Administração de Redes de Computadores

DNS – Domain Name System

Bind / Named

Alexssandro C. Antunes
(Alexssandro.Antunes@unisul.br)

História

- No início da “Internet”, ou seja, utilização do TCP/IP na ARPANET, como existiam poucos computadores, existia uma lista (*tabela estática*) chamada de hosts.txt, que continha os nomes de todos os computadores da Rede (continha linhas relacionando nomes com números IP).
- Mantinda de forma centralizada pelo DOD NIC (*Departamento of Defense Network Information Center*)
- Problemas com o crescimento do número de hosts.
- Difícil manutenção e/ou atualização.
- O Sistema DNS, aboliu a centralização da informação.

Conceitos

Domínio

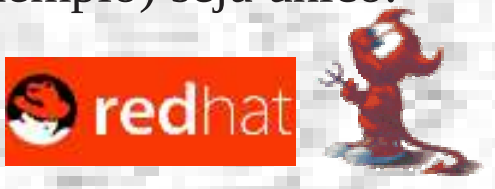
Foi concebido com o objetivo de facilitar a memorização dos endereços de computadores na Internet.

Parte da hierarquia de domínios identificada por um nome de domínio.

Nome que serve para localizar e identificar conjuntos de computadores na Internet.

Um nome de domínio é composto por palavras separadas por pontos, e que se tornam menos genéricas da direita para a esquerda.

Exemplo: terra.com.br é um domínio onde o .br significa que trata-se de um domínio registrado no Brasil, .com significa que este é um domínio de cunho comercial e terra é o nome da empresa.
Importante - todo o conjunto (terra.com.br, no nosso exemplo) seja único.



Conceitos (cont.)

Generic Top Level Domains (gTLD)

Indicam apenas a área em que o registrante atua sem associá-lo a um país específico.

Disponíveis:

.COM para entidades comerciais;

.NET para entidades com serviços de rede ou telecomunicações;

.ORG para organizações sem fins lucrativos, entre outros.

Conceitos (cont.)

Country Code Top Level Domains (ccTLD)

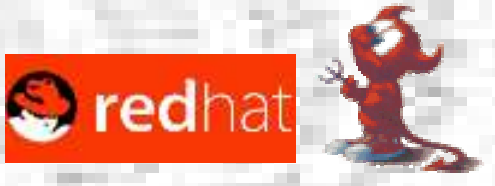
Indicam o país em que o domínio é registrado (códigos de países).

Exemplo: .BR refere-se ao Brasil; .FR à França; .DE à Alemanha e assim por diante.

Cada país mantêm órgãos responsáveis por regulamentar e concentrar as atividades de registro de domínios no ccTLD correspondente.

Determinar os TLD disponíveis em cada ccTLD é também responsabilidade destes órgãos.

Exemplo (TLD no Brasil): .COM.BR ; .EDU.BR; .ORG.BR; .NET.BR; entre outros.



Zonas

Zonas (zone)

- Informações contidas em um arquivo do banco de dados do DNS relativas a uma rede sobre a qual um servidor de DNS tem autoridade.
- Parte de um domínio pela qual um servidor é responsável.
- 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

Registro de Domínio

- **InterNIC**

(Órgão do Departamento de Comércio do Governo dos Estados Unidos)

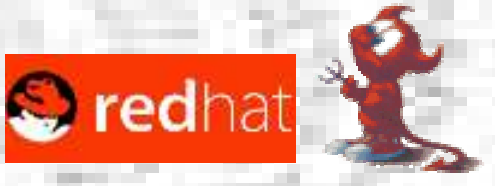
Responsável pelo registro de domínios com terminação .com, .org, .net .info .biz .us, entre outros.
Desde 1993, este órgão se associou à algumas empresas privadas, que são responsáveis pela atribuição de nomes de domínio com as extensões acima citadas. Os domínios lá registrados não possuem extensão designando o país.

http://www.networksolutions.com

- **FAPESP**

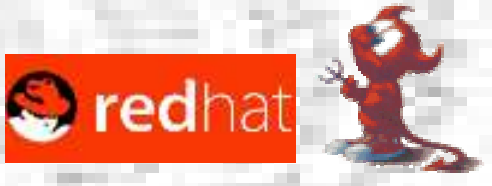
(Fundação de Amparo à Pesquisa do Estado de São Paulo)

Órgão responsável pelo registro e manutenção dos domínios .br .
Todos os domínios com terminação .br são registrados na FAPESP.
http://www.registro.fapesp.br
http://.registro.br



Registro de Domínio (cont.)

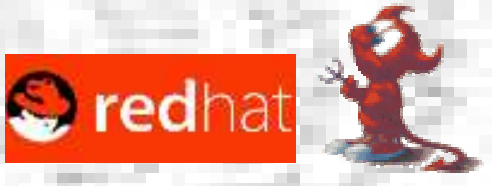
- No Brasil - FAPESP (Fundação de Amparo à Pesquisa de São Paulo)
  - Brasil Pagamento de R$ 30,00 por domínio/ano.
- Verificação de registros.
- Domínios: necessidade de registro.
- Subdomínios: gerenciados pelo administrador de redes.
- Necessário que o domínio não esteja registrado.
- Necessário dois servidores de DNS para responder pelo domínio.



DNS: Problemas com endereços lógicos - Internet Protocol

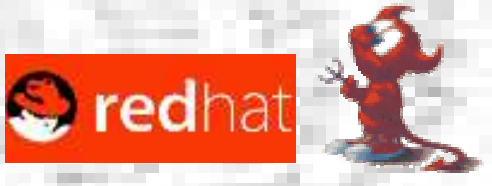
“...os usuários de uma rede sabem o nome da máquina, mas raramente conhecem o endereço IP correspondente...”

192.31.7.130	CISCO.COM
204.71.177.35	YAHOO.COM
152.163.210.7	AOL.COM
198.150.15.234	MAT-MADISON.COM
207.46.131.15	MICROSOFT.COM
192.233.80.9	NOVELL.COM



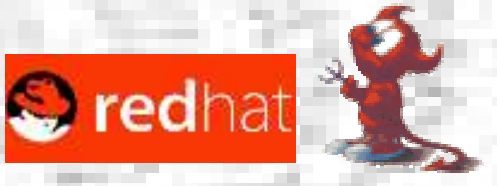
O que é DNS?

- The DNS server is a device on a network that manages domain names and responds to requests from clients to translate a domain name into the associated IP address.
- The DNS system is set up in a hierarchy that creates different levels of DNS servers.



O que é DNS? (cont.)

- DNS é a sigla para **Domain Name System** e/ou “Domain Name Service”.
- É uma base de dados hierárquica, distribuída para a resolução de nomes de domínios em endereços IP e vice-versa.
- Descrito originalmente pelas RCF 1033, RFC 1034 e RCF 1035.



Funcionalidade

•Simplificar a utilização da Internet, convertendo nomes simbólicos em seus respectivos endereços lógicos (ip´s) que são únicos.

Exemplo: unisul.br = 200.18.12.1

www.terra.com.br = 200.176.3.142

• Consulta reversa, converter endereços lógicos (ip´s) em nomes simbólicos.

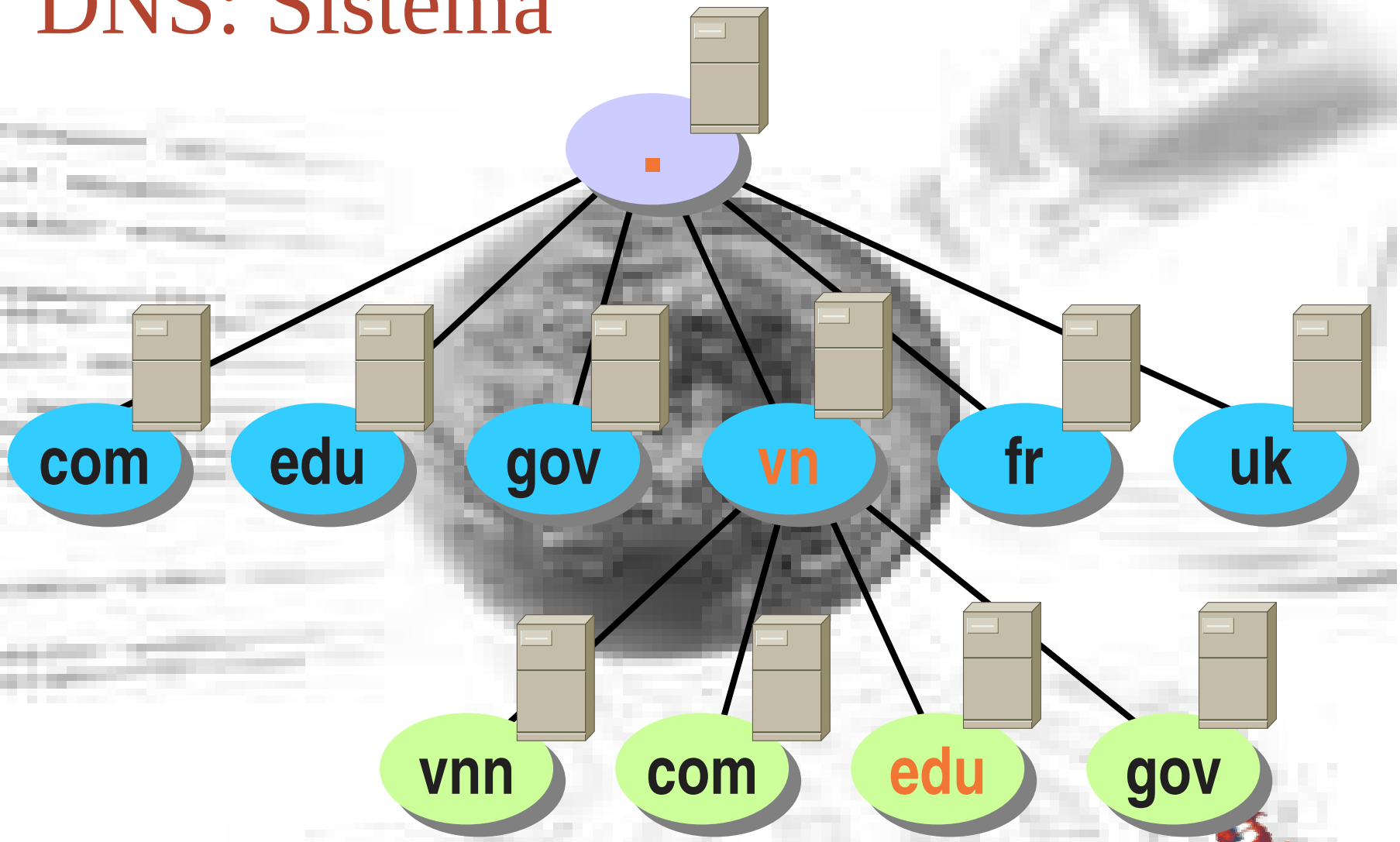
Exemplo: 200.18.12.1 = unisul.br

200.176.3.142 = www.terra.com.br

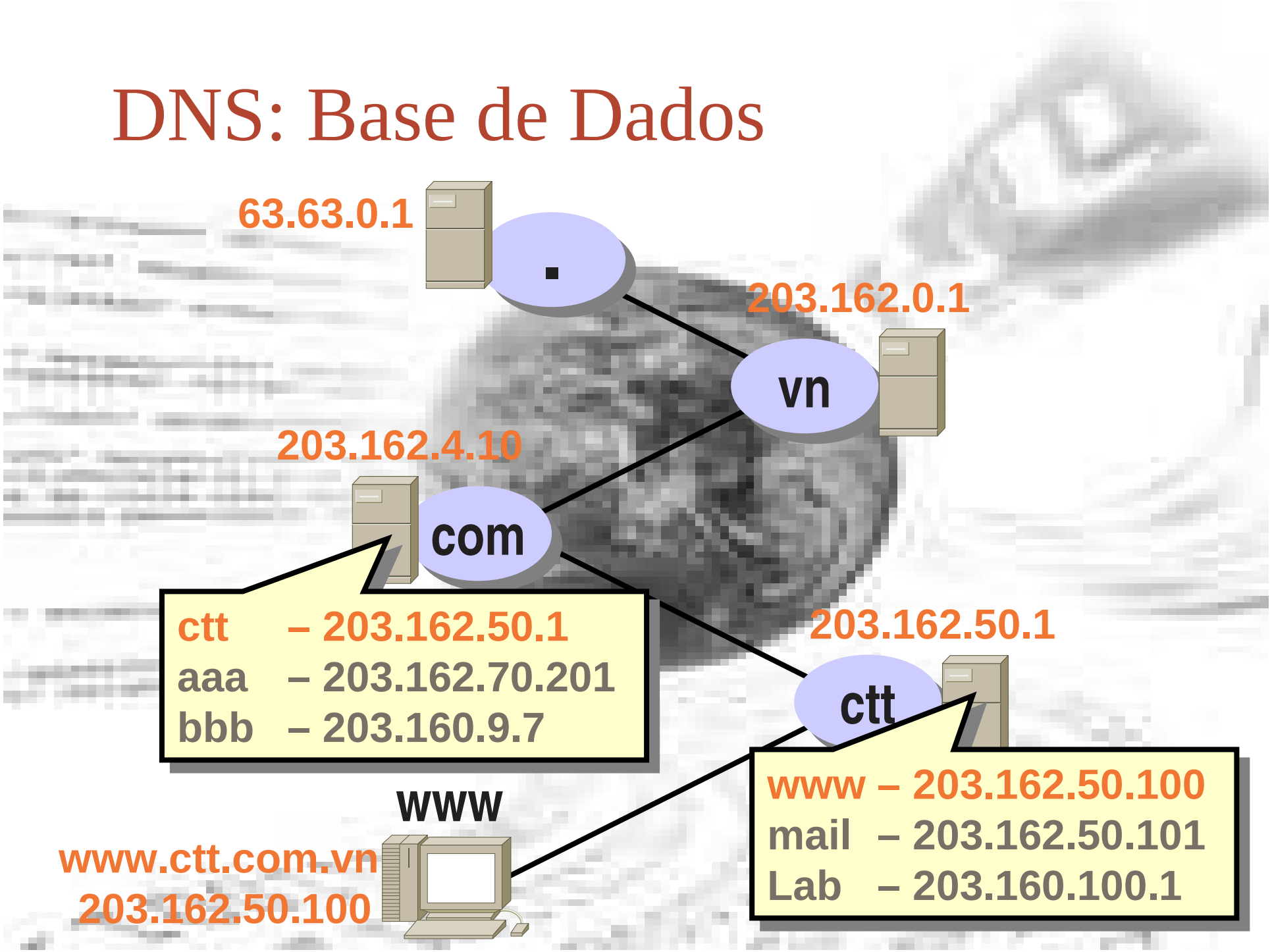
•Sempre que utilizar um serviço que usa o nome de um computador.

Exemplo: e-mail, web, ftp, irc, telnet, ssh, chat, etc.

DNS: Sistema

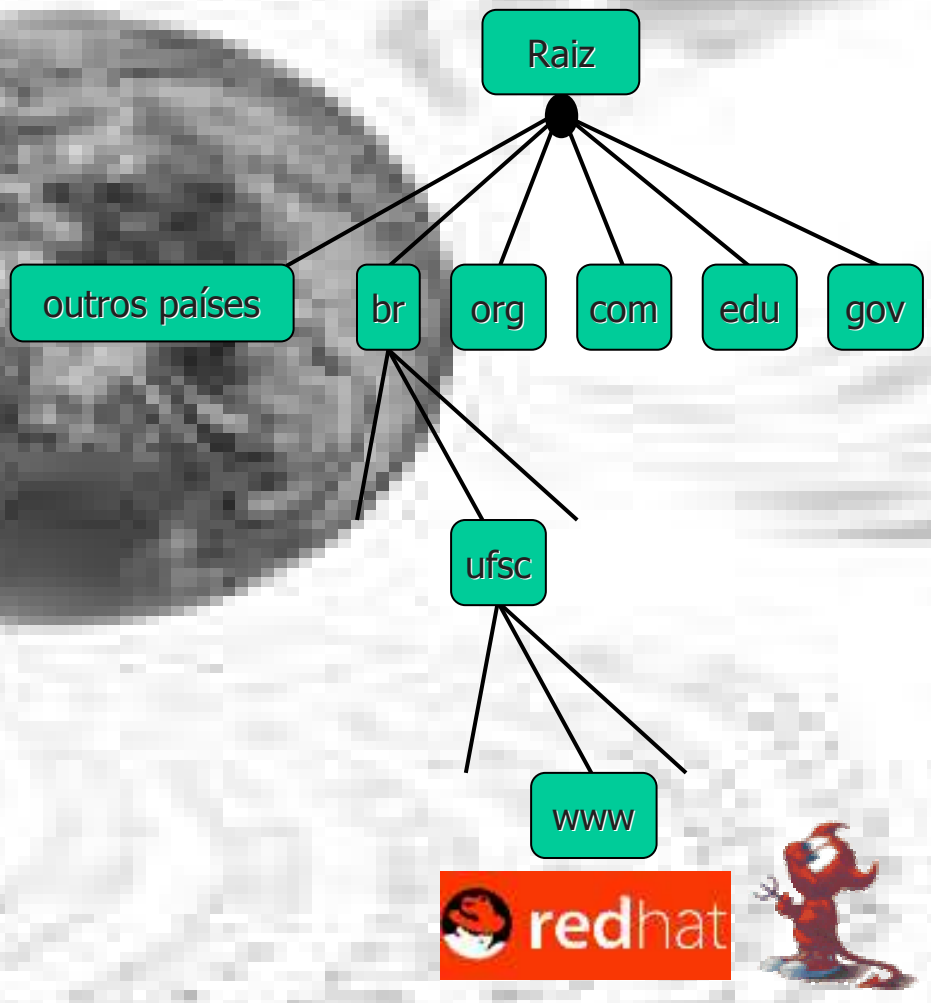


DNS: Base de Dados

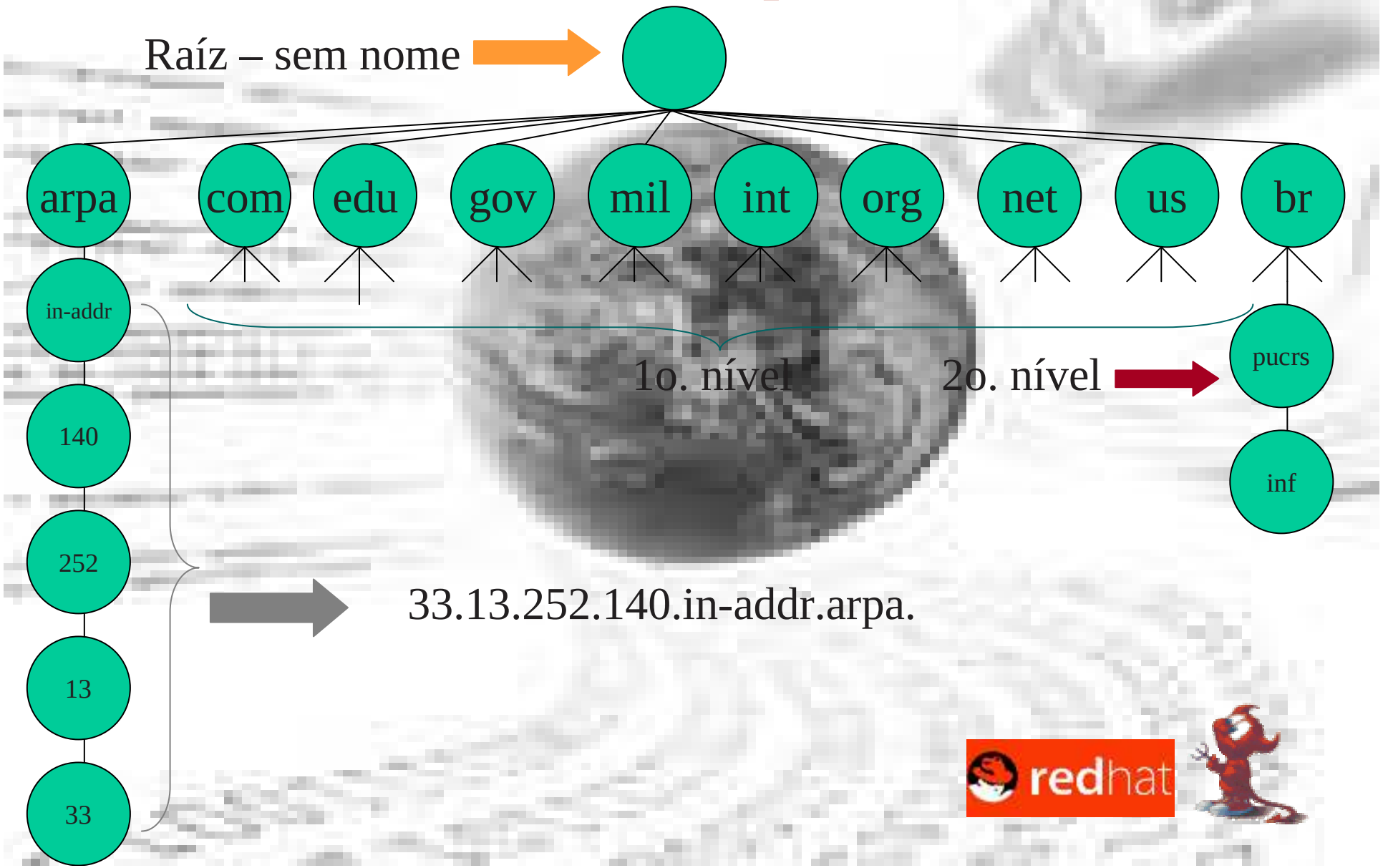


Características

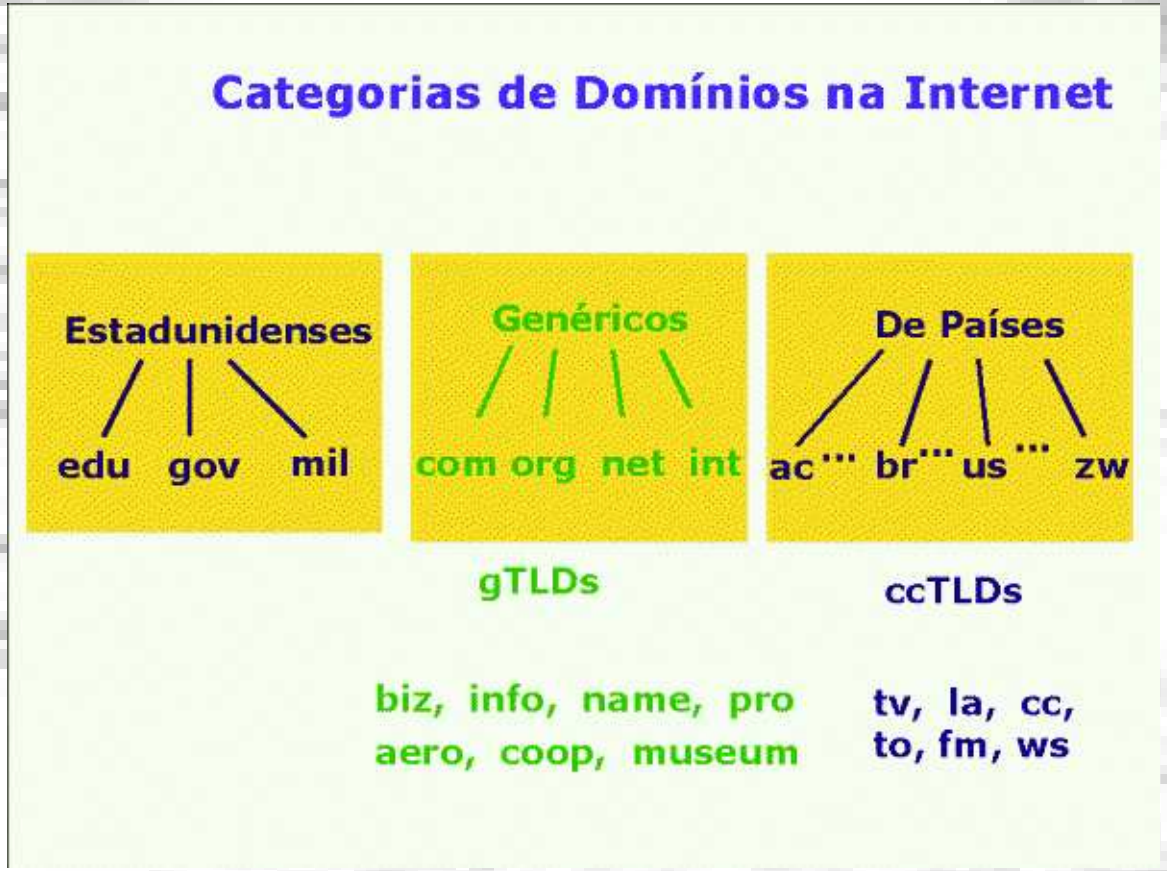
- Sistema hierárquico distribuído.
- Não existe um repositório único de informações.
- Informação distríbuída entre milhares de computadores.
- Estrutura em árvore, semelhante à estrutura de diretórios de sistemas Unix.
- O Controle de nomes é localizado em cada organização, cria-se novos nomes de computadores ou sub-domínios sem ser necessário solicitar isso a ninguém.
- Similar ao sistema de números de telefone : código do país, código da área, código do bairro e código da linha.



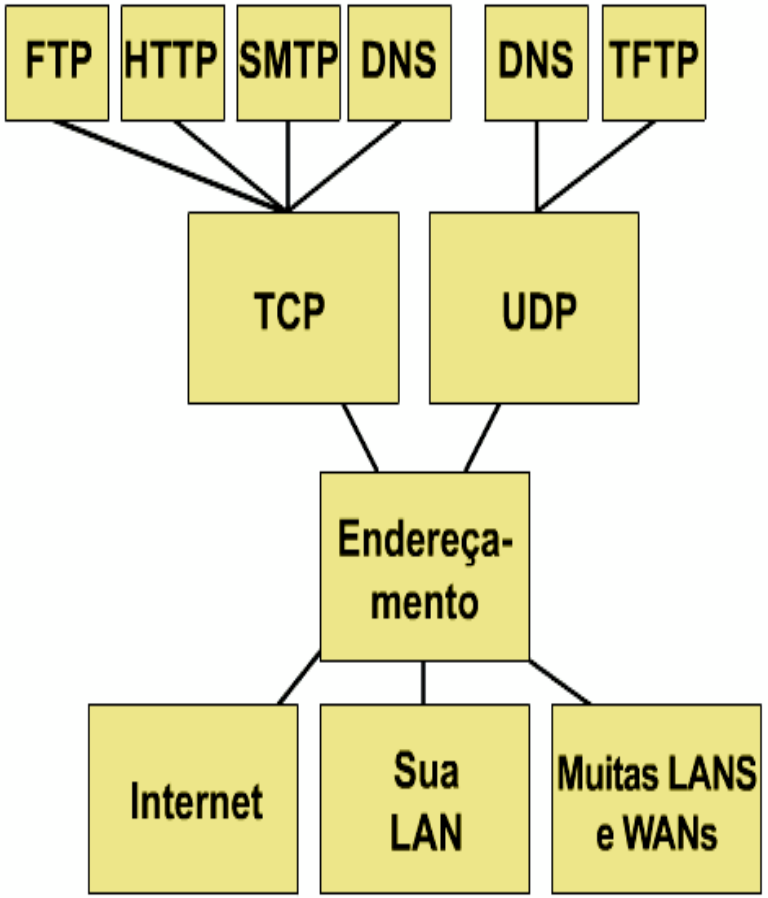
Características (mapamento inverso)



Categorias de Domínios



Protocolo de transporte - TCP/IP



UDP or TCP ?

- TCP quando ocorre transferência do banco de dados para o servidor secundário (replicação).
- UDP para lookups.
- Se a resposta do lookup for maior de 512 bytes o requisitante refaz a requisição usando o TCP.

Formato da mensagem DNS

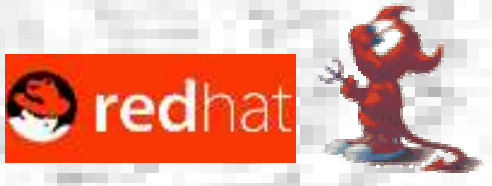
Format of DNS messages

Identical formats are used for queries and responses:

0	16	31
Identification	Parameter	
Number of Questions	Number of Answers	
Number of Authority	Number of Additional Inform.	
Question Section ...		
Answer Section ...		
Authority Section ...		
Additional Information Section ...		

Protocolo DNS

- Header: id, query/response
- Question: nome, classe, tipo do recurso
- Resposta: dados de resposta
- Autoridades: servidores de nomes

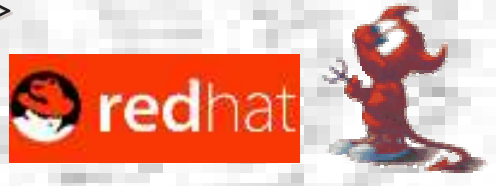


Clientes DNS

Os clientes de DNS fazem uso de uma biblioteca de funções chamada resolver. Esta biblioteca é invocada pelos aplicativos do sistema sempre que se fizer necessário a tradução de um nome simbólico em um endereço lógico (número IP) e endereços em nomes.

Clientes DNS (cont.)

- Configuração default
  - Não é usado o /etc/resolv.conf
  - O servidor é o computador local
  - O domíno local é derivado de hostname ou domainname
- Configuração customizada
  - O arquivo /etc/resolv.conf é usado
  - domain <nomedomínio>
  - nameserver <ip1> <ip2> <ip3>
  - search <sufixo1> <sufixo2> <sufixo3>



Configuração do Cliente DNS Unix / Linux

– Define-se qual a ordem de pesquisa.

Conteúdo do arquivo /etc/host.conf

order hosts,bind

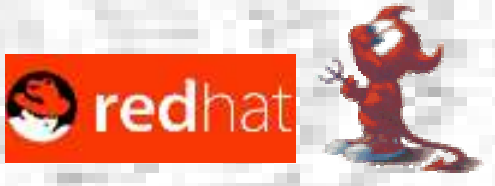
– Define-se qual os nameservers e opcionalmente as diretivas search e domain.

Conteúdo do arquivo /etc/resolv.conf :

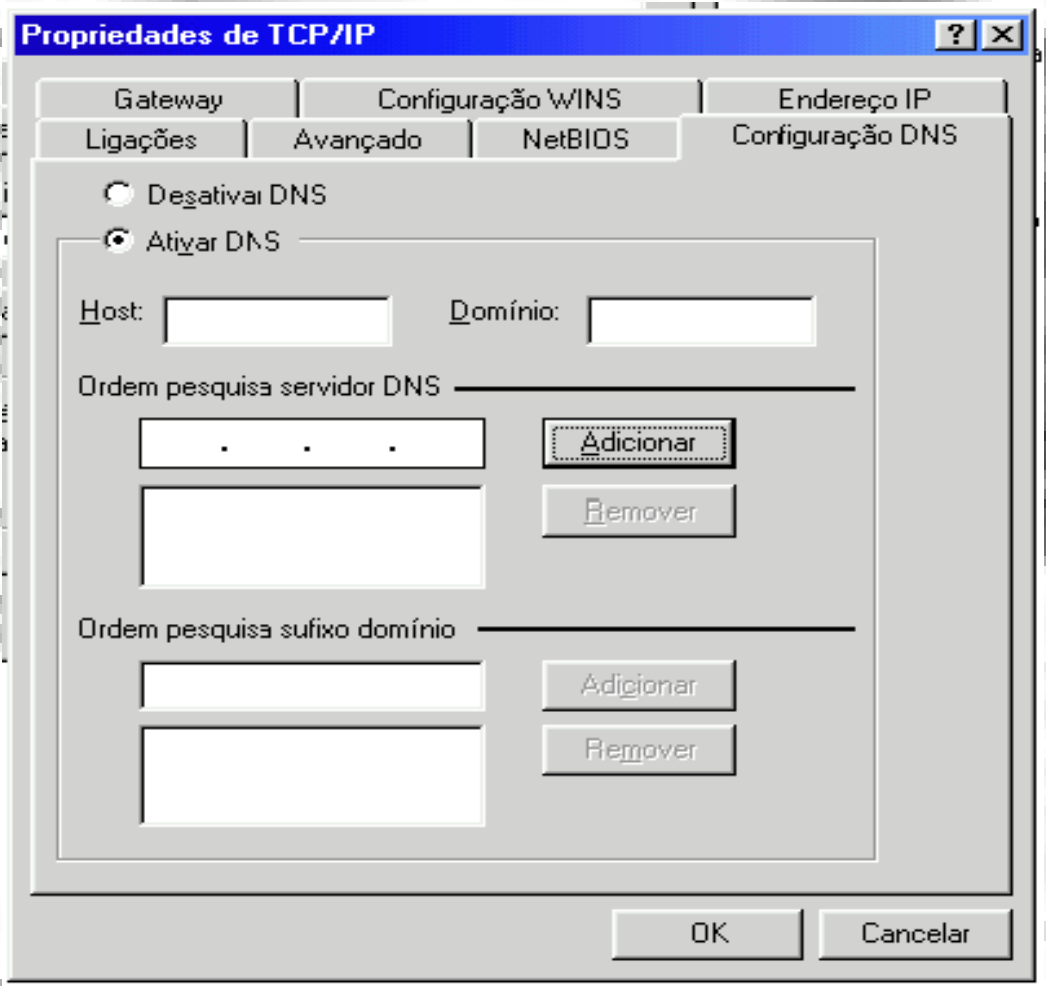
nameserver 200.18.12.30

nameserver 200.18.12.8

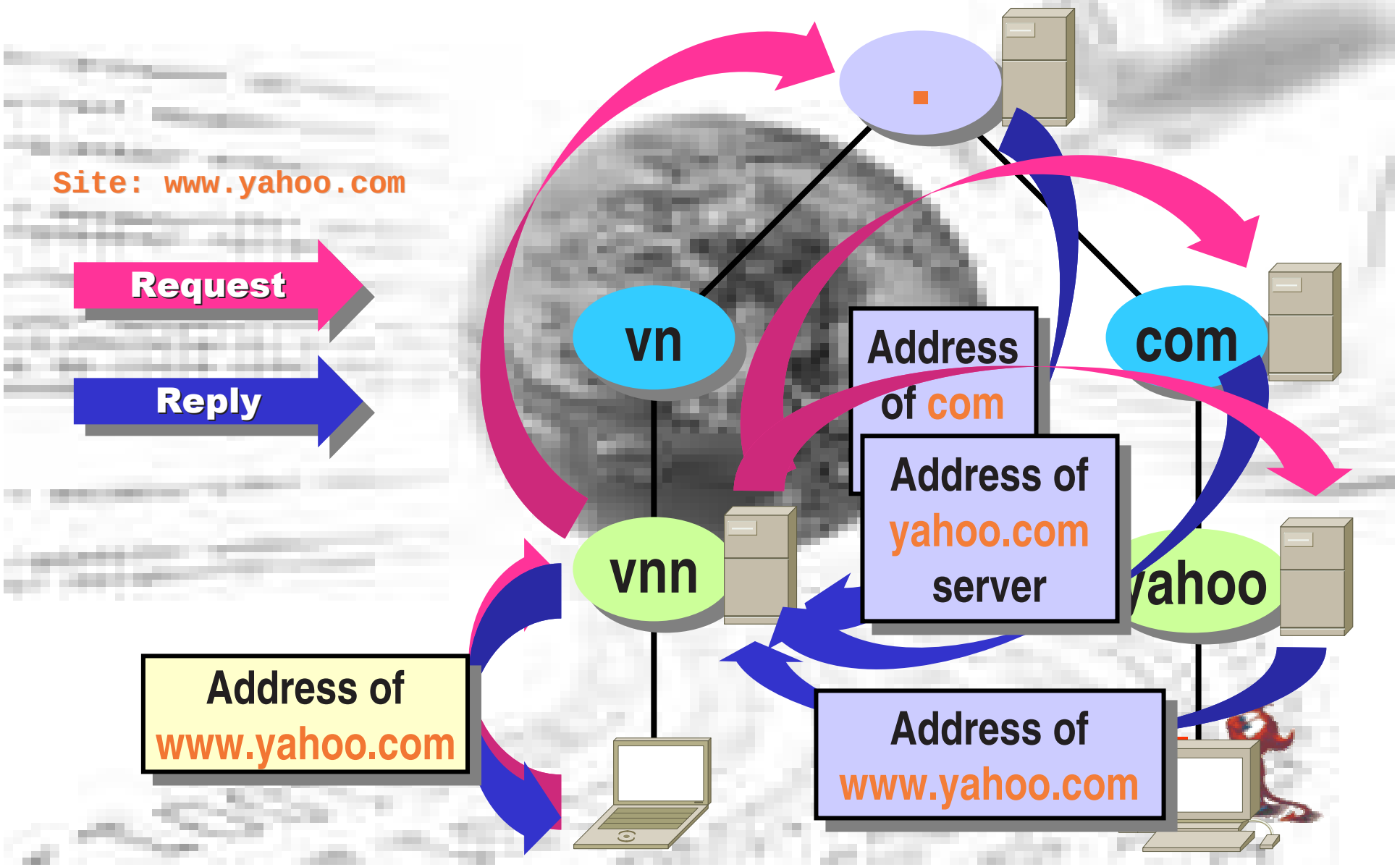
search ara.unisul.br unisul.br



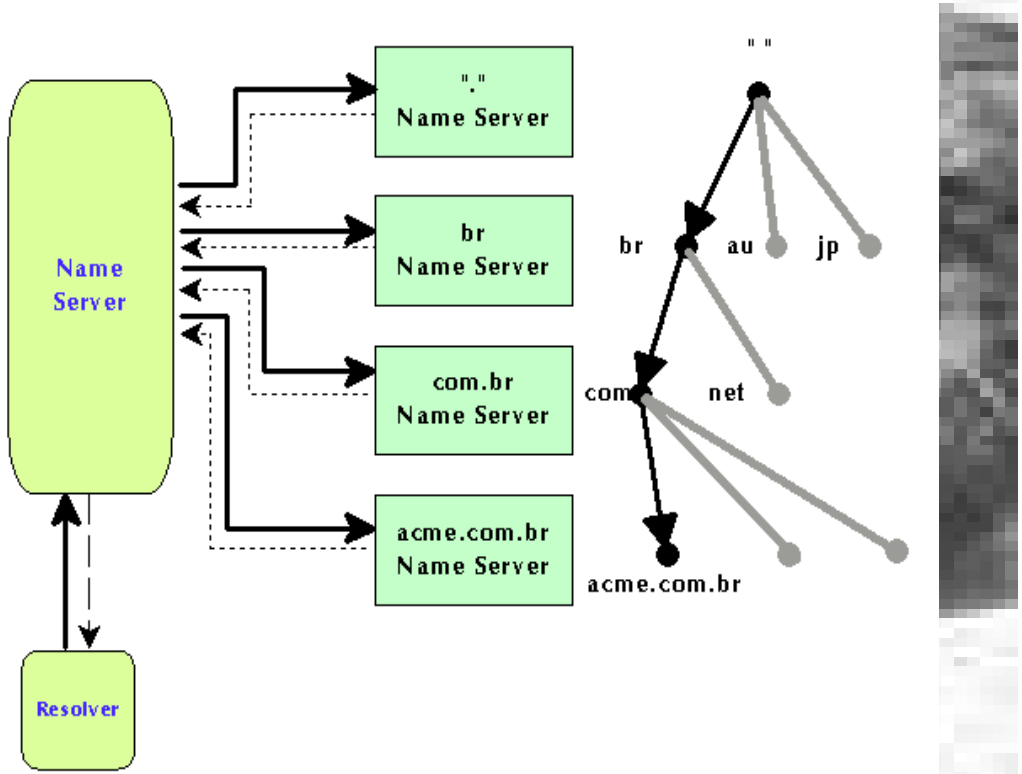
Configuração do Cliente DNS Windows 9x



DNS: Resolve


Site: www.yahoo.com
Request
Reply
.
vn
com
vnn
yahoo
Address of com
Address of yahoo.com server
Address of www.yahoo.com
Address of www.yahoo.com

Exemplo de uma consulta DNS



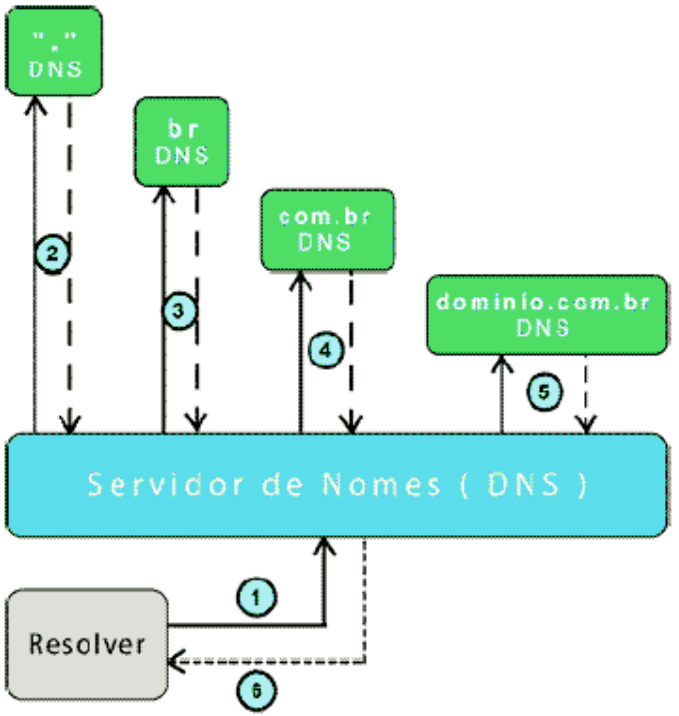


Figura1: Processo de Resolução de Nomes

Processo de Resolução de Nomes

1 - Resolver: O Host consulta o servidor nomes sobre um endereço, no caso: "dominio.com.br".

2 - O DNS recebe a consulta, verifica em seu cache, e se encontrar, responde para o resolver o IP do domínio. Senão, ele segue em frente consultando os servidores de nomes raiz (root name servers). A primeira consulta é o **"."**, que tem como retorno a lista dos servidores raiz, ou seja, os domínios de primeiro nível, como: .br , .com , .net , .org , etc.

3 - Obtida a lista de servidores raiz, ele parte atrás do domínio de primeiro nível responsáveis pelos domínios ".**br**".

4 - Recebendo a resposta do servidor de primeiro nível .br, então o servidor de nomes parte para o próximo domínio ".**com**.br", só que desta vez ele pergunta somente aos DNS que respondem pelos domínios ".br". Neste momento é retornado a lista de servidores responsáveis pelos domínios de segundo nível ".com.br".

5 - A consulta do domínio procurado, "**dominio**.com.br", é enviada apenas para os DNS responsáveis pelos domínios ".com.br", então, ele recebe o IP do servidor responsável pelo domínio. Finalmente é informado ao resolver o IP do domínio consultado, através do servidor nomes. De posse do IP resolver é direcionado ao serviço desejado, seja ele: Web, FTP, e-mail.

Servidores DNS

- Todo servidor de nomes interage com outros servidores na Internet para obter as informações solicitadas por seus clientes.
- Mantém cache das consultas.
- *Podem ser responsável por uma ou mais zonas de um dominio*.
- Podem responder por mais de um domínio.
- Podem ser primários e/ou secundários ao mesmo tempo, desde que sejam domínios diferentes.
- Tem como ponto de partida os servidores root hints (Servidores Raiz) disponíveis na Internet (root name servers).

Servidores DNS (cont.)

- **Primary Server (Authoritatives)**

Servidor com autoridade sobre os dados de um domínio. Informações obtidas de arquivos locais.

Fonte oficial de todas as informações a respeito de um domínio.

- **Secondary Server (Authoritatives)**

Servidor que possui autoridade sobre os dados de um domínio, mas os têm replicados, podendo atender uma requisição de um resolvedor.

Transferem um conjunto completo de informações (Zonas) a partir do servidor primário.

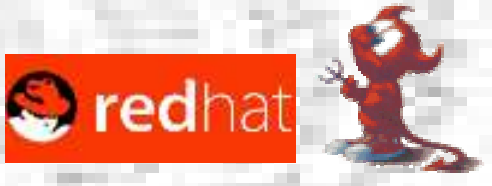
- **Cache Server (Name caching, Non-Authoritatives)**

Somente possui dados derivados das últimas requisições. Mantém nomes recentemente resolvidos. Obtém todas as suas respostas para solicitações do servidor de nome de outros servidores de nome.

Não é fonte oficial de informações a respeito de um domínio.

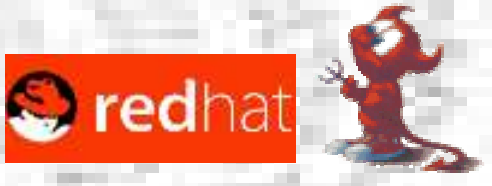
Servidores DNS
Formas de Resolução

- **Resolução interativa** : este tipo de consulta é realizada pelos servidores ***primários*** e ***secundários***, quando recebem uma solicitação que ainda não possui resposta em seu cache. Logo, é necessário procurar em outros que forneçam o caminho até chegar há um servidor que consiga responder a esta requisição.
  - **Consulta distribuída não é automática.**
  - **Devolve endereço de servidores que podem resolver.**
  - **O servidor de nomes retorna ao cliente a melhor resposta que conhece.**
  - **Servidor -> Servidor**



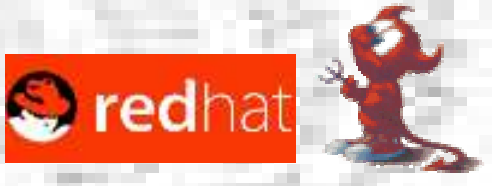
Servidores DNS
Formas de Resolução (cont.)

- **Resolução recursiva** : servidor é configurado para trabalhar como ***caching***. O mesmo não realiza as consultas de nomes diretamente, ele as repassa (forward) para outros servidores DNS, configurados previamente pelo administrador, para que estes, executem o trabalho completo em todo o processo de pesquisa e, após receber o resultado final é entregue ao servidor de cache a resposta desejada.
  - **Consulta distribuída automática.**
  - **Devolve a resolução.**
  - **O servidor de nomes interrogado é então obrigado a obter os dados solicitados.**
  - **Cliente -> Servidor.**
  - **Problema: mascaramento de servidores.**



Servidores DNS
Softwares - Implementação

- Bind (Berkeley Internet Name Domain) /Named (daemon)
  - O BIND é um sistema cliente servidor.
  - O cliente BIND é chamado resolver (formula a consulta e solicita respectivamente a resposta).
  - O servidor DNS chama-se named.
  - É o mais utilizado na Internet.
- Windows Server NT/2K/2003
  - Nativo no Sistema Operacional de Rede.
- Outros menos conhecidos
  - http://djbdns.org/

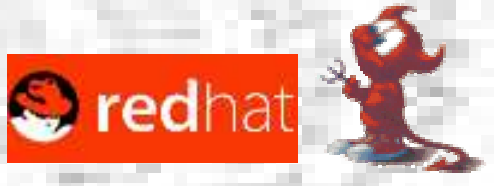


Configuração do Servidor DNS Unix / Linux – Bind/Named

- Site para download:
  ftp://ftp.isc.org/isc/bind9/9.2.3/bind-9.2.3.tar.gz

- Arquivo principal de configuração:

  /etc/named.conf

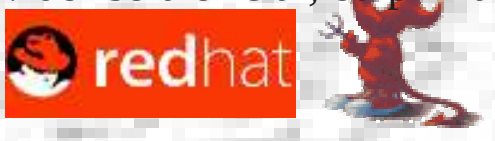


Configuração do Servidor DNS
Opções (/etc/named.conf)

- **directory** - Define o diretório onde os arquivos usados pelo named irão residir.
  - Obs.: O local onde estarão os arquivos deverá estar entre aspas.
- **forwarders** – Define quais servidores deverão ser repassadas todas as consultas.
  - Obs.: Os IP's dos servidores deverão estar entre chaves separados por ponto-e-vírgula e terminados por ponto-e-vírgula após o fecha chaves. Ex: forwarders { 192.168.1.1; 192.168.1.2 };
- **forward only** - Informa ao named que ele deverá, apenas, repassar as consultas.
- **recursion no** - Evita que consultas recursivas sejam realizadas a partir de servidores em modo passivo (Caching-only servers), ou seja, que o servidor responda consultas em nome de outros servidores.
  - Obs.: Dependendo de como estiver configurada a LAN, está opção não poderá ser utilizada. Você pode querer deixar seu servidor primário e secundário atrás do firewall e permitir que o caching externo e por tanto público consulte-os atrás de informações sobre domínios.
- **allow-query** – Define o controle de acesso as consultas do servidor.
  - Obs.: Quem está autorizado a realizar consultas no servidor D.N.S.
- **allow-transfer** - Permite a transferência de zona para o servidor especificado.
  - Obs.: Quem está autorizado a realizar transferência. Normalmente utilizado na transferência de dados do servidor primário para o servidor secudário.
- **check-names** – Determina o que “fazer” ao encontrar hosts inválidos (*fail*) -> cancelar consulta.
  - Obs.: Outras opções: "*warn*" e "*ignore*";

Configuração do Servidor DNS
Opções (/etc/named.conf)

- **notify yes** - Notifica os servidores secundários de todo o update realizado no server primário.
- **also-notify** - Especifica o(s) servidor(es) que deverão ser atualizados toda vez que o servidor primário sofrer atualização.
- **zone** - Define a área de atuação de um servidor.
- **zone "." in** /* informa que a zona de atuação deste servidor são todos os domínios, no caso este seria um servidor raiz, ou seja, "o ponto". Lista de servidores do domínio "." raiz.
- **type** – Especifica o tipo de autoridade do servidor: "***hint***", "***master***" ou "***slave***".
  - **hint** - determina que o named (daemon) leia o named.cache e, localize os servidores raiz, que atuarão sobre toda a net. Também diz que o servidor não terá autoridade sobre domínio algum e que apenas irá armazenar o resultado das consultas.
  - "**master**" e "**slave**" - servem para definir um servidor primário e secundário, respectivamente.
- **file** – Fornece o nome e a localização do arquivo que irá conter as informações a serem utilizadas.
- **0.0.127.in-addr.arpa** - Especifica uma área pré-determinada para a atuação do servidor, e indica através do endereço da sub-rede sobre, a qual, o servidor irá atuar. Neste exemplo, usamos a interface local com o endereçamento reservado para testes. Como trata-se de uma área reservada na Internet como se fosse a sua sub-rede, então, pode-se utilizar a opção "master" para informar ao named que na sub rede 127.0.0 o servidor será oficial, ou primário.



Exemplo - Conteúdo do arquivo /etc/named.conf

```
options {
 directory "/var/named";
 /*
 * If there is a firewall between you and nameservers you
        want
        * to talk to, you might need to uncomment the query-
        source
        * directive below.  Previous versions of BIND always
        asked
        * questions using port 53, but BIND 8.1 uses an
        unprivileged
        * port by default.
        */
        // query-source address * port 53;
};

controls {
        inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};
zone "." IN {
        type hint;
        file "named.ca";
};
```

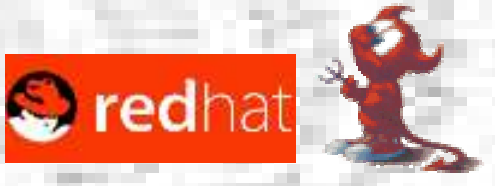
```
zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};
zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};
zone ”redes.com.br" IN {
        type master;
        file ”redes.zone";
};
zone "0.168.192.in-addr.arpa" IN {
        type master;
        file "0.168.192.rev";
}
zone ”adm.redes.com.br" IN {
        type slave;
        file ”adm.zone";
          masters{192.168.1.1;}
};
zone “1.168.192.in-addr.arpa" IN {
        type slave;
        file “1.168.192.rev";
       masters{192.168.1.1;}
}
include "/etc/rndc.key";
```

Resource Record

- Registros dos bancos de dados do DNS.
- Grafia independente da caixa do caractere (maiúsculas ou minúsculas)
- Início na primeira coluna

Resource Record (cont.)

- <nome> <ttl> IN <tipo> <dados>
  - nome: nome do objeto do domínio (*host ou domínio*).
  - ttl: time-to-live. Tempo em segundos que a informação deve permanecer no cache.
  - IN: Internet DNS resource record (*classe internet*).
  - tipo: tipo do registro.
  - dados: informação específica ao tipo do registro.



Tipos de Registros no banco de dados DNS

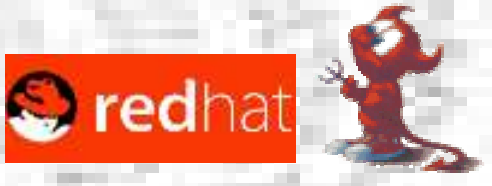
SOA	Indica a autoridade para os dados deste domínio
NS	Lista um servidor de nomes para este domínio
A	Mapeamento de nomes para endereços
PTR	Mapeamento reverso, ou de endereços para nomes
CNAME	Nomes canônicos (para aliases)
TXT	Informações textuais
WKS	Well-Known Services
HINFO	Host Information
MX	Mail Exchanger

O Registro SOA (Start of Autority)

- <zone> <ttl> IN SOA <origin> <contact> (
  serial ; Serial
  refresh ; Refresh
  retry ; Retry
  expire ;Expire
  mininum ;Minimum
)
- Usualmente o primeiro registro de um arquivo de domínio
- Cada domínio tem um SOA

O Registro SOA (Start of Autority)

- **zone**: o nome da zone. O “@” referência o domínio definido em named.conf.
- **origin**: nome do servidor primário para o domínio.
- **contact**: e-mail do adm e/ou gerente do domínio.
- **serial**: número serial (ano, mês, dia, versão).
- **refresh**: indica de quanto em quanto tempo o servidor secundário deve contactar o servidor primário para verificar se houveram mudança nos dados do domínio para o qual é secundário.
- **retry**: indica quanto tempo o servidor secundário deve aguardar para tentar novamente uma conexão com o servidor primário quando houver uma falha na conexão.
- **expire**: tempo máximo em segundos que o servidor secundário poderá ficar com os dados sem um “refresh”. Após este tempo decorrido sem atualização, o servidor secundário deve parar de responder requisições para a zona.
- **minimun**: indica o valor mínimo TTL (*time to live*) em segundos que os registros podem ficar no cache de outro servidor.



O Registro NS (Name Server)

- Define a hierarquia de domínios (um sub-domínio deve se registar no domínio de mais alto nível).
- <domain> [ttl] IN NS <server>

  domain: nome do domínio.

  ttl: time to live (em branco).

  server: nome do servidor que atende a este domínio.

O Registro A (Address)

•Utilizados para converter um nome em endereço ip.

•É necessário sempre que o servidor de nomes encontra-se dentro do domínio sobre o qual é autoridade.

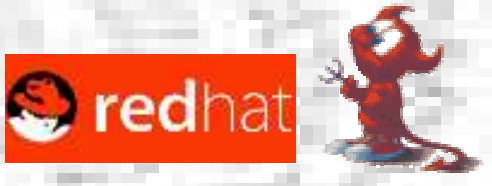
•Pode existir um número de host fora do domínio do SOA, no caso do endereço de um servidor de um sub-domínio.

•<host> [ttl] IN A <addr>

host: nome do host, geralmente é relativo ao domínio corrente.

ttl: time to live (em branco).

addr: endereço IP.



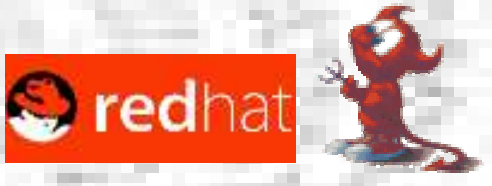
O Registro MX (Mail Exchanger)

- Utilizado para o direcionamento de correio eletrônico.
- <name> [ttl] IN MX <preference> <host>

name: nome da máquina e/ou domínio para que a mensagem eletrônica é direcionada.

preference: número que indica qual servidor tem prioridade no encaminhamento das mensagens.

host: o nome do servidor de mail.



O Registro CNAME (Canonical Name)

- Servem para atribuir diversos nomes diferentes a um mesmo número IP.
- Define um alias para um nome.
- <nickname> [ttl] IN CNAME <host>

  nickname: alias

  host: nome já definido

O Registro PTR

- Utilizado para converter endereço IP para nome (arquivos com nomes reverso)
- <name> [ttl] IN PTR <host>

name: número dentro do domínio in-addr.arpa

usualmente último octeto (endereço ip)

host: nome da máquina

O Registro WKS (well-known services)

- Identifica os serviços de rede suportado pelo host.
- <host> [ttl] IN WKS <addr> <proto> <serv>

  host: nome do host

  addr: endereço IP

  proto: tipo de protocolo de transporte

  serv: lista de serviços
- Exemplo
  - teste IN WKS 143.54.2.10 UDP snmp
    IN WKS 143.54.2.10 TCP smtp
    IN WKS 143.54.2.10 TCP ftp

O Registro HINFO (Host Information)

- Fornece um descrição do hardware e/ou software do host
- <host> [ttl] IN HINFO <hard> <soft>

  host: nome do host

  hard: identifica o hardware

  soft: identifica o sistema operacional
- Exemplo
  - pc1.ufrgs.br IN HINFO IBM-PC/AT DOS

Arquivo de zona : /var/named/redes.zone

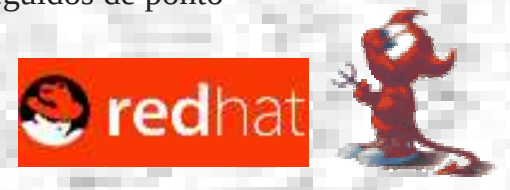
```
; zone file
@ IN  SOA redes.com.br.  root.redes.com.br. (
                        2004092301  ; Serial
                        14400       ; Refresh after 3 hours
                        3600        ; Retry after 1 hour
                        604800      ; Expire after 1 week
                        86400 )     ; Minimum TTL of 1 day

                        NS      dns.embratel.net.br.
                        NS      firewall.redes.com.br.

                        MX 10   redes.com.br.
                        MX 20   firewall


firewall                IN  A    192.168.0.1
smtp                    IN A     192.168.0.1
pop                     IN A     192.168.0.1
server                  IN A     192.168.0.1
redes.com.br.           IN A     192.168.0.1
```

O primeiro registro define o registro SOA (Start Of Authority) que delimita o início de uma zona de autoridade. Cada zona tem um só registro SOA.O caracter @ no início da linha é um sinônimo para o nome do domínio especificado na diretriz "zone" do arquivo named.conf e, assim, neste caso equivale a ”redes.com.br".
O subseqüente "IN" indica estar na Internet e define o tipo de rede.
Depois da SOA vêm, na ordem, o name server e o endereço de e-mail do responsável pela zona (no endereço de e-mail o caracter @, que para o DNS tem um significado particular, deve ser substituído por um ponto).
O registro SOA continua, delimitado por parênteses, na próxima linha aparece o número de série do arquivo. O número pode ser escolhido à vontade, com a condição de que seja atualizado cada vez que se modifica o arquivo de zona.
Posteriormente contêm os tempos em segundos que se referem à interação entre o master os seus slaves.

A linha seguinte é um registro do tipo NS que indica qual é o name server autorizado para a zona. Pode haver mais de uma linha do tipo NS. Note-se que o nome termina com um ponto.

A próxima linha, contém um registro do tipo MX, que contribui para acelerar a transferência da correspondência indicando qual é (ou quais são) os servidores de correio da zona.
Note-se que como depois do nome do host não aparece o ponto, ao próprio nome será articulado o domínio.

Finalmente chegamos aos registros que são usados para transformar os nomes dos hosts em endereços IP (mas não vice-versa: essa é a tarefa do arquivo para a zona 1.168.192). Os registros de tipo A associam os endereços aos nomes dos hosts da nossa rede. Se estivessem presentes outros hosts seriam adicionados outros registros A. Note-se que os nomes dos hosts não são seguidos de ponto



Arquivo de Zona Reversa: /var/named/0.168.192.rev

```
;
; reverse address file
;
@           IN      SOA     redes.com.br. root.redes.com.br. (
                            2004092301  ; Serial
                            14400       ; Refresh
                            3600        ; Retry
                            604800      ; Expire
                            86400       ; Minimum
                            )

                    IN      NS      redes.com.br.

254         in      PTR     firewall.redes.com.br.
1           in      PTR     server.redes.com.br.
2           in      PTR     webserver.redes.com.br.
```

Exemplo - Conteúdo do arquivo /etc/named.conf (mais opções)

```
options {
        directory "/var/named";
        listen-on port 53{
        127.0.0.1; 200.205.206.77;
        };
        allow-transfer  {
        200.205.206.78;
        };

};
    .
    .
    .
    .
zone "64-127.206.205.200.IN-ADDR.ARPA"{
        notify yes;
        type master;
        file "206.205.200";
        allow-transfer  {
        200.205.206.78;
        };
};
/************END named.conf**************************/
```

```
;FILE: /var/named/206.205.200

$ORIGIN 64-127.206.205.200.in-addr.arpa.
64-127.229.199.200.in-addr.arpa.      IN     SOA
machine.mydomain.br.    webmaster.mydomain.br   (
                        2000062803 ; serial
                        3H ; refresh
                        1H ; retry
                        1W ; expire
                        1D ; default_ttl
                        )
64-127.206.205.200.in-addr.arpa.        IN  NS     mydomain.br.
64-127.206.205.200.in-addr.addr.arpa.   IN  NS  secundary.domain.br.
70.64-127.206.205.200.in-addr.arpa.     IN  PTR  www.mydomain.br.
72.64-127.206.205.200.in-addr.arpa.     IN  PTR  proxy.mydomain.br.
75.64-127.206.205.200.in-addr.arpa.     IN  PTR  mail.mydomain.br.
@                                       IN  PTR  mydomain.br.

/****************END 206.205.200**********************/
```

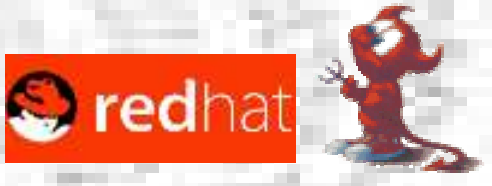
Exemplo - Conteúdo do arquivo /etc/named.conf (caching-only com ACLS)

- O exemplo seguinte é apropriado para um servidor caching-only, usado somente pela rede interna.
- Toda requisição externa é recusada..

```
// Duas redes Internas que poderão fazer consultas ao Servidor de DNS.
acl ”redes-internas" { 192.168.4.0/24; 192.168.7.0/24; };
options {
directory "/etc/namedb";                    // Diretorio de trabalho
pid-file "named.pid";                       // Arquivo que vai armazenar o PID do processo
allow-query { ”redes-internas"; };
};
// Root server hints
zone "." { type hint; file "root.hint"; };// Arquivo que contem os root servers
// Provide a reverse mapping for the loopback address 127.0.0.1
zone "0.0.127.in-addr.arpa" {
type master;                            // Tipo Master
file "localhost.rev";                   // Arquivo que contem o mapa dos hosts - Reverso
notify no;                              // Não notifica o Servidor de Dns Secundário
};
```

Exemplo de configuração (/etc/named.conf) para um servidor Master do domínio “example.com “e slave para o domínio “eng.example.com”

```
options {
directory "/etc/namedb";            // Diretório de Trabalho
pid-file "named.pid";                 // Onde vai ficar o arquivo com  o PID do processo
allow-query { any; };                 // Este é o default
recursion no;                              // Não prove serviço recursivo
};

// Root server hints
zone "." { type hint; file "root.hint"; };
// Provide a reverse mapping for the loopback address 127.0.0.1
zone "0.0.127.in-addr.arpa" {
type master;
file "localhost.rev";
notify no;
};

// Master para o domínio  example.com
zone "example.com" {
type master;
file "example.com.db";
// IP addresses dos servidores slaves que podem transferir zonas do example.com
allow-transfer {
192.168.4.14;
192.168.5.53;
};
};

// Definição do Servidor slave para o domínio eng.example.com
zone "eng.example.com" {
type slave;
file "eng.example.com.bk";
// IP address of eng.example.com master server
masters { 192.168.4.12; };
};
```



Configuração de Sub-Domínios

- Necessário quando se delega autoridade para um servidor de nomes que reside dentro do domínio delegado.
- Delegação de Sub-domínios.
- Registro a ser incluído.

```
subdominio.dominio.com.br.        IN    NS    ns.subdominio.dominio.com.br.
ns.subdominio.dominio.com.br.     IN    A     141.211.164.3
```

Root Servers - Coração da Internet

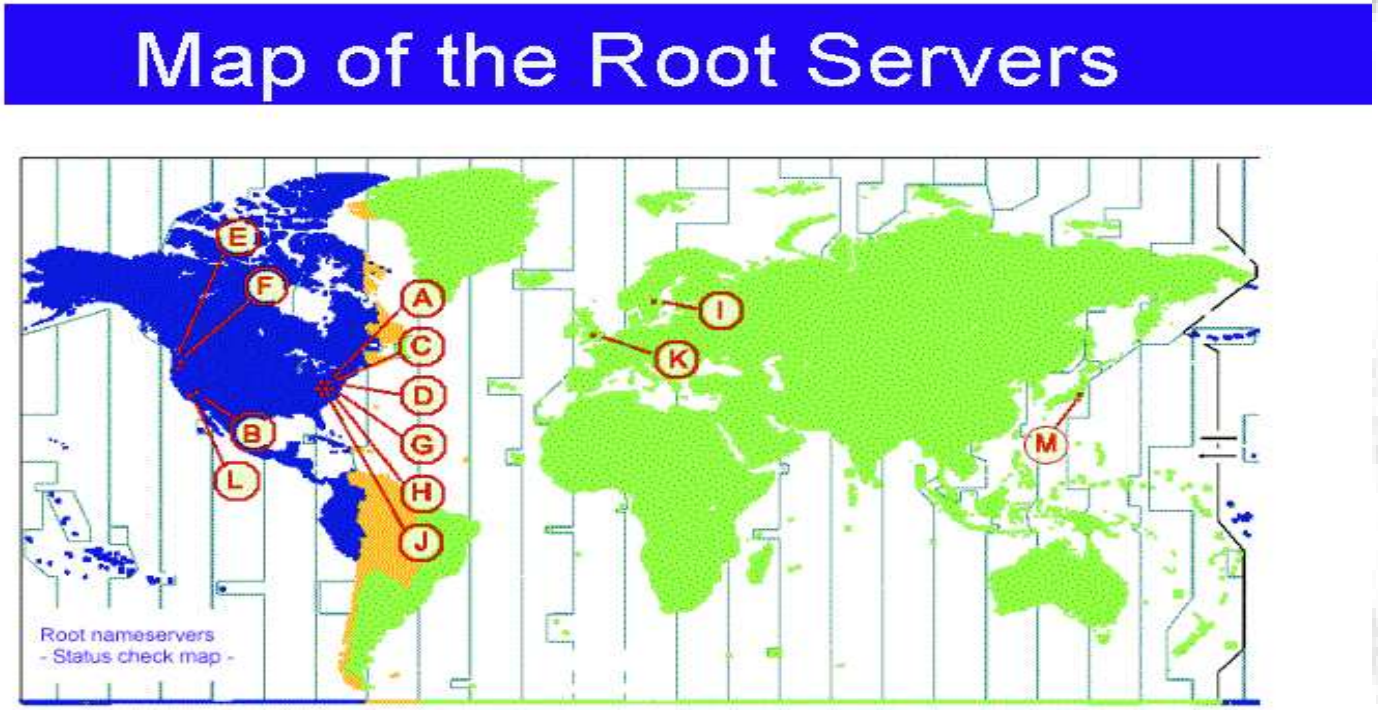
- Informações sobre servidores raiz (root name servers).
- Dado essencial ao funcionamento correto do DNS.
- Requer verificação e se necessário atualização.
- Arquivo atualizado em: ftp://ftp.rs.internic.net/domain/named.root

Arquivo: /var/named/named.ca

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC registration services
;       under anonymous FTP as
;           file                /domain/named.root
;           on server           FTP.RS.INTERNIC.NET
;       -OR- under Gopher at    RS.INTERNIC.NET
;           under menu          InterNIC Registration Services (NSI)
;              submenu          InterNIC Registration Archives
;           file                named.root
;
;       last update:    Aug 22, 1997
;       related version of root zone:   1997082200
;
; formerly NS.INTERNIC.NET
;
.                        3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.      3600000      A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                        3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.      3600000      A     128.9.0.107
;
; formerly C.PSI.NET
;
.                        3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.      3600000      A     192.33.4.12
;
; formerly TERP.UMD.EDU
```

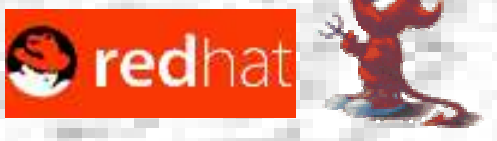
```
.                        3600000      NS    D.ROOT-
SERVERS.NET.
D.ROOT-SERVERS.NET.      3600000      A     128.8.10.90
;
; formerly NS.NASA.GOV
;
.                        3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.      3600000      A     192.203.230.10
;
; formerly NS.ISC.ORG
;
.                        3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.      3600000      A     192.5.5.241
;
; formerly NS.NIC.DDN.MIL
;
.                        3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.      3600000      A     192.112.36.4
;
; formerly AOS.ARL.ARMY.MIL
;
.                        3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.      3600000      A     128.63.2.53
;
; formerly NIC.NORDU.NET
;
.                        3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.      3600000      A     192.36.148.17
;
; temporarily housed at NSI (InterNIC)
;
.                        3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.      3600000      A     198.41.0.10
;
; housed in LINX, operated by RIPE NCC
;
.                        3600000      NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.      3600000      A     193.0.14.129
;
; temporarily housed at ISI (IANA)
;
.                        3600000      NS    L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.      3600000      A     198.32.64.12
;
; housed in Japan, operated by WIDE
;
.                        3600000      NS    M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.      3600000      A     202.12.27.33
; End of File
```

Localização dos Root Servers no Mundo



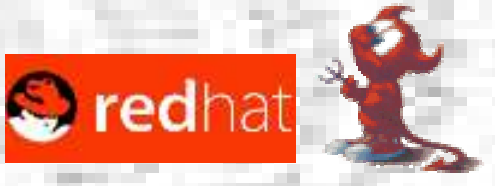
Ferramentas de Análise

- nslookup
- dig
- host
- whois
- Arquivo de log
  - Quando o named é inicializado, toda mensagem gerada pelo daemon é logada no arquivo syslog do sistema, normalmente /var/log/messages



nslookup

- Ferramenta utilizada para interrogar servidores de nomes.
- Distribuída juntamente com o software BIND.
- Permite a qualquer usuário consultar um servidor de nomes e recuperar qualquer informação conhecida por este servidor.
- Extremamente útil para identificar problemas com servidores de nomes.
- Consulta a servidores remotos.
- Pode ser usado diretamente na linha de comando (nslookup acme.com) ou através do modo interativo (***nslookup***).



nslookup (modo interativo)

- Comandos úteis:
  - server *name_server* ou *ip* : muda o servidor DNS a ser questionado.
  - set type = *type* : muda o tipo (A, PTR, MX, NS, Any, etc).
  - set domain = *domain* : muda o nome do domínio pesquisado.
  - ls *domain* : recupera o arquivo de zonas do domínio.
  - exit : sai do modo interativo.
- Outras opções:
  - set all
  - set query=mx,soa,any
    - *domain*

Exemplo – Comando nslookup

% nslookup

>server 200.18.12.8

>set query=soa

>unisul.br

> set query=mx

>unisul.br

>set query=any

>unisul.br

DIG (Domain Information Groper)

- **Comando para consultas no servidor DNS.**
- **“.. substitui o comando nslookup..”**

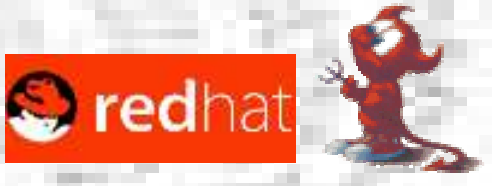
- **Sintaxe do comando em Distribuições Linux :**

- **dig** [*@server*] *domain*
  [*query-type*] [*query-class*] [*+query-option*] [*-dig-option*] [*%comment*]

- **dig @server domain query-type query-class**

query-type is the type of information (DNS query type) that you are requesting. If omitted, the default is ``a'' (T_A = address). The following types are recognized:

a	T_A	network address
any	T_ANY	all/any information about specified domain
mx	T_MX	mail exchanger for the domain
ns	T_NS	name servers
soa	T_SOA	zone of authority record
hinfo	T_HINFO	host information
axfr	T_AXFR	zone transfer (must ask an authoritative server)
txt	T_TXT	arbitrary number of strings



Exemplo – Comando DIG

dig unisul.br
dig unisul.br soa
dig @200.18.12.8 unisul.br soa
dig unisul.br mx
dig @200.18.12.8 unisul.br mx

host

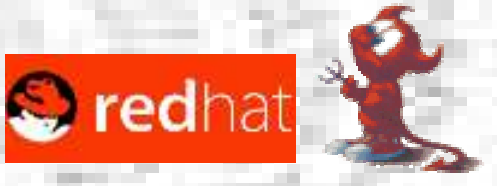
- Comando simples para consultas ao servidor de DNS, sobre nomes dos hosts e endereços IP´s.

- Sintaxe do comando em Distribuições Linux :

- **host** [-aCdlrTwv] [-c *class*] [-N *ndots*] [-t *type*] [-W *timeout*] [-R *retries*] *hostname* [*server*]

Exemplo – Comando host

host unisul.br
host 200.18.12.8
host -t ns unisul.br
host -t SOA unisul.br
host -t MX unisul.br



whois

•Utilizado para descobrir a quem pertence determinado endereço IP, ou a quem pertence determinado domínio/host.

• Consulta um servidor whois, que deve ser especificado no comando ou a consulta por padrão será feita no servidor whois.crsnic.net

• Pode-se fazer consultas diretamente no site da FAPESP registro.br, na opção pesquisas.

•Sintaxe do comando em Distribuições Linux :

Usage: whois [OPTION...] query[@server[:port]]

valid options:

-h server server name

-p port server port

-t timeout query time limit

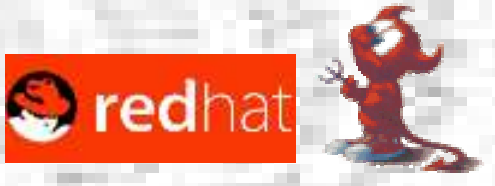
-r force recursion

-n disable recursion

-v verbose mode

-- treat remaining arguments as part of the query

default server is whois.crsnic.net



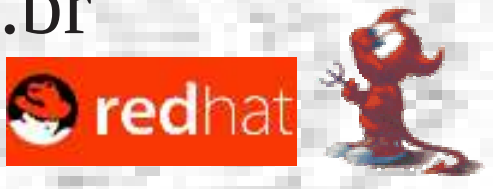
Exemplo – Comando whois

- **Whois de um endereço IP**

whois 200.176.3.142@registro.br

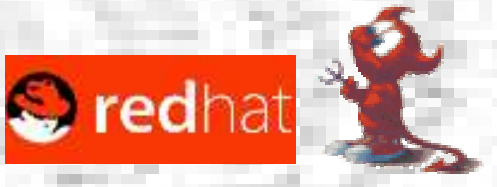
- **Whois de um domínio**

whois terra.com.br@registro.br

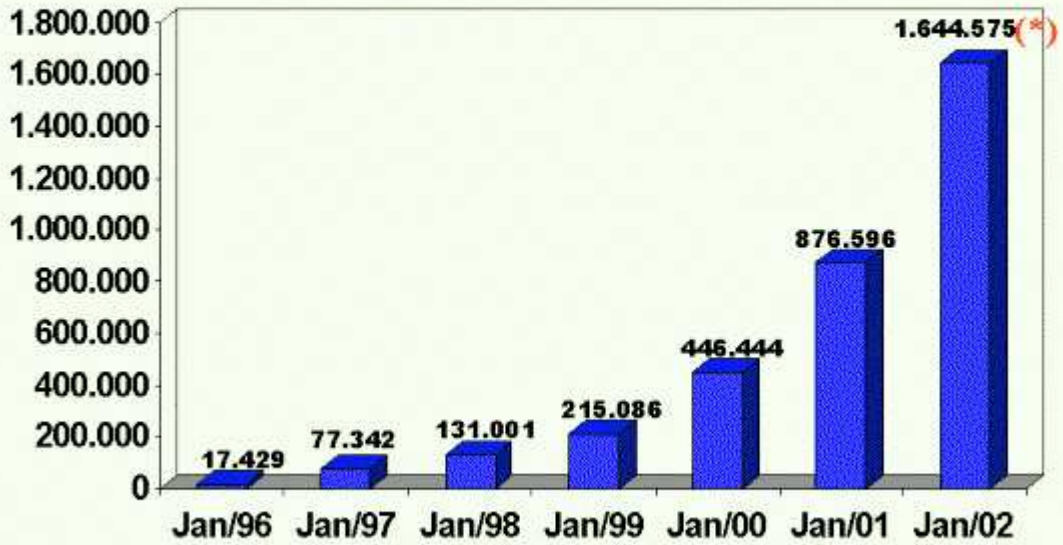


Problemas mais comuns

- A maior parte dos problemas relativos ao DNS geralmente se enquadram em categorias bastante comuns e podem ser resolvidos de modo razoavelmente simples. São eles (não agrupados em ordem de importância ou de ocorrência):
  - Não alterar o número de série dos mapas.
  - Processo named não está no ar.
  - Não sinalizar ao named que algum mapa foi mudado.
  - Servidores secundários não conseguem carregar os dados da zona.
  - Criar a entrada de uma máquina no mapa direto e não fazer o mesmo para o mapa reverso.
  - Erro de sintaxe no arquivo /etc/named.conf ou nos mapas do DNS.
  - Não colocação do "." no final de um nome.
  - Informações ausentes no mapa do cache (named.ca).
  - Falta de conectividade à rede.
  - Delegação incorreta para subdomínios.
  - Delegação de autoridade não efetivada.
  - Erro de sintaxe no arquivo /etc/resolv.conf.
  - Nome do domínio default não definido.

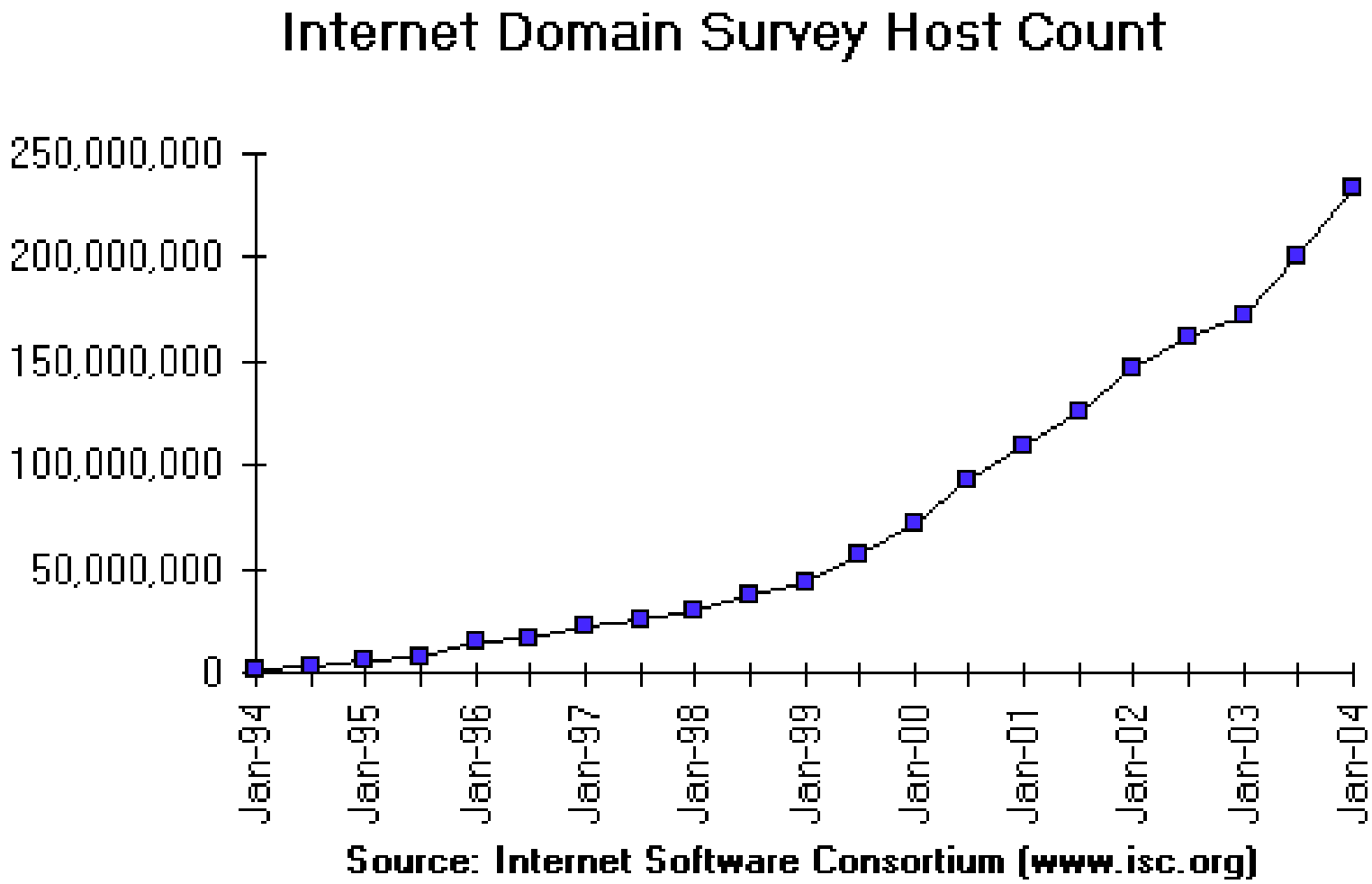


Número de *Hosts* Internet no Brasil



Fonte: http://www.isc.org

(*) 1.988.321 em julho/02


Internet Domain Survey Host Count
250,000,000
200,000,000
150,000,000
100,000,000
50,000,000
0
Jan-94
Jan-95
Jan-96
Jan-97
Jan-98
Jan-99
Jan-00
Jan-01
Jan-02
Jan-03
Jan-04
Source: Internet Software Consortium (www.isc.org)


redhat

Número de *Hosts* em Cada *Domínio*
Classificação Mundial (Jul/2002)

0. gTLDs.....101.723.255	11. Taiwan..... 1.814.090
1. EUA 11.874.880	12. Espanha.... 1.682.434
2. Japão 8.713.920	13. Suécia 1.187.942
3. Canadá 3.129.884	14. México 1.004.637
4. Itália 2.958.899	15. Finlândia... 986.285
5. Alemanha.....2.923.327	16. Dinamarca... 872.328
6. Reino Unido.. 2.508.151	17. Bélgica..... 832.853
7. Austrália 2.496.683	18. Polônia 731.371
8. Holanda 2.150.379	19. Áustria 720.587
9. França 2.052.770	20. Suiça 667.509
10. Brasil 1.988.321	

Fonte: http://www.isc.org


Fim
redhat