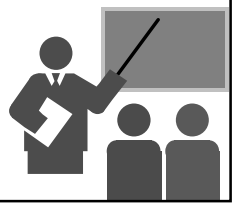
Introdução ao DNS

Rafael Freitas Reale
`reale@ifba.edu.br`
http://www.rafaelreale.net
Cedido por:
Volnys Borges Bernal
`volnys@lsi.usp.br`
http://www.lsi.usp.br/~volnys

Agenda

- **O que é DNS?**
- **Funcionamento básico**
- **Espaço de nomes**
- **Resolver**
- ***Caching***
- **Requisição DNS**
- **Servidores DNS**
- ***Root Name Servers***
- ***Autoritative* e *Delegated***
- **Implementações de servidor de DNS**
- **Portas UDP e TCP utilizadas**

O que é DNS?



O que é DNS?

- **"*Domain Name System*"**
- **Serviço que permite a resolução de nomes ou endereços IP, ou seja, tradução:**
  - nome -> IP
  - IP -> nome
- **Necessário para todos computadores que utilizam a Internet**
- **Protocolo DNS**
  - RFC 1034 - Domain Names - Concepts and Facilities
  - RFC 1035 - Domain Names - Implementation and Specification

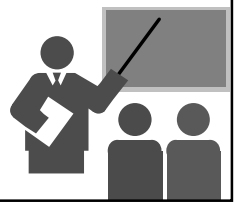
 5

O que é DNS?

- **Existem dois tipos de entidades:**
  - *"Resolver"*
    - Entidade cliente
    - Realiza requisições para de resolução de nome ou endereço
  - *"Name Server"*
    - Entidade servidora
    - Responde às requisições de resolução de nome ou endereço

 6

Funcionamento básico



 7

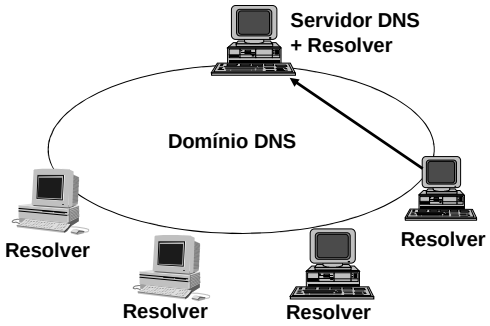
Funcionamento básico

- **Parece um serviço simples, mas é complexo:**
  - Base de dados distribuída pelo mundo
  - Diversos tipos de interações:
    - Resolver → Servidor DNS
    - Servidor DNS → Servidor DNS

 8

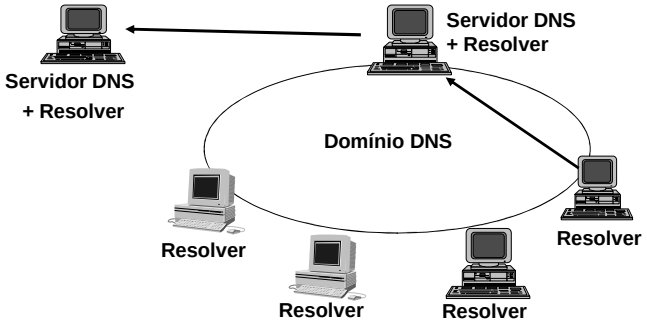
Funcionamento básico

- **Cliente (resolver) pede uma tradução ao servidor DNS**



Funcionamento básico

- **Se o servidor não souber, pede tradução a um outro servidor**



Funcionamento básico

- **Programa nslookup**
  - Programa de teste do serviço DNS
  - Faz o papel de um "resolver" (cliente DNS)

```
# nslookup
Default Server:  localhost.intranet
Address:  127.0.0.1

> www.uol.com.br
Server:  localhost.intranet
Address:  127.0.0.1

Name:    www.uol.com.br
Addresses:  200.221.8.17, 200.221.8.18, 200.221.8.16

> exit
#
```


Exercício

(1) Utilize o utilitário "nslookup" para descobrir ...

(a) O endereço associado ao nome DNS www.uol.com.br
- Se necessário utilize o subcomando "set query=a" (address)

(b) O nome associado ao endereço IP 143.107.161.161
- Informe diretamente 143.107.161.161 ou 161.161.107.143.in-addr.arpa

Exercício

(c) Os servidores DNS associados ao domínio "lsi.usp.br"
- Utilize o subcomando "set query=ns" (name server)

(d) As informações a respeito do mapa principal do domínio "lsi.usp.br"
- Utilize o subcomando "set query=soa" (start of authority)

(d) Os servidores SMTP do domínio "lsi.usp.br"
- Utilize o subcomando "set query=mx" (mail exchange)

Exercício

(2) Utilize o utilitário "host" para descobrir ...

(a) O endereço associado ao nome www.uol.com.br
- host www.uol.com.br

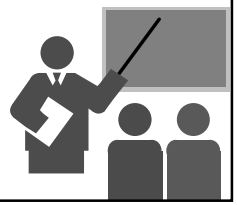
(b) O nome associado ao endereço IP 143.107.161.161
- host 143.107.161.161

(c) Os servidores DNS associados ao domínio "lsi.usp.br"
- host -t ns lsi.usp.br

(d) As informações a respeito do mapa principal do domínio "lsi.usp.br"
- host -t soa lsi.usp.br

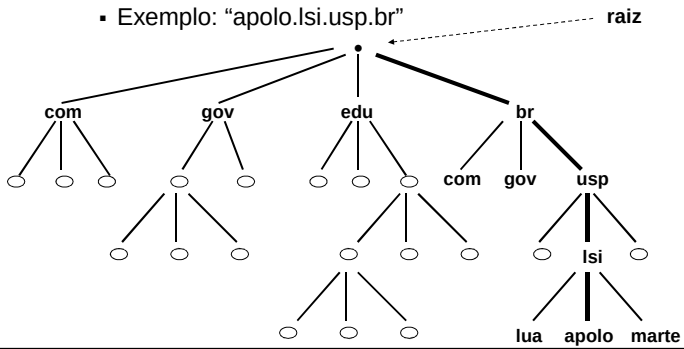
(d) Os servidores de e-mail do domínio "lsi.usp.br"
- host -t mx lsi.usp.br

Espaço de nomes



Espaço de nomes

- **Árvore de nomes da Internet**
  - Semelhante a uma hierarquia de arquivos
    - Exemplo: "apolo.lsi.usp.br"

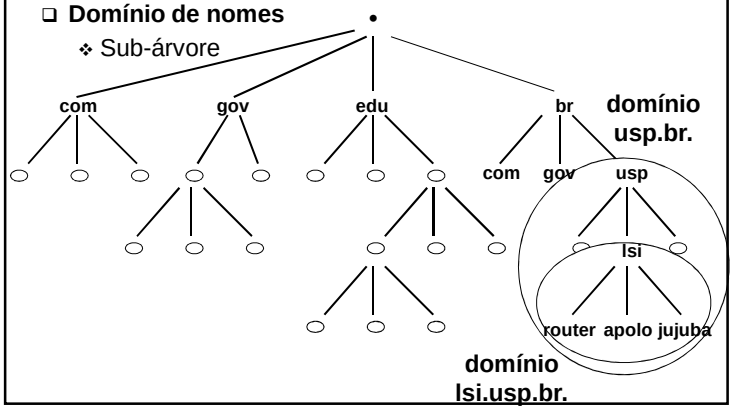


Espaço de nomes

- **Nome**
  - **Absoluto** ou "*Full-qualified domain name*" (FQDN)
    - apolo.lsi.usp.br.
    - (observe o ponto ao final!)
  - **Relativo**
    - apolo
    - apolo.lsi
    - apolo.lsi.usp
    - **apolo.lsi.usp.br**
- **Restrições**
  - Um nó não pode ter dois nós filhos com o mesmo nome
  - Nomes são de no máximo de 63 bytes
  - Caracteres válidos: "A"-"Z" "a"-"z" "0"-"9" "." "-"

Espaço de nomes

- **Domínio de nomes**
  - Sub-árvore



Espaço de nomes

- **Top Level Domain (TLD)**
  - *Coutry Code Top Level Domain* (ccTLD)
    - Relação de códigos paises
    - .br, .uk, .de, ...
    - http://www.iana.org/cctld/cctld-whois.htm
  - *Generic Top Level Domains* (gTLD)
    - .aero, .biz, .com, .coop, .edu, .gov, .info, .int, .mil, .museum, .name, .net, .org, .pro
    - http://www.iana.org/gtld/gtld.htm
  - Domínios de infra-estrutura
    - .arpa
    - http://www.iana.org/arpa-dom/

Espaço de nomes

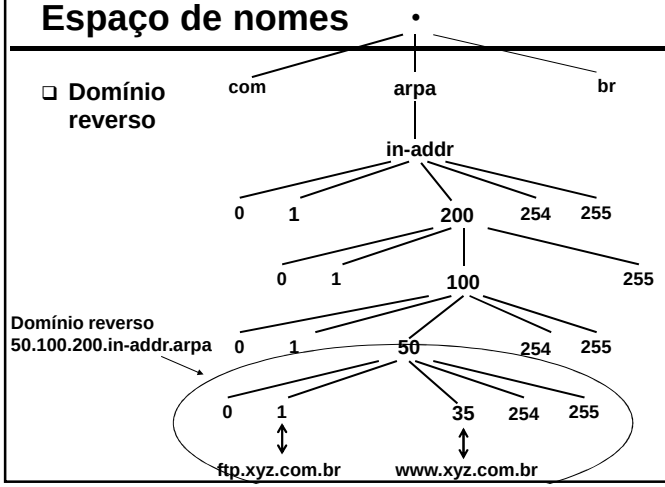
- **Domínios ".br"**
  - Domínio de Primeiro Nível (DPN)
    - Instituições (pessoa jurídica)
      - agr.br, art.br, edu.br, com.br, esp.br, mil.br, ...
    - Profissionais liberais
      - adv.br, arq.br, eng.br, ...
    - Pessoas físicas
      - .nom.br
  - Relação completa em:
    - http://registro.br/info/dpn.html

Espaço de nomes

- **Tipos de domínios**
  - Domínios diretos
    - Utilizados para mapeamento de
      - Nome → endereço IP
  - Domínios reversos
    - Utilizados para mapeamento de
      - Endereço IP → Nome

Espaço de nomes

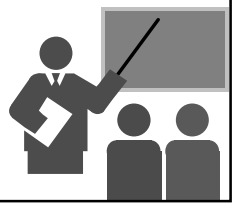
- Domínio reverso



Espaço de nomes

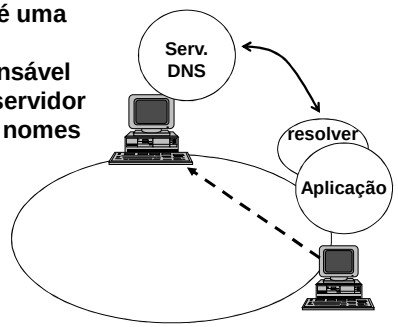
- **Resolução reversa de 200.100.50.35:**
  - 35.50.100.200.in-addr.arpa → www.xyz.com.br

Resolver



Resolver

- **Cliente DNS**
- **Na prática, o resolver é uma biblioteca agregada à aplicação que é responsável pela interação com o servidor DNS para tradução de nomes**
- **O "*resolver*" deve ser configurado em cada maquina**



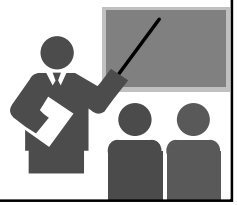
 25

Resolver

- **Informações necessárias para configurar um resolver:**
  - nameservers:
    - servidores DNS que o computador deve contactar
      - deve ser especificado o endereço de dois servidores DNS
      - geralmente os servidores mais próximos
  - domain:
    - domínio ao qual o nome do computador pertence
  - search
    - lista de domínios ao qual o nome deve ser procurado
      - Exemplo: “search lsi.usp.br intranet”.
      - Em uma tradução do nome “terra”, será tentado primeiro “terra.lsi.usp.br” e em seguida “terra.intranet”

 26

Caching



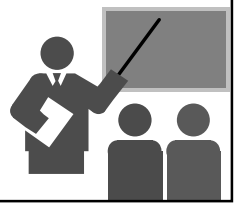
 27

Caching

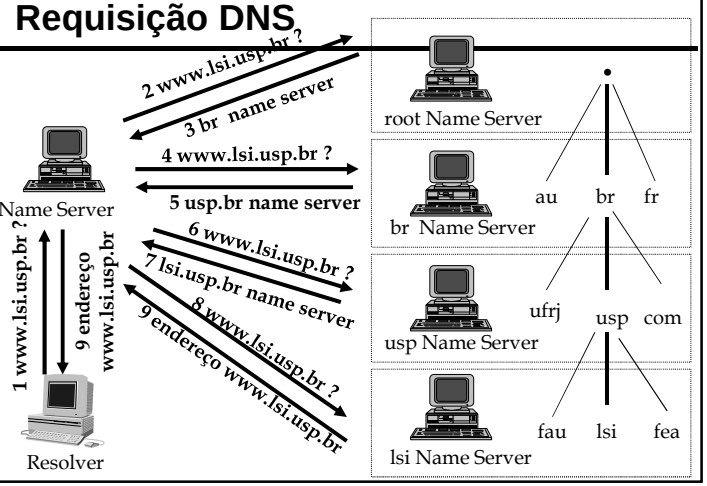
- **Utilizado para diminuir o tempo de resposta de uma requisição ao servidor DNS**
- ***Time-to-Live* (TTL)**
  - Define o tempo de vida de uma entrada no cache de nomes
- **Importância**
  - Uma tradução ip-nome, em uma operação recursiva pode demorar muito tempo.
  - Se já estiver no cache, retorna imediatamente

 28

Requisição DNS



Requisição DNS



Requisição DNS

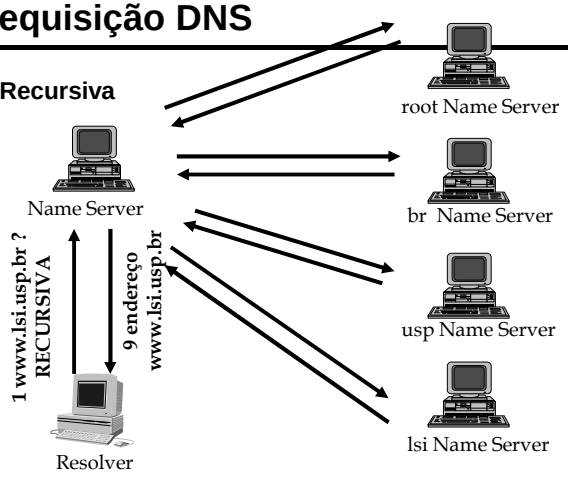
- **Requisição Recursiva**
  - Normalmente gerada pelo "*resolver*"
  - Obriga ao servidor retornar a resposta ou erro (se não encontra-la)
  - Para isso, o servidor pode necessitar consultar
    - cache
    - outros servidores de nomes
  - Mais complexa de ser tratada

Requisição DNS

- **Requisição Interativa (ou não recursiva)**
  - O servidor consulta sua base de dados (inclusive o cache) para poder responder.
  - Não ativa outros servidores de nomes na tentativa de achar a resposta
  - Se não puder responder, procura indicar um servidor de nomes que possa ter a informação requisitada

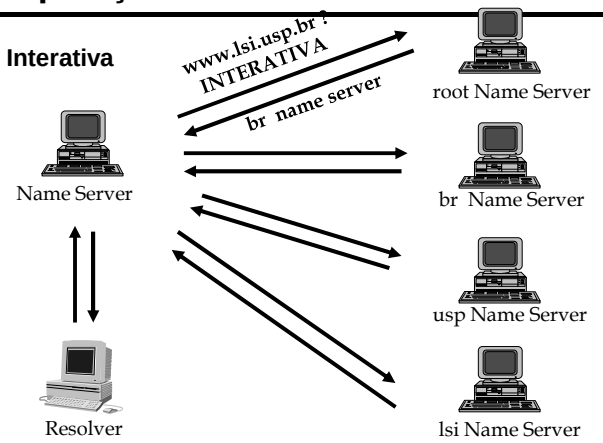
Requisição DNS

- **Recursiva**

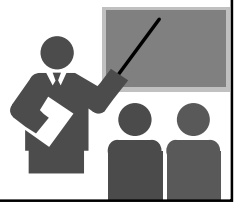


Requisição DNS

- **Interativa**



Servidor DNS



Servidor DNS

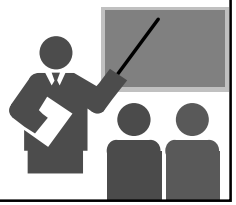
- **Um servidor DNS pode desempenhar dois papeis**
  - Servidor Recursivo
    - Atende aos pedidos de tradução dos resolvers
    - Exemplo: servidor DNS para as máquinas da rede local (intranet) de uma empresa
  - Servidor Interativo (não recursivo)
    - Resolve nomes de um domínio específico
    - Contém configuração dos mapas de traduções para o domínio
    - Exemplo: servidor DNS do domínio “lsi.usp.br”

Servidores DNS

- **Servidor Interativo**
  - Existem milhares de servidores DNS interativos espalhados pelo mundo.
  - Para cada domínio Internet são necessários ao menos 2 servidores interativos:
    - um servidor primário
      - servidor que contém o “mapa” do domínio
      - geralmente localizado no próprio domínio
    - um ou mais servidores secundários
      - buscam do servidor primário os “mapas” do domínio
      - obrigatoriamente em um site diferente do domínio
      - garante confiabilidade do serviço

 37

Root Name Servers



 38

Servidores DNS

- **"*Root Name Servers*"**
  - Servidores Interativos que respondem requisições sobre servidores de nomes do primeiro nível da árvore
  - Quando um servidor local não consegue resolver uma determinada requisição esta é repassada a um "*Root Name Server*"
  - Existem vários "*Root Name Servers*" espalhados pelo mundo (se todos falharem todas as resoluções na Internet irão falhar)
  - Todos servidores DNS devem possuir uma lista atualizada de todos os "*Root Name Servers*"

 39

Root name servers

- **Existem 13 servidores DNS raiz nomeados de:**
  - a.root-servers.net
  - b.root-servers.net
  - ....
  - m.root-servers.net

 40

Root Name Servers

```
# nslookup
> set q=ns
➢ .

K.ROOT-SERVERS.NET      internet address = 193.0.14.129
L.ROOT-SERVERS.NET      internet address = 198.32.64.12
M.ROOT-SERVERS.NET      internet address = 202.12.27.33
I.ROOT-SERVERS.NET      internet address = 192.36.148.17
E.ROOT-SERVERS.NET      internet address = 192.203.230.10
D.ROOT-SERVERS.NET      internet address = 128.8.10.90
A.ROOT-SERVERS.NET      internet address = 198.41.0.4
H.ROOT-SERVERS.NET      internet address = 128.63.2.53
C.ROOT-SERVERS.NET      internet address = 192.33.4.12
G.ROOT-SERVERS.NET      internet address = 192.112.36.4
F.ROOT-SERVERS.NET      internet address = 192.5.5.241
B.ROOT-SERVERS.NET      internet address = 128.9.0.107
J.ROOT-SERVERS.NET      internet address = 192.58.128.30
```

Root Name Servers

Servidor	Operador	Localização
A	Verisign	EUA
B	Information Sciences Institute	EUA
C	Cogent Communications	EUA
D	University of Maryland	EUA
E	NASA Ames Research Center	EUA
F	Internet Software Consortium	Mundo
G	U.S. DOD Network Information Center	EUA
H	U.S Army Research Lab	EUA
I	Autonomica	Europa
J	VeriSign Global Registry Services	EUA
K	Reseaux IP Europeens – Network Coordination Centre	Europa
L	Internet Corporation for Assigned Names and Numbers	EUA
M	WIDE Project	Japão

Root Name Servers

- **Problemas**
  - Protocolo DNS permite somente 13 “root name servers”
    - Como disponibilizar servidores DNS espalhados em cada continente?
  - Disponibilidade do serviço
    - Quanto mais próximo um servidor DNS raíz, menor a indisponibilidade do serviço
  - Latência de resolução
    - Quanto mais próximo um servidor DNS raíz, menor a latência de resolução

Root Name Servers

- **f.root-servers.net**
  - Conjunto de servidores DNS
  - Distribuídos pelo mundo
  - Endereço
    - IPv4 = 192.5.5.241
    - IPv6 = 2001:500::1035
  - Serviço roteado por “anycast”
  - Maiores detalhes:
    - http://f.root-servers.org/

Auckland	Nova Zelandia
São Paulo	Brasil
Hong Kong	China
Joanesburgo	Africa do Sul
Los Angeles	EUA
Nova York	EUA
Madri	Espanha
Palo Alto	EUA
Beijing	China
Roma	Italia
Seul	Coreia
São Francisco	EUA
San Jose	EUA
Moscow	Russia
Otawa	Canada

Root name servers

- **20/08/2003**
  - Disponibilizado o primeiro servidor DNS raiz na América Latina.
  - Localização: São Paulo
  - Mantido por: registro.br
  - Réplica do “f.root-servers.net” mantido pela ISC (Internet Software Consortium, Inc)
  - Anúncio:
    - http://www.isc.org/ISC/news/pr-08202003.html
  - Vantagens
    - Maior disponibilidade do serviço DNS
    - Menor latência de resolução

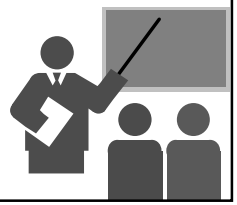
 45

Root Name Servers

- **Anycast**
  - Forma de roteamento de supernet no backbone da Internet
  - www.isc.org/tn/isc-tn-2003-1.html

 46

Autoritative & Delegated



 47

Autoritative

- ***Autoritative***
  - Possuir em sua base de dados as informações sobre as resoluções de um determinado domínio
- **Não *autoritative***
  - O servidor não possui, em sua base de dados local, as informações sobre uma resolução,
  - Mas, responde pois está em seu cache.
- **Problemas**
  - Um servidor de uma zona não está resolvendo como *autoritative*
    - Um servidor primário ou secundário pode se considerar não *autoritative* se existir um erro de sintaxe nos mapas das zonas.

 48

Delegated

- ***Delegated***
  - Ser indicado por um servidor de nível superior para responder a um subdomínio seu

 49

Delegação de domínio

- **Para verificar se seu domínio esta delegado:**
  - domínio direto:
    - nslookup -type=soa <domínio>
  - domínio reverso (domínio a.b.c.*)
    - nslookup -type=soa c.b.a.in-addr.arpa
    - nslookup -type=soa b.a.in-addr.arpa
    - nslookup -type=soa a.in-addr.arpa
- **Exemplos**
  - nslookup -type=soa lsi.usp.br
  - nslookup -type=soa 161.107.143.in-addr.arpa

 50

Autoritative x *Delegated*

- ***Autoritative* e *Delegated***
  - aspectos totalmente distintos
  - porém relacionados
- **Um servidor (primário ou secundário) de uma zona XYZ deve ser sempre:**
  - *autoritative* para a zona XYZ
    - ou seja, ser quem fornece os mapas para a zona
  - *delegated* para a zona XYZ
    - ou seja, os servidores de nível superior na hierarquia de domínio delegam a ele a tarefa de responder pela zona

 51

Autoritative x Delegated

- **Quando ocorrem problemas**

(1) servidor *autoritative* e não *delegated* para a zona XYZ
- o servidor está fornecendo os mapas da zona XYZ cuja resolução não está delegada a ele
- Possíveis causas:
  - problema nos servidores de níveis superiores (por não delegarem a zona)
  - ou, este servidor não deveria estar fornecendo as resoluções da zona XYZ
    - afeta somente as máquinas locais

 52

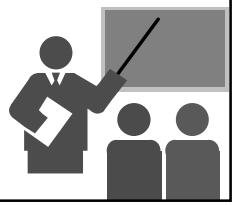
Autoritative x *Delegated*

- **Quando ocorrem problemas (cont.)**

(2) não *autoritative*, mas *delegated* para a zona XYZ
- *lame delegation*
- Isto é um erro de configuração
- Possíveis causas:
  - Erro no servidor da zona XYZ
    - O servidor da zona XYZ esta mal configurado
    - não contém as entradas NS configuradas de forma correta (“NS XYZ.abc.kmp.”)
  - Erro no servidor de nível superior
    - Os servidores de nível superior não deveriam estar delegando a zona XYZ para o servidor

 53

Implementação de servidores DNS



 54

Implementações de servidores DNS

- **Bind**
  - "*Berkeley Internet Name Domain*"
  - Mantido pela ISC ("*Internet Software Consortium"*)
  - Implementação mais utilizada
  - Livre para uso, redistribuição e incorporação em outros produtos
  - Site: http://www.isc.org/bind
  - Versões
    - Bind v4.x (sendo descontinuada)
    - Bind v8.x (primeira versão em maio 1997)
    - Bind v9.x (versão recomendada)

 55

Implementações de servidores DNS

- **Acesse o site www.isc.org e verifique qual a versão mais recente do programa Bind**
  - Versão mais recente do bind: _____

- **Perguntando qual a versão do programa DNS "bind"utilizado:**
  - nslookup

    set class=chaos

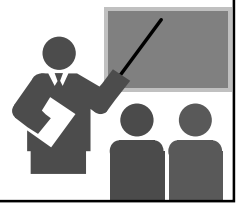
    set q=txt

    version.bind

    exit

 56

Portas UDP e TCP utilizadas



 57

Portas UDP e TCP utilizadas

- **Requisições entre cliente (resolver) e servidor DNS**
  - Requisições curtas:
    - Requisição: UDP alto -> 53
    - Resposta: UDP 53 -> alto
  - Requisições longas
    - Requisição: TCP alto -> 53
    - Resposta: TCP 53 -> alto

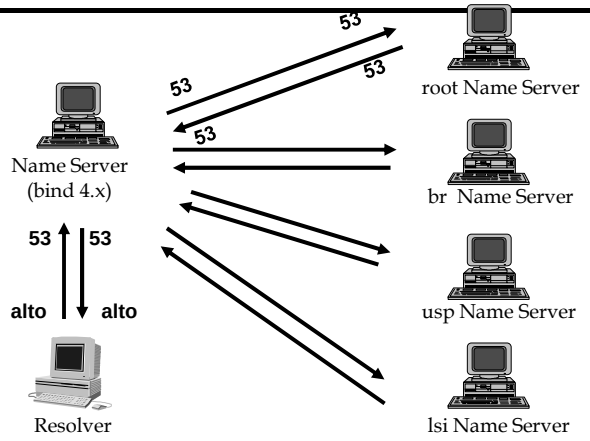
 58

Portas UDP e TCP utilizadas

- **Requisição (recursiva) entre um servidor DNS bind 9.x e outro servidor DNS**
  - Requisições curtas
    - Requisição: UDP alto -> 53
    - Resposta: UDP 53 -> alto
  - Requisições longas, servidor bind 4.x
    - Requisição: TCP alto -> 53
    - Resposta: TCP 53 -> alto
  - OBS: Bind 8.x permite alterar endereço e porta UDP
    - "query-source address * port *" (default)
      - utiliza qualquer endereço da máquina e porta alta
    - "query-source address 143.107.161.220 port 53"
      - utiliza através da interface 143.107.161.220 com porta 53

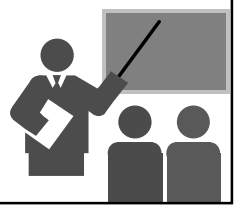
 59

Portas UDP e TCP utilizadas



 60

Referências



 61

Referências

- **Livros:**
  - DNS and BIND
    Albitz, P; Liu, Cricket.
    O'Reilly & Associates, Inc
  - Internet Security - Professional Reference
    Autikns, Derek et. all
    New Riders
- **Artigos:**
  - Name Server Operations Guide for BIND, release 4.9.5.
    Vixie, Paul.

 62

Referências

- **Internet RFC's:**
  - RFC 1034 - Domain Names - Concepts and Facilities
  - RFC 1035 - Domain Names - Implementation and Specification
  - RFC 1033 - Domain Administrator Guide
  - RFC 1713 - Tools for DNS debugging
- **Sites:**
  - www.isc.org/