

AULA Nº 04

Infraestrutura Comp. Alto Desempenho e Sist. Distribuídos

Servidor DNS

Julio Cezar Estrella
ICMC-USP

Introdução

- Acesso a computadores sem que o usuário tenha conhecimento de seu endereço IP (Internet Protocol).
- O DNS (Domain Name Server) é um sistema de gerenciamento de nomes hierárquico e distribuído
- Pertence à camada de aplicação do modelo OSI (Open Systems Interconnection)

Histórico

- Quando a Internet ainda era uma ferramenta de uso militar o acesso aos nomes era possível graças a um arquivo de nome “hosts.txt”
- Esse arquivo cresceu tanto que chegou ao ponto de causar atraso nas atualizações.
- Por volta de 1983, o DNS tomou forma para resolver esse problema

Histórico

- Arquitetura desenvolvida por Paul Mockapetris (USC - EUA)
- **RFCs**
 - RFCs 882 e 883 – Funcionamento básico
 - RFCs 1034, 1035 – Modelo Vigente
 - RFCs 1535, 1536, 1537 – Segurança, Implementação, Adm.
- O DNS passou a ser o serviço de resolução de nomes padrão a partir do Windows 2000 Server

Zonas

- Uma zona é uma sub-árvore de um domínio administrada separadamente.
- **Autoridade de uma zona**
 - Primary Server
 - Secondary Server
- **Obtenção de informações**
 - Zone Transfer – secundário obtém informações (*load*) do servidor primário
 - Atualizações periódicas

Servidores

- **Primary Server**
 - Autoritário (Authoritative)
- **Secondary Server**
 - Não Autoritário (Nonauthoritative)
- **Cache Server**
 - *Name caching*
 - Mantém nomes recentemente resolvidos
- Redução de tráfego (custo para rede)
- Problemas?
 - Atualização das Informações

Consultas

- **Recursivas**
 - Consulta distribuída automática
 - Devolve a resolução
 - Problema: mascaramento de servidores
- **Interativas**
 - Consulta distribuída não é automática
 - Devolve endereço de servidores que podem resolver

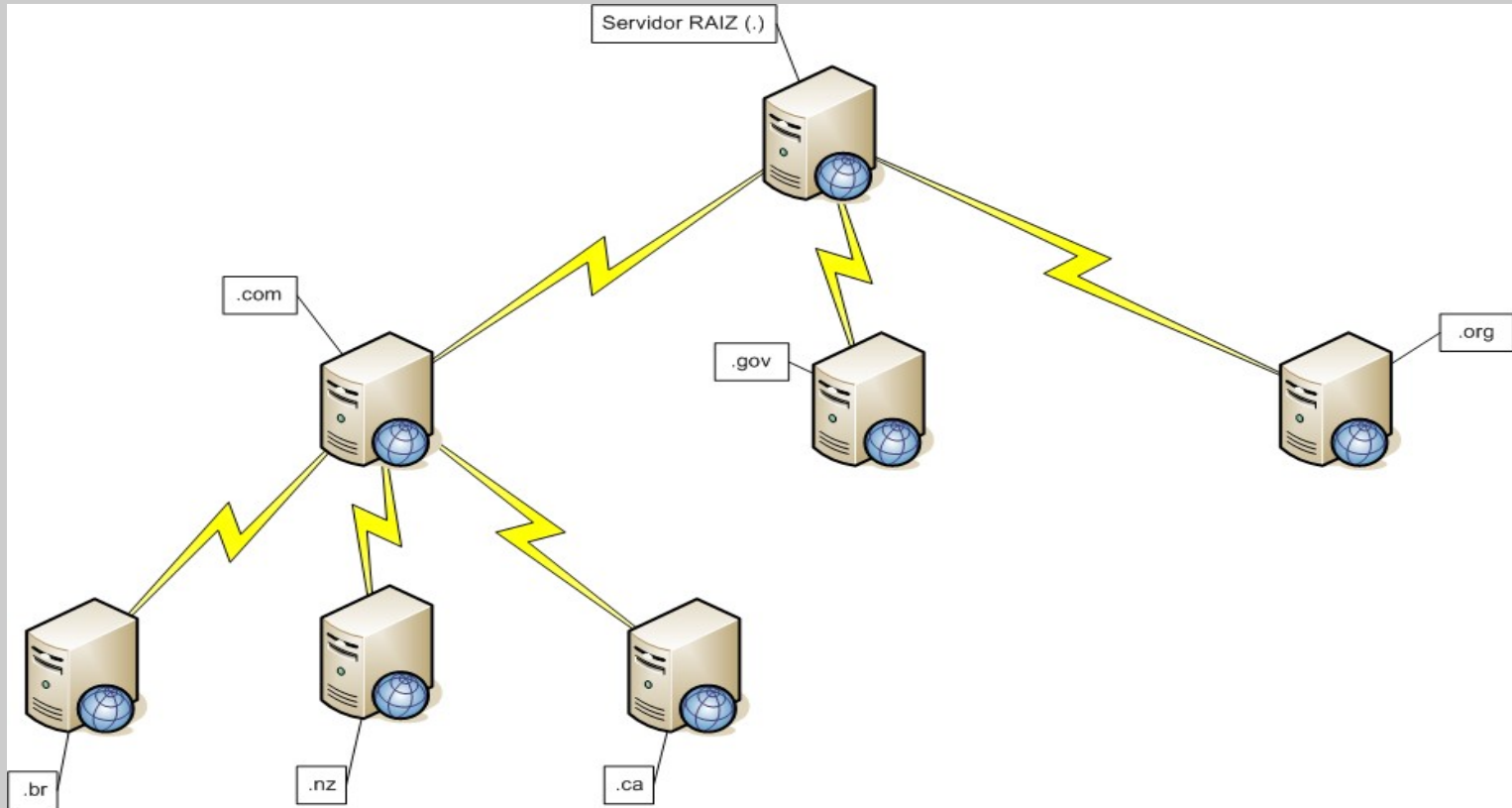
Implementação no Unix

- **Bind**
 - **Named (daemon)**
- **Arquivos de Configuração**
 - **Servidor**
 - ▮ Arq.zone
 - ▮ Arq.revzone
 - ▮ Arq.ca
 - ▮ Arq.boot
- **Cliente**
 - /etc/resolv.conf
- **Exemplos:**
 - <http://www.charvolant.org/~doug/network/html/node10.html#SECTION00064230000000000000>

Problemas do DNS

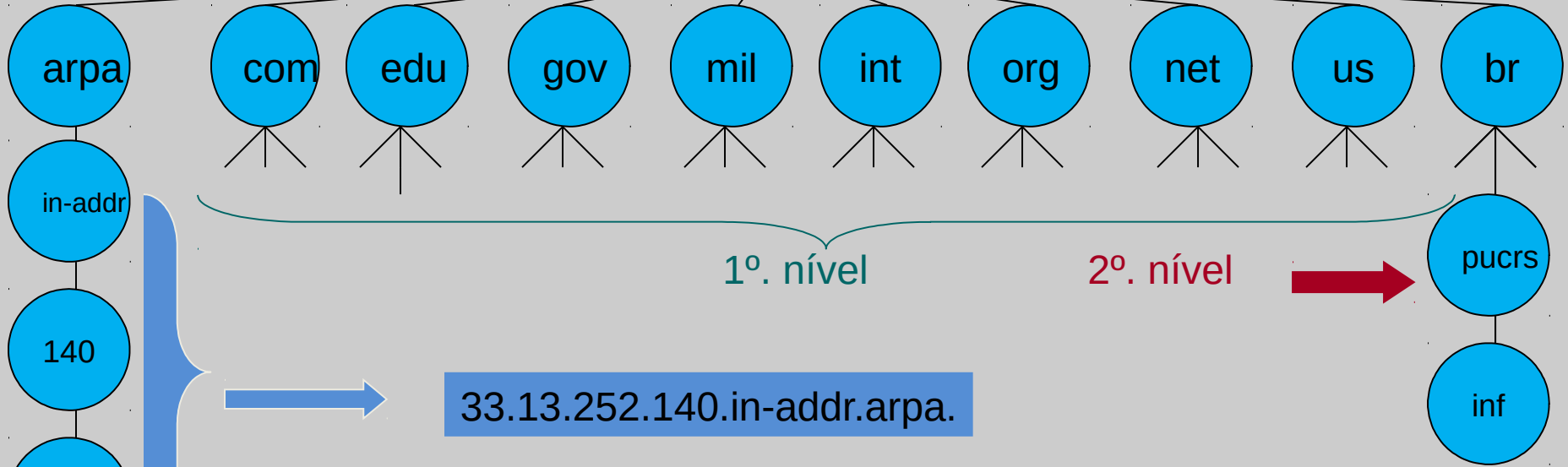
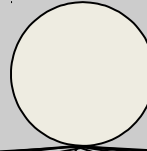
- **Segurança**
 - Bind passa a implementar criptografia e autenticação digital
 - Mascaramento de servidores
- **Carga do servidor**
 - Mecanismo de Round-Robin para distribuição das consultas localmente
- **Erros de Configuração**
 - Lamer: “...name server is listed in the NS records for some domain and in fact it is not a server for that domain.”

Hierarquia



Hierarquia

Raíz – sem nome



Funcionamento

- **Opera segundo duas definições:**
 - Examinar e atualizar seu banco de dados.
 - Resolver nomes de servidores em endereços de rede (IPs).
- Nomes de hosts residentes em um banco de dados podem ser distribuídos entre servidores múltiplos
- Por isso, seu tamanho é ilimitado e o desempenho não degrada tanto quando se adiciona mais servidores nele.

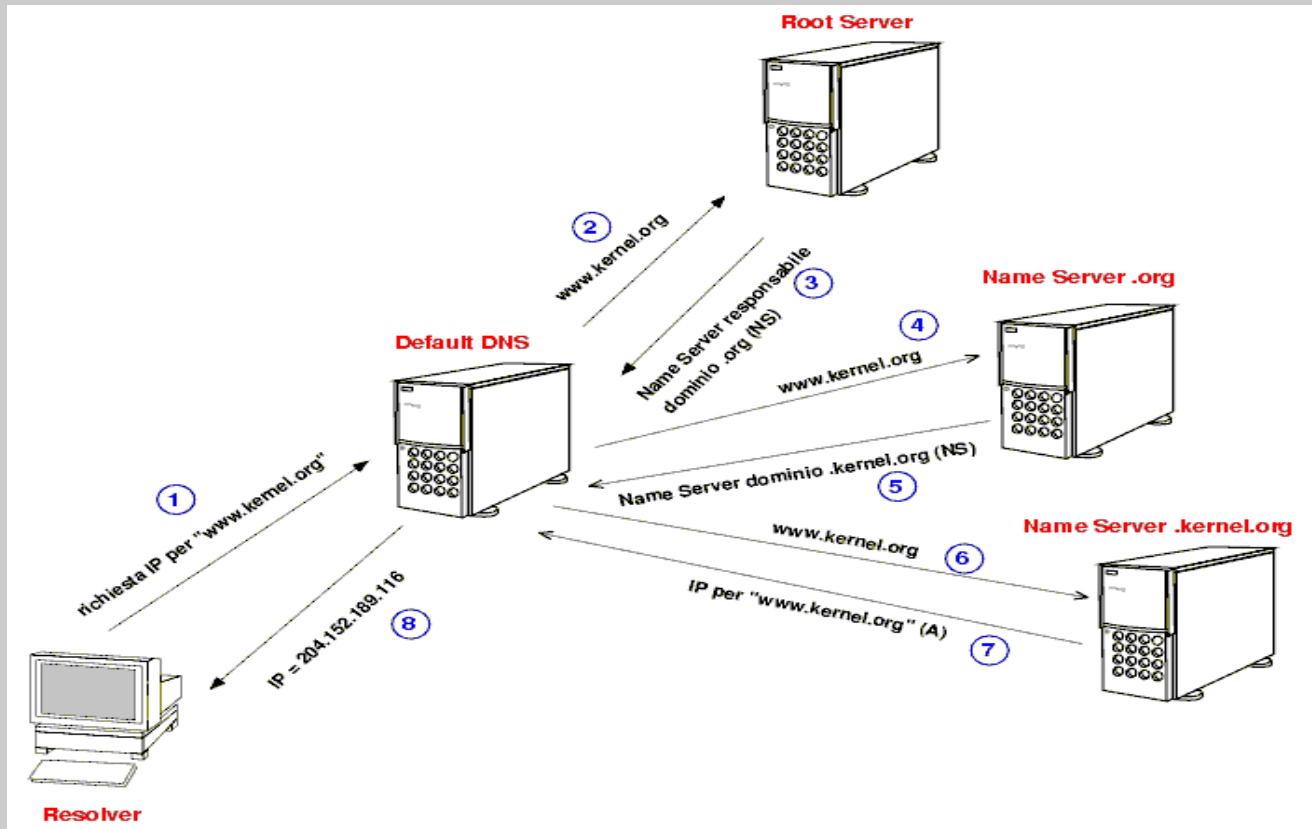
Funcionamento

- O DNS utiliza servidores primário e secundário.
- O servidor secundário é uma espécie de cópia do servidor primário
- Quando não é possível encontrar um domínio através do servidor primário, o sistema tenta resolver o nome através do secundário

Funcionamento

- Na Internet, o serviço de nomes usado é o DNS, que apresenta Arquitetura Cliente-Servidor
- Uma consulta pode envolver vários servidores DNS
- Caso um servidor não contenha uma referência para a consulta, ele encaminha o pedido para outro servidor

Funzionamento



Funcionamento

- **DNS Reverso**
 - Recurso utilizado para resolver um nome através de um endereço IP
 - Utilizado para garantir a confiabilidade do nome a ser apresentado, conferindo o nome com o endereço IP

Funcionamento

- **cache DNS**
 - Uma vez resolvida a requisição, o servidor DNS armazena a relação para agilizar uma nova consulta e envolver menos servidores
 - Cada servidor DNS tem que definir o TTL (*Time-to-Live*) da cache, que determina o tempo de permanência da informação na cache
 - Devido a essa característica, servidores raízes são muito pouco requisitados (em média 500 consultas por dia)

DNS Cache

- Informações em *cache* são marcadas como *nonauthoritatives*
- Frequência de alterações de nomes é baixa
- **Atualizações periódicas**
 - Tempo de permanência de uma informação na *cache* é determinada pelo TTL atribuído pelo servidor primário
 - Servidor descarta informações velhas
 - Busca no servidor Primário informações novas

Registro de Recursos

Formato: Campos (Name, Value, Type, TTL)

Type	Name	Value
A	Nome do hospedeiro	Endereço IP
NS	Nome do Domínio	Nome de um servidor de nomes com autoridade que responde a consultas relativas aos hospedeiros do domínio
CNAME	Apelido do hospedeiro	Nome canônico do hospedeiro
MX	Apelido do hospedeiro	Nome canônico do servidor de correio eletrônico

Estrutura

- Há no mundo 13 servidores DNS do tipo raiz. Eles são denominados pelas letras do alfabeto. Sem eles a Internet não funcionaria.
- Destes, 10 estão localizados nos EUA, um na Ásia e dois na Europa.
- Há réplicas desses servidores em todo o mundo, inclusive no Brasil

Estrutura

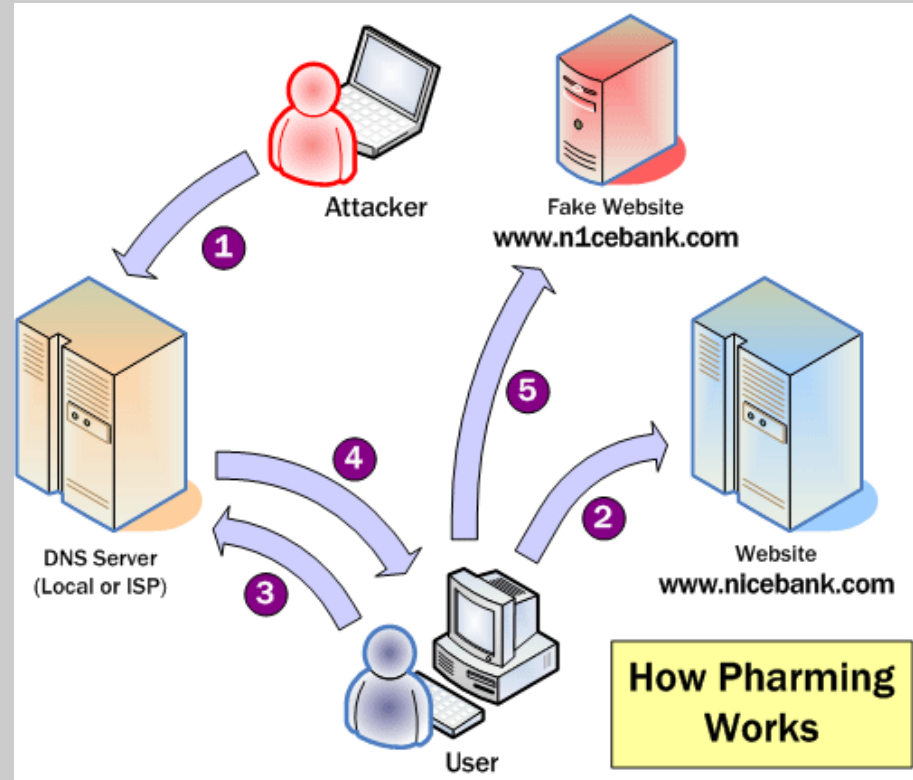
- Na hierarquia de servidores, temos abaixo dos *Roots* os *Top Level Domains*
- ***Há dois tipos de top level domains:***
 - *Generic Top Level Domain: São domínios .com, .edu, .org, etc*
 - *Country Code Top Level Domain: São domínios .br, .fr, .ar, etc*
- No Brasil, a organização que gerencia o domínio .br é a *Registro.br*

Onde Usar?

- É interessante usar DNS também em Intranets, principalmente em redes de médio a grande porte
- Universidades, Empresas, Etc...
- Muito útil para gerenciamento de redes segmentadas

Segurança

- O DNS pode ser aproveitado para ações ilegais.
- Um modo de fazer isso é induzir um nome a apontar para um endereço diferente do correto (**envenenamento**).



Segurança

- **DNSSEC (Domain Name System Security Extensions)**
 - Devido a problemas como o mencionado anteriormente, a IETF (*Internet Engineering Task Force*) criou esta extensão do DNS.
 - Ela autentica as informações do DNS e garante que as mesmas são autênticas e íntegras.
 - Sua adoção depende de cada *Top Level Domain*. No Brasil, o Registro.br já permite o registro de alguns domínios com a extensão DNSSEC

Conclusão

- DNS é fundamental para a arquitetura atual da Internet
- Também é usado para Intranets
- Possui estrutura escalável
- Segurança ainda tem vulnerabilidades

Atividade

- Disponível no Moodle conforme consta no cronograma da disciplina

Referências

<http://registro.br/faq/faq5.html>

<http://www.faqs.org/rfcs/rfc882.html>

<http://www.faqs.org/rfcs/rfc883.html>

<http://www.faqs.org/rfcs/rfc1034.html>

<http://www.faqs.org/rfcs/rfc1035.html>

KUROSE, J.; ROSS, K. W. **Redes de Computadores e a Internet, 2016**

Próxima Aula

- Servidor Web