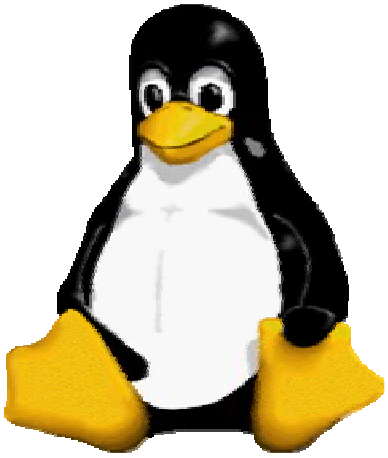
PROJETO DE REDES
www.projetoderedes.com.br

Redes Linux

Comandos gerais e Servidores de redes



Desenvolvido por Jorgeley Inácio Júnior

Instalação do Linux

Particionamento

Caso tenha-se um Windows instalado no PC, particione o HD para instalar o Linux separadamente do Windows. Utilize um FDISK, PARTITION MAGIC ou qualquer outro particionador.

Ao particionar defina o sistema de arquivos da partição do Linux como sendo EXT3, esta partição deverá ter no mínimo 600 MB livres caso a instalação seja do tipo Estação de Trabalho, se for Servidor então o tamanho vai para pelo menos 1.6 GB. O melhor a fazer, é claro é definir um tamanho maior do que este recomendado. Não esqueça de definir o ponto de montagem como sendo "/" para a partição EXT3.

Além da partição EXT3, que é onde o Linux será instalado, é altamente recomendado que se defina uma partição com sistema de arquivos SWAP, esta partição deverá ser de tamanho igual ao dobro da memória do PC. Esta partição será utilizada pelo Linux como partição de troca, ou seja, memória virtual.

Iniciando a instalação

Depois de definir as partições do Linux, entre no Setup do PC e defina o boot a partir do CDROM, coloque o CDROM do Linux e dê o boot.

Siga os passos da instalação normalmente, ao chegar em particionamento escolha "forçar particionamento manual", ao entrar no particionador apenas selecione a partição EXT3 para que o instalador saiba que esta será a partição onde será instalado o Linux, observe se o ponto de montagem está definido, caso não esteja, defina-o.

Quando chegar na tela para escolher o tipo de inicialização escolha o LILO para ser seu sistema de inicialização, ele será utilizado para se escolher o SO que será inicializado no boot, defina a localização do mesmo no "registro mestre de inicialização MBR". Siga o restante dos passos até reiniciar o PC.

Iniciando o uso do Linux

Comandos básicos

O linux possui duas formas de operação, você pode tanto utiliza-lo em modo texto ou em modo gráfico. Além disso, você pode alternar entre os terminais pressionando CTRL+ALT+Fn, sendo n o número do terminal que se deseja.

Logo que o Linux é iniciado ele pedirá login e senha, tanto em modo texto como em modo gráfico.

O super usuário root tem permissão geral no Linux, pode fazer tudo, para saber se você está logado como superusuário basta olhar na linha de comando, caso tenha uma "#" você está logado como super usuário. Os outros usuários precedem de um "$" na linha de comando.

A maioria dos comandos do Linux possui um manual, caso tenha dúvida sobre determinado comando basta digitar na linha de comando:

man <comando>

Todos os comandos possuem argumentos que deverão ser passados ao digita-lo:

comando -<opções argumentos>

Ex: ls – l

Comandos de administração de usuários

Para adicionar um usuário:

useradd <nome usuário> -g <grupo existente>

Ex: useradd Juliana

Para colocar senha para o usuário adicionado:

passwd <usuário>

Ex: passwd Juliana

Para deletar usuário:

userdel <usuário>

Ex: userdel Juliana

Para adicionar um grupo de usuários:

groupadd <novo grupo>

Ex: groupadd amigos

Para apagar um grupo:

groupdel <nome grupo>

Ex: groupdel amigos

Para adicionar um usuário em um grupo:

useradd <nome usuário> -g <nome grupo>

Ex: useradd Gondim –g metal

O arquivo /etc/passwd possui todos os usuários com seus grupos, edite-o com o VI para visualizar. O arquivo /etc/group possui os grupos cadastrados no sistema.

Comandos sobre arquivos

Acessar um diretório:

cd /diretório

Ex: cd /etc

Voltar ao diretório anterior:

cd –

Criar um diretório:

mkdir <novo diretório>

Ex: mkdir guampa

Remover um diretório:

rmdir <diretório>

rm –r <diretório>

Ex: rm –r guampa

Criar um arquivo novo:

touch <novo arquivo>

Ex: touch texto

Remover um arquivo:

rm <arquivo>

Ex: rm texto

Renomear um arquivo ou muda-lo de lugar:

mv <nome_velho_arquivo> <novo_nome_arquivo>

mv /<diretório>/<arquivo> /<novo_diretorio>

Ex: mv /home/texto /mnt/floppy

Mudar o grupo do arquivo ou diretório:

chgrp <novo grupo> <arquivo ou diretório>

Ex: chgrp amigos texto

Mudar a permissão do arquivo ou diretório:

chmod <nnn> <arquivo ou diretório>

*nnn são os números referentes às permissões do arquivo ou diretório. 4=leitura; 2=escrita; 1=execução.

Ex: chmod 740 texto

Listar o conteúdo de um diretório:

ls

Ex: ls /root

Mudar o dono de um arquivo ou diretório:

chown <novo dono> <arquivo ou diretório>

Ex: chown Juliana texto

Copiar arquivo:

cp <arquivo_a_ser_copiado> <nome_cópia>

cp /home/texto /mnt/floppy

Mostrar diretório atual:

pwd

Formatar disquete:

fdformat <dispositivo>

Ex: fdformat /dev/fd0

Criar sistema de arquivos do disquete:

mkfs.msdos /dev/fd0 –f 12

Visualizar um arquivo no terminal:

cat <arquivo>

Ex: cat texto

Mostrar o cabeçalho do arquivo:

head <arquivo>

Ex: head texto

Mostrar o final do arquivo:

tail –f <arquivo>

Ex: tail –f texto

Criar atalho para um arquivo

ln –s <arquivo> <nome_atalho>

Ex: ln –s /etc/samba/smb.conf atalho_smb.conf

Procurar uma palavra em um arquivo:

grep "<palavra>" <arquivo>

Ex: grep "root" passwd

Procurar um arquivo:

find <local> -name <arquivo>

Ex: find /etc –name passwd

(esta forma procura por um arquivo específico)

find / -exec grep "root" {} –ls \;

(esta forma procura por um arquivo contendo uma palavra específica)

Comandos sobre sistemas de arquivos

Para montar qualquer sistema de arquivo utilize a seguinte sintaxe:

mount –t <tipo_sist_arquivos> /dev/<sist_arquivos> /<ponto_mont>

Montar um disquete:

mount –t vfat /dev/fd0 /mnt/floppy

Montar uma partição windows:

mount –t vfat /dev/hda1 /mnt/windows

Montar o CDROM:

mount –t iso9660 /dev/cdrom /mnt/cdrom

Verificar dispositivos montados:

mount

Desmontar qualquer sistema de arquivos:

umount /ponto_de_montagem

Ex: umount /mnt/floppy

No diretório /etc há um arquivo chamado "fstab", neste arquivo há algumas descrições de sistemas de arquivos que podem ser montados na inicialização do linux, uma das linhas descreve o próprio ponto de montagem do linux, no caso o "/" (diretório raiz). Caso queira colocar algum sistema de arquivo para ser montado na inicialização do linux é só adicionar a linha no fstab descrevendo o sistema de arquivo a ser montado. Outra vantagem em colocar um sistema de arquivos no fstab é que além de ele ser montado na inicialização do linux ele poderá ser montado com o comando mount, porém especificando apenas o dispositivo ou o ponto de montagem. Por exemplo: para montar o disquete, bastará digitar "mount /mnt/floppy".

Comandos sobre instalação no Linux

Verificar se pacote instalado:

rpm –q <pacote>

Instalar pacote:

rpm –i <pacote>

Desinstalar pacote:

rpm –e <pacote>

Pode-se utilizar juntamente com a opção "i" ou "e" as opções "vh" para ser mostrado detalhes da instalação ou desinstalação.

Ainda há um detalhe importante, às vezes teremos que baixar o fonte de um determinado software e instalá-lo manualmente, instalando o software na forma mais bruta do linux. Supondo que baixamos o fonte do Apache 2 (que é um software, no caso servidor Web), vejamos como instalá-lo:

1. Entrar no diretório onde foi baixado o fonte do Apache, só pra conferir se realmente o arquivo está lá, supondo que foi baixado no diretório root, então:
    a. cd /root
    b. ls
2. Certamente haverá um arquivo "httpd-2.0.53.tar.gz", no caso "httpd-2.0.53" é o nome do software e ".tar.gz" é a extensão do arquivo, que neste exemplo é um arquivo compactado com tar e com gzip, então temos que descompacta-lo:
    a. primeiro devemos entrar no diretório onde será descompactado, o melhor é o diretório /usr/local, então:
        i. cd /usr/local
    b. agora vamos descompactar o arquivo:
        i. tar –xzvf < /root/httpd-2.0.53.tar.gz –
3. Desta maneira será descompactado o arquivo e então aparecerá um diretório "httpd-2.0.53" que foi extraído do arquivo compactado. Agora é só instalar:
    a. Entre no diretório que foi extraído:
        i. cd httpd-2.0.53
    b. Liste os arquivos:
        i. ls
    c. Haverá um arquivo chamado "configure", que é um arquivo executável. Este arquivo é responsável por configurar o software para posterior instalação, então execute-o:
        i. ./configure --prefix=/etc/apache-2.0.53
    d. depois de configurar é só compilar o fonte do software, então:
        i. make
        ii. make install

Pronto, tá instalado o Apache 2. A única coisa chata é que às vezes você pode encontrar um software que não segue os mesmos passos, mas na maioria será desta maneira. Neste exemplo na hora de executar o configure eu só coloquei o parâmetro --prefix que indica em qual diretório será instalado o software, porém pode haver mais parâmetros. Na maioria das vezes terá que ser feito estes passos: extrair o arquivo, executar o configure, make e make install.

Outros comandos

Desligar o PC:

shutdown –h now
init 0
halt

Reiniciar o PC:

reboot
shutdown –r now
init 6

Listar processos:

ps –aux

Matar processo:

kill –9 <número_processo>

Ex: kill -9 756

killall <nome_processo>

Ex: killall smbd

Compactar arquivo:

zip <arquivo>

Descompactar arquivo:

unzip <arquivo>

Descompactar arquivo ".tar.gz":

tar –xzvf <arquivo>.tar.gz

Ex: tar –xzvf amsn-092.tar.gz

Testar placa de rede:

ping <IP_do_PC>

Ex: ping 192.168.10.69

Checar IP:

ifconfig

Configurar IP:

ifconfig eth0 <IP_host> netmask <máscara_rede> up

Ex: ifconfig eth0 192.168.10.69 netmask 255.255.255.0 up

Visualizar dispositivos PCI's:

lspci

Limpar a tela:

clear

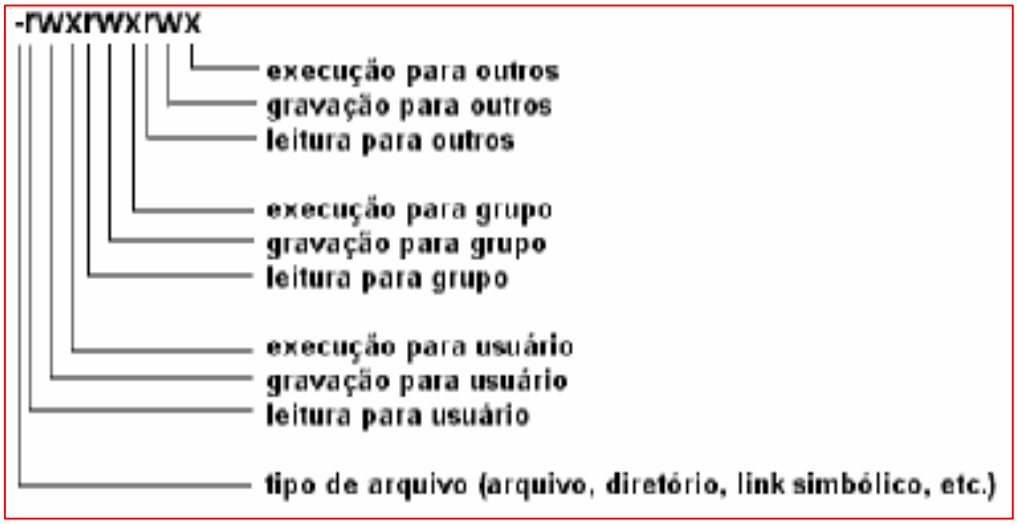
Visualizar calendário:

cal

Ver data atual e hora:

date

Atributos dos arquivos e diretórios



Editor VI

Caso queira editar um arquivo basta digitar VI <arquivo>. Ao entrar no arquivo sempre olhe no rodapé do VI para saber se você está no modo de edição ou comando. Quando o VI é iniciado ele se encontra no modo comando e, sempre que estiver em modo edição e quiser voltar para modo comando apenas pressione ESC. Para manipular o arquivo em modo edição utilize o seguinte:

Alterar o arquivo: Pressione “i”, modo inserção. Aparecerá no rodapé “insert” indicando que você pode alterar o arquivo.

Salvar o arquivo: Depois de modificar o arquivo, para salva-lo é preciso entrar em modo comando, então pressione ESC, no modo comando digite “:w <nome_arquivo>”.

Sair do VI: Alterne para o modo comando e digite “:q”.

Salvar e sair: Alterne para o modo comando e digite “:x”.

Copiar: Alterne para o modo comando e digite “yy” para copiar a linha atual; “yw” para copiar a palavra atual.

Colar: Alterne para o modo comando e digite “p” para colar depois do cursor; “P” para colar antes do cursor.

Desfazer: Alterne para o modo comando e digite “u”.

Apagar: Alterne para o modo comando e digite “dd” para apagara a linha atual; “dj” para apagar a linha atual e a próxima.

Inserir nova linha: Alterne para o modo comando e digite “o” para inserir uma nova linha abaixo; “O” para inserir uma nova linha acima.

Redes

Configurar placa de rede

Para saber os dispositivos PCI’s do seu PC utilize o comando “lspci”. Se sua placa de rede for PCI certamente ela aparecerá na listagem.

Para configurar sua placa de rede utilize o comando ifconfig:

Ex: ifconfig eth0 192.168.10.69 netmask 255.255.255.0 up

Neste exemplo, a primeira placa de rede (eth0), será configurada com o IP 192.168.10.69 e com máscara de rede de classe C e, além disso, já ligará a placa de rede com o novo IP. Para ver se deu certo basta digitar ifconfig.

O único detalhe deste comando é que ao dar outro boot na máquina, a configuração será perdida, neste caso temos que alterar o arquivo de configuração da placa de rede para que não aconteça isso. Nas distribuições Conectiva e Red Hat, há um arquivo chamado: /etc/sysconfig/network-scripts/ifcfg-eth0 que corresponde ao arquivo de configuração da primeira placa de rede, basta usar o VI para editá-lo e configurar a linha “IPADDR” com o IP desejado e a linha “NETMASK” com a máscara de rede, há também o parâmetro “ONBOOT” que diz se a placa de rede deve ser ligada na inicialização, caso queira é só igualar a YES. Já no Slackware (minha distribuição favorita) o arquivo de configuração é o /etc/rc.d/rc.inet1.

Servidor de arquivos - Samba

Compartilhamento Share

O Samba é um software do Linux que possibilita compartilhamento entre máquinas linux e windows, além de possibilitar o controle de compartilhamento através de validação de usuários. Detalhe importante: na verdade o que o SAMBA faz é enganar as máquinas windows fazendo-as pensarem que o servidor de arquivos SAMBA é um servidor Windows NT (pobre windows... tão ingênuo...).

Basicamente o Samba possui dois tipos de compartilhamentos: nível de segurança Share e Server, o primeiro a ser visto será o mais simples que é o Share.

Primeiramente verifique se o samba está instalado, caso não esteja instale-o. Para configurar o Samba há duas maneiras: através do modo gráfico ou através do arquivo de configuração (na unha mesmo). O mais interessante é através do arquivo de configuração, porém para fazermos um compartilhamento do tipo Share vamos utilizar o modo gráfico.

Para possibilitar a configuração do Samba em modo gráfico deve-se editar o arquivo /etc/inetd.conf e descomentar a última linha do mesmo. Para descomentar a última linha do arquivo retire o "#" no início da linha. Todo arquivo do Linux que tiver este "#" no início da linha é porque a linha está comentada. Depois de descomentar a linha salve o arquivo.

Vá até o diretório /etc/rc.d/init.d e inicie o "inet", para isso basta digitar "./inet start", inicie também o "httpd", dê uma reiniciada no Samba também.

Feito isso vá no ambiente gráfico e abra o Netscape ou qualquer outro navegador, digite a url: http://localhost:901. Isto deverá abrir o Samba em modo gráfico, se não der certo retire o "http://". Na parte superior do Samba haverá vários botões, clique no botão Globals. Aparecerá então as variáveis globais do Samba para serem configuradas.

Em workgroup defina seu grupo de trabalho, em netbios name defina o nome que aparecerá nas máquinas clientes referenciando o servidor SAMBA (qualquer coisa), em security escolha a opção Share, em os level digite um número de preferência igual ou maior que 100 (este número definirá quem será servidor na rede), em hosts allow defina a faixa de rede que será permitida no compartilhamento, em hosts deny defina a faixa de rede que não será permitida no compartilhamento.

Até aqui configuramos as variáveis globais do SAMBA as quais definem as opções de compartilhamento, agora só falta definir o que vai ser compartilhado. Para definirmos o que será compartilhado, dessa vez iremos usar o modo texto, então alterne para o modo texto e entre no diretório /etc e edite o arquivo smb.conf. Este arquivo é o arquivo de configuração do Samba, contém as mesmas características do Samba em modo gráfico. Abaixo das variáveis globais ficarão os compartilhamentos, para adicionar um compartilhamento basta seguir o seguinte modelo:

```
########### variáveis globais ###########
#grupo de trabalho
workgroup = Grupo1
#nome q aparece no ambiente de rede do windows abaixo ícone do servidor
netbios name = Servidor Linux
#descrição que aparecerá entre parênteses abaixo do nome do servidor
server string = Linux Server
#nível de segurança do servidor SAMBA, share é o mais baixo
security = share
#maneira como o servidor samba resolverá o nome das máqs para IP
name resolve order = lmhosts hosts wins bcast
#ajusta os sockets de conexão, só pra dizer como o SAMBA se conectar
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
#número q define quem é o servidor, caso haja mais de um servidor
os level = 150
#diz p/ o SAMBA não utilizar consulta DNS para resolução dos nomes
dns proxy = no
#faixa de rede permitida pelo servidor
hosts allow = 192.168.2.
#faixa de rede não permitida pelo servidor
hosts deny = 192.168.7.

########### exemplo de compartilhamento ###########
[Pasta1]
#comentário à toa, aparecerá do lado esquerdo da janela do windows
comment = Pasta1
#caminho para a pasta compartilhada
path = /pasta1
#diretório não será somente leitura
readonly = no
#permite gravação
writeable = yes
#compartilhamento visualizável no browse
browseable = yes
#pasta é pública
public = yes
```

Depois de configurado, é claro que você terá que criar a pasta compartilhada pelo samba, no exemplo acima é a pasta "pasta1" no diretório raiz, então não esqueça de criá-la. Já que o compartilhamento não terá segurança nenhuma, dê permissão total à pasta, utilize o comando "chmod".

Feito isso, você pode testar o arquivo de configuração do samba pelo comando "testparm smb.conf", isso mostrará um relatório sobre as configurações feitas no smb.conf, se der tudo ok, então tá tudo certo. Depois disso é só ligar o SAMBA utilizando o comando "smbd –D" e depois "nmbd –D" no caso da distribuição slackware, se for Conectiva então utilize o comando "service smb start", se preferir você pode rebootar a máquina e também ligar o SAMBA, então dê um reboot só por segurança e reinicie os serviços do Samba. Agora é só configurar as estações windows.

Nas máquinas windows que acessarão o compartilhamento, coloque os IP's das mesmas na mesma faixa de rede do servidor e adicione um gateway com o IP do servidor, configure o grupo de trabalho como sendo o mesmo do servidor.

Agora é só reiniciar os PC's windows e ver os compartilhamentos, na tela de inicialização é só informar um usuário qualquer e depois verificar o seu servidor SAMBA no ambiente de rede do windows.

Compartilhamento Server a nível de grupo

Para este nível de segurança utilizaremos o arquivo smb.conf para montar o compartilhamento, ou seja, montaremos o compartilhamento na unha mesmo.

Neste nível de segurança o compartilhamento será a nível de grupo, ou seja, se o usuário pertencer ao grupo permitido, terá acesso aos compartilhamentos.

As variáveis globais permanecerão inalteradas, a definição do compartilhamento a nível de grupo será feita diretamente no compartilhamento, então edite o smb.conf e coloque um compartilhamento seguindo o seguinte modelo:

```
###################### variáveis globais ######################
workgroup = Grupo1
netbios name = Servidor Linux
server string = Tux
security = Server
encrypt passwords = yes
```

```
update encrypted = yes
log file = /var/log/samba/log.%m
name resolve order = lmhosts hosts wins bcast
#se o compartilhamento ficar por muito tempo aberto na estação, será fechado
time server = yes
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
#indica que o script de logon será a nível de usuário
logon script = %U.bat
#nome do servidor samba na rede que autenticará o logon
logon path = servidor
# indica que o servidor samba será domínio de logon, ou seja, os logons nas
# estações windows serão efetuados no servidor samba
domain logons = yes
# indica que o servidor samba será mestre de domínio, ou seja, as estações que
# acessarem o samba o próprio samba resolverá o nome das mesmas para IP
domain master = true
os level = 100
# caso haja mais de um mestre de domínio na rede, esta opção indica que o
# samba é que preferivelmente será o mestre de domínio
preferred master = true
dns proxy = no
hosts allow = 192.168.2.
hosts deny = 192.168.7.
############### coloque os compartilhamentos abaixo ###############
[Exemplo_de_compartilhamento]
comment = Pasta1
path = /pasta_do_grupo
# grupo de usuários válidos para acessarem o compartilhamento
valid users = @grupo1 @grupo2
# grupo de usuários que podem escrever na pasta
write list = @grupo1
# indica que usuários não autenticados não acessarão o compartilhamento
guest only = no
readonly = no
available = yes
writable = yes
# indica que não somente um usuário acessará a pasta, vários ao mesmo tempo
only user = no
browseable = yes
public = yes
```

usuário administrador do compartilhamento
admin user = @administrador

Adicione um grupo no linux referente ao grupo que poderá acessar o compartilhamento, no exemplo acima é o grupo “grupo1”, e depois adicione um usuário no Linux pertencente a este grupo e coloque senha para o mesmo, este usuário terá acesso aos compartilhamentos então adicione o mesmo usuário no samba, para isso utilize o comando:

smbpasswd –a <usuário_linux>

Será solicitada a senha para o usuário, então digite a mesma senha do usuário linux ao cadastrar.

Depois de ter adicionado o usuário, crie a pasta compartilhada pelo samba, no caso do nosso exemplo é a pasta “pasta_do_grupo”, depois de criada a pasta, mude o dono da pasta para o usuário que você cadastrou há pouco e mude também o grupo da pasta para o grupo que você adicionou, o grupo que pode acessar o compartilhamento no samba. Agora que a pasta pertence ao usuário certo e ao grupo certo, dê permissão total ao usuário dono da pasta e também para o grupo dono da pasta, já os outros usuários dê permissão nenhuma, ou seja, dê um “chmod 770 pasta_do_grupo”.

Por precaução dê um reboot para que as alterações façam efeito melhor e inicie o serviço do samba: “smbd –D” e “nmbd –D” ou “service smb start“(se for Conectiva).

Agora é só configurar as estações windows, só tem um probleminha, se for estação windows 98 é de uma maneira e se for windows NT já é de outra maneira, então vamos ver como configura das duas maneiras. Primeiro vamos ver como configura estação windows 98.

Nas máquinas windows 98 que acessarão o compartilhamento, coloque os IP’s das mesmas na mesma faixa de rede do servidor e adicione um gateway com o IP do servidor, configure o grupo de trabalho como sendo o mesmo do servidor. No serviço de ambiente de rede “cliente para redes Microsoft” abra-o e marque a opção de “Logon no domínio do windows NT” e em “Domínio do Windows NT” coloque o nome do grupo de trabalho do servidor samba. Em “controle de acesso” marque a opção “nível de usuário” e em “obter lista de grupo de usuários” coloque o grupo de trabalho definido no servidor Linux.

Feito isso reboot a máquina windows. Configurada as máquinas windows falta ainda criar o script de logon que será utilizado para validar os usuários ao logarem no servidor Linux, para isso abra o Bloco de Notas do windows e crie o seguinte arquivo:

```
############ script de logon do usuário user1 ############
echo off
echo "acertando a hora da estação com o servidor..."
net time \\server1 /set /yes
echo "mapeando o compartilhamento..."
net use J: \\192.168.69.1\compartilhamento
```

Salve este arquivo com a extensão ".bat" e copie-o para o servidor linux para o diretório /home/samba/netlogon. Reinicie os serviços do Samba e está pronto. Agora quando as máquinas windows forem iniciadas pedirão login e senha que serão validados no servidor Samba. Você terá que digitar o usuário que você cadastrou no samba, o usuário que tem permissão para acessar o compartilhamento. Depois de logar, o script de logon será executado no servidor e aparecerá na estação windows a sua execução, e automaticamente o compartilhamento será mapeado, se você abrir o "meu computador" do windows você verá uma unidade que será o seu compartilhamento. Legal né?

Para aprender como configurar as estações Windows NT, vide anexo I no final desta apostila.

Sistema de arquivo de rede - NFS

O NFS (Network File System) ou Sistema de Arquivo de Rede (traduzindo para goianês), é um protocolo que possibilita o compartilhamento de arquivos através da rede. Utilizaremos o NFS para fazer compartilhamento de máquinas Linux para máquinas Linux.

Primeiramente é claro, temos que ter certeza que o servidor NFS está instalado em nossa máquina, os pacotes a serem instalados são os seguintes:

nfs-server*

nfs-utils

Para ficar mais fácil instale tudo que comece com "nfs-", ou seja, digite o comando:

```
rpm –ivh nfs-*
```

Isso fará com que todos os pacotes que tenham o nome inicializado com a palavra "nfs-" sejam instalados, logo tudo que a gente precisa será instalado.

Para configurar o NFS, podemos utilizar o Linuxconf (que tem uma telinha bem mais bonitinha e interativa) ou então podemos configurar o NFS através de seus arquivos de configuração, como a gente é "bruto" faremos a configuração do modo mais difícil: através dos arquivos de configuração.

Primeiramente vamos definir os diretórios que serão compartilhados, para isso edite o arquivo "/etc/exports" e defina os diretórios compartilhados usando a seguinte sintaxe:

```
/home/jorgeley/inacio        192.168.7.69 (rw)
/home/andre/cunha            192.168.7.*  (rw)
```

Neste exemplo de compartilhamento, o diretório "inácio" está exportado somente para o host "192.168.7.69" para uso completo "rw", ou seja, leitura e escrita. Já o diretório "cunha" está exportado para todos os hosts pertencentes à rede "192.168.7" para leitura e escrita.

Definidos os compartilhamentos, agora vamos definir quais hosts poderão utilizar o serviço "Portmap". O Portmap interligará os clientes NFS com o servidor NFS informando aos clientes NFS como acessar os serviços NFS na máquina servidor. Para definirmos quais hosts acessarão o serviço Portmap, utilizaremos os arquivos "/etc/hosts.allow" e "/etc/hosts.deny". Inicialmente vamos proibir que todos os hosts acessem o Portmap, então edite o arquivo "/etc/hosts.deny" e adicione o seguinte:

```
portmap: ALL
```

Isso proibirá qualquer host, independente da rede, de acessar o Portmap. Bom, mas se proibimos qualquer host de acessar o portmap, isso significa que o NFS não vai rodar, não é mesmo? Claro, não vai rodar mesmo, pois como já foi dito, o Portmap vai dizer às máquinas clientes NFS como utilizar o serviço NFS para acessar os compartilhamentos e, se proibimos todos os hosts de utilizar o Portmap, isso vai impossibilitar que todos os hosts utilizem o NFS para ver os compartilhamentos. Então vamos liberar alguns hosts para acessarem o Portmap, para isso edite o arquivo: "/etc/hosts.allow" e coloque o seguinte:

```
portmap: 192.168.7.0/255.255.255.0
```

Agora sim, acabamos de liberar acesso ao Portmap para todos os hosts pertencentes à rede "192.168.7.0", resumindo: primeiro bloqueamos o acesso ao Portmap a todo mundo e depois desbloqueamos apenas para uma rede, a rede 192.168.7.0, dessa maneira somente esta rede terá acesso ao portmap, e o restante não terá.

Estas configurações são as configurações necessárias para o Servidor NFS funcionar, agora temos que iniciar os serviços NFS, que são muitos. Os primeiros serviços que vamos inicializar são os daemons do NFS, então inicie-os usando os seguintes comandos:

```
/usr/sbin/rpc.nfsd
/usr/sbin/rpc.lockd
/usr/sbin/rpc.statd
/usr/sbin/rpc.mountd
```

/usr/sbin/rpc.rquotad

Temos que atualizar a lista de diretórios exportados basta digitar o seguinte comando:

/usr/sbin/exportfs –ra

Iniciados os daemons, agora inicializaremos o Portmap, então vá ao diretório dos dispositivos inicializáveis (aquele onde você inicializa a placa de rede), é só usar o comando cds para chegar neste diretório e inicie o Portmap pelo seguinte comando:

./portmap start

Belê, agora finalmente inicializaremos o NFS, ainda no diretório dos dispositivos inicializáveis digite o comando abaixo:

./nfs start

Muito bem, o servidor já ta configurado, agora vamos ver se realmente funciona. Nas máquinas clientes digite o seguinte comando:

showmount –e <IP_do_servidor_NFS>

Este comando, digitado nas máquinas clientes, deverá gerar uma lista dos diretórios que você compartilhou no servidor NFS, aqueles diretórios que você colocou no arquivo "/etc/exports" do servidor NFS. Lembre-se que somente funcionará o NFS nas máquinas que você liberou acesso ao Portmap no servidor NFS, então as máquinas clientes deverão estar na faixa de rede que foi especificado no arquivo "/etc/hosts.allow" do servidor NFS.

O comando "showmount –e" só serve para ver os diretórios compartilhados, além de ser uma maneira de conferir se o compartilhamento tá funcionando. Mas ainda não estamos vendo o diretório compartilhado do servidor NFS nas nossas máquinas clientes, para isso teremos que montar os diretórios compartilhados do servidor NFS, mais ou menos parecido com os comandos de montar disquete e CDROM, o comando para montar os diretórios do servidor NFS nas máquinas clientes é o seguinte:

mount –t nfs <IP_do_servidor>:<diretório_compartilhado> <ponto_montagem>

Ex: mount –t nfs 192.168.7.1:/home/jorgeley/inacio /mnt/nfs

Seguindo o exemplo acima, o diretório "inácio" que foi compartilhado no servidor NFS cujo IP é "192.168.7.1" será montado localmente no ponto de montagem "/mnt/nfs", logo, todos os arquivos que estiverem dentro do diretório "inácio" do servidor NFS poderão ser acessados no diretório "/mnt/nfs".

Pronto, está montado o servidor NFS, não doeu! Ou doeu?

Servidor Web - Apache

Um servidor Web nada mais é do que um software que nos permite hospedar uma página, seja ela qual for, em um computador e disponibilizarmos esta página à uma rede local ou a Internet. Todo site na Internet é hospedado em um computador que no caso denominamos de servidor Web.

O Apache é o servidor Web mais utilizado no mundo inteiro, por sua alta performance, confiança e principalmente baixo custo. O Apache foi desenvolvido a partir do daemon httpd, que era um servidor web antigo (o único que existia na época), este daemon httpd, foi desenvolvido por um tal de Rob McCool, que trabalhava numa tal de NCSA (uma empresa americana). Depois que Rob McCool deixou a NCSA o daemon httpd foi abandonado e então webmasters que conheciam o daemon httpd começaram a trabalhar para melhorá-lo, e assim nasceu o Apache. Concluindo, o Apache é o daemon httpd, só que melhorado.

O servidor Apache permite-nos que possamos criar sites em PHP ou qualquer outra tecnologia e disponibilizarmos essas páginas na rede local, ou seja, podemos com o Apache implementar um servidor Web, mas para isso temos que configura-lo para tal.

Primeiramente verifique se o Apache está instalado, basta digitar:

```
httpd –v
```

Se aparecer um monte de informação sobre o Apache é porque ta instalado, senão você deverá instala-lo.

Depois de instalado, entre no diretório onde ficam os arquivos de configuração do Apache: /etc/apache/conf. Neste diretório haverá um arquivo com o nome “hhtpd.conf”, este é o arquivo de configuração do Apache, então edite-o utilizando o VI.

Após ter entrado no httpd.conf, procure as linhas:

```
DocumentRoot “/paginas”
DirectoryIndex index.html index.php
Include /etc/apache/mod_php.conf
```

Deixe o arquivo desta maneira, será o suficiente para que já consigamos hospedar uma página em PHP no nosso servidor web. A primeira linha “DocumentRoot” diz para o Apache qual é o diretório que colocaremos nossos scripts PHP ou HTML, no caso o diretório “/paginas” (certifique-se de ter criado o diretório). A segunda linha “DirectoryIndex” especifica que os scripts “index.html” e “index.php” serão carregados automaticamente pelo servidor

Apache sem a necessidade de digitar seus nomes. A última linha "Include" diz para o Apache para incluir o módulo do php o qual fará que o Apache interprete corretamente os scripts php q criarmos, esta linha estará comentada, é só descomentá-la, não precisa alterá-la. Dependendo da versão do kernel, pode ser que esta última linha esteja diferente, como por exemplo "Include conf/conf.d/*.module", caso esteja assim é só descomentar também, a função é a mesma.

No diretório definido como diretório raiz dos scripts (no caso o diretório /paginas) crie uma página simples só pra testar e salve-a como index.html, ou index.php, senão o Apache não conseguirá encontra-la. Depois disso vá ao modo gráfico, abra o navegador de sua preferência e digite localhost ou o endereço IP da sua placa, se aparecer a página que você criou no diretório raiz dos scripts é porque você acabou de configurar o Apache e ele ta rodando legal.

Esta configuração feita é a configuração básica para o servidor Apache rodar. Vamos fazer algumas configurações mais avançadas.

Primeira configuração adicional que faremos é para o servidor web hospedar mais de uma página (credo! Até isso o Linux faz Jesus! Queima ele Senhor!).

Entre novamente no httpd.conf e procure as seguintes linhas:

```
ServerName www.tux.com.br:80
NameVirtualHost 192.168.10.1:80
```

A primeira linha diz para o Apache qual será o nome do servidor web, no caso: www.tux.com.br o número 80 é referenta a porta TCP que o servidor Web responde (todo servidor Web responde na porta 80) A segunda linha diz para o Apache de onde virão as requisições dos clientes para acessarem as páginas do servidor web, no caso tem que ser o IP do seu servidor Web, da sua máquina.

Agora procure as seguintes linhas:

```
<VirtualHost 192.168.10.1:80>
        ServerAdmin root@tux.com.br
        DocumentRoot /paginas
        #ServerName www.tux.com.br
        ErrorLog /paginas/log/erro.log
        CustomLog /paginas/log/acesso.log common
</VirtualHost>
```

```
<VirtualHost 192.168.10.2:80>
        ServerAdmin root@sub.tux.com.br
        DocumentRoot /paginas/sub
        ServerName www.sub.tux.com.br
        ErrorLog /paginas/sub/log/erro.log
        CustomLog /paginas/sub/log/acesso.log common
</VirtualHost>
```

Deixe desta maneira as linhas, isto fará com que nosso servidor web responda pelo domínio www.tux.com.br e pelo subdomínio www.sub.tux.com.br (se quiser mudar os nomes fique a vontade). Detalhe importante: certifique-se que cada diretório especificado na configuração tenha sido criado.

Pronto, o Apache tá configurado beleza, só temos um problema, dizemos para o Apache responder pelos domínios www.tux.com.br e www.sub.tux.com.br, porém estes nomes não existem, ou seja, nosso servidor web não está configurado com estes nomes, e desta maneira vai dar pau! Então vamos configurar o nosso servidor web para responder por estes nomes, porém o Apache não faz isso, teremos que utilizar o Bind (eita lasquera!).

Servidor de Nomes - Bind

Um servidor de nomes simplesmente é um computador que responde pelo nome de um computador ou mais, sua função é atender requisições de resolução de nomes de computadores para seus respectivos IP's, para conseguir resolver o nome do computador o servidor de nomes utiliza-se do protocolo DNS. Para entender melhor isso é só você se perguntar o que acontece quando você vai no browser e digita www.brdteengal.com ou qualquer outro endereço de Internet. O que acontece é o seguinte: primeiramente sabemos que todo site é hospedado em um servidor web, um servidor web é um computador que contém uma página, ou seja, quando eu vou no browser e digito www.brdteengal.com eu estou na verdade pedindo a página que está no computador chamado www.brdteengal.com. Bom, mas como um computador pode ter um nome? Pois é, um computador pode ter nome sim, e no caso do servidor web eles sempre têm nome, já pensou se para acessar um endereço na Internet você precisasse digitar o número IP do servidor web? Simplesmente você teria que andar com uma caderneta com todos números IP's de todos sites que você costuma acessar. Diante disso, o

computador responsável por resolver o nome de um computador para IP é chamado de servidor de nomes.

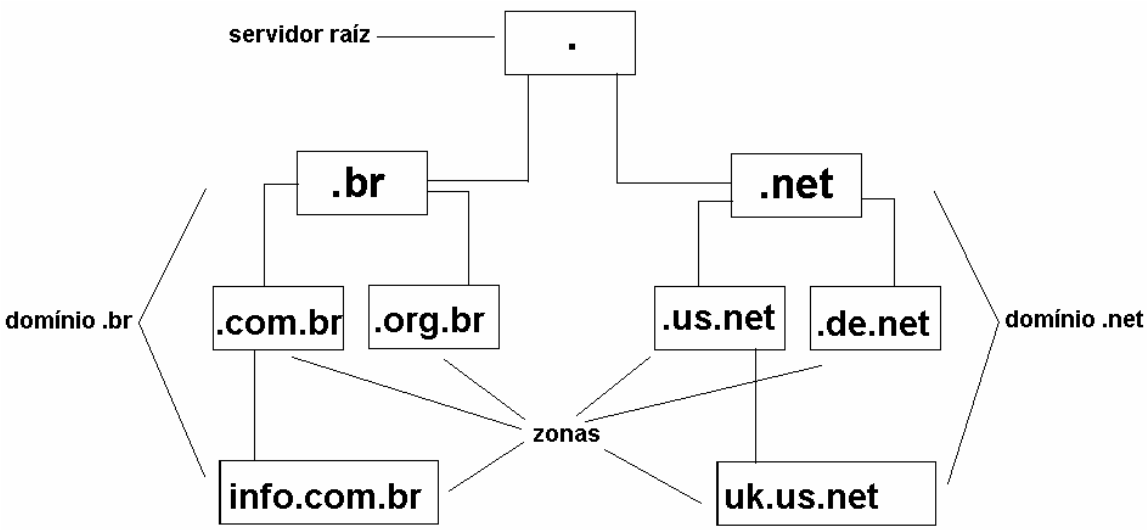
Agora devemos entender os seguintes termos: domínio, sub-domínio e zona. Abaixo as definições.

Domínio nada mais é do que o espaço que um nome abrange, neste espaço encontram-se várias zonas, por exemplo, o domínio ".br" abrange a zona ".com.br", a zona ".edu.br".

Sub-domínio é um domínio abaixo de outro domínio (vixi Maria!), por exemplo observando a zona ".com.br", o domínio ".com" é um subdomínio do domínio ".br", pois está abaixo do domínio ".br".

Zona é uma parte do domínio, por exemplo, o domínio ".br" abrange as zonas ".com.br" e ".edu.br".

Para ficar mais fácil de entender eu fiz um desenho, se você não entender aí só Deus mesmo.



Agora que já entendemos o que é um servidor de nomes, vamos entender como funciona a resolução do nome de um site qualquer, porque na verdade não é um único servidor de nomes que resolve diretamente o nome requisitado, a resolução do nome de um site envolve vários servidores de nomes. Os servidores de nomes responsáveis pela resolução do nome de um site são organizados hierarquicamente, de modo que quando a requisição da resolução do nome chega no servidor raiz, que é sempre o primeiro servidor de nomes a ser consultado, ele vai repassando a consulta para os servidores de

nomes localizados hierarquicamente abaixo, como mostra a figura acima. Os servidores de nomes na verdade são responsáveis por repassar a consulta adiante seguindo os domínios do endereço requisitado até que se chegue ao último servidor de nomes que retornará o endereço IP do servidor Web que contém a página, aí sim a página será retornada para o cliente.

Para provar isso, é só você acessar o diretório /var/named e observar o arquivo "named.ca", este arquivo contém uma lista de servidores raízes responsáveis por receber as requisições das resoluções DNS. Se este arquivo for deletado, sua Internet vai pro pau! Não altere o arquivo.

Agora vamos ao que interessa, anteriormente tínhamos configurado o Apache para responder pelos domínios www.tux.com.br e www.sub.tux.com.br, então vamos fazer as configurações necessárias para que estes nomes existam, ou seja, vamos implementar um servidor de nomes.

Acesse o diretório /etc e procure por um arquivo chamado "named.conf", esse arquivo é responsável pela especificação das zonas, como queremos criar a zona "tux.com.br" teremos que editar este arquivo e colocar nossa própria zona. Observe que já há algumas zonas especificadas, como por exemplo a zona do domínio ".", ou seja, do domínio raiz. Para criarmos nossa zona coloque as linhas abaixo ao final do arquivo named.conf:

```
Zone "tux.com.br" {
        type master;
        file "tux.ca";
};
```

Com isto estaremos criando uma zona chamada "tux.com.br", que no caso é a zona referente ao primeiro domínio que configuramos no Apache. Nas linhas acima, o principal parâmetro é o "file tux.ca;", este parâmetro define o arquivo de registro de recurso de domínio, que é o arquivo responsável pela resolução do nome "tux.com.br" para o respectivo IP do servidor Web, ou seja, no arquivo named.conf apenas configuramos a zona que existirá no servidor de nomes, mas não propriamente configuramos como será feita a resolução do nome para IP, esta resolução será feita pelo arquivo "tux.ca" como especificado nas linhas acima. Então este arquivo deve ser criado e configurado, vamos criá-lo: acesse o diretório /var/named e crie o arquivo "tux.ca", edite-o e coloque o seguinte:

```
$TTL 43200
@       IN      SOA     nomepc.tux.com.br root.tux.com.br. (
                        2005032802
                        3600
                        900
                        1209600
                        43200
                        )
@       IN      NS      nomepc.tux.com.br.
nomepc  IN      A       192.168.10.1
www IN  CNAME   nomepc
```

Pronto, salve o arquivo e agora vamos fazer as configurações finais. Entre no diretório /etc e novamente entre no arquivo named.conf, procure a seguinte linha:

listen-on {127.0.0.1/32; };

Comente esta linha para que o servidor de nomes funcione corretamente, para comentar é só colocar "//" no início da linha. Se esta linha não estiver comentada o servidor de nomes ficará atendendo as requisições pelo IP do localhost que não é o IP de onde virão as requisições dos clientes. Agora edite o arquivo resolv.conf e faça a seguinte alteração:

```
listen tux.com.br
nameserver 192.168.10.1
```

O arquivo resolv.conf é responsável pela configuração do cliente DNS, ou seja, no resolv.conf você coloca o IP do servidor de nomes responsável pela resolução do nome dos endereços que o cliente acessará, estamos configurando com o próprio IP do servidor de nomes para que consigamos no próprio servidor de nomes acessar a página do nosso servidor web, ou seja, nosso servidor web será cliente DNS dele mesmo.

Está pronto nosso servidor DNS, para ver se deu certo dê um ping no domínio que criamos: www.tux.com.br, certamente retornará os pacotes do ping o que significa lógico que deu certo. Faça outro teste: abra o Mozilla e digite o endereço e veja o que acontece, simplesmente retornará a página que hospedamos no Apache, isso porque antes de configurarmos o servidor DNS já tínhamos configurado o Servidor Web para hospedar nossa página com o domínio www.tux.com.br, concluindo: implementamos um servidor web e servidor DNS, o servidor web hospedou a página e o servidor DNS deu um nome para acessar esta página.

Para configurar as estações Windows da rede para acessarem nosso Servidor Web e DNS, basta colocá-las na mesma faixa de rede do servidor Web e DNS, configurá-las como cliente DNS do Servidor DNS, ou seja, coloque o IP do servidor DNS na estação Windows e coloque o IP do gateway como sendo o IP do Servidor DNS e Web. Depois de ter feito isso você acaba de montar uma Intranet, que simplesmente é uma Internet local, pois todas as estações Windows conseguirão acessar a página contida no Servidor Web e DNS, porém isso só funcionará na rede local, por isso o nome Intranet, que traduzindo significaria Internet Interna.

Transferência de arquivos - FTP

A melhor forma de copiar arquivos através da rede sem dúvidas é usando o protocolo FTP, e o Linux já vem com ele instalado, então vamos aprender a usa-lo.

Para acessar uma máquina remota e transferir arquivos dela para a nossa máquina local primeiro devemos nos conectar a máquina remota, para fazer isso use o comando a seguir:

ftp <IP_da_máquina_remota>
ou
ftp <nome_domínio>

Depois de conectado, será solicitados usuário e senha, caso a máquina remota aceite conexão anônima, digite “anonymous” para usuário e para senha não precisará digitar nada. Se caso você já tiver um usuário com uma senha já cadastrados na máquina remota, então digite o nome de usuário e senha.

Pronto, depois de conectar e digitar usuário e senha já estamos dentro da máquina remota, agora é só pegarmos os arquivos que queremos, então para isso use o comando “get”:

get <nome_arquivo>

Caso queira saber em qual diretório da máquina remota você se encontra use o comando “pwd”, se quiser ver os arquivos contidos nesse diretório da máquina remota use o comand “ls”. Abaixo estão relacionados alguns dos comandos úteis do ftp.

Adicionar um arquivo local a um arquivo remoto:
append <arquivo_local> <arquivo_remoto>
Terminar a sessão FTP:
bye
Mudar o diretório remoto:

cd <diretório_remoto>

Mudar permissões do arquivo remoto:

chmod <permissão> <arquivo_remoto>

Apagar arquivo remoto:

delete <arquivo_remoto>

Mudar o diretório da máquina local:

lcd <diretório_local>

Pegar vários arquivos na máquina remota:

mget <arquivos_remotos>

Ex: mget *.txt

Abrir uma conexão com uma máquina remota:

open <IP_da máquina_remota>

Ou

open <nome_domínio_máquina_remota>

Transferir um arquivo local para a máquina remota:

put <arquivo_local>

ou

send <arquivo_local>

Deletar um diretório da máquina remota:

rmdir <diretório>

Ver o SO da máquina remota:

system

Bom, caso você queira configurar seu servidor FTP da sua máquina, utilize o Linuxconf. Dentro do Linuxconf entre em "Configuração-Rede-Tarefas de servidor-Wu FTP-Servidor de FTP", neste local você poderá definir, por exemplo, se seu servidor FTP aceitará login anônimo ou não, poderá controlar também os usuários que poderão acessar seu servidor FTP entre outras configurações, é só seguir os menus que não tem erro.

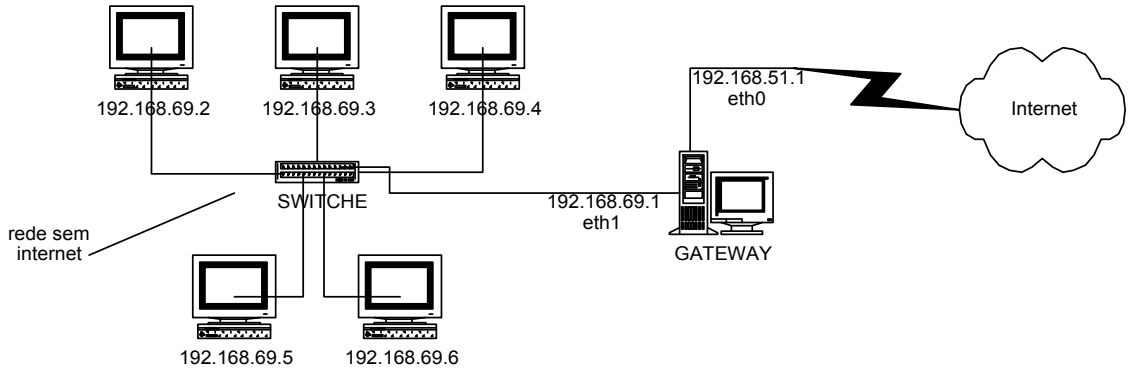
Firewall - IPTABLES

O iptables é um firewall assim como ipchains, a diferença é que o ipchains só há em linux com kernel 2.4 ou inferior e o iptables em linux kernel acima de 2.4. Um firewall é um software (ou pode ser um hardware também) que simplesmente filtra pacotes TCP-IP da rede, ele deixa pacotes passarem ou não, tudo depende de sua configuração, assim você pode dizer que todos os pacotes que vierem do host 192.168.7.69 sejam negados, por exemplo.

No nosso exemplo de compartilhamento de internet via firewall utilizaremos também um “gateway”, mas que droga é essa de “gateway”? Pois é, gateway é um negócio que simplesmente faz ligação de duas redes diferentes, por exemplo: se um computador tem duas placas de rede, sendo que uma conectada à rede 192.168.5.0 e a outra à rede 192.168.6.0 e este computador possibilita que as duas redes repassem pacotes entre si, este computador é um gateway.

Muito bem, vamos montar o compartilhamento de internet.

Vamos partir do princípio que temos um computador com duas placas de rede: eth0 e eth1, lógico, sendo que a placa de rede eth1 está conectada a uma rede que não tem internet e a outra placa de rede eth0 está conectada a uma outra rede que já tem internet, nesse caso este computador será o nosso gateway entre as duas redes, nosso objetivo é compartilhar a internet da placa eth0 para a outra rede através da placa eth1. Vamos dar IP a estas redes: a rede que não tem internet vamos dar o IP 192.168.69.0 e a rede que tem internet vamos dar o IP 192.168.51.0. Vamos também atribuir o IP 192.168.69.1 para eth1 e 192.168.51.1 para eth0. Desenhando nosso esquema fica mais ou menos como descrito abaixo:



Ah! Você não tem duas placas de rede? Seus problemas se acabaram-se! Chegou o Sistema Operacional Linux onde você poderá configurar sua única placa de rede para ter dois IP’s! (Linux não é de Deus! Queima ele Jesus!). Para configurar sua placa de rede para ter um segundo IP é só fazer o seguinte:

ifconfig eth0:0 192.168.69.1 netmask 255.255.255.0 up

Pronto, você acaba de adicionar o IP 192.168.69.1 à sua placa de rede, digite ifconfig e você verá que ela aparecerá logo abaixo do primeiro IP (Cruiz credo!).

Antes de partirmos para a implementação do firewall temos que entender algumas particularidades do protocolo TCP/IP:

O protocolo TCP/IP é o padrão de comunicação da Internet, até aí é fácil, talvez o que você não sabia ainda é que na verdade o padrão de comunicação da Internet é composto por vários protocolos (tcp, udp, http, ftp, dns, smpt, etc). O nome TCP/IP foi dado porque o TCP e o IP são os dois principais protocolos do padrão de comunicação da Internet, porém agora sabemos que não são somente os dois que fazem parte do padrão de comunicação das redes. Outro detalhe importante é o que cada serviço (ftp, http, dns, etc) tem uma porta de identificação específica, esta porta simplesmente é uma maneira de organizar cada serviço, de identificar cada serviço por um número (não vá tentar achar uma porta atrás do seu gabinete, pelo amor de Deus!). Mais outro detalhe importantíssimo é que além de cada serviço ter sua porta específica eles também tem um tipo que no caso é TCP ou UDP, quando o protocolo é do tipo TCP ele é orientado à conexão quando é do tipo UDP não é orientado à conexão, se for orientado a conexão significa que a entrega do pacote (datagrama) ao seu destino é garantida (como se fosse uma carta registrada) e se caso o protocolo for do tipo UDP significa que a entrega do datagrama não é garatinda (como uma carta simples). Minha nossa sinhora da bicicreta! Agora lascou tudo né? Calma, não se desespere, vai ficar mais complicado ainda. Abaixo uma lista dos principais protocolos, suas portas e seu tipo:

http:80/TCP
dns:53/UDP
ftp:21/UDP
ssh:22/UDP
telnet:23/UDP
smtp:25/UDP
pop3:UDP

Então, não esqueça: O padrão TCP/IP é composto por vários protocolos, cada protocolo tem sua porta específica e tipo.

Agora que entendemos o TCP/IP e suas particularidades, vamos ao trabalho então, inicialmente vamos colocar as regras padrão para o iptables fechar todas as portas, o que é o correto, pois é muito mais fácil fechar todas as portas, isolar o computador e depois ir abrindo as portas aos poucos. Entre no VI e digite o seguinte:

```
# fechando tudo
iptables -F
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

Salve o arquivo com o nome firewall e depois dê permissão de execução e execute-o (é só digitar ./firewall).

Pronto, seu firewall tá rodando, o que será que aconteceu? Faça o seguinte, pingue no seu próprio IP e veja o que acontece. Pois é, operação não permitida, porquê? Bom, simplesmente porque as regras que acabamos de colocar no firewall vão fechar todas as portas, seu computador tá super protegido, protegido até dele mesmo! Porque fizemos isso? É exatamente por causa do que definimos anteriormente "é mais fácil fechar todas as portas e depois ir abrindo-as aos poucos". Vamos entender as regras digitadas:

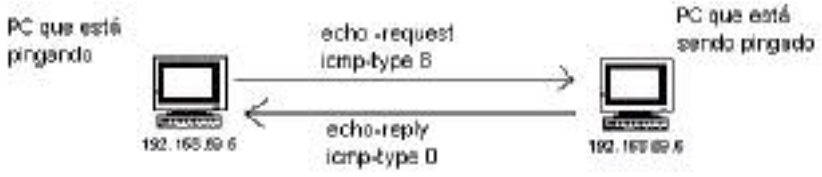
iptables –F : limpa todas as regras de firewall anteriores;

iptables –P FORWARD DROP : adiciona uma regra padrão para bloquear tudo que entra e sai (sem malícia) da placa de rede;

iptables –P INPUT DROP : adiciona uma regra para bloquear tudo que entra na placa de rede;

iptables –P OUTPUT DROP : adiciona uma regra que bloqueia tudo que sai da placa de rede;

Mas não é isso que queremos, queremos proteger nosso computador, mas também não queremos que ele se isole como se não tivesse placa de rede, queremos que ele pingue nele mesmo, nos computadores da sua própria rede e é claro, queremos que ele acesse a internet. Então, vamos liberar os protocolos necessários para que isso funcione, primeiramente vamos liberar os protocolos necessários para que nosso próprio computador pingue nele mesmo. Os protocolos que temos que liberar para que o computador pingue nele mesmo é o ICMP (Internet Control Message Protocol), este protocolo é utilizado toda vez que você dá um pingue em algum computador, e este protocolo tem dois tipos: o tipo 8 e o tipo 0. O ICMP do tipo 8 é utilizado para echo-request e o ICMP do tipo 0 é utilizado para echo-reply, o echo request é enviado pelo computador que está pingando para o computador que está sendo pingado como uma pergunta se o computador está ativo ou não e o echo-reply é enviado pelo computador que está sendo pingado para o computador que enviou o echo-request como uma resposta se está ativo ou não. Desenhando é mais ou menos o seguinte:



Diante disso, concluímos o seguinte:

Dois pacotes ICMP's estão envolvidos no ping: um ICMP do tipo 8 e um ICMP do tipo 0;

O PC que está pingando no outro PC envia um pacote ICMP do tipo 8;

O PC que está sendo pingado recebe o pacote ICMP do tipo 8;

O PC que está sendo pingado, em resposta ao pacote ICMP do tipo 8, envia um pacote ICMP do tipo 0 para o PC que está pingando nele;

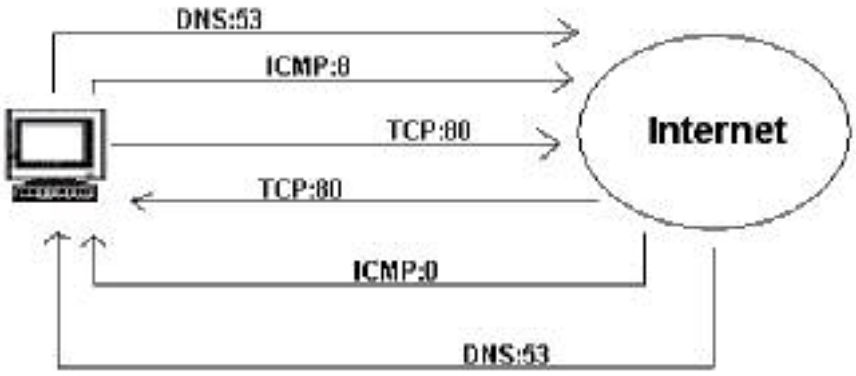
O PC que está pingando recebe o pacote ICMP do tipo 0;

Agora, vamos raciocinar o seguinte: se queremos que nosso próprio PC pingue nele mesmo, então ele enviará um pacote ICMP do tipo 8 para ele mesmo, ele mesmo receberá o pacote ICMP do tipo 8, ele mesmo enviará o pacote ICMP do tipo 0 e ele mesmo receberá o pacote ICMP do tipo 0. As regras que temos que colocar no nosso firewall têm que permitir que tudo isso aconteça, então vamos às regras:

```
iptables -A OUTPUT -p icmp -s 192.168.51.1 -d 192.168.51.0/24 --icmp-type 8 -j ACCEPT
iptables -A INPUT -p icmp -s 192.168.51.1 -d 192.168.51.0/24 --icmp-type 8 -j ACCEPT
iptables -A OUTPUT -p icmp -s 192.168.51.1 -d 192.168.51.0/24 --icmp-type 0 -j ACCEPT
iptables -A INPUT -p icmp -s 192.168.51.1 -d 192.168.51.0/24 --icmp-type 0 -j ACCEPT
```

Beleza, salve e saia do arquivo e dê um ping no seu IP para ver se deu certo. Agora faça o seguinte teste: tente acessar a Internet, com certeza não vai acessar, isso porque também temos que liberar a Internet via firewall. Antes de liberarmos a Internet vamos entender como funciona o processo de acessar a Internet no seu computador:

No acesso a Internet três protocolos estão envolvidos: DNS, ICMP e HTTP. O DNS é um pacote UDP que responde na porta 53, o ICMP como já dito anteriormente é do tipo 8 e 0 e o HTTP é um pacote do tipo TCP que responde na porta 80. Vixi Maria! Complicou né? Então eu desenho de novo:



Como mostra o desenho, primeiramente o computador que está acessando Internet envia um pacote do tipo UDP na porta 53:DNS para servidor DNS do site solicitando a resolução do nome do site, depois a servidor DNS envia um pacote UDP na porta 53:DNS para o computador que está acessando a Internet com o nome resolvido, com o endereço IP do servidor Web que contém a página, depois disso o computador que está acessando a Internet envia um pacote ICMP do tipo 8 para o servidor Web para saber se ele está ativo e então o servidor Web responde com pacote ICMP do tipo 0 dizendo que está ativo, por último o computador que está acessando a Internet envia um pacote do tipo TCP na porta 80:HTTP para o servidor Web requisitando a página, então o servidor Web responde com um pacote TCP na porta 80:HTTP contendo a página solicitada. Legal né? É isso que acontece quando você está simplesmente acessando uma página da Internet, e você nem sabia.

Diante disso, vamos liberar os protocolos necessários para que a Internet então funcione:

```
iptables -A OUTPUT -p udp -s 192.168.51.1 -d 0/0 --dport 53 -j ACCEPT
iptables -A INPUT -p udp -s 0/0 -d 192.168.51.1 --sport 53 -j ACCEPT
iptables -A OUTPUT -p icmp -s 192.168.51.1 -d 0/0 --icmp-type 8 -j ACCEPT
iptables -A INPUT -p icmp -s 0/0 -d 192.168.51.1 --icmp-type 0 -j ACCEPT
iptables -A OUTPUT -p tcp -s 192.168.51.1 -d 0/0 --dport 80 -j ACCEPT
iptables -A INPUT -p tcp -s 0/0 -d 192.168.51.1 --sport 80 -j ACCEPT
```

Agora é só salvar e sair e executar o firewall, depois acesse a Internet que vai estar funcinando legal.

Vamos fazer um compartilhamento de Internet para uma rede interna:

```
iptables -A FORWARD -p udp -s 192.168.69.0/24 -d 0/0 --dport 53 -j ACCEPT
```

```
iptables -A FORWARD -p udp -s 0/0 -d 192.168.69.0/24 --sport 53 -j ACCEPT
iptables -A FORWARD -p icmp -s 192.168.69.0/24 -d 0/0 --icmp-type 8 -j ACCEPT
iptables -A FORWARD -p icmp -s 0/0 -d 192.168.69.0/24 --icmp-type 0 -j ACCEPT
iptables -A FORWARD -p tcp -s 192.168.69.0/24 -d 0/0 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -s 0/0 -d 192.168.69.0/24 --sport 80 -j ACCEPT
```

Pronto, com isso estaremos compartilhando Internet para a rede 192.168.69.0. Implementamos um firewall que faz compartilhamento de Internet, para fazer as estações acessarem Internet através do firewall é só colocá-las na rede 192.168.69.0 e configurá-las com gateway igual ao IP da placa de rede de onde sai o compartilhamento: 192.168.69.1.

Servidor Proxy – Squid

Vamos a definição de proxy: segundo os conceitos do professor Jorgeley, proxy é um maravilhoso software que faz compartilhamento de internet, mas não só isso, ele faz serviço de cache de páginas e também tem controle de acesso, assim podemos definir quais usuários poderão acessar a internet e quais sites serão permitidos, além disso, como foi dito ele faz serviço de cache que simplesmente é uma maneira que o proxy armazena páginas acessadas pelos usuários no próprio servidor proxy, sendo assim da segunda vez que um usuário tente acessar uma página já visitada por outro usuário, esta página não será novamente buscada na internet, ela será entregue ao usuário rapidamente, pois a mesma se encontra no cache do servidor proxy. Imagine o ganho no desempenho da rede quando implementamos um servidor proxy, agora você com certeza entende porque eu disse que o proxy é uma maravilha!

Agora que nos encantamos com o Squid, vamos implementa-lo. Certifique que o Squid esteja instalado, os pacotes a serem instalados são todos que iniciem com a palavra “squid-“, então basta instalar usando o comando:

```
rpm –ivh squid-*
```

Depois de instalado, vamos configura-lo. Configuraremos o squid de maneira que ele compartilhe internet para uma rede qualquer e faça bloqueio de páginas indesejáveis através de palavras chave.

O arquivo de configuração do Squid é o “/etc/squid/squid.conf”, entre nesse arquivo e procure as seguintes linhas:

```
cache_ram MEM 8 MB
```

esta linha está especificando a quantidade de RAM que o squid poderá usar, é bom aumentar, mas tome cuidado para não especificar toda a RAM da máquina, pois existem outros processos que também precisam de RAM.

cache_dir ufs /var/spool/squid 100 16 256

esta linha especifica o diretório que será o diretório de cache do Squid, ou seja, onde ele guardará as páginas acessadas pelos usuários, que no caso acima é o diretório "/var/spool/squid". Especifica também a maneira que será guardada as páginas no diretório "ufs". O número 100 especifica o tamanho máximo do cache. O número 16 indica a quantidade de diretórios que poderão ser criados pelo cache do Squid e o número 256 indica a quantidade de subdiretórios que cada um dos 16 diretórios poderão ter. Fique a vontade para mudar estes valor, mas sempre tome cuidado com essas alterações.

http_port 3128

Nessa linha está indicada qual porta o Squid utilizará, não é necessário mudar.

Essas são as configurações básicas do Squid, agora vamos fazer as configurações para que restrinjamos o acesso a alguns sites. Para fazermos isso teremos que criar algumas ACL's, então procure no squid.conf as linhas onde ficam as ACL's e adicione a nossa própria ACL:

```
acl rede_permitida src 192.168.69.0/255.255.255.0
acl sites_proibidos url_regex –i sexo
```

Agora procure as linhas onde contem as regras de acesso e mude-as para o seguinte:

```
http_access deny sites_proibidos
http_access allow rede_permitida
http_access deny all
```

Pronto, o arquivo de configuração do Squid já está ok, agora vamos iniciar o Squid e ver se funciona. Para inicia-lo basta ir ao diretório dos dispositivos inicializáveis e digitar:

```
squid –z
squid start
```

Para ver se realmente funcionou, tente acessar no servidor Squid mesmo uma página pornô, ou outra que tenha a palavra "sexo" que proibimos pelo squid, caso você não consiga ver a página é porque o Squid a bloqueou, ou seja, deu certo!

Nas máquinas que você quer compartilhar a internet do servidor Squid é só configura-las com proxy=IP do servidor Squid e porta=3128 que foi a porta

especificada no squid.conf. Depois de fizer isso nas máquinas clientes do servidor Squid, certamente elas vão estar acessando a internet, porém com o detalhe de não conseguirem ver as páginas que contenham a palavra "sexo".

Vamos fazer uma configuração adicional agora, vamos fazer um controle de usuário, ou seja, para acessar Internet nas estações Windows o usuário terá que digitar um nome de usuário e senha válidos.

Entre novamente no squid.conf e procure a seguinte linha:

authenticate_program ...

Deixe-a da seguinte maneira:

authenticate_program /usr/bin/ncsa_auth /etc/squid/usuarios

Desta maneira estamos configurando o squid para fazer o controle de usuários utilizando o programa de autenticação "ncsa_auth" (próprio do linux) e ainda configuramos dizendo que o arquivo com os usuários será o "usuarios" e ficará no diretório /etc/squid. Detalhe: ainda não colocamos o "ncsa_auth" no diretório correto e muito menos criamos o arquivo com os usuários, faremos isso depois. Agora vá até onde encontram-se as ACL's e coloque a seguinte ACL:

acl autentica proxy_auth REQUIRED

Depois vá até a linha onde encontram-se as regras de acesso e coloque o seguinte:

http_access allow autentica

Pronto, o squid.conf ta configurado, agora é só colocarmos o "ncsa_auth" no diretório correto e adicionarmos os usuários. Vá até o diretório /usr/doc/squid, neste diretório você encontrará o "ncsa-auth", copie-o para o diretório /usr/bin. Beleza, agora vá até o diretório /etc/squid e digite o seguinte comando:

htpasswd –c /etc/squid/usuarios Juliana

Este comando irá criar o arquivo "usuarios" e já adicionará o usuário Juliana para poder acessar Internet. Depois se quiser adicionar mais usuários

não precisa mais colocar o parâmetro –c, apenas digite "htpasswd /etc/squid/usuarios nomeusuario".

Pronto, agora é só reiniciar o squid, para isso digite "ps –aux" para listar os processos que estão rodando, com certeza o squid estará na lista e aí é só matar os processos, digite "killall squid" que isto resolverá. Depois é só iniciar de novo o squid: "squid start".

Nas estações tente acessar Internet, você verá que quando abrir o browser será solicitado usuário e senha, obrigatoriamente você terá que informar um dos usuários cadastrados no servidor Proxy.

Legal né, o squid tem outras configurações adicionais, porém essas são as principais, não precisa mais que isso.

Sendmail

O sendmail é um software do linux que envia e recebe mensagens usando a rede.

Verifique se o mesmo está instalado, caso não estiver instale-o e siga os passos adiante para configura-lo. Além de instalar o sendmail é necessário instalar também o POP3.

1 - entrar no /etc e editar o arquivo sendmail.cw
   curso.com.br RELAY
   192.168.4 RELAY
   localhost.localdomain RELAY
2 - acessar o path /etc/mail e criar o arquivo relay-domains
   localdomain
   curso.com.br
   192.168.4
3 - acessa o path /etc/services e confira as portas 25 e 110
4 - edita o arquivo /etc/inetd.conf e descomente a linha do pop3
5 - entre no ntsys e habilite o pop3 e sendmail
6 - acesse o path /etc/mail/sendmail.cf
   localize a linha DM e adicione -> DMcurso.com.br
7 - execute o linuxconf - REDE - SENDMAIL -

Para enviar uma mensagem o melhor a fazer é utilizar o próprio software do sendmail, basta digitar sendmail na linha de comando. Caso preferir utilize o comando:

mail <usuário>

O arquivo /var/log/maillog contém todos os logs de e-mail

Para verificar as mensagens vá ao diretório /var/spool/mail ou então utilize o comando:

mail -f <usuário>

IPTRAF

IPTRAF é um software que permite o gerenciamento do tráfego em um servidor.

Para usufruí-lo, instale-o e digite na linha de comando apenas IPTRAF.

Depois de digitar o comando é só seguir os menus.

DIRETÓRIOS

/bin: Armazena os binários (executáveis) dos comandos do Linux
/boot: Os arquivos utilizados na inicialização estão nesse diretório
/dev: Armazena todos os arquivos de dispositivos, mouse, HD, portas, etc.
/etc: Aqui se encontram todos os arquivos de configuração
/home: Este é o diretório local, como se fosse a pasta “Meus Documentos” do Windows.
/mnt: Neste diretório estão os pontos de montagem de dispositivos de armazenamento
/usr: A maioria dos softwares fica neste diretório
/var: Armazena informações diversas, logs, variáveis entre outros.

ANEXO I

Autenticando Windows XP no LINUX PDC

Publicado em 28 de setembro de 2004

Neste tutorial o Carlos Gomes (carloshgomes@hotmail.com) mostra de forma simples e objetiva como autenticar um Windows XP no Samba visto que o mesmo requer uma configuração a mais que família Windows 98.

Autenticando Windows XP no LINUX PDC

Por Carlos Gomes (CH) (carloshgomes@hotmail.com).

Primeiramente, verifique se ambas as máquinas (servidor e estação) estão corretamente configuradas para rede: Interface conectadas, configuradas corretamente com seus drivers, cabos conectados e funcionando, etc.

Após verificado, vamos ao servidor configurar o SAMBA.

Certifique-se que seu arquivo “smb.conf” contém os seguintes parâmetros:

[global]

encrypt passwords = Yes
domain logons = yes
logon drive = H: {aqui é a pasta home do usuário conectado, será mapeado na unidade H, dentro do seu explorer, somente usado para windows xp,200,nt}

Configurando a máquina Windows XP para autenticar no Domínio

Digamos que sua máquina seja chamada de “cliente”, sem as aspas duplas, é claro :)
Crie uma conta de máquina no arquivo /etc/passwd, basta executar o seguinte comando, como root:

useradd -g domainmac -c "Maquina de Dominio" -s /bin/false -d /dev/null cliente$

O comando acima cria uma conta para a máquina cliente$ e torna ela parte do grupo domainmac. É necessário especificar o caracter $ após o nome da máquina para criar uma conta de máquina no domínio, caso contrário o próximo passo irá falhar.

Crie uma conta de máquina no arquivo /etc/samba/smbpasswd, basta executar o seguinte comando, como root:

smbpasswd -m -a cliente

Isto cria uma conta de máquina para o computador cliente no arquivo /etc/samba/smbpasswd. Note que a criação de uma conta de máquina é muito semelhante a criação de um usuário apenas precisa adicionar a opção -m. Quando for criar uma conta com o smbpasswd não é necessário especificar $ no final do nome da máquina.

Após isso, vamos para o Windows XP

1) Logue-se como administrador ou com direitos de administrador.

Primeiramente, vamos adicionar a máquina ao grupo de trabalho, seguindo estes passos:

2) Logue como administrador do sistemas local.

3) Entre no item Sistema dentro do painel de controle. A tela propriedades de sistema será aberta.

4) No campo Descrição do Computador, coloque algo que descreva a máquina (opcional).

5) Clique na TAB Nome do Computador e no botão Alterar na parte de baixo da janela.

6) No campo nome do computador, coloque um nome de no máximo 15 caracteres para identificar a máquina na rede. Como exemplo criamos a máquina CLIENTE.

7) Clique em grupo de trabalho e digite o nome do grupo de trabalho na caixa de diálogo. Aquele que você criou na seção [global] do SAMBA.

8) Clique em OK e aguarde a mensagem confirmando sua entrada no grupo de trabalho. Será necessário reiniciar a máquina.

Após, sucesso, vamos agora cadastrar para entrar no domínio, vejamos como

9) Atualize o registro para permitir a entrada no domínio. Vá em:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netlogon\parameters

e modifique os seguintes parâmetros:

"RequireSignOrSeal"=dword:00000000
"SignSecureChannel"=dword:00000000

10) Após, vá em painel de controle/ferramentas administrativas/diretiva de segurança local/diretivas locais/opções de segurança. Lembre-se de estar como administrador:

11) Desative os seguintes parâmetros, para uma busca mais rápida identifique as linhas começando com:

Membro de domínio

desativando as linhas seguintes:

Membro de domínio: criptografar ou assinar digitalmente os dados de canal seguro (sempre)

Membro de domínio: desativar alterações de senha de conta da máquina

Membro de domínio: requer uma chave de sessão de alta segurança (Windows 2000 ou posterior)

após feito isto feche a tela

12) Reinicie a máquina.

13) Após reiniciar a máquina, volte na tela de alteração de identificação de máquina na rede.

14) Clique com o mouse em "Domínio" e digite o nome do domínio na caixa de diálogo.

15) Na tela seguinte, será lhe pedido o nome de usuário e senha. Entre com o root e senha do root. Ah, lembre-se de cadastrá-lo no samba: smbpasswd -a root

16) Clique em OK e aguarde a mensagem confirmando sua entrada no domínio. Será necessário reiniciar a máquina após concluir este passo.

17) Pronto agora na tela de autenticação, clique em opções para escolher o domínio de sua rede. Escolha um usuário já cadastrado no Linux e no samba.

:)

Algumas observações:

1 – Tive que adicionar o usuário ao meu samba novamente, pois não estava funcionando sem fazer isso. Ex:
smbpasswd -a usuario
Após isso funcionou perfeitamente :)

2 – Criei o perfil alterando os formatos do windows xp e no próximo login tudo estava como antes :) , ou seja, carregou o perfil perfeitamente.

Alguns trechos aqui presentes, foram adaptados ou copiados:

Guia Foca GNU/Linux

Versão 6.38 - quinta, 19 de agosto de 2004

http://focalinux.cipsga.org.br/

by CH. :)

Autor: Carlos Gomes (CH)
Email: carloshgomes@hotmail.com
Postado por fuji em setembro 28, 2004 10:57 AM