

Prática de Laboratório 04

DNS

Esta prática de laboratório tem como objetivo demonstrar o processo de instalação e configuração do DNS. Para tal, será considerado um cenário de uma rede local na qual clientes se conectam ao servidor para obter dados de domínio. O servidor de domínio utilizado no laboratório será o servidor *bind*, uma das principais alternativas para ambiente Linux.

1 Topologia

O cenário de aplicação consiste da conexão de uma rede local, conforme ilustrada na Figura 1. Tal topologia apresenta os seguintes elementos:

- 1 servidor DNS com acesso à Internet;
- 2 sistema final sem acesso à Internet.

Além disso, parte-se da premissa que ambas as máquinas já possuem endereçamento estático definido

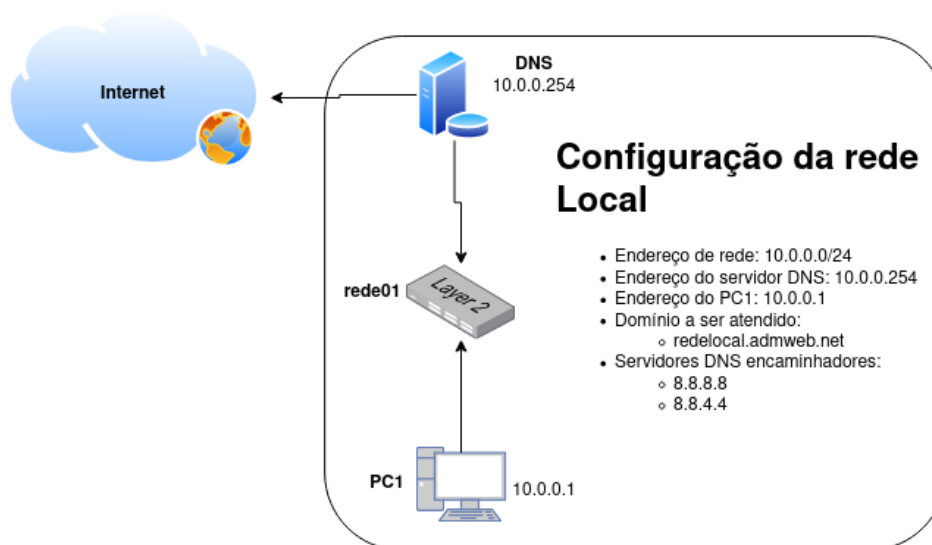


Figura 1: Topologia de rede empregada no cenário de teste.

2 Preparação do ambiente

Para preparação do ambiente, deve-se instalar 2 instâncias Linux, utilizando a imagem registry.gitlab.com/ifal1/admweb/ubuntu-baseline. O arquivo [lab04_dns_cen_01.zip](#) apresenta o laboratório Kathará com a topologia construída, porém sem as configurações do DNS, as quais iremos implementar ao longo deste cenário. Para iniciar o experimento, basta descompactar o arquivo supracitado, iniciar um terminal posicionado no diretório e executar o seguinte comando:

```
ivocalado@darkside: /admweb/labs/lab04_dns_cen01$ kathara lstart
```

Por outro lado, ao término do experimento, pode-se encerrar o experimento através do comando abaixo:

```
ivocalado@darkside: /admweb/labs/lab04_dns_cen01$ kathara lclean
```

3 Passos para configuração do servidor DNS

Após o início do laboratório deve-se executar os seguintes passos na janela aberta para o servidor DNS.

3.1 Instalação do pacote Bind

O passo inicial consiste da instalação do servidor DNS na máquina destinada a servir como servidor. Para tal, deve-se i) atualizar a base do apt-get e ii) solicitar a instalação do pacote bind, documentação e utilitários:

```
apt-get update
```

```
apt-get install bind9 bind9utils bind9-doc bind9-host
```

Durante a instalação será questionado o *timezone* da instalação. Em tal passo deve inicialmente informar o valor **2** para indicar *America* e em seguida o valor **126** para **Recife** (local mais próximo disponível de Alagoas).

Para verificar a versão instalada basta executar o comando abaixo:

```
named -v
```

O comando acima que trará a seguinte saída:

```
root@dhcp:/# named -v
BIND 9.16.1-Ubuntu (Stable Release) <id:d497c32>
```

Por outro lado, para exibir informações mais detalhadas, podemos fazer uso da opção *-V*:

```
root@dhcp:/# named -V
BIND 9.16.1-Ubuntu (Stable Release) <id:d497c32>
running on Linux x86_64 5.8.0-38-generic #43~20.04.1-Ubuntu SMP Tue Jan 12 16:39:47
    ↪ UTC 2021
built by make with '--build=x86_64-linux-gnu' '--prefix=/usr' '--includedir=/usr/
    ↪ include' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--sysconfdir=/
    ↪ etc' '--localstatedir=/var' '--disable-silent-rules' '--libdir=/usr/lib/x86_64-
    ↪ linux-gnu' '--runstatedir=/run' '--disable-maintainer-mode' '--disable-
    ↪ dependency-tracking' '--libdir=/usr/lib/x86_64-linux-gnu' '--sysconfdir=/etc/
    ↪ bind' '--with-python=python3' '--localstatedir=/' '--enable-threads' '--enable-
    ↪ largefile' '--with-libtool' '--enable-shared' '--enable-static' '--with-gost=no
    ↪ ' '--with-openssl=/usr' '--with-gssapi=/usr' '--with-libidn2' '--with-json-c'
    ↪ '--with-lmdb=/usr' '--with-gnu-ld' '--with-maxminddb' '--with-atf=no' '--enable
    ↪ -ipv6' '--enable-rrl' '--enable-filter-aaaa' '--disable-native-pkcs11' '
    ↪ build_alias=x86_64-linux-gnu' 'CFLAGS=-g -O2 -fdebug-prefix-map=/build/bind9-
    ↪ yEt4rt/bind9-9.16.1=. -fstack-protector-strong -Wformat -Werror=format-security
    ↪ -fno-strict-aliasing -fno-delete-null-pointer-checks -DNO_VERSION_DATE -
    ↪ DDIG_SIGCHASE' 'LDFLAGS=-Wl,-Bsymbolic-functions -Wl,-z,relro -Wl,-z,now' '
    ↪ CPPFLAGS=-Wdate-time -D_FORTIFY_SOURCE=2'
compiled by GCC 9.3.0
compiled with OpenSSL version: OpenSSL 1.1.1f 31 Mar 2020
linked to OpenSSL version: OpenSSL 1.1.1f 31 Mar 2020
compiled with libxml2 version: 2.9.10
linked to libxml2 version: 20910
compiled with json-c version: 0.13.1
linked to json-c version: 0.13.1
compiled with zlib version: 1.2.11
linked to zlib version: 1.2.11
linked to maxminddb version: 1.4.2
threads support is enabled

default paths:
  named configuration: /etc/bind/named.conf
```

```
rndc configuration: /etc/bind/rndc.conf
DNSSEC root key: /etc/bind/bind.keys
nsupdate session key: //run/named/session.key
named PID file: //run/named/named.pid
named lock file: //run/named/named.lock
geoip-directory: /usr/share/GeoIP
```

3.2 Habilitando o Bind para funcionar em IPV4

Antes de continuar, vamos colocar o BIND no modo IPv4, já que nossa rede privada usa exclusivamente o IPv4. Este passo consiste na edição do arquivo `/etc/default/named`, editando a linha `OPTIONS` com o seguinte valor:

```
OPTIONS="-u bind -4"
```

Após a configuração supracitada, deve-se reiniciar o servidor DNS:

```
/etc/init.d/named start
```

```
root@dhcp:/# /etc/init.d/named start
* Starting domain name service... named [ OK ]
```

Para verificar o status do servidor DNS podemos executar o seguinte comando:

```
/etc/init.d/named status
```

```
root@dhcp:/# /etc/init.d/named status
* bind is running
```

Uma outra opção é utilizar o comando `rndc` para obter informações mais detalhadas:

```
rndc status
```

```
root@dhcp:/# /etc/init.d/named status
* bind is running
root@dhcp:/# rndc status
version: BIND 9.16.1-Ubuntu (Stable Release) <id:d497c32>
running on dhcp: Linux x86_64 5.8.0-38-generic #43~20.04.1-Ubuntu SMP Tue Jan 12
    ↪ 16:39:47 UTC 2021
boot time: Mon, 01 Feb 2021 21:34:40 GMT
last configured: Mon, 01 Feb 2021 21:34:40 GMT
configuration file: /etc/bind/named.conf
CPUs found: 12
worker threads: 12
UDP listeners per interface: 12
number of zones: 102 (97 automatic)
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is OFF
recursive clients: 0/900/1000
tcp clients: 0/150
TCP high-water: 0
server is up and running
```

3.3 Configuração básica do servidor DNS primário

A configuração do BIND consiste em vários arquivos, que são incluídos no arquivo de configuração principal, o `named.conf`. Estes nomes de arquivos começam com *named* porque este é o nome do processo que o BIND executa (abreviação de ‘domain name daemon’). Vamos começar configurando o arquivo de opções.

3.3.1 Configurando o arquivo `/etc/bind/named.conf.options`

Abra o arquivo `/etc/bind/named.conf.options` e modifique o conteúdo para o seguinte:

```
#Especifica a lista de clientes para o qual consultas recursivas serão permitidas para
    ↪ o servidor DNS
acl "trusted" {
    10.0.0.0/24;
};

#O bloco option especifica a configuração básica para nosso servidor DNS
options {
    directory "/var/cache/bind"; #Indica o local onde serão

    recursion yes; # Habilita consultas recursivas
    allow-recursion { trusted; }; # Define os clientes que podem realizar
    listen-on { 10.0.0.254; }; # Indica o endereço IP da máquina onde o DNS irá
        ↪ operar
    allow-transfer { none; }; # Desabilita a zona de transferência

    # Especifica os encaminhadores que serão utilizados para o caso de não ser
        ↪ possível resolver um dado domínio
    forwarders {
        8.8.8.8;
        8.8.4.4;
    };
};
```

A configuração supracitada possui os seguintes destaques:

- O bloco **acl “trusted”** especifica um ou vários blocos de endereços que serão utilizados em uma regra de ACL para autorizar a consulta recursiva;
- O bloco **option** é o bloco principal de configuração. Nele estão descritas as principais configurações do servidor DNS;
- A entrada **directory** indica onde serão salvos a base de registros do cache DNS;
- A entrada **recursion** indica se o servidor DNS operará requisições recursivas;
- A entrada **allow-recursion** indica qual será o bloco de endereços autorizados. Neste exemplo é passado o bloco “trusted”;
- A entrada **listen-on** indica em qual interface da máquina o servidor DNS irá operar;
- A entrada **allow-transfer** indica se o servidor DNS irá permitir a cópia dos dados da zona DNS;
- O bloco **forwarders** identifica a lista de endereços IPs para servidores DNS de encaminhamento. Tais servidores serão acionados para o caso do servidor DNS não ser capaz de resolver do domínio solicitado.

Antes de prosseguir é importante verificar se o arquivo de configuração está correto. Para tal, basta invocar o comando `named-checkconf`, o qual irá apontar os erros no arquivo caso os encontre. Por exemplo:

```
named-checkconf
```

```
root@dhcp:/# named-checkconf
/etc/bind/named.conf.options:4: missing ';' before '}'
```

Por fim, deve-se reiniciar o servidor DNS, através do comando a seguir:

```
/etc/init.d/named restart
```

```
* Stopping domain name service... named waiting for pid 552 to die
[ OK ]
* Starting domain name service... named [ OK ]
```

3.3.2 Testando o encaminhamento de requisições

Apenas com a configuração já realizada o servidor DNS já trata requisições realizadas encaminhando os pacotes para os servidores de encaminhamento (8.8.8.8 e 8.8.4.4). Para testar tal funcionalidade, temos de acessar o terminal da máquina PC1 e executar o seguinte comando:

```
dig A google.com @10.0.0.254
```

O comando supracitado solicita a resolução da entrada do tipo A do domínio [google.com](https://www.google.com) requisitando ao servidor DNS. Como o servidor não é capaz de resolver o domínio, faz uma consulta recursiva aos servidores DNS marcados como encaminhaadores. A saída do comando **dig** é semelhante à seguinte:

```
root@pc1:/# dig A google.com @10.0.0.254

; <<>> DiG 9.16.1-Ubuntu <<>> A google.com @10.0.0.254
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63636
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d98be75ca1a8d14001000000601887908eb4de5a91f63f0b (good)
;; QUESTION SECTION:
;google.com.      IN A

;; ANSWER SECTION:
google.com. 15 IN A 172.217.30.14

;; Query time: 331 msec
;; SERVER: 10.0.0.254#53(10.0.0.254)
;; WHEN: Mon Feb 01 22:58:24 UTC 2021
;; MSG SIZE rcvd: 83
```

A partir da resposta apresentada, o **PC1** passa a saber que o endereço para o domínio [google.com](https://www.google.com) é o **172.217.30.14**.

3.4 Criação de zonas de resolução de nomes

O passo seguinte na nossa configuração consiste na configuração de zonas de resolução. Considerando o nosso cenário original, queremos adicionar a zona de resolução de nomes para o domínio [redelocal.admweb.net](https://www.redelocal.admweb.net). Para tal, devemos seguir os passos apresentados a seguir.

3.4.1 Configuração do arquivo `/etc/bind/named.conf.local`

No primeiro passo desta etapa deve-se editar o arquivo `/etc/bind/named.conf.local` a fim de possibilitar declaração da zona que será atendida pelo servidor DNS. Para tal, o conteúdo do arquivo deve ser substituído pelo apresentado a seguir:

```

zone "redelocal.admweb.net" {
    type master;
    file "/etc/bind/zones/db.redelocal.admweb.net"; # caminho para a base da zona
};

zone "0.0.10.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.10.0.0"; # Subrede 10.0.0.0/24
};

```

O primeiro bloco da configuração supracitada tem como objetivo a declaração da resolução de nomes para a zona [redelocal.admweb.net](#). O segundo bloco, por sua vez, tem como objetivo a configuração do DNS reverso. Tal configuração permite que servidores DNS verifiquem a autenticidade de endereços, verificando se o endereço IP atual corresponde ao endereço IP informado pelo servidor DNS.

Sobre tal configuração é importante destacar que o bloco definido leva em consideração o endereço da rede na qual o servidor DNS está instalado. No caso em questão o endereço é o 10.0.0.0/24.

3.4.2 Configuração do arquivo de zonas

O arquivo da zona de encaminhamento está onde definimos os registros DNS para pesquisas de encaminhamentos de DNS. Isso é, quando o DNS receber um nome de consulta, “host1.redelocal.admweb.net”, por exemplo, ele olhará no arquivo da zona de encaminhamento para resolver o endereço IP privado correspondente do **host1**. Para tal, o passo inicial será criar o diretório onde será mantido os arquivos de configuração de zonas:

```
mkdir /etc/bind/zones
```

O passo seguinte será a configuração efetiva do arquivo [/etc/bind/zones/db.redelocal.admweb.net](#). Para tal, iremos utilizar como base o arquivo [/etc/bind/db.local](#):

```
cp /etc/bind/db.local /etc/bind/zones/db.redelocal.admweb.net
```

Ao exibir o conteúdo original tem-se o seguinte:

```
cat /etc/bind/zones/db.redelocal.admweb.net
```

```

root@dhcp:/# cat /etc/bind/zones/db.redelocal.admweb.net
;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA localhost. root.localhost. (
        2      ; Serial
        604800 ; Refresh
        86400  ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
@ IN NS localhost.
@ IN A 127.0.0.1
@ IN AAAA ::1

```

O arquivo na forma como está faz resolução para o domínio **localhost**. Ao utilizar tal configuração estamos definindo temporizadores para o funcionamento do servidor DNS, definindo o número de sequência para as entradas e, no último conjunto de entradas, definido quais entradas serão definidas. Sobre tal configuração é importante destacar que a cada nova entrada de zona o número **Serial** deve ser incrementado em uma unidade.

Para esta configuração vamos considerar o cenário onde o servidor DNS irá resolver os seguintes domínios:

1. host1.redelocal.admweb.net, entrada A, para o IP 10.0.0.5;
2. host2.redelocal.admweb.net, entrada A, para o IP 10.0.0.50;
3. host3.redelocal.admweb.net, entrada CNAME, para o host2.redelocal.admweb.net;
4. email.redelocal.admweb.net, entrada A, para o IP 10.0.0.6;
5. redelocal.admweb.net, entrada MX para email.redelocal.admweb.net.

Desta forma, devemos editar o arquivo supracitado substituindo o conteúdo pelo seguinte:

```
$TTL 604800
@ IN SOA dns.redelocal.admweb.net. root.redelocal.admweb.net. (
    3 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;

@ IN NS dns.redelocal.admweb.net.
dns IN A 10.0.0.254
host1 IN A 10.0.0.5
host2 IN A 10.0.0.50
host3 IN CNAME host2.redelocal.admweb.net.
@ IN MX 10 email.redelocal.admweb.net.
email IN A 10.0.0.6
```

3.4.3 Configuração do arquivo de zona reversa

Os arquivos da zona reverso estão onde definimos os registros DNS PTR para pesquisas de DNS reverso. Isso é, quando o DNS recebe uma consulta pelo endereço IP, “10.0.0.5”, por exemplo, ele olhará no(s) arquivo(s) da zona reversa para resolver o FQDN correspondente, sendo ele, o “host1.redelocal.admweb.net” neste caso.

Para cada zona reversa especificada no arquivo **named.conf.local**, crie um arquivo de zona reversa. Vamos basear nosso(s) arquivo(s) de zona reversa no arquivo de zona amostral **db.127**. Copie-o para o local correto com os seguintes comandos (substituindo o nome do arquivo de destino para que ele corresponda à definição da sua zona reversa):

```
cp /etc/bind/db.127 /etc/bind/zones/db.10.0.0
```

Inicialmente, conterá um conteúdo semelhante ao seguinte:

```
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
@ IN SOA localhost. root.localhost. (
    1 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS localhost.
1.0.0 IN PTR localhost.
```

De maneira similar ao arquivo de zona de encaminhamento, edite o registro do SOA e aumente o valor serial. Após isso, edite o arquivo adicionando entradas PTR para o registro reverso. Os registros PTR para todos os seus servidores cujos endereços IP estão na sub-rede do arquivo de zona que está editando.

No nosso exemplo, isso inclui todos os nossos hosts porque eles estão todos na sub-rede 10.0.0.0/24. Note que a primeira coluna consiste nos dois últimos octetos dos endereços IP privados dos seus servidores em reversed order. Certifique-se de substituir os nomes e endereços IP privados para corresponder aos seus servidores:

```
$TTL 604800
@ IN SOA dns.redelocal.admweb.net. root.redelocal.admweb.net. (
                        3 ; Serial
                        604800 ; Refresh
                        86400 ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
; name servers
    IN NS dns.redelocal.admweb.net.
    IN NS ns2.nyc3.example.com.

; PTR Records
5 IN PTR host1.redelocal.admweb.net. ; 10.0.0.5
50 IN PTR host2.redelocal.admweb.net. ; 10.0.0.50
6 IN PTR email.redelocal.admweb.net. ; 10.0.0.6
```

Antes de continuar, execute a checagem dos arquivos de configuração executando o comando a seguir:

```
named-checkconf
```

O comando *named-checkzone* pode ser usado para verificar a correção dos arquivos da sua zona. Seu primeiro argumento especifica um nome de zona e o segundo especifica o arquivo da zona correspondente, sendo que ambos estão definidos em *named.conf.local*.

```
named-checkzone redelocal.admweb.net /etc/bind/zones/db.redelocal.admweb.net
```

```
root@dns:/# named-checkzone redelocal.admweb.net /etc/bind/zones/db.redelocal.admweb.
↪ net
zone redelocal.admweb.net/IN: loaded serial 3
OK
```

Por fim, deve-se reiniciar o servidor DNS:

```
/etc/init.d/named restart
```

```
root@dns:/# /etc/init.d/named restart
* Stopping domain name service... named waiting for pid 743 to die
[ OK ]
* Starting domain name service... named [ OK ]
```

3.4.4 Testando a resolução de nomes

A partir de agora a resolução de nomes no domínio deve funcionar. Para testar tal funcionalidade, temos de acessar o terminal da máquina PC1 e executar o seguinte comando:

```
dig NS redelocal.admweb.net @10.0.0.254
```

```
root@pc1:/# dig NS redelocal.admweb.net @10.0.0.254

; <<>> DiG 9.16.1-Ubuntu <<>> NS redelocal.admweb.net @10.0.0.254
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56832
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2
```



```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: c291151b8fc3f861010000006018cacdbe57341cc6b24255 (good)
;; QUESTION SECTION:
redelocal.admweb.net. IN NS

;; ANSWER SECTION:
redelocal.admweb.net. 604800 IN NS dns.redelocal.admweb.net.

;; ADDITIONAL SECTION:
dns.redelocal.admweb.net. 604800 IN A 10.0.0.254

;; Query time: 0 msec
;; SERVER: 10.0.0.254#53(10.0.0.254)
;; WHEN: Tue Feb 02 03:45:17 UTC 2021
;; MSG SIZE rcvd: 111
```

```
dig A dns.redelocal.admweb.net @10.0.0.254
```

```
root@pc1:/# dig A dns.redelocal.admweb.net @10.0.0.254

; <<>> DiG 9.16.1-Ubuntu <<>> A dns.redelocal.admweb.net @10.0.0.254
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40324
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: bffb8ece6cc53037010000006018cb1351ef00134bd03f0c (good)
;; QUESTION SECTION:
dns.redelocal.admweb.net. IN A

;; ANSWER SECTION:
dns.redelocal.admweb.net. 604800 IN A 10.0.0.254

;; Query time: 0 msec
;; SERVER: 10.0.0.254#53(10.0.0.254)
;; WHEN: Tue Feb 02 03:46:27 UTC 2021
;; MSG SIZE rcvd: 97
```

```
dig A host1.redelocal.admweb.net @10.0.0.254
```

```
root@pc1:/# dig A host1.redelocal.admweb.net @10.0.0.254

; <<>> DiG 9.16.1-Ubuntu <<>> A host1.redelocal.admweb.net @10.0.0.254
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50285
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: d485eb0e37ead6ff010000006018cb474523aad060bb0b1e (good)
;; QUESTION SECTION:
host1.redelocal.admweb.net. IN A
```

```
;; ANSWER SECTION:
host1.redelocal.admweb.net. 604800 IN A 10.0.0.5

;; Query time: 3 msec
;; SERVER: 10.0.0.254#53(10.0.0.254)
;; WHEN: Tue Feb 02 03:47:19 UTC 2021
;; MSG SIZE rcvd: 99
```

```
dig MX redelocal.admweb.net @10.0.0.254
```

```
root@pc1:/# dig MX redelocal.admweb.net @10.0.0.254

; <<>> DiG 9.16.1-Ubuntu <<>> MX redelocal.admweb.net @10.0.0.254
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48801
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a3d8e6eab7446808010000006018cb8aa323301228cbf549 (good)
;; QUESTION SECTION:
;redelocal.admweb.net. IN MX

;; ANSWER SECTION:
redelocal.admweb.net. 604800 IN MX 10 email.redelocal.admweb.net.

;; ADDITIONAL SECTION:
email.redelocal.admweb.net. 604800 IN A 10.0.0.6

;; Query time: 3 msec
;; SERVER: 10.0.0.254#53(10.0.0.254)
;; WHEN: Tue Feb 02 03:48:26 UTC 2021
;; MSG SIZE rcvd: 115
```

4 Configurando o servidor DNS

O passo final da configuração é a configuração do servidor DNS no cliente **PC1**. Para tal, deve-se modificar o arquivo `/etc/resolv.conf` com o seguinte conteúdo:

```
nameserver 10.0.0.254
```

Após isso, pode-se fazer requisições a partir do **PC1** sem indicar explicitamente o servidor DNS:

```
dig MX redelocal.admweb.net
```

```
root@pc1:/# dig MX redelocal.admweb.net

; <<>> DiG 9.16.1-Ubuntu <<>> MX redelocal.admweb.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21149
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
```

```
; COOKIE: f5718bc136176d56010000006018ce37cfeee43e40ff2321 (good)
;; QUESTION SECTION:
redelocal.admweb.net. IN MX

;; ANSWER SECTION:
redelocal.admweb.net. 604800 IN MX 10 email.redelocal.admweb.net.

;; ADDITIONAL SECTION:
email.redelocal.admweb.net. 604800 IN A 10.0.0.6

;; Query time: 0 msec
;; SERVER: 10.0.0.254#53(10.0.0.254)
;; WHEN: Tue Feb 02 03:59:51 UTC 2021
;; MSG SIZE rcvd: 115
```

5 Configurando o Laboratório Kathará para que a configuração seja persistida

Por fim, para que as configurações do laboratório sejam persistidas faz-se necessário que sejam utilizados os arquivos de startup e o diretório de inicialização dos dispositivos. O laboratório [lab04_dns_cen_02.zip](#) é idêntico ao laboratório 01 apresentando as seguintes modificações:

- Foi modificado o arquivo `dns.startup` adicionando os comandos de instalação na máquina **DNS**;
- Foram modificados os arquivos **pc1.startup**;
- Foram adicionados os arquivos de configuração discutidos no diretório `dns`.