

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



Endereços IPv6

- Nova versão do protocolo IP
- Criada principalmente por causa do esgotamento do IPv4
- IPv4 = 2^{32} endereços diferentes \approx 4 bilhões
- IPv6 = 2^{128} endereços diferentes \approx Muitos!
- 340.282.366.920.938.463.463.374.607.431.768.211.456
- 340 undecilhões de endereços
- Além do novo espaço de endereços o IPv6 traz algumas vantagens como:
 - Fim da fragmentação
 - Fim do broadcast
 - Auto-configuração com endereço global



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 \Leftrightarrow 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`

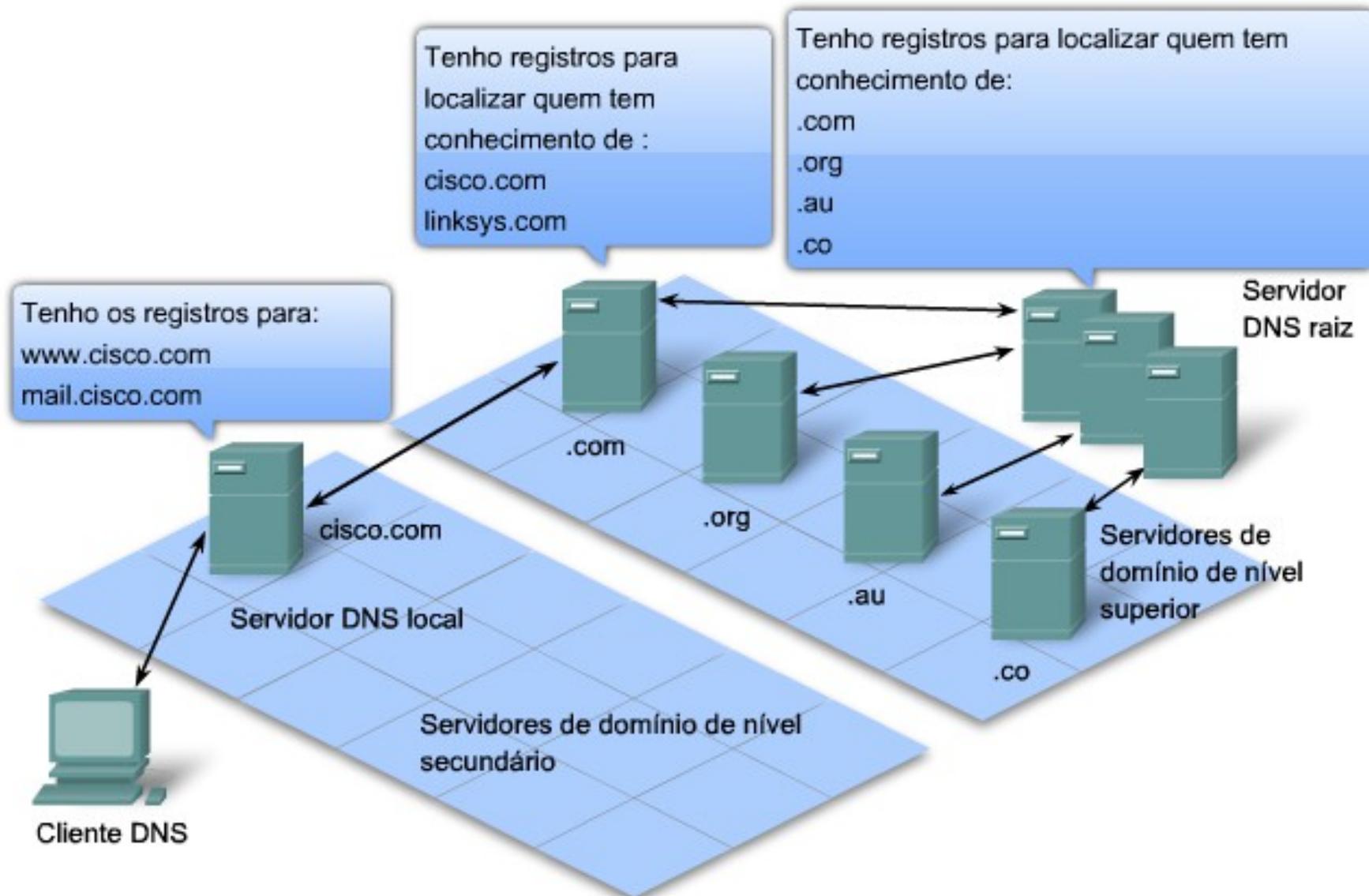


Hierarquia de DNS

- 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

- **Recursivo**
 - Um servidor local que pode armazenar um cache dos últimos pedidos
 - Caso não conheça o endereço pedido, repassará para um servidor superior na árvore
- **Autoritativo**
 - O servidor responsável por um determinado domínio
 - Pode ser master ou slave



Servidor Autoritativo

- Master
 - O servidor principal de um domínio
- Slave
 - Um ou mais servidores que tem cópias do servidor Master
 - Está constantemente sendo atualizado com possíveis mudanças no servidor Master

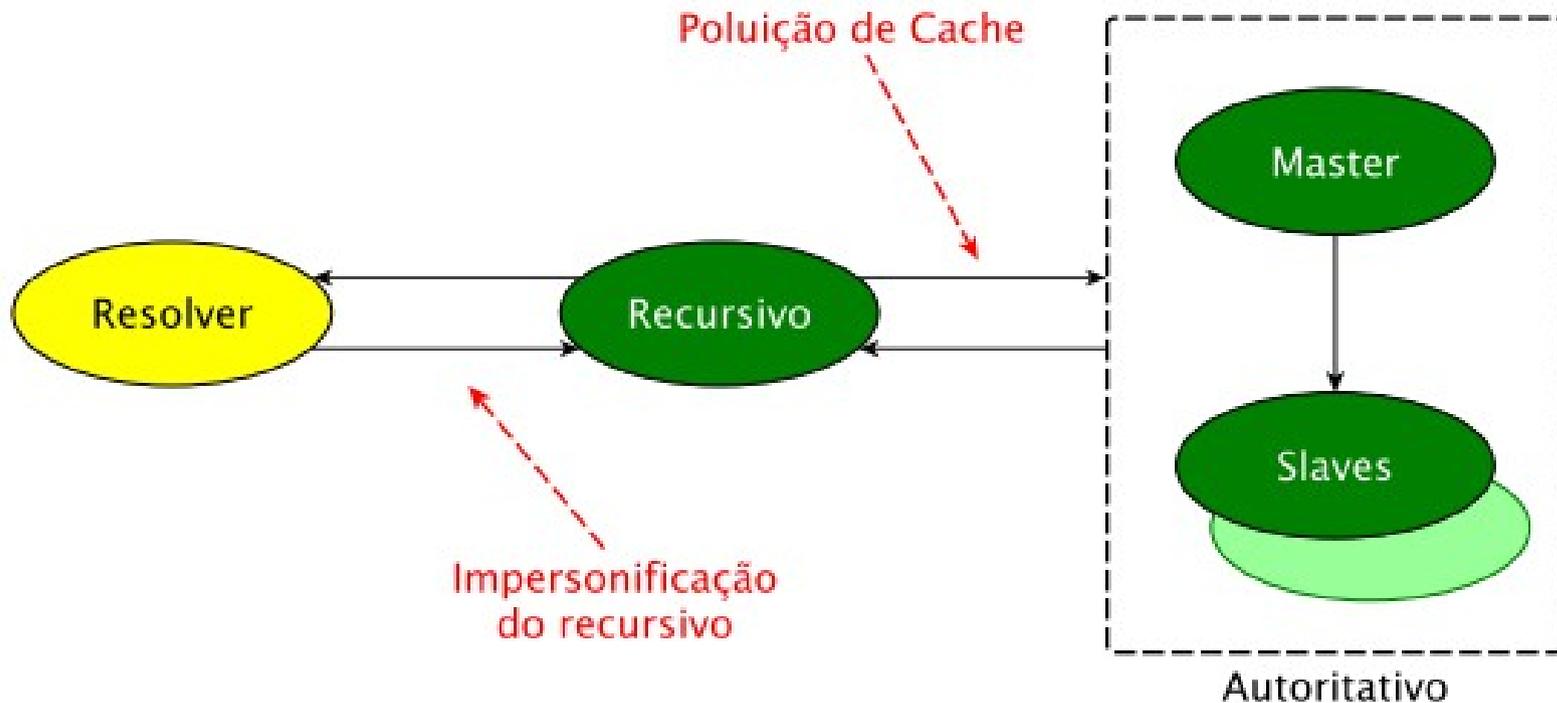
Segurança

- Como muitos serviços de rede o DNS não foi projetado pensando em segurança
- Um ataque conhecido como DNS Spoofing pode comprometer toda a estrutura de segurança de uma rede
- Nesse ataque o atacante substitui o servidor de DNS por um outro servidor mal configurado propositalmente



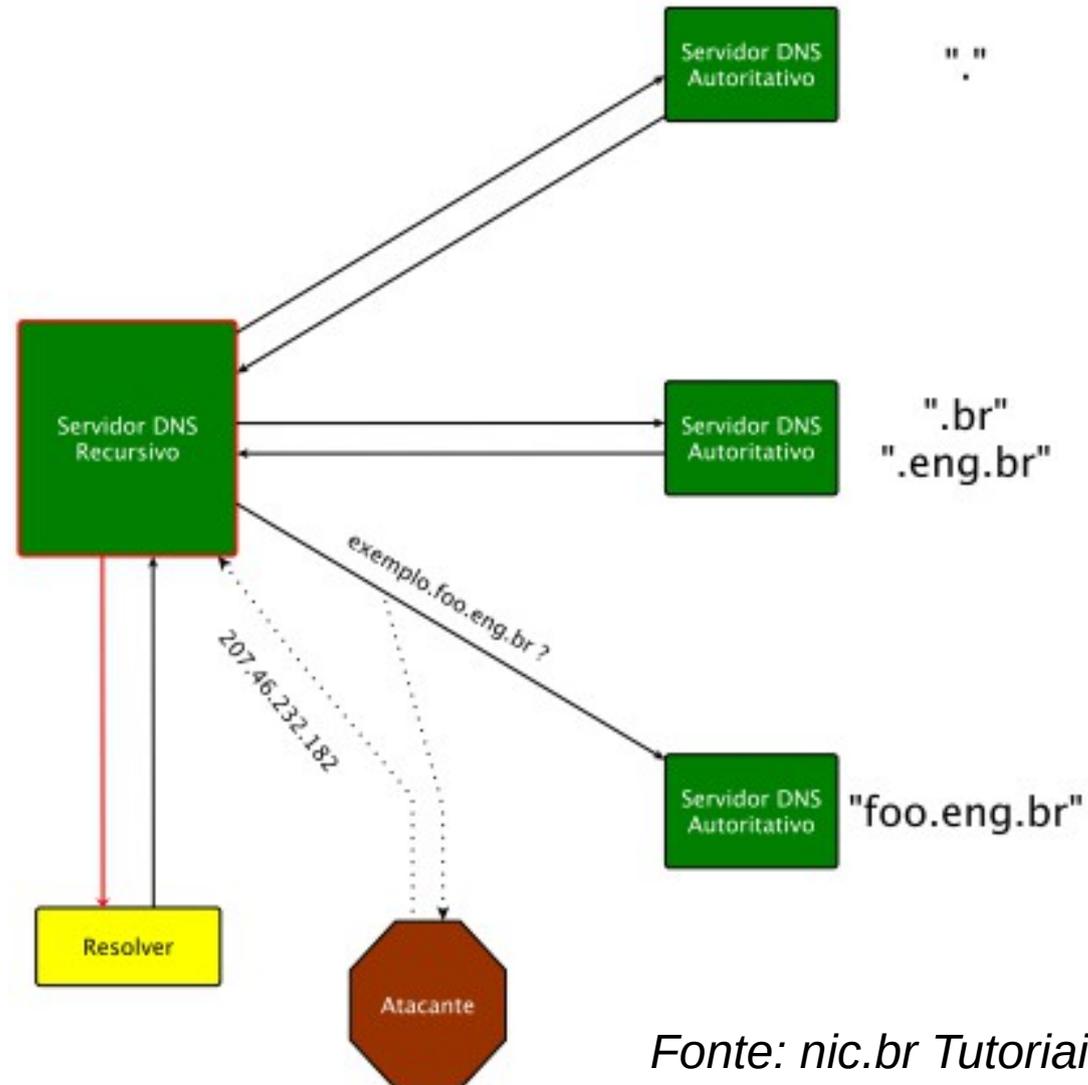
DNS Spoofing

- 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 autoritativo Master e Slave.
- Qual a função do DNSSEC?

