Organização e Conectividade de Sistemas Computacionais 1 - Prática de Laboratório

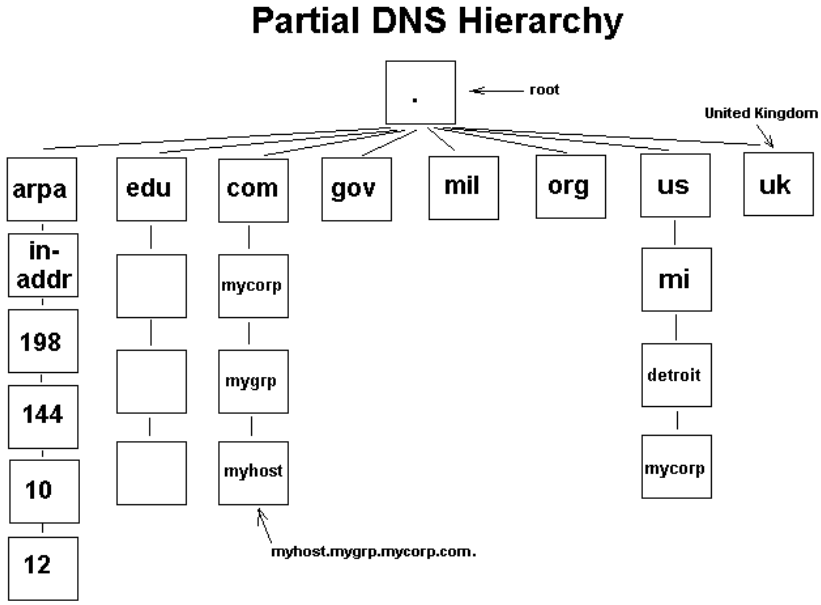
DS - Coltec/UFMG

8 de novembro de 2023

Sumário

Capítulo 1

Configurando o DNS para uma Intranet - Básico



1.1 Introdução

Este tutorial é baseado do seguinte sítio:
`http://www.guiadohardware.net/tutoriais/instalando-servidor-dns/`
É importante considerar que este tutorial foi adaptado para atender as idiossincrasias do Ubuntu server ;)
Introduzimos dizendo que DNS significa *Domain Name System* ou Sistema de nomes de Domínio[1]
A essência do DNS é a invenção de um esquema hierárquico de distribuição de nomes para máquinas conectadas na Internet. O DNS é um banco de dados distribuído e hierárquico.
Seu funcionamento pode ser resumido em mapear um nome completo de uma máquina para um endereço IP. Para um usuário leigo o resultado prático proporcionado pelo DNS é o aumento na usabilidade para referenciar as máquinas na Internet. Sem o DNS o usuário deve obrigatoriamente navegar com números IP, com o DNS o usuário necessita apenas do nome de um determinado *site*.
O programa responsável pelo funcionamento do DNS, que em nosso caso será o BIND 9 (*Berkeley Internet Name Domain*), acionará uma função chamada ***resolver***. O parâmetro de entrada ou argumento desta função será o nome da máquina alvo.
Portanto ao transformar o IP em um nome temos um processo conhecido como resolução de nome.

[1] Inventado por *Paul V. Mockapetris Jon Postel* em 1983.

O DNS é definido tecnicamente em documentos mantidos pelo *Internet Engineering Task Force* (IETF) referenciados como RFC 1034 e 1035[2].
Alguns dos objetivos deste módulo:

- Compreender a importância da utilização do DNS
- Entender por que o DNS é divido em zonas ou domínios de nomes
- O que é o *Forward Lookup Zone*?
- O que é o *Reverse Lookup Zone*?

1.2 Instalação e configuração do servidor de DNS

Utilize sempre a última versão estável do Ubuntu server.

1.2.1 Instale o DNS:

```
apt install bind9
```

1.2.2 Tenha certeza que o OpenSSH server está operacional

1.2.3 Configure a rede da sua máquina virtual

Caso o modo *Bridged Adapter* não funcionar na sua intranet habilite o *Network Adapter* para *Internal Network*.
Pergunte ao seu professor o motivo desta configuração.
`http://even.archlinux-br.org/blog/virtualbox-configuracoes-de-rede`

1.2.4 Reconfigure a rede da sua máquina virtual

Modifique os seguintes arquivos:

Arquivo /etc/hosts:

```
127.0.0.1 localhost
10.0.0.80 server1.enois.org.br  server1

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

e

/etc/netplan/01-netcfg.yaml

Lembre-se que você está criando uma rede para um DNS de Intranet.

[2]RFC significa Request for Comments

1.2.5 Se em seu ambiente não for necessário "setar" os parâmetros acima. O que pode estar ocorrendo para a sua rede interna estar funcionando normalmente?

R:

1.2.6 Instale o DNS utilizando IP estático

Seu arquivo `/etc/netplan/01-netcfg.yaml` pode possuir a seguinte configuração:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp03s:
      dhcp4: no
      addresses:
       - 10.10.10.2/24
      routes:
        - to: default
          via: 10.10.10.1
      nameservers:
        search: [enois.org.br]
        addresses: [10.0.0.1, 10.0.0.254]
```

[frame=single]

As 3 últimas linhas mostram dois parâmetros importantes:

- `search: [enois.org.br]`
  Este parâmetro é conhecido como prefixo do DNS. Nada mais é do que o nome do domínio do seu *site* Qual a utilidade deste parâmetro? Este parâmetro complementa o primeiro nome acrescentando o nome do domínio configurado no DNS. Isto resulta no `F.Q.D.N` da máquina.
  Por exemplo:
  Caso você não tenha inserido o parâmetro `search` será necessário incluir todo o `F.Q.D.N` para que a máquina responda alguma solicitação da rede.
  Exemplo:

  ```
  ping zabumba.coltec.ufmg.br
  ```

- `addresses: [10.0.0.1, 10.0.0.81]`
  O parâmetro `nameservers` escreve no arquivo `/etc/resolv.conf` quais os servidores DNS que a sua máquina irá procurar. A ordem é importante, o primeiro IP vai apontar para o servidor de DNS primário, o segundo será o secundário e assim por diante.

  Após a inclusão do parâmetro no arquivo `etc/netplan/01-netcfg.yaml` teremos apenas que colocar o primeiro nome da máquina:
  Exemplo:

  ```
  ping zabumba
  ```

Parece bobagem, mas acaba sendo um detalhe que auxilia a produtividade do administrador da rede ;)

Lembre-se! O arquivo será parecido, mas não igual.

1.2.7 O arquivo /etc/resolv.conf

Ele indica quais servidores DNS sua máquina irá procurar. Atualmente ele é preenchido de forma automática e normalmente não deve ser editado manualmente.

Por que é importante fixar o IP do servidor de DNS?

R:

1.2.8 Configurando o DNS

Uma vez instalado o BIND9 configure-o para que ele se torne operacional em sua rede.

Os arquivos de configuração do BIND

O BIND possui diversos arquivos de configuração, como visto na aula teórica, mas na prática você perceberá que o arquivo `/etc/bind/named.conf` é um arquivo fundamento pois é ele que "chama" todos os outros arquivos por meio de entradas.
No *Ubuntu server* o arquivo `named.conf` "chama" o arquivo `named.conf.local` que por sua vez também chama mais 2 arquivos que respondem pela base de dados do seu DNS.
Como exemplo, neste tutorial criamos 2 arquivos *database*: `db.algumacoisa` e `db.algumacoisa.rev`
Há um outro importante arquivo denominado `db.root`. Este arquivo mantém informações sobre os servidores de DNS raiz da Internet (*DNS Root Servers*)

Como definir um domínio para o seu site?

Agora chegou o momento de definir um nome para o seu domínio. Por exemplo: `enois.org.br`
Utilizando-se do exemplo a seguir forçamos a configuração automática do arquivo `/etc/resolv.conf`:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp3s0:
      dhcp4: no
      addresses:
       - 10.10.10.2/24
      routes:
        - to: default
          via: 10.0.0.1
      nameservers:
          search: [enois.org.br]
          addresses: [10.0.0.1]
```

Qual a utilidade do arquivo **/etc/resolv.conf**?

R:

Por que não é necessário configurar o arquivo supracitado em uma instalação padrão de um Ubuntu Desktop?

R:

Crie o arquivo db.nomedealgumacoisa

Ex: `db.enois`

Exemplo do conteúdo e do formato:

```
@ IN  SOA server1.enois.org.br. humberto.honda.gmail.com. (
  2019071649 3H 15M 1W 1D )
  IN  A 10.0.0.80
  NS  server1.enois.org.br.

server1 A 10.0.0.80
coltec-h A  10.0.0.81
h-laptop A  10.0.0.82
```

Lembre-se! Este é um arquivo de configuração básico para qualquer servidor de DNS - BIND. **Respeite** a formatação do arquivo, o descumprimento desta norma acarretará no não funcionamento do DNS.

Questionamentos importantes sobre este arquivo de configuração:

- Qual o significado do `@`?
  R:
  Indica a origem do domínio e também o início do arquivo de configuração

- Qual o significado de `IN SOA`?
  R:
  O `"IN"` é abreviação de `IN`ternet e `S.O.A` é acrônimo de *Start Of Authority*. O S.O.A pode ser entendido como inicío domínio ou zona de nomes. O S.O.A sempre é gerenciado por uma máquina computacional que através de um *software* como o Bind irá responder pela resolução de nomes.
  Cada zona possui ao menos um servidor DNS ou servidor de nomes com autoridade (*Authoritative Name Server*).

- O que significa a diretiva `A` no arquivo de configuração db.enois?
  R:
  O `A` é a abreviação de *Address Mapping* é usado em entradas onde um domínio ou subdomínio é relacionado a um endereço. O `A` é um *Resource Record* ou simplesmente `RR`. Os outros tipos de `RR`s são:

  - S.O.A - indica o início da zona de autoridade
  - N.S - *Name Server* ou nome do servidor DNS
  - CNAME - *Canonical Name* trata-se de um apelido que pode ser atribuído a uma máquina do domínio
  - MX - este RR é oriundo de *Mail Exchange* ou servidor de *e-mail*
  - PTR - ponteiro que aponta para um outro nome. A utilidade deste RR é permitir a consulta pelo IP para assim retornar o nome da máquina.

- TXT - "COLTEC-UFMG"
- HINFO - Host Info.

Para criar um novo domínio é necessário a autorização do S.O.A do qual este novo domínio irá pertencer.
Um outro termo técnico muito utilizado é o domínio ou zona direta de consulta (*Forward Lookup Zone*).
Este termo indica um domínio onde as relações entre nome da máquina são armazenadas. Quando um computador consulta este este domínio com um nome o resultado será o IP da máquina consultada.
Há um domínio complementar a este conhecido como o domínio ou zona reversa de consulta (*Reverse Lookup Zone*). Ele é referido simplesmente como reverso.

1.2.9 Insira a localização deste arquivo em `/etc/bind/named.conf.local`

Este tipo de configuração é uma característica do Ubuntu, em outras distribuições é comum o administrador inserir a localização deste arquivo em `/etc/bind/named.conf`.
Veja como poderia ficar o seu arquivo `/etc/bind/named.conf.local`:

```
zone "enois.org.br" IN {
  type master;
  file "/etc/bind/db.enois";
};
```

Reinicie o DNS:

```
service bind9 restart
```

Vasculhe o arquivo /var/log/syslog

Este arquivo conhecido como `log` do sistema mostra o comportamento do *daemon* inicializado. Como você acaba de reiniciar o `bind9` é bastante provável que ele seja o último registro no `syslog`. Verifique o `syslog` com o seguinte comando:

```
tail /var/log/syslog
```

ou

```
vim /var/log/syslog
```

o resultado deve ser algo semelhante ao `log` abaixo:

```
root@ubuntu:/etc/bind# tail /var/log/syslog
Sep 12 15:48:24 ubuntu named[10121]: managed-keys-zone: journal file is
   out of date: removing journal file
Sep 12 15:48:24 ubuntu named[10121]: managed-keys-zone: loaded serial 2
Sep 12 15:48:24 ubuntu named[10121]: zone 0.in-addr.arpa/IN: loaded
   serial 1
```

```
Sep 12 15:48:24 ubuntu named[10121]: zone 127.in-addr.arpa/IN: loaded
   serial 1
Sep 12 15:48:24 ubuntu named[10121]: /etc/bind/db.enois:1: no TTL
   specified; using SOA MINTTL instead
Sep 12 15:48:24 ubuntu named[10121]: zone enois.org.br/IN: loaded serial
   2010071649
Sep 12 15:48:24 ubuntu named[10121]: zone localhost/IN: loaded serial 2
Sep 12 15:48:24 ubuntu named[10121]: zone 255.in-addr.arpa/IN: loaded
   serial 1
Sep 12 15:48:24 ubuntu named[10121]: all zones loaded
Sep 12 15:48:24 ubuntu named[10121]: running
```

Sempre incremente o serial do DNS ao realizar alguma mudança em sua configuração

1.2.10 Teste compulsivamente o seu DNS até acreditar que ele realmente funciona

Uma forma clássica de testar o DNS é utilizando o programa `dig`.[3] O `dig` é uma ferramenta de linha de comando que consulta informações sobre um servidor DNS. Quais informações?

- Endereços de máquinas
- Servidores de e-mail (MTA)
- Servidores de DNS

dig básico

Ao aplicar o seguinte comando:

```
dig enois.org.br @10.0.0.80
```

Deve-se obter algo como:

```
; <<>> DiG 9.6.1-P2 <<>> enois.org.br @10.0.0.80
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 281
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;enois.org.br.      IN  A

;; ANSWER SECTION:
enois.org.br.   86400 IN  A 10.0.0.80

;; AUTHORITY SECTION:
enois.org.br.   86400 IN  NS  server1.enois.org.br.

;; ADDITIONAL SECTION:
server1.enois.org.br. 86400 IN  A 10.0.0.80
```

[3] Há uma versão para Windows no site www.isc.org

```
;; Query time: 7 msec
;; SERVER: 10.0.0.80#53(10.0.0.80)
;; WHEN: Thu Apr 15 08:15:55 2010
;; MSG SIZE  rcvd: 84
```

1.2.11 Diversos exemplos básicos com o dig

Os exemplos abaixo ilustram o funcionamento do dig na prática:

1. Aplicando um dig completo teremos como saída:

```
$ dig uol.com.br
```

```
; <<>> DiG 9.8.1-P1 <<>> uol.com.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60553
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;uol.com.br.      IN  A

;; ANSWER SECTION:
uol.com.br.   300 IN  A 200.221.2.45
uol.com.br.   300 IN  A 200.147.67.142

;; AUTHORITY SECTION:
uol.com.br.   2082  IN  NS  charles.uol.com.br.
uol.com.br.   2082  IN  NS  borges.uol.com.br.
uol.com.br.   2082  IN  NS  eliot.uol.com.br.

;; ADDITIONAL SECTION:
eliot.uol.com.br. 3357  IN  A 200.221.11.98
borges.uol.com.br.  3357  IN  A 200.147.255.105
charles.uol.com.br. 3357  IN  A 200.147.38.8

;; Query time: 15 msec
;; SERVER: 150.164.102.68#53(150.164.102.68)
;; WHEN: Thu Sep 12 16:13:43 2013
;; MSG SIZE  rcvd: 171
```

A saída possui diversos blocos que são resumidamente explicados a seguir:

- **HEADER:** mostra a versão do `dig` utilizada.
- **QUESTION SECTION:** mostra o que foi perguntado pelo o `dig`

- **ANSWER SECTION:** mostra o que foi respondido para o `dig`
- **AUTHORITY SECTION:** mostra o(s) nome(s) do(s) servidore(s) DNS que possuem autoridade para responder a consulta realizada pelo `dig`
- **ADDITIONAL SECTION:** mostra o(s) IP(s) do(s) servidore(s) DNS da **AUTHORITY SECTION:**
- O final é conhecido como `Stats section` que mostra informações como tempo de consulta a partir da máquina utilizada pelo comando dig, o IP e a porta utilizada para realizar a consulta e também quantos pacotes foram gastos para obter a consulta.

2. Percebe-se que o `dig` retorna uma quantidade generosa de informações. Uma forma de resumir a resposta adquirida pelo dig seria aplicando semelhante comando:

```
$ dig uol.com.br +nocomments +noquestion +noauthority +noadditional +
   nostats
```

Resultado:

```
; <<>> DiG 9.8.1-P1 <<>> uol.com.br +nocomments +noquestion +
   noauthority +noadditional +nostats
;; global options: +cmd
uol.com.br.    300 IN  A 200.147.67.142
uol.com.br.    300 IN  A 200.221.2.45
```

3. O comando a seguir gera um resultado equivalente ao anterior

```
$ dig uol.com.br +noall +answer
```

4. Um comando mais enxuto pode ser escrito semelhante a este exemplo:

```
$ dig www.ufmg.br +short
150.164.250.1
```

ou

```
$ dig www.uol.com.br +short
200.147.67.142
200.221.2.45
```

5. Como através de uma parâmetro do DNS eu obtenho uma informação mais específica? Um exemplo disto é através do parâmetro `ns`:

```
$ dig www.coltec.ufmg.br ns +short
web.coltec.ufmg.br.
```

6. Como visualizar todos os parâmetros de um servidor de DNS com o dig?

```
$ dig vet.ufmg.br ANY +noall +answer

; <<>> DiG 9.8.1-P1 <<>> vet.ufmg.br ANY +noall +answer
;; global options: +cmd
vet.ufmg.br.    86400 IN  TXT "v=spf1 ip4:150.164.0.0/16 ~all"
vet.ufmg.br.    86400 IN  MX  10 mail2.grude.ufmg.br.
vet.ufmg.br.    86400 IN  MX  90 mav2.ufmg.br.
vet.ufmg.br.    86400 IN  MX  10 mail1.grude.ufmg.br.
vet.ufmg.br.    86400 IN  A 150.164.122.2
vet.ufmg.br.    86400 IN  NS  basalto.dcc.ufmg.br.
vet.ufmg.br.    86400 IN  NS  apoio.rede.ufmg.br.
vet.ufmg.br.    86400 IN  NS  indicus.vet.ufmg.br.
vet.ufmg.br.    86400 IN  NS  felix.lcc.ufmg.br.
vet.ufmg.br.    86400 IN  SOA indicus.vet.ufmg.br. root.vet.ufmg.br.
   2950932917 7200 3600 2592000 86400
```

1.3 Configurando clientes DNS

Configure clientes Windows e Linux para testar o servidor de DNS. Utilize ping com o nome *hostname* ou o FQDN.
Ex:

```
ping server1
```

ou

```
ping server1.enois.org.br
```

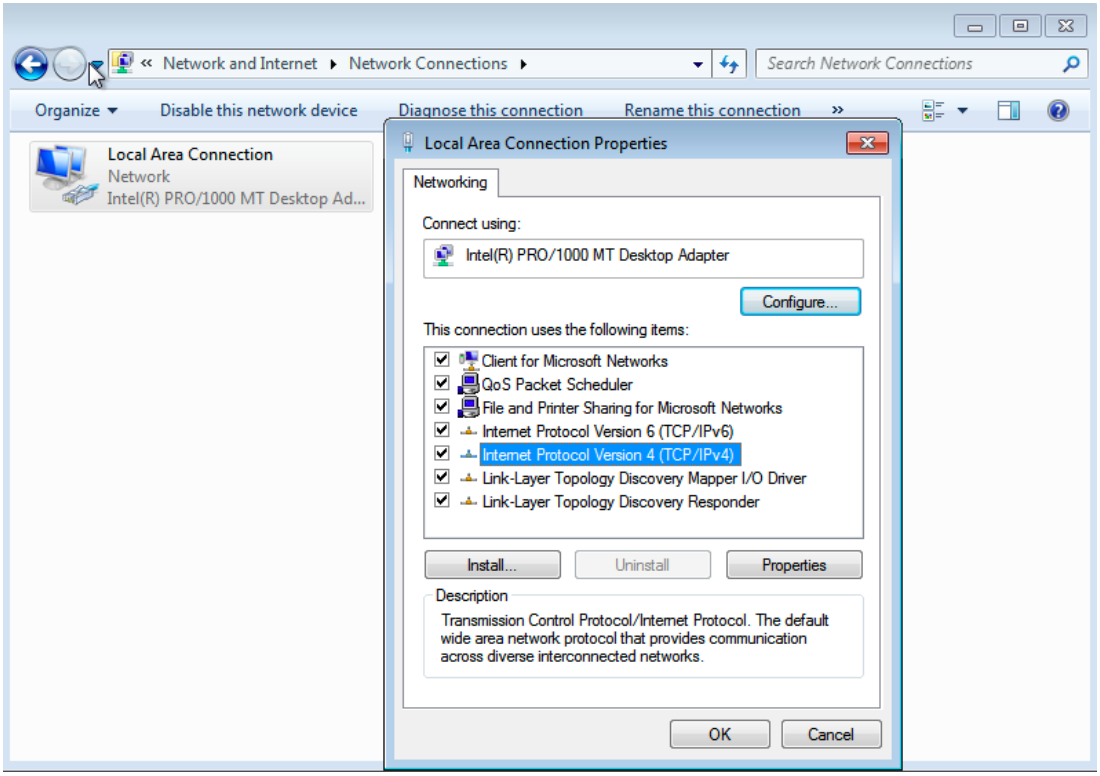
1.3.1 Configurando um cliente Linux

Utilize os conhecimentos adquiridos no capítulo 3.

1.3.2 Configurando um cliente Windows

Passo 1 -

Vá em propridades de rede e escolha a opção mostrada na figura a seguir:

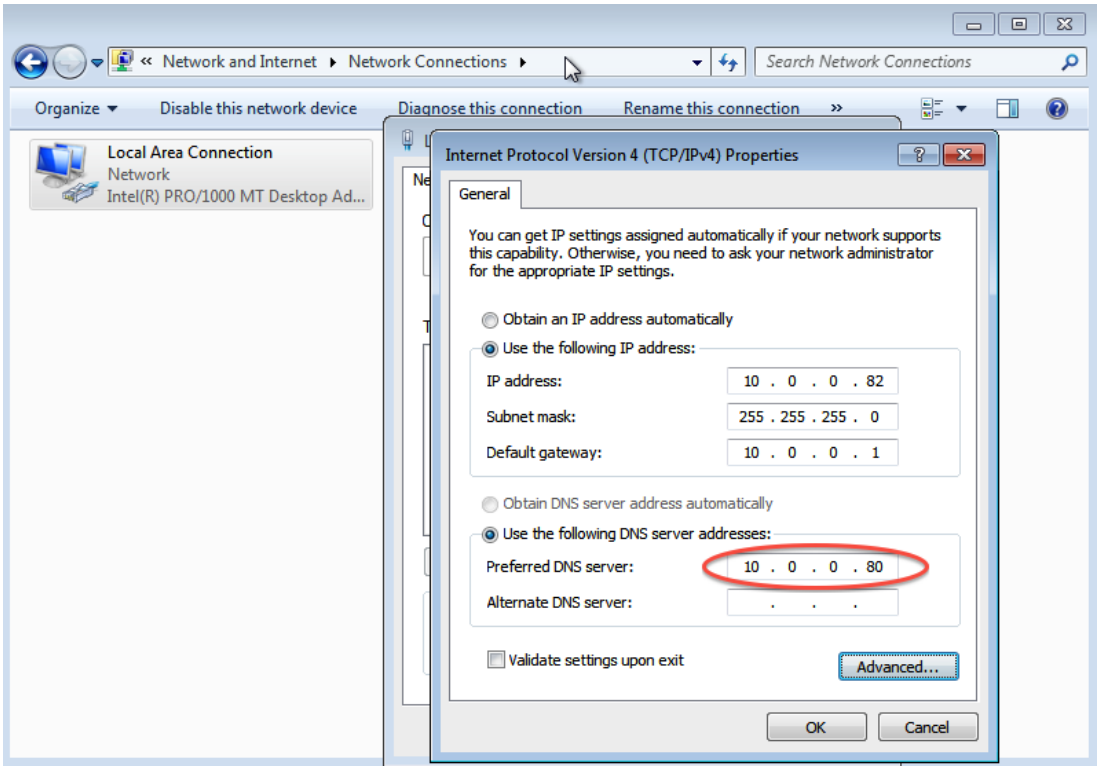


Passo 2 -

Modifique as 4 parâmetros de rede conforme a próxima figura:

Passo 3 -

Clique no botão Avançado para inserir o sufixo do seu domínio:



Passo 4 -

Insira agora o sufixo do F.Q.D.N ou domínio da sua rede:

1.3.3 Teste a partir do servidor de DNS

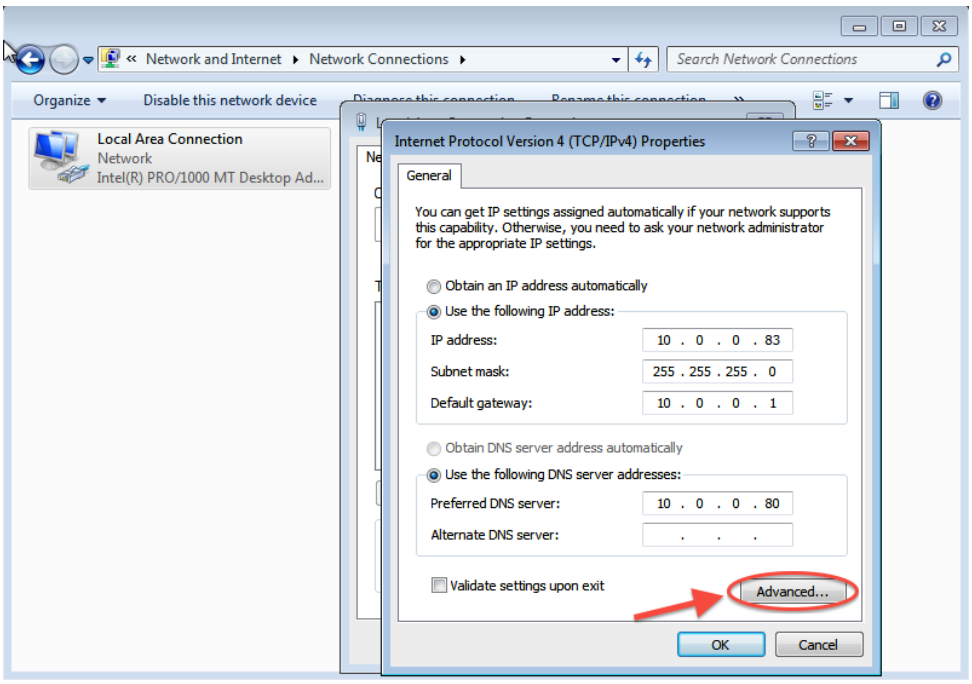
"pingue" os clientes a partir do servidor DNS

1.4 Inserindo um *alias*

O que é um *alias*?
O *alias* é um apelido que você pode atribuir a qualquer máquina de seu domínio. O registro utilizado para atribuir um apelido é o `CNAME`.
Para entender a utilização do *alias* adapte o exemplo a seguir em seu arquivo de configuração:
Adicione no arquivo de configuração do DNS um *alias*. Seu arquivo ficará semelhante ao exemplificado a seguir:

```
@ IN  SOA server1.enois.org.br. humberto.honda.gmail.com. (
  2010071649 3H 15M 1W 1D )
  IN  A 10.0.0.80
  NS  server1.enois.org.br.

server1 A 10.0.0.80
coltec-h A  10.0.0.81
h-laptop A  10.0.0.82
ze IN CNAME coltec-h
```



Teste pingando a máquina ze a partir de seu servidor

Ex:

```
ping ze
```

1.5 Configurando o DNS reverso

O DNS reverso ou *Reverse Lookup Zone* também é conhecido como RDNS (*Reverse DNS*). Sua principal utilidade consiste em garantir que uma máquina com IP real seja mais confiável por estar cadastrado em um servidor DNS autêntico. Isto tem um peso maior em servidores de *e-mail*, também denominado M.T.A (*Mail Transport Agent*).
O erro abaixo ilustra a necessidade de se utilizar o DNS reverso:

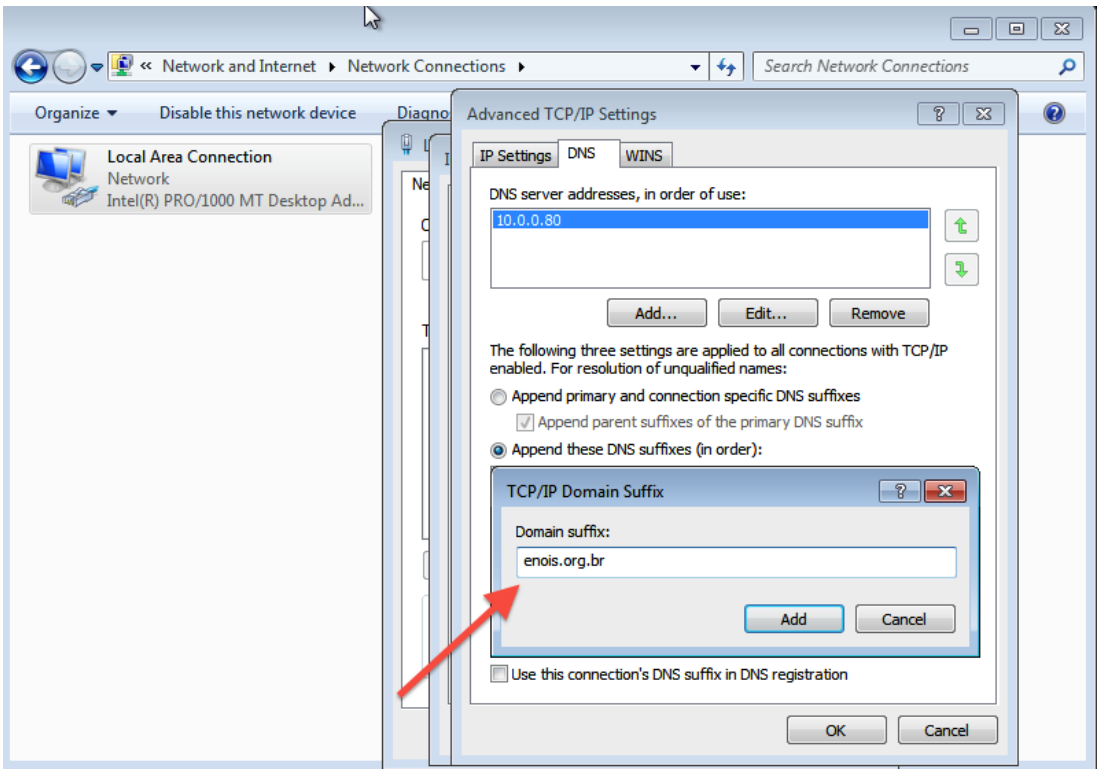
```
"Your message addressed to the target domain (*******.com.br)
could not be delivered because the mail server responsible for
this domain returned a permanent error.

The server returned:

550 rejected because RDNS"
```

O M.T.A não enviou a mensagem pois ela foi gerada de uma máquina sem entrada no DNS reverso. Podemos entender o RDNS como uma forma de filtrar *spam*.
Até aqui podemos resumir que o servidor de DNS, objeto de nosso estudo, gera dois domínios de atuação:

- O primeiro já conhecido e fácil de entender é o domínio direto ou DNS direto (*Forward Lookup Zone* ou *Forward DNS resolution*). Aqui ocorre a tradução do F.Q.D.N para um IP.
- O segundo é o domínio ou grupo reverso onde através de um IP chega-se ao F.Q.D.N. Há uma base de dados somente para o domínio reverso que possui também servidores raízes, cujo



domínio é conhecido como `ARPA` (*Address and Routing Parameters Area*). No caso do IPV4 o domínio raiz é conhecido como `in-addr.arpa` e no IPV6 é o `ipv6.arpa`. O processo reverso de resolução de IP para um F.Q.D.N usa um registro no arquivo de configuração do reverso conhecido como `PTR` de *pointer DNS*.

É possível testar o reverso de um IP real através do seguinte sítio:

```
http://remote.12dt.com
```

1.5.1 Quais seriam outras utilidades do DNS reverso? Em nossa intranet é necessário a utilização do reverso? Justifique.

1.5.2 Para criar um DNS reverso abra um novo arquivo. Ex: `db.enois.rev`

O formato será semelhante ao descrito abaixo:

```
@ IN  SOA server1.enois.org.br. humberto.honda.gmail.com. (
  2010061647 3H 15M 1W 1D )
  NS  server1.enois.org.br.

80  PTR server1.enois.org.br.
81  PTR coltec-h.enois.org.br.
82  PTR h-laptop.enois.org.br.
```

1.5.3 Insira esta nova entrada no `named.conf.local`

Ex:

```
zone "0.0.10.in-addr.arpa" IN {
  type master;
  file "/etc/bind/db.enois.rev";
};
```

1.5.4 Teste o reverso com o `dig`

Ex:

```
dig enois.org.br
```

ou

```
dig -x 10.0.0.80
```

Saída:

```
;; QUESTION SECTION:
;80.0.0.10.in-addr.arpa.    IN  PTR

;; AUTHORITY SECTION:
80.0.0.10.in-addr.arpa. 86400 IN SOA  server1.enois.org.br. humberto.
   gmail.com.
 2010061647 10800 900 604800 86400

;; Query time: 1 msec
;; SERVER: 10.0.0.80#53(10.0.0.80)
;; WHEN: Thu Apr  8 08:16:39 2010
;; MSG SIZE  rcvd: 120
```

1.5.5 Teste o reverso no Windows

Abra uma janela de comando e teste com exemplos semelhantes:

```
nslookup enois.org.br
```

ou

```
nslookup 10.0.0.80
```

1.5.6 Um erro sutil na configuração do reverso

Muitas vezes pode-se inserir o seguinte erro na configuração do reverso como no exemplo a seguir:

```
zone "0.0.0.10.in-addr.arpa" IN {
  type master;
  file "/etc/bind/db.enois.rev";
};
```

Este tipo de erro gera uma lentidão no acesso às máquinas. Compare a velocidade de resposta do `ping` na configuração certa e na errada e sinta a diferença.
Onde está o erro?

1.6 Configurando um DNS secundário

1.6.1 DNS secundário em uma outra máquina

Esta configuração utiliza dois servidores, configurados como *master* e *slave*. A idéia é que o *slave*, ou DNS secundário, realize a redundância da máquina *master* (DNS primário).
Siga os seguintes passos para instalar e configurar o secundário:

passo 1: Instale o DNS secundário em uma outra máquina clonando o seu servidor DNS principal e altere os seguintes arquivos de configuração: `/etc/hostname`, `/etc/hosts`, `/etc/netplan/01-netcfg.yaml`

O nome dado ao DNS *slave* nos exemplos a seguir será: `secundario` e o IP será `10.0.0.79`

passo 2: Desligue a máquina ou o serviço de DNS

passo 3: Ligue novamente a máquina secundária e repare que ela já assumiu as novas configurações do passo anterior

passo 4: Reinicie a máquina e em seguida teste a rede da mesma

passo 5: Remova o `bind9` com `apt remove --purge bind9`

Por que é melhor remover completamente a instalação antiga do bind9?

passo 6: Instale novamente o `bind9` com `apt install bind9`

passo 7: Altere a rede da máquina virtual para *Internal Network*

passo 8: Configure o DNS primário

Faça as seguintes modificações no DNS primário:
Modifique o arquivo `/etc/bind/named.conf.local` inserindo a linha `"allow transfer"` nas entradas para as zonas direta e reversa
Esta configuração indica que o servidor primário (*master*) "aponta"para o servidor secundário. Permitindo desta assim a transferência dos arquivos de *database* ("db") para o servidor secundário.
Veja o exemplo a seguir:

```
zone "enois.org.br" IN {
  type master;
  file "/etc/bind/db.enois";
  allow-transfer { 10.0.0.79; };
};

zone "0.0.10.in-addr.arpa" IN {
```

```
  type master;
  file "/etc/bind/db.enois.rev";
  allow-transfer { 10.0.0.79; };
};
```

passo 9: Configure o DNS secundário

Na configuração do DNS secundário indique que você é um tipo secundário (`type` *slave*) e qual o I.P do servidor primário para realizar o sincronismo de *database* do direto e do reverso.
Isto será configurado no arquivo `named.conf.local`
Ex:

```
zone "enois.org.br" IN {
  type slave;
  file "/var/cache/bind/db.enois";
  masters { 10.0.0.80; };
};

zone "0.0.10.in-addr.arpa" IN {
  type slave;
  file "/var/cache/bind/db.enois.rev";
  masters { 10.0.0.80; };
};
```

Repare que o bind gravará o sincronismo na pasta `/var/cache/bind/` Isto é uma característica do Ubuntu, em outras distribuições é possível configurar a gravação na própria pasta `/etc/bind`.
Por exemplo:
Gravação em `/etc/bind/slave`
O Ubuntu faz isto por questões de segurança.

passo 11: Faça o mesmo para entrada do reverso em named.conf.local

passo 12: Teste!

Desligue o servidor e veja se os clientes conseguem "conversar" via `ping` apenas com os nomes das máquinas

1.6.2 Configurando um DNS secundário na mesma máquina

1.7 Configurando um DNS para Intranet com DHCP

1.8 Exercícios

1. Por que o DNS é um banco de dados distribuído e hierárquico?
2. Qual a utilidade de empresas que alugam domínios do tipo GoDaddy ou LocaWeb?
3. Um coltecano elaborou um produto concorrente do Facebook. Qual seria o procedimento técnico para colocar seu produto na Web? Considere apenas o domínio, o storage e um banco de dados genérico.
4. Com o estabelecimento do IPV6 o DNS sofreu alguma alteração no contexto do bind? Justifique.
5. Qual a utilidade do DNS reverso? Exemplifique.

6. Qual o significado de 2019060549?

7. Qual o significado de 3H 15M 1W 1D? R:
   Estes 4 parâmetros orientam o sincronismo do DNS secundário em relação ao primário:

   O primeiro parâmetro (`3H`): Indica o tempo que o servidor aguarda entre as atualizações automáticas. A cada 3 horas ele atualiza o secundário.

   O segundo parâmetro (`15M`): Caso o secundário perceba que o primário caiu ele tenta realizar a transfrência de zona (operação onde o secundário assume o domínio). Se esta transferência de zona falhar o secundário irá esperar mais 15 minutos e tentar transferência de zona novamente. A prática mostra que a transferência de domínio para o secundário demora de um a dois dias.

   O terceiro parâmetro (`1W`): Indica por quanto tempo o secundário irá responder pelo domínio (zona). Neste exemplo o tempo é uma semana (1 week). Tempo mais do que o suficiente para o administrador reparar o servidor primário.

   O quarto parâmetro (`1D`): Indica quanto tempo o o secundário demora para devolver o S.O.A para o primário. Neste exemplo este tempo é igual a 24 horas.

8. Em qual situação ocorre a transferência de zona? Exemplifique.
   R:
   As transferências de zona são sempre iniciadas pelo servidor DNS secundário. O servidor DNS primário simplesmente responde a solicitação de uma transferência de zona. Uma transferência de zona ocorrerá em qualquer um dos seguintes cenários:

   - Ao iniciar o serviço DNS no servidor DNS secundário.
   - Quando expira o tempo de atualização.
   - Quando alterações são salvas no arquivo de zona primária (ex: `db.enois`) e o serial é incrementado

9. Simule uma transferência de zona utilizando parâmetros de sincronismo compatíveis com o tempo da aula de lab de OCS.

10. O que é uma transferência de zona incremental?

11. Qual a diferença entre zona e domínio?

12. Qual a utilidade do sufixo DNS?

13. Como configurar o sufixo DNS no Linux?

14. Como configurar o sufixo DNS no Windows?

15. Quando pode ocorrer o DNS *poisoning*?

16. Como especificar endereços IPV6 no named.conf?

17. Quais seriam outras alternativas de servidores DNS? Cite pelo menos 5 exemplos.

18. Dada uma certa configuração o comando *ping* a partir do DNS secundário para seus clientes tem uma resposta lenta. Como resolver este pequeno problema?

19. Por que o DNS reconhecidamente realiza uma consulta recursiva?

20. Escreva um *script* em *bash* para listar as máquinas de um domínio no qual você é o administrador.

21. Escreva um *script* em *bash* para inserir e deletar máquinas em um domínio. As entradas deste *script* serão o nome da máquina e último octeto (*host*) do IP. O domínio/IP pode ser alterado no próprio *script*. Somente o administrador poderá executar deste *script*.