

Capítulo 2: Camada de aplicação

REDES DE
COMPUTADORES
E A INTERNET 5ª edição

Uma Abordagem Top-Down

- ❑ 2.1 Princípios de aplicações de rede
- ❑ 2.2 A Web e o HTTP
- ❑ 2.3 FTP
- ❑ 2.4 Correio eletrônico
 - ❖ SMTP, POP3, IMAP
- ❑ 2.5 DNS
- ❑ 2.6 Aplicações P2P
- ❑ 2.7 Programação de sockets com UDP
- ❑ 2.8 Programação de sockets com TCP

DNS: Domain Name System

peessoas: muitos
identificadores:

- ❖ CPF, nome, passaporte

**hospedeiros da Internet,
roteadores:**

- ❖ endereço IP (32 bits) - usado para endereçar datagramas
- ❖ "nome", p. e., ww.yahoo.com - usado pelos humanos

P: Como mapear entre
endereço IP e nome?

Domain Name System:

- ❑ *banco de dados distribuído* implementado na hierarquia de muitos *servidores de nomes*
- ❑ *protocolo em nível de aplicação* hospedeiro, roteadores, servidores de nomes se comunicam para *resolver* nomes (tradução endereço/nome)
 - ❖ Nota: função básica da Internet, implementada como protocolo em nível de aplicação
 - ❖ complexidade na "borda" da rede

DNS

Serviços de DNS

- ❑ tradução nome de hospedeiro -> endereço IP
- ❑ Apelidos (aliases) de hospedeiro
 - ❖ nomes canônicos
- ❑ apelidos de servidor de correio
- ❑ distribuição de carga
 - ❖ servidores Web replicados: conjunto de endereços IP para um nome canônico

Por que não centralizar o DNS?

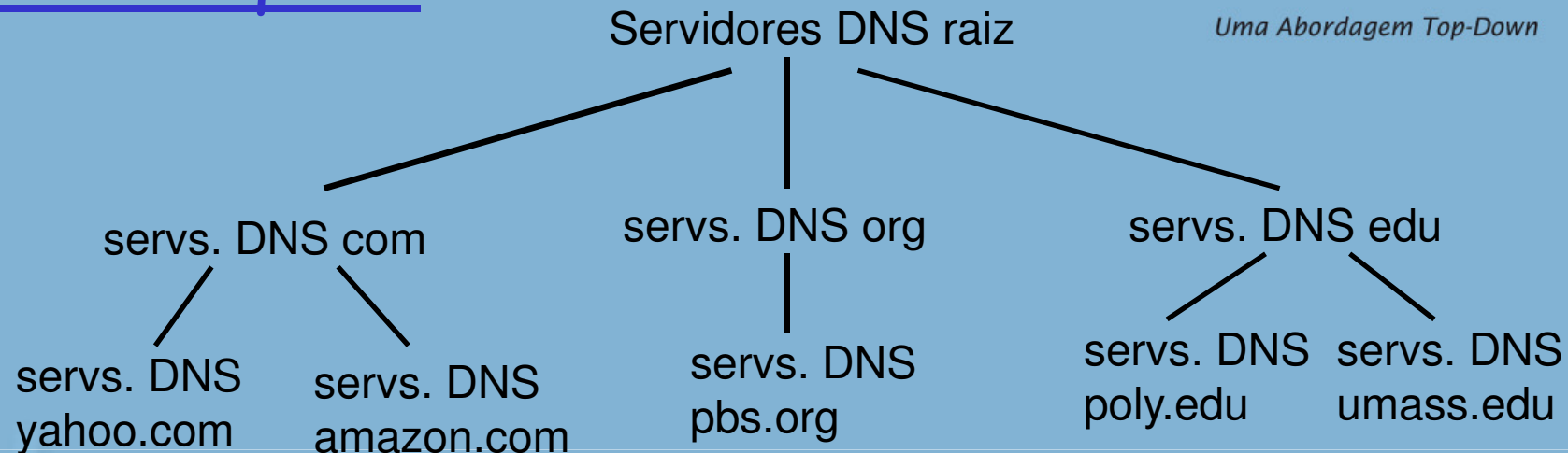
- ❑ único ponto de falha
- ❑ volume de tráfego
- ❑ banco de dados centralizado distante
- ❑ manutenção

Não é escalável!

Banco de dados distribuído, hierárquico

REDES DE
COMPUTADORES
E A INTERNET 5ª edição

Uma Abordagem Top-Down

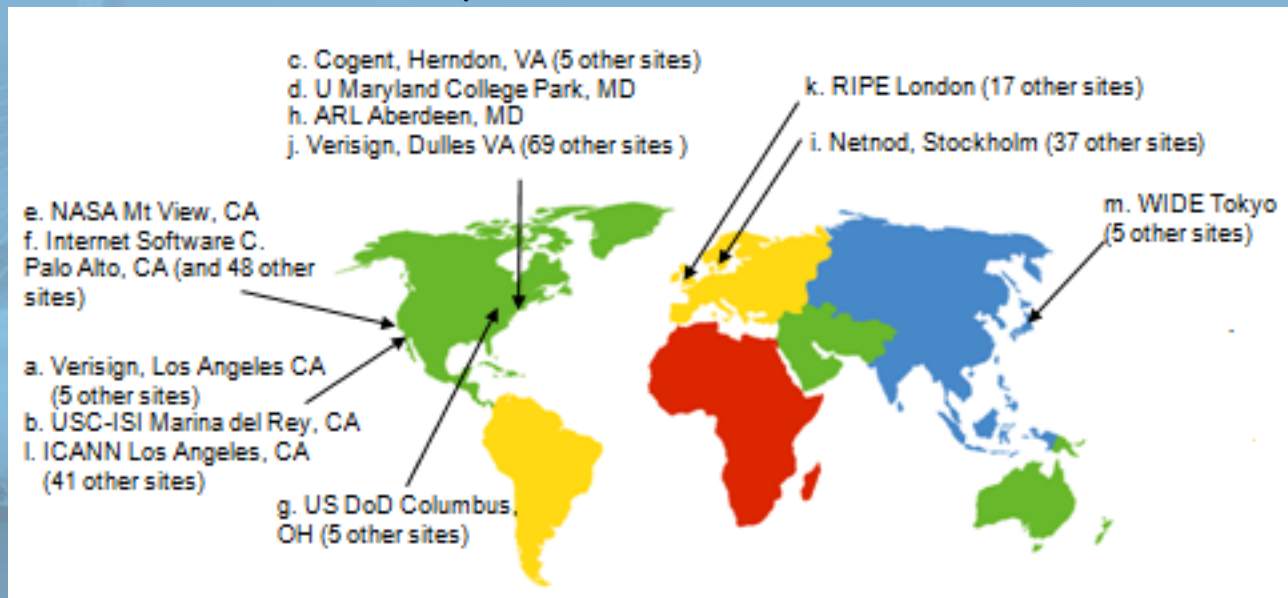


Cliente quer IP para www.amazon.com; 1ª aprox:

- ❑ cliente consulta serv. raiz para achar servidor DNS com
- ❑ cliente consulta serv. DNS com para obter serv. DNS amazon.com
- ❑ cliente consulta serv. DNS amazon.com para obter endereço IP para www.amazon.com

DNS: Servidores de nomes raiz

- ❑ contactados por servidores de nomes locais que não conseguem traduzir nome
- ❑ servidores de nomes raiz:
 - ❖ contacta servidor de nomes com autoridade se o mapeamento não for conhecido
 - ❖ obtém mapeamento
 - ❖ retorna mapeamento ao servidor de nomes local



13 servidores de
nomes raiz no mundo

-> <http://www.root-servers.org/>

TLD e servidores com autoridade

❑ servidores de domínio de alto nível (TLD) :

- ❖ responsáveis por com, org, net, edu etc. e todos os domínios de país de alto nível: br, uk, fr, ca, jp.
- ❖ A Network Solutions mantém servidores para TLD com
- ❖ Educause para TLD edu

❑ servidores DNS com autoridade:

- ❖ servidores DNS da organização, provendo nome de hospedeiro com autoridade a mapeamentos IP para os servidores da organização (p. e., Web, correio).
- ❖ podem ser mantidos pela organização ou provedor de serviços

Servidor de nomes local - Servidor de Autoridade

REDES DE
COMPUTADORES
E A INTERNET 5ª edição

Uma Abordagem Top-Down

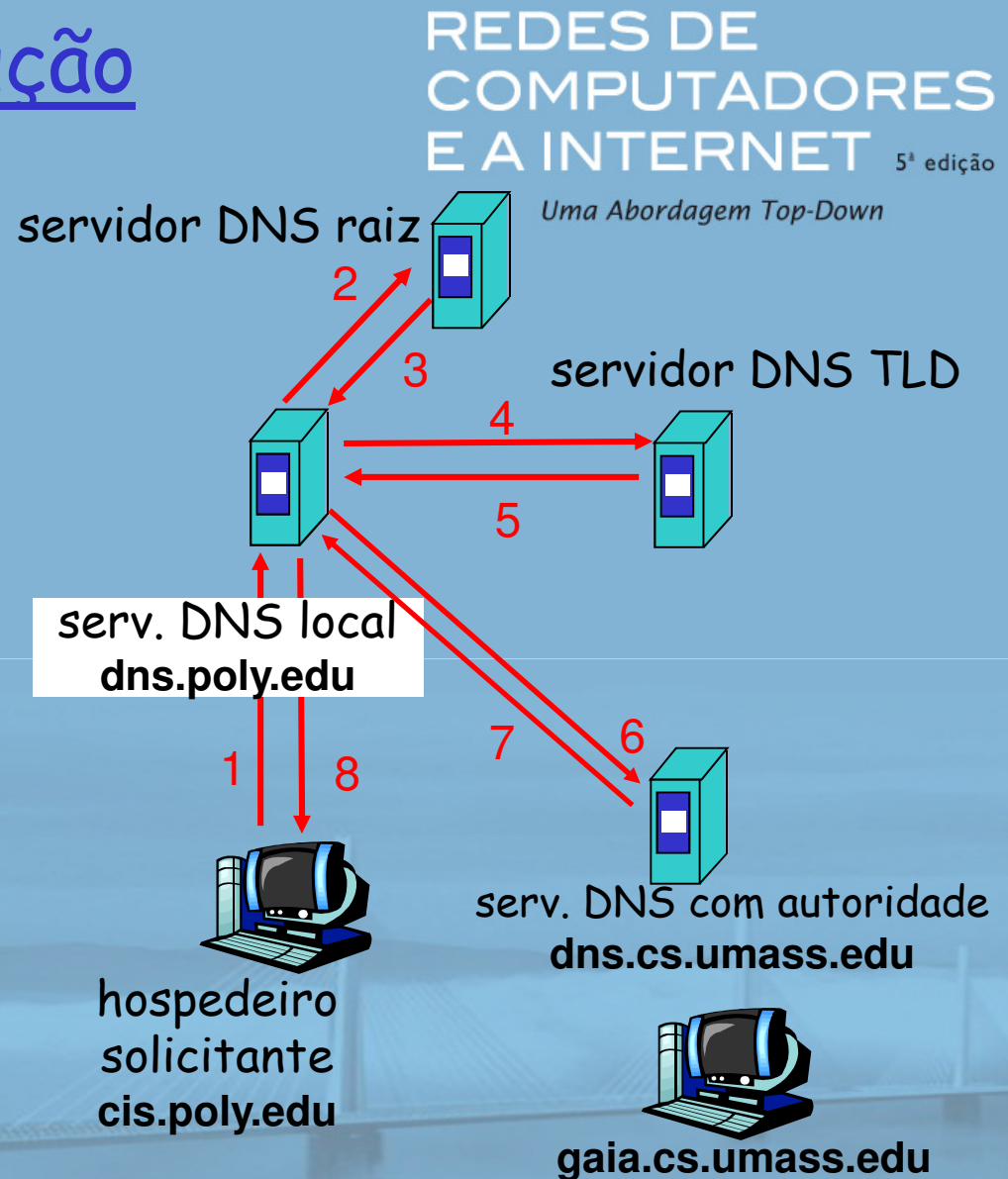
- ❑ não pertence estritamente à hierarquia
- ❑ cada ISP (ISP residencial, empresa, universidade) tem um.
 - ❖ também chamado "servidor de nomes default"
- ❑ quando hospedeiro faz consulta ao DNS, consulta é enviada ao seu servidor DNS local
 - ❖ atua como proxy, encaminha consulta para hierarquia

Exemplo de resolução de nome DNS

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

consulta iterativa:

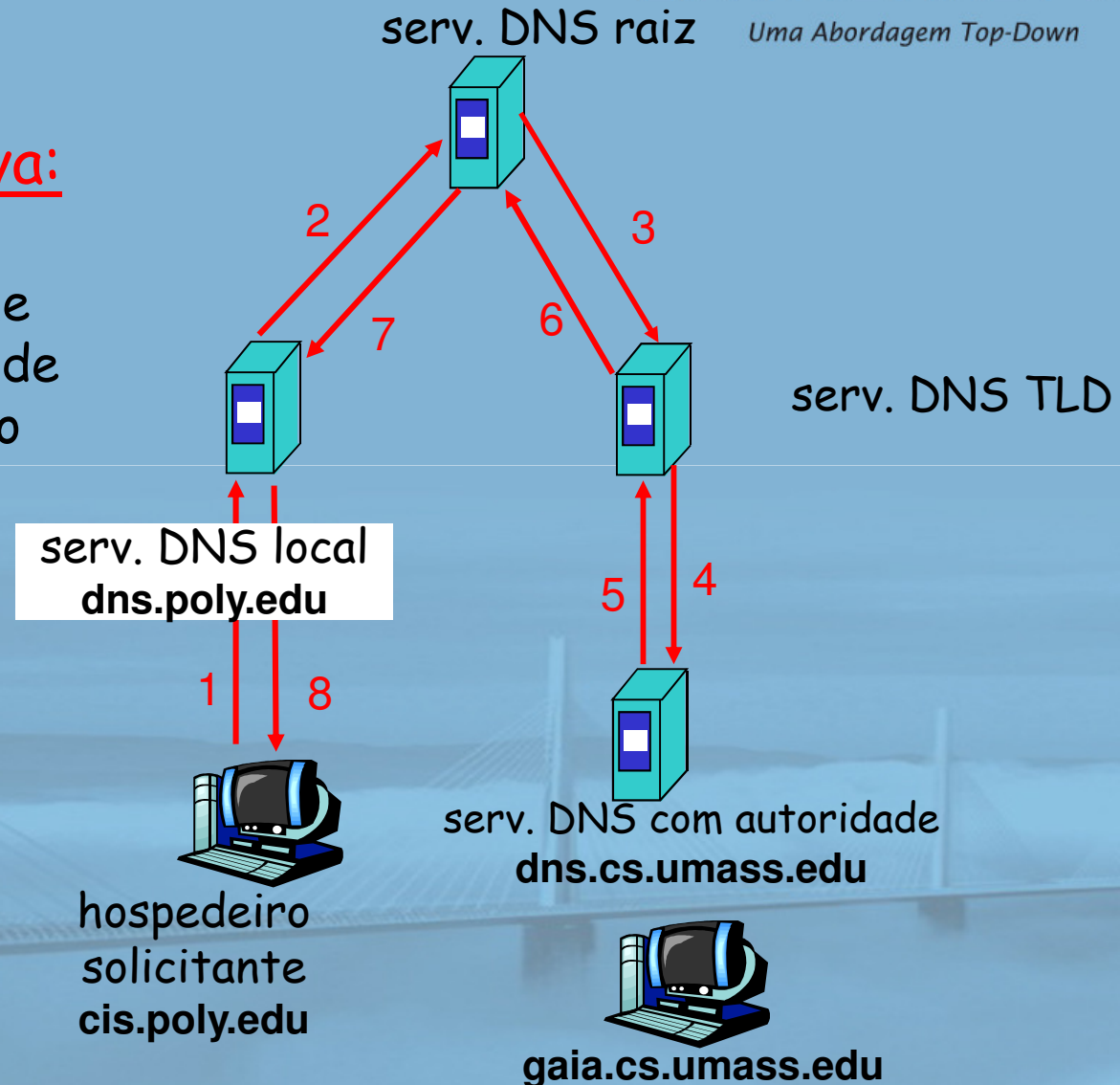
- servidor contactado responde com nome do servidor a contactar
- "não conheço esse nome, mas pergunte a este servidor"



Uma Abordagem Top-Down

consulta recursiva:

- coloca peso da resolução de nome sobre o servidor de nomes contactado
- carga pesada?



DNS: caching e atualização de registros

- ❑ quando (qualquer) servidores de nomes descobre o mapeamento, ele o mantém em *cache*
 - ❖ entradas de cache esgotam um tempo limite (desaparecem) após algum tempo
 - ❖ servidores TLD normalmente são mantidos em caches nos servidores de nomes locais
 - Assim, os servidores de nomes raiz não são consultados com frequência
- ❑ mecanismos de atualização/notificação em projeto na IETF
 - ❖ RFC 2136
 - ❖ <http://www.ietf.org/html.charters/dnsexp-charter.html>

Registros de DNS

DNS: BD distribuído contendo registros de recursos (RR)

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

□ Tipo = A

- ❖ nome é o "hostname"
- ❖ valor é o endereço IP

□ Tipo = NS

- ❖ nome é o domínio (p. e. foo.com)
- ❖ valor é o "hostname" do servidor de nomes com autoridade para este domínio

□ Tipo = CNAME

- ❖ nome é apelido para algum nome "canônico" (real)

www.ibm.com é na realidade

servereast.backup2.ibm.com

- ❖ valor é o nome canônico

□ Tipo = MX

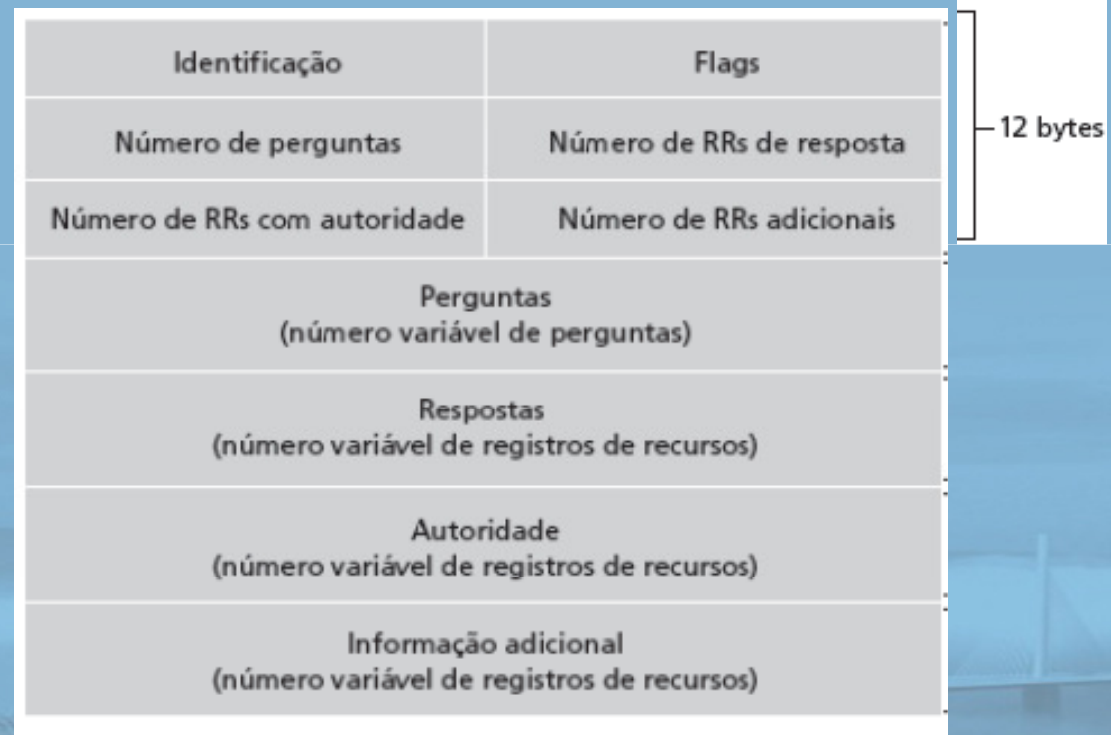
- ❖ valor é o nome do servidor de correio associado ao nome

Protocolo DNS, mensagens

protocolo DNS: mensagens de *consulta/query* e *resposta*, ambas com algum *formato de mensagem*

cabeçalho da
mensagem

- ❑ **identificação**: # de 16 bits para consulta; resposta usa mesmo #
- ❑ **flags**:
 - ❖ consulta ou resposta
 - ❖ recursão desejada
 - ❖ recursão disponível
 - ❖ resposta é com autoridade



Protocolo DNS, mensagens

REDES DE COMPUTADORES E A INTERNET 5ª edição

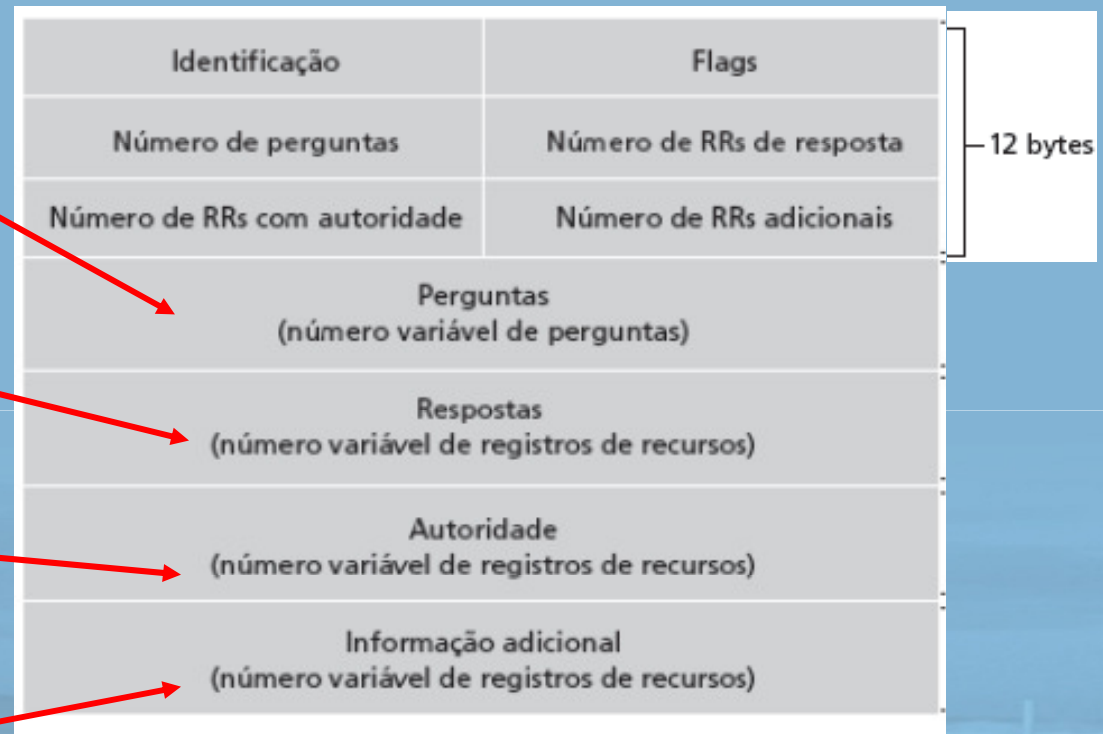
Uma Abordagem Top-Down

campos de nome e tipo
para uma consulta

RRs na resposta
à consulta

registros para servidores
com autoridade

informação adicional
"útil" que pode ser usada



Inserindo registros no DNS

- ❑ exemplo: nova empresa "Network Utopia"
- ❑ registre o nome networkutopia.com na *entidade registradora de DNS* (p. e., Network Solutions)
 - ❖ oferece nomes, endereços IP do servidor de nomes com autoridade (primário e secundário)
 - ❖ entidade insere dois RRs no servidor TLD com:

(networkutopia.com, dns1.networkutopia.com, NS)

(dns1.networkutopia.com, 212.212.212.1, A)

- ❑ crie registro Tipo A do servidor com autoridade para www.networkutopia.com; registro Tipo MX para networkutopia.com
- ❑ *Como as pessoas obtêm o endereço IP do seu site?*

Atacando o DNS

Ataques DDoS

- ❑ Bombardear servidores raiz com tráfego (2002)
 - ❖ Não obteve sucesso
 - ❖ Filtragem de Tráfego
 - ❖ Servidores DNS Locais guarda em cache os Ips dos Servidores TLD
- ❑ Bombardear servidores TLD
 - ❖ Potencialmente mais perigoso

Ataques de Redirecionamento

- ❑ Man-in-middle
 - ❖ Intercepta consultas
- ❑ DNS poisoning (envenenamento)
 - ❖ Envio de respostas falsas para o servidor DNS, que a armazenará em cache

Exploração do DNS para DDoS

- ❑ Envio de consultas com endereço de origem falsificado (spoofed): IP do alvo
- ❑ Requer Amplificação

Exercícios

□ Fixação

- ❖ Kurose, página 130, questão 19

□ Práticos

- ❖ Disponíveis no Acadêmico
- ❖ Upload no Moodle
- ❖ 1 - DNS e o Wireshark
 - Questão de 1-8
 - Salvar trace do Wireshark para questões de 4-8
- ❖ 2 - Whois
- ❖ 3 - Configuração de Servidores no packet tracer