Redes de Computadores

Parte 06 – camada de aplicação – DNS

Prof. Kleber Vieira Cardoso

INSTITUTO DE
INFORMÁTICA
UFG

Tópicos

- Serviços fornecidos pelo DNS
- Visão geral do funcionamento do DNS
- Registros e mensagens do DNS

DNS: *Domain Name System*

Pessoas: muitos identificadores:

- CPF, nome, no. da Identidade, passaporte

Hospedeiros, roteadores da Internet:

- endereço IPv4 (32 bit) - usado para endereçar pacotes
  - De onde vieram e para onde devem ir
- "nome", e.g., ares.inf.ufg.br - usado pelas pessoas

P: como mapear entre nome e endereço IP?

Domain Name System:

- *base de dados distribuída* implementada por uma hierarquia de muitos *servidores de nomes*
- *protocolo de camada de aplicação* permite que hospedeiros e servidores de nomes se comuniquem para *resolver* nomes (tradução endereço/nome)
  - nota: função imprescindível da Internet implementada como protocolo de camada de aplicação
  - complexidade na borda da rede

DNS (cont.)

Serviços DNS

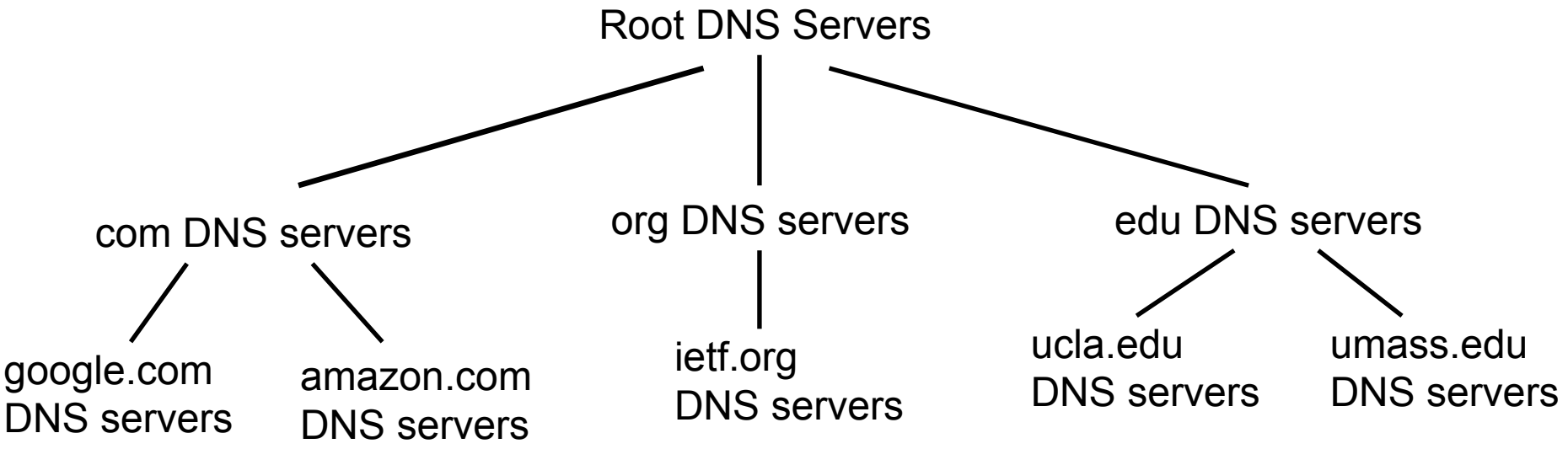
- Tradução de nome de hospedeiro para IP
- Apelidos para hospedeiros (*aliasing*)
  - Nomes canônicos e apelidos
- Apelidos para servidores de *e-mail*
- Distribuição de carga
  - Servidores *Web* replicados: conjunto de endereços IP para um nome

Por que não centralizar o DNS?

- Ponto único de falha
- Volume de tráfego
- Estaria distante para a maioria dos *hosts*
- Manutenção de uma grande base de dados

Não é escalável!

Base de Dados Hierárquica e Distribuída

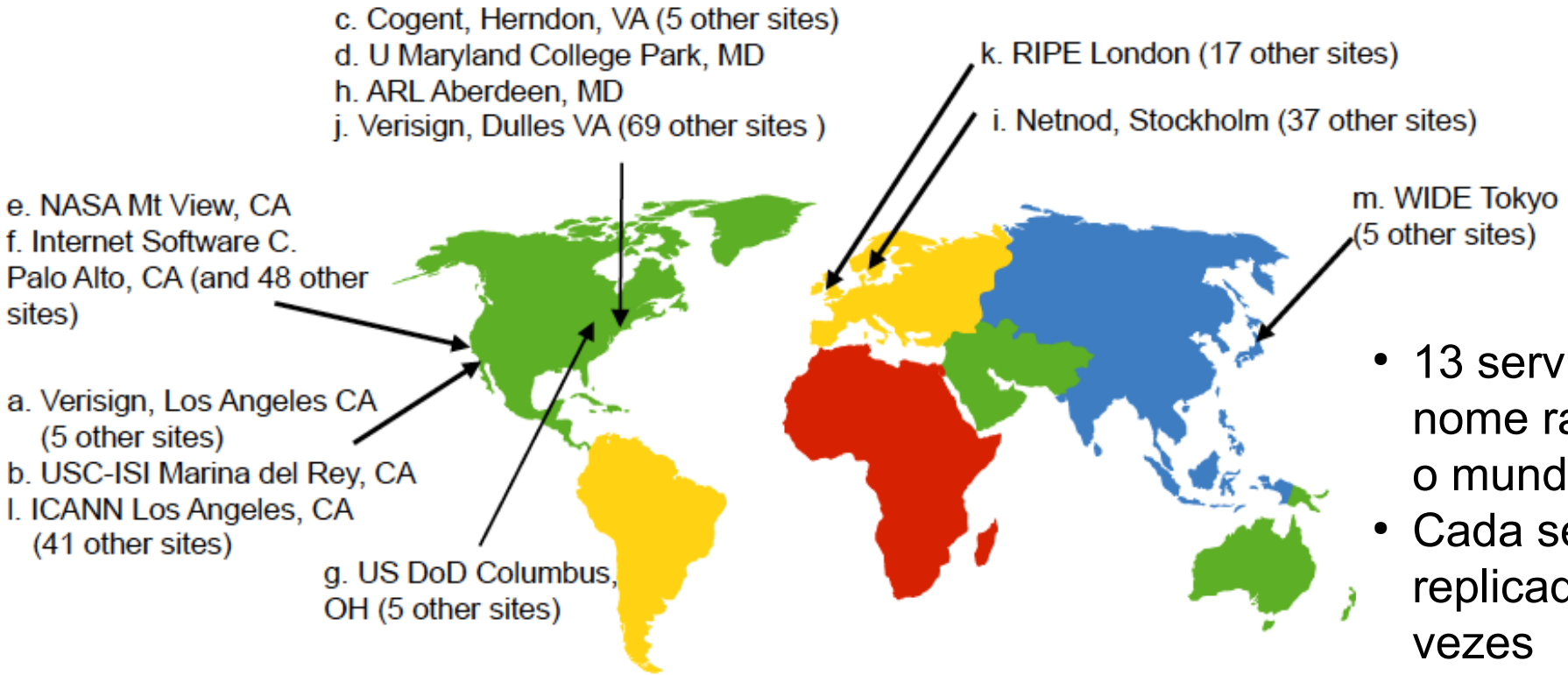


Cliente quer IP para www.amazon.com;

- Cliente consulta um servidor raiz para encontrar um servidor DNS .com
- Cliente consulta servidor DNS .com para obter o servidor DNS para o domínio amazon.com
- Cliente consulta servidor DNS do domínio amazon.com para obter endereço IP de www.amazon.com

DNS: servidores raiz

- Procurado por servidor local que não consegue resolver o nome
  - Servidor raiz responde com o servidor de nomes de domínio de nível mais alto (detalhes a seguir)



- 13 servidores de nome raiz em todo o mundo
- Cada servidor replicado várias vezes

Lista completa: www.root-servers.org

Servidores TLD e oficiais

- Servidores *Top-level domain* (TLD):
  - servidores DNS responsáveis por domínios .com, .org, .net, .edu, ... e todos os domínios de países como .br, .uk, .fr, .ca, .jp. Exemplos:
    - Network Solutions (e +11 empresas) mantêm servidores para domínio .com
    - EDUCAUSE responde pelo domínio .edu
    - Registro.br controla o domínio .br
- Servidores oficiais (ou autorizados):
  - servidores DNS das organizações, provendo mapeamentos oficiais entre nomes de hospedeiros e endereços IP para os servidores da organização (e.g., *Web* e *e-mail*)
  - podem ser mantidos pelas organizações ou pelo provedor de acesso

Mais sobre servidores TLD

- A partir de 2015:
  - *infrastructure top-level domain* (ARPA): .arpa - mantido por questões históricas
  - *generic top-level domains* (gTLD): .com, .gov, .org, .net, ...
    - A partir de 2000, vários outros: .app, .audio, .bike, .biz, .blackfriday, .christmas, .coffee, .farm, .info, .name, ...
  - *sponsored top-level domains* (sTLD): .asia (DotAsia Organisation), .cat (Fundació puntCat), .post (Universal Postal Union)
  - *country-code top-level domains* (ccTLD): .us, .br, .jp, .fr, ...
  - *internationalized country code top-level domains* (IDN ccTLD): ccTLDs em conjuntos de caracteres não-latinos (e.g., Arábico, Cirílico, Hebraico, Chinês)
  - *test top-level domains* (tTLD): testes do IDN, não aparecem na zona raiz

Serviços de nomes no Brasil

Domínios .br registrados até o momento

23/03/2017

3.865.814

Domínios registrados por categorias

Genéricos

CATEGORIAS	QUANTIDADE	%
COM.BR	3.557.451	92,02
ECO.BR	10.337	0,27
EMP.BR	850	0,02
NET.BR	89.468	2,31

» Ver evolução - total genéricos

Pessoas Físicas

CATEGORIAS	QUANTIDADE	%
BLOG.BR	9.285	0,24
FLOG.BR	144	0,00
NOM.BR	1.471	0,04
VLOG.BR	299	0,01
WIKI.BR	501	0,01

» Ver evolução - total de pessoas físicas

Universidades

CATEGORIAS	QUANTIDADE	%
BR	1.206	0,03
EDU.BR	2.739	0,07

» Ver evolução - total de universidades

Pessoas Jurídicas

CATEGORIAS	QUANTIDADE	%
SEM RESTRIÇÃO		
AGR.BR	2.147	0,06

Fonte: https://registro.br/estatisticas.html

Servidor de Nomes Local

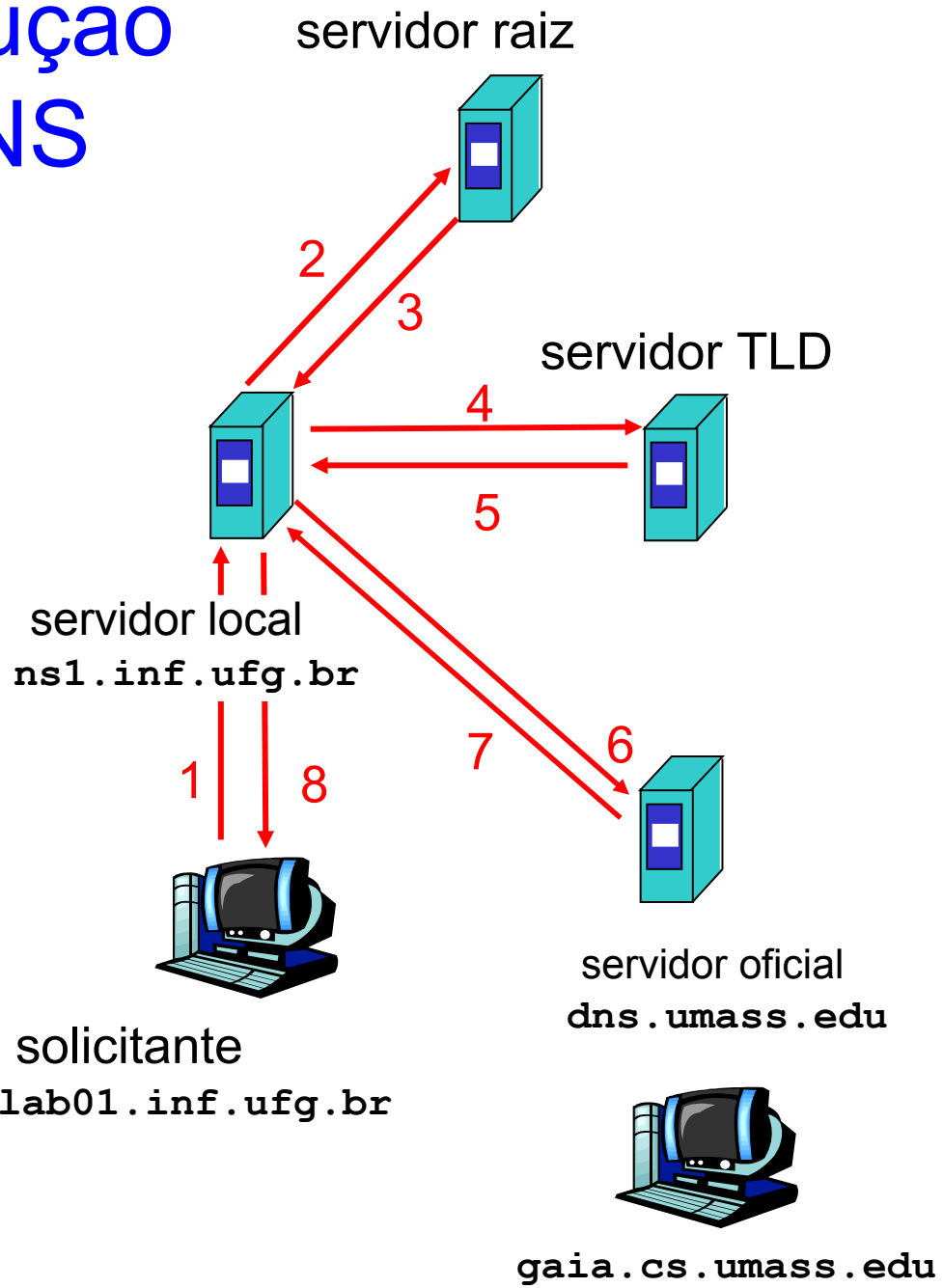
- Não pertence necessariamente à hierarquia
- Cada ISP (ISP residencial, companhia, universidade) possui um
  - Também chamado de “servidor de nomes padrão (*default*)”
- Quando um hospedeiro faz uma consulta DNS, a mesma é enviada para o seu servidor DNS local
  - DNS local atua como um intermediário (*proxy*), enviando consultas para a hierarquia
  - Possui cache das traduções recentes, as quais podem estar desatualizadas

Exemplo de resolução de nome pelo DNS

- Hospedeiro em lab01.inf.ufg.br quer o endereço IP para gaia.cs.umass.edu

Consulta interativa:

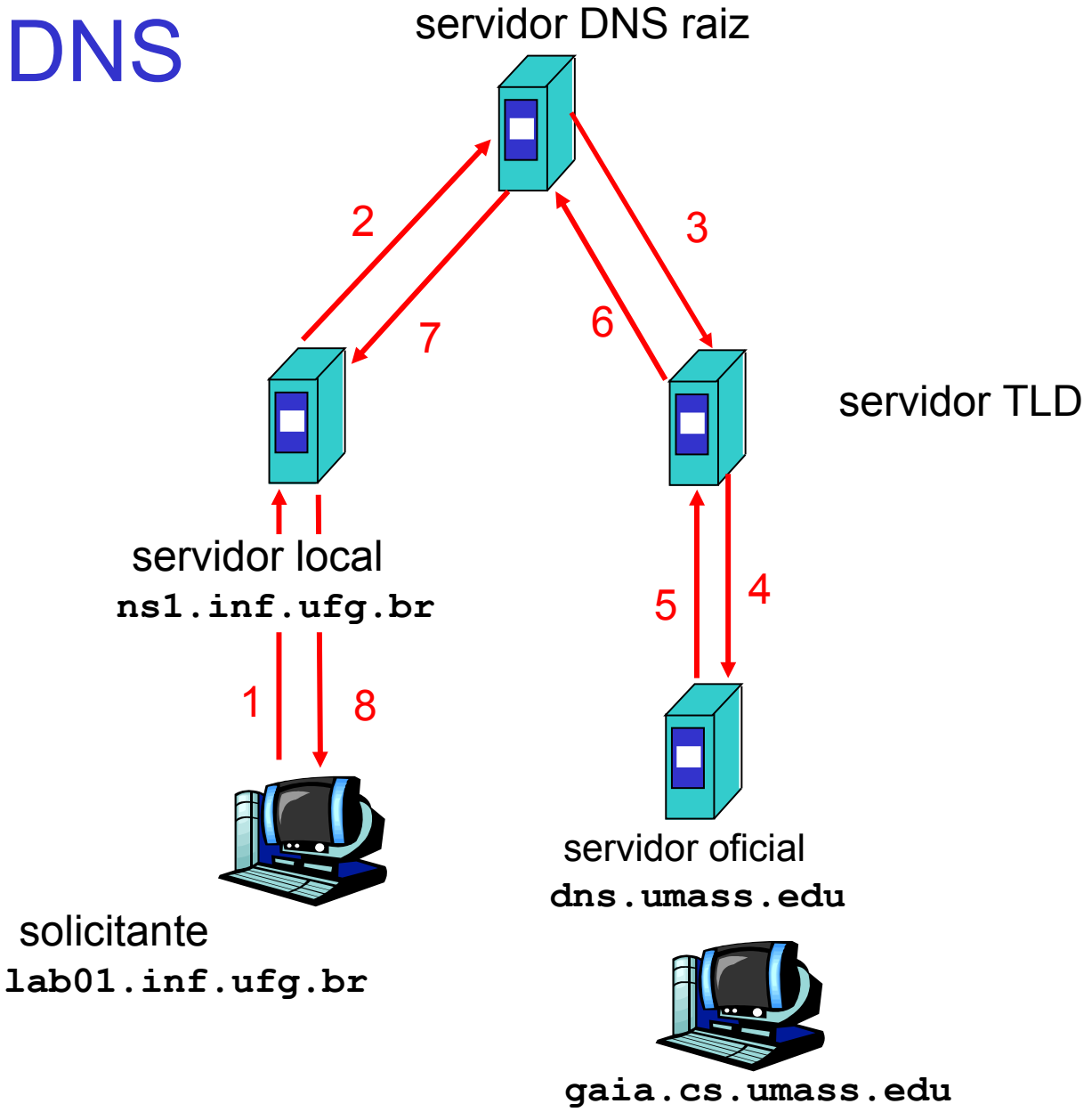
- Servidor consultado responde com o nome de um servidor de contato
  - "Não conheço este nome, mas pergunte para o seguinte servidor"



Exemplo de resolução de nome pelo DNS

Consulta recursiva:

- Transfere a responsabilidade de resolução do nome para o servidor de nomes contatado
- Figura apenas ilustrativa, pois servidor raiz e TLD não oferecem esse tipo de consulta



DNS: uso de cache

- Uma vez que um servidor qualquer aprende um mapeamento, ele o coloca numa *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
    - Servidores raiz acabam não sendo visitados com muita frequência

Registros DNS

DNS: BD distribuído contendo *registros de recursos* (RR)

formato RR: **(nome, valor, tipo, sobrevida)**

- Tipo=A
  - **nome** é nome de hospedeiro
  - **valor** é o seu endereço IP
- Tipo=NS
  - **nome** é domínio (ex.: foo.com.br)
  - **valor** é endereço IP (ou nome) de servidor oficial de nomes para este domínio
- Tipo=CNAME
  - **nome** é nome alternativo (alias) para algum nome "canônico" (verdadeiro)
  - **valor** é o nome canônico
- Tipo=MX
  - **nome** é domínio
  - **valor** é nome (ou endereço IP) do servidor de correio para este domínio

DNS: protocolo e mensagens

Protocolo DNS: mensagens de *requisição* e *resposta*, ambas com o mesmo *formato*

Cabeçalho da mensagem

identificação: ID de 16 bit para requisição, resposta ao requisição usa mesmo ID

flags:

- requisição ou resposta
- recursão desejada
- recursão permitida
- resposta é oficial

DNS: protocolo e mensagens

Inserindo registros no DNS

- Exemplo: a empresa “Network Utopia” é criada
- Registra o nome netutopia.com.br em uma entidade registradora (e.g., Registro.br)
  - Tem de prover para a registradora os nomes e endereços IP dos servidores DNS oficiais (primário e secundário)
  - Registradora insere dois RRs no servidor TLD .br para cada servidor:

```
(netutopia.com.br, dns1.netutopia.com.br, NS)
(dns1.netutopia.com.br, 211.211.211.1, A)
(netutopia.com.br, dns2.netutopia.com.br, NS)
(dns2.netutopia.com.br, 212.212.212.22, A)
```

- Põe no servidor oficial um registro do tipo A para www.netutopia.com.br e um registro do tipo MX para netutopia.com.br

```
(www.netutopia.com.br, 211.211.211.10, A)
(netutopia.com.br, 212.212.212.20, MX)
```

Ataques a DNS

- DNS é um alvo importante porque afeta vários serviços (e.g., Web, e-mail, e-commerce)

- Ataques DDoS
  - Servidores raiz
    - Sem sucesso efetivo até o momento, graças a: filtragem de pacotes e servidores locais manterem IPs de servidores TLD em cache
  - Servidores TLD
    - Potencialmente, mais perigoso

- Ataques de redirecionamento
  - *Man-in-the-middle*: interceptar requisições e falsificar respostas
  - Envenenamento de DNS: atualizar cache do servidor com informações falsas
- Explorando o DNS para DDoS
  - Envia requisições com origem alterada: alvo IP
  - Exige amplificação, i.e., resposta maior que requisição

Exercícios

1) Sobre DNS, indique V (verdadeiro) ou F (falso) para as afirmações que seguem.

a) Através da cache do servidor DNS local de uma instituição é possível determinar (pelo menos de maneira aproximada) quais são os servidores Web fora da instituição que são os mais populares entre os usuários dessa instituição.

b) Apenas um usuário privilegiado (ou seja, um administrador de sistemas/rede) consegue determinar se houve um provável acesso a um determinado site da Web nos últimos segundos, pois é necessário ter acesso ao servidor DNS local.

c) É possível definir um cenário (extremo) em que o uso de um servidor DNS local leva a desempenho pior que realizar todas as consultas (para tradução de nome para IP) por conta própria ou utilizar um servidor DNS de outra instituição.

d) O fato de um administrador de uma instituição configurar em seus servidores oficiais um valor muito baixo (por exemplo, 1 segundo) para o TTL (*Time To Live*) das entradas de sua base de dados do DNS não tem influência sobre o desempenho das caches de servidores DNS locais de outras instituições.

Exercícios

2) É possível que o servidor Web e o servidor de correio (e-mail) de uma organização tenham exatamente o mesmo apelido para um nome de hospedeiro (por exemplo, foo.com)?

3) Qual é o tipo de RR que contém o nome de hospedeiro do servidor de correio?