



Campus Taguatinga
Coordenação de Informática
Manutenção e Suporte



Sistemas Operacionais Aplicados a Redes

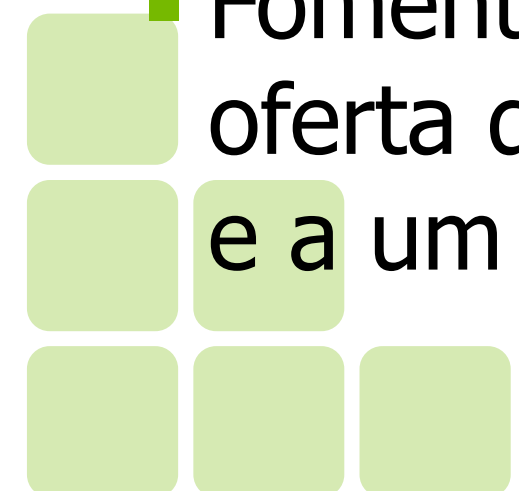
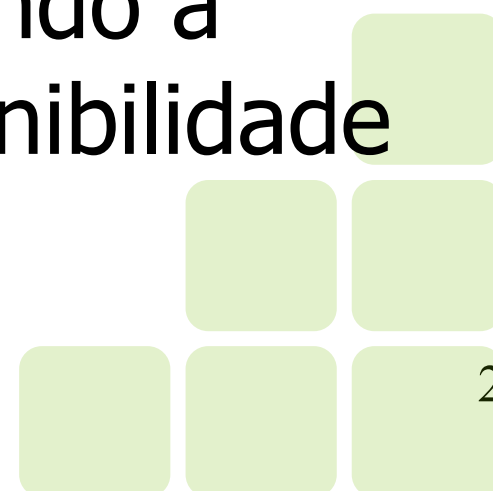
SERVIÇO DE RESOLUÇÃO DE NOMES (DNS)

Prof. Bruno Pereira Pontes
bruno.pontes@ifb.edu.br

Carga Horária: 80 horas-aulas

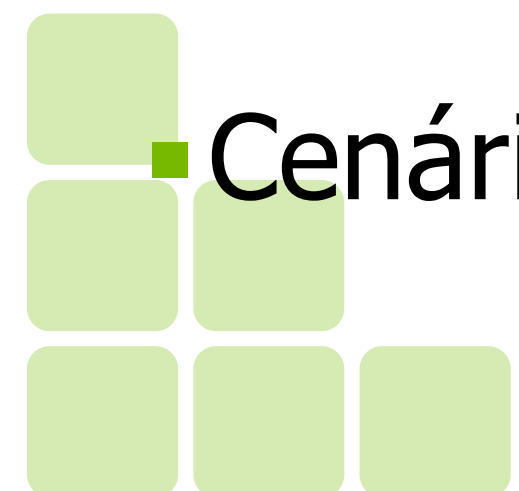
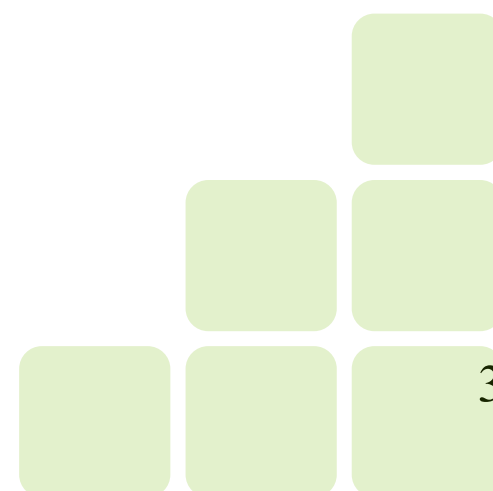


Objetivos

- 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;
- Vulnerabilidades do DNS;
- 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.



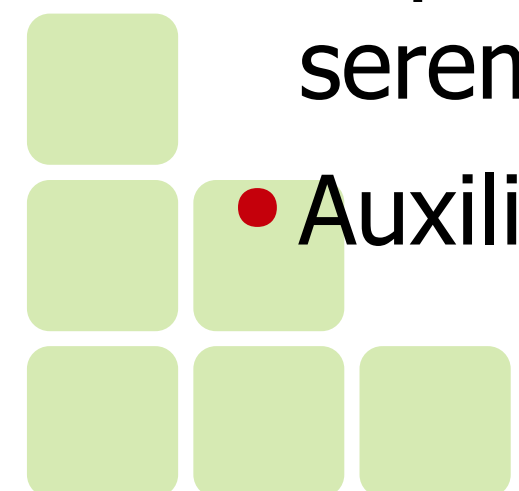
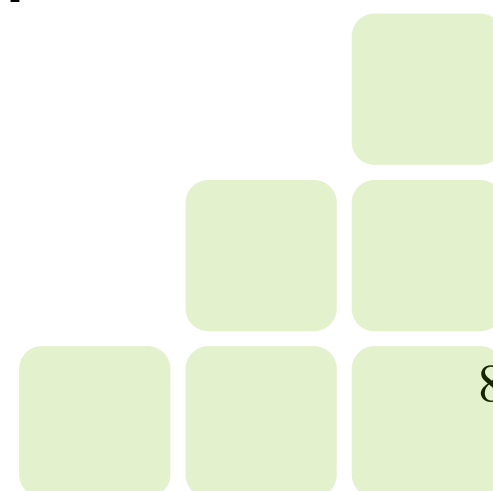
- Servidor – Name Server

- Cliente – Resolver (Envia Queries para o Server)



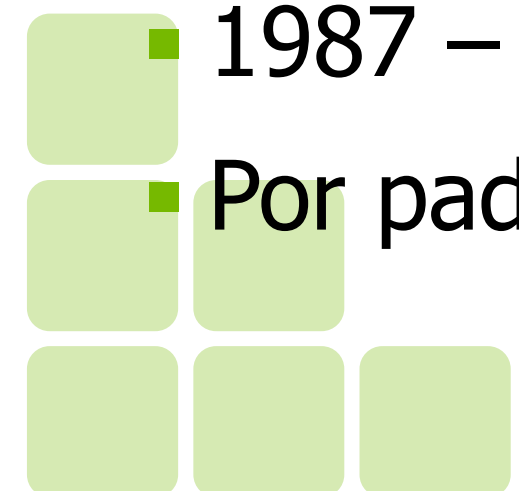
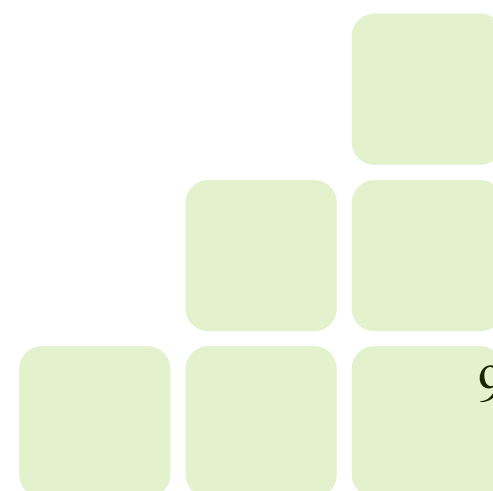


Fundamentos do DNS

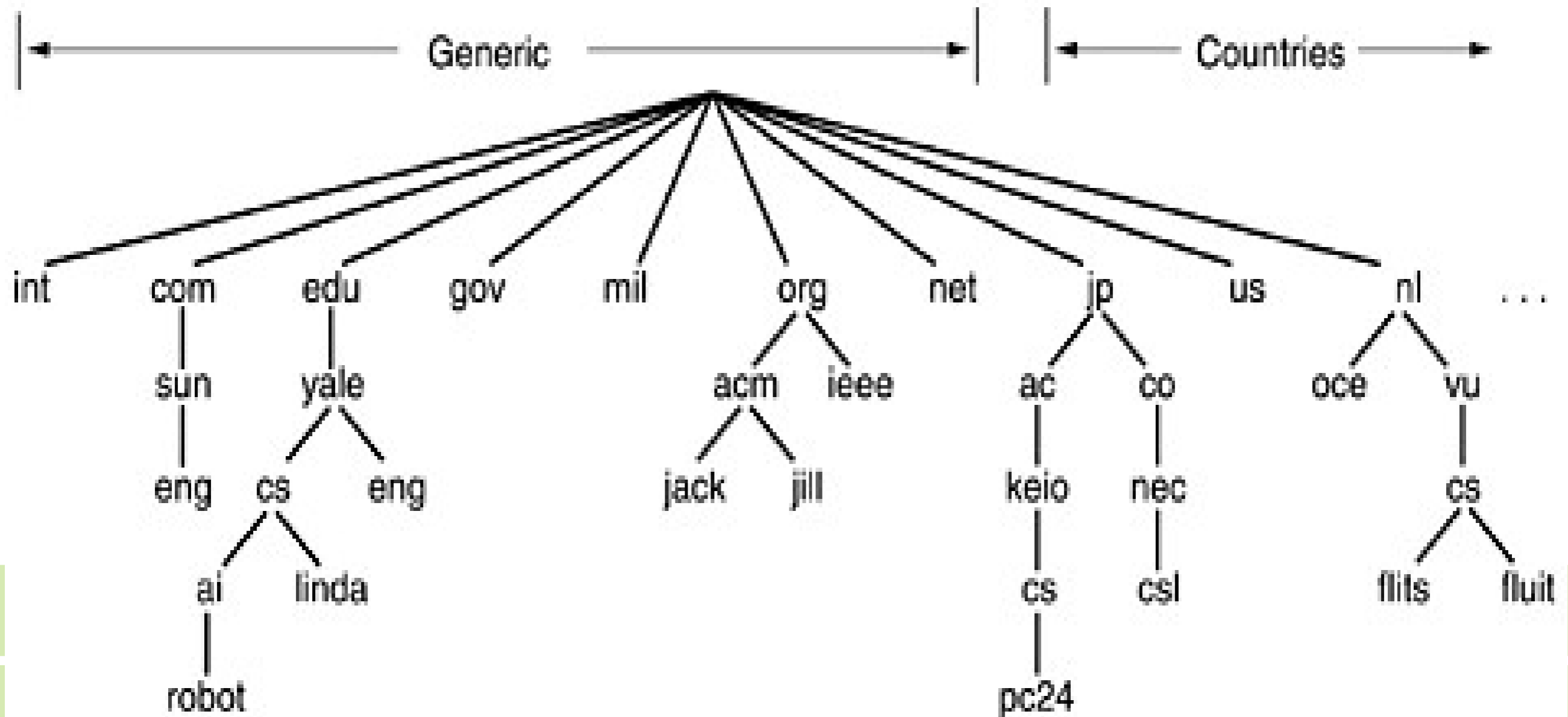
- A distribuição da base DNS não segue nenhuma divisão geográfica ou de hardware;
 - Dois tipos de resolução são possíveis com o DNS:
 - **Nome → IP**
 - **IP → Nome** (mapeamento reverso)
 - Mapeamento reverso é necessário a dois fins:
 - Representar endereços numa forma mais simples de serem lidos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

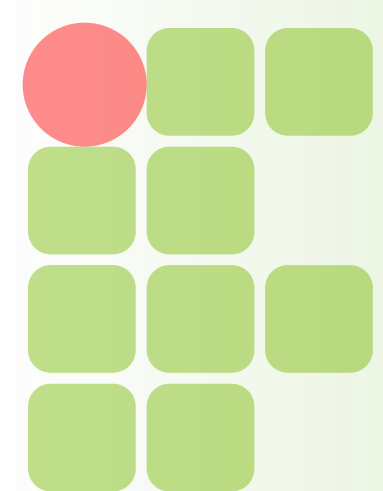


Fundamentos do DNS

- 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 possibilita 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

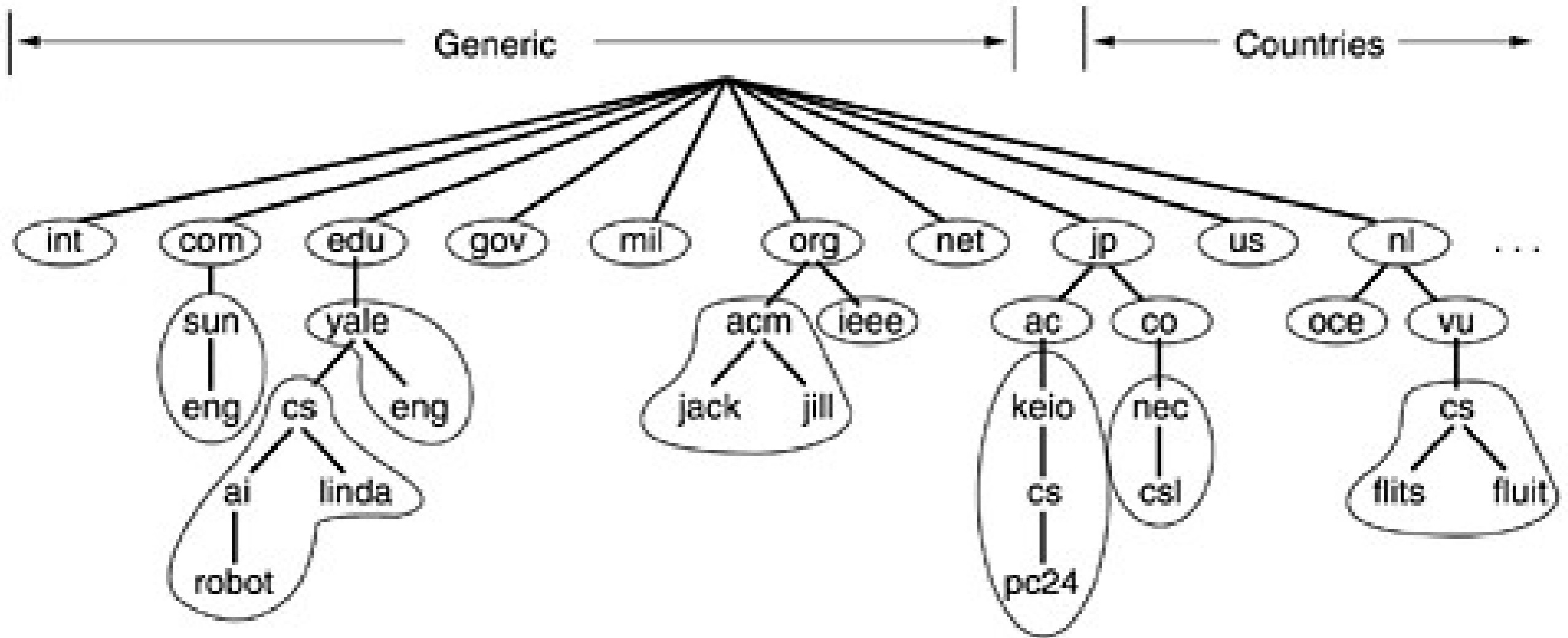
- A representação pode ser relativa ou absoluta (FQDN);
- Na representação relativa, os nomes têm de ser interpretados de acordo com o domínio onde está localizado. Geralmente identificam máquinas;
 - saturno, www, servidor1
- Nome de Domínio Totalmente Qualificado (FQDN):
 - saturno.uol.com.br, alecrim.ifrn.edu.br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



Delegação


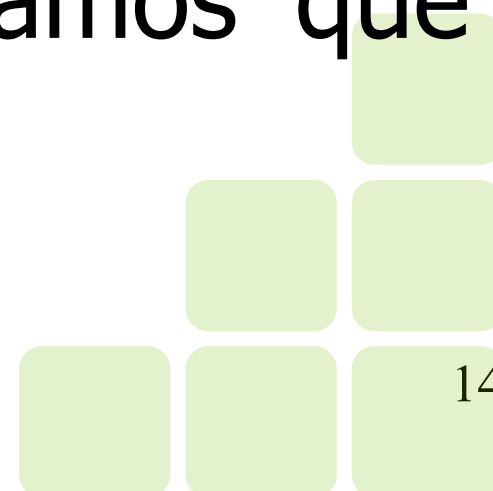
- Um único servidor de nomes poderia conter o banco de dados DNS inteiro e responder a todas as consultas referentes ao banco;
- Esse servidor ficaria tão sobrecarregado que seria inútil;
- Caso esse servidor viesse a ficar fora do ar, toda a Internet seria atingida;
- O Banco de Dados é quebrado em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

Delegação



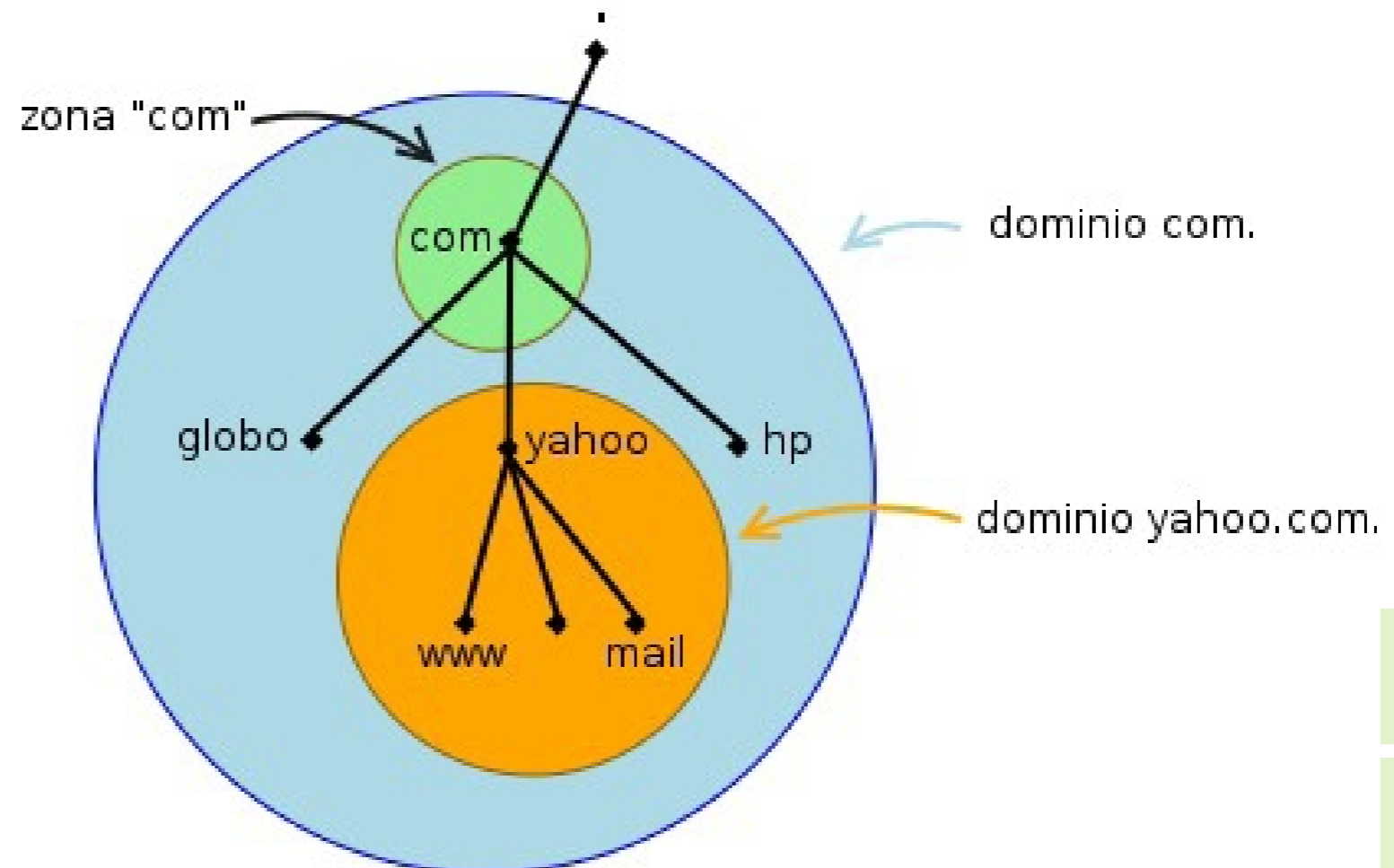


Zona X Domínio

- 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) servidor(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;



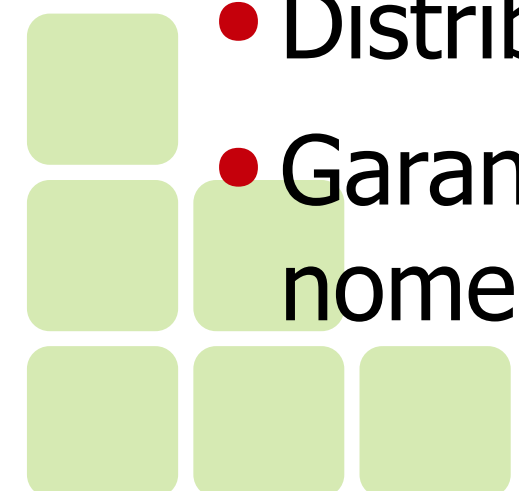
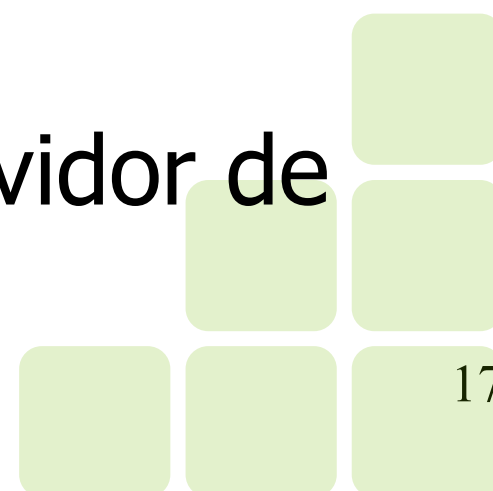


Servidores DNS Básicos

- 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;

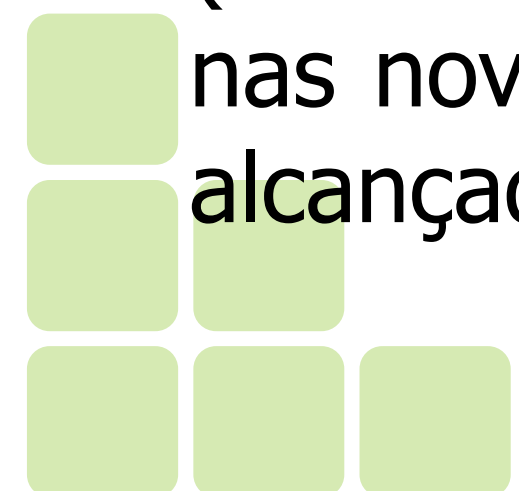
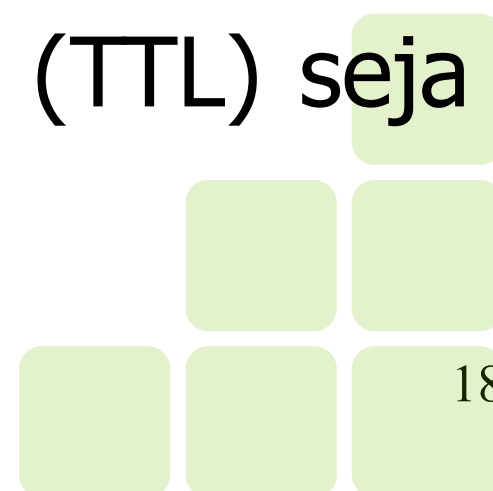


Servidores DNS Básicos

- 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;
- 
- 



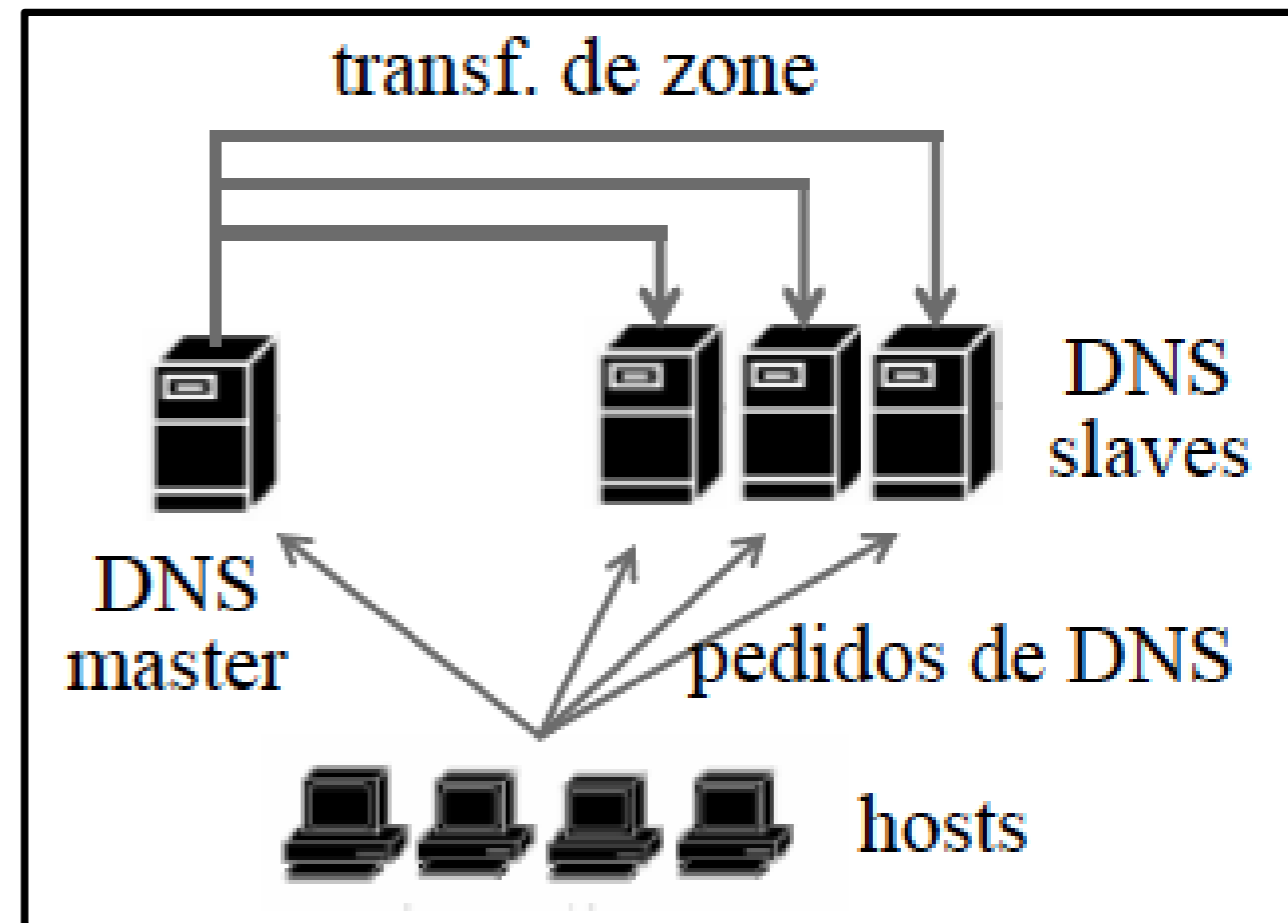
Servidores DNS Atuais

- **Forwarding** (Proxy, Client, Remote): Retransmite todas as 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:**

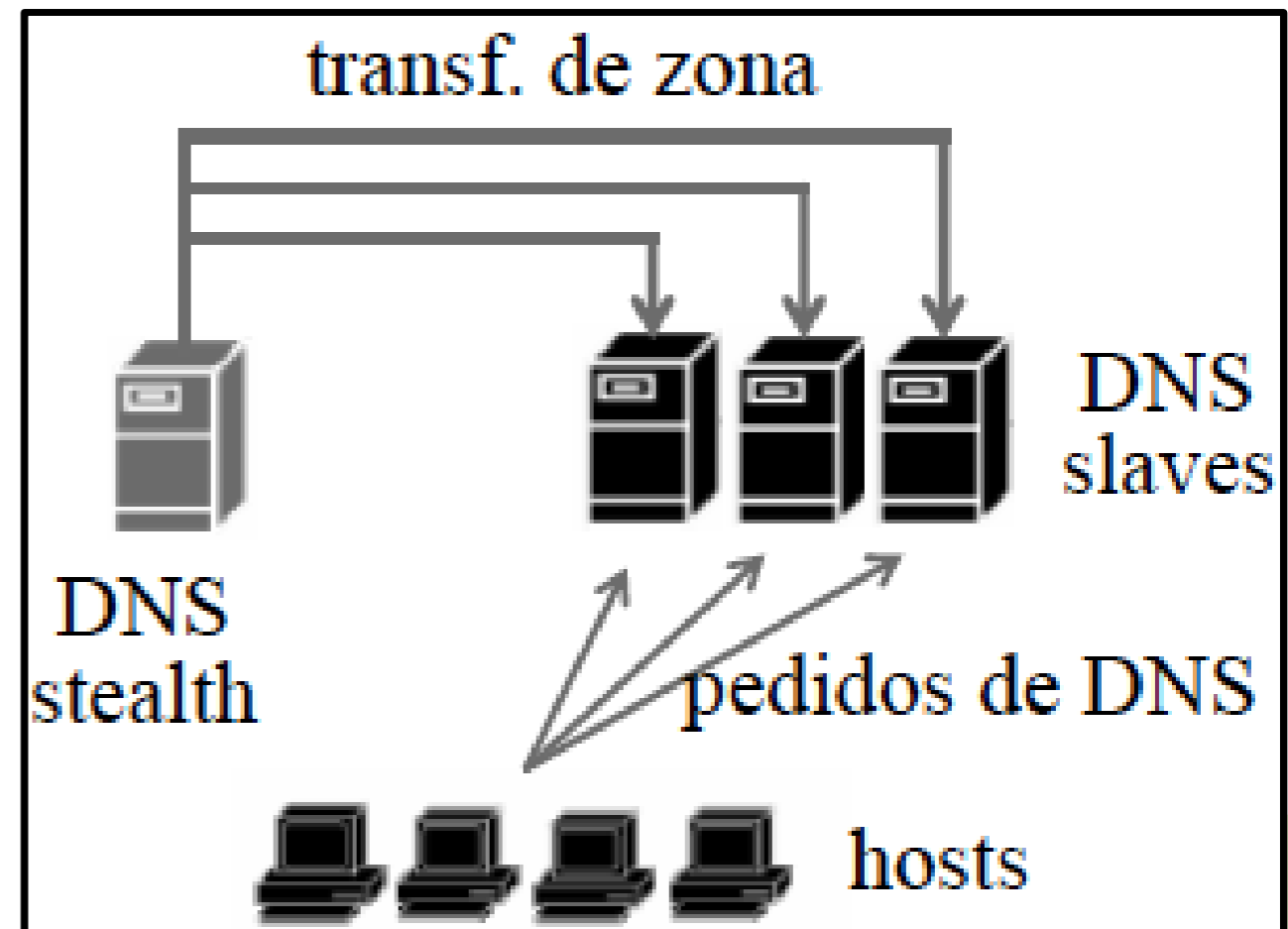
- Carga é balanceada
- Aumento de redundância



Cenários Típicos

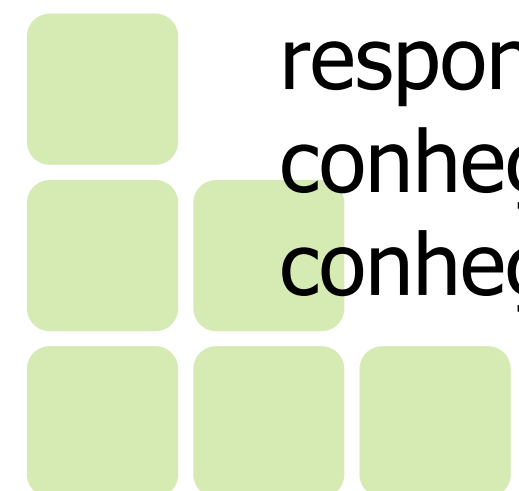
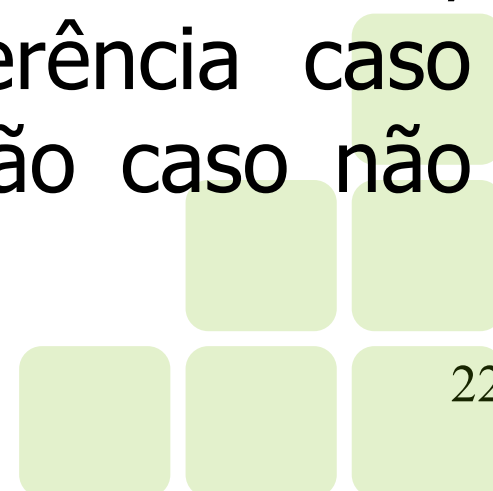
- **Um DNS *stealth* e vários slaves:**

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

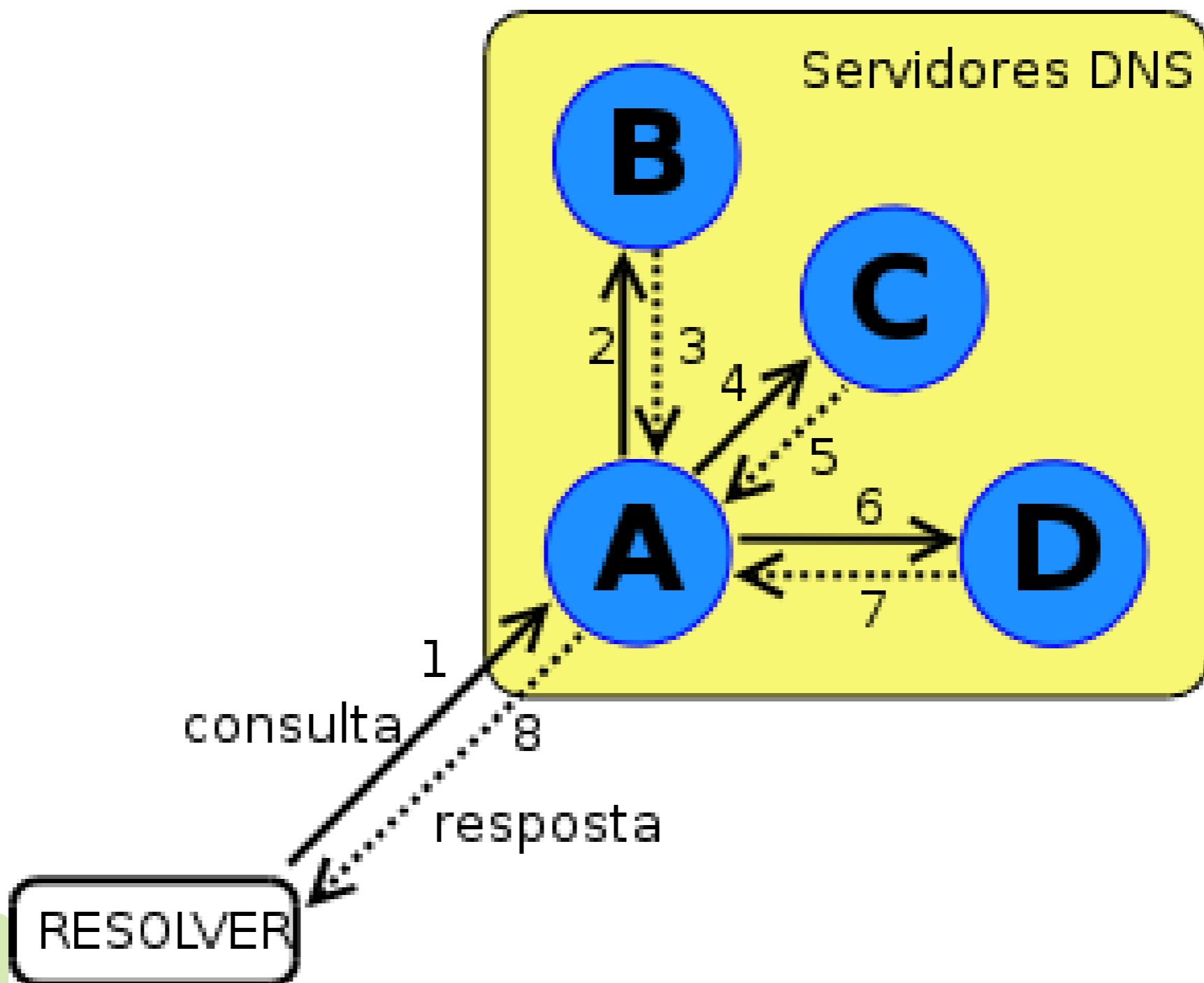




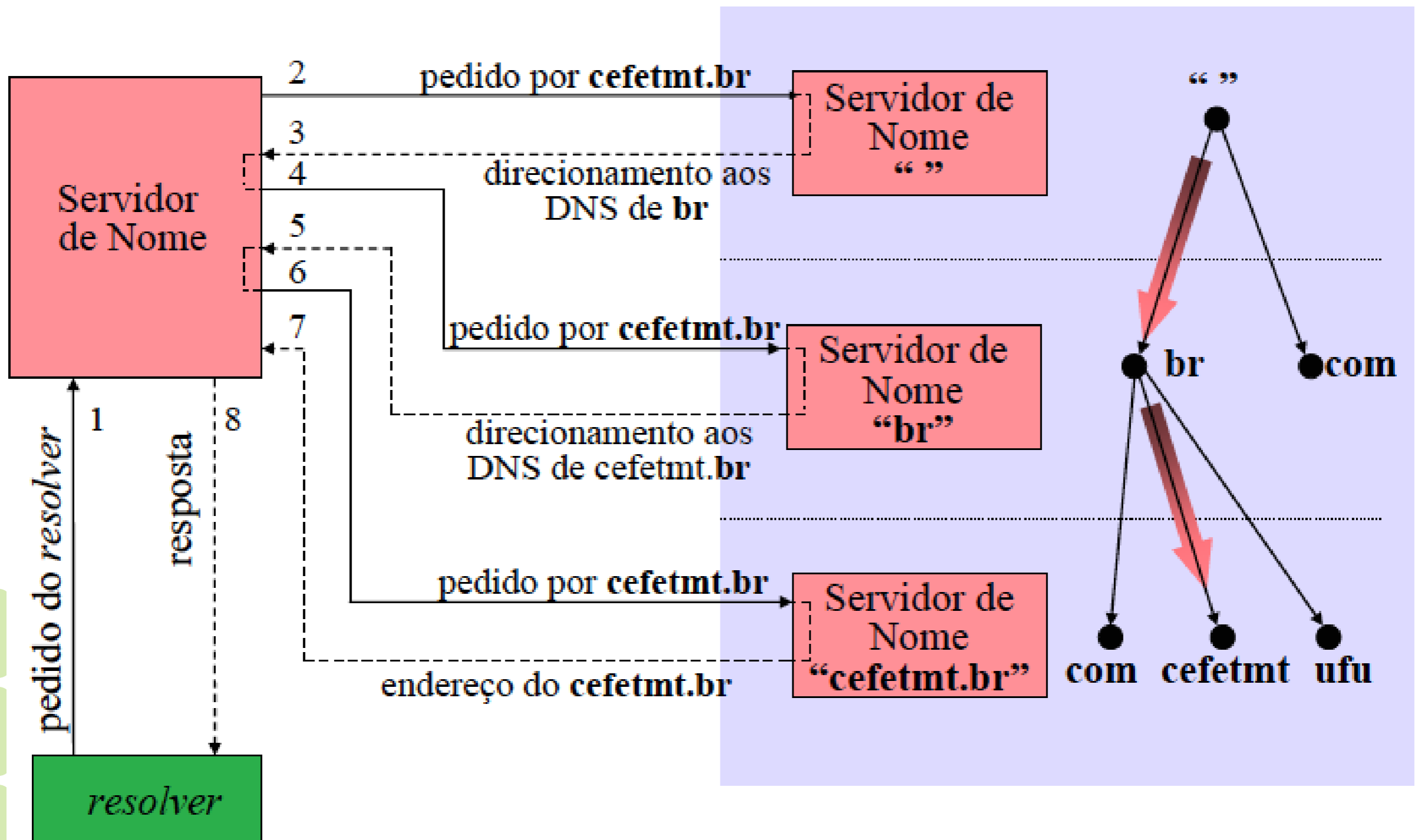
Métodos de resolução de nomes

- 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;
- 
- 

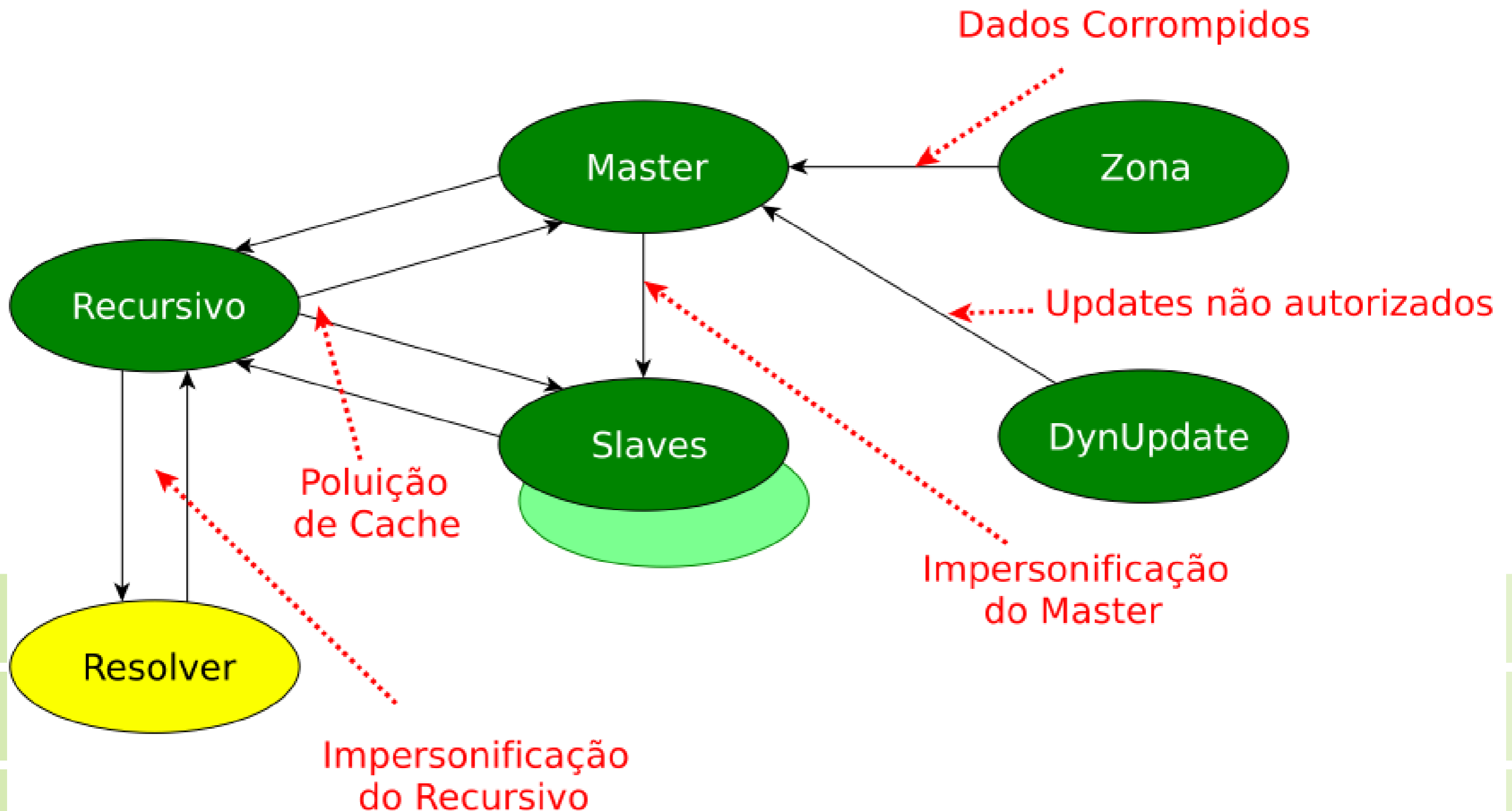
Métodos de resolução de nomes



Métodos de resolução de nomes



Vulnerabilidades do DNS



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, 4^a Edição, Campus.