



Introdução ao DNS

Volnys Borges Bernal

volnys@lsi.usp.br

<http://www.lsi.usp.br/~volnys>

Laboratório de Sistemas Integráveis

<http://www.lsi.usp.br/>



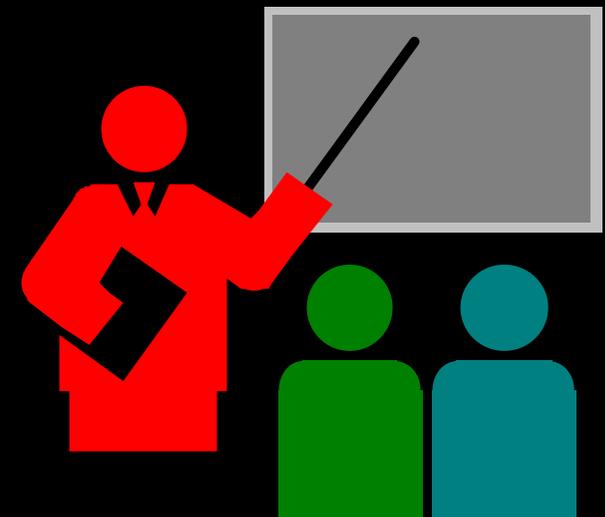


Agenda

- ❑ O que é DNS?
- ❑ Servidores DNS
- ❑ Requisição DNS
- ❑ *Caching*
- ❑ *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 necessário para todos os computadores que utilizam a Internet**
- ❑ **Serviço que permite a resolução dos nomes de um domínio**
 - ❖ tradução: nome -> IP
 - ❖ tradução: IP -> nome
- ❑ **Protocolo DNS**
 - ❖ RFC 1034 - Domain Names - Concepts and Facilities
 - ❖ RFC 1035 - Domain Names - Implementation and Specification



O que é DNS?

❑ O funcionamento do protocolo DNS:

❖ Existem dois tipos de entidades:

⇒ “Resolver”

- ◆ entidade cliente
- ◆ realizam requisições para de resolução de nomes/endereços

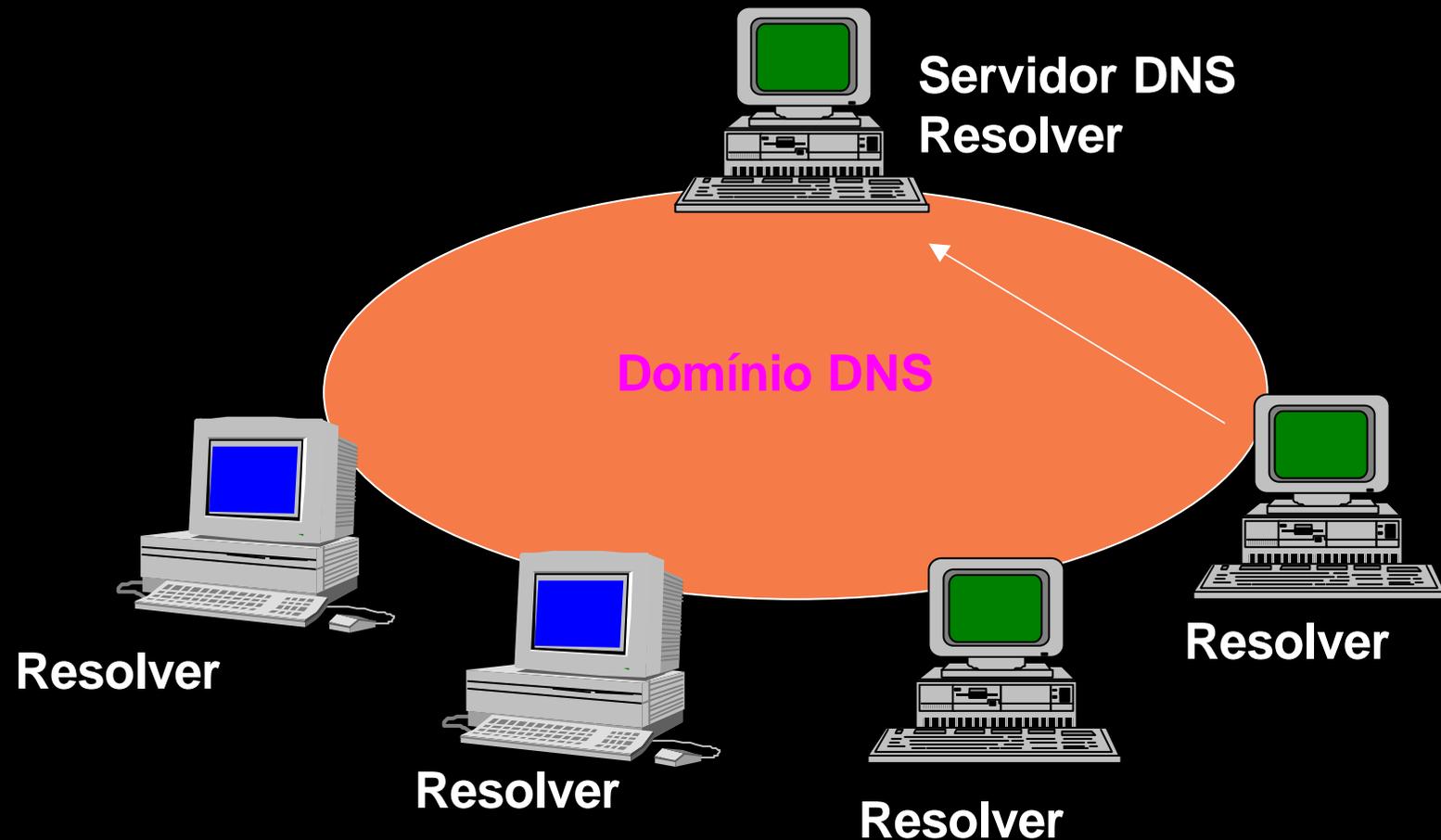
⇒ “Name Server”

- ◆ entidade servidora
- ◆ respondem às requisições de resolução de nome/endereço
- ◆ são capazes de traduzir nome para IP e vice versa
- ◆ é necessário existir no mínimo 2 servidores por domínio
 - 1 servidor primário
 - 1 ou mais servidores secundários



O que é DNS?

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





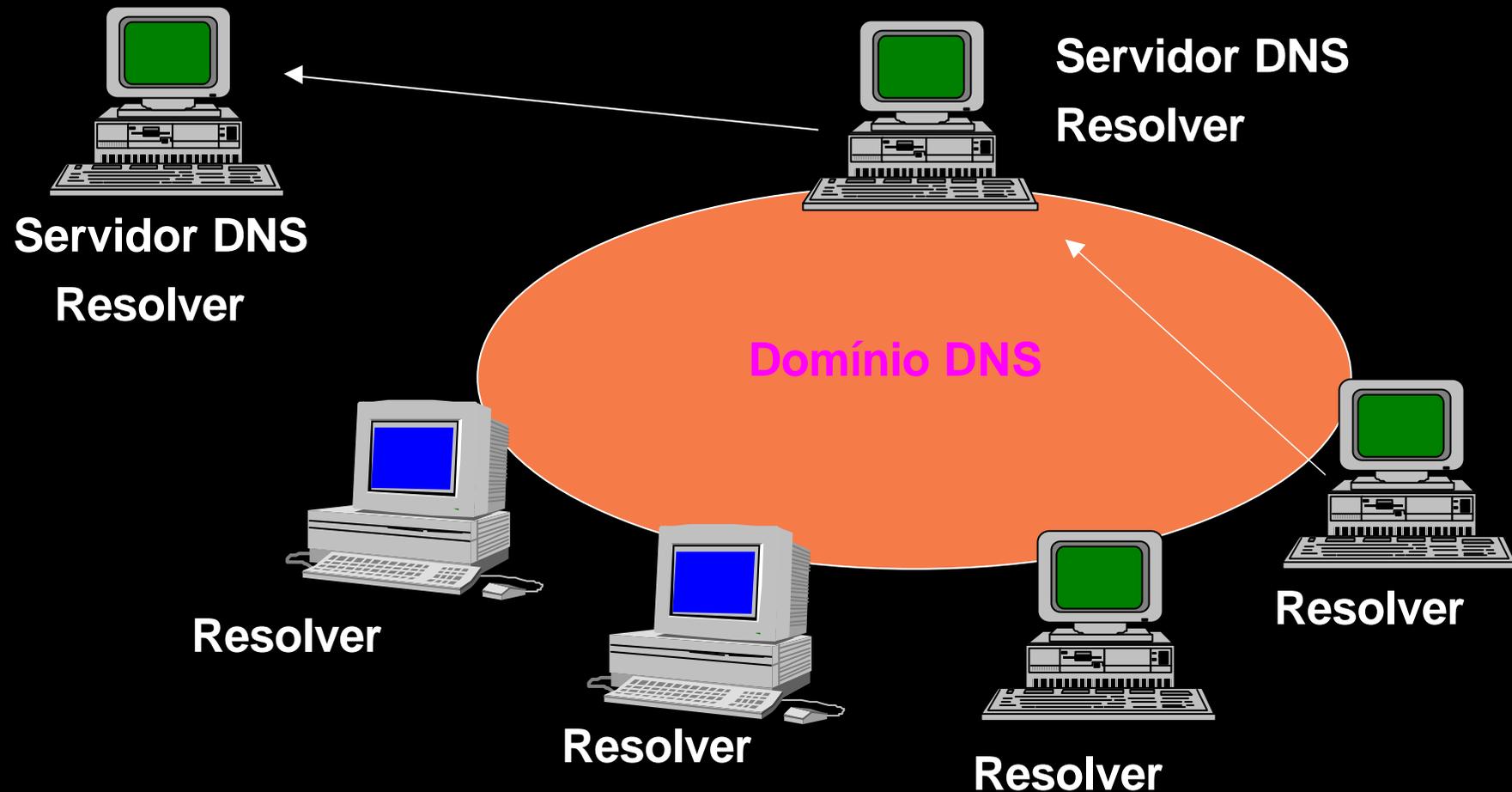
O que é DNS?

- ❑ **Parece um serviço simples, mas é complexo**
 - ❖ Base de dados distribuída pelo mundo
 - ❖ Um servidor de nomes também pode realizar requisições para outros “Servidores de nomes”



O que é DNS?

- ❑ Servidor pede tradução a um outro servidor

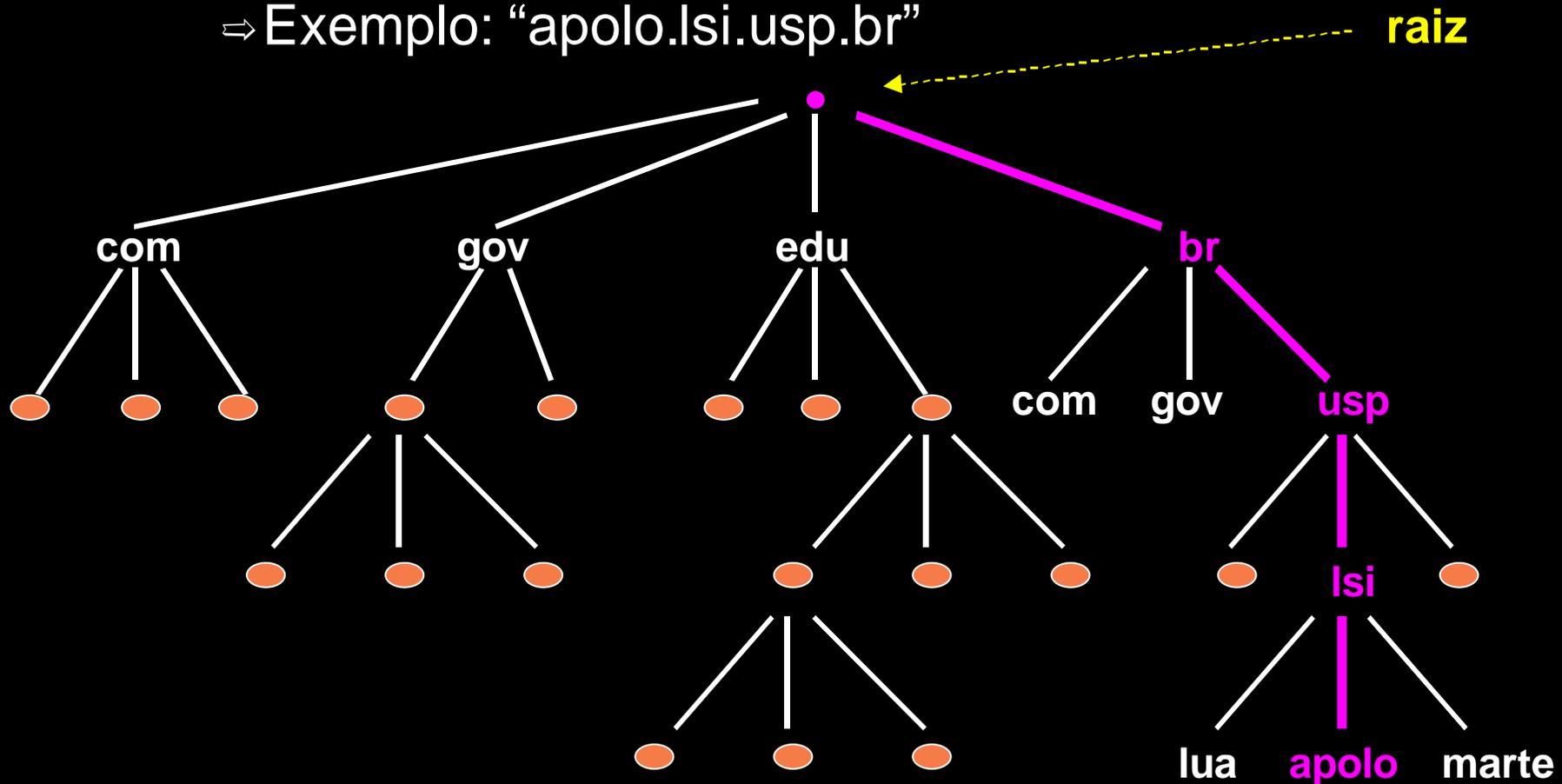


O que é DNS?

□ Árvore de nomes da Internet

❖ Semelhante a uma hierarquia de arquivos

⇒ Exemplo: “apolo.lsi.usp.br”





O que é DNS?

❑ Nomes do primeiro nível

- ❖ com
- ❖ edu
- ❖ gov
- ❖ mil
- ❖ net
- ❖ org
- ❖ arpa
- ❖ br
- ❖ fr
- ❖ us
- ❖



O que é DNS?

□ Nome

- ❖ **Absoluto** ou “*Full-qualified domain name*” (FQDN)

 - ⇒ apolo.lsi.usp.br.

- ❖ **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

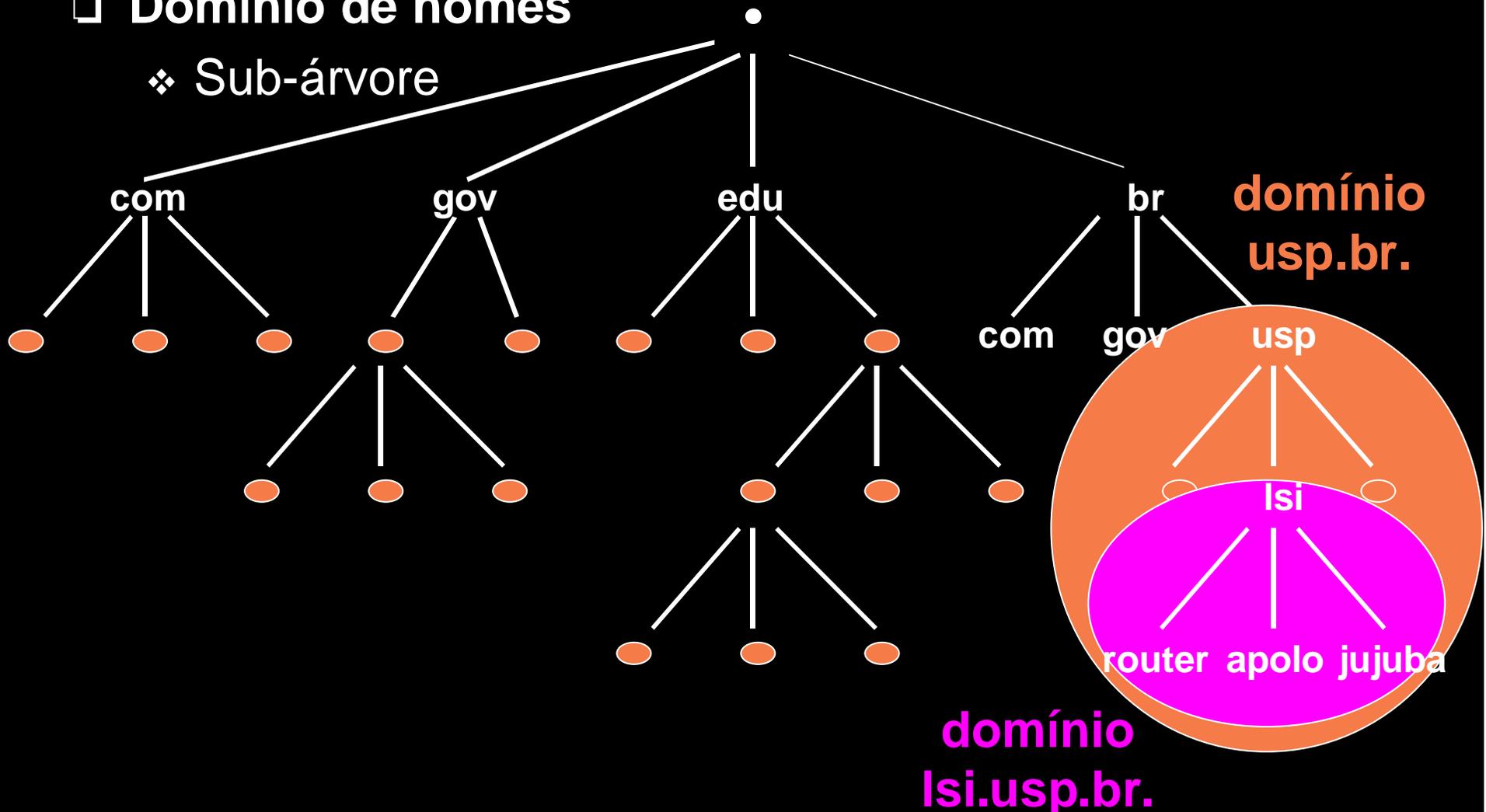
- ❖ Caracteres válidos: “a”-”Z” ”a”-”z” ”0”-”9” “.” “-”



O que é DNS?

□ Domínio de nomes

❖ Sub-árvore





Exemplo

❑ Pedindo para traduzir um nome

❖ nslookup

apolo.lsi.usp.br

www.lsi.usp.br

exit

❑ Pedindo para traduzir um endereço

❖ nslookup

143.107.161.220

exit



Exemplo

- ❑ Perguntando quais são os “*name servers*” de um domínio

- ❖ nslookup
set q=NS
lsi.usp.br
exit

- ❑ Perguntando dados sobre um domínio

- ❖ nslookup
set q=SOA
lsi.usp.br
exit

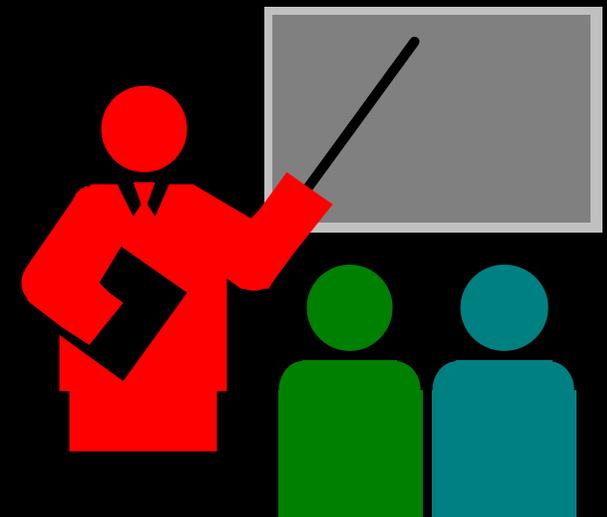


Exemplo

- ❑ Perguntando quais são os “*mail exchangers*” de um domínio
 - ❖ nslookup
 - set q=MX
 - lsi.usp.br
 - exit



Servidores DNS





Servidores DNS

- ❑ **Existem milhares de servidores de nomes espalhados pelo mundo.**

- ❑ **Podem ser divididos em:**
 - ❖ *“Root Name Servers”*
 - ⇒ São os servidores responsáveis pelo domínio da raiz
 - ❖ Servidores de zona (domínio)
 - ⇒ São os servidores dos outros domínios



Servidores DNS

❑ “*Root Name Servers*”

- ❖ Respondem requisições sobre servidores de nomes do primeiro nível da árvore
- ❖ Existem vários “*Root Name Servers*” espalhados pelo mundo
- ❖ Quando um servidor local não consegue resolver um determinada requisição esta é repassada a um “*Root Name Server*”.
- ❖ Fundamental para o serviço DNS: se todos falharem todas as resoluções na Internet irão falhar
- ❖ Os “*Name Servers*” devem possuir uma lista atualizada de todos os “*Root Name Servers*”

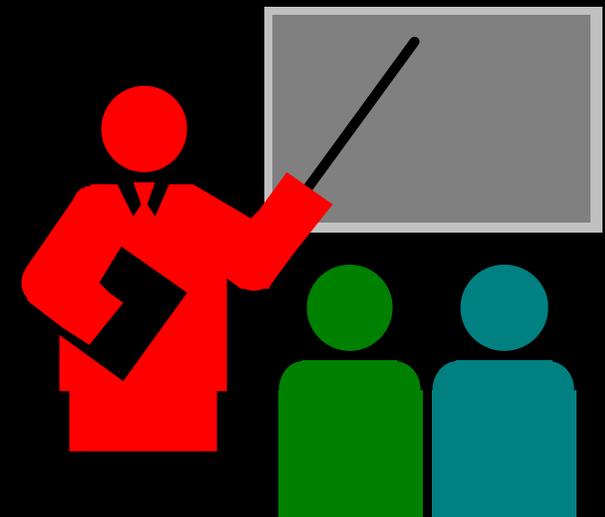


Servidores DNS

- ❑ **Para cada domínio Internet são necessários ao menos 2 servidores:**
 - ❖ 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



Resolvers



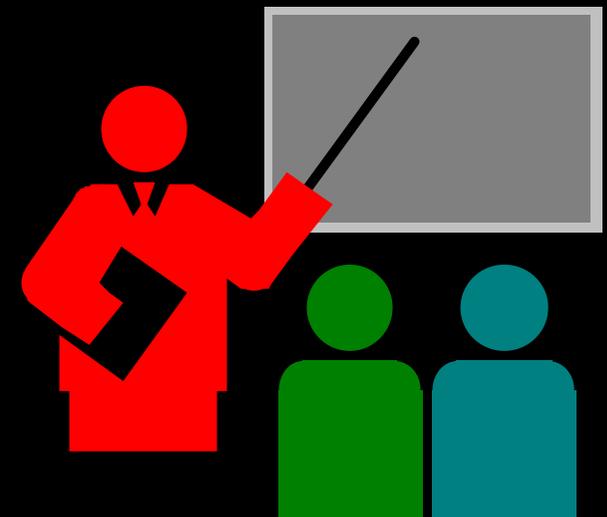


Resolvers

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



Requisição DNS





Requisição DNS

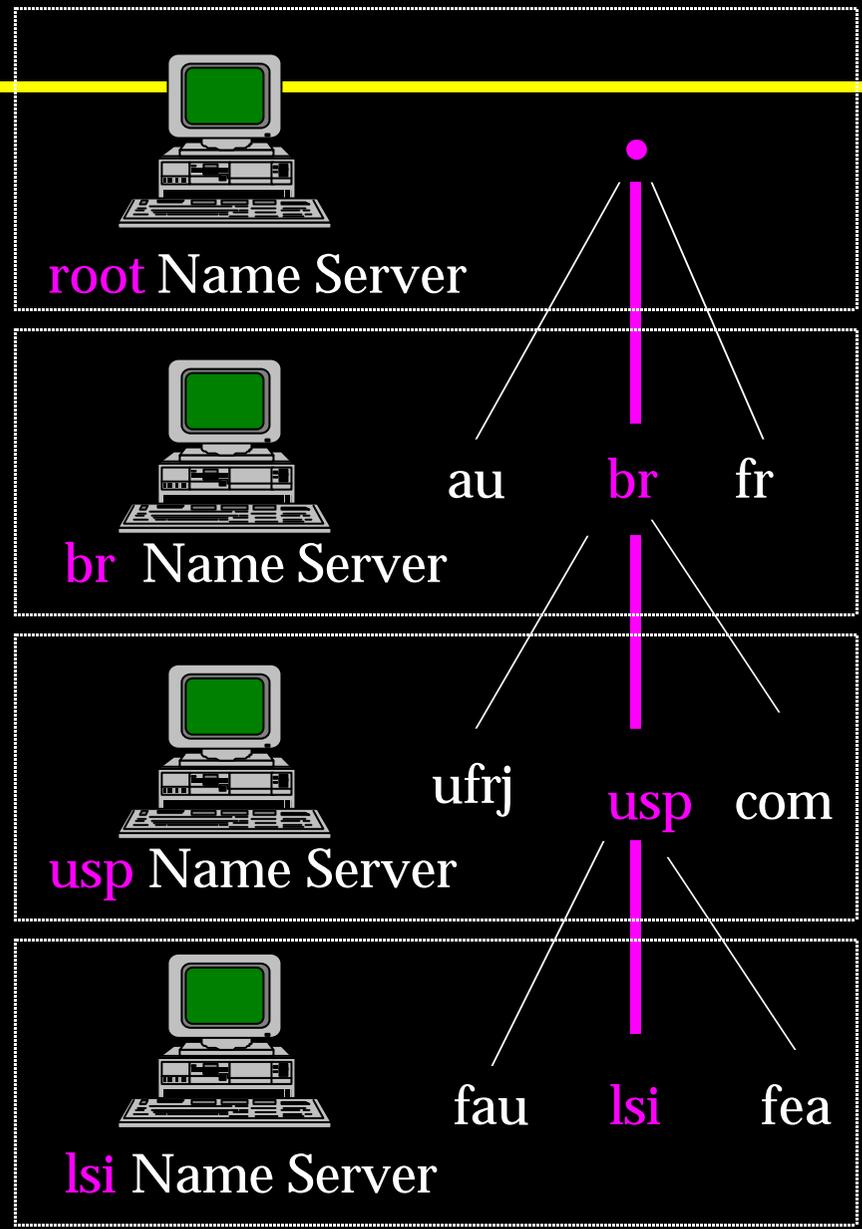


Name Server

1 **www.lsi.usp.br?**
9 **endereço**
www.lsi.usp.br



Resolver





Requisição DNS

❑ Requisição Recursiva

- ❖ Obriga ao servidor retornar a resposta ou, se não encontra-la, um erro.
- ❖ Para isso, o servidor pode necessitar consultar outros servidores de nomes
- ❖ Normalmente gerada pelos “*resolvers*”
- ❖ Mais complexa de ser tratada



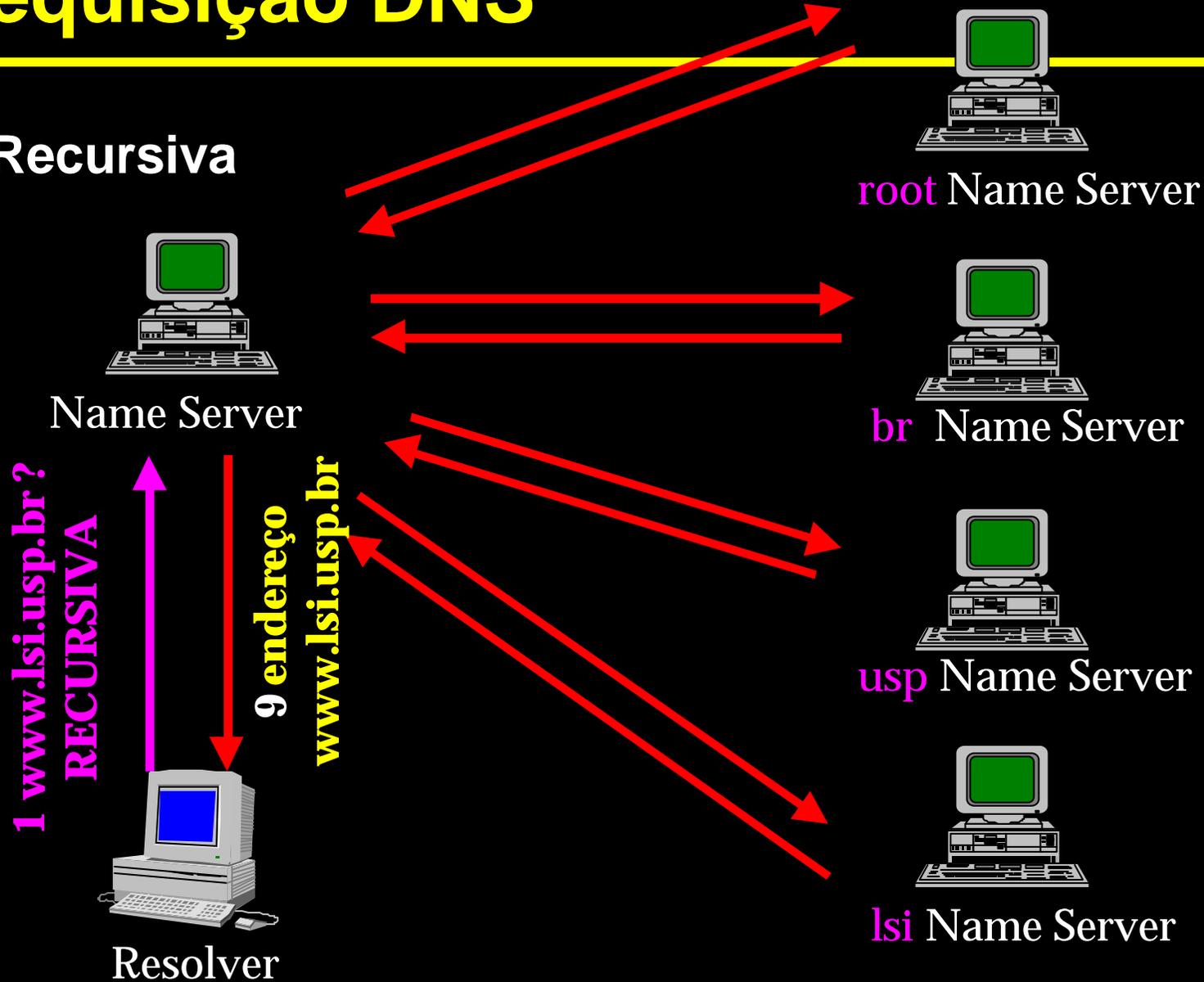
Requisição DNS

- ❑ **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



Name Server



Resolver

www.lsi.usp.br?
INTERATIVA

br name server



root Name Server



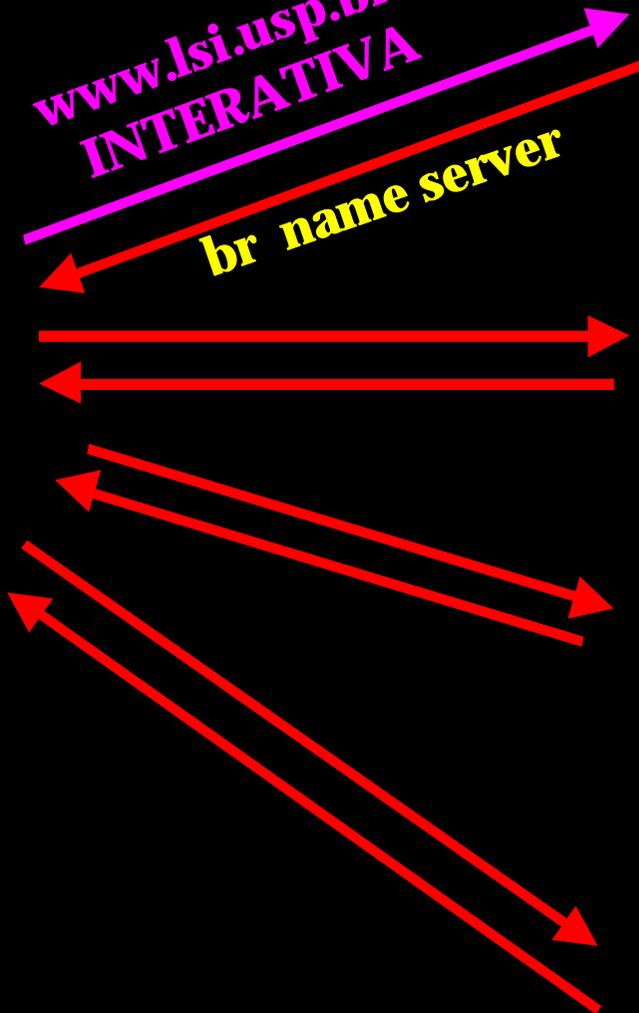
br Name Server



usp Name Server

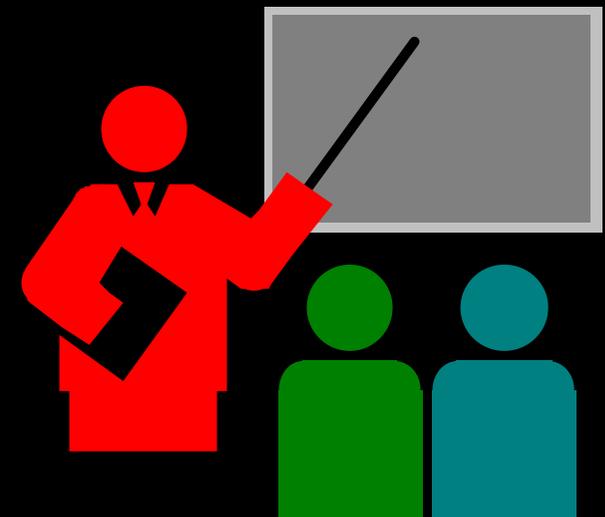


lsi Name Server





Caching



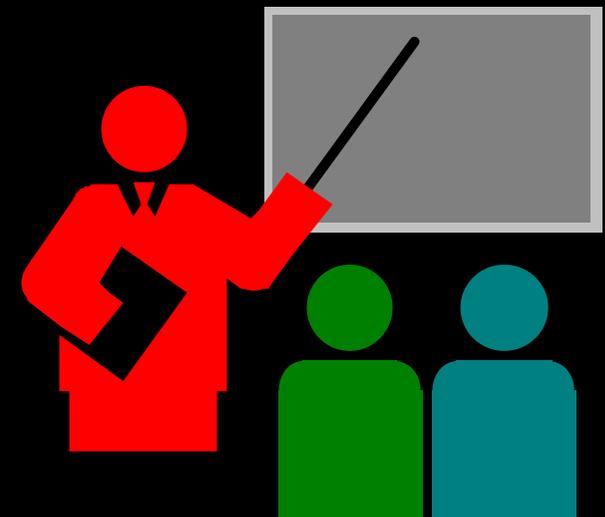


Caching

- ❑ **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



Autoritative & Delegated





Authoritative

❑ ***Authoritative***

- ❖ Possuir em sua base de dados as informações sobre as resoluções de um determinado domínio

❑ ***Não authoritative***

- ❖ 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 *authoritative*
 - ⇒ Um servidor primário ou secundário pode se considerar *não authoritative* se existir um erro de sintaxe nos mapas das zonas



Delegated

❑ *Delegated*

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



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



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



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



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

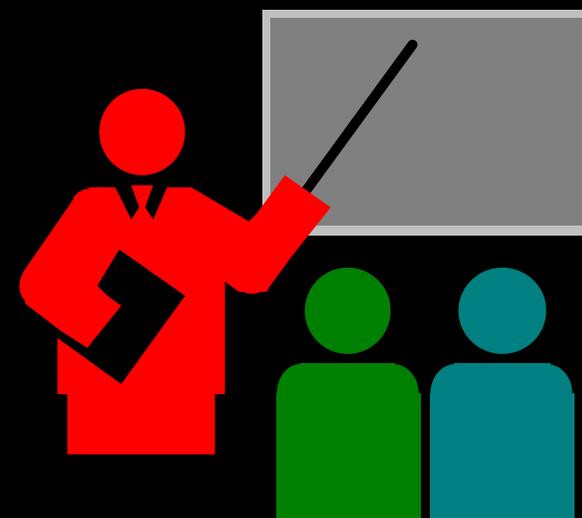
– não contém as entradas NS configuradas de forma correta (“NS XYZ.abc.kmp.”)

◆ Erro no servidor de nível superior

– Os servidores de nível superior não deveriam estar delegando a zona XYZ para o servidor



Implementação de servidores DNS





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 (com tendência a ser descontinuado)
 - ◆ Não possui várias configurações de segurança que são suportadas pela versão 8
 - ⇒ Bind v8.x (primeira versão em maio 1997)



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 v8: _____

- ❑ **Perguntando qual a versão do programa DNS utilizado:**

- ❖ nslookup

- set class=chaos

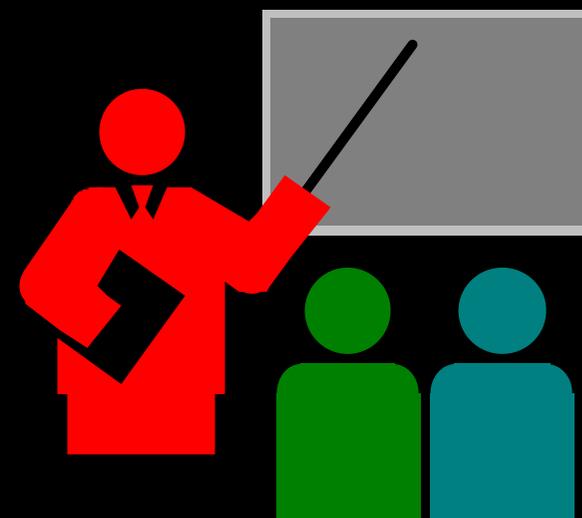
- set q=txt

- version.bind

- exit



Portas UDP e TCP utilizadas





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



Portas UDP e TCP utilizadas

❑ Requisição (recursiva) entre um servidor DNS bind 4.x e outro servidor DNS

❖ Requisições curtas

⇒ Requisição: UDP 53 -> 53

⇒ Resposta: UDP 53 -> 53

❖ Requisições longas, servidor bind 4.x

⇒ Requisição: TCP 53 -> 53

⇒ Resposta: TCP 53 -> 53

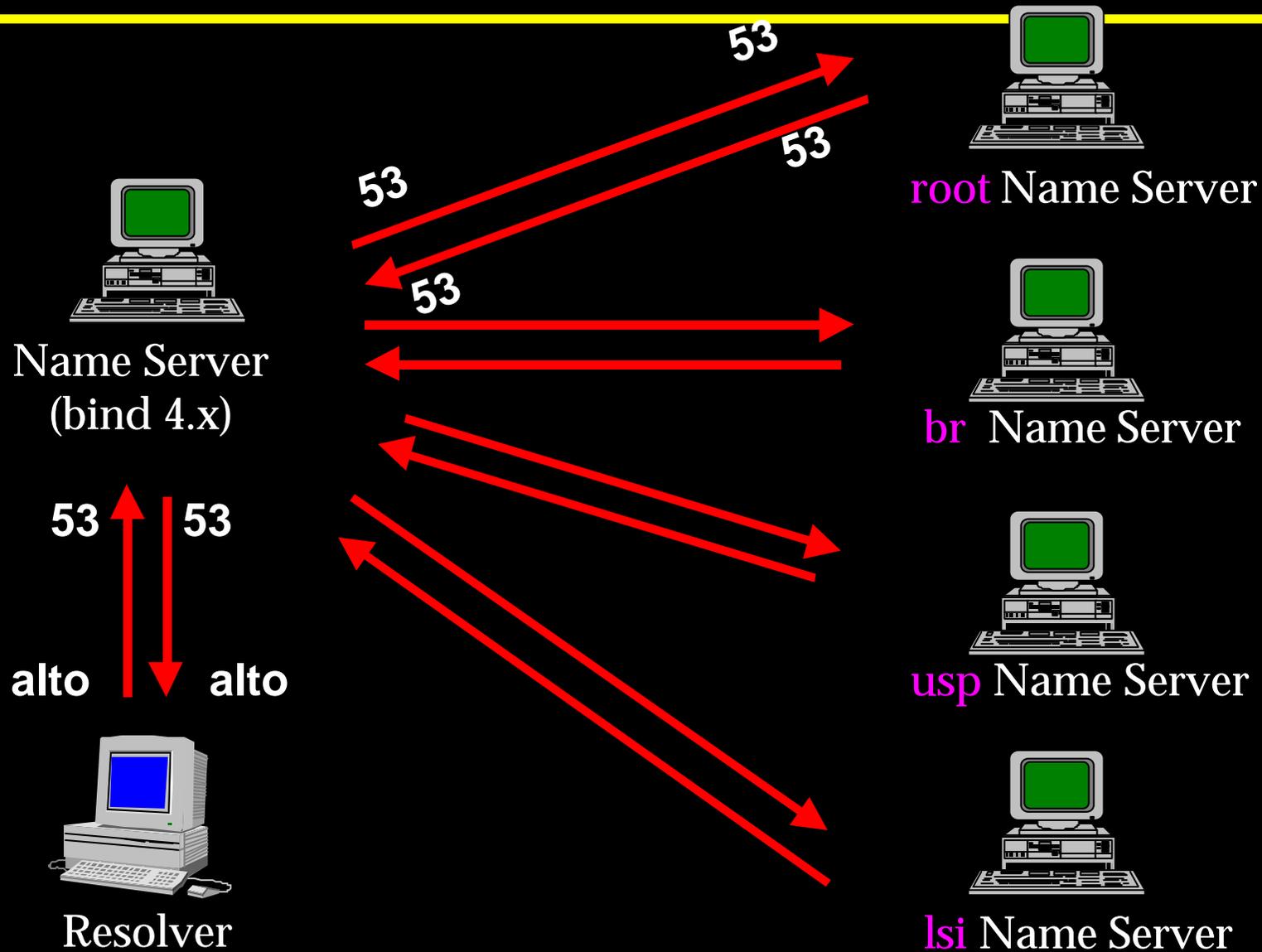


Portas UDP e TCP utilizadas

- ❑ **Requisição (recursiva) entre um servidor DNS bind 8.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

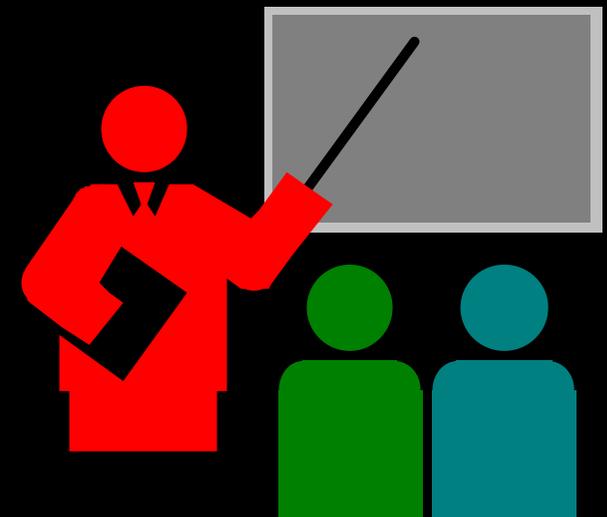


Portas UDP e TCP utilizadas





Referências





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.



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/