

Redes de Computadores

Capítulo 2.5 - DNS

Prof. Jó Ueyama
Março/2012

DNS: Domain Name System

Pessoas: muitos identificadores:

- RG, nome, passaporte.

Hosts e roteadores na Internet:

- endereços IP (32 bits)
 - endereça datagramas;
 - hierárquico, organizado em 4 bytes.
- “nome”, ex.: `www.icmc.usp.br` - usados por humanos.

P.: Como relacionar nomes com endereços IP?

DNS: Domain Name System

- **Base de dados distribuída implementada numa hierarquia de servidores de nomes.**
- **Protocolo de camada de aplicação que permite que hosts se comuniquem com servidores de nomes para resolver nomes (tradução nome/ endereço):**
 - é uma função interna da Internet, implementada como protocolo da camada de aplicação.
 - complexidade na “borda” da rede.

DNS

- Arquitetura cliente-servidor.
- Protocolo de transporte: UDP.
- Porta: 53.
- Software mais popular: BIND (Berkeley Internet Name Domain) para Unix.
- RFCs 1034 e 1035, além de RFCs com atualizações.

Serviços DNS

- Tradução do nome do *host* para endereço IP.
- Apelidos de hosts (*aliasing*):
 - nome canônico: relay1.west-coast.enterprise.com
 - alias: www.enterprise.com
- Apelidos de servidor de correio:
 - registro MX indica o servidor de email do domínio.
- Distribuição de carga:
 - Servidores Web replicados: conjunto de endereços IP para um nome canônico.

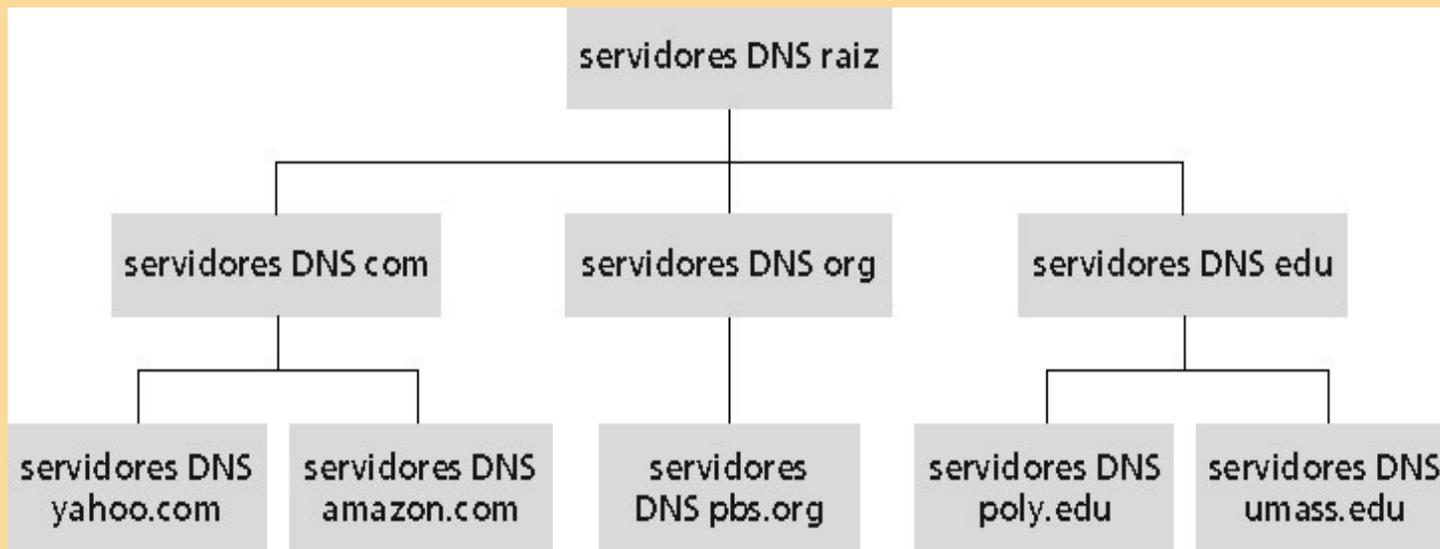
Por que não centralizar o DNS?

- Ponto único de falha.
 - Volume de tráfego.
 - Base centralizada de dados distante.
 - Manutenção.
-
- **Não é escalável!**

Banco de dados distribuído e hierárquico

Cliente quer o IP para www.amazon.com:

- 1) Consulta um servidor de raiz para encontrar o servidor DNS [.com](#)
- 2) Consulta o servidor DNS [com](#) para obter o servidor DNS [amazon.com](#)
- 3) Consulta o servidor DNS [amazon.com](#) para obter o endereço IP para [www.amazon.com](#)



DNS: servidores de nome raiz

- ∇ São contatados pelos servidores de nomes locais que não podem resolver um nome.
- ∇ Servidores de nomes raiz:
 - 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.

DNS: servidores de nome raiz

Existem 13 (conglomerados de) servidores de nomes raiz no mundo.
Nomeados de A a M.



Servidores de Domínio de Alto Nível

- ou top-level domain (TLD) servers .
- Responsáveis pelos domínios com, org, net, edu etc. e todos os domínios **top-level** nacionais uk, fr, ca, jp.
- Network Solutions mantém servidores para o TLD “com”.
- Educause para o TLD “edu”.

Servidores de nomes com autoridade

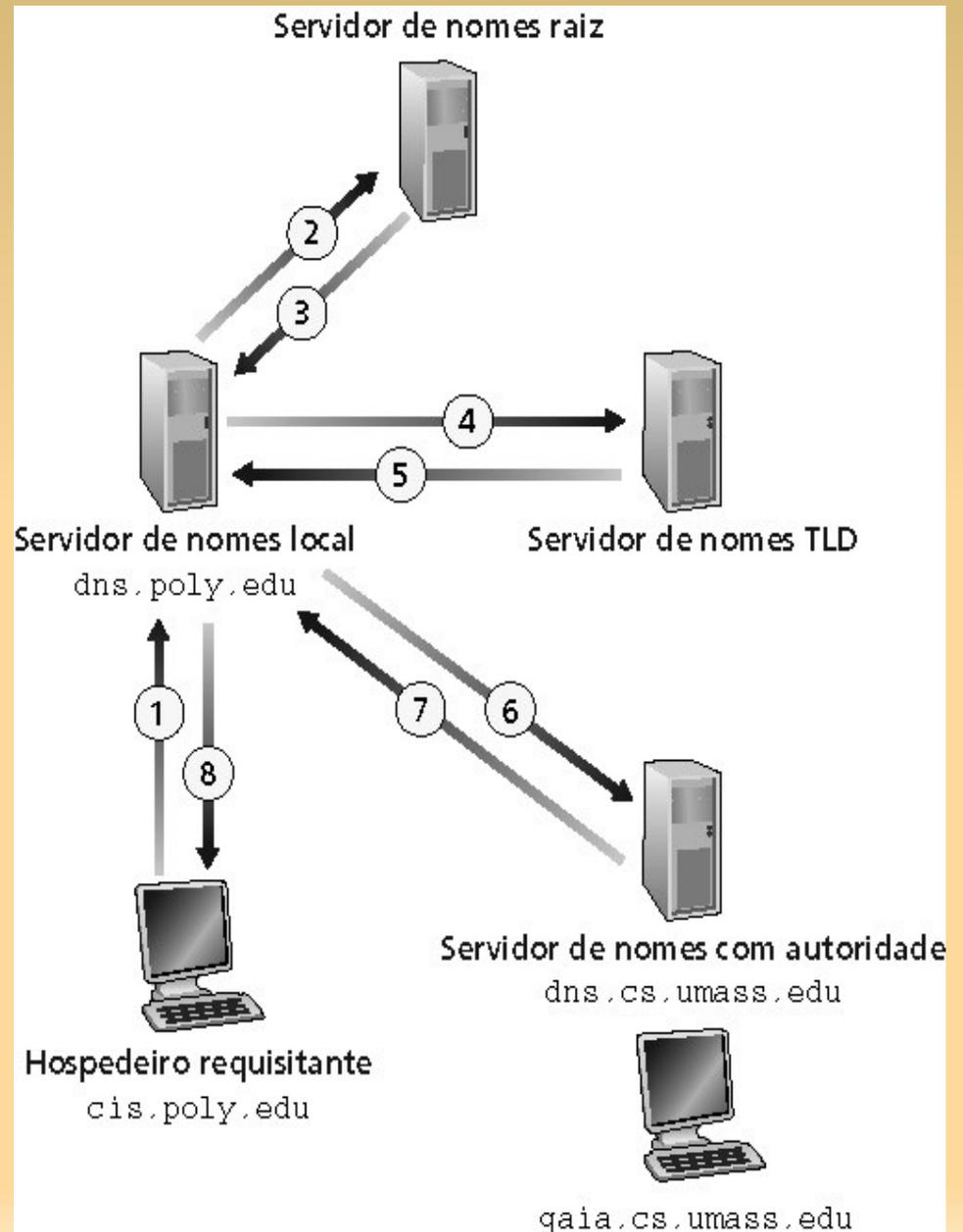
- Servidores DNS de organizações.
- Provêem: nome de hospedeiro autorizado para mapeamentos IP para servidores de organizações:
 - Ex.: Web e mail.
- Podem ser mantidos por uma organização ou provedor de serviços.

Servidor de nomes local

- Não pertence estritamente a 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 proxy, encaminhando as perguntas para dentro da hierarquia.

Exemplo

O hospedeiro em
cis.poly.edu quer o
endereço IP para
gaia.cs.umass.edu



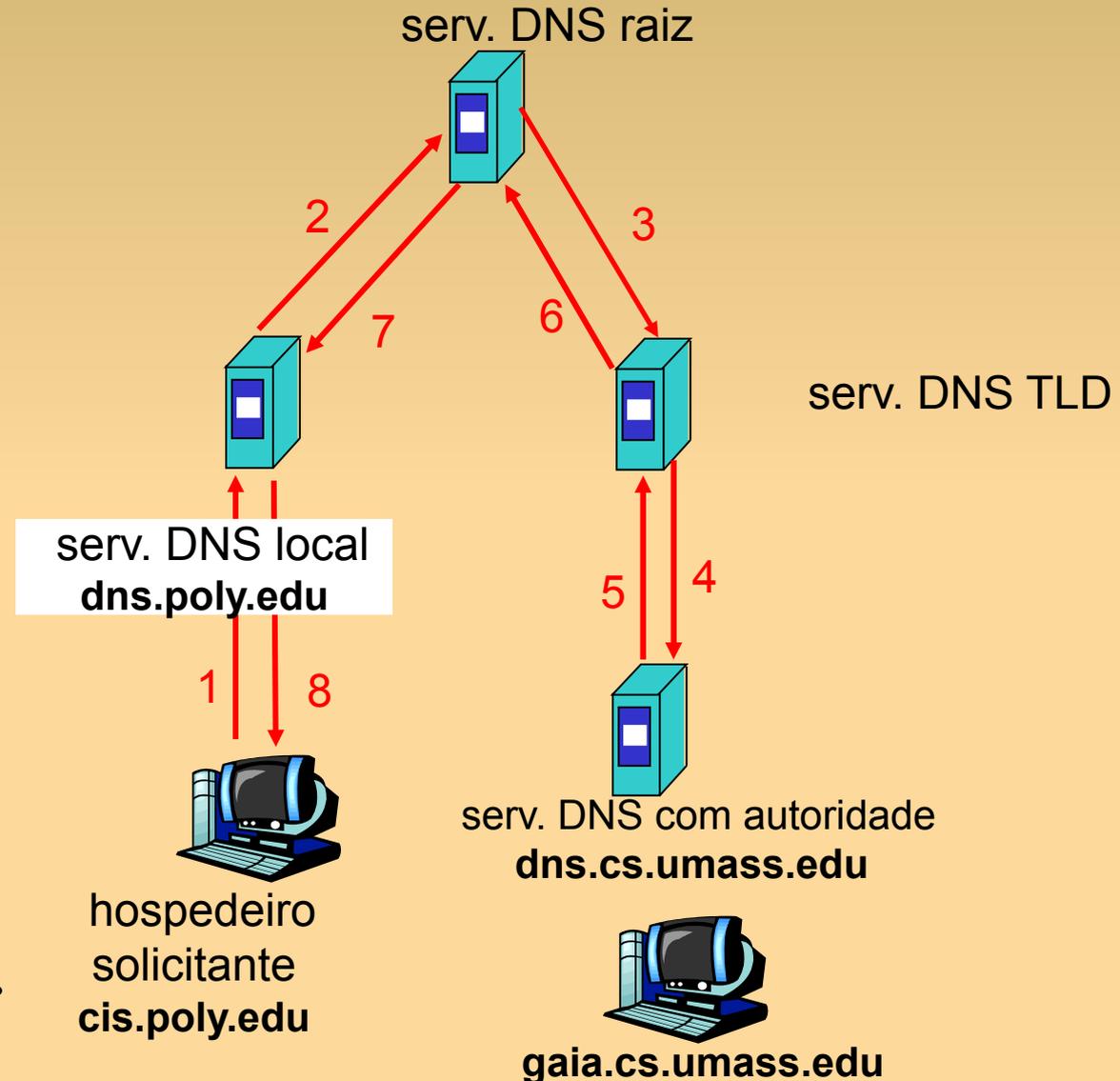
Consultas encadeadas e recursivas

Consulta recursiva:

- Transfere a tarefa de resolução do nome para o servidor de nomes consultado.
- Carga pesada?

Consulta encadeada:

- Servidor contatado responde com o nome de outro servidor de nomes para contato.
- “Eu não sei isto, mas pergunte a este servidor”.



DNS: cache e atualização de registros

- Uma vez que um servidor de nomes aprende um mapeamento, ele armazena o mapeamento num registro do tipo **cache**.
- Registros do cache tornam-se obsoletos (desaparecem) depois de um certo tempo.
 - tipicamente 2 dias.
- Servidores TLD: tipicamente armazenados em cache nos servidores de nome locais.

Registro do 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

ex.: (foo.com, dns.foo.com, NS)
- Type = CNAME
 - **name** é um “apelido” para algum nome “canônico” (o nome real)
www.ibm.com é realmente servereast.backup2.ibm.com
 - **value** é o nome canônico
- Type = MX
 - **value** é o nome do servidor de correio associado com **name**

ex.: (foo.com, mail.foo.com, MX)

DNS: protocolo e mensagens

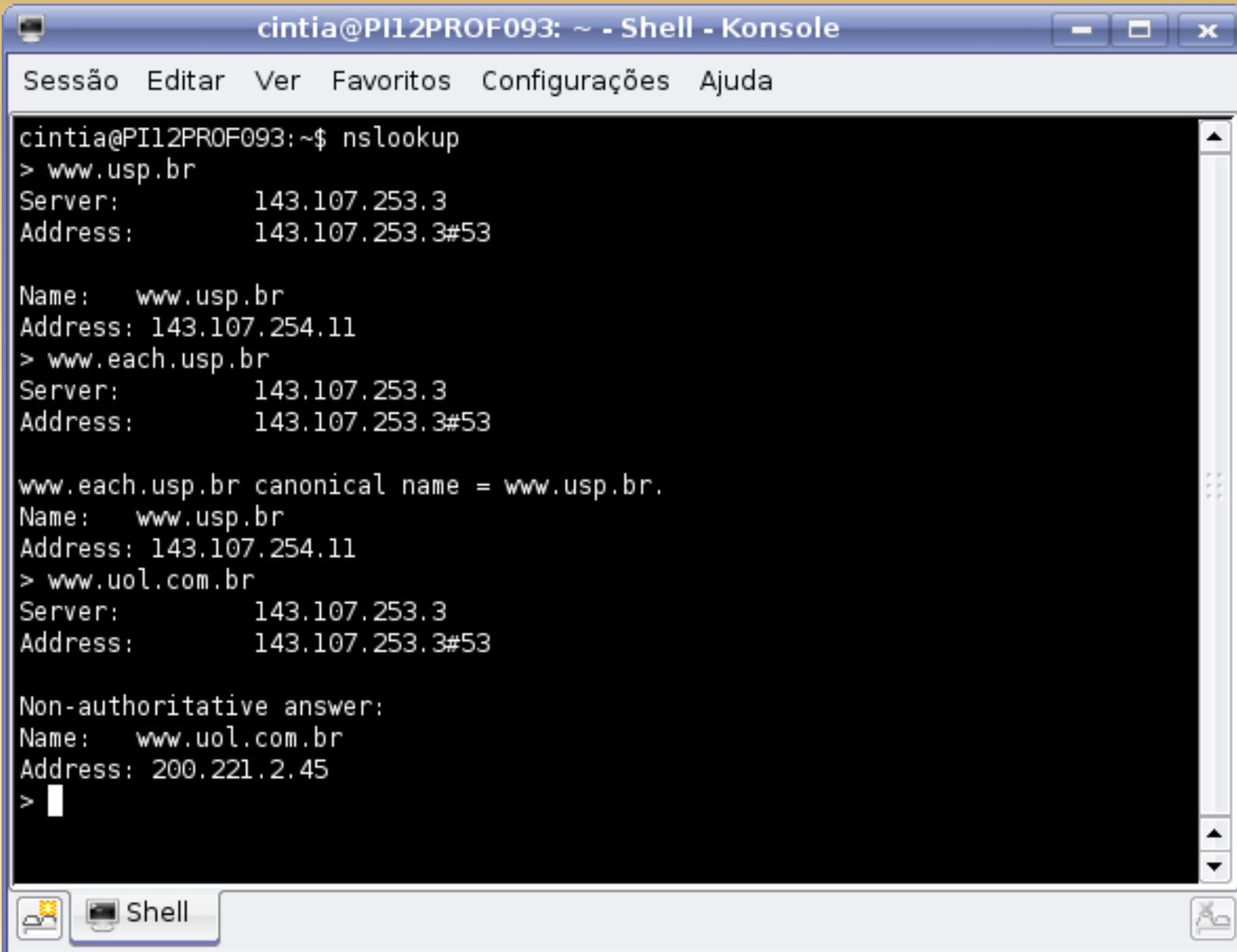
Protocolo DNS: mensagem de **consulta** e **resposta**, ambas com o mesmo **formato de mensagem**

Cabeçalho da msg:

- **Identificação:** número de 16 bits para consulta, resposta usa o mesmo número
- **Flags (1 bit cada):**
 - Consulta ou resposta
 - Recursão desejada
 - Recursão disponível
 - Resposta é autorizada

Identificação	Flags	12 bytes
Número de perguntas	Número de RRs de resposta	
Número de RRs com autoridade	Número de RRs adicionais	
Perguntas (número variável de perguntas)		Nome, campos de tipo para uma consulta
Respostas (número variável de registros de recursos)		RRs de resposta à consulta
Autoridade (número variável de registros de recursos)		Registros para servidores com autoridade
Informação adicional (número variável de registros de recursos)		Informação adicional 'útil', que pode ser usada

nslookup – consultas DNS



```
cintia@PI12PROF093: ~ - Shell - Konsole
Sessão Editar Ver Favoritos Configurações Ajuda
cintia@PI12PROF093:~$ nslookup
> www.usp.br
Server:          143.107.253.3
Address:         143.107.253.3#53

Name:   www.usp.br
Address: 143.107.254.11
> www.each.usp.br
Server:          143.107.253.3
Address:         143.107.253.3#53

www.each.usp.br canonical name = www.usp.br.
Name:   www.usp.br
Address: 143.107.254.11
> www.uol.com.br
Server:          143.107.253.3
Address:         143.107.253.3#53

Non-authoritative answer:
Name:   www.uol.com.br
Address: 200.221.2.45
> 
```

Inserindo registros no DNS

- Exemplo: empresa recém-criada “Network Utopia”.
- Registrar o nome networkutopia.com num “registrar” (entidade registradora).
 - ex.: Network Solutions, registro.br
- É necessário fornecer ao registrar os nomes e endereços IP do seu servidor de nomes com autoridade (primário e secundário).
- Registrar insere dois RRs no servidor TLD do domínio com:
 - (networkutopia.com, dns1.networkutopia.com, NS)
 - (dns1.networkutopia.com, 212.212.212.1, A)
- No servidor autorizado, inserir um registro Tipo A para www.networkutopia.com e um registro Tipo MX para networkutopia.com

Atualizações dinâmicas

- Mecanismos de atualização e notificação:
 - RFC 2136: abril/1997;
 - opção UPDATE;
 - UDP ou TCP, requisitante escolhe;
 - formato de mensagem específico;
 - <http://www.ietf.org/rfc/rfc2136.txt>