Capítulo 9

Administração de redes

- Usuários e grupos no Windows
- Usuários e grupos no Linux
- Acesso remoto via rede
- Acesso remoto via rede no Linux
- Acesso remoto via rede (modo texto)
- Virtualização de computadores
- Instalando novos sistemas operacionais em máquinas virtuais
- Servidor DHCP
- Servidor Proxy
- Servidor de arquivos

Os sistemas operacionais têm papel importante nas redes de computadores. São eles os responsáveis pelo cadastramento dos serviços, das aplicações e dos usuários da rede. É possível aproveitar ao máximo os recursos desses sistemas na administração de redes.

9.1. Usuários e grupos no Windows

O gerenciamento de usuários e grupos no Windows é uma tarefa que, geralmente, é deixada de lado quando se trata de computadores de usuários domésticos. No entanto, o assunto ganha importância quando se fala em um servidor de rede. Vamos então aprender a criar usuários e grupos no Windows Vista para poder controlar o que cada um faz em nosso computador. Depois separamos os arquivos e as configurações de cada usuário do sistema.

9.1.1. Criando novos usuários no Windows Vista

Para criar um novo usuário no Vista, acesse o Painel de Controle e clique no link "Contas de usuário". Aparecerá a tela mostrada na figura 248.

Clique em "Adicionar ou remover contas de usuário" para gerar, por exemplo, uma conta para que seu irmãozinho possa utilizar o computador, ter arquivos separados dos seus e até seu próprio papel de parede.

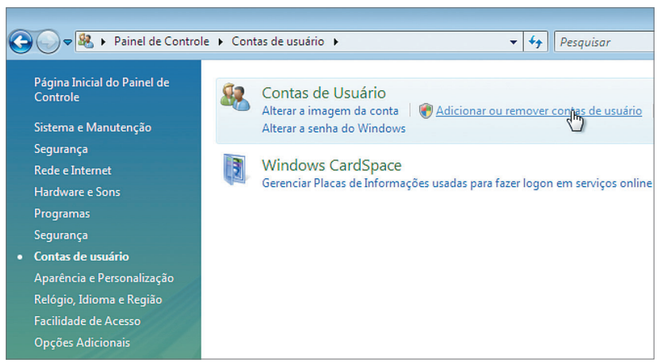


Figura 248
Painel de controle / Contas de Usuário.

Figura 249
Visualização de contas já existentes.

Clique no link "Criar uma nova conta" para ver as telas da figuras 249 e 250.

Digite o nome do usuário ou uma palavra que representa a pessoa que irá utilizar essa conta e escolha seu tipo. Pode ser "Usuário padrão" (comum) ou "Administrador". O ideal é colocar seu irmãozinho como usuário comum, o que lhe dará permissões mínimas para alterar as configurações do computador. Clique em "Criar conta" para finalizar, como está na figura 250.

Pronto. Você tem mais uma conta. As imagens que aparecem na tela representam os usuários cadastrados em seu PC. A conta de "Convidado" é criada pelo Windows Vista, segundo padrão do sistema operacional. Clique na imagem "Ir-

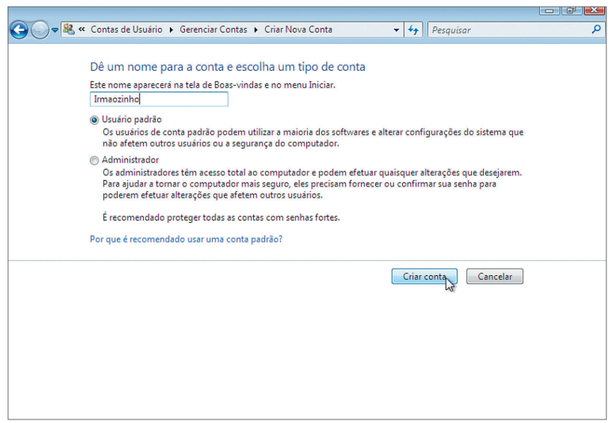


Figura 250
Criação de uma nova conta.

Figura 251
Gerenciando contas.

mãozinho", para alterar a figura apresentada na tela de boas-vindas do Windows Vista e na tela de logon, aquela que solicita a escolha do usuário quando ligamos o computador (figura 251). Escolha a imagem que melhor representa o seu irmãozinho e clique em "Alterar imagem" (figura 252).

Quando você reiniciar o computador, verá que uma tela de login, como a da figura 253, será apresentada antes que a área de trabalho do usuário apareça.

9.1.2. Criando novos grupos no Windows Vista

O conceito de grupos em um sistema operacional está fortemente ligado a questões de segurança da rede e do próprio sistema. É conveniente, portanto, criar grupos para distinguir conjuntos de usuários que tenham características em comum. Assim poderemos restringir o acesso desse grupo a determinado recurso ou área. Por ser um sistema operacional desenvolvido para estações de trabalho, o Windows Vista tem recursos de gerenciamento de grupos de usuários ocultos e bastante limitados. Já um sistema desenvolvido para servidores, como o Windows Server, tem poderosos recursos para essa finalidade e que ficam disponíveis para que o administrador do sistema possa tomar decisões a respeito e definir permissões.

Em uma escola, por exemplo, pode-se criar um grupo de usuários "Professores" e outro grupo "Alunos" para diferenciar o que cada um pode ou não fazer. Tra-

Figura 252
Escolha de uma imagem para o usuário.

Figura 253
Tela de login do Windows Vista.

balhar com grupos também facilita a administração das permissões. Isso porque, ao adicionar uma nova impressora, por exemplo, não será necessário atribuir permissão a cada usuário professor; basta adicioná-la para o grupo "Professores".

9.2. Usuários e grupos no Linux (modo gráfico e texto)

Quanto ao gerenciamento do Linux podemos trabalhar tanto no modo texto quanto no gráfico. O mesmo vale para a criação e manipulação de usuários. É possível fazer o gerenciamento de usuários e grupos, contando com os mesmos recursos, tanto nas distribuições com interface gráfica quanto nos servidores que têm somente interface de modo texto. Vale, então, aprender a criar usuários, grupos e privilégios no Linux.

No modo gráfico

O primeiro passo é criar um novo usuário do Linux pelo Gnome, que é a interface gráfica padrão do Ubuntu. Para fazer isso, clique no menu Administração / Usuários e Grupos (figura 254).

Figura 254
Utilitário de gerenciamento de usuários e grupos do Ubuntu.

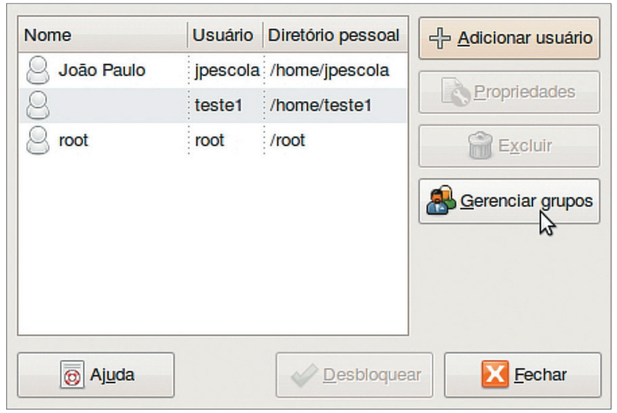
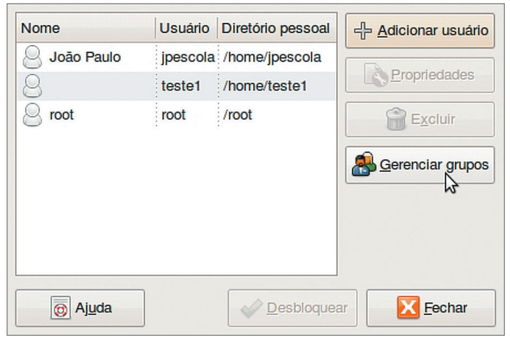


Figura 255
Adicionando um novo usuário no sistema operacional.



Como essa providência é função do administrador do sistema, é preciso clicar em "Desbloquear" para que os botões necessários fiquem ativos. Será solicitada a sua senha de usuário comum, como mostra a figura 255.

Agora clique em "Adicionar usuário" e, depois, em "Gerenciar grupos". Vamos escolher a primeira opção para criar um usuário "Aluno" pelo gerenciador gráfico do Ubuntu. À esquerda há uma relação dos usuários já cadastrados no sistema.

Quando clicamos no botão "Adicionar usuário", aparecerá na tela a janela mostrada na figura 256. Digite o login do usuário (nome que ele usará para acessar o sistema) e o seu nome completo (nome real), que aparecerá formalmente no canto superior direito da área de trabalho quando ele "logar" o sistema.

Observe que no item "Perfil" podemos escolher o tipo de usuário que será criado (consulte o quadro "Tipos de usuário" na página 187).

Digite também uma senha para o usuário e clique na aba "Contatar" para digitar os dados pessoais do usuário, como endereço e telefone. Esses dados não são obrigatórios.

Figura 256
Preenchendo os dados do usuário.

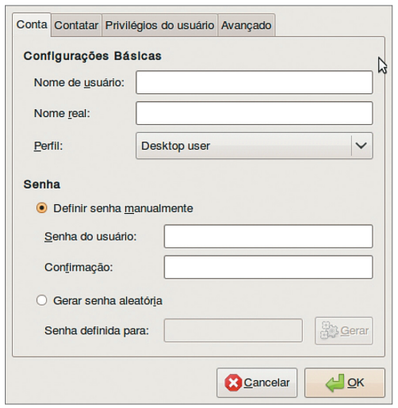
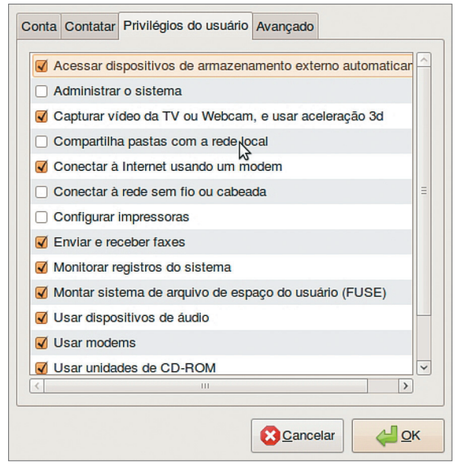


Figura 257
Privilégios do usuário.



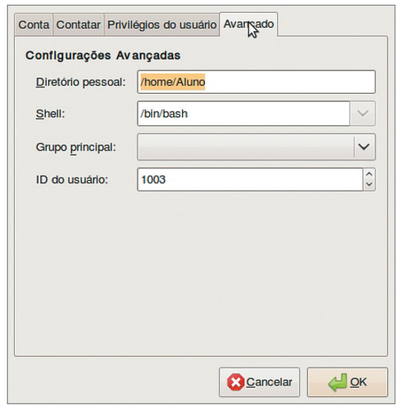
Na aba "Privilégios do usuário", você pode habilitar e desabilitar permissões para o usuário. É possível impedi-lo de usar recursos do sistema, como o drive de CD, por exemplo (figura 257).

Na aba "Avançado" ainda é possível alterar a pasta do usuário. Mesmo que, por padrão, ela fique em "/home", você pode criá-la em qualquer lugar, já que é o administrador do sistema (figura 258).

9.2.1. Criando novos usuários e grupos no Linux (modo texto)

Existem diversos comandos para gerenciar, criar ou excluir usuários e grupos no terminal do Linux. Para criar um usuário, podemos utilizar o comando "adduser", passando, como parâmetro, o nome do usuário. Por exemplo, "professor". Lembre-se de que, antes, é preciso dar o comando "sudo".

Figura 258
Finalizando o cadastro do usuário.



TIPOS DE USUÁRIO

Desktop user (usuário de desktop): com algumas restrições no sistema.
Administrador: com permissão total e irrestrita a todos os componentes do sistema.
Unprivileged user (usuário sem privilégios): comum, não consegue digitar comandos com "sudo".

Figura 259
Adicionando o usuário professor.

```
Arquivo  Editar  Ver  Terminal  Ajuda
jpescola@jpescola-laptop:~$ sudo adduser Professor
adduser: Por favor, insira um nome de usuário que se adeque à expressão regular
configurada
através da variável de configuração  NAME_REGEX[_SYSTEM] . Use a opção '--force-
badname'
para evitar essa verificação ou reconfigure NAME_REGEX ou NAME_REGEX_SYSTEM.
jpescola@jpescola-laptop:~$ sudo adduser professor
Adicionando o usuário `professor' ...
Adicionando novo grupo `professor' (1002) ...
Adicionando novo usuário `professor' (1001) ao grupo `professor' ...
Criando diretório pessoal `/home/professor' ...
Copiando arquivos de `/etc/skel' ...
Digite a nova senha UNIX:
```

Veja que o sistema vai criar um usuário com o nome informado, um grupo com o mesmo nome e a pasta pessoal do usuário na pasta "/home" (figura 259).

Depois de criar o usuário, será solicitada a senha inicial dessa pessoa (figura 260).

Após digitar e redigitar a senha do usuário, serão solicitadas informações pessoais, como nome completo, telefone etc. E aparecerá uma mensagem de confirmação no final. Pressione "Enter" para concluir a operação.

A partir de agora, temos o usuário "professor" para logar a máquina. Esse usuário foi criado com privilégios restritos, ou seja, não pode digitar comandos com "sudo". Para que isso seja possível, precisamos alterar as configurações do arquivo "/etc/sudoers". Esse arquivo armazena os nomes dos usuários que podem executar comandos como administrador (figura 261).

Você pode abrir o arquivo utilizando o gedit, por exemplo, e adicionar o nome do usuário recém-criado – "professor". Assim, esse usuário poderá digitar comandos com "sudo" e alterar as configurações do computador como se fosse um administrador. Para isso, basta utilizar a mesma sintaxe da linha "root ALL=(ALL) ALL" para o usuário "professor".

Ao analisar o código do arquivo sudoers, você chegará à conclusão de que também é possível atribuir permissões de administrador a um grupo. Na última linha do arquivo, aparecerá o caractere % representando um grupo. Isso significa que os membros do grupo "admin" também podem executar comandos como administrador por meio do padrão no Ubuntu.

DICA

Para excluir um usuário, use o comando "userdel" ou "userdel -r". Este último excluirá também a pasta pessoal do usuário. Para logar no Linux com o novo login, pressione CTRL+ALT+F1 a F6 para abrir um "tty" e digite o novo usuário e sua senha.

Figura 260
Finalizando o cadastro do usuário professor.

```
Adicionando novo usuário `professor' (1001) ao grupo `professor' ...
Criando diretório pessoal `/home/professor' ...
Copiando arquivos de `/etc/skel' ...
Digite a nova senha UNIX:
Redigite a nova senha UNIX:
passwd: senha atualizada com sucesso.
Modificando as informações de usuário para professor
Informe o novo valor ou pressione ENTER para aceitar o padrão
        Nome Completo []: Professor
        Número da Sala []:
        Fone de Trabalho []:
        Fone Doméstico []:
        Outro []:
Esta informação está correta?[S/n]
```


Figura 261
Arquivo "sudoers" da pasta "/etc".

```
Arquivo  Editar  Ver  Terminal  Ajuda
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#

Defaults        env_reset

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL

# Uncomment to allow members of group sudo to not need a password
# (Note that later entries override this, so you might need to move
# it further down)
# %sudo ALL=NOPASSWD: ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
jpescola@jpescola-laptop:~$
```

O comando "groupadd" permite criar um grupo de usuários. Veja o exemplo na figura 262.

Figura 262
O comando "groupadd".

```
Arquivo  Editar  Ver  Terminal  Ajuda
jpescola@jpescola-laptop:~$ sudo groupadd alunos
jpescola@jpescola-laptop:~$
```

Nesse exemplo, estamos criando o grupo "alunos" para posteriormente adicionar a ele os usuários individuais de cada aluno. Dessa forma, qualquer mudança de permissão para os alunos ocorrerá nesse grupo e não afetará os demais usuários. Isso significa que a vida do administrador está ficando mais prática.

O comando **"usermod"** permite alterar as configurações de um usuário existente. O parâmetro "-G" permite adicionar o usuário a um ou mais grupos já criados no sistema. No nosso exemplo, vamos adicionar o usuário "professor" ao grupo "professores" (figura 263).

Para saber mais sobre os parâmetros disponíveis no comando "usermod", acesse o manual do comando, digitando "man usermod".

Figura 263
O comando "usermod".

```
Arquivo  Editar  Ver  Terminal  Ajuda
jpescola@jpescola-laptop:~$ usermod -G professores professor
```

Você pode visualizar a lista de grupos da qual faz parte digitando o comando "groups" no terminal, como aparece na figura 264.

Figura 264
O comando "groups".

```
Arquivo  Editar  Ver  Terminal  Ajuda
jpescola@jpescola-laptop:~$ groups
jpescola adm dialout cdrom plugdev lpadmin admin sambashare
jpescola@jpescola-laptop:~$
```

O Windows possui uma tecnologia chamada Conexão de área de trabalho remota. Para saber mais sobre ela, procure no Help do seu Windows.

9.3. Acesso remoto via rede

Para um administrador de redes é importante poder acessar as máquinas remotamente. Assim, quando precisar instalar um novo programa, ele poderá fazê-lo de uma das máquinas da rede local ou via internet. Vamos, portanto, conhecer algumas das tecnologias de acesso remoto disponíveis. A maioria é gratuita, tanto para Windows quanto para Linux.

9.3.1. Introdução à tecnologia VNC

A tecnologia VNC (Virtual Network Computing ou: computação em rede virtual) possibilita acesso remoto de um computador a outro com interface gráfica. Os softwares que trabalham com o protocolo VNC permitem que um usuário de uma máquina assuma o controle de outra da rede ou somente monitore as atividades de um usuário em um computador **remoto**. Vamos adotar aqui o UltraVNC, um software gratuito que permite a utilização dessa tecnologia.

9.3.2. Instalando o UltraVNC em um servidor de acesso

Para baixar o UltraVNC, pesquise o endereço em um site de busca ou utilize seu site de downloads preferido. Após baixar o pacote, dê duplo clique no arquivo para iniciar a instalação do aplicativo. O processo é bem parecido com o de qualquer outro software para Windows. A diferença está em alguns detalhes. Escolhemos a opção "Full Instalation" (instalação completa) para que o assistente instale em nossa máquina um servidor VNC (figura 265). A partir daí, o PC poderá ser acessado por usuários que também possuam o cliente VNC instalado. Assim, será possível acessar, a partir da nossa máquina, outros computadores ligados à rede. Da mesma forma, se estivermos em outros computadores da rede, conseguiremos entrar no nosso remotamente.

Ao final da instalação, a página de configuração do aplicativo vai aparecer na tela, conforme mostra a figura 266. Nessa tela, o usuário configurará a forma como vai acessar esse computador remotamente. Observe que, na mesma figura, está destacada a parte na qual podemos criar uma senha de usuário. Assim, ao habilitarmos a opção "Require MS Logon", permitiremos que qualquer usuário (com senha cadastrada no sistema) acesse a máquina remotamente.

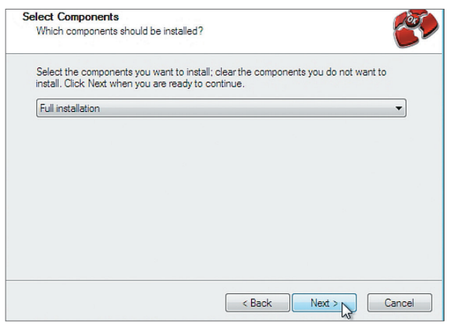


Figura 265
Instalação do UltraVNC.

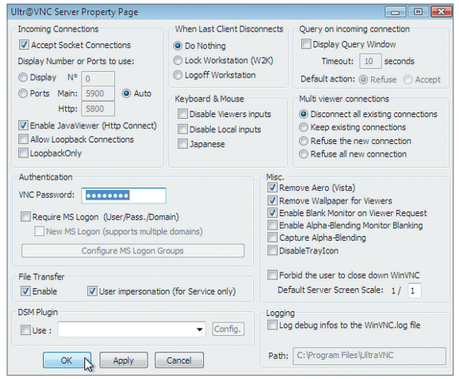


Figura 266
Configuração do servidor UltraVNC.

9.3.3. Instalando o VNCViewer em uma máquina da rede (cliente)

O **VNCViewer** é um aplicativo que permite visualização e controle da área de trabalho do computador remoto. Como escolhemos a opção "Full Instalation", o assistente de instalação providenciou também esse componente. É possível, portanto, acessar essa máquina por meio do VNCViewer. Ou, então, você pode instalar o UltraVNC no PC de origem toda vez que quiser realizar essa operação. Copie, então, o VNCViewer em um pen-drive e passe-o para outra máquina da rede local, a fim de testar o acesso remoto no computador com Windows Vista.

Tenha sempre o aplicativo VNCViewer à disposição (no pen-drive, por exemplo) para que possa acessar suas máquinas de qualquer ponto da rede local.

9.3.4. Acessar um PC remotamente usando a tecnologia VNC no Windows

Dê um duplo clique no arquivo e digite o nome ou o IP do computador servidor UltraVNC (figura 267) a partir do qual você quer acessar e clique no botão "Connect". Uma janela contendo a área de trabalho remota vai ser apresentada.

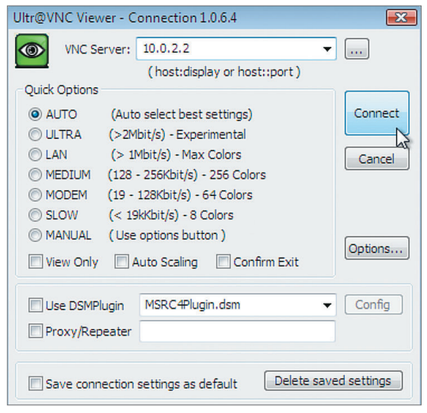
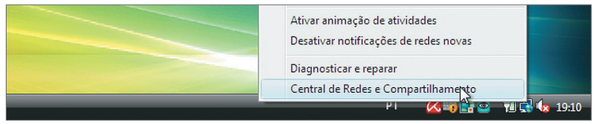


Figura 267
VNCViewer.

Figura 268
Acesso à central de redes e compartilhamento.



A partir de agora, pode-se visualizar a área de trabalho do computador e ainda executar qualquer configuração ou comando sem precisar ir até o local onde ele está instalado. Se uma mensagem de erro aparecer, pode ser necessário habilitar o UltraVNC no Firewall do Windows.

Para fazer isso, clique com o botão direito do mouse sobre o ícone de rede que aparece ao lado do relógio do Windows e escolha a opção "Central de Redes e Compartilhamento". Na janela aberta, clique na opção "Firewall do Windows" (figura 268).

Clique na opção "Firewall do Windows" para abrir as configurações do Firewall, que é o software do Windows responsável por gerenciar as conexões de rede com destino à máquina local (figura 269). Ele é muito importante para a segurança de seu computador, porque bloqueia o acesso de pessoas ou aplicações não autorizadas.

Figura 269
Acessando o firewall do Windows.

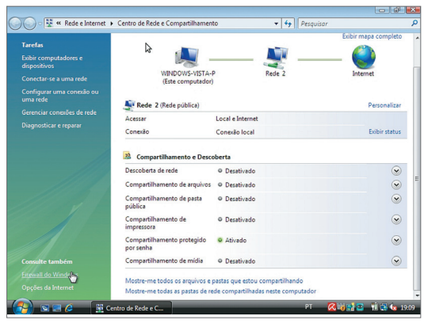


Figura 270
Habilitando o Ultra VNC no Firewall.

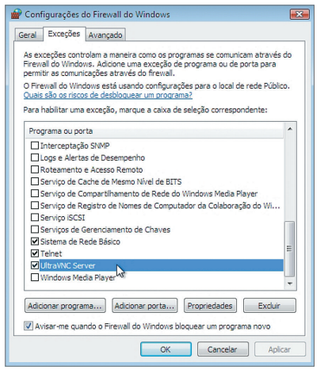
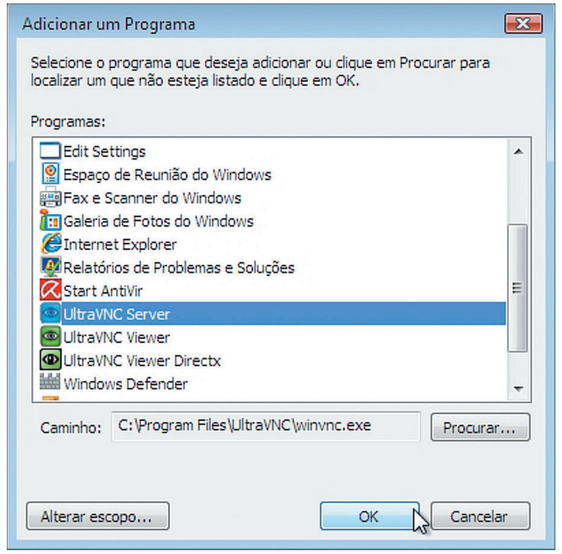


Figura 271
Adicionando programa ao Firewall do Windows.



Vamos, portanto, habilitar o UltraVNC no Firewall para que ele não bloqueie mais as conexões. Clique no botão "Adicionar programa" como na figura 270.

Clique em "UltraVNC Server" e depois no botão "OK" para confirmar. O aplicativo está habilitado para permitir conexões por meio do Firewall (figura 271). Agora você deve conseguir se conectar ao servidor VNC. Clique em VNCViewer e digite o IP ou o nome da máquina. Se a conexão for bem-sucedida, aparecerá uma tela (figura 272) solicitando a senha de acesso configurada na máquina, no momento da instalação do UltraVNC.

Figura 272
Digitando a senha de acesso.

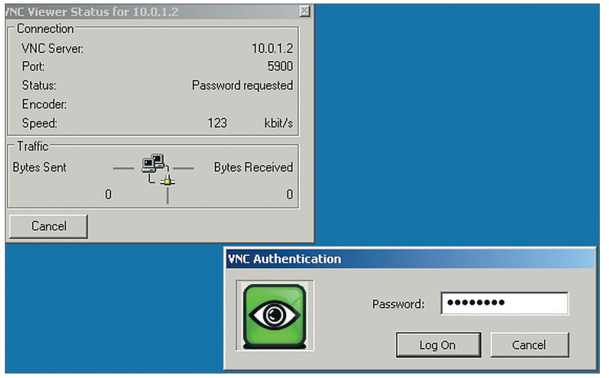
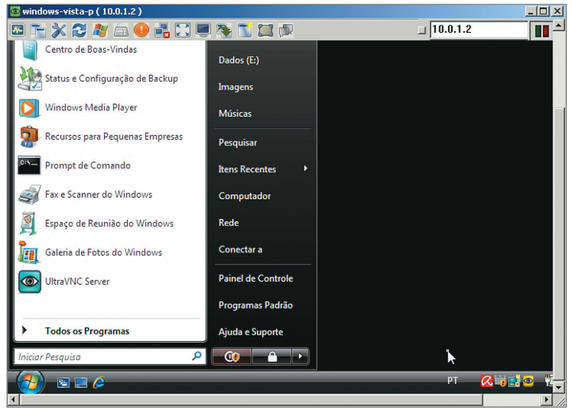


Figura 273
Acessando um computador remotamente.



Após confirmar a senha, a janela com a área de trabalho da máquina remota surgirá na tela, permitindo que você visualize e assuma o controle da máquina remota (figura 273).

9.4. Acesso remoto via rede no Linux

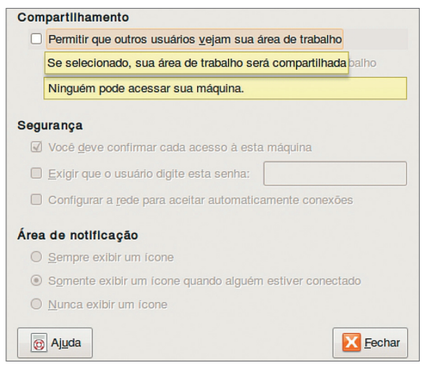
No Linux, também é possível acessar uma máquina remotamente por meio do protocolo VNC. No caso da distribuição Ubuntu, essa facilidade vem instalada como padrão.

9.4.1. Habilitando o PC para ser um servidor de conexão remota

Para habilitar um PC como servidor de conexão remota VNC, clique no menu "Preferências / Área de trabalho remota". Deve surgir na tela um utilitário como o exibido na figura 274.

Para habilitar o servidor de acesso remoto, clique na opção "Permitir que outros usuários vejam sua área de trabalho". Nesse momento, as outras opções ficarão ativas. Clique em "Exigir que o usuário digite esta senha" e digite uma senha para acesso ao PC. Depois, clique em "Fechar" (figura 275). Agora vamos acessar essa máquina por meio de outro PC com Ubuntu instalado.

Figura 274
Habilitando o servidor acesso remoto no Ubuntu.



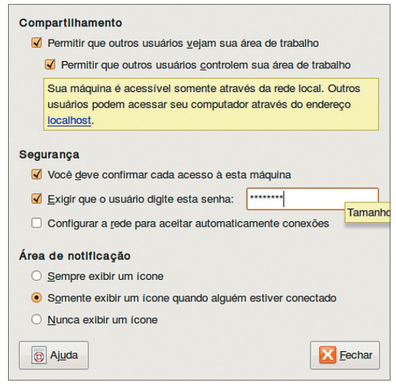


Figura 275
Configurando o acesso remoto no Ubuntu.

9.4.2. Acessar um PC remotamente usando a tecnologia VNC (Linux x Linux)

Para acessar um computador habilitado e permitir acesso remoto pelo Ubuntu, clique no menu "Aplicativos / Internet / Visualizar área de trabalho remota". Digite o IP ou o nome da máquina de destino (figura 276) e clique no botão "Conectar".

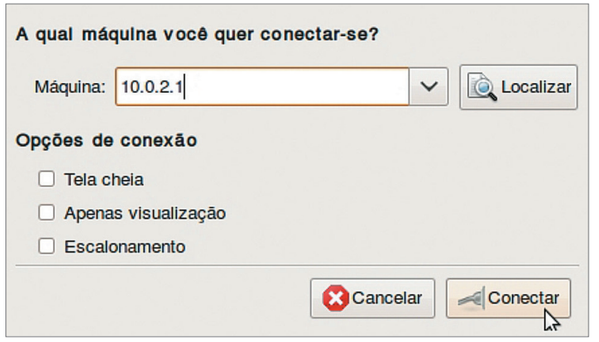
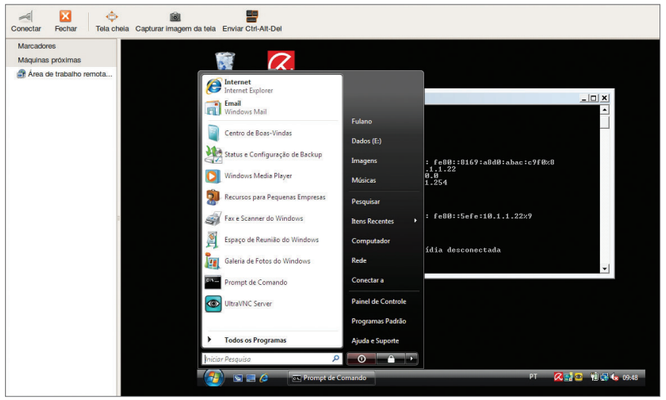


Figura 276
Digitando o IP da máquina a ser acessado.

9.4.3. Acessar um PC remotamente usando a tecnologiaVNC (Linux x Windows)

Se a máquina que você quer acessar tiver o Windows, basta que algum software com protocolo VNC esteja instalado nela para que a operação seja possível, mesmo que se trate de equipamentos com sistemas operacionais diferentes.

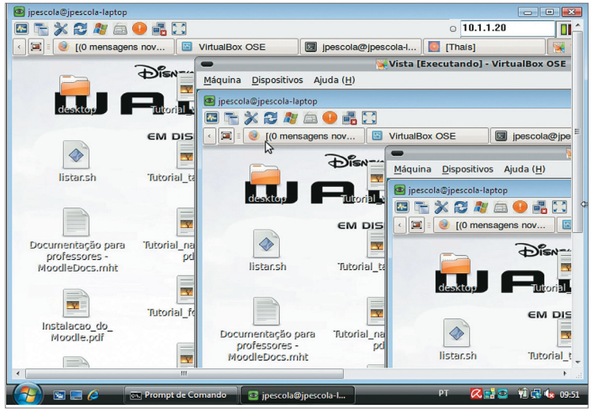
Figura 277
Acessando, via VNC, um PC com Windows Vista, a partir do Ubuntu.



No exemplo da figura 277, mostramos um usuário acessando uma máquina com Windows Vista a partir de uma com Ubuntu.

A mesma regra se aplica caso o usuário queira acessar, por meio de um PC com Windows Vista, um computador da mesma rede que tenha o Ubuntu instalado (figura 278).

Figura 278
Acessando, via VNCViewer, um PC Ubuntu.



9.5. Acesso remoto via rede (modo texto)

Apesar de existir o protocolo VNC, em muitos casos pode ser mais útil ou viável acessar um PC remotamente pelo modo texto (prompt de comandos). O modo texto permite o acesso mesmo quando a conexão é lenta e só trafegam dados básicos na rede. Afinal, quanto maior a quantidade de dados com imagens e resolução de cores utilizada numa conexão, maior o fluxo de dados a serem transmitidos.

9.5.1. Introdução ao Telnet e ao SSH

Tanto no Linux quanto no Windows é possível acessar um PC remotamente pelo prompt de comandos. No Windows, a tecnologia Telnet – muito utilizada, mas depreciada por sua pouca segurança na transmissão dos dados – é a alternativa mais comum. Para o Linux, o protocolo SSH (Secure Shell) permite conexões seguras entre máquinas Linux. Assim, o administrador pode gerenciar qualquer equipamento remotamente por meio de comandos do prompt.

9.5.2. Acessar um PC remotamente utilizando Telnet (Windows)

Inicialmente vamos acessar um computador com Windows Vista, a partir de outro com Windows XP. Para que o protocolo Telnet funcione entre essas duas máquinas, é necessário habilitar o serviço Telnet no servidor. No nosso caso, essa função fica com o PC que vai receber a conexão e que tem Windows Vista.

Para efetuar essa configuração, clique no menu "Iniciar. Na caixa de pesquisa, digite "services.msc" para abrir o utilitário de configuração de serviços do Windows Vista. No utilitário, procure a opção "Telnet", clique com o botão direito do mouse e escolha a opção "Propriedades" (figura 279).

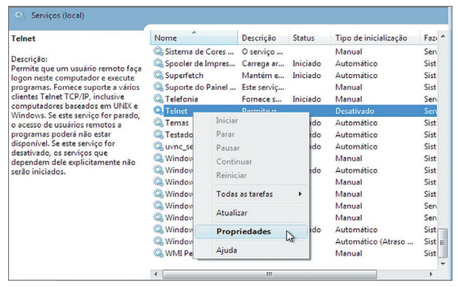


Figura 279
Habilitando o serviço "Telnet" no Windows Vista.

Para que o serviço seja habilitado e executado toda vez que o Windows for iniciado, escolha a opção "Automático" e clique no botão "Aplicar" (figura 280).

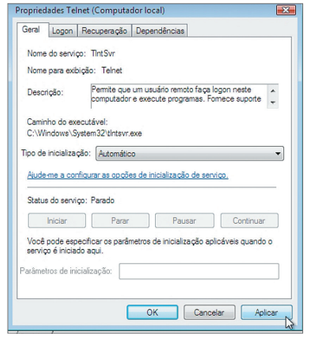
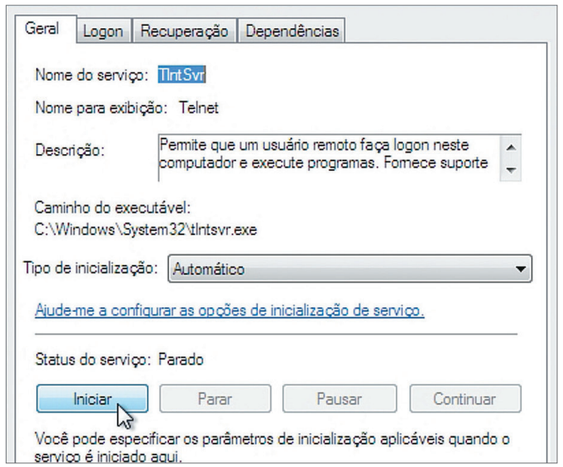


Figura 280
Configurando o serviço "Telnet" como Automático.

Figura 281
Iniciando o serviço manualmente.

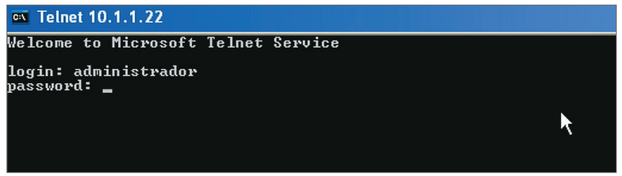


É necessário conhecer o login e a senha cadastrados no servidor para que seja possível acessá-lo via telnet. Por isso, habilitamos temporariamente o usuário "Administrador" e configuramos uma senha para que nossos testes possam ser realizados.

Da próxima vez que o Windows for iniciado, o serviço estará ativo. Mas, para fazer o teste sem precisar reiniciar a máquina, clique no botão "Iniciar" (figura 281).

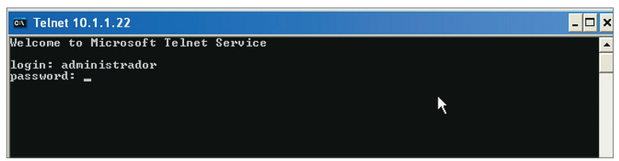
Agora vamos para outro computador da rede. Digitamos "Telnet <ip>" para acessar a nossa máquina Windows Vista pelo prompt. No nosso caso, a máquina servidora Telnet tem o IP 10.1.1.21. Por isso, digitamos no prompt "Telnet 10.1.1.21". O **login de usuário** e a senha serão solicitados. Digite-os e pressione "Enter" (figura 282).

Figura 282
Logando uma máquina remota por meio do serviço "Telnet".



Se o usuário e a senha estiverem corretos, você verá uma tela como a da figura 283. Pronto. A conexão foi realizada com sucesso. Agora você pode digitar comandos no prompt da máquina remota e executar diversas tarefas sem a necessidade de estar fisicamente onde está instalado o PC remoto.

Figura 283
Conexão telnet realizada com sucesso, a partir do Windows XP.



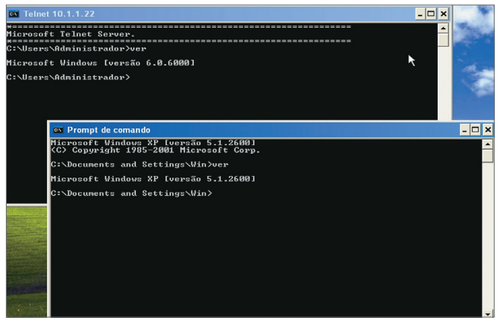


Figura 284
Prompt conectado a um servidor Telnet e um prompt local.

Por meio do comando "ver" do prompt, é possível visualizar a versão do sistema operacional de cada máquina. No prompt que estamos utilizando o telnet, a versão apresentada é maior do que a da máquina local (Windows XP). É porque estamos acessando o Windows Vista (figura 284).

9.5.3. Acessar um PC remotamente usando SSH (Linux)

Para acessar um PC remoto utilizando a tecnologia SSH, precisamos ter à disposição pelo menos dois computadores com Linux ligados em rede. Além disso, o computador que será acessado (servidor SSH) deverá ter o pacote "openssh-server". Na máquina cliente, o pacote "openssh-client" é necessário, mas no caso do Ubuntu ele já vem instalado como padrão. Para instalar o "openssh-server" no computador servidor, use o comando "apt-get install openssh-server". Não se esqueça do comando sudo, caso não esteja logado como "root".

Após a instalação do pacote, vamos acessar a máquina remota digitando o comando exibido na figura 285.

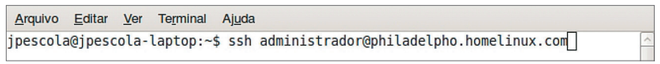


Figura 285
Acessando um PC remoto com "ssh.

Digitar o comando "ssh", seguido do nome do usuário e do endereço do servidor – tudo separado pelo caractere @ – é suficiente para que o seu PC encontre a máquina na rede e a acesse por "ssh". No nosso caso, estamos acessando um computador fora da rede local, que tem um endereço (domínio) configurado. No entanto, podemos utilizar também o número IP da máquina tanto na rede local quanto para acessá-la via internet. Veja na figura 286 que a porta padrão

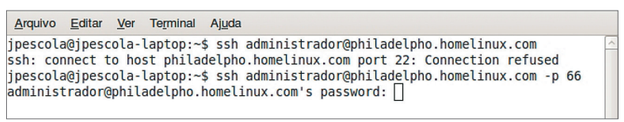


Figura 286
Digitando a senha para conexão remota com "ssh.

Figura 287
Conexão "ssh" realizada com sucesso.

```
Arquivo  Editar  Ver  Terminal  Ajuda
jpescola@jpescola-laptop:~$ ssh administrador@philadelpho.homelinux.com
ssh: connect to host philadelpho.homelinux.com port 22: Connection refused
jpescola@jpescola-laptop:~$ ssh administrador@philadelpho.homelinux.com -p 66
administrador@philadelpho.homelinux.com's password:
Linux srvproxy 2.6.27-11-server #1 SMP Wed Apr 1 21:53:55 UTC 2009 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sat Oct  3 00:38:50 2009 from 189-19-109-199.dsl.telesp.net.br
administrador@srvproxy:~$
```

(22) foi modificada. Então, devemos especificar a porta que o servidor está utilizando para responder às conexões, que no nosso caso é a 66. Para isso acrescente os parâmetros "-p 66". Se a porta fosse configurada como 100, utilizaríamos o parâmetro "-p 100". Agora a máquina remota, é encontrada e a aplicação solicita a senha do usuário remoto configurado na linha de comando.

Digite a senha do usuário configurado na linha de comandos e pressione "Enter". Nossa conexão foi realizada com sucesso (figura 287).

Agora o cursor apresenta o nome da máquina remota depois do @. E o usuário que estamos utilizando não é mais o "jpescola", como na máquina local, mas sim "administrador", que é o usuário da máquina remota. Todo comando que for digitado a partir daí será executado na máquina remota e não mais na local.

Após realizar a administração remota necessária no PC, digite o comando "exit" para sair e voltar a controlar sua máquina local (figura 288).

Podemos transferir arquivos de uma máquina para outra, via rede, com um único comando que utiliza a mesma tecnologia do "ssh". Esse comando é o "scp" (secure copy, ou cópia segura), conforme ilustra a figura 289.

Figura 288
Fechando a conexão "ssh" com o comando "exit".

```
Arquivo  Editar  Ver  Terminal  Ajuda
jpescola@jpescola-laptop:~$ ssh administrador@philadelpho.homelinux.com
ssh: connect to host philadelpho.homelinux.com port 22: Connection refused
jpescola@jpescola-laptop:~$ ssh administrador@philadelpho.homelinux.com -p 66
administrador@philadelpho.homelinux.com's password:
Linux srvproxy 2.6.27-11-server #1 SMP Wed Apr 1 21:53:55 UTC 2009 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
Last login: Sat Oct  3 00:38:50 2009 from 189-19-109-199.dsl.telesp.net.br
administrador@srvproxy:~$ exit
logout
Connection to philadelpho.homelinux.com closed.
jpescola@jpescola-laptop:~$
```


Figura 289
Copiando um arquivo via rede com "scp".

```
Arquivo  Editar  Ver  Terminal  Ajuda
jpescola@jpescola-laptop:~$ scp -P 66 1.iso administrador@philadelpho.homelinux.com:/h
ome/administrador/
```

9.5.4. Transferindo arquivos para máquinas remotas em modo texto (SCP)

A sintaxe do comando pode parecer complicada, mas não é. Primeiro, temos o comando "scp", depois o parâmetro "-P" (maiúsculo), que serve para especificar a porta que a aplicação usa no servidor remoto (se a porta for a 22, padrão, não precisaremos especificá-la). O próximo parâmetro será o nome do arquivo que queremos transferir (se o arquivo estiver em outra pasta, podemos especificar o caminho). Os últimos parâmetros serão o nome do usuário seguido do caractere @, do endereço da máquina e do caminho no qual será armazenado o arquivo no PC destino. Quando a aplicação terminar de transferir o arquivo, o cursor voltará a ficar disponível na máquina local (figura 290). Quer dizer que não ficaremos logados na máquina remota, como no comando "ssh", pois solicitamos apenas uma cópia de arquivo, e não uma conexão remota.

Figura 290
Cópia do arquivo realizada com sucesso via "scp".

```
Arquivo  Editar  Ver  Terminal  Ajuda
jpescola@jpescola-laptop:~$ scp -P 66 1.iso administrador@philadelpho.homelinux.com:/h
ome/administrador/
administrador@philadelpho.homelinux.com's password:
1.iso                                         100%  646KB 646.0KB/s   00:00
jpescola@jpescola-laptop:~$
```

9.6. Virtualização de computadores

Já imaginou criar uma rede de três, quatro ou mais máquinas utilizando somente um único PC? Pois isso já é possível, graças a uma tecnologia interessante e muito utilizada atualmente, denominada **virtualização de computadores,** o que nos permite criar uma máquina virtual (VM, sigla para a expressão em inglês Virtual Machine) dentro de uma máquina real. A virtual compartilhará os recursos da outra, mas será totalmente independente em relação ao sistema operacional e às aplicações instaladas na real (hipertexto a seguir).

Lembre-se de que os fundamentos aqui empregados poderão ser adotados em qualquer outro software de virtualização que você utilizar. O que muda são algumas funcionalidades e botões em locais diferentes.

Quando criamos uma máquina virtual, especificamos a quantidade de memória que ela vai usar da real. Assim, quando a virtual estiver em execução, a parte da memória configurada para ela ficará à sua disposição e a máquina real não poderá mais utilizar essa fatia de memória do equipamento. Em relação ao disco rígido, a VM pode ser configurada para utilizar uma partição do disco local, de outro disco instalado, ou criar um disco em forma de arquivo (normalmente expansível). Ao especificarmos, por exemplo, um tamanho máximo de 10 GB (gigabytes) para o HD virtual, teremos inicialmente um arquivo com poucos KB (kilobytes). Após a instalação do sistema operacional e das outras aplicações, esse arquivo vai se expandindo conforme a quantidade de dados armazenados na VM. Placas de rede também podem ser configuradas na máquina virtual. Assim, conseguiremos

acessar a rede local ou navegar na internet pela VM, compartilhando os recursos de rede da máquina real. Muitos recursos também podem ser configurados para rede, com a criação de uma rede local entre a VM e a máquina real. Existem diversos tipos de virtualização e aplicações para criação de máquinas virtuais (veja três exemplos no quadro "Principais tipos de virtualização").

Tabela 7

PRINCIPAIS TIPOS DE VITUALIZAÇÃO

Tipo	Descrição
Virtualização total	Boa parte do gerenciamento da VM é feita diretamente entre o virtualizador e o hardware, sem a necessidade de passar pelo sistema operacional. Isso resulta num melhor desempenho de execução da VM.
Paravirtualização	É necessário modificar o sistema operacional para implementar algumas melhorias de desempenho para a VM. O que impossibilita sua adoção em sistemas operacionais proprietários.
Emulação	Nesse modelo, a aplicação deve converter, bit a bit, os dados da VM para o sistema operacional. Isso porque, em muitos casos, utilizamos uma plataforma virtualizada em uma plataforma de hardware diferente (Ex: PowerPC em X86).

9.6.1. Softwares de virtualização disponíveis no mercado

Essa tecnologia permite uma operação até pouco tempo atrás inconcebível: criar uma máquina virtual com Linux em uma real com Windows, por exemplo.

Entre os softwares disponíveis no mercado, vamos adotar inicialmente o VirtualPC (Freeware), da Microsoft, já que ele utiliza a tecnologia de virtualização total. Seu desempenho é excelente em relação aos demais. Outros bons exemplos de softwares disponíveis que utilizam a mesma tecnologia são o VirtualBox (OpenSource) e o VMWare (algumas versões Freeware). O mais conhecido para executar paravirtualização é o Xen, disponível para Linux e outros sistemas operacionais OpenSource. Nesse caso, é fundamental dispor do código fonte do sistema operacional para fazer a alteração e a recompilação adicionando alguns patchs do **virtualizador**. Para a tecnologia de emulação, temos atualmente o Qemu e o Bochs, que são bastante lentos por causa da tecnologia empregada. O VirtualPC2007 está disponível gratuitamente no site da Microsoft e em outros sites de download disponíveis na internet. Vamos aprender a utilizá-lo.

9.6.1.1. Instalação do VirtualPC no Windows

Baixe o VirtualPC2007 do site da Microsoft por meio de um site de busca. Aqui vamos baixar a versão 32 bits, mas você pode optar pela versão 64 bits, caso seu PC seja compatível (figura 291).

Após baixar o instalador, use o botão "Executar" ou dê duplo clique no arquivo baixado para iniciar a instalação do virtualizador VirtualPC. Esse programa vai permitir que você crie e gerencie suas máquinas virtuais (figura 292).

Ao executar o assistente de instalação, você perceberá que o procedimento é bem

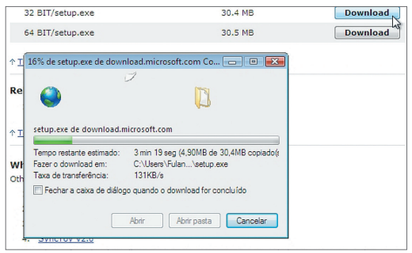


Figura 291
Baixando o VirtualPC2007.

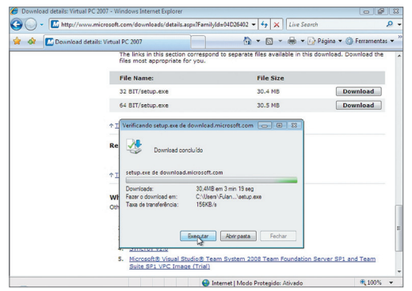


Figura 292
Executando o instalador do virtualPC2007.

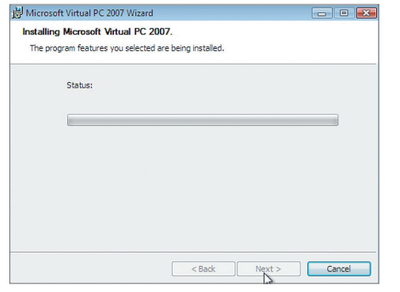


Figura 293
Instalando o VirtualPC2007.

simples, idêntico à instalação de qualquer software para Windows. Siga todos os passos, clicando sempre em "Next". Ao final, clique em "Install" para visualizar o processo de instalação (figura 293). Depois basta ir até o atalho criado e executá-lo, como ilustra a figura 294.

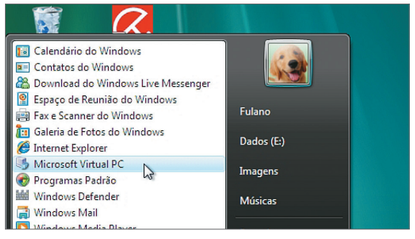
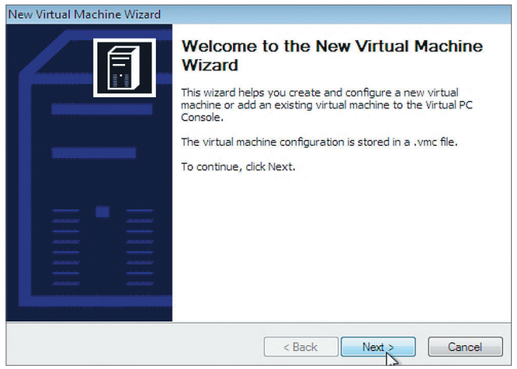


Figura 294
Executando o VirtualPC2007.

Figura 295
Criando uma nova máquina virtual no VirtualPC.

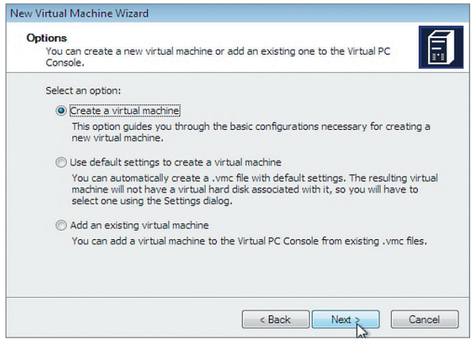


9.6.1.2. Criando máquinas virtuais no VirtualPC

Quando você executar o VirtualPC pela primeira vez, um assistente de criação de máquinas virtuais vai aparecer na tela, informando o passo-a-passo. Clique em "Next" para iniciar a criação da VM (figura 295).

O próximo passo é escolher uma das três opções (figura 296). A primeira permitirá criar uma nova máquina virtual. A segunda serve para criar uma máquina virtual utilizando as configurações padrão do VirtualPC (você não poderá configurar a VM inicialmente). E a última é para adicionar uma VM já existente.

Figura 296
Escolhendo a primeira opção para criar a VM.



Em seguida, digite o nome da nova máquina virtual. Aqui o escolhido foi Ubuntu, mas você pode digitar qualquer um e clicar em "Next" (figura 297).

Neste ponto, escolha o sistema operacional que será instalado na VM. Perceba que essa opção serve somente para que o VirtualPC opte por uma quantidade de memória RAM e o disco rígido compatível com os requisitos do sistema operacional escolhido (figura 298). Entretanto, você poderá alterar essas configurações posteriormente.

Figura 297
Nomeando a nova VM.

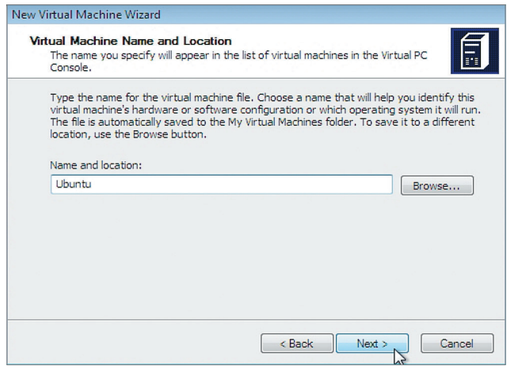
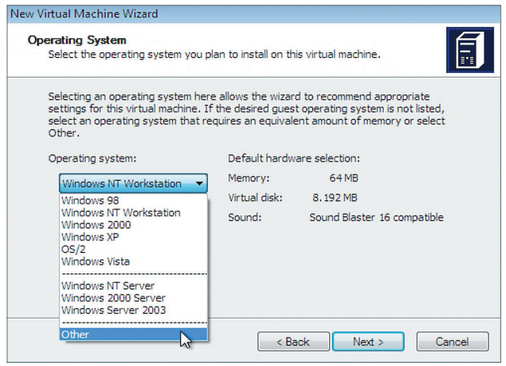


Figura 298
Especificação do sistema operacional a ser instalado na VM.



A tela seguinte mostra que podemos clicar no primeiro item para usar a quantidade de memória sugerida pelo VirtualPC ou configurar uma nova quantidade, clicando no segundo item (figura 299).

Figura 299
Configurando a quantidade de memória para a VM.

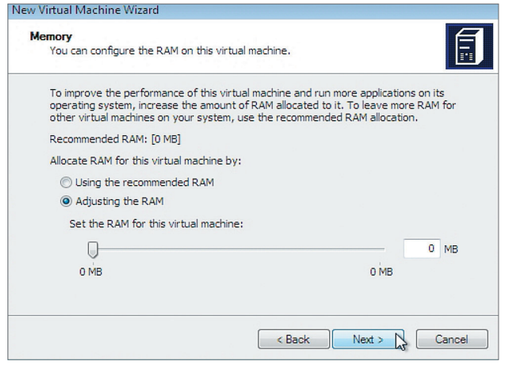
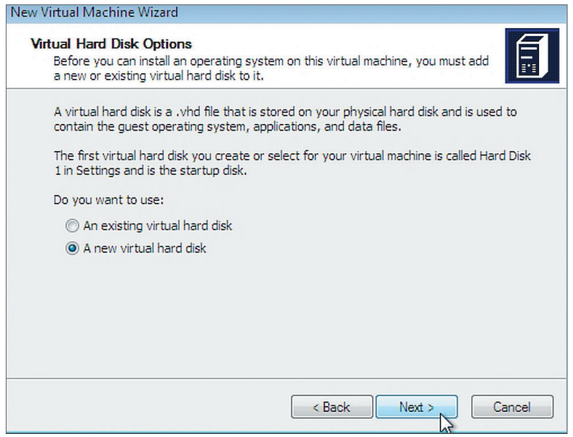


Figura 300
Criando um novo disco rígido virtual.

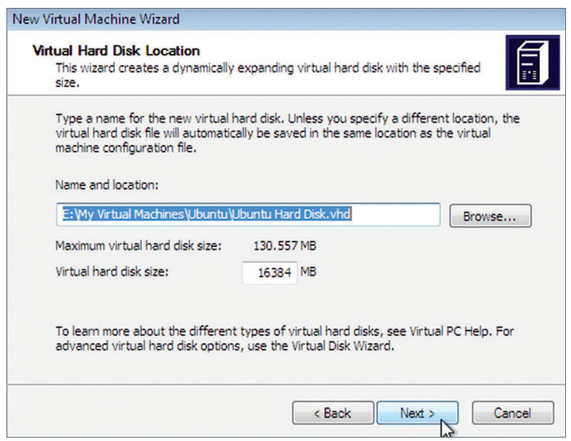


Podemos utilizar um disco já existente (primeira opção que aparece na tela, como mostra a figura 300). Mas, se quisermos criar um novo HD (segunda opção), basta escolher o diretório em que será salvo o disco rígido virtual e um nome para o arquivo que armazenará seu conteúdo.

Podemos escolher também o tamanho máximo do HD. Perceba que o arquivo só poderá chegar até o tamanho especificado (figura 301). Por exemplo, se você criar um HD de 10 GB, ele vai começar com 10 GB livres e, quando estiver cheio, o sistema operacional da VM dará essa informação, mesmo que o HD real ainda tenha espaço livre.

Pronto. Foi criada nossa primeira máquina virtual. Agora é só clicar em "Finish" para terminar o processo (figura 302).

Figura 301
Especificação do tamanho do disco rígido virtual.



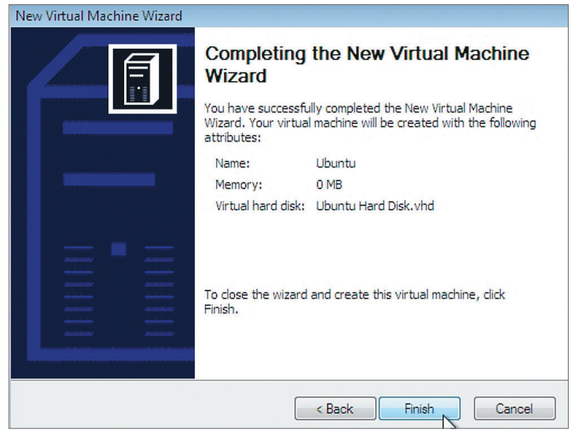


Figura 302
Finalizando a criação da VM.

9.6.1.3. Configuração do VirtualPC

O console do VirtualPC (figura 303) é uma aplicação que permite gerenciar as VMs existentes e ainda criar novas a qualquer momento. Nessa etapa, temos uma máquina virtual criada, mas é como se comprássemos as peças de um PC para montá-lo. Por isso é necessário instalar o sistema operacional nessa máquina para que ela funcione corretamente. O processo é idêntico ao da instalação em uma máquina real.

Clique no botão "Settings" para alterar as configurações da VM (em seguida veremos a imagem que aparece na figura 304, com as opções disponíveis para configurar a VM). Veja que podemos alterar a quantidade de memória RAM e adicionar mais discos rígidos à VM etc.

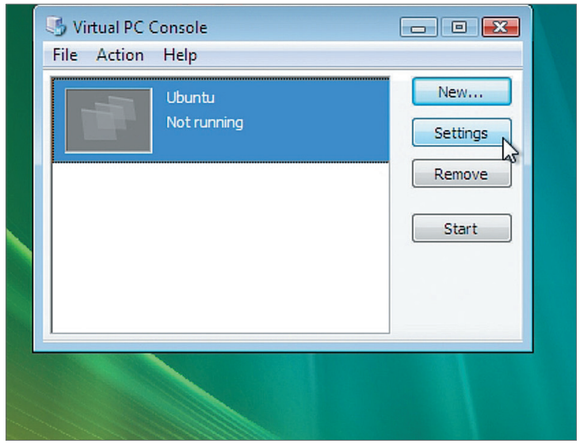
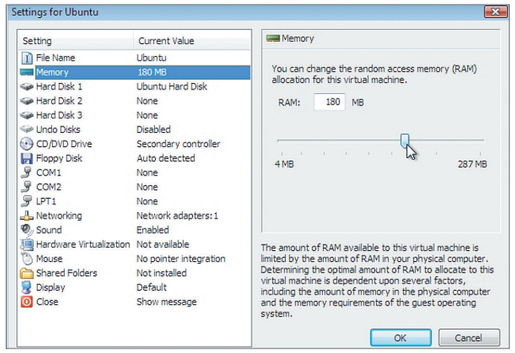


Figura 303
Alterando as configurações da VM recém-criada.

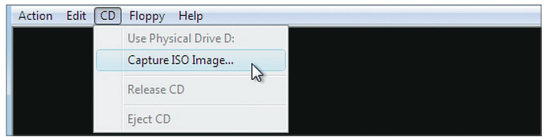
Figura 304
Interface de configuração da VM.



9.7. Instalando novos sistemas operacionais em máquinas virtuais

Para instalar o sistema operacional na VM, é preciso atentar para o uso do drive de CD ou de DVD da máquina real pela máquina virtual. Ao executarmos a máquina virtual com um CD de instalação de sistema operacional inserido no drive, ela o reconhecerá automaticamente e iniciará a instalação. Podemos utilizar um arquivo de imagem como se fosse um CD de instalação, sem a necessidade de gravá-lo em disco. Para isso, ao executar a VM clique no menu "CD" e escolha "Capture ISO image..." para apontar a imagem e utilizá-la como se fosse um CD de instalação de verdade (figura 305).

Figura 305
Instalação de um sistema operacional na VM.



Um recurso importante da virtualização é a opção de salvar o estado de uma máquina virtual. Ao clicar no botão "Fechar", uma janela (figura 306) vai ser exibida em sua tela. Se escolher a opção "Turn off", a VM será desligada como se você puxasse o cabo de energia "virtual" da tomada. A outra opção "save state" salva o estado atual da VM. Isso permite que você continue a sua utilização a partir do ponto em que parou.

Figura 306
Desligando depois de usar a VM.

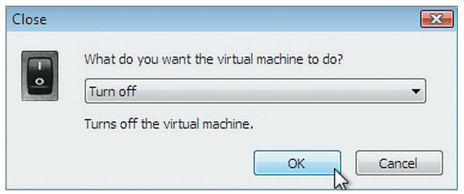
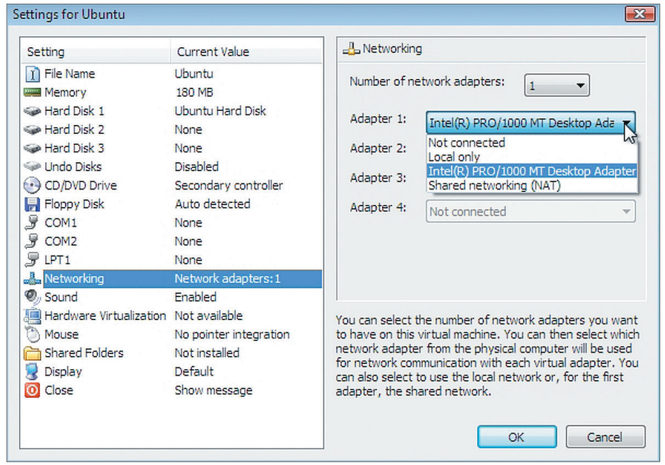


Figura 307
Opções de configuração.



9.7.1. Configuração de rede entre máquinas virtuais

Para alterar as configurações de rede da máquina virtual é necessário que ela esteja desligada. Clique no botão "Settings" e depois na opção "Networking" para ver as configurações de rede (figura 307) (consulte o quadro "Quatro opções de rede").

Tabela 8

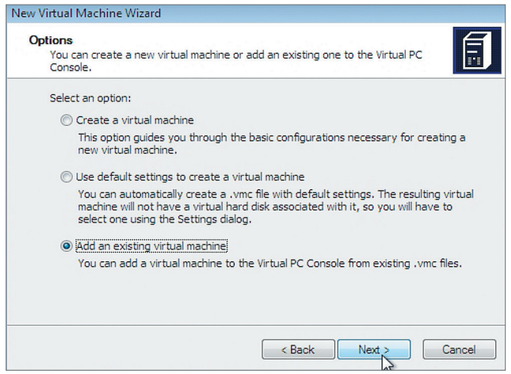
QUATRO OPÇÕES DE REDE	
Tipo	**Descrição.**
Not connected	Rede desabilitada.
Local only	Cria uma rede local entre o PC real e a VM.
Placa de rede da máquina real	Utiliza a placa de rede do PC real para acessar a mesma rede local desse PC.
Shared networking (NAT)	Cria um serviço virtual no qual a conexão de internet do PC real será compartilhada com a máquina virtual. Isso possibilita que a VM navegue também na internet.

9.7.2. Backup e replicação de máquinas virtuais

No console do VirtualPC, podemos adicionar uma VM criada anteriormente ou uma VM que você copiou de um PC de um amigo, por exemplo. Para isso, clique no botão "New..." e escolha a opção "Add an existing virtual machine" no assitente de criação (figura 308).

É possível replicar uma única máquina virtual para todo um laboratório, durante uma aula, ou levar nossa máquina virtual no pen-drive para onde quisermos.

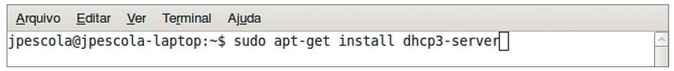
Figura 308
Adiconando uma VM já existente.



9.8. Servidor DHCP

Um servidor DHCP é um computador que fornece IP aos demais da rede que não estão configurados com um IP fixo. No caso do Windows, podemos baixar programas que fazem isso. No entanto, para ter um servidor de rede Windows, é recomendável dispor de uma versão mais adequada para esse tipo de serviço, como o Windows 2003 ou 2008. Primeiro, porém, vamos criar um servidor DHCP por intermédio do Linux. É simples. Primeiro acesse seu PC Ubuntu e digite o comando do "apt-get para instalar o aplicativo "dhcp3-server". Após configurar a faixa de IPs que será fornecida às máquinas da rede, você transformará seu computador num servidor DHCP (figura 309).

Figura 309
Instalando o "dhcp3-server".



Quando digitar o comando de instalação, o "apt-get vai buscar na internet todos os pacotes necessários para que o seu computador se torne um servidor DHCP da rede local (figura 310).

Figura 310
Aguardando a instalação do software "dhcp3-server".

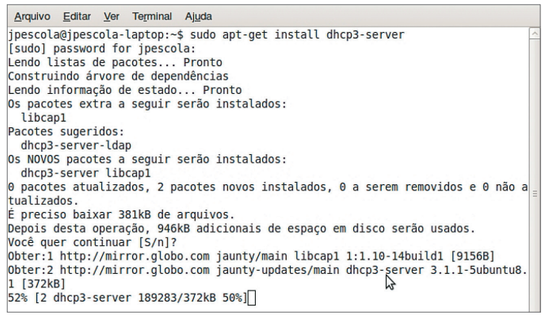


Figura 311
Abrindo o arquivo de configuração do servidor DHCP.

Ao final da instalação, edite o arquivo de configuração para especificar a faixa de IPs que será atribuída aos computadores da rede, bem como o IP do gateway e dos servidores DNS (figura 311).

O arquivo de configuração do servidor é o "dhcpd.conf" e pode ser visualizado na figura 312.

As linhas que iniciam com o caractere # estão desabilitadas e não serão levadas em consideração pelo software. Procure a linha que contém a frase "This is a very basic subnet". Ou, então, adicione em qualquer parte do arquivo de configuração os comandos informados a seguir. Essas configurações serão lidas pela aplicação ao iniciarmos o serviço e toda vez que o computador for ligado.

Na figura 313, vemos que configuramos uma a rede 192.168.0.0 com a máscara de sub-rede 255.55.255.0, que é uma rede de classe C. Também configuramos a faixa de IPs que será disponibilizada aos computadores configurados para receber IP pelo protocolo DHCP. A faixa é do IP 192.168.0.10 ao 192.168.0.200.

Na linha "option routers", configuramos o **IP** do gateway da rede, que normalmente é o computador que nos liga à internet. Por último, configuramos os servidores DNS, que podem ser tanto internos quanto externos. Para executar o servidor, digite o comando "sudo /etc/init.d/dhcp3-server start". Os parâmetros "stop" e "restart" poderão ser utilizados a qualquer momento que for necessário.

Saiba mais sobre IP no livro *Redes e manutenção de computadores*, desta coleção.

Figura 312
Arquivo de configuração original "dhcpd.conf".

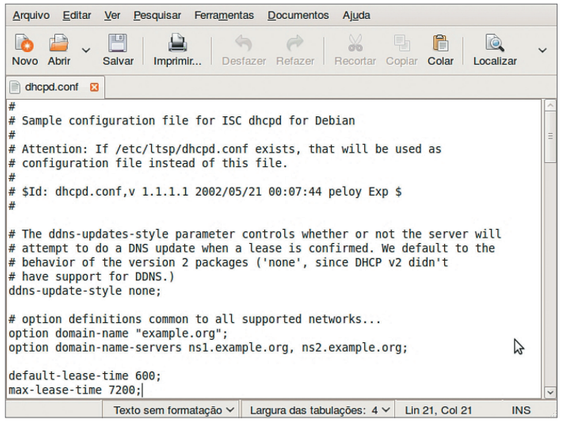
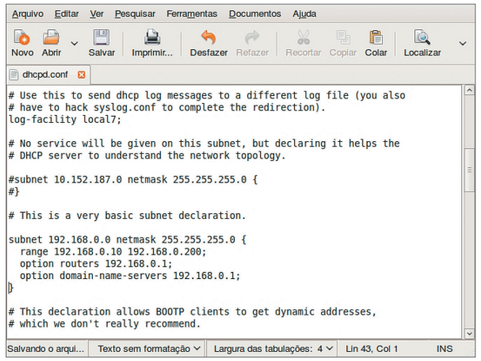
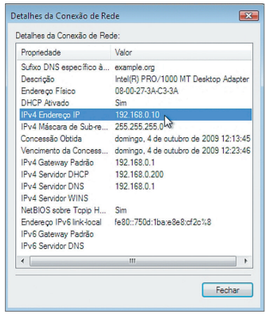


Figura 313
Arquivo dhcpd.conf modificado.



Ao configurar um cliente da rede para receber IP dinamicamente (DHCP), podemos verificar se isso aconteceu realmente. Em um PC Windows Vista, basta abrir a "Central de redes e compartilhamento", clicar no botão "Exibir status" e depois em "Detalhes" para ver as informações de rede (figura 314).

Figura 314
Verificando se o cliente recebeu o endereço IP.



O comando "ipconfig" no prompt de comandos do Windows também permite visualizar essa informação (figura 315).

Figura 315
Verificando, via prompt, se o cliente recebeu o endereço IP.

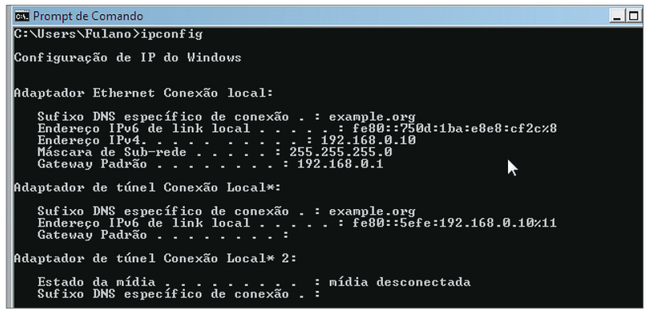
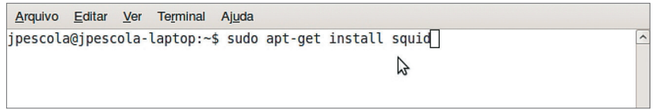


Figura 316
Instalando o Squid.



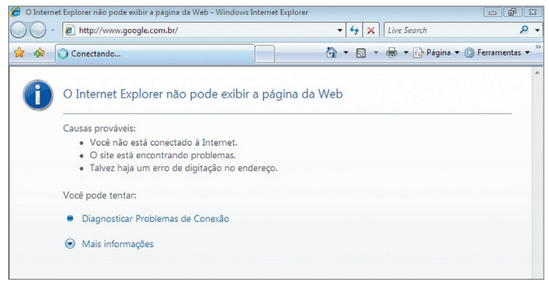
9.9. Servidor Proxy

Proxy é um servidor que recebe a conexão de internet e distribui para a rede local. Já o Squid, o software Proxy mais utilizado atualmente, oferece outros recursos importantes, como registro de conteúdo, armazenamento das páginas acessadas pelos usuários e controle de acesso. Ele permite que o administrador do sistema bloqueie determinados sites e libere outros para serem acessados pelos usuários da rede local.

Para instalar o Squid, digite o comando (figura 316). Após a instalação desse software, o servidor estará pronto para ser utilizado. Vamos, então, configurar uma das máquinas da rede para poder utilizar o Proxy como recurso de acesso à internet.

Observe na figura 317 que nosso PC com Windows Vista ainda não pode se conectar à internet, pois não foi configurado para isso.

Figura 317
Windows Vista sem a configuração de roteamento no gateway.



Para configurar o navegador, clique no menu "Ferramentas / Opções da Internet" e na aba "Conexões" (figura 318).

Figura 318
Configurando o navegador para acessar a internet pelo Proxy Squid.

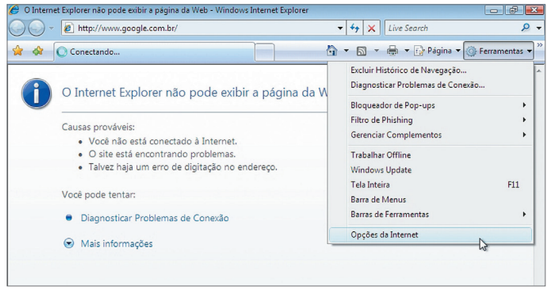
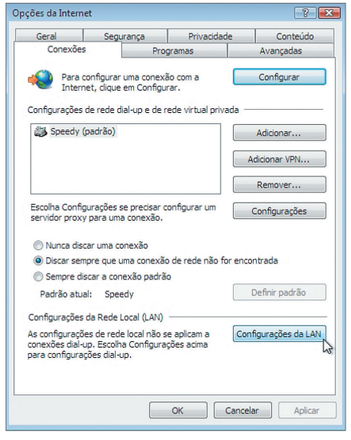


Figura 319
Configuração da LAN.



Na aba "Conexões", clique em "Configurações de LAN" (figura 319). Digite o IP do servidor Proxy e a porta que ele está utilizando para responder às conexões internas. A porta padrão é 3128, mas é recomendável alterá-la no arquivo de configuração posteriormente.

Clique no botão "OK" e tente agora acessar a internet (figura 320).

Conforme mostra a figura 321, o Squid bloqueia o conteúdo da internet. Libere, então, o acesso aos usuários da rede, editando o arquivo "Squid.conf" que está

Figura 320
Digitando o IP do servidor Proxy e a porta que ele utiliza.

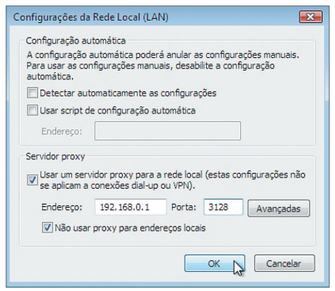
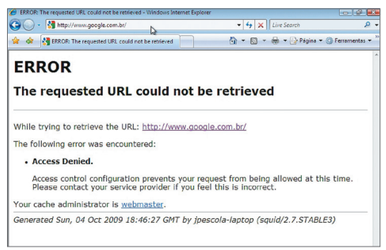


Figura 321
O Squid bloqueia todo conteúdo por padrão.



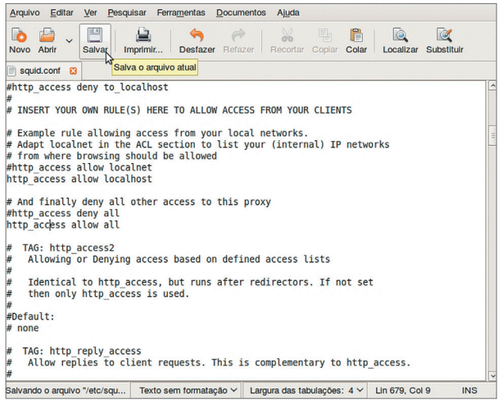


Figura 322
Alterando o arquivo "squid.conf".

armazenado na pasta "/etc/squid". É preciso localizar a linha "http_access deny all" (impedir acesso http para todos) e digitar um caractere de sustenido (#) na frente da linha para transformá-la num comentário (figura 322).

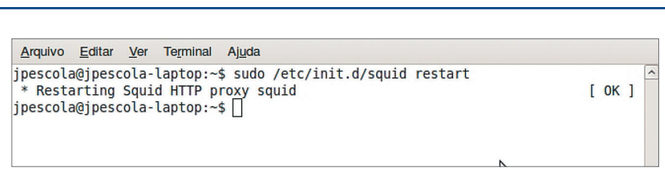


Figura 323
Reiniciando o serviço para que as mudanças sejam efetivadas.

Adicione agora a linha "http_acess allow all" (liberar acesso http para todos), salve o arquivo e reinicie o serviço (figura 323).

Veja, na figura 324, que o acesso à internet foi liberado.

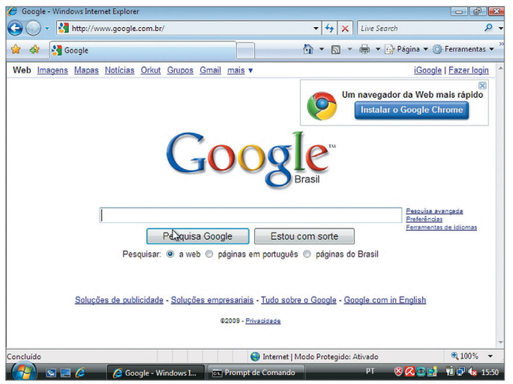


Figura 324
Agora, o acesso à internet.

Figura 325
Criando uma ACL.

```
# And finally deny all other access to this proxy
#http_access deny all
#http_access allow all

acl pcsproibidos src 192.168.0.10-192.168.0.100
http_access deny pcsproibidos

#  TAG: http_access2
#   Allowing or Denying access based on defined access lists
#
#   Identical to http_access, but runs after redirectors. If not set
#   then only http_access is used.
#
#Default:
# none
```

É possível, também, configurar palavras que serão utilizadas para bloquear sites e configurar horário para acesso à internet. Por exemplo, criamos uma ACL (Acess control list – Lista de controle de acesso), que nos permitirá definir regras para que os usuários da rede local acessem a internet (figura 325). Bloqueamos a internet para a faixa de IPs 192.168.0.10 a 100 e reiniciamos o serviço para efetivar as mudanças.

Outro exemplo interessante é bloqueio por palavras-chave. Caso o usuário digite qualquer uma delas em um site de busca, a pesquisa será automaticamente bloqueada. O mesmo acontece com endereços de sites que contenham as palavras escolhidas (figura 326).

Figura 326
Criando uma ACL para palavras-chave.

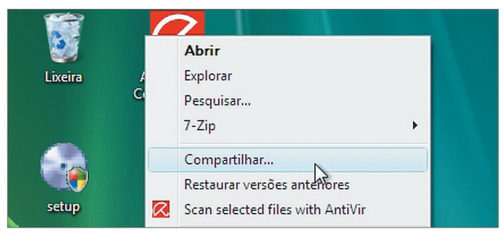
```
#acl pcsproibidos src 192.168.0.10-192.168.0.100
#http_access deny pcsproibidos

acl palavrasproibidas url_regex -i /etc/squid/palavrasproibidas.txt
http_access deny palavrasproibidas

#  TAG: http_access2
#   Allowing or Denying access based on defined access lists
```

Para fazer isso, crie um arquivo de texto chamado “palavrasproibidas.txt” na pasta “/etc/squid” e adicione algumas palavras que devam ser bloqueadas. Por exemplo, as palavras “sexo” e “Orkut”. Reinicie o serviço e tente acessar essas páginas para ver o resultado. Elas não serão exibidas.

9.10. Servidor de arquivos

Uma máquina da rede que tenha uma pasta compartilhada pode ser considerada um servidor de arquivos. Compartilhar uma pasta como essa ajudará o

Figura 327
Compartilhando uma pasta da área de trabalho na rede.



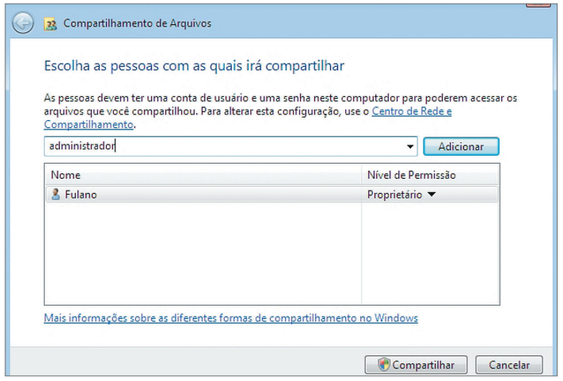


Figura 328
Adicionando usuário ao compartilhamento.

administrador da rede na manutenção dos equipamentos e facilitará a vida dos usuários, que poderão deixar seus arquivos na rede e acessá-los de qualquer outro computador que a integre. Para compartilhar uma pasta no Windows Vista, clique com o botão direito do mouse sobre ela e escolha a opção “Compartilhamento” (figura 327).

O utilitário de compartilhamento de pastas do Windows Vista vai ser exibido na tela. O seu usuário é configurado como proprietário da pasta. Com seu login e sua senha, você poderá acessar essa pasta de qualquer PC da rede. Para acrescentar mais usuários ao compartilhamento, permitindo que eles visualizem a pasta compartilhada ou alterar dados contidos nela, digite o login do usuário e clique em “Adicionar” (figura 328).

Para finalizar, clique no botão “Compartilhar”. Ao finalizar o compartilhamento, o Windows Vista vai apresentar uma janela como a da figura 329. Clique no botão “Pronto” para concluir o compartilhamento.

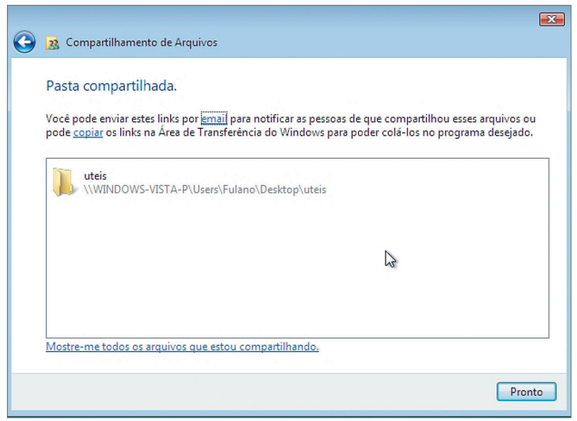
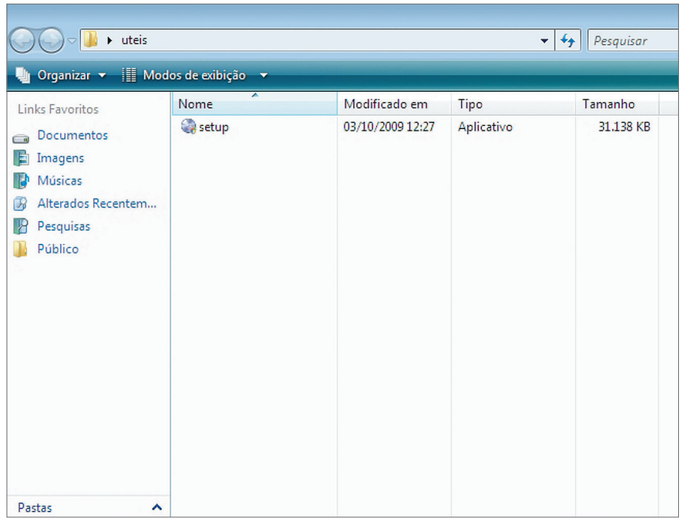


Figura 329
Finalizando o compartimento.

Figura 330
Visualizando a pasta compartilhada.



Vamos agora abrir a pasta compartilhada que está vazia e adicionar um arquivo qualquer (figura 330).

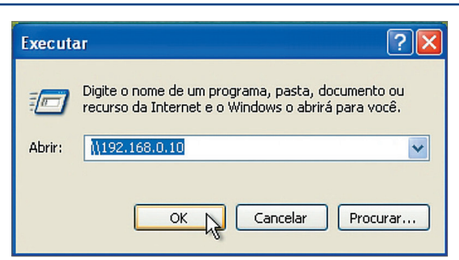
Agora, todos os arquivos copiados para a pasta poderão ser acessados pelos usuários configurados no compartilhamento.

Em outro PC, vamos tentar acessar a pasta compartilhada que está no computador com Windows Vista cujo IP é o 192.168.0.10. Para isso, clique em "Iniciar" e em "Executar" (se estiver usando o Windows XP) ou clique em "Iniciar" e digite na caixa "Pesquisar" do Windows Vista (figura 331).

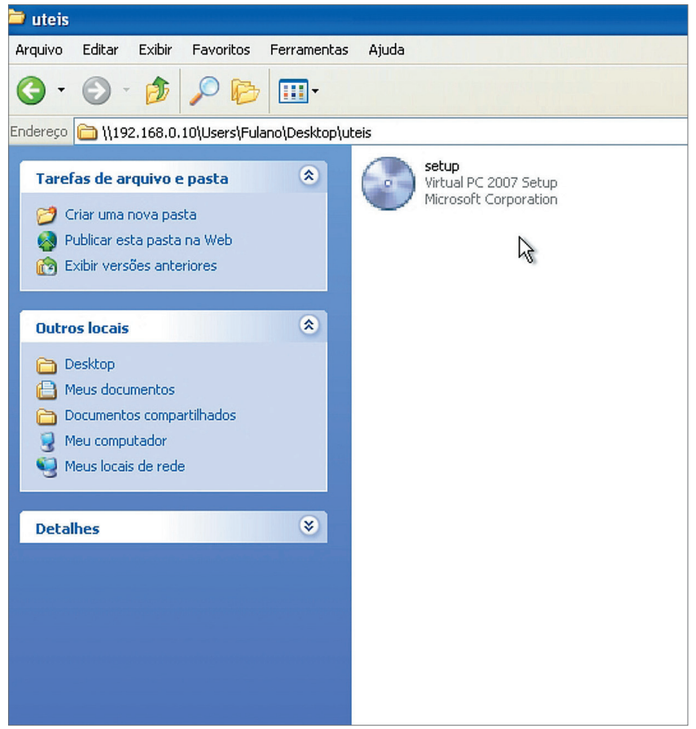
Ao clicar em "OK", o nome do usuário e a senha serão solicitados. Digite-os para visualizar a janela de compartilhamento do servidor. O Windows Vista cria uma estrutura de pastas diferente da que foi criada pelo Windows XP, por exemplo (figura 332).

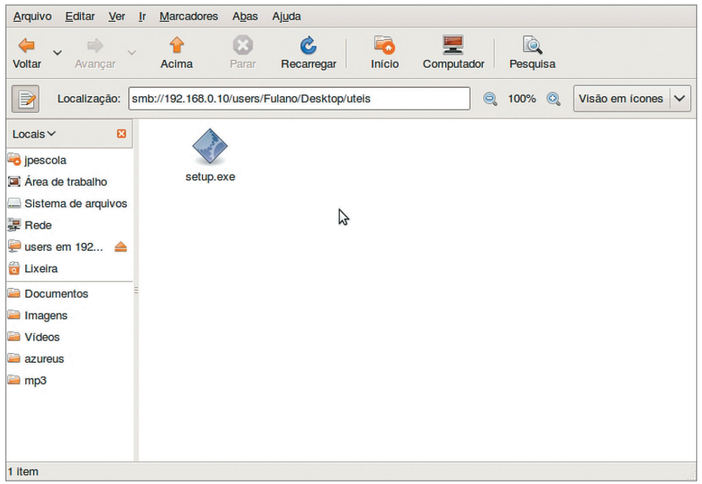
É possível também acessar essa pasta compartilhada a partir de uma máquina Linux. Basta abrir qualquer janela de arquivos ou uma pasta no computador

Figura 331
Acessando um servidor de arquivos da rede local.



Figuras 332 e 333
Visualizando o compartilhamento pelo Windows XP.

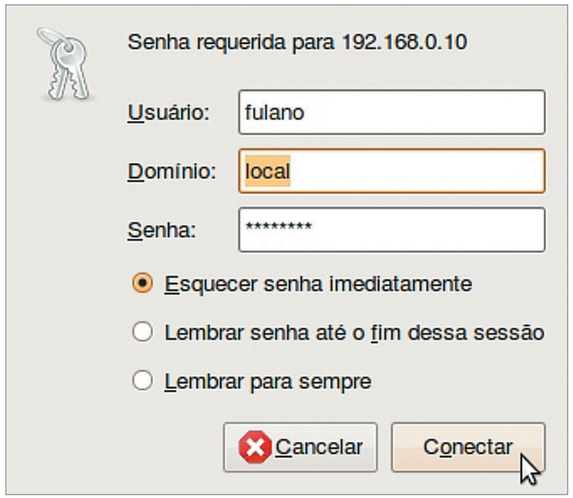




que tenha o Ubuntu instalado e digitar o endereço do servidor utilizando como prefixo os caracteres "**smb://**".

smb é a sigla do protocolo "samba", que permite o compartilhamento de arquivos entre máquinas Linux e Windows.

Figura 334
Digitando usuário e senha para acessar o compartilhamento.



Digite o nome do usuário e a senha na janela que aparece na tela (figura 334).

Agora, vamos compartilhar uma pasta no Ubuntu e acessá-la a partir do Windows (figura 335). Para fazer isso, clique com o botão direito do mouse sobre a pasta que você quer compartilhar e escolha "Opções de compartilhamento".

Na janela que surge, vamos configurar o nome do compartilhamento (figura 336). Veja que podemos configurar a pasta para que ela seja acessada sem a necessidade de digitar um usuário e senha (acesso anônimo). É possível também permitir que outros usuários escrevam na pasta, ou seja, gravem arquivos, deletem, alterem.

Figura 335
Visualizando o compartilhamento por meio do Ubuntu.

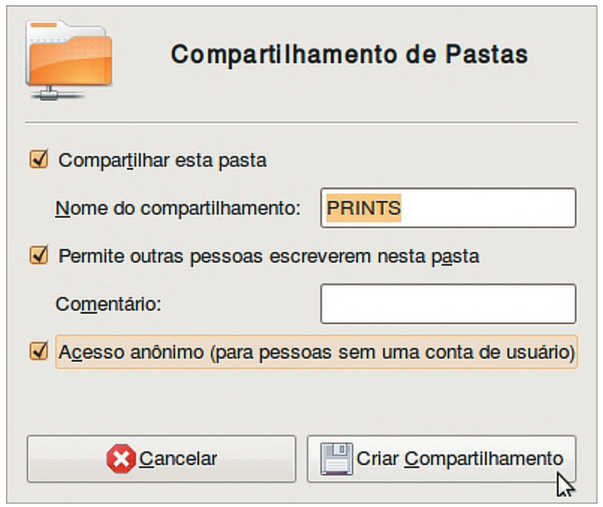
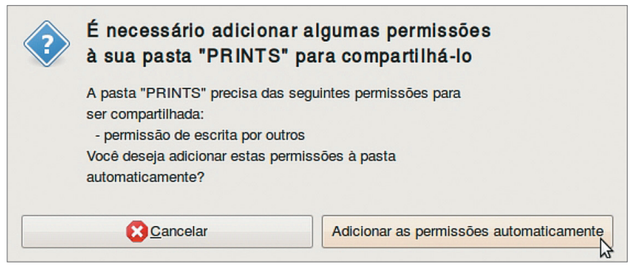


Figura 336
Criando um compartilhamento pelo Ubuntu.

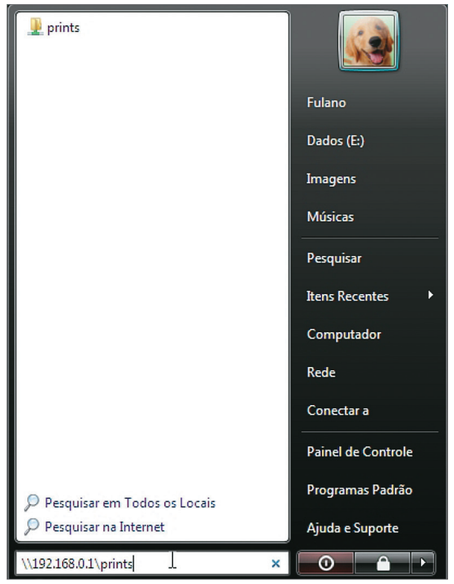


Se o Ubuntu apresentar a informação mostrada na figura 337, clique no botão "Adicionar" para alterar as permissões da pasta. Caso contrário, os usuários não conseguirão acessá-la.

Como último teste, vamos acessar a pasta que está sendo compartilhada no servidor de arquivos Ubuntu por meio do Windows Vista.

Clique no menu "Iniciar". Na caixa de pesquisa, digite as duas barras invertidas seguidas do IP do servidor de arquivo (figura 337).

Figura 337
Habilitando as permissões na pasta.



Você terá acesso aos arquivos da pasta “Prints” (figura 338).

É importante frisar que o compartilhamento de arquivos na rede pode ser muito útil, principalmente se você for atuar como administrador de redes. Além disso, esse recurso facilitará muito a vida de todos os usuários da rede.

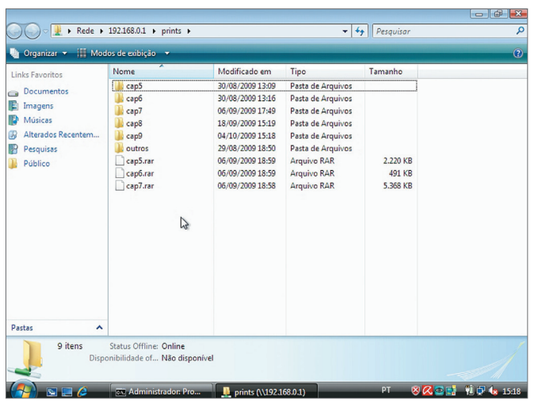


Figura 338
Visualizando a pasta compartilhada no Ubuntu.