

Apendice I - DNS

1ª Etapa - Inicialmente, iremos compreender o conceito de resolução a partir do arquivo `/etc/hosts` de nomes e a utilização dos comandos de clientes para consulta em uma base DNS.

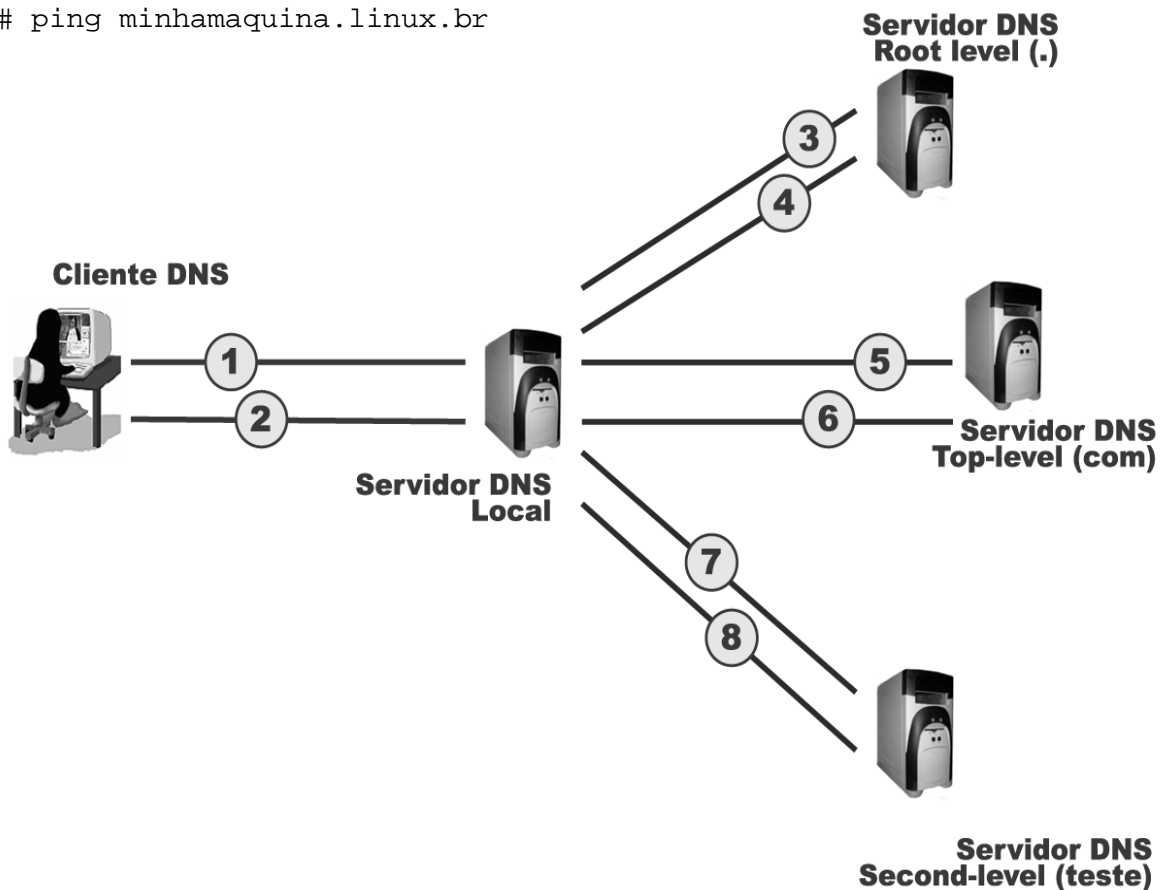
1- Vamos considerar que o host 192.168.0.161 responda pelo servidor FTP da rede local e não está sendo utilizado um DNS interno para fazer a resolução dos nomes das aplicações da minha intranet. Como posso resolver o nome do Servidor FTP da intranet nas minhas estações de trabalho Linux?

R: Insira a seguinte linha no arquivo `/etc/hosts` das estações:

```
127.0.0.1 localhost
192.168.0.161 minhaquina.linux.br minhaquina
```

2- Teste a resolução de nomes.

```
# ping minhaquina.linux.br
```



DNS (Domain Name System)

A função básica do DNS é resolver nomes de hosts para endereços ips e vice-versa. No nosso caso, vamos utilizar o bind (Berkeley Internet Name Domain), que inclui o servidor DNS conhecido como named. O cliente DNS é conhecido como resolver, quando um computador precisa saber a qual endereço ip um nome se refere, solicita a resolução de nomes ao servidor DNS.

Considerando o exemplo acima, o cliente DNS faz uma requisição para resolução do endereço "www.teste.com". Por sua vez o servidor DNS fará uma consulta ao servidor DNS responsável pelo domínio "teste.com", para saber o ip do host "www" (antes porém é feita uma solicitação ao servidor responsável pelo domínio ".com"). Feito isso, o servidor DNS do domínio "teste.com" busca em seu cadastro o ip do host de nome "www" e retorna ao servidor DNS do domínio de onde surgiu a requisição de resolução, que repassa o endereço ao cliente.

1- Configure o /etc/resolv.conf e ative o nslookup.

```
# nslookup <ENTER>
```

Você deverá obter como resultado um prompt com o sinal de > (maior), onde poderá realizar as seguintes pesquisas:

Consultar o do nameserver:

```
>set type=ns  
>set all  
>4linux.com.br
```

2- Consultando quem é o mail exchanger ou servidor de correio atual:

```
>set type=mx  
>set all  
>4linux.com.br
```

3- Para consultarmos somente informações sobre nomes canônicos em seu DNS, use:

```
> set q=cname <enter>  
>4linux.com.br <enter>
```

4- Ativando nslookup e verificando os valores de suas definições:

```
>nslookup <enter>  
> set all <enter>
```

5- Consultando informações de um domínio:

```
> set type=any <enter>
> 4linux.com.br <enter>
```

6- Exemplo de consulta reversa:

```
> server 4linux.com.br
> set type=ptr
> 200.170.203.70
```

7- Consultando o registro Mail Exchange:

```
> seq=mx
> 4linux.com.br
```

8- Consulta genérica de registros:

```
> set q=any
> 4linux.com.br
```

9- Consultando a autoridade do domínio:

```
> set q=soa
> 4linux.com.br
```

10- Elaborando um consulta não recursiva:

```
> set norec
> set all
> disney.com
```

11- Desabilitando o modo de busca:

```
> set nosearch
> set all
> nasa.org
```

12- Utilizando o nslookup, consulte o DNS e verifique qual ou quais IP's estão vinculados ao endereço "www.google.com"

13- Ative o modo debug.

14- Verifique se o modo debug foi ativado.

15- Consulte novamente as informações vinculadas ao endereço do "www.google.com".

- 16- Desative o modo debug (no domínio www.google.com).
- 17- Altere o valor da variável “querytype” para mx (no domínio www.google.com).
- 18- Verifique se o valor “querytype” foi alterado.
- 19- Consulte qual ou quais são os servidores de SMTP do domínio yahoo.com.
- 20- Altere o valor da variável “querytype” para PTR (no domínio www.yahoo.com).
- 21- Verifique se o valor “querytype” foi alterado.
- 22- Faça uma consulta reversa (no domínio www.yahoo.com).
- 23- Altere o valor da variável “querytype” para NS para o servidor do domínio yahoo.com.
- 24- Verifique se o valor “querytype” foi alterado.
- 25- Descubra quem são os servidores DNS do domínio da uol.com.br.
- 26- Descubra quem são os servidores DNS do domínio linux.org.
- 27- Saia do nslookup.
- 28- Usando o comando Host, execute um consulta ao DNS.
: host -t any uol.com.br
- 29- Consulte quem é o smtp do domínio terra.com.br.
R: host -t mx uol.com.br

30- Consulte de forma reversa o ip 200.221.2.49.

```
R: host -t ptr 200.221.2.29
```

31- Faça a consulta anterior no modo Verbose.

```
R: host -v -t ptr 200.221.2.29
```

32- Consultando a autoridade do domínio.

```
R: host -v -t soa uol.com.br
```

```
R: host -v -t soa google.com
```

33- Usando o comando dig identifique quem é o Servidor DNS.

```
R: dig -t any uol.com.br
```

34- Consulte quem é o smtp do domínio terra.com.br.

```
R: dig -t mx uol.com.br
```

35- Consulte de forma reversa os IP's:

```
R: dig -x 200.221.2.29
```

```
R: dig -x 200.170.203.70
```

36- Consultando a autoridade dos domínios:

```
R: dig -t soa uol.com.br
```

```
R: dig -t soa google.com
```

```
R: dig -t soa 4linux.com.br
```

```
R: dig -t soa linux.org
```

37- O número de servidores DNS Root Names Server é 13, para identificar seus endereços iremos utilizar o nslookup:

```
# nslookup
> set type=ns
> set all
> .
```

2ª Etapa - Inicialmente, compreenderemos o conceito de resolução a partir do arquivo /etc/hosts de nomes e a utilização dos comandos de clientes para consulta em uma base DNS.

Configuração do servidor DNS passo a passo:

Estrutura de Arquivos inicial sugerida para nosso projeto de DNS primário

```
/etc/named.conf

/var/named

    named.ca
    localhost
    primary/
    zone/
    dominio.conf
    db.dominio
    rev.dominio
```

Pacotes necessários:

bind -> servidor DNS

caching-nameserver -> arquivos de configuração

1- Primeiramente, vamos editar o arquivo `/etc/named.conf` -> Apontamento das zonas do DNS

```
Options {
    directory "/var/named";
};

zone "." {
    type hint;
    file "named.ca";
};

zone "0.0.127.in-addr.arpa"
{
    type master;
    file "zone/named.local";
};

include "primary/morpheio.conf";
```

2- Vimos no arquivo `/etc/named.conf` que todo o nosso DNS será estruturado abaixo do diretório `/var/named`. Vá para esse diretório e liste o seu conteúdo.

```
R: cd /var/named
    ls
```

3- O diretório `/var/named` deve conter o seguinte conteúdo:

```
R: dump localhost.zone named.ca named.local
```

Edite os seguintes arquivos:

`named.ca` -> armazena os endereços ip dos root level domains

`named.local` -> é utilizado como base para a construção dos arquivos db e rev

4- No final do arquivo /etc/named.conf utilizamos o comando include para apontar que o arquivo que armazenará as informações do domínio do DNS é o /var/named/primary/morpheio.conf. Então, vamos editá-lo:

```
Zone "morpheio.xxx.br" {
    type master;
    file "zone/db.morpheio";
};
```

R: vi /var/named/primary/morpheio.conf -> este arquivo irá apontar também a localização dos arquivos db e rev

5- Agora, iremos editar o arquivo db.morpheio, que de acordo com o arquivo /var/named/primary/morpheio.conf, está localizado no /var/named/zone

R: vi /var/named/zone/db.morpheio -> resolve nomes para ips

```
@      IN          SOA ns.morpheio.xxx.br.  root.morpheio.xxx.br.
(
        1997022700 ; serial
        28800 ; refresh
        14400 ; retry
        3600000 ; expire
        86400 ; default_ttl )
@      IN          NS ns.morpheio.xxx.br.
morpheio.xxx.br.  IN          A          192.168.1.2
ns      IN          A          192.168.1.2
www     IN          CNAME morpheio.xxx.br.
ftp     IN          CNAME morpheio.xxx.br.
pop     IN          A          192.168.1.2
mail    IN          CNAME morpheio.xxx.br.
@      IN          MX 10 mail.morpheio.xxx.br
```

6- Edite o arquivo /var/named/zone/rev.morpheio

R: vi /var/named/zone/rev.morpheio -> resolve ips para nomes

```
@ IN SOA ns.morpheio.xxx.br. root.morpheio.xxx.br.
(
    1997022700 ; serial
    28800 ; refresh
    14400 ; retry
    3600000 ; expire
    86400 ; default_ttl
)

@ IN NS ns.morpheio.xxx.br.
@ IN PTR mail.morpheio.xxx.br.
2.1.168.192.in-addr.arpa. IN PTR www.morpheio.xxx.br.
```

7- Agora vamos configurar o arquivo do cliente DNS, o /etc/resolv.conf

R: vi /etc/resolv.conf

8- Isto posto, vamos subir o daemon do servidor DNS.

```
R: # /etc/init.d/ bind stop
    # /etc/init.d/ bind start
```

9- Por fim, dê uma olhada nos logs do sistema e verifique se o serviço subiu corretamente.

R: tail -f /var/log/messages

10 - Verifique os processos ativos inerentes ao Bind.

```
# ps aux | more
```

11 - Verifique as portas e os respectivos serviços que estão rodando na porta.

```
# nstat -an | more
# fuser -v porta/protocolo
```

12 - Configure o cliente para consultar pelo seu servidor DNS.

```
# vi /etc/ resolução
```

13- Execute os respectivos testes:

- a) ping -R ns.morpheio.xxx.br
- b) ping www.morpheio.xxx.br
- c) ping mail.morpheio.xxx.br
- d) ping pop.morpheio.xxx.br
- e) ping ftp.morpheio.xxx.br

14- Consulte com o comando Host:

- a) host -t any morpheio.xxx.br
- b) host -t mx morpheio.xxx.br
- c) host -l -v -t any morpheio.xxx.br

15 - Consulte com o comando dig:

- a) dig -t any morpheio.xxx.br
- b) dig-t mx morpeio.xxx.br

Configuração do servidor DNS secundário

Para configuração do servidor DNS secundário temos que instalar os pacotes bind e caching-nameserver no servidor, em seguida, editar o arquivo `/etc/named.conf` e colocar o seguinte conteúdo:

```
#echo "include secondary/morpheio.sec" >> /etc/named.conf
# mkdir /var/named/secondary
# mkdir /var/named/zonesec
```

```
/etc/named.conf
/var/named
    named.ca
    localhost
    primary/
        dominio.conf
    secondary/
        dominio.sec
    zone/
        db.dominio
        rev.dominio
    zonesec/
        dbsec.dominio
```

Conteúdo do arquivo morpheio.sec

```
Zone "morpheio.xyz.br " {

    type slave ;

    file "zonesec/dbsec.morpheio";
    masters {
        192.168.0.171;
    };
};
```

Para uma melhor compreensão, considere o servidor primário morpheio.xyz.br. Assim sendo, devemos inserir a política de transferência de zonas no /etc/named.conf do servidor primário do domínio morpheio.xyz.br.

```
options {
    directory "/var/named";
    allow-transfer { 192.168.1.2; };
};
```

Definindo a política de zona dentro da configuração do domínio morpheio.xyz.br, considerando como servidor primário o servidor 192.168.1.2

```
Zone "171.0.168.192.in-addr.arpa" {
    type master;

    allow-transfer { 192.168.1.2; };

    file "zone/rev.morpheio";
};
```

Considerando como servidor primário o servidor 192.168.1.2, vamos editar seu conteúdo do arquivo morpheio.sec.

```
Zone "morpheio.xyz.br " {
    type slave ;

    file "zonesec/dbsec.morpheio";
    allow-transfer { none; };
    masters {
        192.168.0.171;
    };
};
```

Uma dica interessante é o uso da diretiva “version” com um valor falso para não possibilitar a identificação da versão de servidor utilizada. Com essa informação, nossa seção “options” ficaria assim:

```
options {  
    directory "/var/named";  
    allow-transfer { 192.168.1.2; };  
    version "Saifora"  
};
```

APENDICE II - Apache

CAPÍTULO 5

Neste segundo momento, nossos objetivos serão instalar os pacotes necessários.

1- Verifique os pacotes necessários:

Debian:

```
# dpkg -l | grep apache
```

Redhat:

```
# rpm -qa | grep apache  
# rpm -qa | grep php  
# rpm -qa | grep mod_ssl
```

Usando o apt:

```
# apt-get install apache  
# apt-get install apache-ssl
```

2- Configurações Clássicas:

Entre no arquivo de configuração do servidor apache:

```
# vi /etc/apache/httpd.conf
```

a) Verifique a porta que será inicializado:

```
Port 80
```

b) Confira o usuário e o grupo do apache. Deve ser um usuário comum, como nobody, para em caso de vulnerabilidades o impacto e comprometimento do sistema sejam menores.

```
User nobody  
Group nobody
```

c) Constate se o Apache será inicializado em modo Standalone:

```
ServerType standalone
```

d) Verifique o diretório padrão de configuração do Apache, que novamente deve ser:

```
ServerRoot /etc/httpd
```

e) Verifique o valor mínimo de servidores, defina-o para 3:

```
MinSpareServers 3
```

f) Confira o valor máximo de servidores ativos, defina-o para 6:

```
MaxSpareServers 6
```

g) Defina que inicialmente serão inicializados 2 servidores:

```
StartServers 2
```

h) Defina o número máximo de conexões de clientes para 180:

```
MaxClients 180
```

3- Inicialize o Apache:

R:

4- Verifique os processos do apache que foram inicializados.

```
# ps aux | grep apache
```

5- Confira as portas que foram abertas para o servidor web.

```
# netstat -nl | more
```

6- Verifique quais processos estão vinculados às portas identificadas.

R:

3ª Etapa - Configurar o suporte a PHP e fazer a integração do Apache com o servidor DNS.

7- Instalando o suporte a php4:

```
# apt-get install php4
```

8- Configurando Domínio Virtual:

```
# Hosts Virtuais
NameVirtualHost www.morpheio.xxx.br
<VirtualHost www.morpheio.xxx.br
    DocumentRoot /var/www/morpheio
    ServerName morpheio.xxx.br
    ServerAdmin webmaster@morpheio.xx.br
</VirtualHost>
```

APENDICE III – Servidor DHCP

Nota: Estudaremos um serviço muito utilizado em redes de TCP/IP. Nosso foco será o DHCP.

O arquivo de configuração é o dhcpd.conf. Abaixo, um exemplo:

```
ddns-update-style interim;
ignore client-updates;

subnet 192.168.200.0 netmask 255.255.255.0 {

    option routers          192.168.200.2;
    option subnet-mask     255.255.255.0;
    option domain-name     "intranet.morpheio.xxx.br";
    option domain-name-servers 192.168.200.254,200.170.203.70;
    option time-offset     -10800;

    range dynamic-bootp 192.168.200.1 192.168.200.200;
    default-lease-time 21600;
    max-lease-time 43200;
}
```

Principais diretrizes do arquivo de configuração

default-lease-time 600 - Servidores DHCP cedem endereços sob pedido por um tempo pré-determinado. O padrão nesse exemplo é ceder o endereço IP por 600 segundos, ou 10 minutos.

max-lease-time 7200 - Caso o cliente solicite um tempo maior, o tempo máximo permitido será de 7.200 segundos (2 horas).

option subnet-mask 255.255.255.0 - Essa opção define a máscara de subrede a ser fornecida aos clientes.

option broadcast-address 255.255.255.255 - Essa opção define o endereço de envio para requisições de broadcast.

option routers 192.168.200.2 - O cliente, além do número IP, recebe também a informação do número do host que é o gateway de sua rede.

option domain-name-servers 192.168.200.254, 200.170.203.70 - Essa opção lista os servidores de nomes (DNS) a serem utilizados para resolução de nomes.

`option domain-name "intranet.morpheio.xxx.br"` - O servidor de domínio do cliente.

É possível fixar o IP via DHCP para máquinas respectivas. Para isso, precisamos associar o MAC ADDRESS da placa com um IP.

Considere que:

Máquina	MAC ADDRESS	IP FIXADO
Micro 1	00:80:C7:D2:F8:D5	192.168.200.210
Micro 1	88:3D:BE:00:C7:00	192.168.200.214

Para esse cenário ser possível, seria necessária a respectiva entrada no arquivo de configuração `/etc/dhcpd.conf`:

```
host micro1 {
    hardware ethernet 00:80:C7:D2:F8:D5;
    fixed-address 192.168.200.210
}

host micro2 {
    hardware ethernet 88:3D:BE:00:C7:00;
    fixed-address 192.168.200.214;
}
```

O Arquivo `/etc/dhcpd.conf` ficaria assim:

```
ddns-update-style interim;
ignore client-updates;

subnet 192.168.200.0 netmask 255.255.255.0 {
    option routers      192.168.200.2;
    option subnet-mack  255.255.255.0
    option domain-name  "intranet.morpheio.xxx.br";
    option domain-servers
192.168.200.254,
    option domain-offset -10800;

    range dynamic-bootp 192.168.200.1 192.168.200.200;
    default-lease-time 21600;
    max-lease-time 43200;
    host micro {
        hardware ethernet 00:80:C7:D2:F8:D5;
        fixed-address 192.168.200.210
    }
    host micro2 {
        hardware ethernet 88:3D:BE:00:C7:00;
        fixed-address 192.168.200.214;
    }
}
```

APENDICE IV – Servidor Samba

O Samba é um aplicativo que disponibiliza seus compartilhamentos em um servidor para seus clientes e permite que, através do protocolo SMB, diversas máquinas se comuniquem, até mesmo equipamentos operando em diferentes plataformas.

A maior utilização do Samba se dá na integração Linux/Windows, onde diversas empresas e universidades possuem servidores Linux rodando Samba como servidor de arquivos, impressão e até para disponibilizar logon para seus clientes.

Devido a sua estabilidade com o Windows, o Samba permite que servidores Linux atuem como se fossem verdadeiros servidores Windows NT.

O Samba é um servidor de compartilhamento de arquivos e/ou impressoras, e, para isso, usa o protocolo SMB (Server Message Block), que também é o protocolo padrão para compartilhamento em redes Microsoft. Por esse motivo, ele é muito utilizado para interoperabilidade entre redes Linux e Microsoft.

1 - Instalando os pacotes necessários para o serviço do Samba:

```
# apt-get install samba smbclient smbfs
```

Ele instalará os seguintes pacotes:

```
samba - servidor Samba  
samba-common - arquivos de configuração do Samba  
smbclient - cliente Samba para Linux  
smbfs - montagem de compartilhamentos através do Linux
```

2 - Vamos agora acessar o arquivo de configuração do Samba:

```
# vi /etc/samba/smb.conf
```

Visualizando algumas linhas específicas:

```
[global] -> aqui se inicia a seção de configuração do servidor Samba
```

a) Linha onde é definido em qual grupo de trabalho ou domínio da rede Microsoft ele estará contido:

```
workgroup = MATRIX
```

b) O nome que irá aparecer na descrição do Ambiente de Rede é:

```
server string = Samba Server
```

c) Arquivo onde localizam-se as impressoras configuradas no meu sistema:

```
printcap name = /etc/printcap
```

d) Especifica que as impressoras listadas em /etc/printcap deverão aparecer como disponíveis no compartilhamento:

```
load printers = yes
```

e) Aqui eu defino o valor padrão utilizado para impressão (o mais utilizado é o valor “cups”):

```
printing = lprng
```

f) Conta do usuário convidado (DETALHE: o ponto-e-vírgula indica que a opção está COMENTADA, não sendo interessante habilitá-la):

```
; guest account = pcguest
```

g) Arquivo de log gerado pelo Samba (o valor “%m” indica que o nome do arquivo terá o nome NetBIOS do host de acesso):

```
log file = /var/log/samba/%m.log
```

h) Tamanho máximo do arquivo de log (em KB):

```
max log size = 0
```

i) Configuração da política de acesso e autenticação para os serviços compartilhados. O nível “user” indica que haverá autenticação de usuários específicos e respectivas senhas para acesso nos recursos:

```
security = user
```

j) Opção que habilita o Samba a trabalhar com criptografia de senhas na rede:

```
encrypt passwords = yes
```

k) O arquivo dos usuários de acesso aos recursos do Samba:

```
smb passwd file = /etc/samba/smbpasswd
```

l) Se a opção for “yes” especifico que o Samba tentará se tornar o servidor de recursos principal (master browser) dentro do meu grupo de trabalho:

```
; local master = no
```

m) Definição da candidatura do servidor Samba para eleger-se o master browser da minha rede:

```
; os level = 33
```

n) Definição do Samba como o master browser do domínio:

```
; domain master = yes
```

o) Nesta opção, eu digo que o Samba sempre tentará ser o servidor master browser na minha rede, “forçando” para que haja a eleição na rede:

```
; preferred master = yes
```

p) Permite que clientes 9x/NT se autentiquem no domínio como se fosse um domínio Microsoft, tornando o Samba um PDC:

```
; domain logons = yes
```

q) Caminho dos scripts de logon na autenticação dos usuários (arquivos “.bat” e “.cmd”):

```
; logon script = %m.bat
```

r) Path dos profiles (perfis móveis) dos usuários Windows:

```
; logon path = \\%L\Profiles\
```

s) O Samba se tornará o servidor WINS da rede NetBIOS:

```
; wins support = yes
```

t) Se já existir um servidor WINS na rede, aqui eu coloco o endereço IP do servidor, tornando o Samba um cliente WINS:

```
; wins server = w.x.y.z
```

A próxima seção nos fala sobre o compartilhamento dos homes dos usuários

```
[homes]
```

a) Descrição do compartilhamento:

```
comment = Home Directories
```

b) Define se o compartilhamento será listado junto com os demais recursos no Ambiente de Rede:

```
browseable = no
```

c) Define se o compartilhamento aceita gravação:

```
writable = yes
```

d) Permissão padrão de criação de arquivos no compartilhamento:

```
create mode = 0664
```

e) Permissão padrão de criação de diretórios no compartilhamento:

```
directory mode = 0775
```

Já esta seção nos fala sobre o compartilhamento das impressoras

```
[printers]
```

```
comment = All Printers
```

a) Diretório do spool de impressão no servidor:

```
path = /var/spool/samba
```

b) Aqui, eu configuro se o acesso à minha impressora será público:

```
guest ok = no
```

c) Significa que os clientes podem mandar arquivos para o diretório de spool no momento da impressão:

```
printable = yes
```

3 - Depois de analisar o arquivo de configuração, vamos adicionar o nosso próprio compartilhamento. No final do arquivo, insira as seguintes linhas para criar estes dois compartilhamentos:

[LINUX] -> nome do compartilhamento

comment -> teste do Samba

path = /tmp/samba -> diretório a ser compartilhado

valid users = tux teste -> usuários que poderão acessar o compartilhamento

writable = yes

create mask = 0600 -> o mesmo que o parâmetro create mode

directory mask = 0700 -> o mesmo que o parâmetro directory mode

[arquivos]

comment -> outro teste

path = /tmp/arquivos -> diretório a ser compartilhado

writable = yes

write list = @unix -> grupo que terá permissão para gravação no compartilhamento

valid users = @unix -> somente os usuários do grupo "unix" poderão acessar o compartilhamento

create mask = 0660

directory mask = 0770

Salve e saia do arquivo

4 - Podemos rodar agora o utilitário testparm para saber se o arquivo possui erros:

```
# testparm /etc/samba/smb.conf
```

R:

5 - Subindo o serviço do Samba:

```
# /etc/init.d/samba start
```

6 - Verificando se os compartilhamentos do servidor estão ativos:

```
# smbclient -L <ip do servidor samba> -N
```

R:

7 – Agora eu preciso adicionar os usuários, já existentes no sistema na base de dados de usuários do Samba:

```
# smbpasswd -a tux  
# smbpasswd -a teste
```

8 - Monte, através do comando smbmount, o compartilhamento Linux com o usuário tux e, quando ele pedir a senha, coloque a que você definiu no comando smbpasswd:

```
# smbmount //192.168.100.100/linux /mnt/samba -o username=tux
```

DETALHE: se você tentar montar com qualquer outro usuário que não foi definido com permissão de acesso ao compartilhamento, ele retornará um erro.

9 - Depois disso, teste o acesso aos recursos do Samba pelo cliente Windows, através do Ambiente de Rede.

9.1 - Samba como PDC

Quando estamos em uma rede Microsoft onde os clientes se autenticam em um domínio específico, as configurações de segurança e autenticação ficam centralizadas em um único lugar, o chamado Controlador de Domínio (PDC). O Samba permite que nós façamos uma máquina Linux/Unix se tornar o Controlador de Domínio de uma rede com clientes Windows.

1 - Entramos novamente no arquivo de configuração do Samba:

```
# vi /etc/samba/smb.conf
```

E adicionamos as seguintes linhas, na seção [global]:

a) Definição do nome NetBIOS do servidor Samba:

```
netbios name = SCORPION
```

b) Denominação do domínio:

```
workgroup = DEBIAN
```

c) Definir como master browser do domínio:

```
domain master = yes
```

d) Este valor é para que o Samba vença a eleição de master browser na rede:

```
os level = 80
```

e) Forçar a eleição do Samba:

```
preferred master = yes
```

f) Torná-lo um servidor de logon do domínio (um PDC):

```
domain logons = yes
```

g) Driver mapeado no Windows para os homes dos usuários:

```
logon drive = H:
```

h) Diretório home dos usuários do Windows:

```
logon home = \\%L\profiles\
```

i) Grupo responsável pelo ingresso das máquinas no domínio (somente os usuários com UID=0 neste grupo serão considerados habilitados para darem esse ingresso):

```
domain admin group = root
```

Definição dos compartilhamentos principais**a) Compartilhamento dos scripts de logon:**

```
[netlogon]
  path = /home/netlogon
  writable = no
  browsable = no
```

b) Compartilhamento dos homes dos usuários do Windows:

```
[profiles]
  comment = Servidor de Dominio
  public = no
  path = /home/%u -> o diretório de compartilhamento será o
próprio homes dos usuários
  browsable = yes
  writable = yes
  create mask = 0600
  directory mask = 0700
```

Agora eu salvo o meu arquivo smb.conf

2 - Se na sua rede houver clientes NT/2000/XP, você deve criar no servidor o que chamamos de "trust account", onde, para cada máquina ingressada no domínio é necessária uma chamada "conta de máquina", pois é com essa conta que ele se registrará no domínio. Para isso, dou os seguintes comandos:

```
# groupadd trust -> cria um grupo específico para conter as contas de máquina  
# useradd -g trust -s /dev/null -d /dev/null maquina01$ -> aqui eu crio a  
conta de máquina, onde o nome do usuário será o mesmo nome NetBIOS do cliente  
Windows (maquina01 é o nome do meu cliente Windows)
```

OBS: o sinal de \$ no final é SEMPRE necessário

3 - Adiciono a conta de máquina na base de dados dos usuários do Samba:

```
# smbpasswd -a -m lamer
```

4 - Eu preciso agora de um usuário com UID=0 do grupo root para ser um usuário autorizado a ingressar os clientes no domínio:

```
# smbpasswd -a root (o usuário root será o responsável pelo ingresso das máquinas no  
domínio)
```

5 - Vamos reinicializar o servidor Samba:

```
# /etc/init.d/samba stop  
# /etc/init.d/samba start
```

6 - Eu posso fazer um teste para saber se o master browser e o PDC estão respondendo na minha rede, com o comando nmblookup:

```
# nmblookup -A -M <ip da rede>
```

R:

7 - Agora, é preciso configurar a máquina Windows para ele ingressar no domínio. Siga os seguintes passos:

PARA WINDOWS 95/98/Me:

- Na opção Rede do Painel de Controle, clique em Clientes para Redes Microsoft e marque o item "Login" em "Domínio do Windows NT". Depois, entre com o nome do domínio, no caso DEBIAN.

PARA WINDOWS 2000:

- Clique com o botão direito em Meu Computador e escolha a opção Propriedades. Na aba Identificação de Rede, clique no botão Propriedades e marque, no frame "Membro de", a opção "Domínio" e especifique o nome (no caso DEBIAN), dando depois um OK. Ele irá pedir o nome do usuário que fará o ingresso da máquina no domínio. No caso, especifique o usuário "root" e a senha dele da base de dados do smbpasswd.