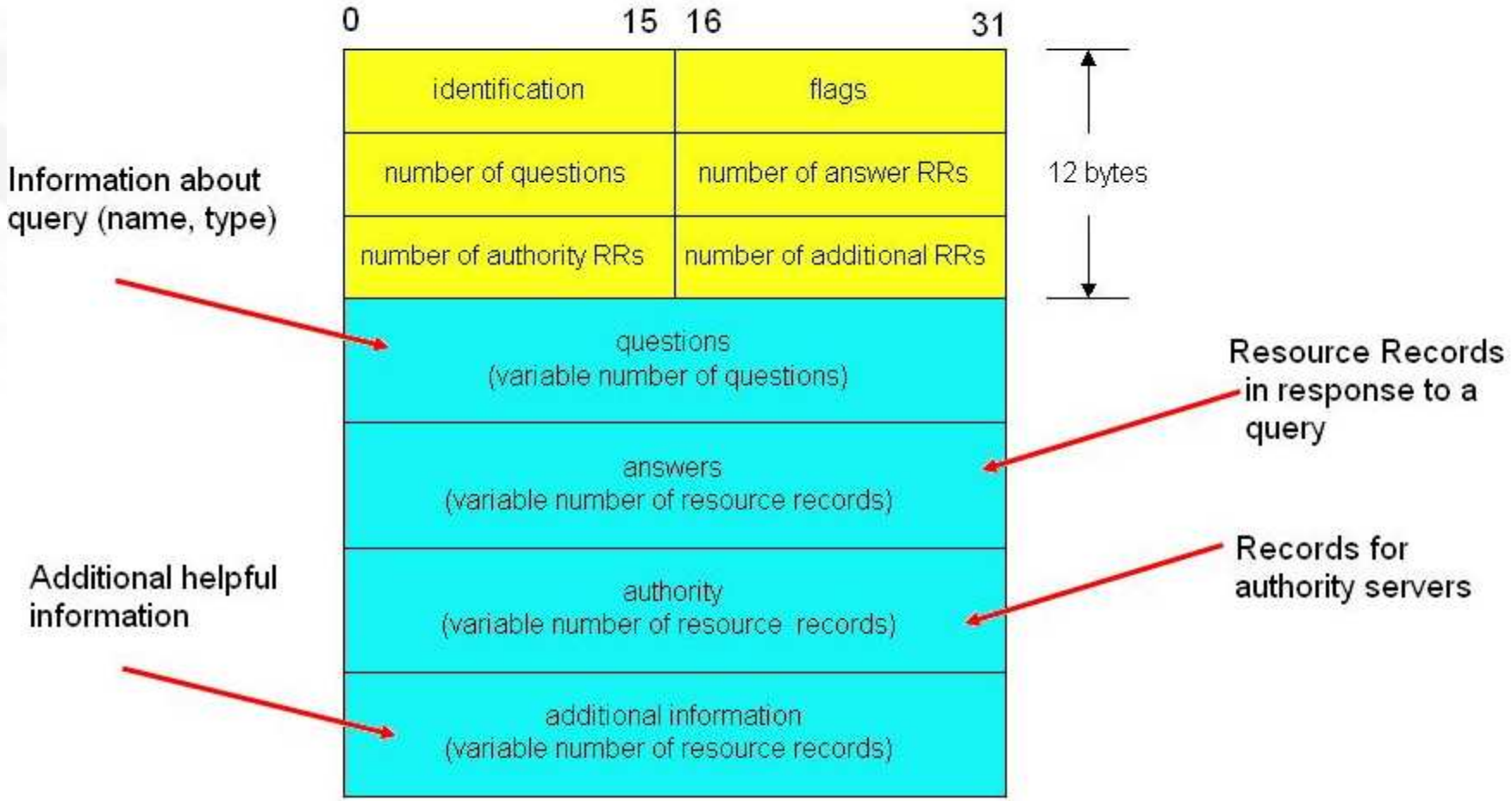
DNS Reverso (cont.)



Exemplo: Resolver 200.176.3.142

- O *resolver* de DNS inverte o IP e adiciona ".in-addr.arpa" no final, transformando 200.176.3.142 em 142.3.176.200.in-addr.arpa. O *resolver* então consulta os *root servers* pelo registro PTR para 142.3.176.200.in-addr.arpa. O
- Os *root servers* encaminham a consulta para os servidores de DNS encarregados da faixa 200.in-addr.arpa, que cobre todos os IP's que começam com 200.
- Em quase todos os casos, os *root servers* irão encaminhar o *resolver* de DNS para um "RIR" ("Registro de Internet Regional"). Estas são as organizações que distribuem os IP's. Usualmente, LACNIC controla os IP's da América Latina e Caribe, ARIN controla os IP's da América do Norte, APNIC controla os IP's da Ásia e do Pacífico, e RIPE controla os IP's da Europa.
- O *resolver* de DNS irá perguntar aos servidores de DNS do "RIR" indicado pelos *root servers* pelo registro PTR do 142.3.176.200.in-addr.arpa.
- Dependendo do "RIR", a resposta pode ser um encaminhamento direto para a entidade que recebeu o range de IP's (como faz a ARIN) ou, como no nosso caso, um encaminhamento para uma organização nacional que controla os IP's no país dentro da região de abrangência do "RIR". Por exemplo, a LACNIC responderia que os servidores de DNS encarregados da faixa 176.200.in-addr.arpa são os do registro.br, que controla a distribuição de IP's no Brasil. Nesse segundo caso, o *resolver* de DNS irá perguntar agora para os servidores do registro.br pelo registro PTR do 142.3.176.200.in-addr.arpa.
- Os servidores de DNS do registro.br vão encaminhar o resolver de DNS para a entidade que recebeu o range de IP's. Estes são, normalmente os servidores de DNS do seu provedor de acesso ou de meio físico.
- O resolver de DNS irá perguntar aos servidores de DNS do provedor pelo registro PTR do 142.3.176.200.in-addr.arpa.
- Os servidores de DNS do provedor vão encaminhar o *resolver* de DNS para os servidores de DNS da organização que de fato está usando o IP.
- O resolver de DNS irá perguntar aos servidores de DNS da organização pelo registro PTR do 142.3.176.200.in-addr.arpa.
- Finalmente, os servidores de DNS da organização irão responder com "exemplo.hipotetico.com.br".

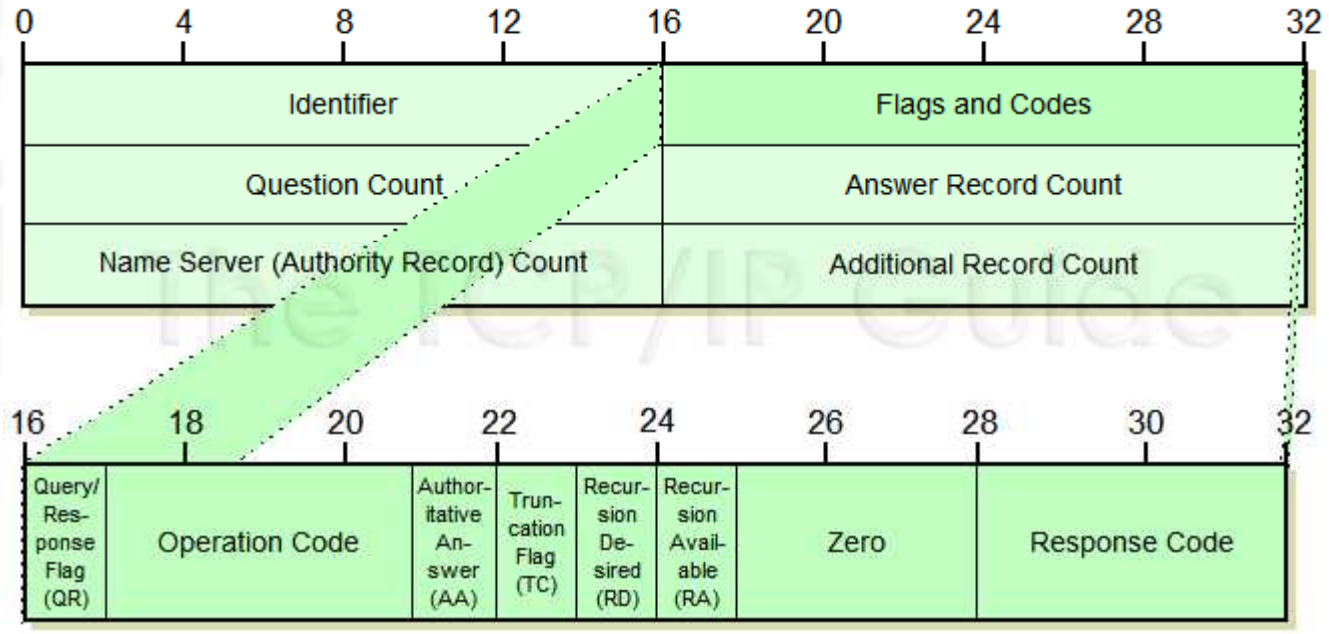
Formato da Mensagem DNS



Formato da Mensagem DNS (cont.)

- *Identification*:
  - Id da mensagem, definida pelo cliente e retornada nas respostas do servidor. Permite ao cliente fazer o casamento entre as requisições e as respostas.
- *Flags*:
  - Dividido em vários campos (vide adiante).
- *Number of questions*:
  - Para queries é igual a 1, com os outros campos = 0. Para *answers* é igual a 0.
- *Number of answers*:
  - Número de Resource Records (RRs) existentes na resposta.

Formato da Mensagem DNS: Flags



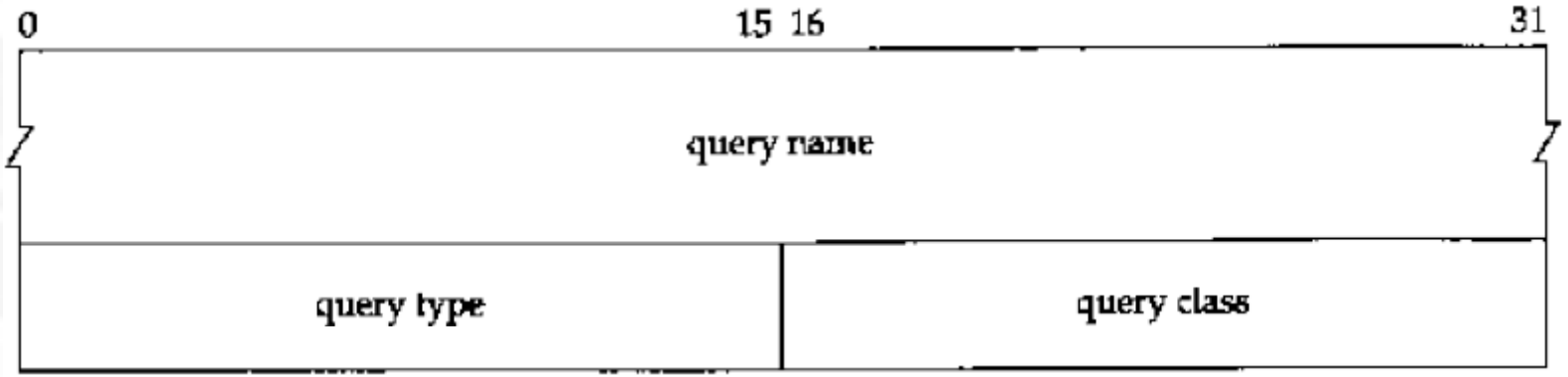
Formato da Mensagem DNS: Flags

- *QR: Messagem Type*
  - 0-query; 1-response
- *opcode: Operation Code*
  - 0-standard query; 1-inverse-query; 2-server status request
- *AA: Authoritative Answer*
  - O nome do servidor é autoritativo para o domínio definido na seção de "question".
- *TC: Truncated*
  - No caso de UDP, o tamanho total da resposta excedeu 512 bytes (apenas 512 bytes foram retornados).

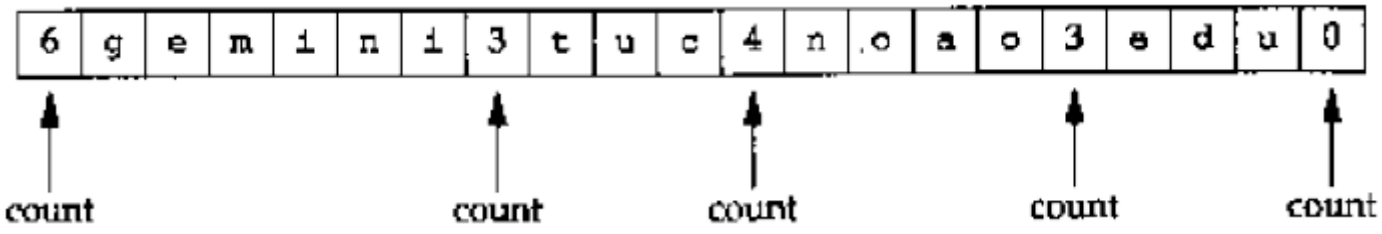
Formato da Mensagem DNS: Flags (cont.)

- *RD: Recursion Desired*
  - Ligado ("setado") na consulta (*query*) e retornado na resposta. Diz ao servidor para tratar essa consulta como recursiva. Se não "setado" e o servidor não tiver uma resposta autoritativa, o servidor retorna uma lista de servidores para se contatar para obter a resposta (neste caso, ele a trata como uma consulta interativa).
- *RA: Recursion Available*
  - É "setado" em 1 na resposta, se o servidor suporta recursão. A maioria dos servidores suporta a recursão, exceto os *root servers*.
- *RCODE: Response Code*
  - 0-no error; 3-name error
  - Um *name error* é retornado apenas pelo servidor autoritativo e significa que o nome de domínio especificado na *query* não existe.

DNS Questions



- *Query Name:*
  - É o nome que está sendo consultado (domínio a ser resolvido).
  - É uma sequência de um ou mais labels, cada um deles começando com um contador que especifica o número de bytes que segue. O nome é terminado com 0 (zero), que é o tamanho do *label* da raiz do DNS (“.”).
  - Ex: gemini.tuc.noao.edu



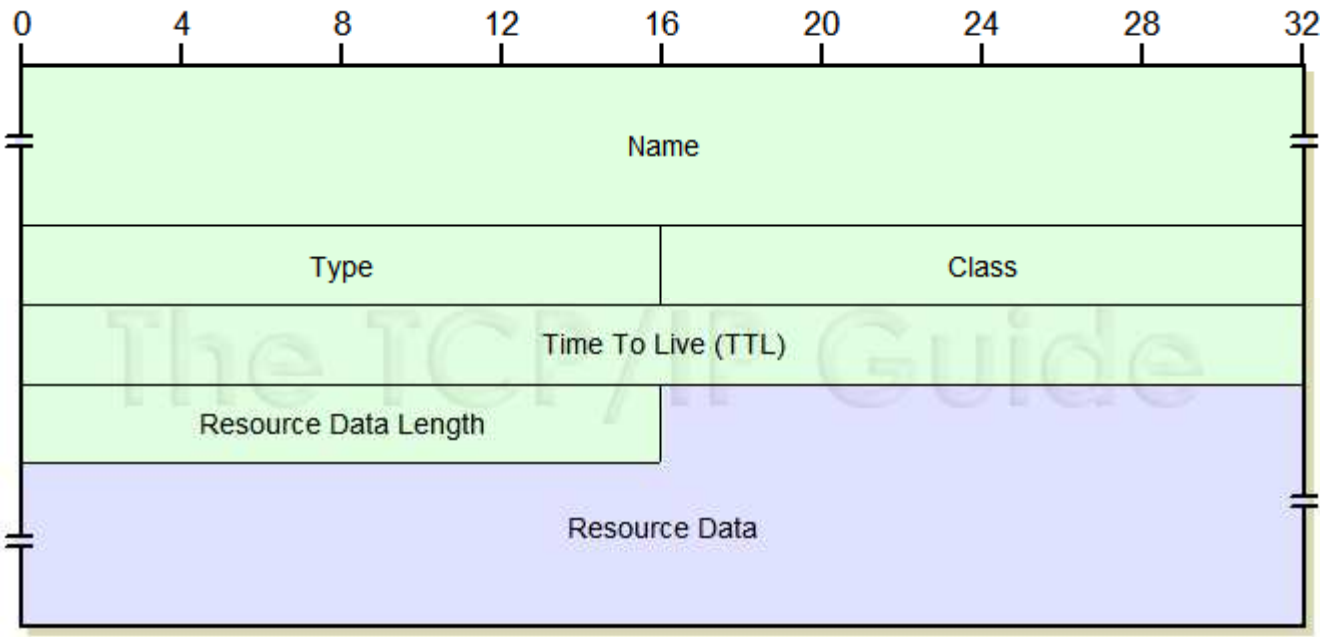
DNS Questions (cont.)

- *Query Type:*
  - Cada consulta tem uma *query type* e cada resposta (denominada Resource Record – RR), tem um *type*.

Name	Numeric value	Description	*type?*	*query type?*
A	1	IP address	*	*
NS	2	name server	*	*
CNAME	5	canonical name	*	*
PTR	12	pointer record	*	*
HINFO	13	host info	*	*
MX	15	mail exchange record	*	*
AXFR	252	request for zone transfer		*
* or ANY	255	request for all records		*

- *Query Class:*
  - Normalmente igual a 1 (Internet address).

DNS Responses: Resource Records (RRs)

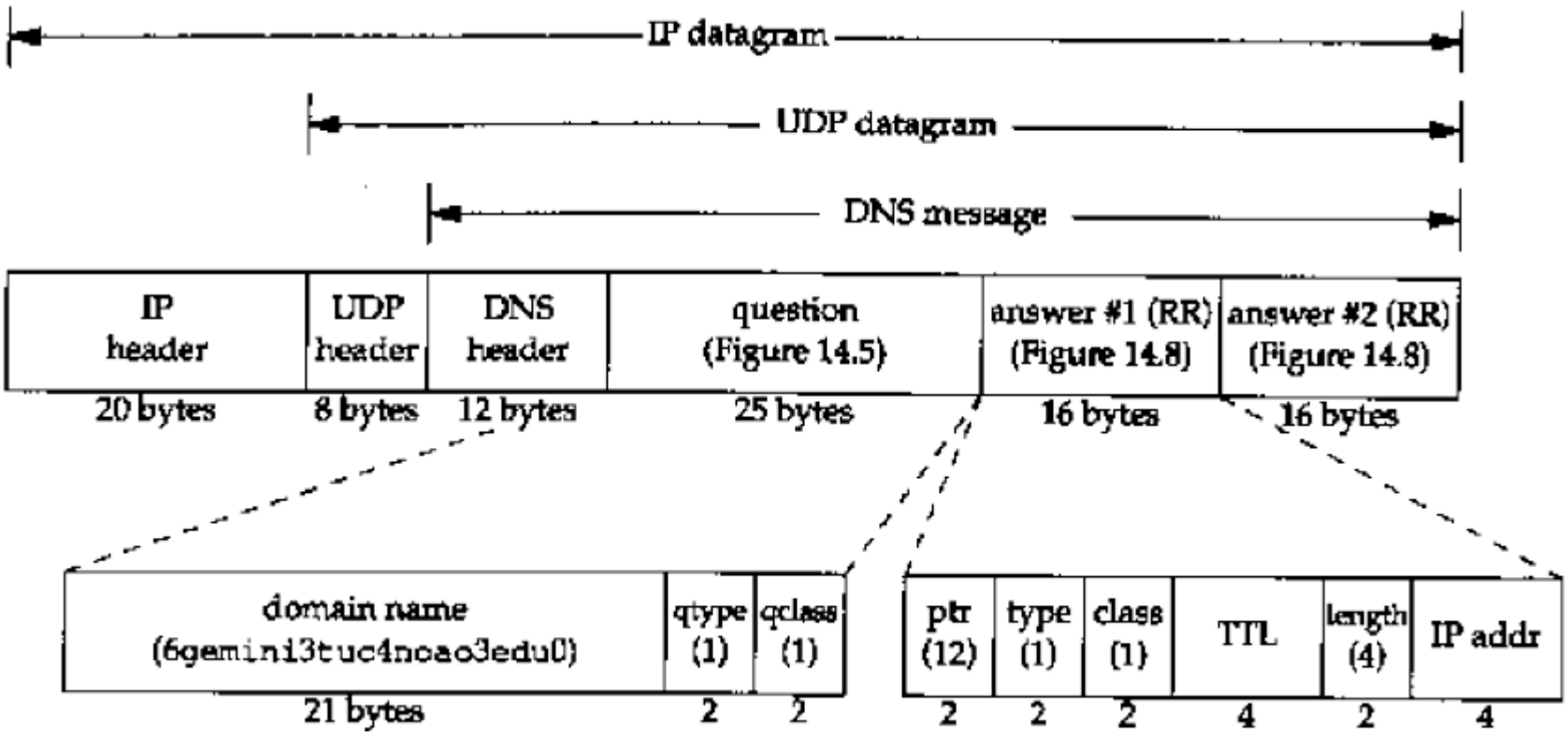


- Os três campos finais da mensagem DNS (*answers*, *authority* e *additional information*) compartilham um formato comum, que é chamado de *Resource Record* (RR).

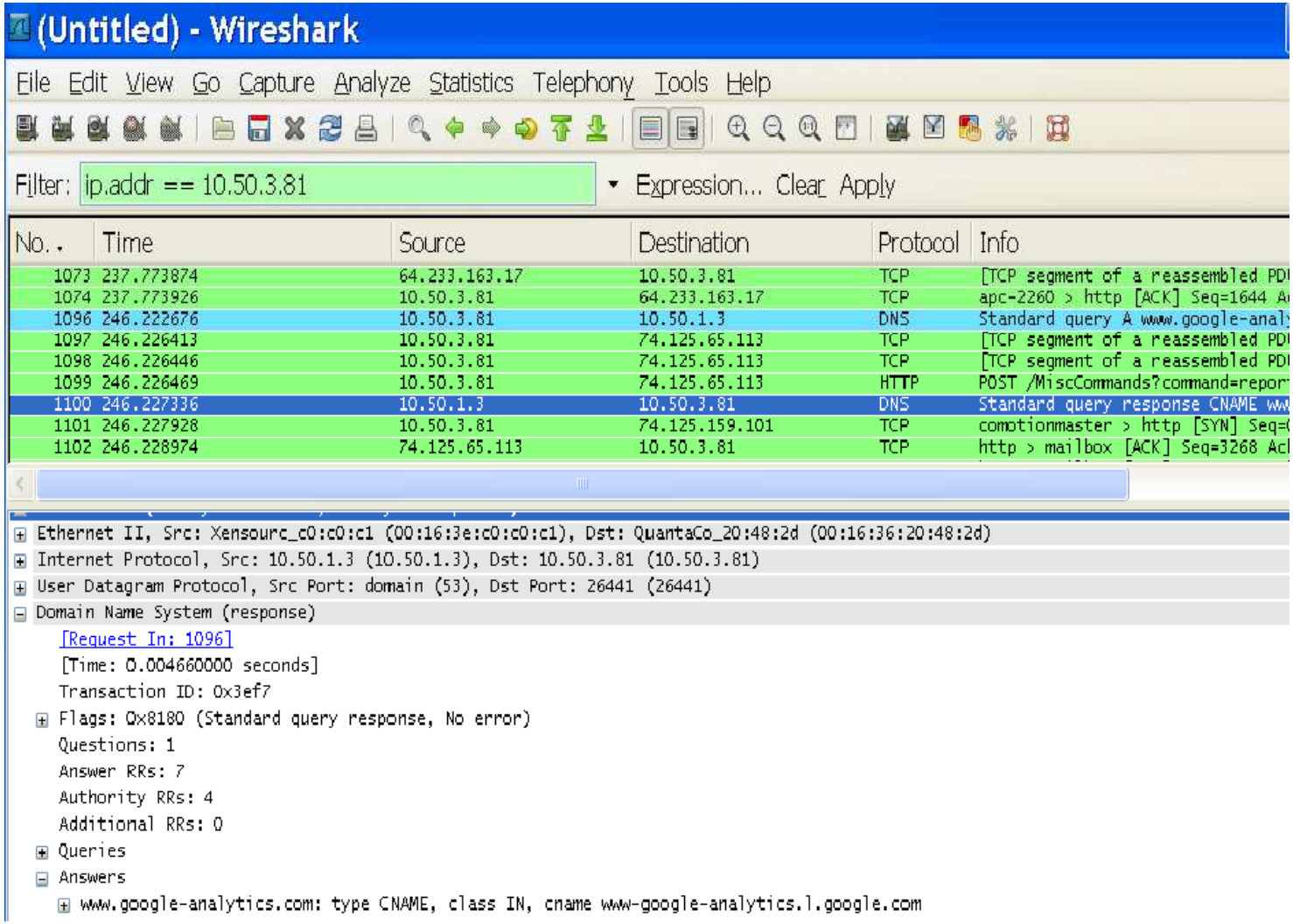
DNS Responses: Resource Records (RRs) (cont.)

- *Domain Name:*
  - Nome do domínio ao qual o RR pertence (idem formato da *query name*).
- *Type*:
  - Especifica o tipo do registro RR (idem *query type*).
- *Class*:
  - Normalmente 1 (Internet data).
- *TTL*:
  - Número de segundos que o RR pode ficar em cache no cliente.
  - RRs normalmente tem um TTL de dois dias (172.800 segundos).
- *Resource Data Length*:
  - Especifica o tamanho dos dados. O formato deste campo depende do tipo do RR. Para um RR do tipo 1 (“A”) o tamanho é de 4 bytes, que é o tamanho de um endereço IP.

Encapsulamento



Exemplo: Query



Exemplo - Response

No.	Time	Source	Destination	Protocol	Info
1073	237.773874	64.233.163.17	10.50.3.81	TCP	[TCP segment of a reassembled
1074	237.773926	10.50.3.81	64.233.163.17	TCP	apc-2260 > http [ACK] Seq=164
1096	246.222676	10.50.3.81	10.50.1.3	DNS	Standard query A www.google-a
1097	246.226413	10.50.3.81	74.125.65.113	TCP	[TCP segment of a reassembled
1098	246.226446	10.50.3.81	74.125.65.113	TCP	[TCP segment of a reassembled
1099	246.226469	10.50.3.81	74.125.65.113	HTTP	POST /MiscCommands?command=re
1100	246.227336	10.50.1.3	10.50.3.81	DNS	Standard query response CNAME
1101	246.227928	10.50.3.81	74.125.159.101	TCP	comotionmaster > http [SYN] S

```
[Request In: 1096]
[Time: 0.004660000 seconds]
Transaction ID: 0x3ef7
⊞ Flags: 0x8180 (Standard query response, No error)
Questions: 1
Answer RRs: 7
Authority RRs: 4
Additional RRs: 0
⊞ Queries
⊞ Answers
⊟ Authoritative nameservers
  ⊟ google.com: type NS, class IN, ns ns3.google.com
      Name: google.com
      Type: NS (Authoritative name server)
      Class: IN (0x0001)
      Time to live: 1 day, 19 hours, 3 minutes, 18 seconds
      Data length: 6
      Name server: ns3.google.com
  ⊞ google.com: type NS, class IN, ns ns2.google.com
  ⊞ google.com: type NS, class IN, ns ns1.google.com
  ⊞ google.com: type NS, class IN, ns ns4.google.com
```

```
0020  03 51 00 35 67 49 01 06  2d a5 3e f7 81 80 00 01   .Q.5gI.. -.>.....
0030  00 07 00 04 00 00 03 77  77 77 10 67 6f 6f 67 6c   .......w ww.googl
0040  65 2d 61 6e 61 6c 79 74  69 63 73 03 63 6f 6d 00   e-analyt ics.com.
```