IP e DNS

O protocolo IP

- Definir um endereço de rede e um formato de pacote
- Transferir dados entre a camada de rede e a camada de enlace
- Identificar a rota entre hosts remotos
- Não garante entrega confiável
- Atualmente na versão 4 (IPV4)
- Escassez de endereços 2^{32}
- Deve ser gradualmente substituído pelo IPV6

Endereço de Rede

- Comumente conhecido como endereço IP
- Composto de 32 bits comumente divididos em 4 bytes e exibidos em formato decimal
  - 192.168.10.1
  - 200.137.2.120
- Para que possam se comunicar os hosts em uma mesma rede precisam de endereços IP exclusivos

Endereço de Rede

- Podem ser:
  - Estático
  - Dinâmico
- É atribuído a cada interface de rede
- Um computador com várias placas de rede receberá vários endereços IP
- Comumente este computador estará ligado a cada rede com uma placa diferente

Endereço de Rede

- Exemplos de endereços IP

Binário: 11000000.10101000.00000001.00001000 e 11000000.10101000.00000001.00001001

Decimal: 192.168.1.8 e 192.168.1.9

- O endereço é dividido em duas partes como um CEP
- A primeira parte identifica a rede e a segunda parte identifica o host

DNS
Domain Name System

DNS

- Computadores em uma rede são reconhecidos pelo seu número IP
  - Ex.: 192.168.3.9
- Conhecer os números de todos os servidores que se deseje acessar é difícil
- Mais simples seria conhecê-los por um nome
- O DNS busca traduzir nomes em números IP

DNS

- É mais fácil lembrar de um nome de domínio como
  - www.google.com
- Do que de um endereço IP
  - 74.125.234.73
- Alterações no número IP ficam transparente para o usuário

DNS

- Inicialmente o número de servidores na rede era pequeno
- A relação nome <=> IP podia ser gravada em um arquivo na própria máquina
  - HOSTS
- Com o aumento no número de máquinas na rede isso ficou inviável

O Protocolo DNS

- Define o formato das perguntas
- Das respostas
- E dos dados trafegados
- O DNS não tem um aplicativo cliente como os outros protocolos da camada de aplicação
- Ele na verdade trabalha para vários aplicativos clientes, traduzindo nomes em IPs

DNS

- Uma máquina na rede tem na sua configuração o IP de 1 ou mais servidores de DNS
- O comando nslookup pode ser usado para fazer uma pesquisa manual ao DNS
  - nslookup google.com
- Um registro DNS é constituído basicamente de 3 campos:
  - Nome
  - Endereço IP
  - Tipo

DNS

- Os Tipos de Registro
  - A – Endereço de dispositivo final
  - NS – Nome de servidor confiável
  - CNAME – Nome Canônico ou Nome de domínio completo, utilizado quando vários serviços têm um único endereço de rede, mas cada serviço tem sua própria entrada no DNS
  - MX – registro de troca de e-mail

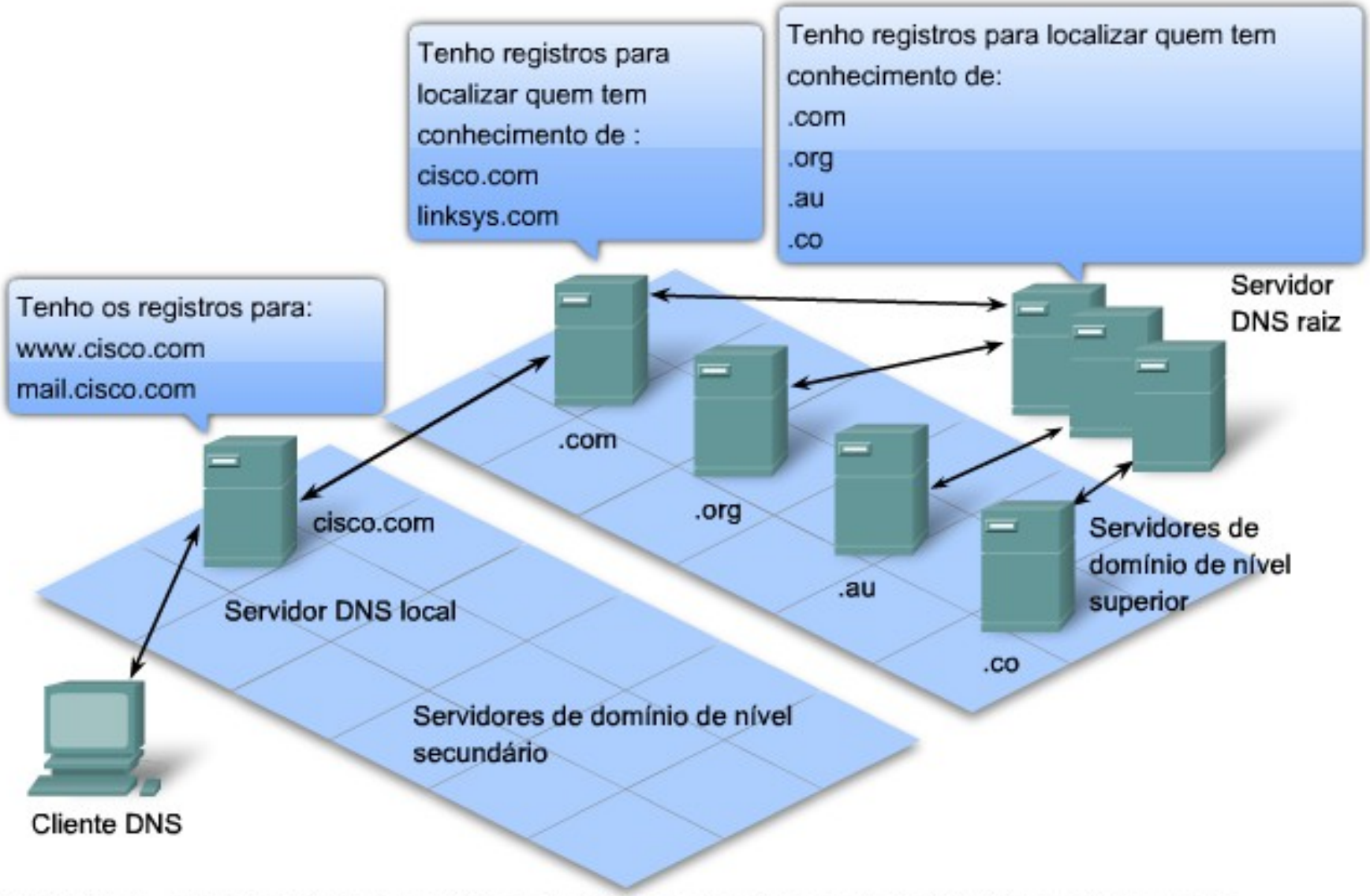
DNS

- O DNS funciona de maneira hierárquica
- Se um servidor de DNS não tem em seu registros o IP para o nome que está sendo procurado
- É necessário pedir para o servidor superior
- Uma vez que o servidor superior responda o endereço pode ser armazenado no cache local
- No windows podemos ver o cache dns fazendo:
  - ipconfig /displaydns

Hierarquia de DNS

- As consultas de DNS são resolvidas usando uma árvore
- Os servidores de nível superior respondem por um país ou um tipo de organização
  - Ex.: .com .br .org .jp
- Depois dos domínios de nível superior há os domínios de segundo nível e os de níveis inferiores

Hierarquia de DNS



Hierarquia de servidores DNS que contêm os registros dos recursos correspondentes aos nomes com endereços.

Tipos de servidores DNS

- Autoritativo
  - Servidor responsável por um determinado domínio
  - É o servidor de referência para aquele domínio ao qual ele pertence
- Recursivo
  - É um servidor que responde por domínios perguntando a outros servidores
  - Comum em redes locais como um cache de DNS

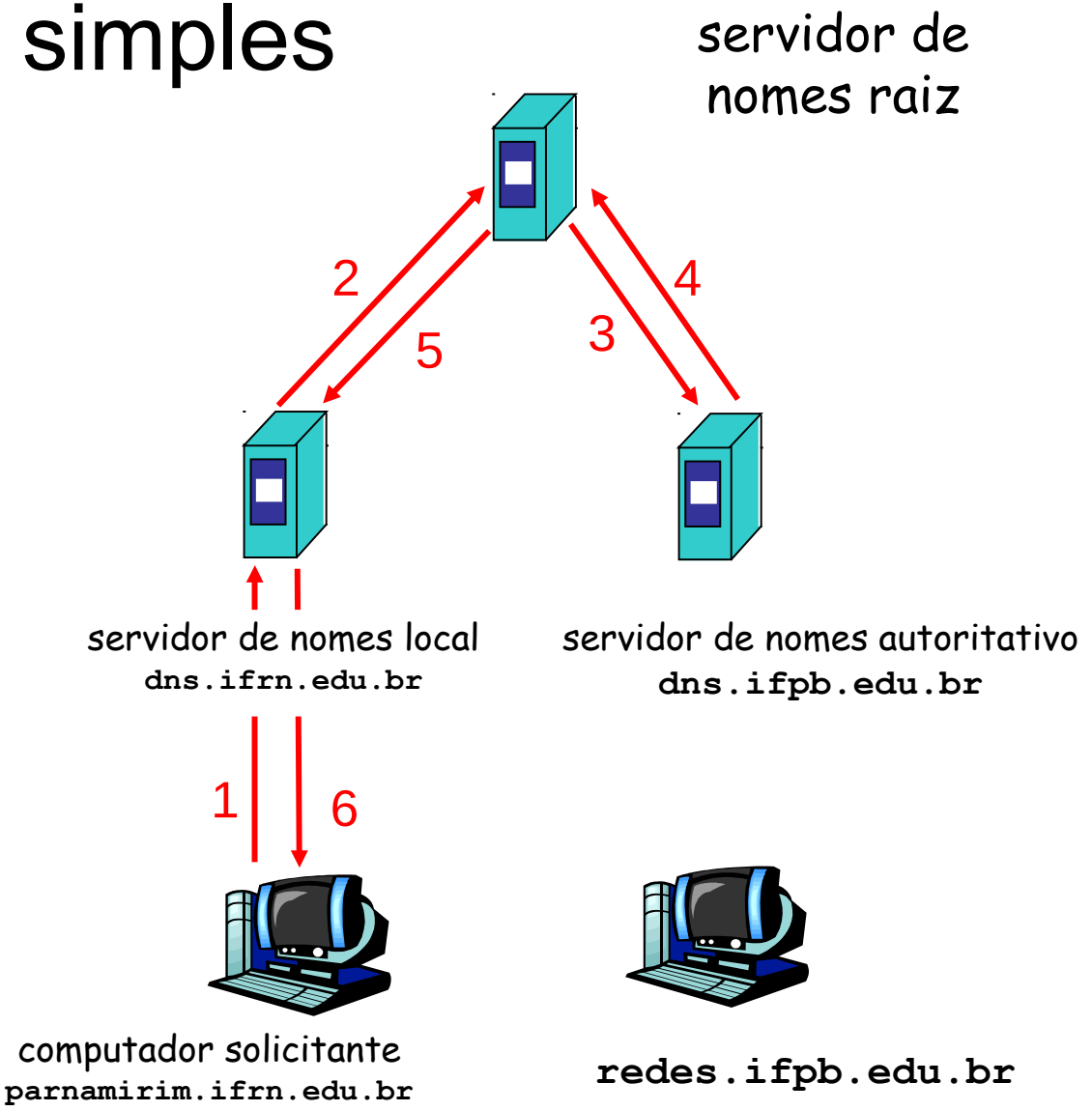
Redundância de servidores DNS

- Como o serviço de DNS é muito importante para o funcionamento de outros serviços, é comum termos um segundo servidor caso o primeiro falhe
- Este segundo servidor é chamado servidor DNS ***slave*** (escravo)
- O DNS slave mantém uma cópia atualizada de todos os registros DNS do servidor principal chamado de ***master*** (mestre)

DNS: exemplo simples

Host **parnamirim.ifrn.edu.br** quer o endereço IP de **redes.ifpb.edu.br**

1. contata seu servidor DNS local, **dns.ifrn.edu.br**
2. **dns.ifrn.edu.br** contata o servidor de nomes raiz se necessário
3. o servidor de nomes raiz contata o servidor de nomes autoritativo, **dns.ifpb.edu.br**, se necessário

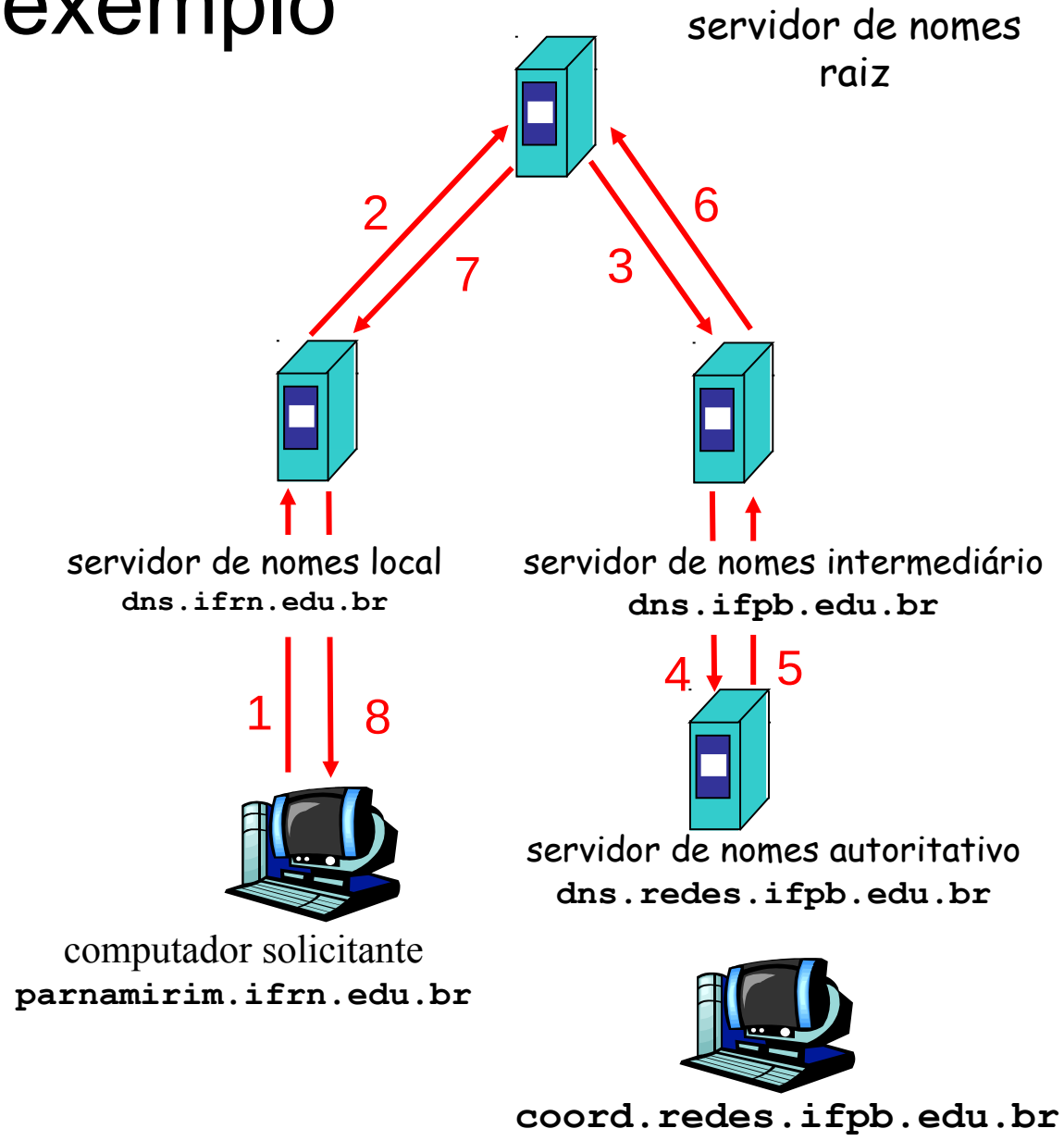


DNS: exemplo

Host
`parnamirim.ifrn.edu.br`
quer o endereço IP de
`coord.redes.ifpb.edu.br`

Servidor de nomes raiz:

- pode não conhecer o servidor de nomes autoritativo para um certo nome
- pode conhecer: *servidor de nomes intermediário:* aquele que deve ser contactado para encontrar o servidor de nomes autoritativo



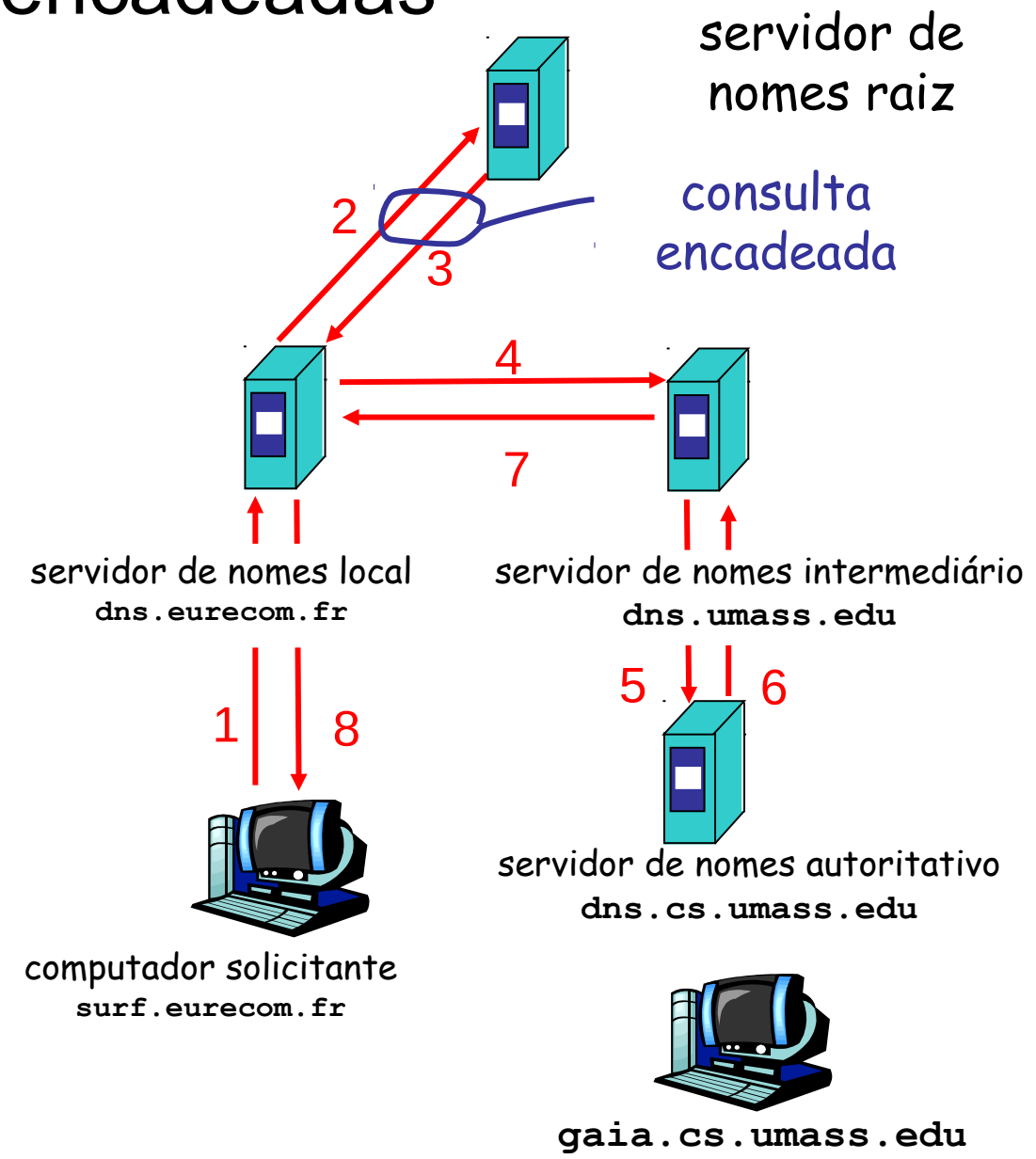
DNS: consultas encadeadas

consulta recursiva:

- transfere a tarefa de resolução do nome para o servidor de nomes consultado
- carga pesada?

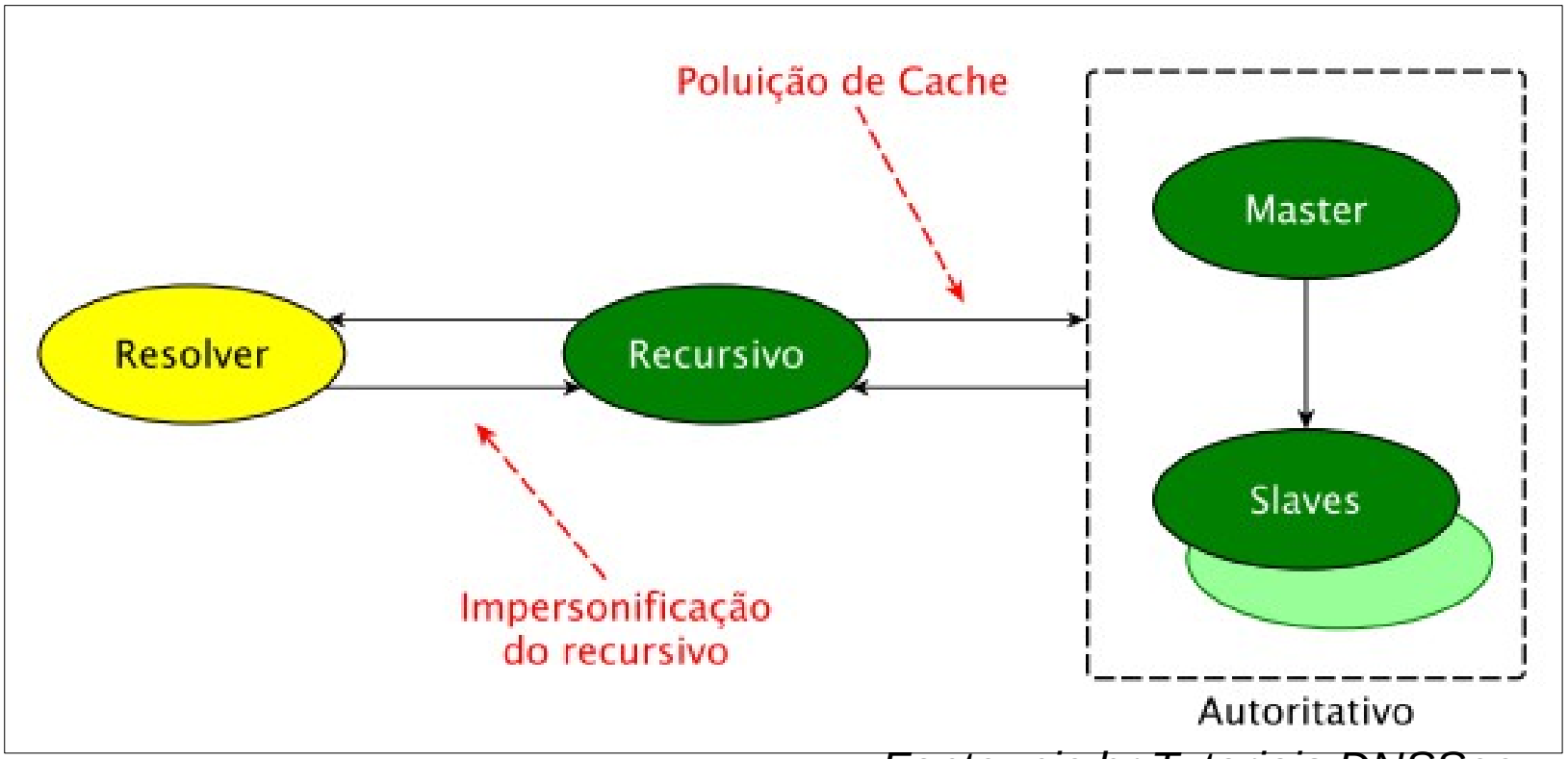
consulta encadeada:

- servidor contactado responde com o nome de outro servidor de nomes para contato
- *"Eu não sei isto ,mas pergunte a este servidor"*



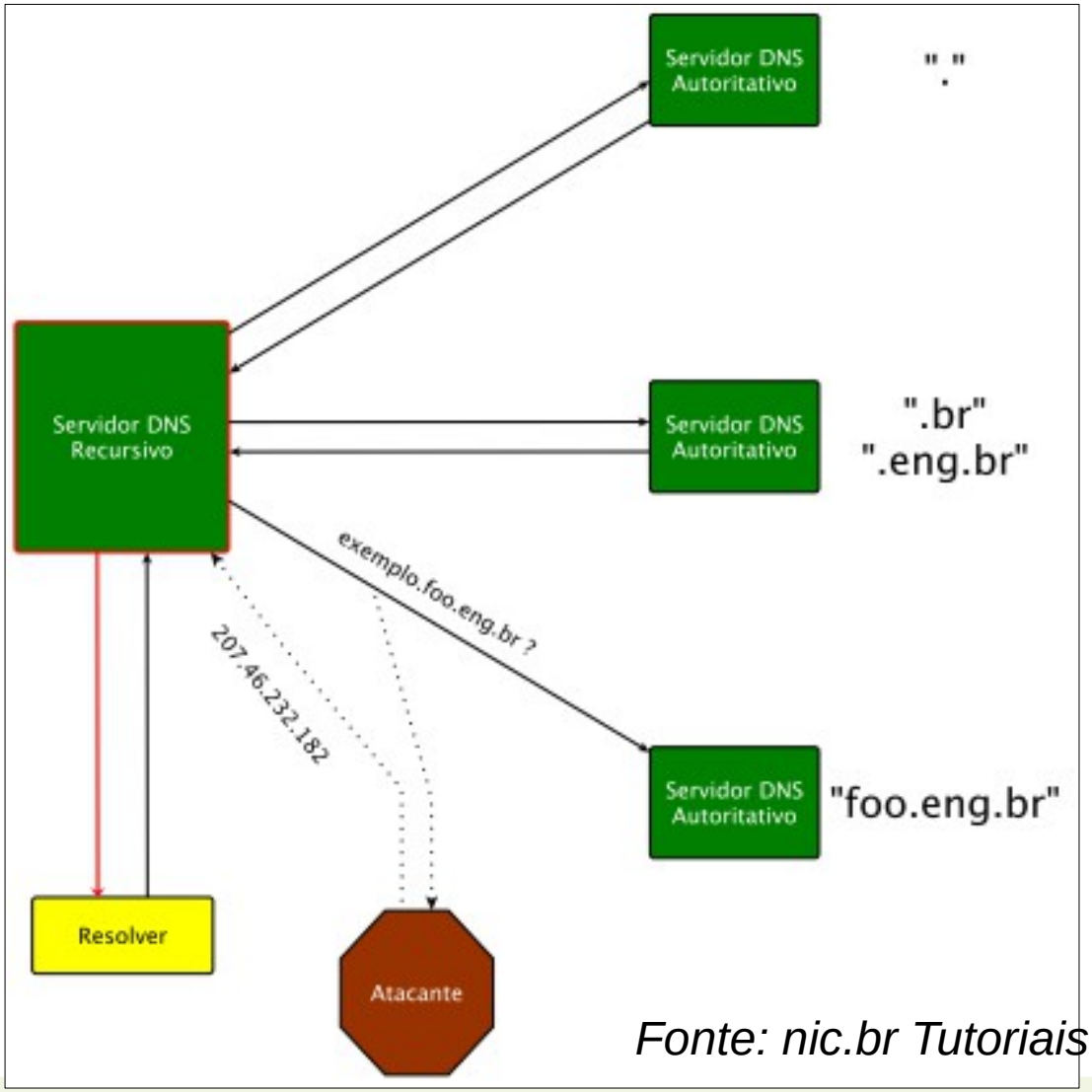
DNS Spoofing

- Possíveis momentos de ataque com DNS spoofing



Fonte: nic.br Tutoriais DNSSec

Ataque DNS Spoofing



Fonte: nic.br Tutoriais DNSSec

DNSSEC

- Garantias de:
  - Origem
  - Autenticidade
- Sempre que uma requisição é feita o servidor deve enviar uma assinatura (usando criptografia de chave pública/privada)
- Essa assinatura garante a origem e autenticidade das mensagens, **mas não o sigilo**

Atividade

- Qual a função básica do servidor DNS?
- Por que é necessário existir uma hierarquia de DNS?
- Descreva os tipos de registro DNS em um servidor.
- Diferencie um servidor autoritavo Master e Slave.
- Qual a função do DNSSEC?

Endereço de Entrega: https://goo.gl/T6J6Ns