

# PTC 3450 - Aula 08

## 2.4 DNS – O serviço de diretório da Internet

(Kurose, p. 95 - 106)

(Peterson, p. 239-242)

31/03/2016

# Capítulo 2: conteúdo

2.1 Princípios de aplicativos de rede

2.2 Web e HTTP

2.3 Correio eletrônico

- SMTP, POP3, IMAP

2.4 DNS

2.5 Aplicativos P2P

2.6 *Streaming* de vídeo e redes de distribuição de conteúdo

2.7 Programando *socket* com UDP e TCP

# DNS: Domain Name System (RFC 1034 e 1035)

*peessoas*: vários identificadores:

- CPF, nome, num. do passaporte
- Cada um mais relevante em cada situação

*hosts e roteadores Internet*:

- **Endereço IP** (32 bit – 4 bytes) – usado para endereçar datagramas
- **Hostname** - “nome”, e.g., www.yahoo.com – usado por humanos

**Q:** como mapear entre endereço IP e nome, e vice versa?

**Domain Name System (1983):**

- ❖ *banco de dados distribuído* implementado de forma hierárquica em muitos *name servers* (ou servidores DNS)
- ❖ *protocolo da camada de aplicação*: *hosts* e *name servers* comunicam-se para *decifrar* nomes (tradução endereço IP/nome)
  - nota: função de núcleo da Internet, implementada como protocolo da camada de aplicação
  - complexidade na “borda” da rede

# DNS: serviços, estrutura

## *serviços DNS*

- ❖ tradução nome do *host* para endereço IP
- ❖ apelidos para *host*
  - nomes canônicos, apelidos
- ❖ apelidos para servidores de *mail*
- ❖ distribuição de carga
  - servidores Web replicados: muitos endereços IP correspondem a um só nome
- ❖ Usa UDP porta 53
- ❖ *Software* Berkley Internet Name Domain (BIND)

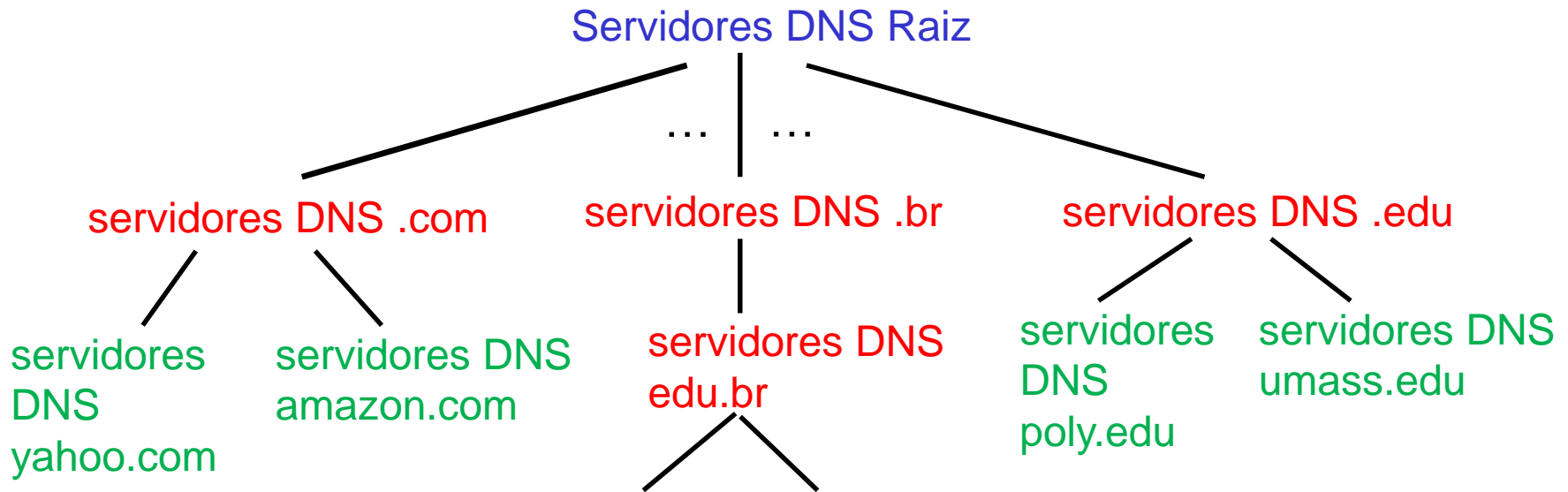
## *por que não centralizar DNS?*

- ❖ Ponto único de falha
- ❖ Volume de tráfego
- ❖ Banco de dados centralizado distante
- ❖ Manutenção
- ❖ Segurança

## *R: não é escalável!*

- ❖ Utilizado por outros protocolos da camada de aplicação: HTTP, SMTP, FTP, ...
- ❖ Pode ser fonte importante de *delay*

# DNS: banco de dados hierárquico e distribuído

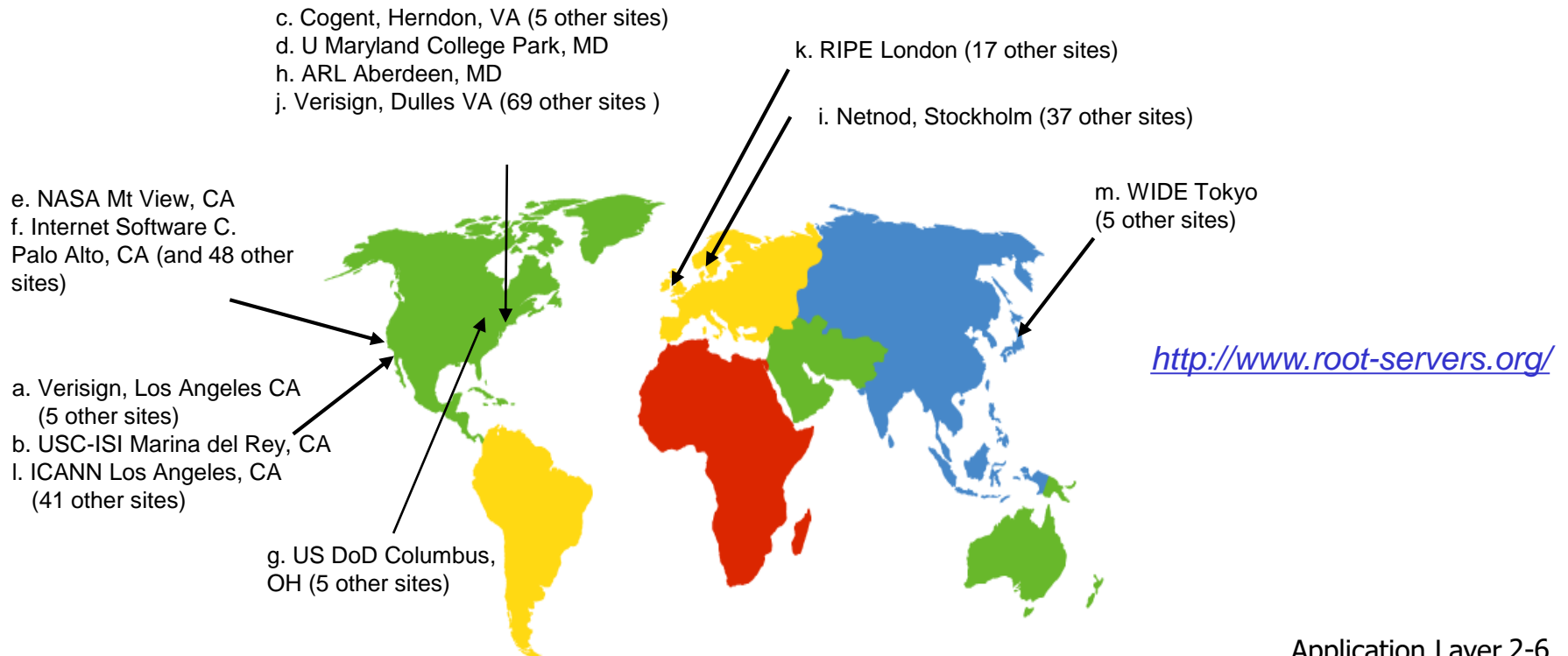


*cliente quer IP para www.amazon.com; 1ª abordagem:*

- ❖ cliente pede a **servidor DNS raiz** encontrar servidor DNS .com
- ❖ cliente pede a **servidor DNS top level domain (TLD) .com** obter servidor amazon.com
- ❖ cliente pede a **servidor DNS autoritário** de amazon.com obter endereço IP para www.amazon.com

# DNS: name servers raízes

- ❖ Contactado, retorna endereços IP de servidores TLD para o domínio desejado (.com, .br, .edu, etc.)
- ❖ 13 “name servers” raízes ao redor do mundo (247 servidores)
- ❖ Verisign, USC-ISI, Cogent, UMD, NASA-ARC, ISC, DOD-NIC, ARL, Netnod, RIPE NCC, ICANN, WIDE



# TLD e servidores autoritários

## *servidores top-level domain (TLD):*

- responsáveis por .com, .org, .net, .edu, .aero, .jobs, .museums, e todos domínios de nível mais alto de países, e.g.: .br, .uk, .fr, .ca, .jp
- VeriSign Global Registry Services mantêm servidores para TLD .com (<http://www.networksolutions.com/>)
- Educause para TLD .edu (<http://www.educause.edu/>)
- CGI.br para TLD .br (<http://www.cgi.br/>)
- Lista completa em <http://www.iana.org/domains/root/db>

## *servidores DNS autoritários:*

- servidor(es) DNS da própria organização, fornecendo mapeamentos autoritários entre nomes de *host* e IP para os *hosts* da organização nomeados
- podem ser mantidos por organização ou provedor de serviços

# Name server DNS local

- ❖ não está estritamente na hierarquia
- ❖ cada ISP (ISP residencial, empresa, universidade) tem um
  - também chamado de “*default name server*”
  - IP fornecido pela rede
- ❖ quando *host* faz consulta DNS, consulta é enviada para seu servidor DNS local
  - tem *cache* local de traduções nome-endereço recentes (mas algumas podem estar desatualizadas!)
  - age como *proxy*, repassando consulta para hierarquia

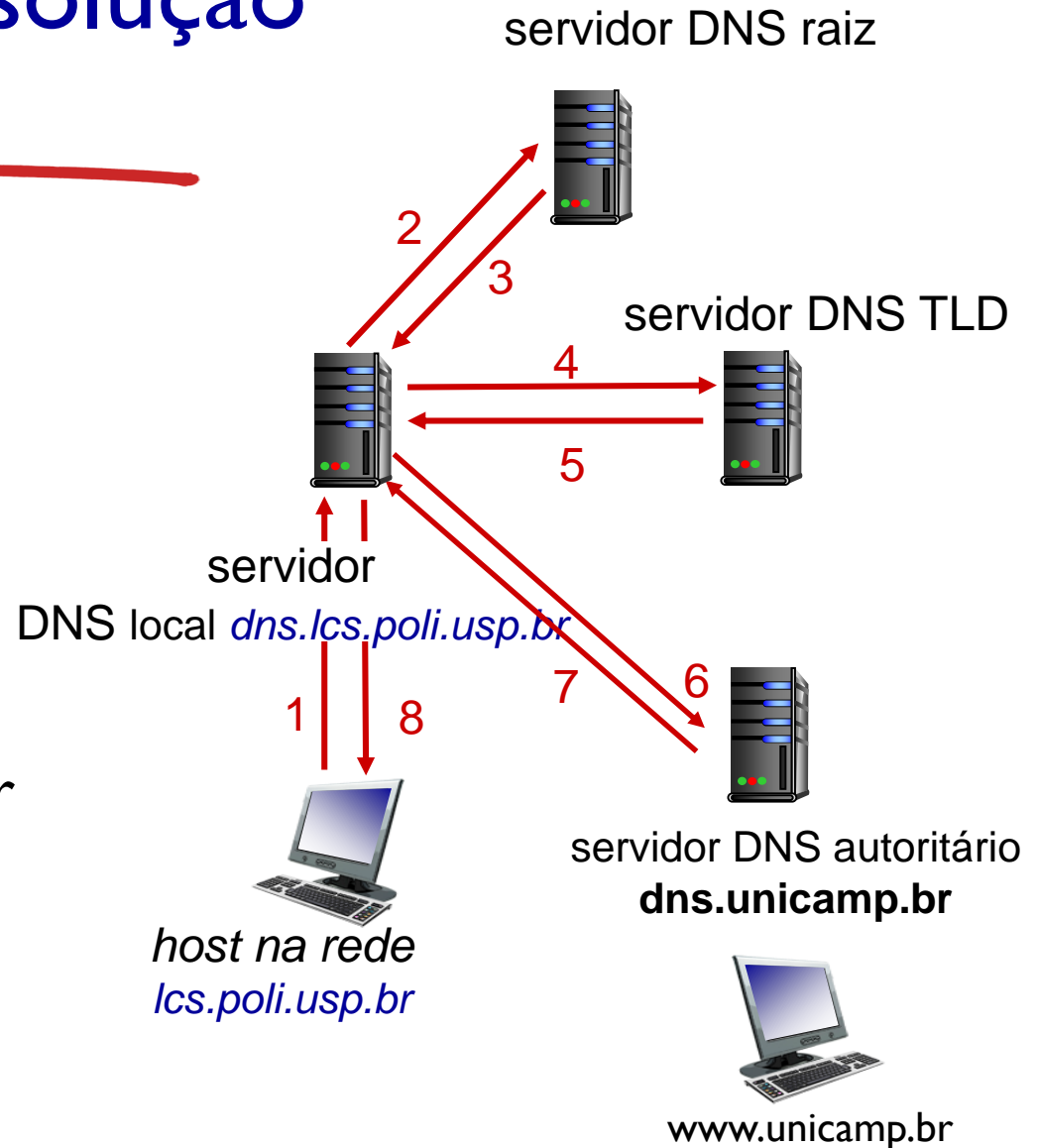


# Exemplo de resolução de nome DNS

- ❖ *host* em `lcs.poli.usp.br` quer endereço IP para `www.unicamp.br`

## *consulta iterativa:*

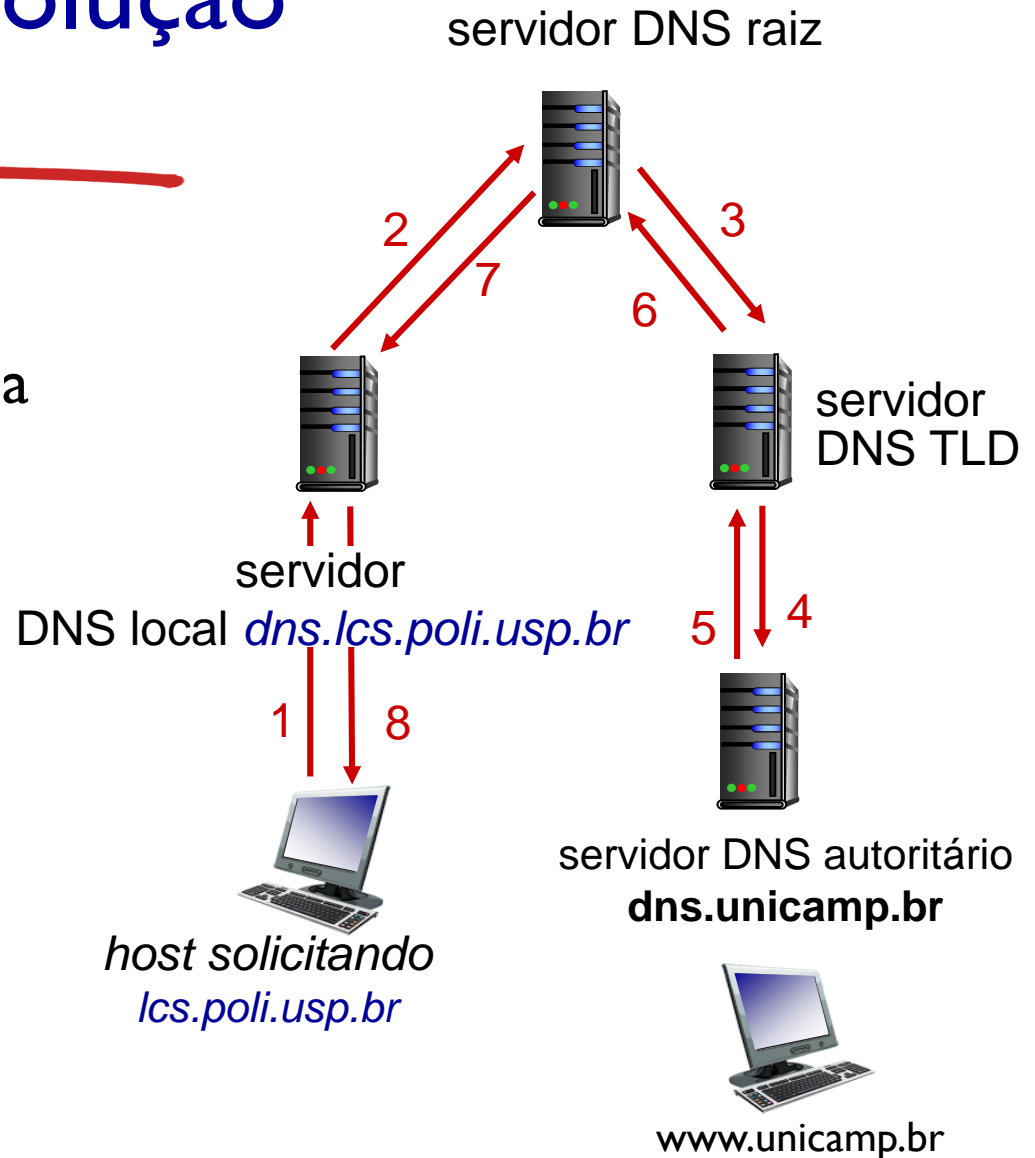
- ❖ servidor contatado responde com nome do servidor a contatar
- ❖ “Eu não conheço esse nome, mas pergunte a esse servidor”
- ❖ **Note que são necessárias 8 mensagens DNS para resolver!**



# Exemplo de resolução de nome DNS

## *consulta recursiva:*

- ❖ coloca responsabilidade da decifração do nome no *name server* contatado
- ❖ carga mais pesada nos níveis mais altos da hierarquia?
- ❖ Não usual



# DNS: *caching*, atualizando registros

- ❖ uma vez que (qualquer) *servidor DNS* aprende **mapeamento**, ele o *guarda*
  - registros do *cache* são *apagados (timeout)* depois de algum tempo (TTL - *time-to-live* – muitas vezes, 2 dias)
  - servidores TLD tipicamente guardados em *name servers* locais
    - assim *name servers* raízes são raramente visitados
- ❖ registros guardados podem estar **desatualizadas** (tradução nome-para-endereço com melhor esforço!)
  - se nome do *host* muda de endereço IP, ele pode não ser conhecido na Internet toda até que todos os TTLs expirem
- ❖ mecanismos de atualização/notificação propostos como padrão IETF
  - [RFC 2136](#)
  - **Testar nslookup!**

# Registros DNS

**DNS:** banco de dados distribuído guardando *resource records* (RR)

formato RR : (nome, valor, tipo, ttl)

## tipo=A (Address)

- **nome** é nome de *host*
- **valor** é endereço IP
- (www.lcs.poli.usp.br, 143.107.162.201, A)

## tipo=NS (Name Server)

- **nome** é domínio (e.g., unicamp.br)
- **valor** é nome de *host* de *name server* autoritário para esse domínio
- (foo.com, dns.foo.com, NS)

## tipo=CNAME (Canonic Name)

- **nome** é nome apelido para algum nome “canônico” (o real)
- **www.microsoft.com** é realmente **www.microsoft.com-c-2.edgekey.net**
- **valor** é nome canônico
- (www.microsoft.com, www.microsoft.com-c-2.edgekey.net, NS)

## tipo=MX (Mail Server)

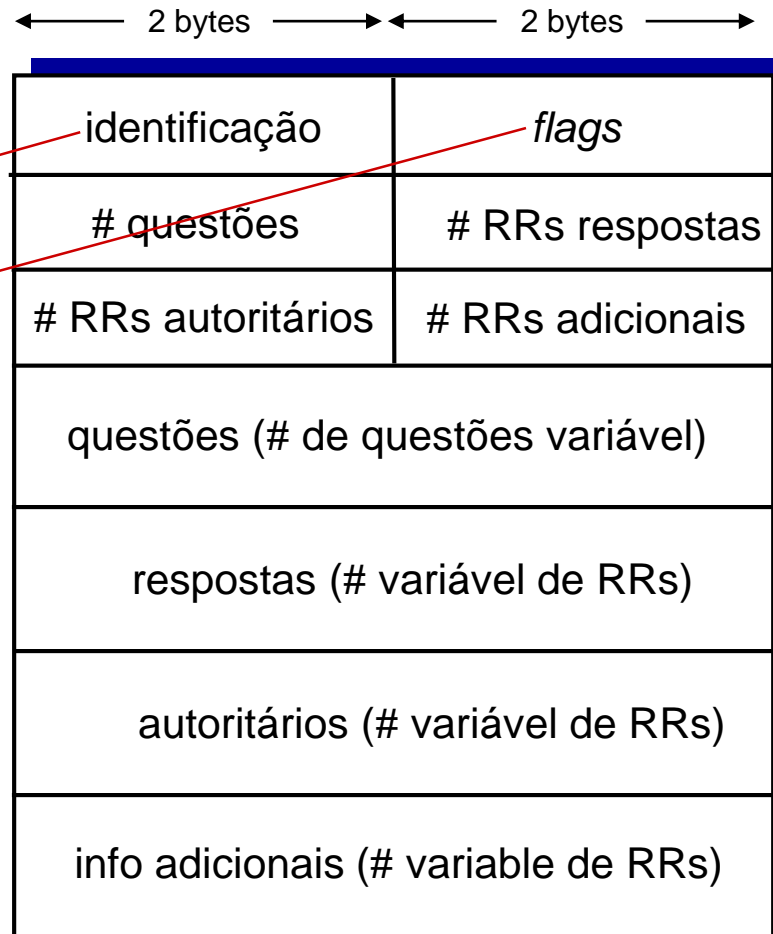
- **valor** é servidor de *mail* associado com **nome**
- (lcs.poli.usp.br, mail.lcs.poli.usp.br, MX)

# Protocolo DNS, mensagens

- ❖ mensagens *consulta* e *resposta*, ambas com mesmo *formato de mensagem*

cabeçalho da msg (12 bytes)

- ❖ **identificação**: # de 16 bit para consulta, resposta a essa consulta usa mesmo #
- ❖ **flags**:
  - consulta ou resposta
  - recursão desejada
  - recursão disponível
  - resposta é autoritária



# Protocolo DNS, mensagens

← 2 bytes → ← 2 bytes →

identificação	<i>flags</i>
# questões	# RRs respostas
# RRs autoritários	# RRs adicionais
questões (# de questões variável)	
respostas (# variável de RRs)	
autoritários (# variável de RRs)	
info adicionais (# variável de RRs)	

campos nome e tipo  
para uma consulta

RRs em resposta  
a consulta

registros de  
servidores autoritários

info adicionais “úteis”  
que podem ser usadas

(ex. IP para endereço canônico)

# Inserindo registros em DNS

- ❖ exemplo: nova empresa “Doces Gostosos”
- ❖ registrar nome docesgostosos.com.br em um *registrator de DNS* (e.g., [registro.br](http://registro.br), <http://www.internic.net/> )
  - nomes e endereços IP do *name server* autoritário (primário e secundário)
  - registrator insere 2 RRs no servidor TLD .com.br:  
(docesgostosos.com.br, dns.docesgostosos.com.br, NS)  
(dns.docesgostosos.com.br, 192.168.1.100, A)
- ❖ criar registro tipo A no servidor autoritário para `www.docesgostosos.com.br`; registro tipo MX para `docesgostosos.com.br`

CRIAR CONTA

 ACESSAR CONTA

Sobre Domínios ▾ Tecnologia ▾ Ajuda ▾ Quem Somos Contato 

Pesquise e registre o domínio desejado  **PESQUISAR**

**DOCESGOSTOSOS.COM.BR**  
disponível para registro

CUSTO  
**R\$ 30,00** por 1 ano  
» outros valores

► CONSULTE AS DEMAIS OPÇÕES DISPONÍVEIS

**REGISTRAR**