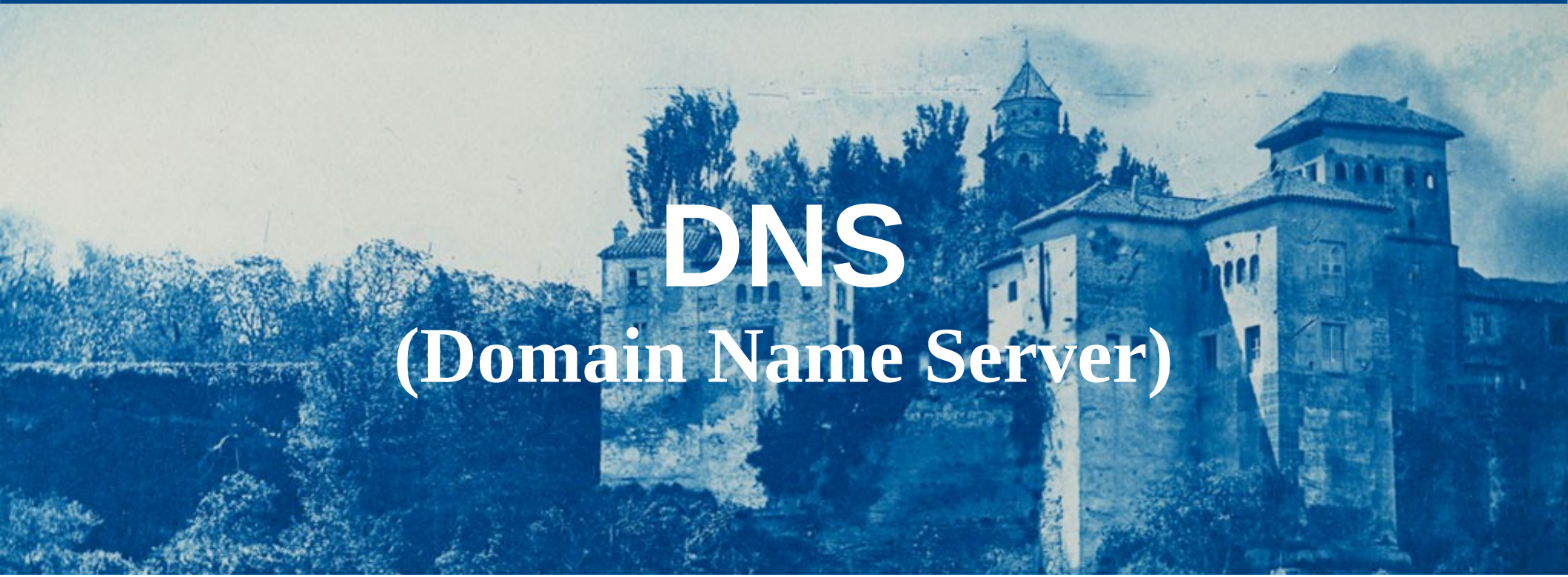
Aula 03



DNS
(Domain Name Server)

Prof. Roitier Campos Gonçalves

Objetivos

- Entender o funcionamento do DNS
- Configurar clientes DNS
- Configurar e testar Servidores DNS

DNS – Domain Name Server

O DNS - Domain Name Server - se enquadra nos principais serviços de redes TCP/IP. A finalidade do DNS é converter nomes como www.conectiva.com.br em endereços IP como 200.242.140.10. É

importante salientar que o DNS faz também a resolução reversa, ou seja, converte endereços IP para nomes.

Nos sistemas Linux existem duas técnicas para fazer resoluções, a primeira forma é através de uma tabela de hosts (/etc/hosts), a outra é feita através da consulta a um servidor de nomes (DNS).

o DNS é um banco de dados com servidores distribuídos e organizados de forma hierárquica, espalhados por toda Internet; de forma que todo servidor de nomes é também cliente de outro, pois caso um não consiga resolver um nome (traduzir para um número IP), este consultará outro e assim por diante.

Fonte: http://pt.wikibooks.org/wiki/Administra%C3%A7%C3%A3o_de_Redes_GNU/Linux

Os 13 Servidores Raiz

Existem 13 servidores raiz distribuídos ao redor do mundo (10 nos EUA, 2 na Europa e 1 na Ásia; dos 10 nos EUA, a maioria é operada por agências governamentais americanas).

Este é o número máximo tecnicamente possível. Se um servidor quebrar, os outros 12 ainda continuam funcionando, e mesmo se os 13 servidores caírem simultaneamente a resolução dos nomes de domínio (a principal função dos servidores raiz) continuaria sendo feita em outros servidores de nome de domínio distribuídos hierarquicamente através da Internet.

Para aumentar a base instalada destes servidores, foram criadas réplicas localizadas por todo o mundo, inclusive no Brasil.

Fonte:http://pt.wikipedia.org/wiki/Servidor_Raiz

Sugestão de leitura:

http://www.nic.br/imprensa/clipping/2012/midia459.htm

Porque ter um Sevidor DNS Local

A resolução de nomes é uma tarefa, muitas vezes, onerosa para a rede, tendo em vista que cada requisição feita à rede busca, inicialmente, um DNS Server para resolver o nome, antes que esta prossiga ao seu destino.

Algumas situações em que o Servidor DNS é relevante:

- O Cliente paga pelo tráfego gerado na rede;
- O Cliente não tem acesso a Internet;
- O Destino é um host da rede local;
- Criar um Servidor DNS Cache;

Funcionamento do DNS

Cenário: Abrir o site “www.linux.com” em um navegador:

O sistema faz as seguintes etapas:

1 - Verifica se o www.linux.com existe no arquivo /etc/hosts. Se sim, resolve,

2 - Se não, ele usará um dos name servers em /etc/resolv.conf e pergunta para eles. Agora que começa a ficar interessante.

DNS Resolver

Os Servidores que aparecem no /etc/resolv.conf são chamados de Servidores de Cache ou simplesmente "DNS Resolvers" (resolvedores).

Eles buscam os nomes na internet e armazenam uma cópia em memória (cache). A pergunta chega ao DNS Cache vindo da rede local e, caso o cache ainda não tenha essa resposta, ele para a Internet.

Hierarquia do DNS

O DNS é hierárquico pois é baseado em conceitos tais como espaço de nomes e árvore de domínios. Assim existe isolamento de nomes e delegação de autoridade.

A Figura a seguir apresenta uma visão abreviada da estrutura do DNS definida para a Internet. O principal domínio, o root, o de mais alto nível foi nomeado como sendo um ponto (.). No segundo nível foram definidos os chamados "Top-level-domains" TLD. Estes domínios são bastante conhecidos, sendo os principais:

com: Organizações comerciais

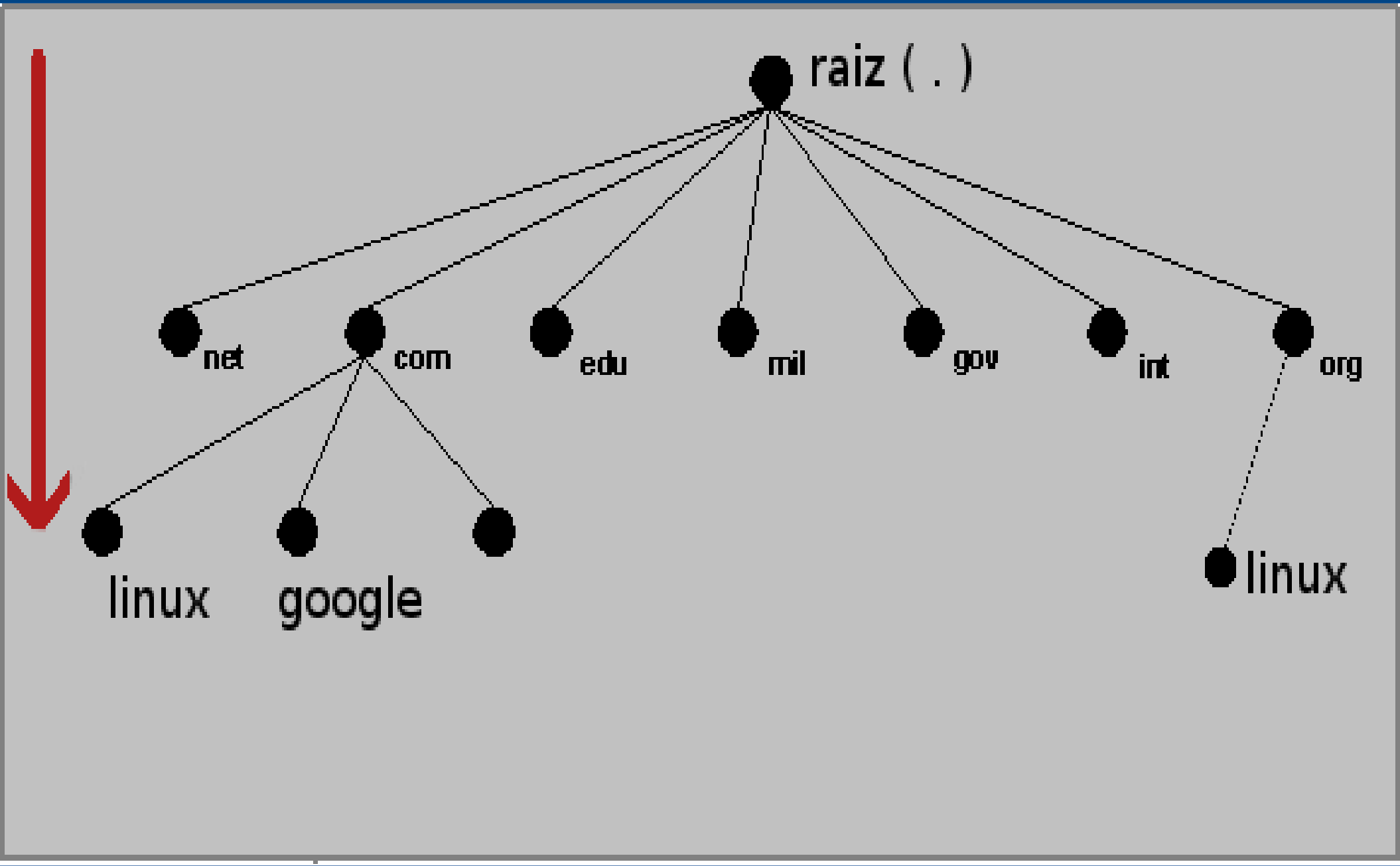
gov: Organizações governamentais

edu: Instituições educacionais

org: Organizações não comerciais

net: Serviços de rede e comunicação

...Hierarquia do DNS



Descobrir o IP (no braço)

O comando “dig” é o acrônimo para "***domain information groper***", que significa algo como **"aquele que busca por informações de domínio no escuro"**, e ao mesmo tempo, a palavra dig em inglês significa literalmente **"escavar"**.

```
root@Notebook-RCG:/home/roitier# dig www.iftm.edu.br

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> www.iftm.edu.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59947
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.iftm.edu.br.          IN    A

;; ANSWER SECTION:
www.iftm.edu.br.     169  IN    A     187.72.225.18

;; Query time: 111 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Mar  2 14:01:46 2015
;; MSG SIZE  rcvd: 49
```

Algumas ações de reconhecimento

- dpkg -L bind9 – Lista diretorios criados pela instalação;
- cat /etc/bind/db.root – Visualizar os 13 servidores raiz;
- cat /etc/resolv.conf – Visualizar os Servidores DNS da máquina;
- #service bind9 status - Mostra status do daemon

Tipos de DNS

Existem basicamente três tipos de servidores DNS:

- **Servidor Caching:** Definido como um servidor que guarda em cache consultas que já foram anteriormente solicitadas, de forma a melhorar a performance da resolução de nomes. Este tipo de servidor também é definido como um servidor que é capaz apenas de fazer consultas para resolver endereços , ou seja, ele é um servidor destinado a fazer e guardar consultas, não sendo responsável por nenhuma zona;

- **Servidor Primário:** Definido como um servidor autorizado (servidor que tem autoridade sobre uma zona), ou seja, que mantém a base de dados de um determinada zona. Este servidor além de fazer consulta a servidores raízes também é consultado por outros servidores DNS como responsável (autorizado) pela zona em que foi delegada;

- **Servidor Secundário:** Este servidor é definido como uma cópia do servidor primário [master]. É utilizado pelos clientes quando o servidor master, por algum motivo, pára de funcionar;

- **Servidor Forwarding:** que remete a solicitação para outros servidores de nomes.

BIND

O BIND (Berkeley Internet Name Domain) é o servidor de nomes utilizado na grande maioria dos servidores da Internet, provendo uma estável e robusta arquitetura sobre a qual as organizações podem construir sua estrutura de nomes. Ele pode ser instalado através do APT, como abaixo:

 # aptitude install bind9

ou

 # apt-get install bind9 bind9-doc bind9utils dnsutils

Obs: Por padrão, o Bind vem configurado como Servidor Cache.

Utilize o comando a seguir para verificar o que o BIND9 criou em seu Sistema Operacional

#dpkg -L bind9

Estrutura do diretorio/etc/bind

bind.keys

db.0

db.127

db.255

db.empty

db.local

db.root -

named.conf

named.conf.default-zones

named.conf.local

named.conf.options

rndc.key

zone.rfc1918

OBSERVAÇÃO:

O Debian divide o arquivo named.conf em vários outros, a fim de melhorar a dinâmica das consultas.

Observe que o arquivo named.conf, a partir da divisão, passa a funcionar como um direcionador de consultas, dada a utilização da função include:

Exemplo:

include "/etc/bind/named.conf.local";

BIND

Existem 3 arquivos principais que precisam de uma maior atenção:

- **named.conf.local –** arquivo onde são criadas as zonas de domínio,
- **resolv.conf -** arquivo do próprio linux onde são especificados os endereços de servidores DNS
- **named.conf.local -** arquivo que contém os RR (Resource Records);

Além destes arquivos, dando um comando ls dentro da pasta do bind podemos observar a existência de outros.

Configuração do BIND9

A primeira coisa a fazer é criar a zona de dominio. Para isso, utilize o arquivo “ named.conf.local”::

- Edite o arquivo “named.conf.local”

#nano /etc/bind/named.conf.local

... /etc/bind/named.conf.local...

 # Zona direta - Responsável pela conversão de nomes para Ips. Caso esse servidor # atenda duas zonas, crie dois blocos como abaixo:

zone “roitier.com.br” { //Informe o nome do domínio desejado

type master; //master é servidor primário e slave é secundário

file “/etc/bind/db.zonaRoitier”; //indica o local onde o arquivo que contém os endereços de DNS ficará

};

 # Zona de reverso - convertendo IP’s em nomes.

zone “20.in-addr.arpa” {

type master;

file “/etc/bind/db.20reverso”;

};

/etc/bind/db.zonaRoitier

Este arquivo contém a configuração do dominio que foi apontado no arquivo named.conf.local:

```
@ IN SOA servidor.roitier.com.br. hostmaster.roitier.com.br. (

2008061645 3H 15M 1W 1D )

NS servidor.roitier.com.br.

IN MX 10 servidor.roitier.com.br.

roitier.com.br. A 100.100.100.100

www A 100.100.100.100

ftp A 100.100.100.100

smtp A 100.100.100.100
```

OBSERVAÇÕES:

Nesse arquivo a formatação é especialmente importante.

Você pode usar espaços e tabs (ambos têm o mesmo efeito) para organizar as opções, mas existem algumas regras.

As linhas "IN SOA" até "IN MX" precisam ficar justificadas (como no exemplo) e você não pode esquecer dos espaços entre as opções. Caso queira incluir comentários, use ";" ao invés de "#", como em outros arquivos.

Explicando..../etc/bind/db.zonaRoitier

@ IN SOA servidor.roitier.com.br. hostmaster.roitier.com.br.

“@” - indica a origem do domínio e, ao mesmo tempo, o início da configuração. Ela é sempre usada, assim como em um endereço de e-mail.

“IN” é abreviação de "internet" e o "SOA" de "Start of autority". Em seguida vem o nome do seu servidor seguido do e-mail de contato do administrador (você).

Nota: Todos os nomes de domínio terminam com um ponto; em muitas situações o ponto é omitido, mas ele é obrigatório dentro da configuração do Bind.

A linha diz:

“na internet, o servidor "servidor" responde pelo domínio "roitier.com.br" e o
e-mail do responsável pelo domínio é "hostmaster@roitier.com.br(“

Explicando..../etc/bind/db.zonaRoitier

A primeira linha termina com um parênteses, o que indica o início da configuração do domínio. Temos então:

2008061645 3H 15M 1W 1D)

- O "2015030845" é o valor de sincronismo, que permite que o servidor DNS secundário se mantenha sincronizado com o principal, detectando alterações na configuração. *Uma observação é que o número no servidor primário deve ser sempre superior ao número no servidor secundário, caso contrário a atualização nunca é disparada.*
- Os quatro campos seguintes (3H 15M 1W 1D) orientam o servidor DNS secundário (caso você tenha um). O primeiro campo indica o tempo que o servidor aguarda entre as atualizações (3 horas). Caso ele perceba que o servidor principal está fora do ar, ele tenta fazer uma transferência de zona, ou seja, tenta assumir a responsabilidade sob o domínio. Caso a transferência falhe e o servidor principal continue fora do ar, ele aguarda o tempo especificado no segundo campo (15 minutos) e tenta novamente.

...

Explicando..../etc/bind/db.zonaRoitier

- O terceiro campo indica o tempo máximo que ele pode responder pelo domínio, antes que as informações expirem e o tempo mínimo antes de devolver o domínio para o servidor principal quando ele retornar (1 dia).

***Nota**: Se você acha que uma semana é inadequado, você pode aumentar ou diminuir o valor, usando, por exemplo, "4W" (4 semanas).*

OBS: outra opção é separar os valores por linha, incluindo comentários, como em:

2008061645; serial

10800; refresh, seconds

900; retry, seconds

604800; expire, seconds

86400); minimum, seconds

Explicando..../etc/bind/db.zonaRoitier

As duas linhas a seguir concluem a seção inicial:

NS servidor.roitier.com.br.

IN MX 10 servidor.roitier.com.br.

- "NS" (Name Server) diz quem são os servidores DNS responsáveis pelo domínio. Ao usar apenas um servidor DNS, você simplesmente repete o nome do servidor, seguido pelo domínio, como adicionamos na primeira linha. Caso você esteja usando dois servidores, então você precisa declarar ambos, como segue:

NS servidor.gdhn.com.br.

NS ns2.gdhn.com.br.

Explicando..../etc/bind/db.zonaRoitier

A linha "IN MX" (Mail Exchangers) é necessária sempre que você pretende usar um servidor de e-mails. No exemplo, a mesma máquina está sendo usada para tudo, por isso novamente o "servidor.gdhn.com.br", que acumula mais esta função. Assim como no caso do DNS, você pode especificar um servidor de e-mails secundário, que passa a receber os e-mails caso seu servidor principal saia fora do ar. Nesse caso, você adiciona uma segunda linha, como em:

IN MX 10 servidor.gdhn.com.br.

IN MX 20 outroservidor.outrodominio.com.br.

Obs: Os números indicam a prioridade de cada servidor.

Explicando..../etc/bind/db.zonaRoitier

Depois dessas linhas iniciais, temos a parte mais importante, em que você especifica o endereço IP do servidor e pode cadastrar subdomínios, como em:

roitier.com.br. A 100.100.100.100

www A 100.100.100.100

ftp A 100.100.100.100

smtp A 100.100.100.100

Obs: Este arquivo incluí três subdomínios, o "www", "ftp" e "smtp", ambos relacionados ao IP do servidor. Isso permite que os visitantes digitem "www.roitier.com.br" ou "ftp.roitier.com.br" no navegador.

Ao trabalhar com dois servidores DNS, adicione também uma entrada para o servidor secundário, especificando o nome do segundo servidor (ns2 no exemplo) e o endereço IP, como em:

ns2 A 100.100.100.200

db.reverso (arquivo exemplo)

```
; BIND zone file for 192.168.1.xxx
;
$TTL    3D
;
@       IN      SOA    ns.home.lan.       root.home.lan. (
                              2013050601     8H 2H 4W1D )
;
                NS      ns.home.lan.    ; Nameserver address
100             PTR     server.home.lan.
100             PTR     ns.home.lan.
100             PTR     mail.home.lan.
101             PTR     virtual.home.lan.
1               PTR     router.home.lan.
```

named.conf.default-zones

Arquivo responsável pelas configurações de zonas padrão do Servidor DNS. Cada uma das seções indica a localização de um arquivo, onde vai a configuração referente a ela.

***Por exemplo**, na primeira seção ("zone ".") é indicado o arquivo "/etc/bind/db.root", que contém os endereços dos 13 root servers, que o Bind contactará na hora de resolver os domínios.*

Obs: Esta configuração vem incluída por padrão e não deve ser alterada.

named.conf.default-zones

```
zone "." {
type hint;
file "/etc/bind/db.root";
};
zone "localhost" {
type master;
file "/etc/bind/db.local";
};
zone "127.in-addr.arpa" {
type master;
file "/etc/bind/db.127";
};
zone "0.in-addr.arpa" {
type master;
file "/etc/bind/db.0";
};
zone "255.in-addr.arpa" {
type master;
file "/etc/bind/db.255";
};
```

/etc/bind/named.conf.options

```
options {
    directory "/var/cache/bind";
    version "bind8";
    listen-on { 172.16.0.1;192.168.0.1; };
    forwarders { 8.8.8.8; 200.67.222.222; };
    dnssec-validation auto;
    auth-nxdomain no;
    listen-on-v6 { any;};
};
```

/etc/bind/named.conf.options

- directory: diretório padrão do BIND 9.
- version: informa versão no BIND, para fins de segurança, oculte ou altere a versão do daemon.
- listen-on: IP das interfaces do servidor que responderão às requisições nas portas 53 UDP e TCP.
- forwarders: IP dos servidores que o servidor usará para pesquisar sobre domínios aos quais ele não responda.

/etc/resolv.conf

Este arquivo indica qual o servidor é responsável por resolver as requisições da máquina. Com esta configuração, o servidor desta máquina passa a ser ela mesma, apontada pelo endereço de loopback.

#nano /etc/resolv.conf

domain home.lan

search home.lan

Nameserver 127.0.0.1

Obs: Assim, quando nos referirmos ao sistema “server”, este será procurado no domínio “home.lan”, resultando no nome “server.home.lan”.

Reiniciar o serviço

Para reiniciar o BIND9 utiliza um dos comandos a seguir:

 # /etc/init.d/bind9 restart

 # service named restart

 # systemclt bind9 restart

Testando....

Alguns comandos podem ser utilizados para testar as configurações e funcionalidades:

 # named-checkconf

 # named-checkzone

 # nslookup;

 # dig;

 # ping;

 # traceroute