DNS - Um serviço Indispensável

Artur V. Gomes Neto[1]**,Andre Moraes**[1]

[1]Curso Superior de Tecnologia em Redes de Computadores
FACULDADE DE TECNOLOGIA SENAC PELOTAS (FATEC PELOTAS)
Rua Gonçalves Chaves, 602 – 96.015-000 – Pelotas – RS – Brasil

rutrars@gmail.com, chameoandre@gmail.com

Abstract. *This article describes the Domain Name System-DNS, where its main purpose is to associate host names to IP addresses. This need arises from the principle that users often use names to identify machines on the world wide web.*

Resumo. *Este artigo descreve o Domain Name System-DNS, onde seu propósito principal é associar nomes de hosts a endereços IP . Essa necessidade surge do principio que usuários normalmente utilizam nomes para identificar máquinas na rede mundial de computadores.*

1. Introdução

Você já parou para pensar o que acontece quando digitamos uma URL em nosso navegador favorito? Ponderamos, quanto digitamos uma url no navegador o primeiro passo antes do conteúdo ser exibido é converter o nome (url) em IP, este processo é realizado pelo Servidor DNS, Sistema de Nomes e Domínios (Domain Name System), o endereço do servidor DNS é previamente configurado na máquina, seja por DHCP ou fixado manualmente, o servidor DNS é responsável por devolver ao navegador o IP do site solicitado, somente depois que a consulta é realizada que o navegador realizará a solicitação ao servidor web que responde pela url solicitada, após o conteúdo do site é exibido em sua seu navegador. O DNS foi criado com o objetivo de tornar as coisas mais fáceis para o usuário, permitindo assim, a identificação de computadores na Internet ou redes locais através de nomes (é como se tivéssemos apenas que decorar o nome da pessoa ao invés de um número de telefone). A parte responsável por traduzir os nomes como www.nome.com.br em um endereço IP é chamada de resolvedor de nomes.

2. Estrutura do sistema de DNS

No inicio da Internet, quando era chamada de Arpanet, a conversão entre o nome da máquina e o seu IP era realizada utilizando o arquivo denominado de hosts.txt [RNP 2011]. Os administradores enviavam via e-mail as alterações dos seus domínios e buscavam via FTP tal arquivo para atualizar os hosts na rede que por ele era administrada.

Com o crescimento da Internet tal mecanismo tornou-se completamente inviável, surgindo o DNS, um sistema descentralizado, fornecendo as características necessárias em relação aos problemas de carga gerada no tráfego na rede, de colisão de nomes e de consistência dos dados.

Devido ao intenso tráfego da internet e devido à segurança da rede, a estrutura do banco de dados DNS é distribuída e hierárquica. Ou seja, ao invés de um banco de dados

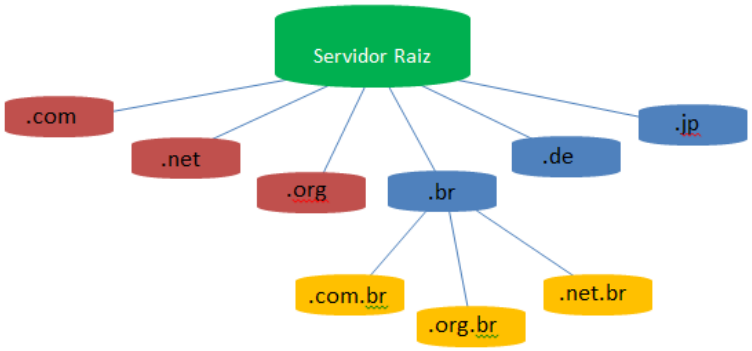

Figura 1. Exemplo de Herárquia distribuida dos servidores DNS

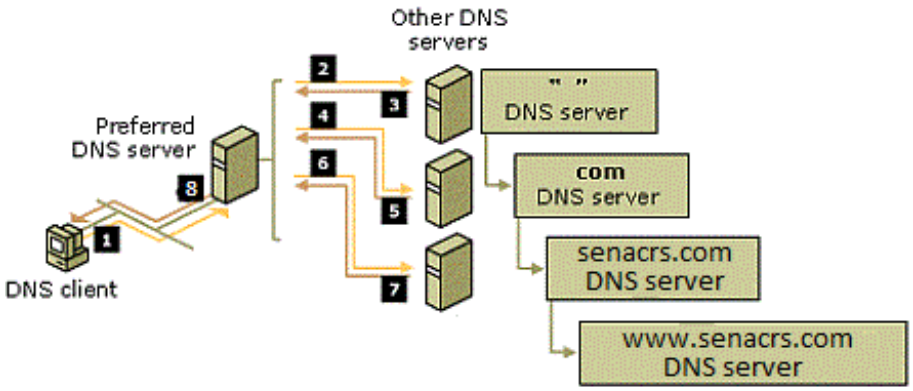

Figura 2. Exemplo de resolução de nomes

central e único com informações de todos os domínios, a resolução ocorre consultando-se diversos servidores DNS e sua resolução é hierárquica (um servidor DNS pode apontar para outro servidor DNS e assim sucessivamente). A estrutura hierárquica equivale a uma árvore invertida, conforme ilustra a Figura 1, ou seja, existe um servidor principal que aponta para um secundário que aponta para um terceiro e assim sucessivamente. O servidor DNS que está no topo da internet é o servidor raiz. Uma lista completa dos servidores raízes pode ser encontrada [Root-Servers 2011].

2.1. Como Funciona uma resolução de Nomes

A figura 2 demostra a resolução de nomes para o endereço www.senacrs.com:

O servidor de nomes do cliente verifica que www.senacrs.com não faz parte do seu domínio e interroga o servidor de nomes da raiz (2). Este desconhece o endereço IP de www.senacrs.com, mas tem uma referência para o servidor de nomes do subdomínio com, que devolve ao servidor de nomes (3). Este pode então, interrogar o servidor de nomes de ?com? sobre o endereço IP de www.senacrs.com (4) e obter assim, uma referência para o servidor de nomes de senars.com que devolve ao servidor de nomes local (5). Este interroga, finalmente o servidor de senacrs.com (6) que pode resolver o endereço pretendido (7). Termina assim o processo de resolução e o servidor de nomes local devolve ao cliente o endereço IP correspondente ao nome solicitado.

3. Bind

BIND (Berkeley Internet Name Domain) é o servidor para o protocolo DNS mais utilizado na Internet, especialmente em sistemas do tipo Like-Unix, onde ele pode ser considerado um padrão. Foi criado por quatro estudantes de graduação, membros de um grupo de pesquisas em ciência da computação da Universidade de Berkeley, e foi distribuído pela primeira vez com o sistema operacional 4.3BSD. O programador Paul Vixie, enquanto trabalhava para a empresa DEC, foi o primeiro mantenedor do BIND. Atualmente o BIND é suportado e mantido pelo Internet Systems Consortium [ISC 2011]. Para a versão 9, o BIND foi praticamente reescrito. Ele passou a suportar, dentre outras funcionalidades, a extensão DNSSEC e o protocolo IPv6. [Registrobr 2011] Assim como os programas Sendmail e WU-FTPD, e outros sistemas que remontam aos primeiros dias da Internet, as versões 4 e 8 do BIND tinham uma série de vulnerabilidades, por isso, o seu uso é hoje fortemente desencorajado. Uma das motivações para reescrever o BIND, e lançar o BIND 9, foi disponibilizar um sistema mais seguro e competitivo com as ofertas de servidores DNS da Microsoft. [POP-BA 2011]

3.1. Tipos de Servidores

Servidor Autoritativo: É responsável por manter os mapas referentes a uma zona local e responder a requisições vindas de máquinas de todo o mundo, que precisarem resolver nomes de domínio da zona sobre a qual este servidor tem autoridade.

Servidor Recursivo: É responsável por receber as consultas DNS dos clientes locais e consultar os servidores externos, de modo a obter respostas às consultas efetuadas, após realizar a consulta externa o mesmo armazena o resultado em cache para uma futura utilização.

3.2. Instalação do Bind

O Bind é hoje em dia o servidor de nomes mais utilizado na internet, sua distribuição é livre e existem portes para a maioria dos sistemas operacionais modernos. Para obter uma copia do servidor Bind acesse http://www.isc.org/ [ISC 2011]. Para fins deste artigo foi utilizado o versão 9.7.3-P1 para os dois sistemas abordados.

3.2.1. Microsoft Windows 2008

A instalação inicia com o download do bind9 para windows da página oficial do projeto. Após realizar o download, descompacte o arquivo, entre no diretório criado e execute o arquivo BINDInstall, a seguinte tela aparecerá, como demonstra a Figura 3.

Na tela que surge devemos configurar algunas opções:
Targer Director: `c:\bind` – Define o local de instalação do bind
Service Accont name: named – Define o nome do usuário utilizado pelo bind
Service Account Password: Senha para usuário criado

Na guia option deixe marcada a opção Automatic Startup, para o serviço do bind ser inicializado junto com o boot do sistema. Para facilitar a documentação assumiremos que o bind foi instalado no diretório `c:\bind`.

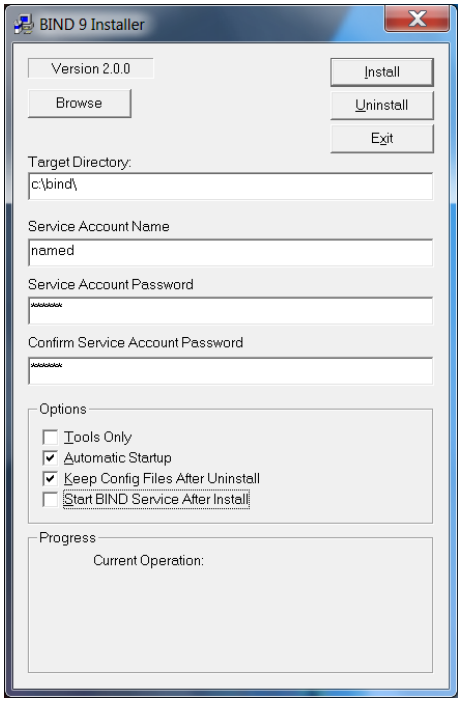

Figura 3. Tela de Instalação do Bind

Diferente de seu irmão o bind para windows não esta previamente configurado com um servidor DNS recursivo ou cache como é chamando pelos profissionais da área. Para iniciar a configuração, acesse o diretório que foi instalado o bind e execute os comando conforme Figura 4.

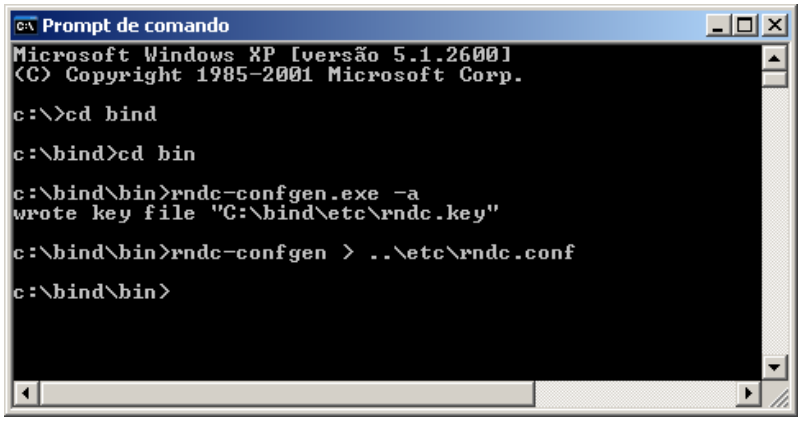

Figura 4. Exemplo de configuração dos bind para windows

Com estes comando iniciamos a configuração do bind criando a chave key caso seja implementado o paramento de atualização dinâmica para o servidor DDNS.

Acesse o diretório `c:\bind\etc` e edite o arquivo rndc.conf, salve-o no mesmo diretório com o nome de named.conf, o arquivo named.conf é responsável por armazenar as configurações do nosso servidor de DNS. Após editar o arquivo e deixe-o como a Código 1 que já descreve o significado das opções.

```
// Opções globais do servidor
```

```
options {
// Especifica a pasta base dos arquivos
directory "C:\bind\etc";
// Especifica o arquivo de processo
pid-file "C:\bind\var\named.pid";
// Não escutar em nenhuma interface ipv6
//listen-on-v6 { none; };
// Escutar no seguinte endereço
listen-on { any; }; // Clientes autorizados a realizar consultas
allow-query { 127.0.0.1; 192.168.200.0/24; 10.1.1.0/8; };
// Realiza pesquisas recursivas
recursion yes;
// Servidores de forward
// forwarders { 8.8.4.4; 8.8.8.8;};};
key "rndc-key" {
algorithm hmac-md5;
  secret "Hve9TJIiPW2m/keWbmJcng==";};
controls {
inet 127.0.0.1 port 953
allow { 127.0.0.1; } keys { "rndc-key"; }; };
// Zona raíz
zone "." IN {
type hint;
file "named.root";};
```

Código 1: named.conf - Configuração para servidor recursivo

Feito isso, salve e feche o arquivo, para terminar a configuração do bind como um servidor DNS cache ou recursivo, acesse o link `http://www.internic.net/zones/root.zone` e baixe o arquivo que contem as zonas raízes. O arquivo deve ser salvo dentro do diretório `c:\bind\etc` com o nome named.root.

Pronto, com estas configurações temos um servidor de DNS recursivo instalado e configurado em nossa máquina. Vamos configurar a máquina local para utilizar o servidor, para isso edite as configurações da rede local para acessar o IP 127.0.0.1, ou seja, a própria máquina, como mostra a Figura5.

Agora temos que iniciar o bind, acesse o painel de controle / ferramentas administrativas / Serviços, na lista procure ISC BIND e logo após em iniciar serviço, como detalhado na Figura 6 se tudo foi configurado corretamente o bind esta pronto para responder as solicitações de DNS.

Para testar o bind podemos utilizar a ferramenta nslookup disponível no windows, abra um terminal de digite os comando como mostrado na Figura 7 :

Observer o retângulo em vermelho que o servidor esta definido para sua própria máquina pelo IP de localhost, abaixo temos consultas de dns para os endereços do cade.com.br e google.com.br com as devidas respostas de endereços IP.

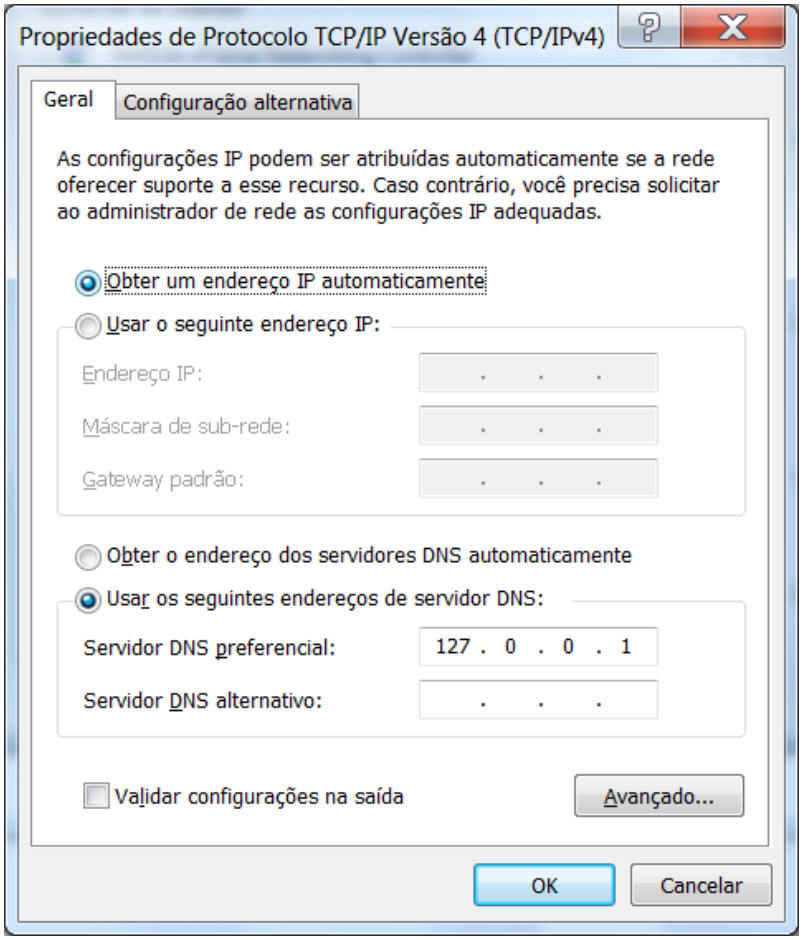

Figura 5. Configuração do DNS para máquina Windows

3.2.2. Configurando um servidor Autoritativo

Seguindo as orientações do site Registro.br para registrar um domínio no Brasil, o primeiro passo é configurar os servidores DNS autoritativos master e slave, servidores que respondem quando uma consulta DNS é solicitada por um cliente(Geralmente um Browser), para exemplificar vamos configurar o dominio pinguim.com, utilizando a máquina windows como master do domínio e o Linux como slave. Edite o arquivo named.conf e acrescente as linhas mostradas no Código 2.

```
...
// Zona Pinguim.com
zone "pinguim.com" IN {
type master;
file "db.pinguim.zone";
allow-transfer { 10.1.1.7; };
};
...
```

Código 2: Exemplo de configuração do named.conf para criação de zona Master

Note que foi adicionado a zona pinguim.com e o arquivo que conterá as informações sobre esta zona é o arquivo db.pinguin.zone.

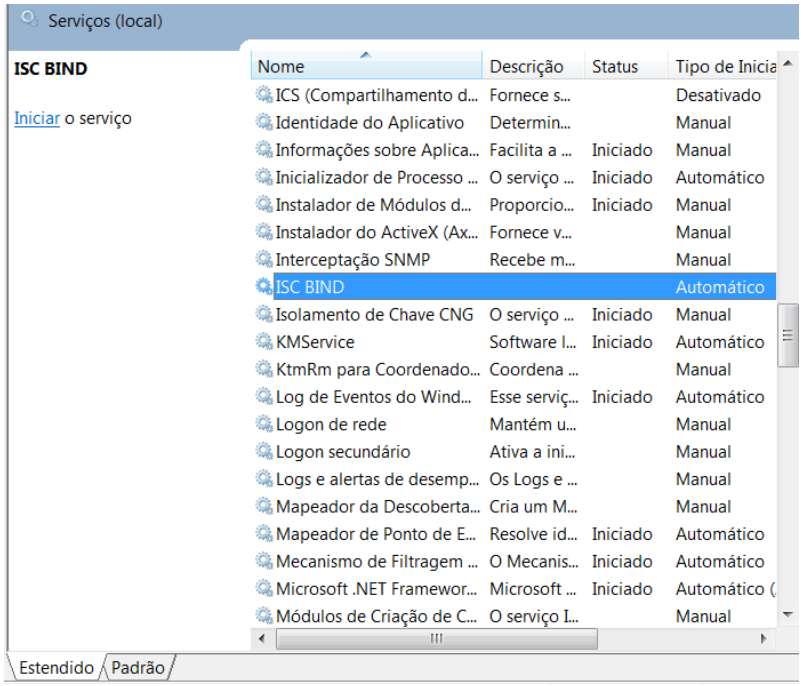

Figura 6. Configuração do DNS para máquina Windows

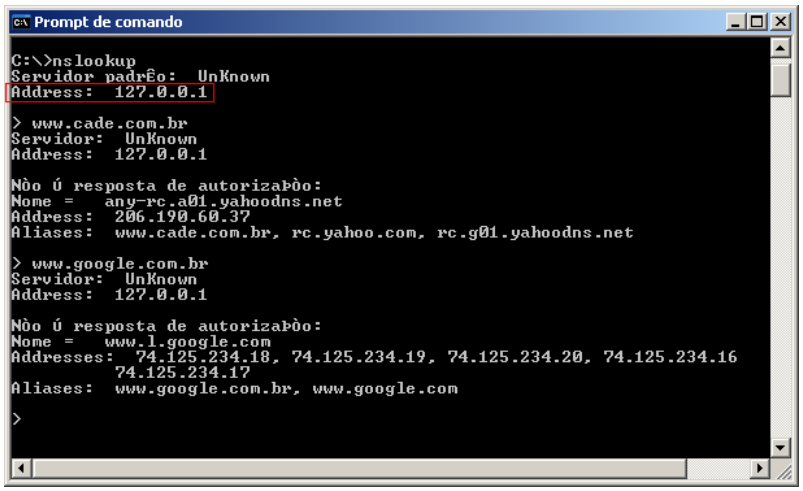

Figura 7. Teste do DNS com a ferramenta nslookup

3.2.3. Criando o arquivo de Zona

Vamos criar o arquivo que contém as informações do nosso domínio, veja o exemplo no Código 3.

```
$TTL 6h
pinguim.com.  IN SOA ns1.pinguim.com. hostmaster.pinguim.com. (
5         ; Serial
             10800     ; Atualizar após 3 horas
             3600      ; Tentar novamente após 1 hora
             604800    ; Expirar após 1 semana
```

```
            86400 )  ; TTL mínimo de 1 dia
;Servidores DNS

@ NS ns1.pinguim.com.
@ NS  ns2.pinguim.com.
;Servidor de email
@ IN MX 10 mail.pinguim.com.
;
; Nomes das Máquinas
pinguim.com  IN  A 10.0.0.6
ns1  IN  A  10.0.0.6
ns2  IN  A 10.0.0.7
;
```

Código 3: Exemplo de configuração para zona Master

Os registros DNS mais frequentemente usados:
SOA – início da zona de autoridade
NS – um servidor de nome autoritativo
A – Um endereço de sistema (host address)
CNAME – o nome canônico para um apelido (alias)
MX – servidor de correio (mail exchanger)
PTR – um ponteiro de nome de domínio (usado em DNS reverso)

3.2.4. Instalação configuração Bind no Linux - Debian

Em sistemas linux exites diversas formas de instalar um pacote, para fins deste tutorial utilizaremos os repositórios da distribuição.

Em um terminal digite como root:

#apt-get install bind9

Após a instalação, o bind já está em execução em sua máquina e configurado para responder como servidor DNS recursivo para rede local, pode variar dependendo da distribuição.

Para verificar se o bind esta em execução digite o seguinte comando como root:

`#ps` auxwww `|` grep bind

`bind` 2918 0.0 3.4 42156 8780 Ssl May28 0:00 /usr/sbin/named -u bind

Vamos agora configurar a máquina para utilizar o DNS instalado em nossa máquina local, para isso, edite o arquivo /etc/resolv.conf e altera a linha nameserver como exemplificado no Código 4.

```
nameserver 127.0.0.1
```

Código 4 - Exemplo de configuração /etc/resolv.conf

Podemos utilizar ferramentas como dig ou nslookup para realizar consultas DNS. A Figura 8 mosta a utilização do dig para realizar consultas recursivas.

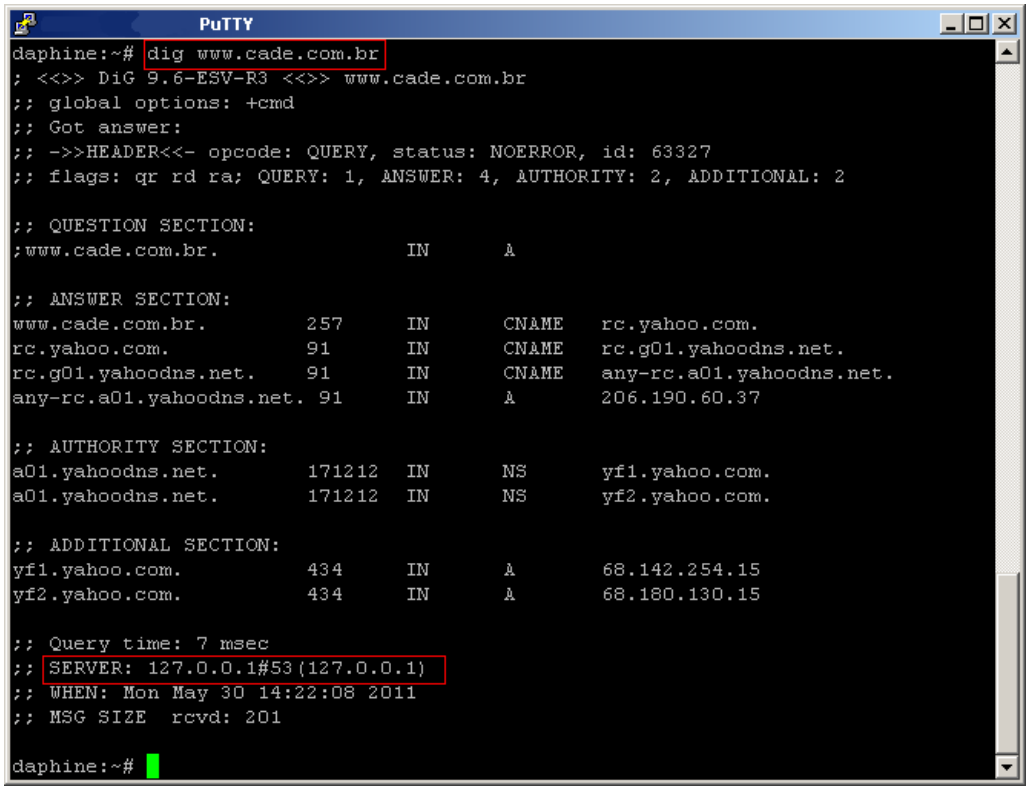

Figura 8. Exemplo de utilização da ferramenta dig

3.3. Criando o Servidor Slave para o Domínio

Como vimos, até o momento criamos o servidor DNS recursivo e logo após implementamos um servidor DNS autoritativo, porem todo o domínio deve possuir dois servidores DNS um master, já criado com Sistema Windows, e um slave, que criaremos agora com o Sistema Linux.

A criação do servidor autoritativo slave é mais fácil, pois toda a configuração de zona é enviada do servidor master para o servidor slave através da sincronização das zonas, esta sincronização ocorre no período de tempo pré definido no arquivo de zona master, campo logo abaixo do serial.

O serial é utilizado para verificar se alguma informação na zona master foi alterada, durante o sincronismo, este serial é verificado, se o serial é o mesmo não é realizado a transferência de zona. Importe lembrar que sempre que for alterado o arquivo de zona master o serial deve ver incrementado, pois somente assim o servidor DNS slave ira realizar atualização do arquivo de zona.

3.3.1. named.conf para o Servidor Slave

Edite o arquivo named.conf, que por padrão é encontrado no diretório `/etc/bind` do servidor slave e acrescente as linhas mostradas no Cógigo 5.

```
// Zona Pinguim.com
zone "pinguim.com" IN {
        type slave;
        file "/etc/bind/slave/db.pinguim.slave";
        masters { 10.1.1.6; };
```

Código 5 - Exemplo de configuração da zona slave.

Note que no parametro file colocamos o arquivo de zona slave dentro do diretório `/etc/bind/slave`, este diretório não exite no sistema e devemos criar e dar permissão para o bind escrever dentro do mesmo.

Após ocorrer a transferência de zona o arquivo db.pinguim.slave ficara como o exemplo do Código 6.

```
$ORIGIN .
$TTL 21600 ; 6 hours
pinguim.com IN SOA ns1.pinguim.com. hostmaster.pinguim.com. (
2          ; serial
10800      ; refresh (3 hours)
3600       ; retry (1 hour)
604800     ; expire (1 week)
86400      ; minimum (1 day)
)
NS ns1.pinguim.com.
$ORIGIN pinguim.com.
ns1 A 10.0.0.6
```

Código 6 - Arquivo de zona slave.

Note que este arquivo não deve ser criado manualmente e sim criado automaticamente na sincronização das zonas master e slave. O Código 7 mostra o arquivo syslog do servidor linux realizando a transferência de zona entre o servidor slave e master.

```
May 28 23:22:43 dns named[2764]:
zone pinguim.com/IN: Transfer started.
May 28 23:22:43 dns named[2764]:
transfer of 'pinguim.com/IN' from 10.1.1.6#53:
connected using 10.1.1.7#42062
May 28 23:22:44 dns named[2764]:
zone pinguim.com/IN: transferred serial 2
May 28 23:22:44 dns named[2764]:
ransfer of 'pinguim.com/IN' from 10.1.1.6#53: Transfer completed:
 1 messages, 5 records, 166 bytes, 0.216 secs (768 bytes/sec)
```

Código 7 - Log do sistema.

3.4. Teste em ambiente real

Teste-1 Teste realizado na rede local da empresa com aproximadamente 20 máquinas com acesso a internet.
Configurações de Hardware:
Pentium Dual Core 2.4 GHz
RAM 2 GB / HD 80 GB
Sistema Operacional: Windows 2008
Tempo em produção: 15 Dias (2 Semanas)
Conclusões: Ao final do teste foi constatado que o Bind rodando sobre a plataforma windows mostrou-se estável e foi imperceptível para o usuário final.

Teste-2 Teste realizado em rede com 4000 usuários com acesso a internet executando os mais variados serviços de rede.
Configurações de Hardware:
HP Server TC 2120
Pentium III Xeon
RAM 512 MB/40GB-SCSI
Sistema Operacional: Windows 2003
Tempo em produção: 7 Dias (1 Semana)
Conclusões: O teste decorreu sem problemas, o uso do servidor foi transparente para os usuários, não houve problemas ou travamentos no servidor. Foi notado porém um elevado uso de CPU/Memória da máquina, o que não ocorre em servidores executando Linux.

4. conclusão

Podemos dizer que sem a utilização de servidores DNS a Internet seria algo bem complicado de se utilizar, e ficaria restrito a poucas pessoas, a utilização do DNS torna a internet um facilitador, pois mandamos e-mail, navegamos, postamos em redes sociais sem nos preocupar com todo o processo de conversão de nomes em IP, que fica em uma camada de abstração para o usuário final.

Já quanto a utilização do BIND como servidor de DNS, o mesmo se mostrou maduro o suficiente para rodar em diversos Sistemas Operacionais com estabilidade e escalabilidade.

Referências

ISC (2011). Isc. Disponível em: <http://www.isc.org>. Acesso em: Abril 2011.

POP-BA (2011). Pop-ba. Disponível em: <http://www.pop-ba.rnp.br>. Acesso em: Abril 2011.

Registrobr (2011). Perguntas frequentes. Disponível em: <http://registro.br>. Acesso em: Abril 2011.

RNP (2011). Rede nacional de pesquisa - rs. Disponível em: <http://www.pop-rs.rnp.br /carros>. Acesso em: Abril 2011.

Root-Servers (2011). Root servers. Disponível em: <http://www.internic.net/zones/root.zone>. Acesso em: Abril 2011.