Diretoria de Educação e Tecnologia da Informação

Análise e Desenvolvimento de Sistemas

INSTITUTO FEDERAL
RIO GRANDE DO NORTE

REDE FEDERAL DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
1909-2009

Administração de Sistemas Operacionais

SERVIÇO DE RESOLUÇÃO DE NOMES

DNS

Prof. Bruno Pereira Pontes
tenpontes@gmail.com

Objetivos

- Conhecer as características, funcionalidades e componentes do serviço de resolução de nomes (Domain Name Service – DNS);
- Capacitar o aluno a projetar, instalar, configurar e disponibilizar o DNS;
- Incentivar a utilização correta e bem ajustada dos serviços de produção;
- Fomentar a utilização de boas práticas objetivando a oferta de serviços adequados, com ótima disponibilidade e a um custo razoável;

Sumário I

- Introdução;
- Fundamentos do DNS;
- Representação dos nomes;
- Delegação, Zona e Domínio;
- Servidores DNS Básicos e Atuais;
- Cenários Típicos;

Sumário II

- Métodos de resolução de nomes;
- Mapeamento reverso;
- Vulnerabilidades do DNS;
- O Banco de dados DNS;
- Registros de Recursos;
- Comandos em arquivos de zonas;
- Servidores DNS;

Introdução

- A necessidade de associar nomes a endereços surgiu durante o desenvolvimento inicial da Internet, na então ARPAnet;
- A ARPAnet era uma rede de pesquisa que interligava sobretudo as universidades americanas;
- Com a adoção do protocolo TCP/IP (anos 80), a ARPAnet cresceu fenomenalmente;

Introdução

- O modelo usado para a translação dos nomes em endereços tornou-se inviável:
  - Um computador central mantinha um arquivo HOSTS.TXT;
  - Alterações em qualquer parte da rede era informada ao gerenciadores do computador central (via e-mail);
  - Cada host na rede tinha que atualizar os seus dados com base no HOSTS.TXT atualizado (via FTP)

Fundamentos do DNS

- O Sistema de Nomes de Domínio é um banco de dados distribuído onde cada servidor detém um ”pedaço” do Banco;
- Isso permite um controle local dos segmentos do banco de dados global, embora os dados em cada segmento estejam disponíveis em toda a rede através de um esquema cliente-servidor.
  - Servidor – Name Server
  - Cliente – Resolver (Envia Queries para o Server)

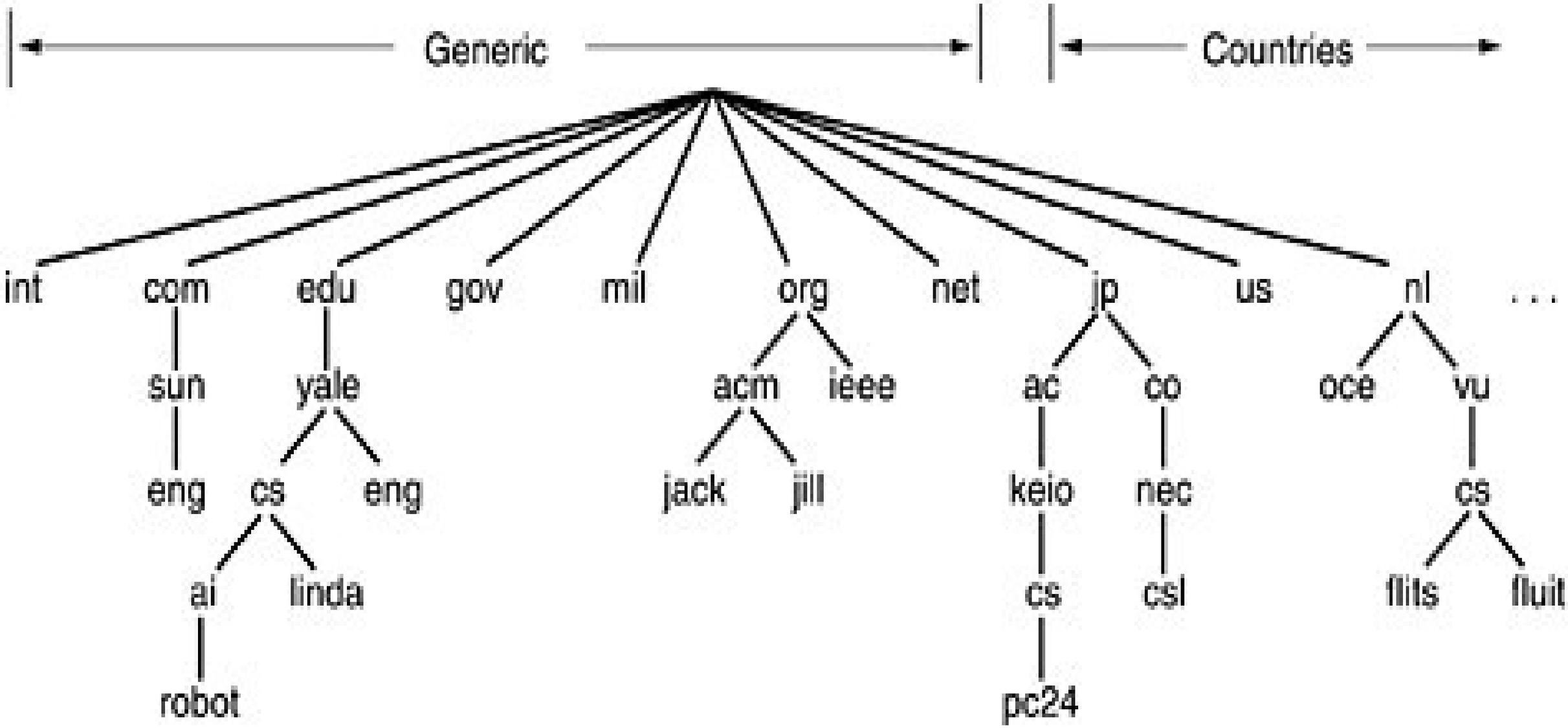
Fundamentos do DNS

- A distribuicao da base DNS nao segue nenhuma divisão geográfica ou de hardware;
- Dois tipos de resolução são possíveis com o DNS:
  - **Nome → IP**
  - **IP → Nome** (mapeamento reverso)
- Mapeamento reverso é necessário a dois fins:
  - Representar endereços numa forma mais simples de serem lidos por seres humanos;
  - Auxiliar alguns sistemas de autorização;

Fundamentos do DNS

- O DNS associa nomes a endereços IP de forma hierárquica (árvore inversa de domínios);
- O nó mais alto é o RAIZ e é representado por ".";
- A hierarquia do DNS possibilida delegação de autoridade na busca pelo IP/nome, o que viabiliza o gerenciamento do sistema e assegura unicidade;
- 1984 – Descrito pelas RFCs 882 e 883
- 1987 – Redefinição pelas RFCs 1034 e 1035
- Por padrão, utiliza TCP e UDP com a porta 53

Fundamentos do DNS



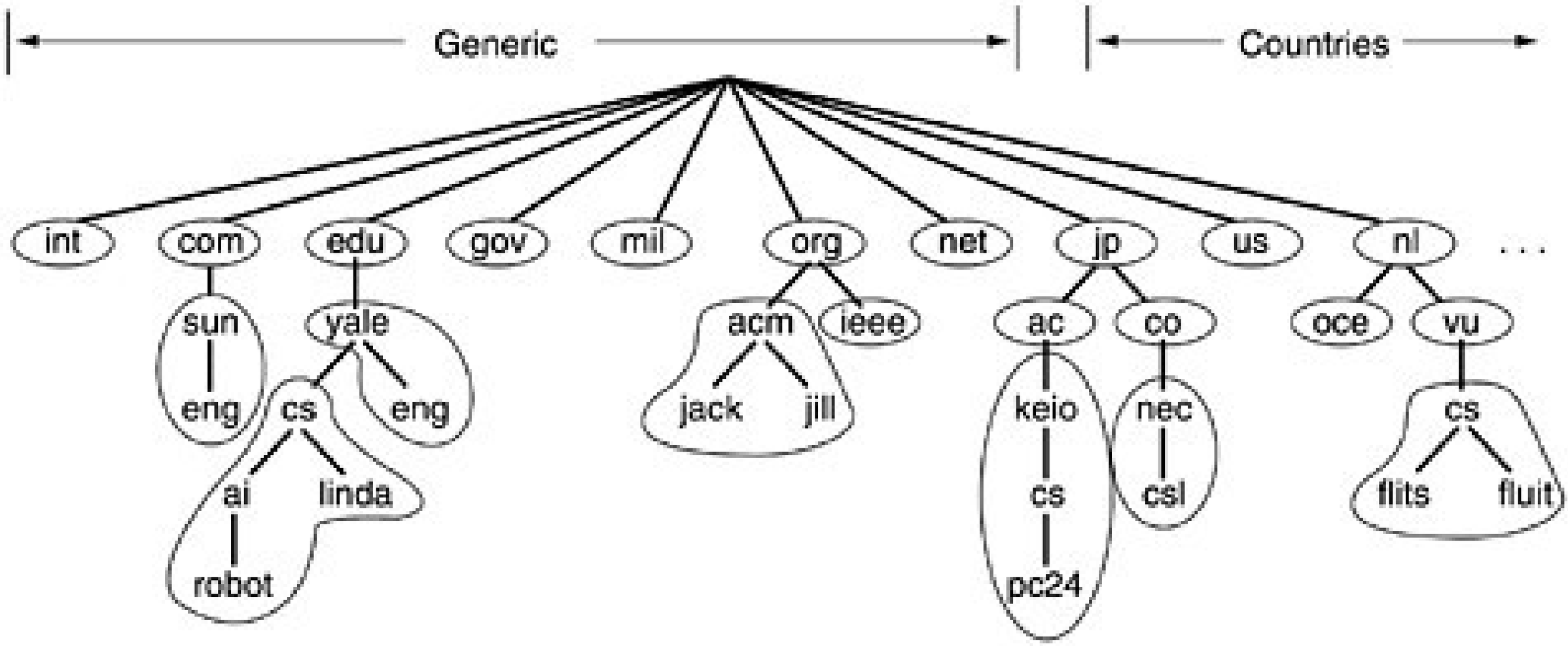
Representação dos nomes

- A representação pode ser relativa ou absoluta (FQDN);
- Na representação relativa, os nomes têm de ser interpretados de acordo com o domínio onde está localizado. Geralmente identificam máquinas;
  - saturno, www, servidor1
- Nome de Domínio Totalmente Qualificado (FQDN):
  - saturno.uol.com.br, alecrim.ifrn.edu.br
- Um Nome pode representar um domínio ou uma máquina;

Delegação

- Um único servidor de nomes poderia conter o banco de dados DNS inteiro e responder a todas as consultas referentes ao banco;
- Esse servidor ficaria tão sobrecarregado que seria inútil;
- Caso esse servidor viesse a ficar fora do ar, toda a Internet seria atingida;
- O Banco de Dados é quebrado em vários subdomínios que são delegados a vários Servidores;

Delegação

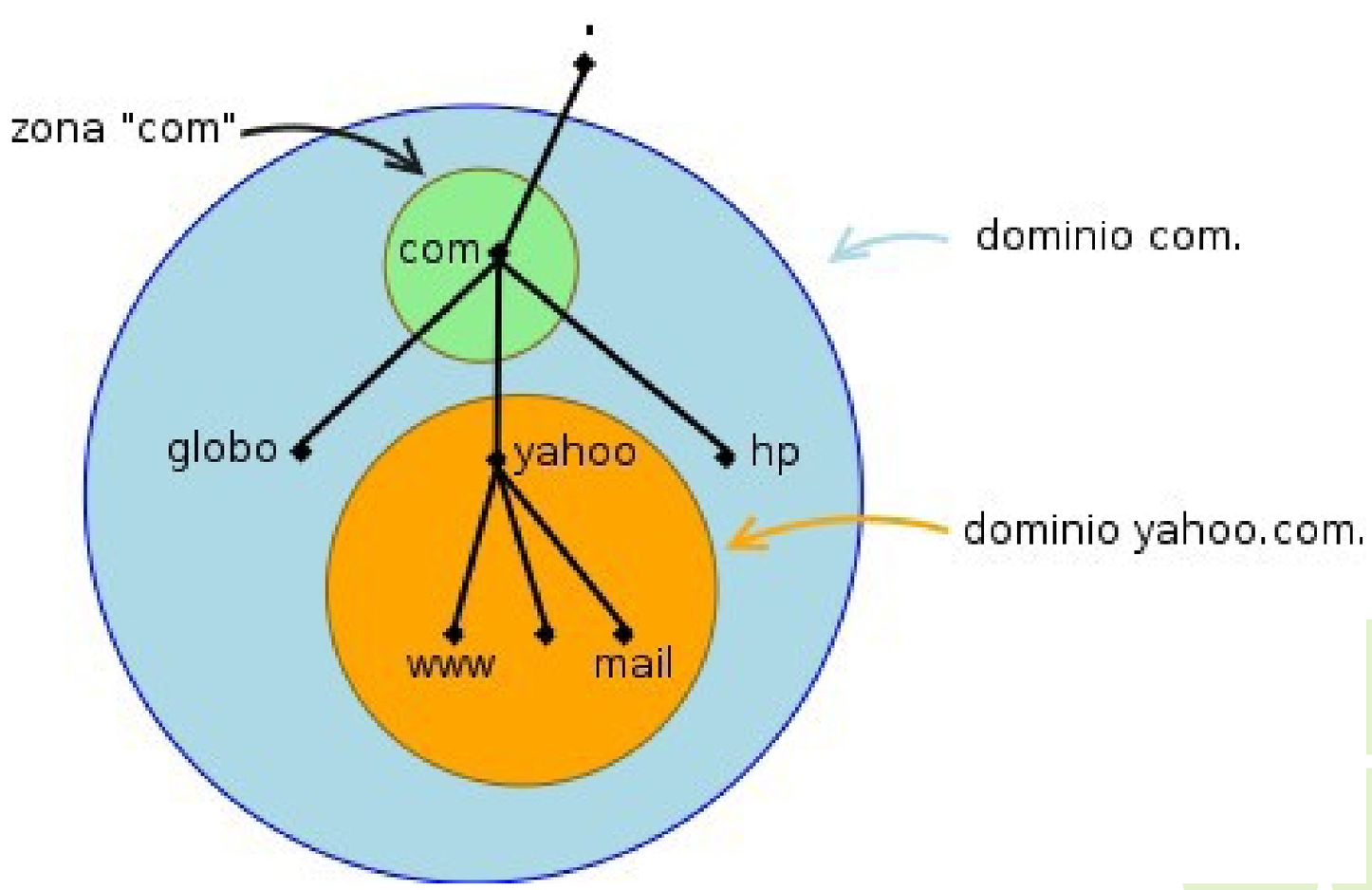

Generic
Countries
int
com
edu
gov
mil
org
net
jp
us
nl
. . .
sun
yale
acm
ieee
ac
co
oce
vu
eng
cs
eng
jack
jill
keio
nec
cs
flits
fluit
ai
linda
cs
csl
robot
pc24

Zona X Domínio

- Conceitos parecidos;
- A zona delimita que informações de um domínio são delegadas a um servidor;
- A abrangência depende da autoridade de um servidor;
- Domínio significa todos os ramos abaixo de um nó;
- Zona significa a parte de um ou mais ramos que está delegada a um servidor;

Zona X Domínio

- O(s) sevidor(es) DNS em cada domínio é (são) responsável(is) por zonas específicas e não por todo o domínio;
- Aqui o servidor DNS da zona **com** delega autoridade aos subdomínios;



Servidores DNS Básicos

- No princípio definiu-se duas configurações de Servidores DNS:
  - **Primary (*Master*):** lê dados das zonas de um arquivo em seu *host;*
  - **Secondary (*Slave*):** obtém dados das zonas de outro servidor ***master*** de nomes que tem autoridade sobre aquela zona;
- Ambos os tipos de servidores têm autoridade sobre a zona em questão;

Servidores DNS Básicos

- Na inicialização ocorre a transf. de zona do *master* para o *slave;*
- Os arquivos de cada zona só são transferidos novamente quando os mesmos mudam no master;
- Vantagens de se ter mais de um servidor de nome por zona são:
  - Redundância;
  - Distribuição de carga;
  - Garantir que cada host na zona tenha um servidor de nome por perto;

Servidores DNS Atuais

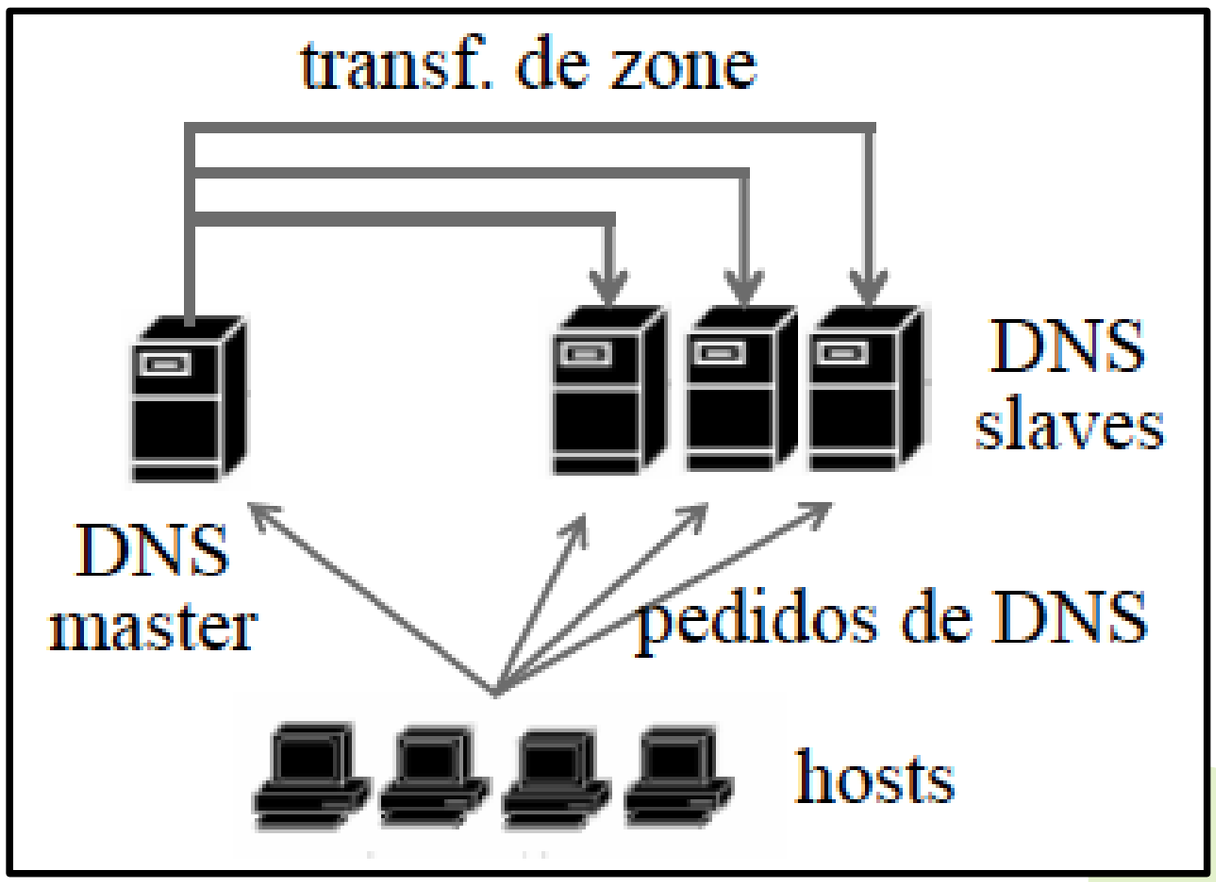
- **Master (Primary):** Recebe autoridade sobre uma zona a ele delegada. Normalmente o *master* notifica os *slaves* sobre mudanças em suas zonas (SERIAL!!!);
- **Slave (Secondary):** Tem autoridade sobre a zona do master mas copia os dados das zonas do master (periodicamente ou quando notificado);
- **Caching (hint):** Contêm "apenas" a zona dos TLDs (domínio "."). Armazena (cache) zonas do *master* e as usa nas novas solicitações até que o período limite (TTL) seja alcançado;

Servidores DNS Atuais

- **Forwarding** (Proxy, Client, Remote): Retransmite todas a solicitações a correspondentes servidores *master;*
- **Stealth** (DMZ or Split): Um servidor que não aparece em nenhum "registro NS" por privacidade;
- **Authoritative Only:** Somente responde à questionamentos das zonas sobre as quais o mesmo tem autoridade;

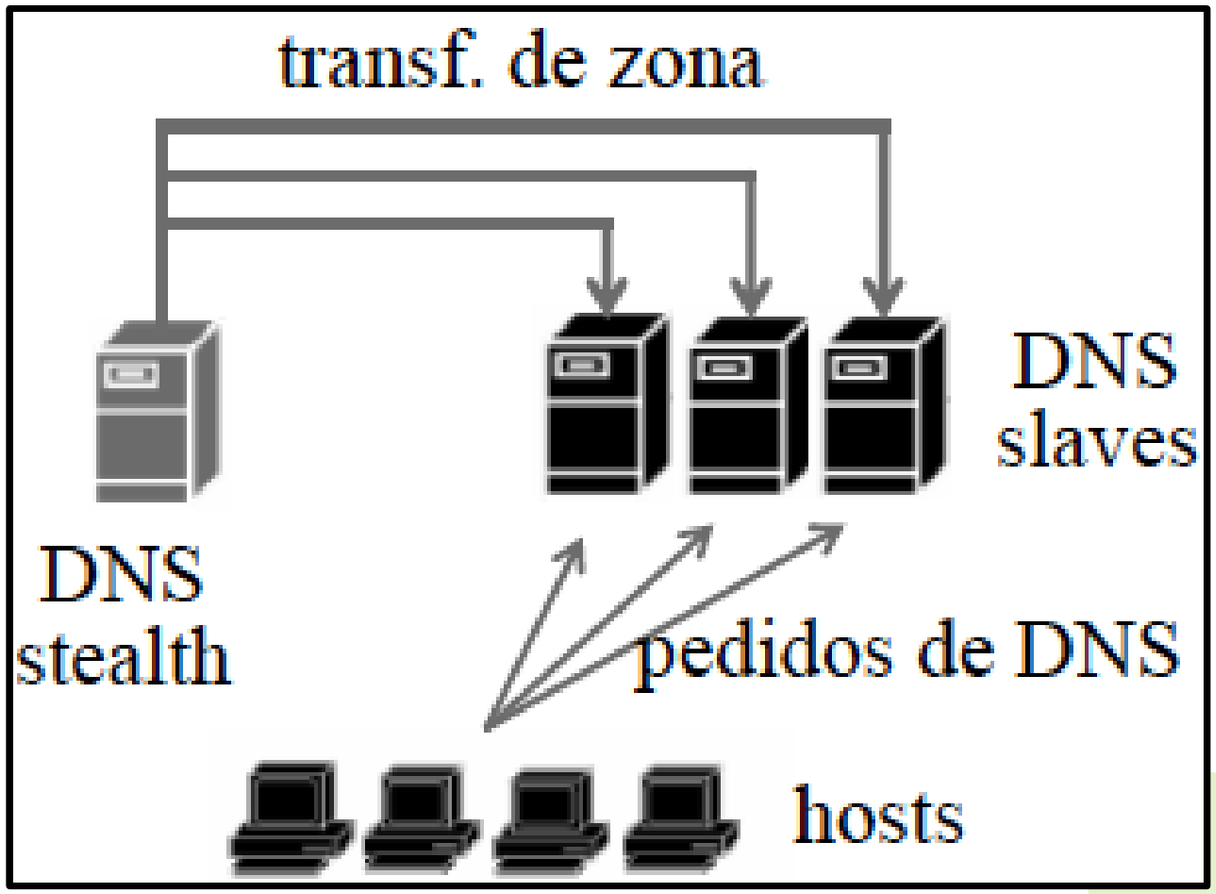
Cenários Típicos

- **Um DNS *master* e vários Slaves:**
  - Carga é balanceada
  - Aumento de redundância



Cenários Típicos

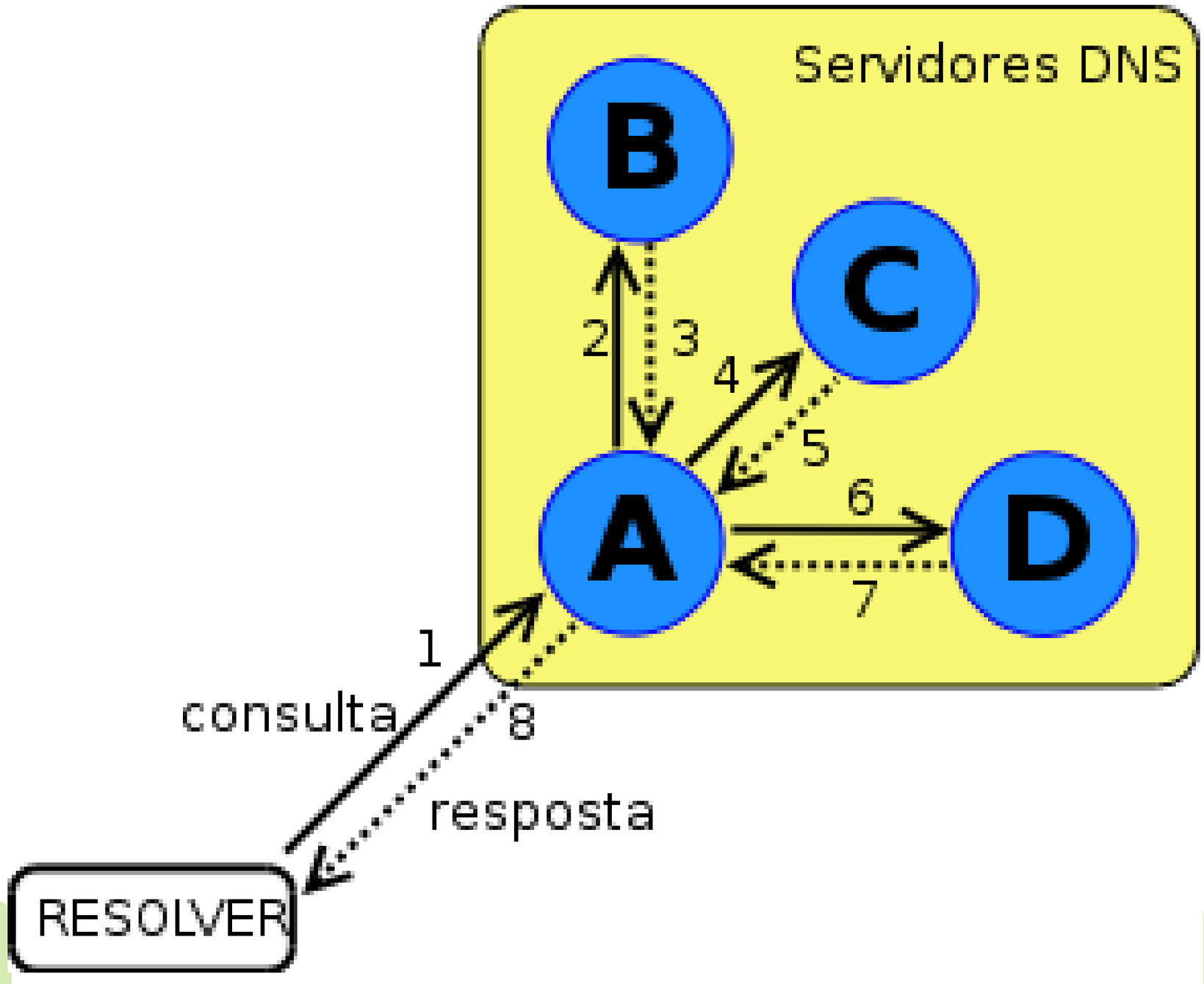
- **Um DNS *stealth* e vários slaves:**
  - Todas as resoluções são realizadas nos *slaves;*
  - O *master stealth* pode ser alterado sem que o sistema seja interrompido;
  - Privacidade do stealth



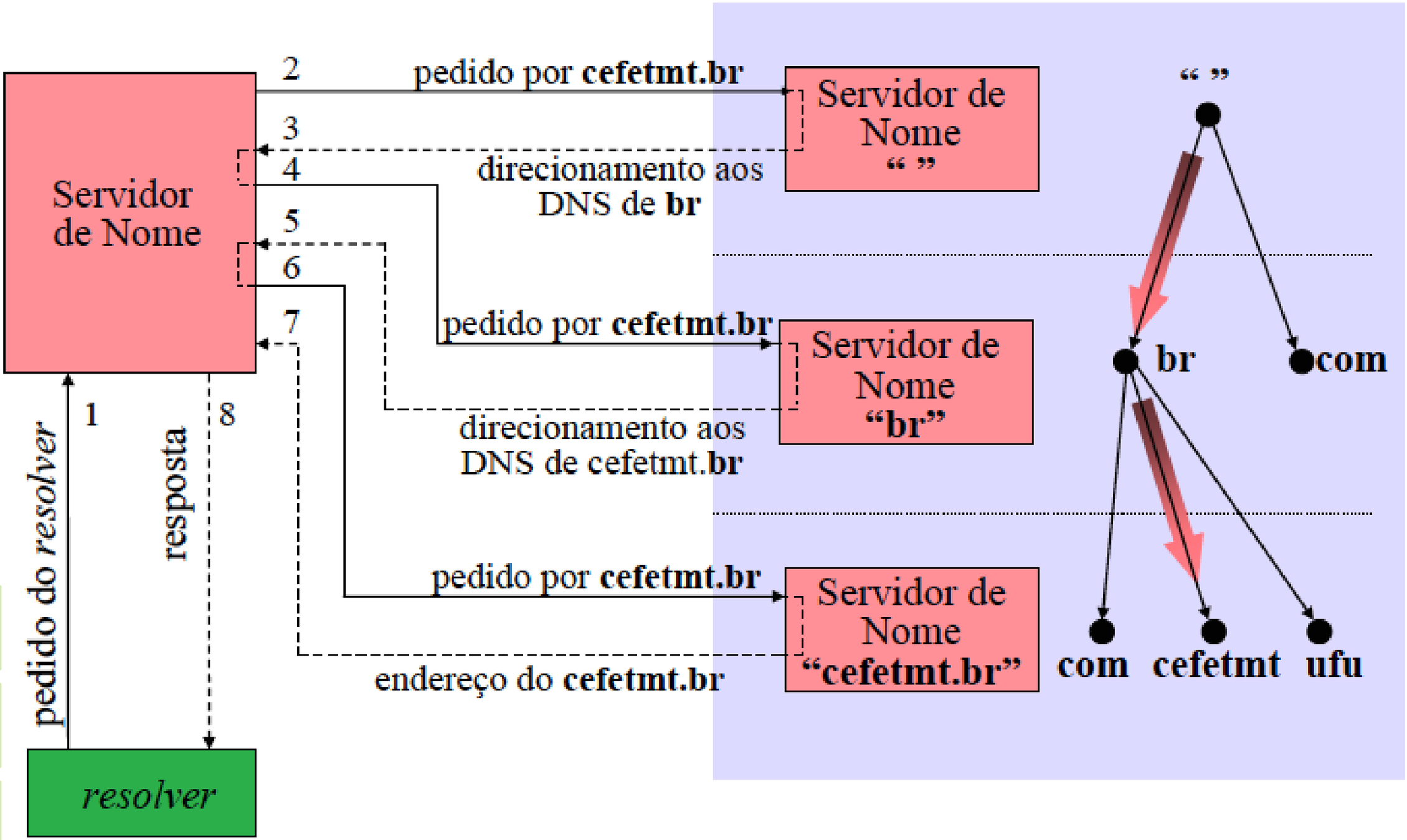
Métodos de resolução de nomes

- Um servidor DNS pode receber muitas solicitações de resolução sobre domínios para os quais o mesmo não tem responsabilidade. Nesses casos, dois comportamentos são possíveis:
  - **Recursivo:** Ao receber requisições de resolução de nomes, faz requisições para os servidores autoritativos e conforme a resposta recebida dos mesmos continua a realizar requisições para outros servidores autoritativos até obter a resposta satisfatória;
  - **Iterativo:** Ao receber requisições de resolução de nome, responde um endereço caso possua, uma referência caso conheça o caminho da resolução ou uma negação caso não conheça;

Métodos de resolução de nomes



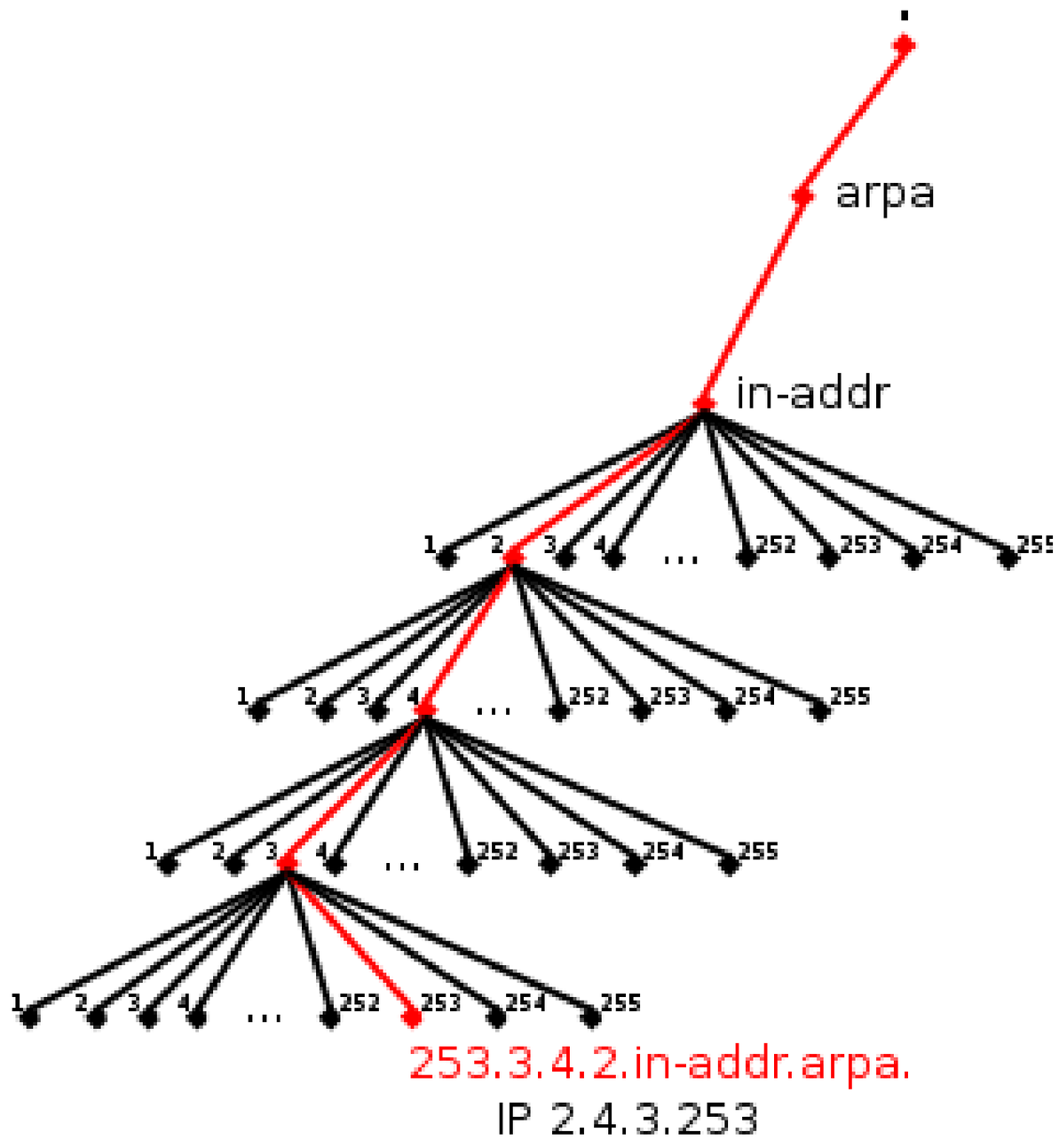
Métodos de resolução de nomes



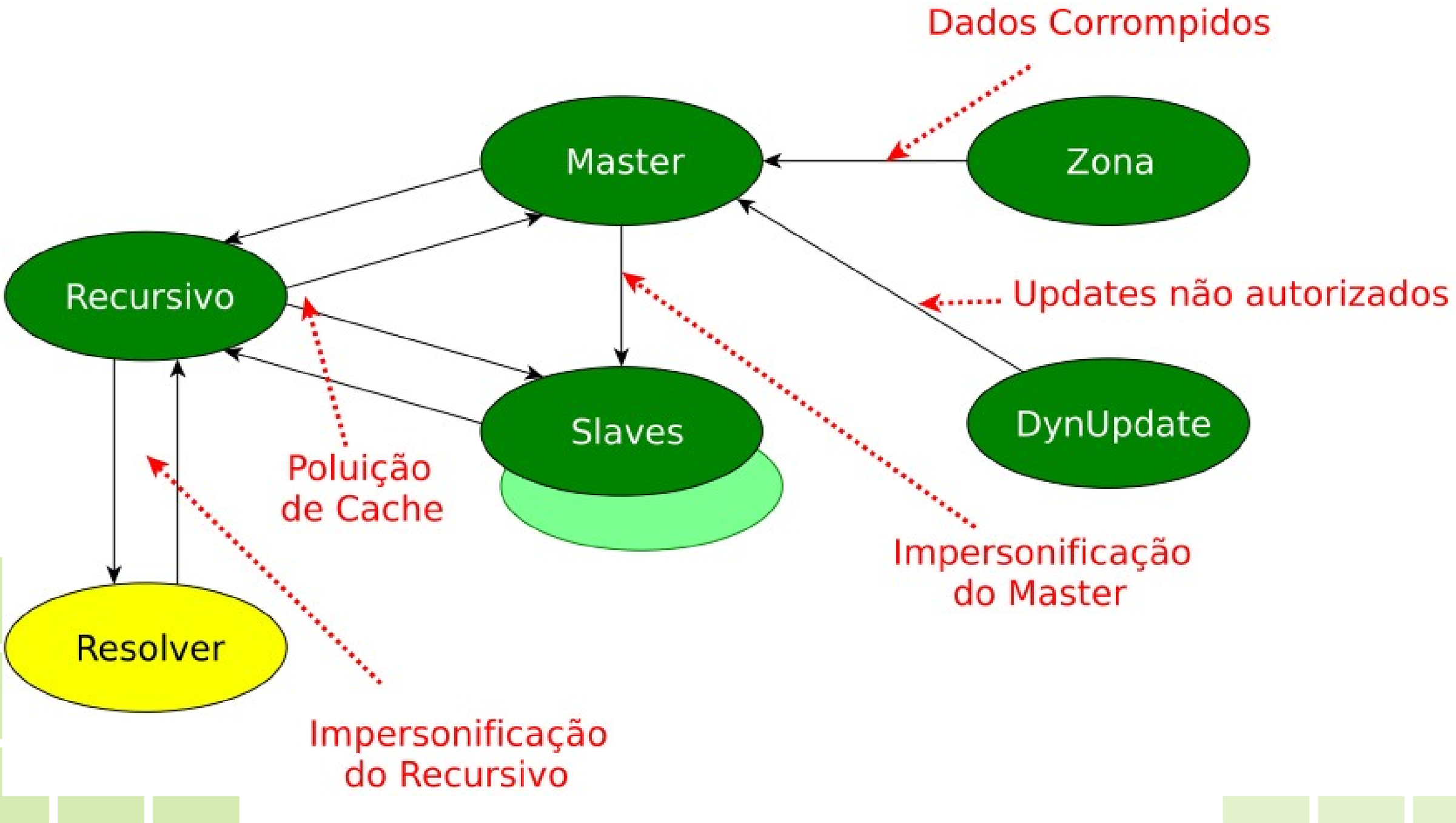
Mapeamento reverso

- O mapeamento reverso ou mapeamento de endereço para nome é feito através de um espaço de nomes específico:
  - in-addr.arpa.
- O domínio in-addr.arpa possui 256 nós que representam o primeiro octeto de um número ip:
  - Possui apenas 4 níveis, referentes ao 4 octetos de um número ip e a leitura na árvore in-addr.arpa é o contrário do resto da árvore DNS;

Mapeamento reverso



Vulnerabilidades do DNS



O Banco de dados DNS

- O banco de dados DNS de um domínio é um conjunto de arquivos de texto mantidos pelo administrador no servidor de nomes mestre do domínio;
- Esses arquivos de textos são normalmente chamados de arquivos de zonas;
- Arquivos de zonas contém dois tipos de entradas: comandos do analisador sintático e os chamados registros de recurso (RRs);
- Os RRs são os dados que descrevem o(s) domínio(s) e apenas eles realmente fazem parte do banco de dados;
- Os comandos do analisador sintático simplesmente fornecem algumas maneiras reduzidas para introduzir registros;

Registros de Recursos

- Os dados associados com os nomes de domínio estão contidos em Resource Records ou RRs (Registro de Recursos);
- São divididos em classes e tipos;
- Atualmente existe uma grande variedade de tipos;
- Um registro de recurso é uma tupla de cinco campos;
- Os campos são separados por espaços em branco e podem conter os caracteres especiais mostrados abaixo:

Caractere	Significado
;	Introduz um comentário
@	O nome da zona atual

Registros de Recursos

[Name]	[Time_to_live]	[Class]	Type	Value

- **Name:** identifica a entidade (um host ou domínio) que o registro descreve. Pode ser relativo ou absoluto. Os absolutos devem terminar com um . (ponto);
- **Time_to_live:** fornece uma indicação do tempo de vida do registro em cache;
- **Class:** especifica o tipo de rede. No caso de informações relacionadas à Internet, ele é sempre IN;
- **Type:** informa qual é o tipo do registro;
- **Value:** Pode ser um número, um nome de domínio ou um string ASCII. A semântica dependerá do tipo de registro;

Registros de Recursos

Tipo	Significado	Valor
SOA	Início de autoridade	Parâmetros para essa zona
A	Endereço IP de um host	Inteiro de 32 bits
MX	Troca de mensagens de correio	Prioridade, servidor disposto a aceitar correio *eletrônico*
NS	Servidor de nomes	Nome de um servidor para este domínio
CNAME	Nome canônico (sinônimo) do nome oficial do host	Nome oficial do host
PTR	Ponteiro	Nome alternativo de um endereço IP (Reverso)
HINFO	Descrição de host	CPU e sistema operacional em ASCII
TXT	Texto	Texto ASCII não interpretado

Registros de Recursos

- Parâmetros do RR SOA:
  - Serial: O número de revisão do arquivo de zona. Tem efeito na transferência de zona;
  - Refresh: O tempo, em segundos, que um servidor DNS secundário espera antes de consultar a origem da zona para tentar renová-la;
  - Retry: O tempo, em segundos, que um servidor secundário espera antes de tentar novamente uma transferência de zona falha;
  - Expire: O tempo, em segundos, antes que o servidor secundário pare de responder às consultas depois de transcorrido um intervalo de atualização no qual a zona não foi renovada ou atualizada;
  - Minimum: Tempo de sobrevida de respostas negativas que são armazenadas em cache;

Registros de Recursos

- Observações importantes a respeito do RR CNAME:
  - Registros MX, NS, CNAME, ou SOA só devem se referir a um registro A;
  - RRs referindo-se a um CNAME podem ocasionar problemas de buscas e carga extra na rede;

Comandos em arquivos de zona

- Os comandos são apenas diretivas do analisador de sintaxe que ajudam a torna o manutenção dos arquivos de zona mais legível e mais fácil de manter;
- Os comandos influenciam a maneira como o analisador de sintaxe interpreta os registros subsequentes;
- Os comandos têm obrigatoriamente que começar na primeira coluna e cada um deles deve ocupar uma linha exclusiva;

Comandos em arquivos de zona

- Existem três comandos principais:
  - $ORIGIN *nomeDeDomínio*
  - $INCLUDE *nomeDeArquivo [origem]*
  - $TTL *padrãottl*
- Os comandos $ORIGIN e $TTL são especificados nas RFCs e devem ser entendidos por todos os servidores de nomes;

Servidores DNS

	Autoritativo	Recursivo	Caching	DNSSEC[a]	DNSSEC bis[b]	NSEC3[c]	TSIG	IPv6
ANS	√			√	√		√	√
BIND	√	√	√	√	√		√	√
CNS		√	√	√	√		√	√
djbdns	√	√	√					√
IPControl	√	√	√	√	√		√	√
IPM DNS	√	√	√	√	√		√	√
MaraDNS	√	√	√					?
Microsoft DNS	√	√	√	√			√	√
NSD	√			√	√	√	√	√
PowerDNS	√	√	√					√
Unbound		√	√		√	√		√
VitalQIP	√	√	√	√	√		?	√

[a] Versão antiga do protocolo não suportada pelo Registro.br

[b] Versão atual do protocolo

[c] Versão aprimorada do protocolo DNSSEC também suportada pelo Registro.br

Servidores DNS

	BSD[a]	Solaris	Linux	Windows	MAC OS X
ANS	√	√	√	?	?
BIND	√	√	√	√	√
CNS	√	√	√	?	?
djbdns	√	√	√		√
IPControl		√	√	√	
IPM DNS	√	√	√		√
MaraDNS	√	√	√	√[b]	√
Microsoft DNS				√	
NSD	√	√	√		√
PowerDNS	√	√	√	√	√[c]
Unbound	√	√	√		√
VitalQIP		√	√	√	

[a] Sistema compatível com a norma POSIX assim como outros clones do Unix.

[b] Apenas nas versões mais recentes do sistema operacional

[c] Software em versão Beta

Servidores DNS

	Criador	Código Aberto	Grátis
ANS	Nominum		
BIND	Internet System Consortium	√	√
CNS	Nominum	√	
djbdns	Daniel J. Bernstein	√	√
IPControl	INS		
IPM DNS	EfficientIP		
MaraDNS	Sam Trenholme	√	√
Microsoft DNS	Microsoft		
NSD	NLnet Labs	√	√
Unbound	NLnet Labs	√	√
PowerDNS	PowerDNS.com / Bert Hubert	√	√
VitalQIP	Lucent Technologies		

Bibliografia

- FERREIRA, R. E., Guia do Administrador do Sistema, Novatec Editora, 2003
- MORIMOTO, C. E., Redes e Servidores Linux: Guia Prático - GDH Press e Sul Editores, 2008
- NEMETH, E., SYNDER, G. e HEIN, T. R., Manual Completo do Linux: Guia do Administrador, Pearson, 2007;
- TANENBAUM, S. A., Redes de Computadores, 4ª Edição, Campus.