

MANUAL DO ALUNO

# DISCIPLINA COMUNICAÇÃO DE DADOS

Módulo 5 (parte 2)

República Democrática de Timor-Leste  
Ministério da Educação



## FICHA TÉCNICA

### TÍTULO

MANUAL DO ALUNO - DISCIPLINA DE COMUNICAÇÃO DE DADOS  
Módulo 5 (parte 2)

### AUTOR

BRUNO MORAIS

COLABORAÇÃO DAS EQUIPAS TÉCNICAS TIMORENSES DA DISCIPLINA  
XXXXXX

### COLABORAÇÃO TÉCNICA NA REVISÃO



### DESIGN E PAGINAÇÃO

UNDESIGN - JOAO PAULO VILHENA  
EVOLUA.PT

### IMPRESSÃO E ACABAMENTO

XXXXXX

### ISBN

XXX - XXX - X - XXXXX - X

### TIRAGEM

XXXXXXX EXEMPLARES

COORDENAÇÃO GERAL DO PROJETO  
MINISTÉRIO DA EDUCAÇÃO DE TIMOR-LESTE  
2015



## Índice

<b>Instalação e Configuração de Rede .....</b>	<b>7</b>
Registo de unidades organizacionais .....	8
Mover contas de utilizadores para unidades organizacionais .....	8
Criar grupos .....	10
Desativar contas .....	11
Alterar palavra-passe de uma conta .....	11
Alterar propriedades de vários utilizadores.....	11
Políticas de grupo .....	12
Utilizadores não abrangidos pelas diretivas .....	17
Remover software .....	17
Acesso às partilhas SYSVOL e NETLOGON .....	18
Partilhas de ficheiros .....	18
Permissões NTFS e de partilha .....	18
Heranças de permissões.....	20
Permissões.....	20
Partilhar pastas.....	24
Gerir as partilhas .....	26
Definir quotas de utilização de disco.....	27
Scripts de login .....	28
Criar um servidor de impressora .....	29
Instalar e partilhar uma impressora local.....	29
Instalar uma impressora partilhada na rede.....	31
Adicionar uma impressora ao diretório de uma UO.....	32
Controlar o acesso à impressora .....	33
<b>Partilha de Ligação com a Internet.....</b>	<b>34</b>
Rede com Internet.....	34
As três funções básicas.....	35

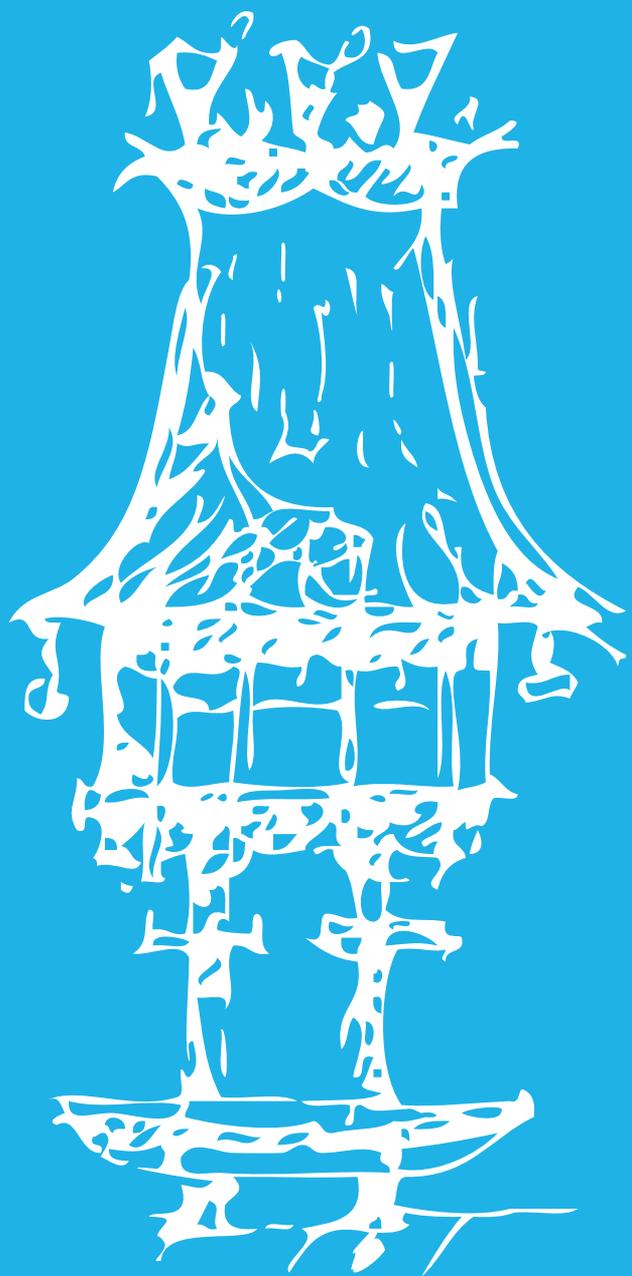


Instalação de modem ADSL .....	39
Descobrir o IP do modem .....	40
O Setup do modem.....	41
Restet para as configurações de fábrica .....	42
Configuração do modem .....	43
Verificação da ligação .....	45
Firewall .....	45
Partilha de ligação ADSL ou a cabo através de um computador.....	46
Computador como Router .....	46
Computador com Internet a cabo .....	46
Computador com banda larga ADSL.....	46
Assistente de rede .....	47
Configuração dos outros computadores .....	51
Instalação de um ADSL Router:D-Link 502G, configuração automática .....	53
Configuração manual de um ADSL Router.....	57
Partilhas com ADSL Modem e Broadband Router .....	60
<b>Redes sem fio .....</b>	<b>69</b>
Padrões.....	69
Técnicas de Transmissão .....	70
Elementos de Hardware .....	71
Tipos de WLAN .....	73
Indoor .....	73
Instalação de uma rede wi-fi AD-HOC .....	76
Instalação de uma rede wi-fi AD-HOC com WEP .....	83
Instalação de uma rede wi-fi com Wireless Broadband Router.....	87
Instalação de uma rede wi-fi com Wireless Broadband Router e WEP .....	94
<b>Segurança em Redes.....</b>	<b>101</b>
Segurança Física da Rede.....	102
Segurança Preventiva de Dados .....	103



Sistemas Ativos de Segurança.....	103
Firewall .....	104
Colocar a nossa rede acessível .....	106
DMZ (DeMilitarized Zone Network).....	108
Filtragem de Conteúdo .....	111
Filtragem de E-Mail.....	111
Filtragem Web .....	112
<b>Bibliografia .....</b>	<b>114</b>







# Instalação e Configuração de Rede

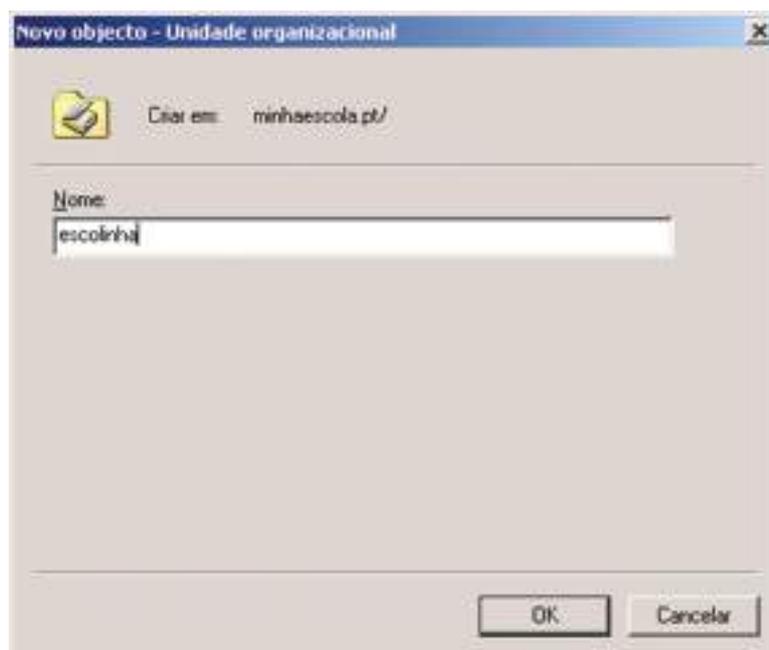
Módulo 5 (continuação)

### *Registo de unidades organizacionais*

As unidades organizacionais são úteis em grandes redes, como de empresas de média ou grande dimensão, o que não é o caso do nosso domínio de uma escola.

Por isso, ficam aqui apenas os passos que indicam como criar uma UO:

1. Acedemos a **Utilizadores e computadores do Active Directory**.
2. Seleccionamos o domínio e clicamos em **UO**.
3. Surge o ecrã em que deve indicar o nome da nova UO.



4. Clicamos em **OK**. Está criada!
5. Podíamos agora repetir os passos 2 a 4, mas já seleccionando no passo 2 uma UO se quiser criar uma dentro de outra. Lembre-se que a ideia das UO é refletir a organização interna da empresa à qual a rede pertence, fazendo distribuição por departamentos, filiais, etc.

### *Mover contas de utilizadores para unidades organizacionais*

Para mover o utilizador **bm** para a UO **escolinha**, siga os passos seguintes:

1. Abrimos a pasta **Users**. Seleccionamos o utilizador **Bruno Morais** com o botão direito do rato e escolhemos **Mover**.

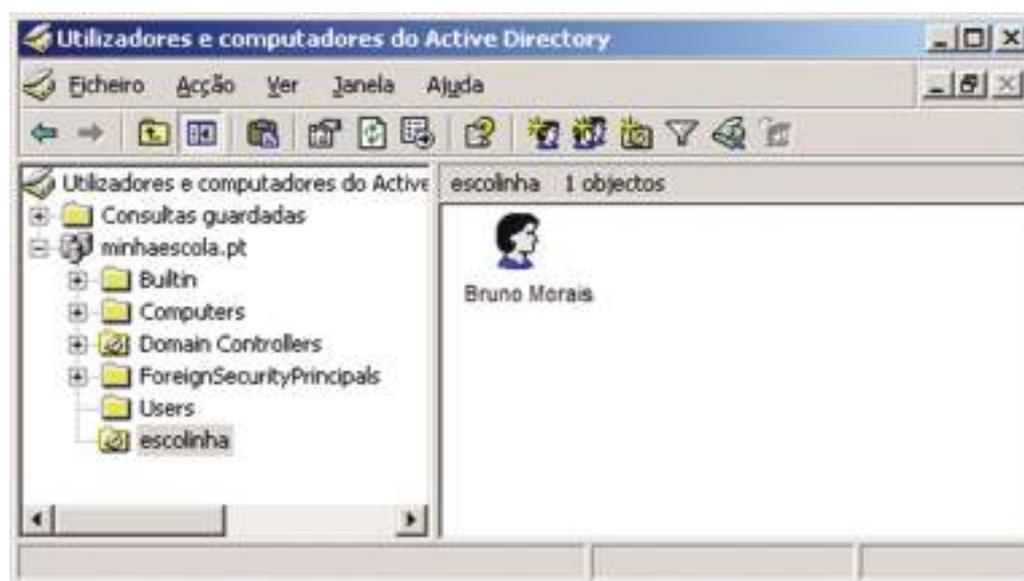




2. Indicamos o seu destino: **escolinha**.



3. Clicamos em OK para terminar a operação. Clicamos agora em **escolinha** para ver o novo membro.

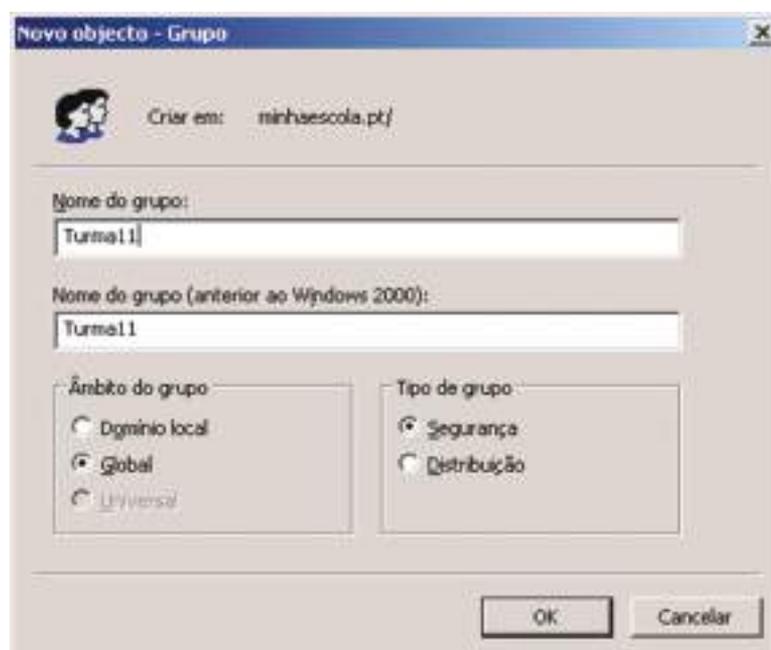


## Criar grupos

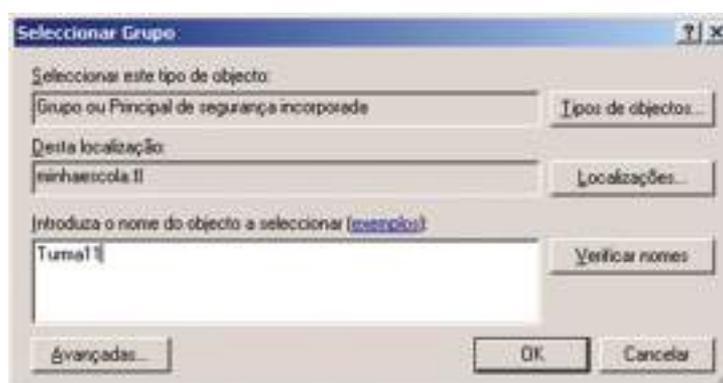
É fácil criar grupos de contas e isso pode facilitar imenso as definições de permissões que vamos ver a seguir. Imagine que, por exemplo, o administrador da rede da escola quer definir permissões para as contas dos alunos de uma turma do 11º ano diferentes das de uma turma de 10º. Agrupando as contas dos alunos numa conta de turma, podemos depois definir permissões para a turma e não aluno a aluno.

Para definir um grupo, siga os passos seguintes:

1. Clicamos no domínio da **minhaescola**. Clique em  .
2. Surge uma caixa onde podemos introduzir o nome do grupo. Clicamos em **OK**.



3. Para juntar contas de utilizadores a este grupo, vamos à lista de utilizadores do domínio, seleccionamos os pretendidos com **Ctrl-clique** e clicamos com o botão direito do rato sobre um dos seleccionados.
4. Do menu que surge, escolhemos **Adicionar a um grupo...** na caixa introduza o nome do grupo.



5. Clicamos em **OK**. Surge uma mensagem de confirmação de aderência ao grupo. Clicamos em **OK** de novo.

## *Desativar contas*

Sempre que uma conta não seja mais necessária, podemos eliminá-la. Siga os passos seguintes:

1. Acedemos à lista de utilizadores.
2. Clicamos com o botão direito do rato sobre a conta que queremos desativar.
3. Escolhemos a opção **Desativar conta**.

## *Alterar palavra-passe de uma conta*

Sempre que queiramos alterar uma palavra-passe de uma conta, pode fazê-lo sem ter de saber a palavra-passe anterior! É muito útil para quem se esqueceu da sua. Siga os passos seguintes:

1. Aceda à lista de utilizadores.
2. Clicar com o botão direito do rato sobre a conta de que quer mudar a palavra-passe.
3. Escolhemos a opção **Repor palavra-passe**.

## *Alterar propriedades de vários utilizadores*

No Server 2003 tornou-se possível editar propriedades de várias contas de utilizadores em simultâneo. Para isso, siga os passos seguintes:

1. Acedemos à lista de utilizadores.
2. Seleccionamos os vários utilizadores através de **Ctrl-clique**.
3. Clicamos com o botão direito do rato sobre um dos seleccionados e escolhemos **Propriedades**. Poderemos alterar propriedades como a do caminho para o perfil, etc.



### *Políticas de grupo*

Uma coisa que faz perder muito tempo aos administradores das redes é a correção das asneiras que os utilizadores fazem, muitas das vezes sem intenção. Mas existe uma forma de diminuir bastante as hipóteses de alguém fazer o que não deve através da gestão centralizada das interfaces das estações de trabalho dos utilizadores através das **políticas de grupo**. Veja alguns exemplos:

- Os computadores de um grupo de funcionários de uma empresa têm apenas os programas com que necessitam trabalhar no menu **Iniciar**.
- Esses programas são instalados e atualizados a partir do servidor pelo administrador.
- O papel de parede do Ambiente de trabalho é o mesmo em todos e não pode ser alterado.
- Os atalhos no Ambiente de trabalho são apenas **O meu computador** e **Os meus documentos**.
- O conteúdo da pasta **Os meus documentos** está armazenado no servidor.
- O Painel de controlo não está acessível.

Usando a ferramenta **Utilizadores e computadores do Active Directory** é possível definir **políticas de grupo** que permitem:

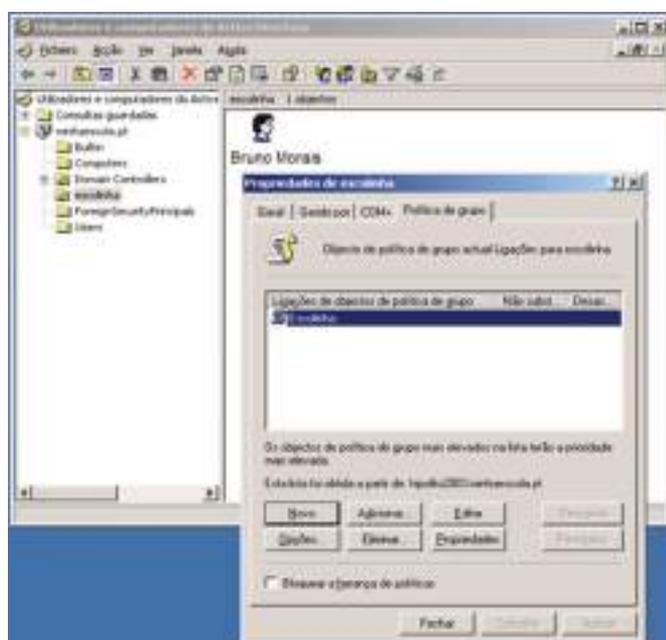
- **Instalações, atualizações e remoções de software** nas estações dos utilizadores
- **Redirecionamento de pastas** – pastas como **Os meus documentos**, **Ambiente de trabalho** e **Dados de aplicação** podem ser redirecionados para pastas no servidor
- **Configuração do ambiente** – pode estabelecer definições para **Ambiente de trabalho**, menu **Iniciar**, etc nas várias estações dos clientes.

Vejamos um exemplo de como fazer para conseguir isto. Acompanhe os passos seguintes:

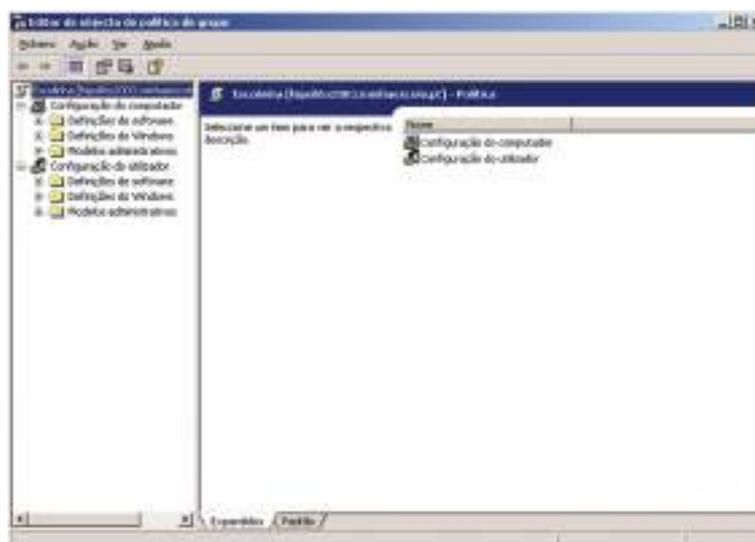
1. Acedemos a **Utilizadores e computadores do Active Directory**.
2. Seleccionamos a Unidade Organizacional **escolinha**.
3. Clicamos sobre ela com o botão direito do rato e seleccionamos **Propriedades**.
4. Seleccionamos o separador **Política de grupo**.



5. Clicamos no botão **Novo**.
6. Escrevemos 'escolinha' e carregamos **ENTER**.



7. Clicamos no botão **Editar**. Surge uma nova consola.



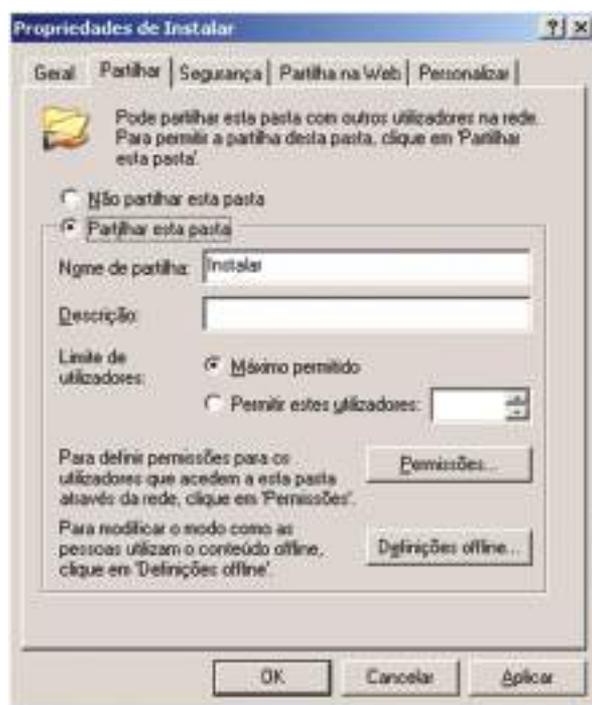
Nessa consola podemos navegar por mais de 640 itens configuráveis para os computadores e utilizadores da OU **escolinha**. Vejamos como estão desde logo separadas as configurações em: **Configuração do computador** e **Configuração do utilizador**. Estas últimas acompanham o utilizador para qualquer computador que vá, desde que tenha o Windows 2000, XP, ou superior.

Neste exemplo, vamos definir os programas a serem utilizados na **escolinha** e restringir o acesso ao **Painel de Controlo**.

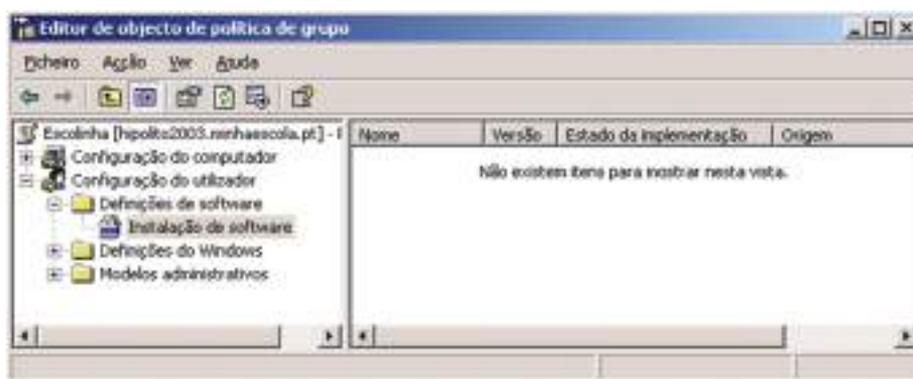


A instalação de software a partir do servidor pressupõe que o pacote de instalação esteja no formato MSI (do *Windows Installer*) e não num executável do tipo **Setup.exe**. De qualquer forma, através de programas como o Advanced Installer da Aphyon é possível criar estes pacotes.

8. Criamos uma pasta chamada **Instalar** na raiz da unidade dos dados (seja **D:**) e copiamos para lá os pacotes MSI dos programas que queremos instalar.
9. Acedemos às **Propriedades** da pasta **Instalar** e no separador **Partilhar** clicamos em **Partilhar esta pasta**. Clicamos em **OK**.



10. Voltamos à consola do **editor de políticas de grupo**. Seleccionamos o item **Configuração do utilizador-> Definições de software->Instalação de software**.



11. Clicamos sobre esse item com o botão direito do rato e escolhemos **Novo...>pacote**.

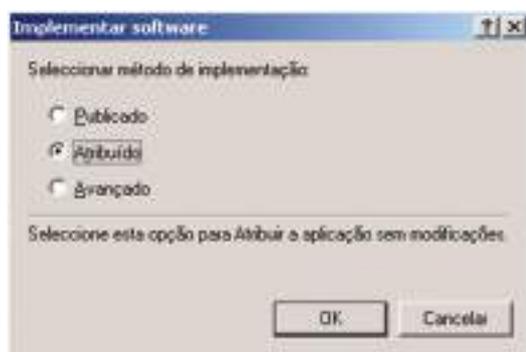


12. Abre-se uma janela a partir da qual podemos indicar o pacote MSI desejado.
13. Na caixa **Nome do ficheiro** escrevemos \\HIPOLITO2003\Instalar e carregamos **ENTER**. Abre-se a pasta Instalar.

**NOTA:**

Existem dois modos para instalar software deste modo centralizado. Um é mais usado para aqueles programas mais frequentemente usados como o Microsoft Office: é o modo atribuído. Ao utilizar este modo, os atalhos para os programas são inseridos no menu Iniciar e a instalação dá-se na primeira utilização. O segundo modo, o publicado, é recomendado para utilitários como o WinZip e outros. Neste modo, os programas são colocados na lista Adicionar/remover programas do Painel de controlo. Depois, o utilizador instala-o quando pretender.

14. De lá selecionamos um dos pacotes MSI a instalar. Clicamos em Abrir. Selecionamos o modo, por exemplo Atribuído. Clicamos em OK. Pronto, definimos um pacote que será instalado a próxima vez que for selecionado pelos utilizadores no menu Iniciar.



15. Vamos agora restringir o acesso ao **Painel de controlo**. Acedemos ao item **Configuração do utilizador->Modelos administrativos->Painel de controlo**.

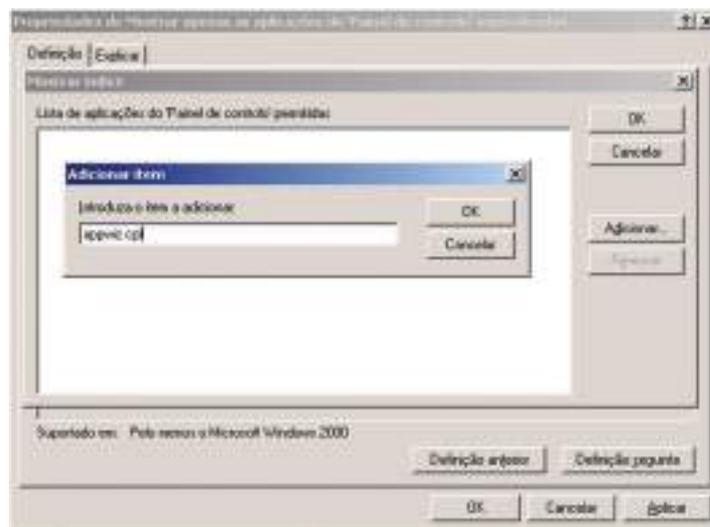


16. Damos um duplo clique no item **Mostrar apenas as aplicações do Painel de controlo especificadas**.

17. Clicamos em **Ativado** e depois em **Mostrar**.



18. Clicamos em **Adicionar...** e depois em **appwiz.cpl**.



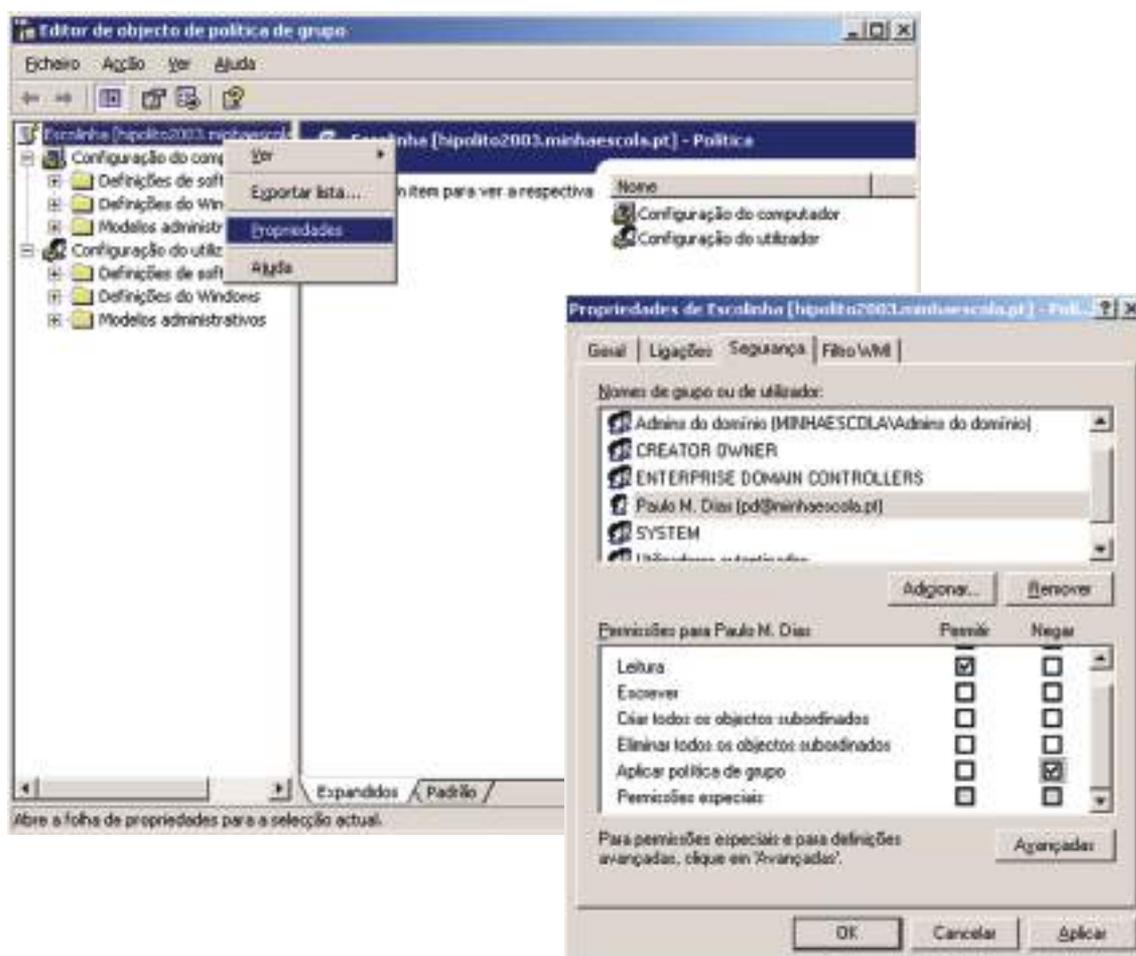
19. Clicamos em **OK**. Clicamos novamente em **Adicionar** e escrevemos **main.cpl**. Clicamos em **OK** duas vezes para fechar a janela da política. Cada ficheiro **.cpl** designa um ou mais ícones do Painel de controlo (**cpl – control panel**). Com estes dois exemplos vedamos o acesso à adição/remoção de *software* e ao controlo de *hardware*.

Há Muitas outras diretivas possíveis, mas assim já terá ficado com uma ideia de como proceder.



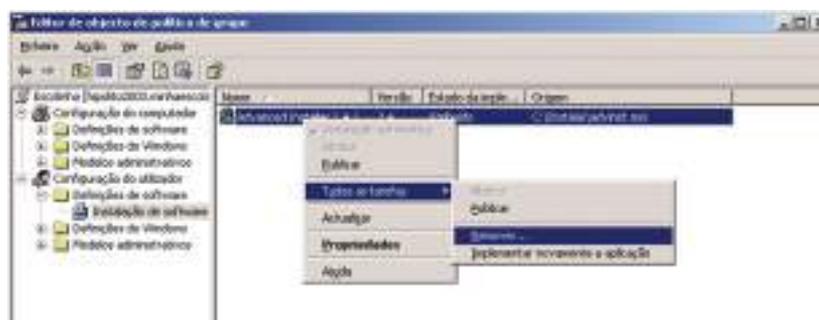
## Utilizadores não abrangidos pelas diretivas

Para fazer com que alguns utilizadores da UO não sejam afetados pelas políticas restritivas, podemos aceder às **Propriedades** da OU e lá, no separador **Segurança**, especificar para quem não quisermos incluir, a **negação** de **Aplicar política de grupo**.



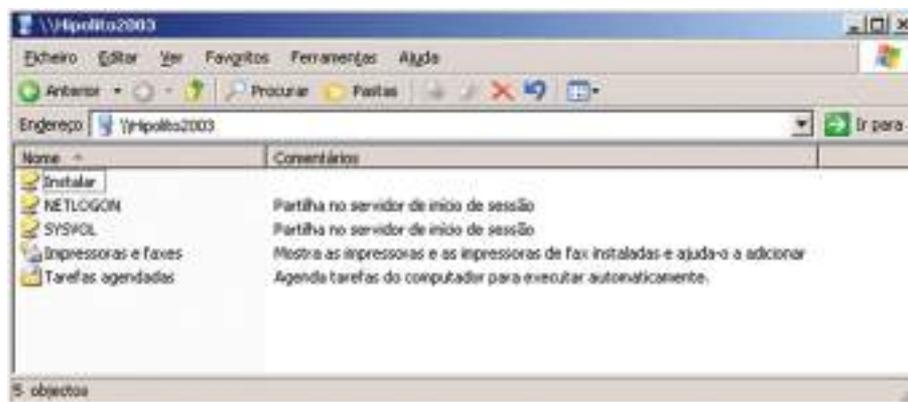
## Remover software

Quando quisermos 'desinstalar' um programa instalado, basta clicar sobre ele na secção de **Instalação de software** com o botão direito do rato, seleccionar **Remover...** e depois **Desinstalar imediatamente do software dos utilizadores e computadores**.



## Acesso às partilhas SYSVOL e NETLOGON

É importante testar este acesso. Tente aceder-lhes através d'O meu computador:



Se não estiverem disponíveis, tentamos reiniciar o serviço **Início de sessão de rede** através da ferramenta **Serviços** das **Ferramentas administrativas** ou, mais facilmente, pela **linha de comandos**:

- net stop netlogon [ENTER]
- net start netlogon [ENTER]

Para erros mais graves, no CD do Windows Server 2003, encontramos uma ferramenta designada **DCDIAG.EXE** que faz uma análise completa e gera um relatório pormenorizado.

## Partilhas de ficheiros

Vamos fazer aqui uma introdução àquela que é a tarefa mais comum numa rede: a partilha de ficheiros e impressoras. Um aspeto que convém lembrar é o do tipo de sistema de partilhas. Numa rede *peer-to-peer* constituída por computadores com o Windows XP, temos a **partilha de ficheiros simples** e a **partilha de ficheiros avançada**. No Windows 2000 o sistema de partilhas era muito semelhante ao da partilha avançada.

## Permissões NTFS e de partilha

Quando estamos numa rede cliente/servidor, a única forma de partilha é a **avançada**. E aí convém lembrar a questão das permissões.

- Primeiro: no separador **Segurança** definem-se as permissões de **acesso local**, ou seja, as permissões para as contas que iniciam sessão nesse computador e tentam aceder à pasta.



- Segundo: no separador Partilhar podem definir-se permissões para a pasta que se pretende partilhar.
- Terceiro: quando um utilizador acede pela rede a uma pasta partilhada, o Windows Server (e o XP, já agora...) verifica as suas permissões nas duas listas e, caso a conta esteja nas duas, a permissão que o Windows dá é a que for mais restritiva das duas. Por exemplo, se definir que a permissão a nível de partilha para um dado utilizador é de **Modificar**, mas a nível local for **Leitura**, é esta que vale.

Permissões para pastas	NTFS	Permite ao utilizador
<b>Ler</b>		Ver ficheiros e subpastas na pasta e ver a quem a pasta pertence, suas permissões e atributos.
<b>Escrever</b>		Criar novos ficheiros e subpastas nesta pasta, alterar os atributos da pasta, ver a quem a pasta pertence, suas permissões e atributos.
<b>Listar o conteúdo das pastas</b>		Ver os nomes dos ficheiros e sub-pastas lá contidos.
<b>Ler e executar</b>		Passear-se pela pasta para chegar a outras subpastas, mesmo que os utilizadores não tenham permissões para essas pastas, e executar o que é permitido pelas permissões <b>Ler</b> e <b>Listar o conteúdo das pastas</b> .
<b>Modificar</b>		Eliminar a pasta mais o que é permitido pelas permissões <b>Escrever</b> e <b>Ler e executar</b> .
<b>Controlo total</b>		Mudar as permissões, ficar com a pasta para si, eliminar ficheiros e subpastas e o que é permitido por todas as outras permissões.



Permissão NTFS para ficheiros	Permite aos utilizadores
<b>Ler</b>	Ler o ficheiro, ver os seus atributos, permissões e a quem pertence.
<b>Escrever</b>	Alterar o ficheiro, mudar os seus atributos, ver as suas permissões e a quem pertence.
<b>Ler e executar</b>	Executar aplicações, mais o que é permitido pela permissão <b>Ler</b> .
<b>Modificar</b>	Modificar e eliminar o ficheiro, mais o que é permitido pelas permissões <b>Escrever</b> e <b>Ler e executar</b> .
<b>Controlo total</b>	Mudar permissões, ficar seu dono, mais todas as outras permissões anteriores.

## Heranças de permissões

As permissões para uma unidade de disco são herdadas por todas as pastas lá criadas.

Cuidado: nunca altere as permissões para a unidade C: (ou outra onde estiver o Windows instalado).

## Permissões

Vamos experimentar definir e verificar as permissões para um ficheiro. Siga os passos seguintes:

1. Acedemos à nossa pasta **Os meus documentos**.
2. Criamos um novo ficheiro de texto (**Novo->Documento de texto**).
3. Damos ao ficheiro o nome de **meutexto.txt**.
4. Acedemos às **Propriedades** do ficheiro com o botão direito do rato.
5. No separador **Segurança**, observe as permissões NTFS. Repare como as permissões estão a cinzento, porque foram herdadas da pasta. Não podem ser modificadas. Também não podemos remover nenhuma entidade da lista. (Experimente!)





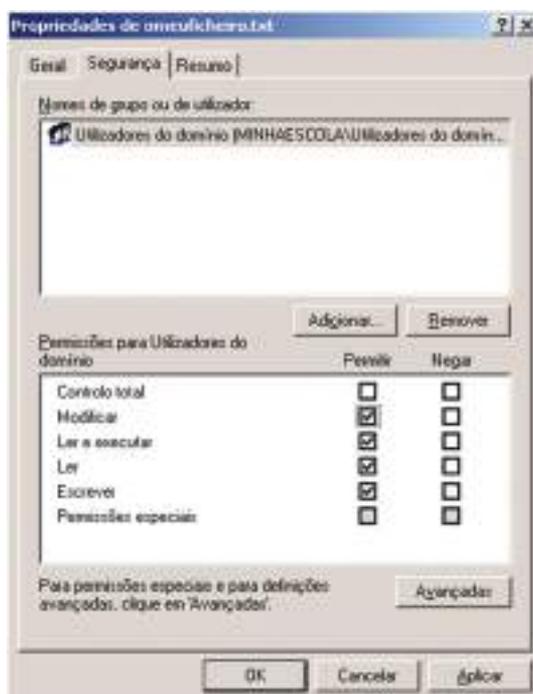
6. Para remover a ligação da herança, clicamos em **Avançadas**. Desmarcamos a opção **Permitir que as permissões herdáveis(...)**. Ao romper a ligação da herança, o sistema dá-nos duas opções: remover as permissões que anteriormente eram aplicadas ou copiar as permissões que foram aplicadas anteriormente. Clicamos em **Remover**. Clicamos em **OK**.



7. Surge uma mensagem de aviso. Clicamos **Sim**.

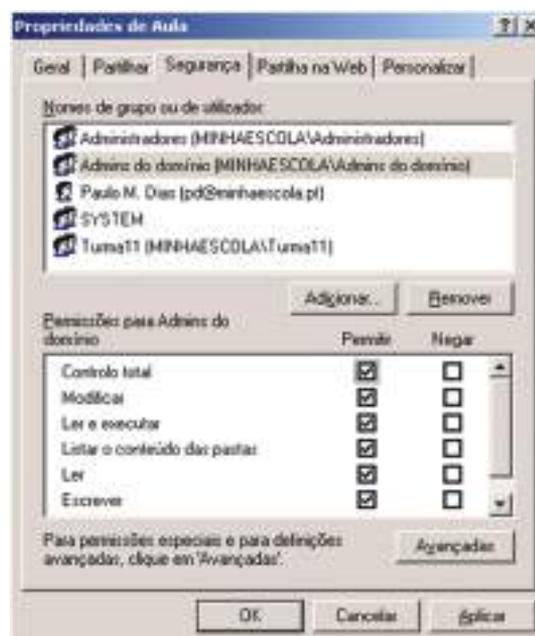


8. Agora já podemos definir novas permissões. Clicamos em **Adicionar**. Escrevemos **utilizadores do domínio** e clicamos em **OK**.
9. Damos-lhes a permissão de **Modificar**.
10. Clicamos em **OK**.

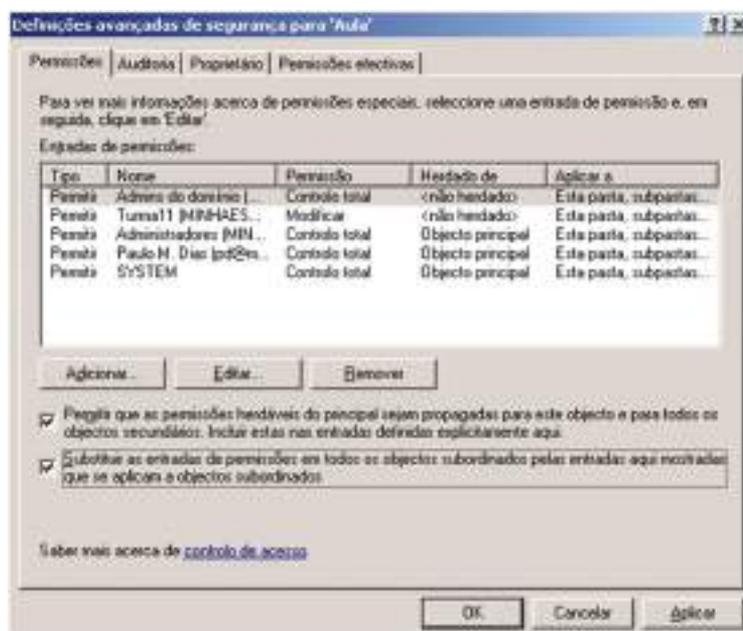


Podemos definir as permissões de uma pasta e de todo o seu conteúdo. Querem experimentar? Siga os passos seguintes:

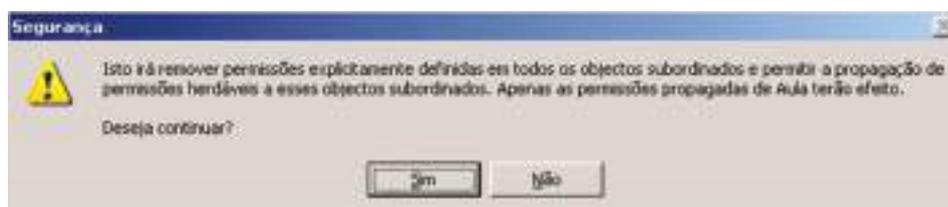
1. Criamos uma pasta de nome **Aula** sob a pasta **Os meus documentos**.
2. Acedemos às suas **Propriedades**, separador **Segurança**.
3. Permitimos **Modificar** aos utilizadores do grupo **Turma11** e Controlo total ao grupo dos **Admins do domínio**.



4. Clicamos em **Avançadas**.
5. Marcamos a opção **Substituir as entradas(...)** e clicamos em **OK**.



6. É-nos pedida a confirmação. Lemos com atenção e carregamos **Sim**.



7. Clicamos em **OK**.

Pronto, modificamos as permissões para esta pasta e para todo o seu conteúdo dando permissões a mais alguém.

E quanto a negar permissões? Negar contraria qualquer permissão. Para tal siga os passos seguintes:

1. Criamos um utilizador **João Antunes** neste domínio. Lembram-se como?
2. Voltamos a **Os meus documentos** e criamos um documento de texto na pasta **Aula** com o nome **tampa.txt**.
3. Acedemos às permissões do documento e no separador **Segurança** clicamos em **Adicionar**. Adicionamos o utilizador **João** às permissões e **negamos** a permissão de **Leitura**.
4. É-nos pedida uma confirmação. Confirmamos clicando em **Sim**.
5. Terminamos sessão e iniciamos outra com o utilizador **João**. Experimentem aceder ao ficheiro **tampa.txt**. Que aconteceu?



## Partilhar pastas

Para partilhar uma pasta, siga os passos seguintes:

1. Clicamos com o botão direito sobre a pasta a partilhar.
2. Seleccionamos a opção **Partilha e segurança**.
3. Marcamos a opção **Partilhar esta pasta**.
4. Definimos um nome para a partilha.
5. Introduzimos um comentário que poderá ser visto nos outros computadores aproximando o cursor do rato do ícone da partilha. A partilha ficará facilmente acessível pelo caminho **\\HIPOLITO2003\BM**.



6. Clicamos no botão **Permissões**.

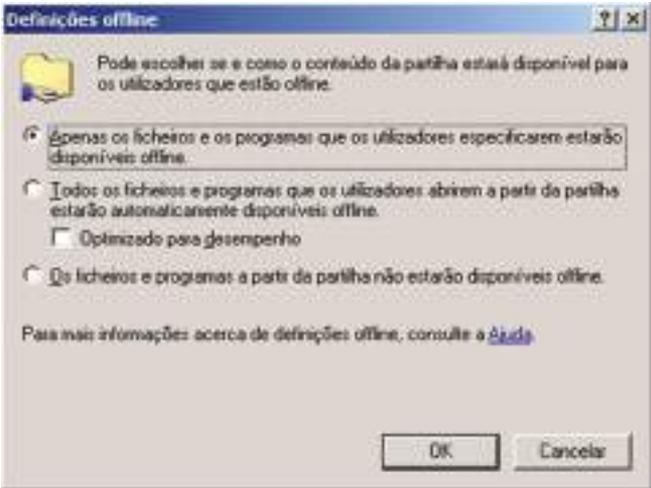


7. Observe que a pasta surge com permissão de leitura para o grupo **Todos**. Vamos agora refinar esta **lista de controlo de acesso**. Clicamos em **Remove** e depois em **Adicionar**.
8. Escrevemos **utilizadores** e depois clicamos em **Verificar nomes**.



9. Seleccionamos **Utilizadores do domínio** e clicamos **OK** duas vezes.
10. Seleccionamos – se não estiver já – o grupo **Utilizadores do domínio** e marcamos a opção **Alterar** na coluna **Permitir**.
11. Repetimos o procedimento anterior para o grupo **Admins do domínio** e marcamos para eles a opção **Controlo total** na coluna **Permitir**.

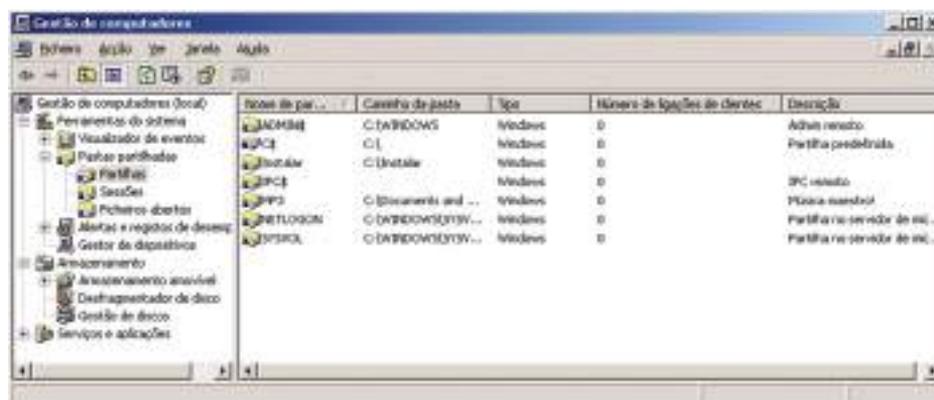


12. Clicamos em **OK**.
13. Voltando à caixa inicial, repare que ainda podemos definir na caixa **Permitir estes utilizadores** o número de utilizadores que, em simultâneo, podem aceder a esta partilha. Indiquemos 10.
14. Clicamos no botão **Definições offline**. Esta opção é muito útil, pois permite sincronizar os ficheiros partilhados na rede com os computadores clientes durante o início e/ou o fim de sessão. Como podem ver, existem três possibilidades.
 
15. Mantemos a primeira selecionada que é a mais razoável e clicamos em **OK** duas vezes.
16. E pronto! Partilhamos uma pasta com os nossos colegas de domínio: os utilizadores podem fazer alterações à pasta mas não eliminá-la, coisa que só os administradores podem.

## Gerir as partilhas

Na ferramenta **Gestão de computadores** é possível controlar o acesso às partilhas. Siga os passos seguintes:

1. Abrimos a ferramenta **Gestão de computadores** das **Ferramentas administrativas**.
2. Em **Pastas partilhadas->Partilhas** podemos controlar as partilhas e os acessos.



Podemos cancelar uma partilha clicando com o botão direito do rato sobre a partilha e escolhemos a opção **Deixar de partilhar**.

Podemos criar uma nova partilha clicando com o botão direito sobre **Partilhas** e escolhemos **Nova partilha...** teremos um Assistente para nos ajudar a definir a partilha.

Para um maior controlo de todas as sessões abertas, clicamos em **Partilha->Sessões**.

Para ver os ficheiros acedidos, clicamos em **Partilha->Ficheiros abertos**.

## Definir quotas de utilização de disco

É conveniente limitar o espaço em disco usado pelos utilizadores. Para isso sigamos os passos seguintes para ver um exemplo para a unidade **C:** mas que é normalmente usada para a unidade de dados onde estão pastas partilhadas, etc:

1. Acedemos às propriedades de **C: n' O meu computador**.
2. Acedemos ao separador **Quota**.

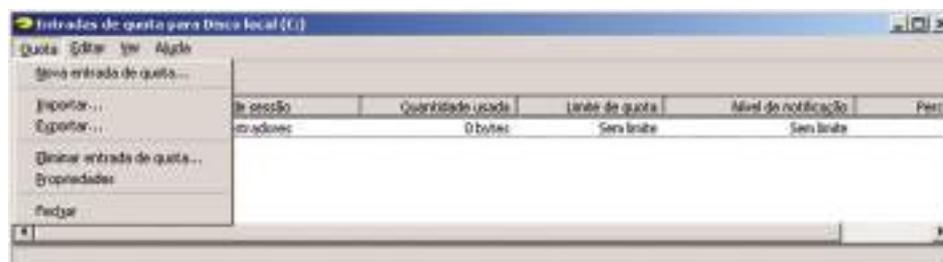


3. Marcamos as opções **Ativar gestão de quotas**, **Negar espaço em disco para utilizadores que excedam o limite de quota**, **Registar evento quando um utilizador excede o respectivo limite de quota** e **Registar evento quando um utilizador excede o respectivo nível de aviso**.
4. No campo **Limitar espaço em disco** digitamos valor de 600MB (não se esqueçam de alterar a unidade de KB para MB). No campo **Definir nível de notificação como**

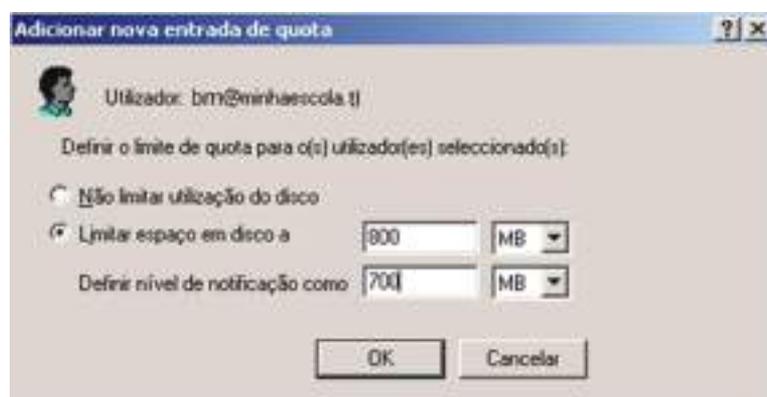


introduzimos um valor ligeiramente abaixo do anterior, como 500MB. É apenas para gerar um aviso!

5. Para discriminarmos quotas por utilizador, carregamos em **Entradas de quota**.
6. No menu **Quota**, escolhemos **Nova entrada de quota**.



7. Tal como nas permissões, podemos adicionar contas individuais, de grupo, etc. Adicione uma conta individual como **Bruno Morais**. Defina limites para esta conta.



## Scripts de login

É importante saber que podemos criar *scripts* que obriguem à execução de comandos no início de sessão de alguns utilizadores. Já nos referimos a isso antes, na criação de contas de utilizadores. Os *scripts* e os utilizadores que os vão ter podem então ser definidos no separador **Perfil** das propriedades das contas, usando a ferramenta **Utilizadores e computadores do Active Directory**. Assim, eles são colocados na pasta **C:\WINDOWS\SYSVOL\Sysvol\nomedodomínio\scripts**.

Siga os passos para acompanhar este processo:

1. Iniciamos sessão com a conta **Administrador**.
2. Entramos na **linha de comandos**.
3. Escrevemos **cd \windows\sysvol\sysvol\minhaescola.pt\scripts** e prima **ENTER**.



4. Escrevemos **edit** e teclamos **ENTER**.
5. Criamos um ficheiro com as 2 linhas seguintes:
6. NET TIME \\HIPOLITO2003 /SET /YES
7. NET USE E: /D
8. Gravamos o ficheiro com o nome **ENTRADA.BAT**.
9. Saímos da linha de comandos com **EXIT**.
10. Acedemos agora à ferramenta **Utilizadores e computadores do Active Directory**.
11. Acedemos às propriedades de um utilizador, por exemplo o Bruno Morais.  
(Podemos selecionar mais com a tecla Ctrl).
12. No separador **Perfil**, escrevemos no campo **Script de início de sessão**: ENTRADA.  
BAT e clicamos **OK**.
13. Terminamos sessão e iniciamos com a conta **bm** (ou aquela para a qual inseriu o script).
14. Observamos como o *script* foi executado.

### *Criar um servidor de impressora*

Como já foi referido anteriormente, numa rede podemos ter impressoras ligadas diretamente à rede ou ligadas a computadores que, nessa altura, as podem partilhar. E o Server 2003 permite acesso por HTTP a impressoras, com um endereço do tipo `http://servidor/printers/impressora` se o servidor tiver o IIS instalado.

### *Instalar e partilhar uma impressora local*

Siga os passos seguintes:

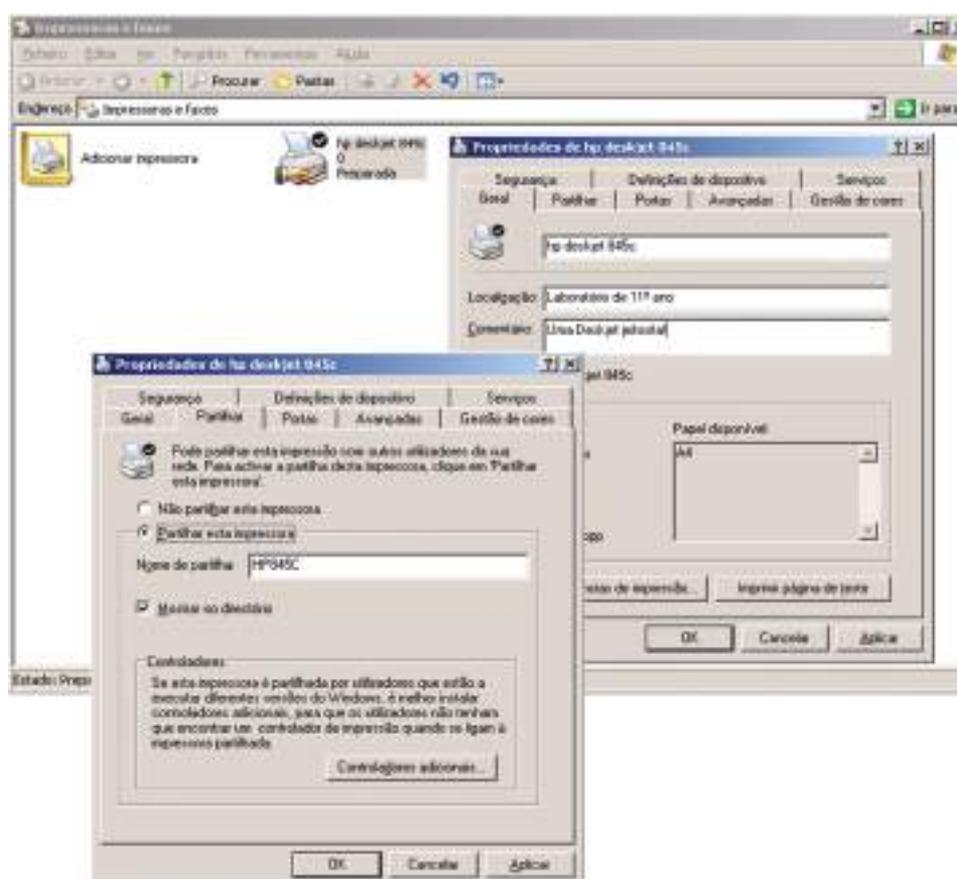
1. Ligamos a impressora ao servidor.
2. Acedemos a menu **Iniciar->Impressoras e faxes**.
3. Damos um duplo clique em **Adicionar impressora**.
4. Seguimos as instruções do Assistente.





A maioria das impressoras atuais são Plug&Play, por isso, muito naturalmente o Windows vai detetá-la e instalá-la sozinho. Repare que, no final, ela estará partilhada. Há agora que introduzir alguns dados sobre ela, nomeadamente:

- A localização;
- Um comentário;
- Um nome de partilha.



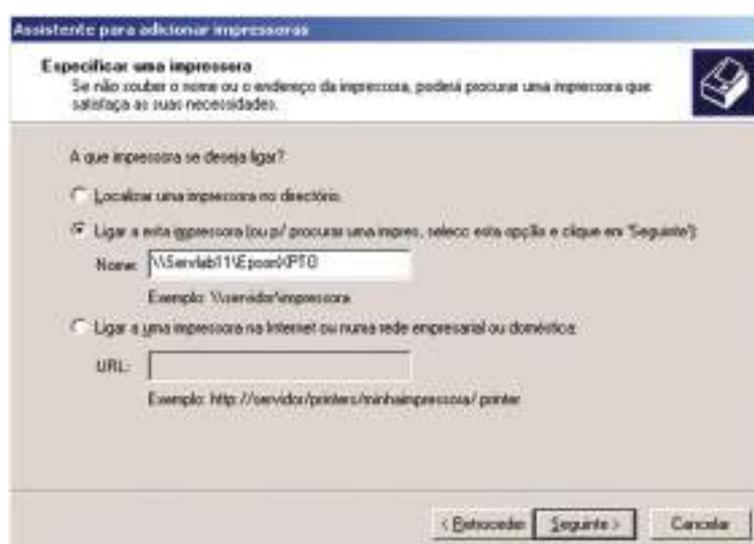
## Instalar uma impressora partilhada na rede

Siga os passos seguintes:

1. Ligamos a impressora ao servidor.
2. Acedemos ao menu **Iniciar->Impressoras e faxes**.
3. Damos um duplo clique em **Adicionar impressora**.
4. No segundo passo do Assistente, escolhemos a opção **Uma impressora de rede ou uma impressora ligada a outro computador**.



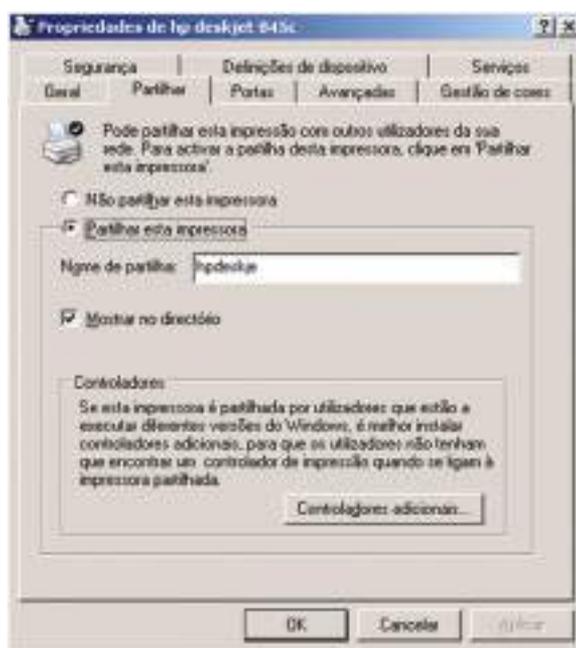
5. No passo seguinte, podemos optar por pesquisar a impressora no diretório ou indicar o seu endereço, se o soubermos.
6. Siga o Assistente até ao final e peça para imprimir uma página de teste.



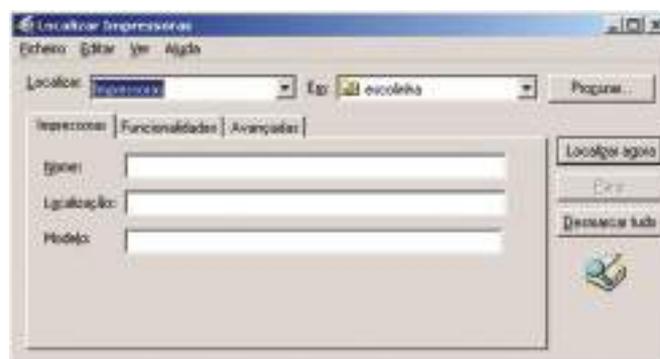
## Adicionar uma impressora ao diretório de uma UO

Uma impressora tem de ser adicionada ao Active Directory para que conste dele como um objeto físico e assim possa ser localizada. Siga os passos seguintes para saber como adicionar uma impressora ao AD:

1. Acedemos às **Propriedades** da impressora.
2. Vamos ao separador **Partilhar**.
3. Verificamos se a opção **Mostrar no diretório está ativa**. Senão, ativamo-la.



4. Acedemos à ferramenta **Utilizadores e computadores do Active Directory**.
5. Seleccionamos o domínio **minhaescola.tl**. Clicamos no botão  e seleccionamos **Impressoras** no campo **Localizar**.



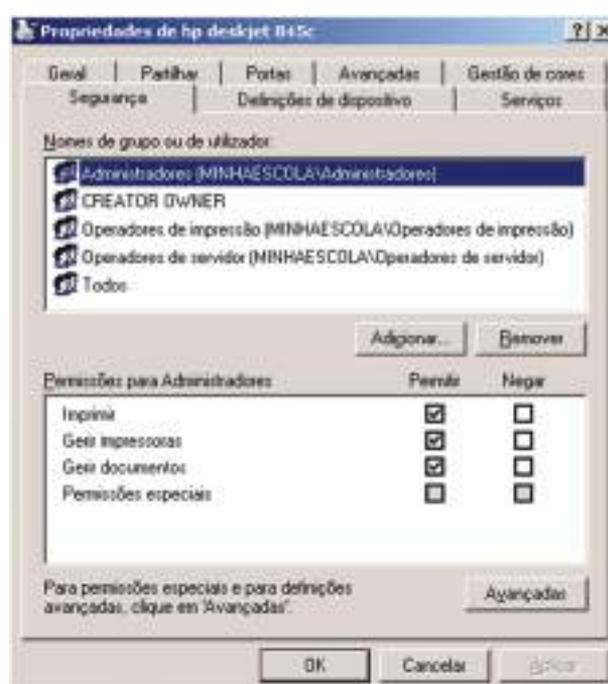
6. Clicamos em **Localizar agora**. As impressoras localizadas serão listadas.
7. Seleccionamos a impressora que queremos adicionar e clicamos sobre ela com o botão direito do rato, seleccionando **Mover...**



8. Seleccionamos a Unidade Organizacional **escolinha**.
9. Clicamos em **OK**. A impressora também passa a estar acessível na **escolinha** a partir de agora.

## Controlar o acesso à impressora

É possível controlar o acesso a uma impressora para gerir melhor o gasto dos tinteiros, *toners*, etc. Basta aceder ao separador **Segurança** das **Propriedades** da impressora e definir permissões, quase como sobre uma pasta.



# Partilha de Ligação com a Internet

## Rede com Internet

Sem dúvida um dos mais importantes tipos de partilha é o da conexão com a Internet. As redes instaladas em empresas, há muito oferecem acesso à Internet. Já as redes de pequeno porte, sobretudo as domésticas, somente há pouco tempo têm oferecido este recurso.

Um grande marco para a difusão da Internet em redes pequenas foi o Windows 98SE, que trazia o recurso ICS (Internet Connection Sharing, a partilha de conexão com a Internet). Para partilhar uma conexão de Internet com dois computadores basta conectá-los através de duas placas de rede e um cabo crossover, e configurá-los adequadamente, como mostraremos mais adiante.

Esta partilha aplica-se a conexões por linha telefónica (dial-up) e banda larga.

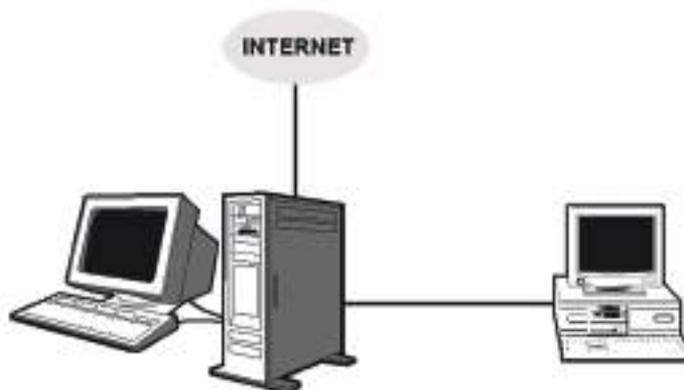


Figura 156: Exemplo de rede com Internet.

O acesso à Internet pode ser distribuído para todos os computadores da rede, e existem vários métodos para o fazer. Todos os métodos têm uma coisa em comum: é preciso que os computadores estejam ligados em rede, através de hub ou switch.

No exemplo da figura 157, o computador que está ligado à Internet foi configurado para partilhar a sua conexão. Quando um computador faz este papel, é chamado **gateway**. O método apresentado na figura tem apenas uma desvantagem: exige que o gateway esteja ligado para que os outros computadores acessem à Internet.

NOTA: Existem outros métodos de partilha que não exigem que um computador seja ligado para que os outros tenham acesso. Basta usar um Router.



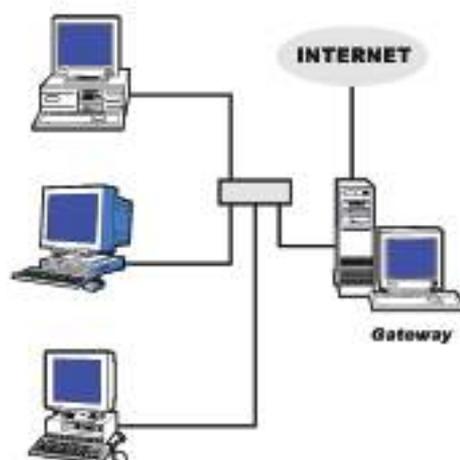


Figura 157: Exemplo de partilha de internet nom Gateway

### As três funções básicas

A partilha com a Internet pode ser feita de inúmeras formas, mas em todas elas podemos destacar três funções básicas. Na maioria dos casos usamos equipamentos que acumulam duas delas, ou até mesmo as três:

- 1) Modem: Faz a interface com a Internet
- 2) Router: Distribui a conexão para uma rede interna
- 3) Concentrador: Pode ser um hub ou switch, fornece a conexão para a rede

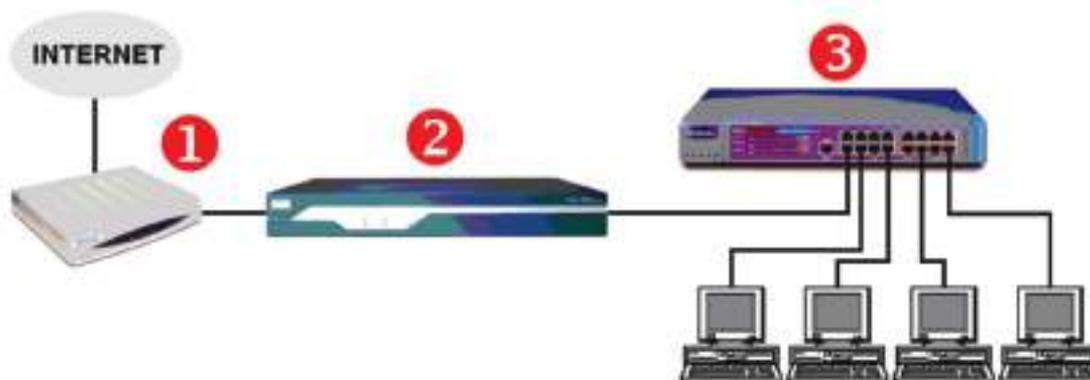


Figura 158: As tres funções básicas.



## Exemplo 1:



Figura 159: Exemplo de partilha de Internet

Um router de banda larga (Broadband Router) pode ser ligado a modems ADSL (Velox, Speedy) ou Cable modem, e distribuir a conexão para a Internet. Muitos desses routers integram também um switch, portanto acumulam as funções 2 e 3 do nosso diagrama. O modelo do exemplo acima é um router com switch integrado para 4 portas Ethernet. Se quisermos ligar um número maior de computadores podemos ligar um switch comum, em cascata.

## Exemplo 2 (Broadband Router/Switch):

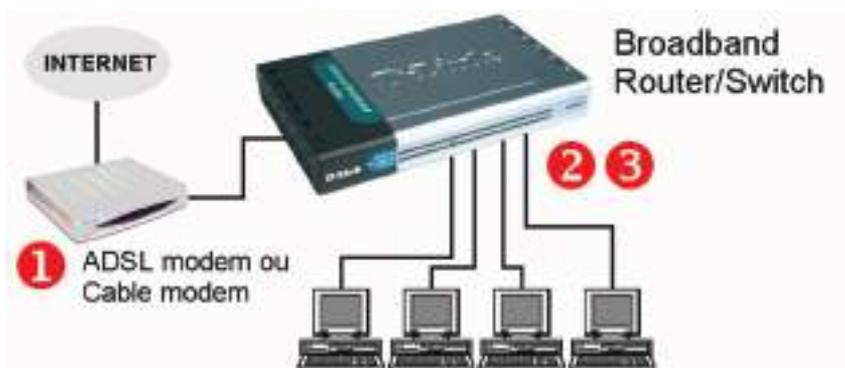


Figura 160: Broadband Router/Switch

Muitas vezes chamado apenas de broadband router, este aparelho é ligado num modem de banda larga (Cable ou ADSL) através de uma conexão Ethernet (RJ-45). Possui em geral quatro conexões Ethernet operando em modo switch, permitindo a conexão a quatro computadores. Como aceita conexões de internet vindas de modems a cabo ou ADSL, serve para os dois mais populares tipos de banda larga: ADSL ou a cabo.



**Exemplo 3 (ADSL Router):***Figura 161: ADSL Router*

O ADSL Router é ao mesmo tempo um modem ADSL e um router (funções 1 e 2). Sendo ligado a um switch ou hub, permite distribuir o acesso à Internet para os computadores da rede.

A maioria dos ADSL Routers possuem duas ligações para computadores, sendo uma Ethernet (a mais usada) e outra USB. Normalmente ambas podem operar ao mesmo tempo. Quando queremos ligar apenas dois computadores, não precisamos portanto utilizar um switch, basta usar ambas as conexões. Nesse caso o ADSL Router também opera como um switch de duas portas.

*Figura 162: ADSL Router*

NOTA: Para usar a conexão USB com o ADSL Router, normalmente é preciso instalar um “USB Network driver”, encontrado no CD-ROM que acompanha o produto. Este driver cria um adaptador de rede virtual que é direcionado para a porta USB.



## Exemplo 4 (Banda larga para dois computadores):



Figura 163: Banda larga para dois computadores

Conexões de banda larga, sejam a cabo ou ADSL, podem ser partilhadas pelo processo indicado em baixo. Um computador pode operar como router, desde que este recurso seja configurado. O Windows 98SE e superiores permitem tal configuração. Este computador deve ter duas placas de rede, uma para ligação no modem e outra para ligação na rede interna.

Esta configuração é ideal para quem já possui um modem de banda larga, em vez de um modem/router. Desta forma não é necessário comprar um modem/router, nem um switch para ligar os dois computadores. A desvantagem é que é necessário ligar o primeiro computador para que o segundo tenha acesso à Internet. É recomendável que o computador conectado à Internet seja ligado antes do outro.

## Exemplo 5 (Computador como Router):



Figura 164: Computador como Router



Quando configuramos o recurso ICS – Partilha de ligação com a Internet, este computador passa a operar na verdade como um router. Pode usar a Internet normalmente, e também distribuir esta conexão de Internet pela rede interna, através de um switch. Neste computador que é ligado à Internet devemos instalar um firewall para proteger a rede interna.

#### Exemplo 6 (Router wireless):

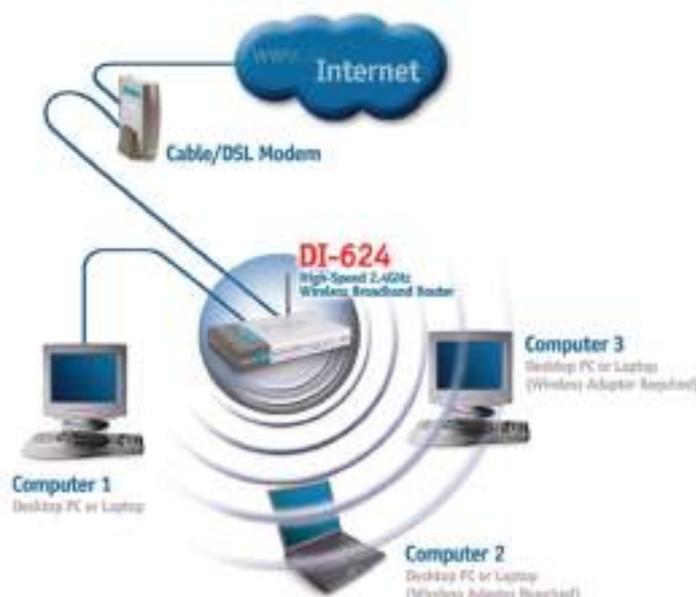


Figura 165: Router wireless

Este aparelho é ligado a um modem de banda larga (cabo ou ADSL) e distribui a conexão de banda larga através de uma rede sem fio (wireless). Os computadores que farão acesso sem fio precisam de ter um adaptador de rede wireless adequado. Normalmente esses routers possuem também uma conexão Ethernet que permite a ligação de um ou mais computadores, através de hub ou switch.

### Instalação de modem ADSL

Antes de aprender a partilhar uma ligação com a Internet, devemos saber configurá-la num computador só. Neste exemplo vamos ligar um modem ADSL a um computador. Posteriormente veremos como partilhar esta conexão.

Este tipo de ligação pode ser feita tanto em modems ADSL, como em ADSL Routers, operando em modo bridge. Quando um ADSL Router opera em modo bridge, é funcionalmente similar a um modem ADSL.



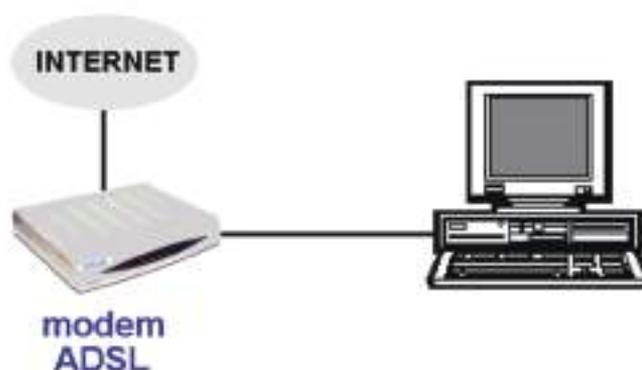


Figura 166: Exemplo de instalação de modem ADSL

## Descobrir o IP do modem

Inicialmente temos de fazer o SETUP do modem ADSL. Para fazê-lo precisamos de saber o seu IP. A maioria dos modems e routers de banda larga podem ser configurados através de um SETUP em HTML, similar a uma página de Internet. Para chegar ao seu SETUP basta digitar no nosso navegador, o IP do modem ou router.

Devemos então clicar no ícone da conexão para chegar ao seu STATUS. Clicamos em SUPORTE e em REPARAR (Windows XP/2000). No Windows 98 e compatíveis fazemos a mesma operação através do programa WINIPCFG (Renovar tudo).

Depois disso verificamos o IP do Gateway padrão, que é o modem ou router.



Figura 167: Status de conexão local

No nosso exemplo:

IP do modem: 10.0.0.2

IP do computador: 10.0.0.14

Os modems e routers ADSL operam também como DHCP, ou seja, distribuem endereços IP para os computadores da rede interna. Usamos o comando STATUS ou o WINIPCFG para descobrir o IP deste DHCP (ou Gateway padrão). No nosso exemplo o IP do modem é: **10.0.0.2**



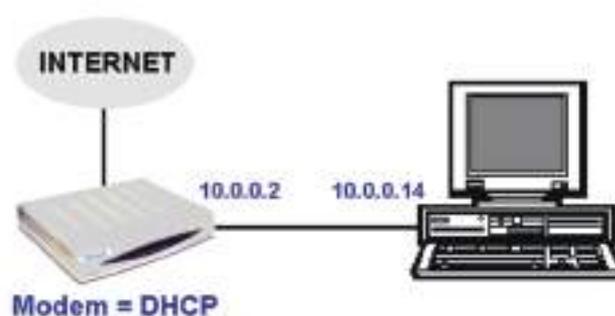


Figura 168: Exemplo de instalação de modem ADSL

## O Setup do modem

Para chegar ao Setup do modem usamos um navegador qualquer (ex: Internet Explorer) e digitamos o seu IP. No nosso exemplo digitamos:

**http://10.0.0.2**

O Setup será aberto como página web protegida por senha. Na maioria dos casos devemos usar nome=admin e senha=admin, mas existem exceções. Em caso de dúvida consultamos o manual do produto.



Figura 169: Entrada no setup do modem

O layout varia de um produto para outro, assim como o endereço IP utilizado. Ainda assim provavelmente conseguiremos fazer a configuração pelo processo descrito aqui, mesmo sem o manual.



O Setup de um modem é normalmente dividido em áreas separadas como STATUS (mostra as configurações atuais) e CONFIGURATION (onde podemos alterar as configurações). No exemplo da figura em baixo selecionamos STATUS / WAN. No caso, WAN (Wide Area Network) refere-se à conexão da Internet, e LAN refere-se à rede local.

Figura 170: Exemplo de entrada no setup de um modem.

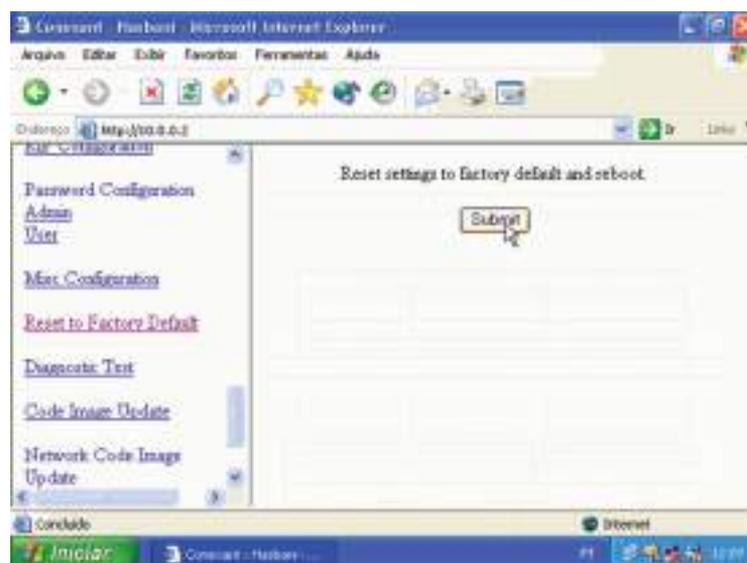


NOTA: No exemplo acima vemos que a conexão WAN ainda não possui um endereço IP. Isto significa que ainda não existe uma conexão estabelecida, apesar da linha telefónica estar fisicamente ligada ao modem.

## Restet para as configurações de fábrica

Devemos inicialmente fazer um reset para as configurações de fábrica, para anular eventuais configurações que tenham sido anteriormente realizadas no modem. Isto é útil por exemplo, quando transferimos o modem para outra linha, ou quando alteramos o seu modo de funcionamento.

Figura 171: Reset de um modem.



NOTA: Normalmente é possível fazer um reset introduzindo um palito num pequeno orifício na parte traseira do modem (devemos fazê-lo com o modem desligado).

## Configuração do modem

Depois de ser feito o reset para a configuração de fábrica, vamos ao item CONFIGURATION (ou similar) e preenchemos os seguintes parâmetros:

**VPI e VCI:** Preencher de acordo com o estado ou operadora telefónica. Por exemplo, para o sapo adsl usamos VPI=0 e VCI=35.

**Encapsulamento:** Use 1483 Bridged IP LLC.

**Modo Bridge:** Enabled.

**Nome do serviço:** Pode ser qualquer nome. Use por exemplo, TimorTelecom.

**Utilizador:** Usualmente é o número do telephone.

**Senha:** Idem. Diferentes operadoras podem usar outros esquemas.

Outros comandos podem variar de um modem para outro. O modem do nosso exemplo possui um comando AUTOMATIC RECONNECT. O seu uso é recomendável, faz com que o modem inicie a conexão automaticamente ao ser ligado, e que faça uma nova conexão caso a anterior seja descontinuada.

O Setup do modem é dividido em outras páginas, mas em geral as configurações que precisam de ser realmente feitas ficam reunidas numa página principal. No nosso exemplo, as configurações estão na página WAN. Alguns modems possuem uma página chamada ONE PAGE SETUP.



Figura 172: Configuração do modem.



No final da página onde foram feitas as configurações encontraremos um botão SUBMIT. Ao usarmos este botão, o modem passará a operar no modo programado, porém estas configurações serão perdidas quando o modem for desligado. Para que as configurações sejam permanentes devemos usar o comando SAVE TO FLASH ROM ou similar.



Figura 173: Guardar as configurações efetuadas.

No nosso exemplo encontramos o comando SAVE SETTINGS, que por sua vez apresenta um outro botão SUBMIT com a indicação “Write settings to flash and reboot”. O modem será reiniciado depois de as alterações serem gravadas na Flash ROM.

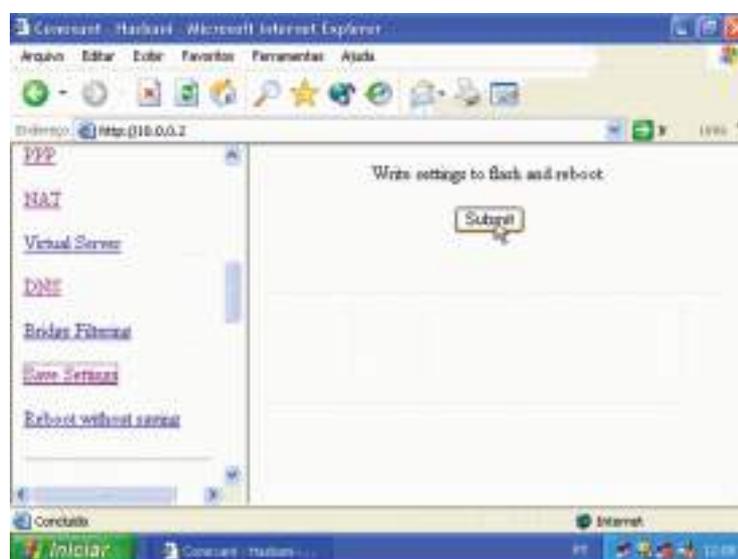


Figura 174: Guardar as configurações efetuadas na memória ROM.



## Verificação da ligação

Usando o comando Status / WAN podemos verificar que no campo WAN já existe um endereço IP e um endereço MAC ativos no modem. Isto mostra que o modem aceitou as configurações realizadas.

É importante usar também o comando STATUS / ADSL. Serão mostrados valores de decibéis (dB) para a relação sinal/ruído e para a atenuação na linha.

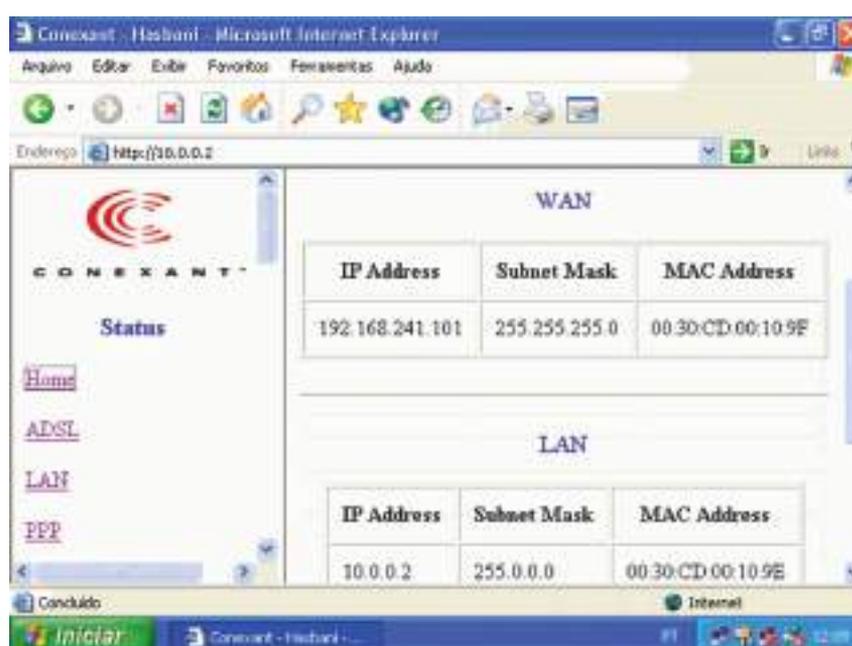


Figura 175: Verificação do estado da conexão.

## Firewall

A Firewall é um software que protege o computador e a rede, protegendo-os de acessos indevidos solicitados por um computador externo, através da Internet. Hackers podem descobrir conexões com computadores desprotegidos e iniciar uma invasão, onde podem roubar ou apagar dados, instalar vírus e outros programas maliciosos. Muitos modems e routers possuem uma firewall embutida, que é ativada através do seu Setup. Também é recomendável instalar um software firewall no computador que está fisicamente ligado à Internet. Existem várias firewalls no mercado, como o Norton Firewall, o McAfee Firewall e o Zone Alarm, entre outros.



## Partilha de ligação ADSL ou a cabo através de um computador Computador como Router

Neste método de partilha, um computador irá operar como router. Usaremos o ICS – Internet Connection Sharing, presente no Windows 98SE e superiores. O computador deverá ter duas placas de rede: uma na qual o modem está ligado e a outra que será ligada à rede. A ligação de banda larga poderá ser via cabo (o computador estaria ligado a um cable modem) ou ADSL (o computador estaria ligado a um ADSL modem, ou a um ADSL ROUTER operando em modo BRIDGE).



Figura 176: Exemplo de computador a operar como router.

## Computador com Internet a cabo

O computador que irá partilhar a ligação com a Internet já deve estar com esta ligação a funcionar. A conexão por Internet a cabo é permanente. Basta ligar o computador e ele estará ligado à Internet. Esta conexão é feita por uma placa de rede e pelo cable modem instalado pela operadora.

Antes de começar a configuração da partilha, verificamos se este computador está realmente ligado à Internet. Este computador deverá possuir uma segunda placa de rede com a qual será ligada à rede interna, através de um hub ou switch.



Figura 177: Cable modem.

## Computador com banda larga ADSL

Se o computador que irá operar como router estiver ligado à Internet por uma Ligação ADSL, devemos ativá-la. A conexão também precisa de ser autenticada (login no provedor).



Assim como ocorre com a conexão via cabo, este computador deve ter duas placas de rede, sendo uma para a conexão com a Internet e o outro para ligação com a rede interna, através de um switch ou hub.

Note que devemos utilizar neste caso um MODEM ADSL, ou então um ADSL ROUTER a operar em modo BRIDGE. Não podemos instalar um ADSL ROUTER a operar em modo ROUTER e usar um segundo router (o computador).



Figura 178: ADSL Router.

## Assistente de rede

No Windows 98SE, usamos o ICS – partilha de conexão com a Internet, naquele computador que irá funcionar como router. No Windows ME/XP, usamos o Assistente de rede, que entre outras coisas, faz também a partilha de conexão com a Internet.

Nos outros computadores devemos ir ao Painel de controlo e usar:

- Opções da Internet
- Conexões
- Conexão via LAN (rede local)

No caso do Windows ME e do XP, podemos configurar os outros computadores também pelo assistente, e apenas indicar “este computador acede à Internet através da rede”. Nesse caso não precisamos usar o método manual (Painel de controlo).

No caso do Windows ME/XP, usamos o Assistente de rede, localizado em:

Todos os programas/Acessórios/  
Comunicações/Assistente para  
configuração de rede.



Figura 179: Assistente para configuração de rede.



O Assistente de rede pedirá para que sejam feitas algumas verificações iniciais:

1. Placas de rede e modems devem estar corretamente configurados e em funcionamento normal.
2. Todos os modems, computadores e impressoras da rede devem ser ligados.
3. A conexão com a Internet deve estar ativa.

Não está indicado, mas também é preciso ligar todos os hub e switches, além dos cabos estarem conectados.

Figura 180: Verificações iniciais do assistente de rede.



O Assistente começa com uma pergunta sobre a ligação à Internet. Devemos configurar inicialmente o computador que irá operar como router. Para este computador, marcamos no quadro da figura 181 a opção

*“Este computador conecta-se diretamente à Internet e os outros computadores da rede conectam-se à Internet por meio deste computador”.*

A segunda opção deste quadro deverá ser usada quando executarmos o Assistente de rede nos outros computadores da rede.

Figura 181: Escolha das opções para o computador que funcionará como router.



O Assistente poderá perguntar qual das ligações de rede disponíveis será usada para a Internet. No nosso caso temos duas placas de rede (D-Link ligada na rede local e NVIDIA ligada no ADSL Modem). Existe uma terceira conexão de rede virtual, chamada “Velox”. Esta ligação foi criada quando instalamos o software da operadora. Devemos seleccionar esta conexão para o acesso à Internet.



Figura 182: Indicação da ligação à internet.

Eventualmente o Assistente poderá perguntar qual a placa de rede que é usada para ligação com a rede interna. No quadro da figura 183, seleccionamos a placa D-Link, ou a que tivermos instalada no nosso computador.



Figura 183: Indicação da conexão com a rede.



Este assistente não configura apenas a partilha de ligação com a Internet, mas também a rede local. Por isso é apresentado um quadro para identificação do computador:

- Nome do Computador.
- Descrição do computador

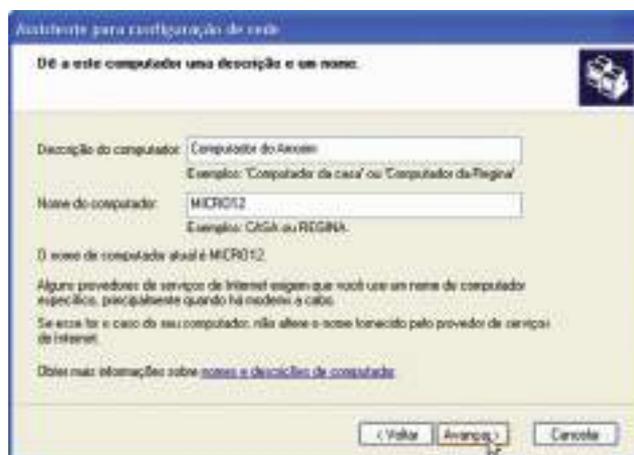


Figura 184: Identificação do computador.

Também será perguntado o nome do grupo de trabalho. Este assistente sugere o nome MSHOME, mas podemos utilizar outro nome se desejarmos.



Figura 185: Grupo de trabalho.

O Assistente de rede está pronto para aplicar as configurações. Se quisermos fazer alguma alteração podemos clicar em Voltar e alterar o que for preciso.

Note que a janela da figura 186 indica que a ligação à Internet é a “Conexão Velox”, que a partilha para esta conexão está ativa, assim como o Firewall para proteção desta conexão.





Figura 186: Aplicação das configurações.

## Configuração dos outros computadores

Outros computadores da rede que tenham o Windows XP ou o Windows ME podem ser configurados com seus próprios assistentes de rede. Computadores com Windows 98 podem ser configurados com o disco de configuração gerado quando executamos o Assistente de rede pela primeira vez, ou então executando o Assistente de rede diretamente a partir do CD-ROM de instalação do Windows XP.



Figura 187: Escolha das opções para o computador que se vai ligar à internet através de outro computador.

Ao executar o Assistente de rede nos outros computadores, indicamos como na figura 187 a opção:

*Este computador conecta-se à Internet por meio de outro computador na rede...*



Em vez de configurarmos os restantes computadores da rede utilizando o Assistente, podemos fazer as configurações de rede manualmente. Basicamente é preciso definir o nome do computador, grupo de trabalho, protocolos, etc. Os computadores que usam a Internet através da rede podem ser configurados manualmente através do comando Opções da Internet, no Painel de controlo. Clicamos então em Conexões e a seguir em Configurações de LAN.



Figura 188: Propriedades de Internet Win 98.

Será então apresentada a janela da figura 189, no qual marcamos a opção “Detectar automaticamente as configurações” e clicamos em OK.

Esta configuração foi mostrada para o Windows 98, mas em outras versões os comandos são semelhantes.

No Windows XP também configuramos os computadores manualmente para acesso à Internet via rede. Usamos o comando Opções da Internet no Painel de controlo e clicamos em Conexões, a seguir em “Configurações de LAN”.



Figura 189: Propriedades de internet Win XP.



Selecionamos então a opção “Detectar automaticamente as configurações” e clicamos em OK.

Este procedimento é padronizado para qualquer computador que aceda à Internet através da rede, não importa qual método de partilha utilizado.



Figura 190: Configurações LAN.

## Instalação de um ADSL Router: D-Link 502G, configuração automática

Encontraremos no mercado alguns modelos de ADSL Routers acompanhados de softwares de instalação criados por uma parceria entre o fabricante e as operadora telefónicas. É o caso do D-Link 502G, um roteador que vem acompanhado de um software de instalação. O uso desses softwares é mais simples que usar o SETUP do router. Exemplificaremos a instalação deste router com o seu software, mas na seção seguinte mostraremos a configuração manual.

É recomendável que antes de ligar a rede inteira no router, através de um hub ou switch, começarmos por ligar apenas um computador, diretamente ao router. Verificamos o tipo de cabo que deve ser usado nesta conexão. A maioria dos routers utiliza um cabo crossover para ligação com hub/switch, e um cabo normal para ligação com o computador. Verificamos se o LED “Ethernet” do router está aceso.

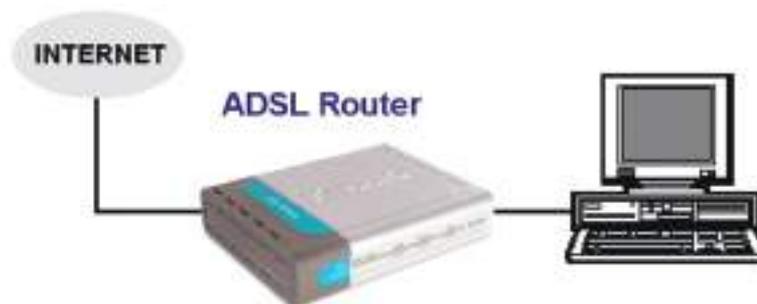


Figura 191: Ligação de um computador diretamente ao Router.



Depois de configurada a conexão podemos ligar o hub/switch e os restantes computadores da rede. A partilha de conexão é automática.

Mesmo com um software de instalação automática, é preciso realizar manualmente algumas etapas. É preciso por exemplo usar o comando Reparar conexão (Windows 2000/XP) ou Renovar conexão (Windows 9x/ME). Este cuidado pode ser dispensado se vivermos o cuidado de ligar o router antes e o computador depois. No nosso exemplo, o router usa o IP 10.1.1.1. Observe que o computador ligado ao Router usa o endereço 10.1.1.3.



Figura 192: Verificação do IP do ADSL router.

O software existente no CD que acompanha este produto é personalizado para configurar automaticamente este modem, sem que seja preciso usar o seu SETUP interno.

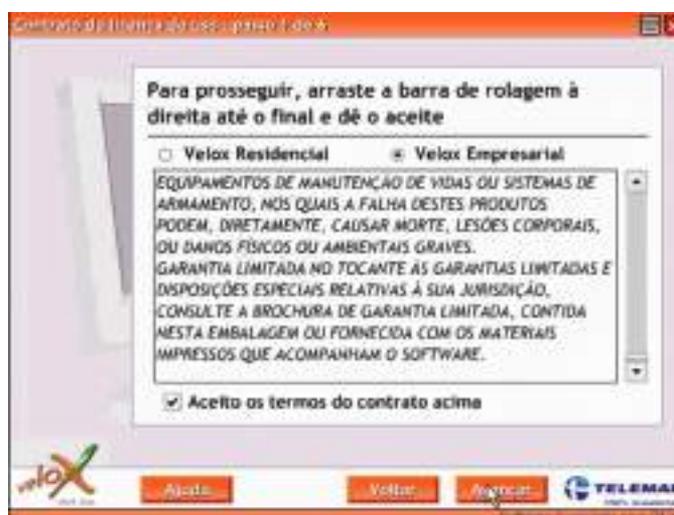


Figura 193: Janela de contrato da operador.



Este software é personalizado para dois modelos da D-Link: DSL-500G e DSL-502G. Devemos selecionar o modelo correto. No nosso exemplo usamos o DSL-502G.

Figura 194: Identificação do modem.



O programa de instalação perguntará a conexão a ser usada. No nosso exemplo foi oferecida apenas a opção Ethernet.



Figura 195: Identificação da ligação a ser utilizada.

O programa pedirá que informações como placa de rede, estado, modo e telephone sejam preenchidas. Para que o aparelho funcione como router, selecionamos a opção “Velox Empresarial Router”.

Figura 196: Formulário de instalação.



Devemos a seguir verificar se os LEDs do modem estão como indica a figura 197, o que confirma que a linha telefónica e o cabo Ethernet estão corretamente conectados.



Figura 197: Status do modem.

O software entrará no processo de programação do modem, operação que demora alguns minutos. Terminada a programação, o software fará uma análise da linha, apresentando os níveis de relação sinal/ruído e atenuação para download e upload. Marcas verdes indicarão que os níveis estão dentro dos padrões.

**IMPORTANTE:** Ativar a Firewall do ADSL Router. Isto deve ser feito através do seu SETUP.



Figura 198: Finalização da instalação.



## Configuração manual de um ADSL Router

Para fazer a configuração manual de um ADSL Router, permitindo a partilha da conexão com a Internet, devemos procurar e configurar os seguintes itens:

VPI e VCI: Preencher de acordo com o estado ou operadora telefónica. No nosso exemplo, usamos VPI=0 e VCI=33.

- Encapsulamento: Use PPPoE LLC.
- Modo Bridge: Disabled.
- Nome do serviço: Pode ser qualquer nome.
- Utilizador: Usualmente é o número do telefone.
- Senha: Idem. Diferentes operadoras podem usar outros esquemas.

Todo ADSL Router opera como DHCP para a rede interna. Para descobrir o seu IP usamos o programa WINIPCFG (Windows 98/ME) ou o Status da Conexão (Windows 2000/XP). Observe o endereço do Gateway ou do DHCP. Este é o IP do ADSL Router. No nosso exemplo este IP é:

### 10.0.0.2



Figura 199: Endereço IP do router.

Para chegar ao Setup do ADSL Router, executamos um navegador de internet e digitamos o nosso IP, precedido de "http://". No nosso exemplo executamos o Internet Explorer e digitamos:

http://10.0.0.2

Depois de alguns segundos será pedido um nome de utilizador e senha para permitir o acesso. Na maioria dos casos, usamos admin/admin. Consulte o manual do seu produto para confirmar.



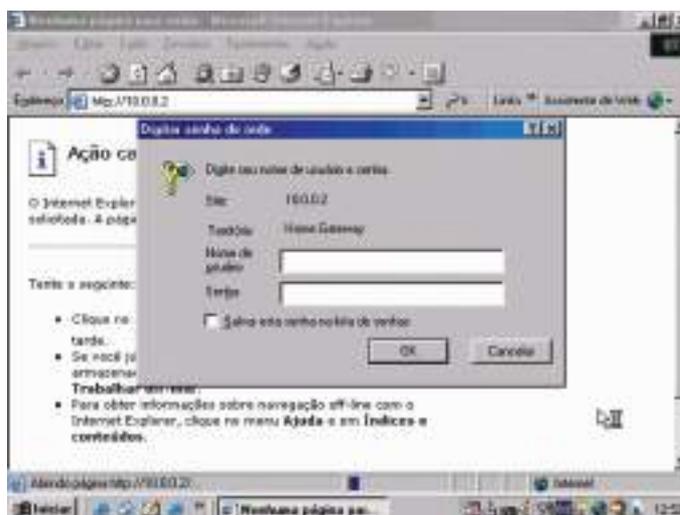


Figura 200: Janela de acesso as configurações do Router.

Procure o comando Reset to Factory Defaults ou similar, como mostrado anteriormente. Desta forma, alguma configuração indevida feita anteriormente será anulada. Vamos agora à seção Status / Configuration. Poderá ser constatado que na seção WAN não existe conexão indicada. Isto é normal porque o modem acaba de sofrer um reset e foi desconfigurado.

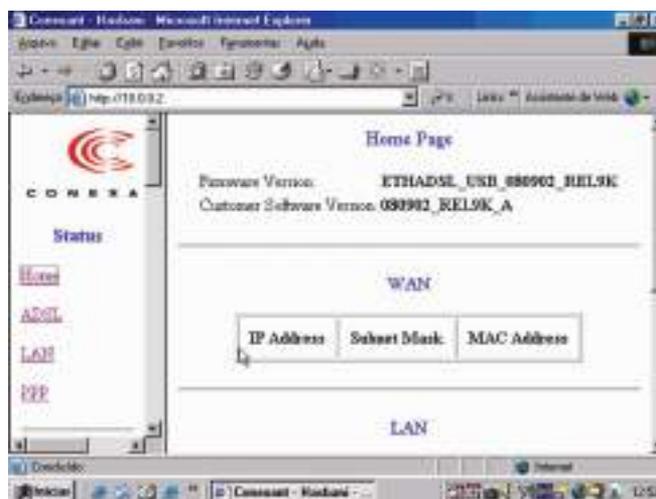
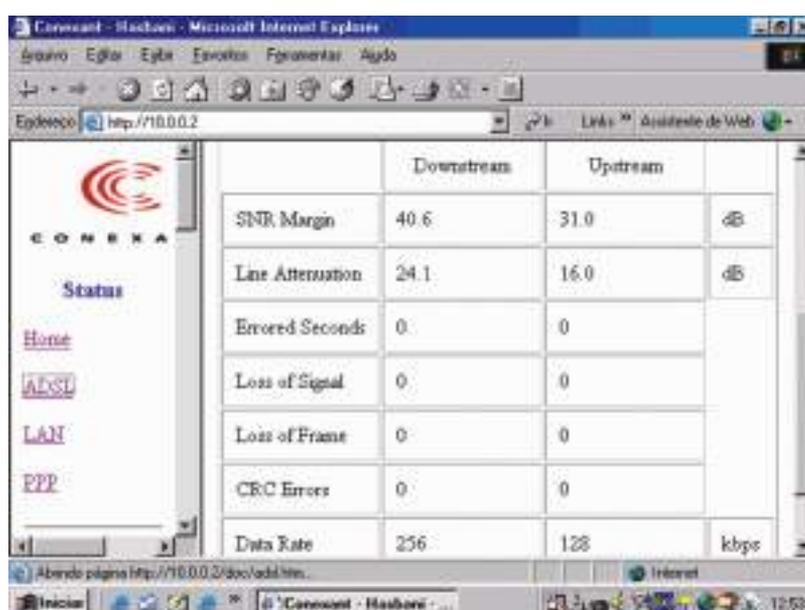


Figura 201: Status do router.

Na seção Status / ADSL encontraremos informações sobre a relação sinal/ruído (quanto maior, melhor) e atenuação da linha (quanto menor, melhor), medidas em decibéis. Normalmente são também informadas as taxas de recepção (downstream) e transmissão (upstream), que no nosso caso são de 256 kbps e 128 kbps.





	Downstream	Upstream	
SNR Margin	40.6	31.0	dB
Line Attenuation	24.1	16.0	dB
Errored Seconds	0	0	
Loss of Signal	0	0	
Loss of Frame	0	0	
CRC Errors	0	0	
Data Rate	256	128	kbps

Figura 202: Verificação das condições da linha.

O Status da conexão PPP (Point to Point Protocol) mostrará que não existe conexão estabelecida com a companhia telefónica.

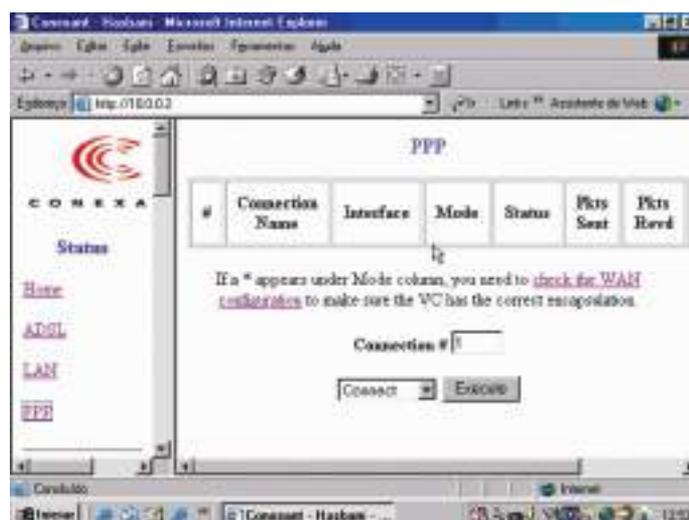


Figura 203: Status PPP.

Vamos à página de configuração do router. Na seção WAN usamos os parâmetros:

- VPI e VCI: 0 e 33 (Consulte tabela para outros estados)
- Encapsulation: PPPoE LLC
- Bridge: Disabled
- Nome e telefone
- Automatic Reconnection: Habilitar



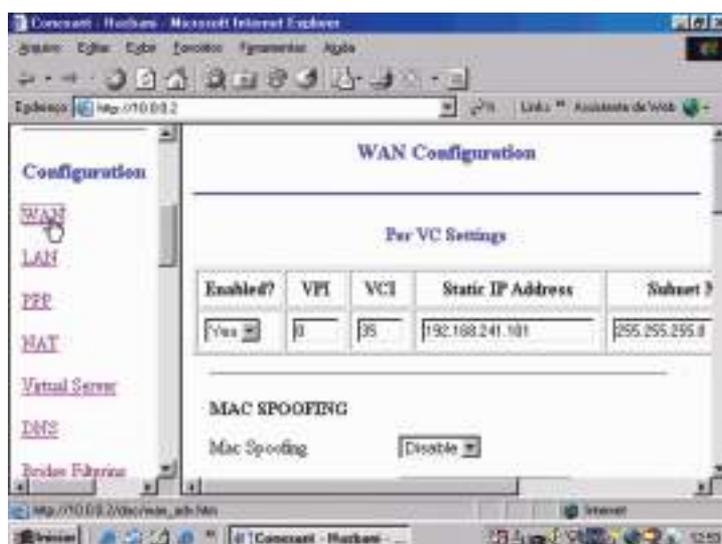


Figura 204: Janela de início ed configuração.

Clicamos agora em Submit na página de configurações para efetuar as mudanças na RAM do roteador.

Além deste comando é preciso usar um outro que salva as alterações de forma permanente na Flash ROM. O uso do comando Submit, caso exista, deve ser sempre feito antes daquele que guarda as alterações na Flash ROM. No exemplo da figura 205 estamos a fazer a gravação permanente na Flash ROM.

## Partilhas com ADSL Modem e Broadband Router

O chamado “Broadbando Router” (router de banda larga) são na verdade uma mistura de router e switch. São ligados a um modem (Cabo ou ADSL) e possuem normalmente quatro portas para ligação de computadores que irão formar uma rede e usar a conexão de Internet partilhada.



Figura 205: Exemplo de rede com Broadband router.



NOTA: É preciso que o modem tenha sido anteriormente configurado, ligado diretamente a um computador, e esteja em pleno funcionamento. Apenas depois de ter certeza de que o seu modem está ligado corretamente à Internet deveremos partir para a partilha. Neste caso vamos usar no nosso exemplo um broadband router modelo XRT 401D, fabricado pela Planet ([www.planet.com.tw](http://www.planet.com.tw)).



*Figura 206: Broadband Router XRT 401D*

Este router possui quatro portas LAN (Ethernet, RJ-45) para conexão com os computadores da rede local, e uma porta WAN (Ethernet, RJ-45) para ligação com o modem.



*Figura 207: Vista traseira do Router XRT 401D.*

Tecnicamente, nada impede que sejam feitas logo de início, as ligações definitivas, ou seja, a conexão de todos os computadores da rede. Entretanto é recomendável começar com uma configuração mais simples, pois em caso de problemas será mais fácil descobrir a causa.

Quando ligamos o modem e um computador no router, deverão estar acesos os LEDs WAN e da porta LAN correspondente.





Figura 208: Indicação do funcionamento através dos leds.

Se o nosso modem estava a funcionar anteriormente ligado a um computador através de um cabo normal (direto), a ligação entre o modem e o router deve ser feita por um cabo crossover.

Ligamos um só computador numa das portas LAN do router. Terminadas todas as configurações poderemos ligar os restantes computadores da rede. Se existirem mais de quatro computadores, poderá ser ligado mais um hub ou switch, em cascata com o router.

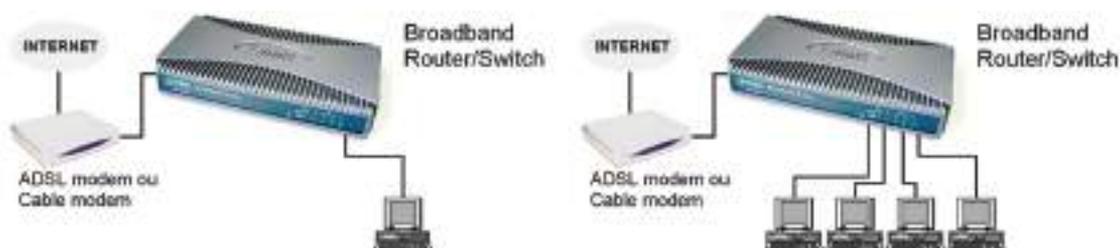


Figura 209: Exemplo de ligações com o router.

Como já foi dito anteriormente o router opera também como DHCP, portanto o nosso computador deverá ter recebido um IP. Esta atribuição de IP já deverá ter sido feita se tivermos ligado o router antes do computador. Se não fizemos isso podemos reiniciar o computador, ou então usar o comando REPARAR, no Status da ligação.

No nosso exemplo constatamos o seguinte:

- IP do computador: 192.168.0.100
- IP do router: 192.168.0.1





Figura 210: Detalhes da conexão de rede.

Para entrar no Setup do router, executamos mais uma vez um navegador de internet e escrevemos o IP do aparelho. No nosso exemplo digitamos:

http://192.168.0.1

O computador será conectado ao router, e será apresentado um quadro para preencher nome e senha. No caso deste produto, usamos, admin / 1234.



Figura 211: Janela de acesso ao Router.

NOTA: É aconselhável alterar o username e password do router antes de ligar os outros computadores da rede, evitando assim surpresas desagradáveis, pois as pass e usenames padrão qualquer um pode tentar adivinhar .



Os Setups de routers são mais simples que os de modems. A conexão através do modem já está configurada, então falta apenas indicar ao router o tipo de modem que utilizamos.



Figura 212: Página de setup do nosso router.

Como já vimos é sempre recomendável carregar as configurações de fábrica antes de configurar um modem ou router. No caso deste produto, existe um comando RESET que deve ser usado.

Normalmente é possível carregar as configurações de fábrica pressionando o botão RESET, encontrado num pequeno orifício na parte traseira do aparelho.



Figura 213: Reset do router.



Usamos agora o comando Quick Setup Wizard da figura 212, que fará algumas perguntas e colocará logo o router a funcionar.

O Setup perguntará o tipo de modem ao qual o router será ligado. São suportados diversos tipos, entre eles o ADSL e a conexão a cabo.



Figura 214: Escolha do tipo de modem.

Para a banda larga ADSL, indicamos o tipo de conexão como:

#### PPPoE xDSL



Figura 215: Tipo de ligação ADSL.



É preciso a seguir indicar o username e password para a conexão PPPoE. Neste caso é usado, o número do telefone, precedido pelo código de área. Indicamos também o nome do serviço, dados fornecidos pela operadora telefónica.

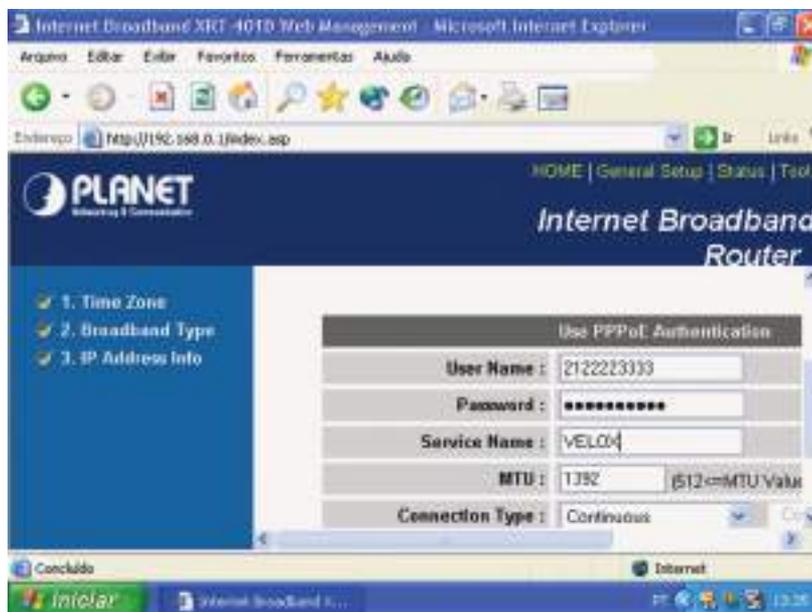


Figura 216: Introdução dos dados da operadora.

Existem diferentes implementações de banda larga. Uma das características que pode variar diz respeito à forma de conexão e desconexão. Neste exemplo, configuramos a conexão como contínua. Assim que o modem e o router forem ligados, a conexão ficará estabelecida. Já a autenticação é feita quando o primeiro computador da rede se liga à Internet.

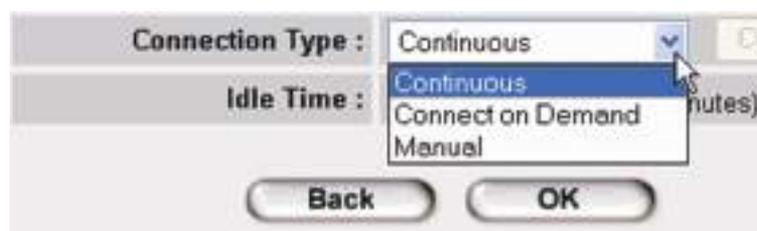


Figura 217: Tipo de ligação.

NOTA: Ligue os equipamentos na seguinte ordem:

1. Ligamos o modem e esperamos o LED indicado como LINK ficar aceso, sem piscar.
2. Ligamos o Router e esperamos alguns segundos



3. Ligamos hubs ou switches, caso existam
4. Ligamos os computadores

Respondidas todas as perguntas, o Setup guarda as configurações no router. Podemos agora sair do Setup, mas antes de usar a Internet é recomendável reiniciar o computador ou usar o comando Reparar ou Renovar (Status da conexão / WINIPCFG).



Figura 218: Janela de configurações guardadas com sucesso.

Antes de sair do Setup podemos ainda verificar o Status da ligação à Internet, o que comprovará o correto funcionamento do conjunto modem / router. Observe que o modem recebeu um IP externo, atribuído pelo fornecedor do serviço:

200.216.17.148



Figura 219: Status da ligação.



Ligamos agora os outros computadores da rede no router. Devem ser configurados com nome e grupo de trabalho adequados (no nosso exemplo, GRUPO). Os computadores aparecerão na rede e já poderão usar a Internet.



Figura 220: Computadores ligados à rede.

Este roteador possui quatro portas LAN, mas se precisarmos de ligar um número maior de computadores, podemos fazer a ligação de um hub ou switch em cascata. Não esquecer de verificar o tipo correto de cabo (direto ou crossover) para fazer esta conexão, como já abordamos no anteriormente.

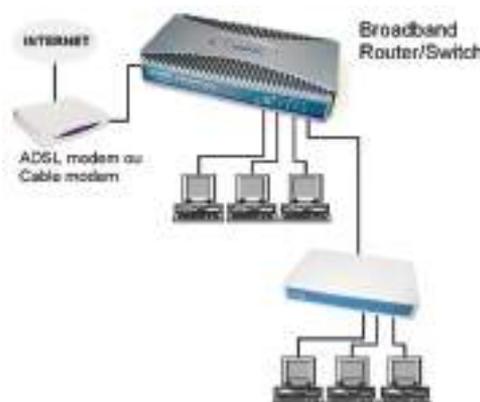


Figura 221: Alargamento da rede através de um hub/switch.

No nosso exemplo, ligamos três computadores diretamente no router e usamos a quarta porta para ligar um switch. Neste switch, ligamos mais três computadores. Esta rede ficou portanto com 6 computadores, como mostra a figura 222.

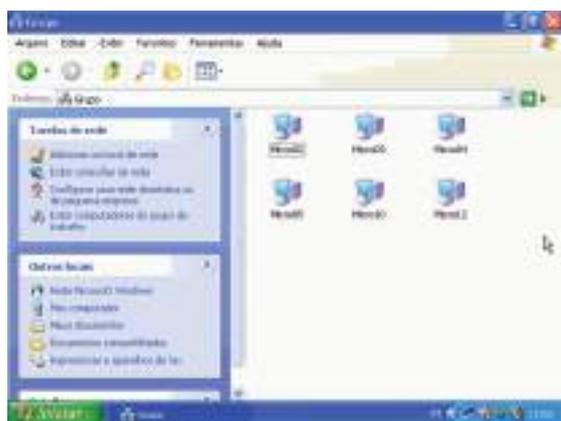


Figura 222: Total de computadores da rede.



## Redes sem fio

As Redes sem fio ou wireless (WLANs) surgiram da mesma forma que muitas outras tecnologias, no meio militar. Havia a necessidade de implementação de um método simples e seguro para troca de informações em ambiente de combate. O tempo passou e a tecnologia evoluiu, deixando de ser restrita ao meio militar e tornou-se acessível a empresas, faculdades e ao utilizador doméstico. Nos dias de hoje podemos pensar em redes wireless como uma alternativa bastante interessante em relação as redes por cabo, embora ainda com custo elevado. As suas aplicações são muitas e variadas e o fato de ter a mobilidade como principal característica, tem facilitado a sua aceitação, principalmente nas empresas.

A evolução dos padrões oferecendo taxas de transmissão comparáveis a Fast Ethernet por exemplo, torna as redes wireless uma realidade cada vez mais presente. WLANs usam ondas de radio para transmissão de dados. Comumente podem transmitir na faixa de frequência 2.4 Ghz ou 5 Ghz.

### Padrões

Como as WLANs usam o mesmo método de transmissão das ondas de radio AM/FM, as leis que as regem são as mesmas destas. O FCC (Federal Communications Commission), regula o uso dos dispositivos WLAN. O IEEE (Institute of Electrical and Electronic Engineers) é responsável pela criação e adoção dos padrões operacionais. Citamos os mais conhecidos:

IEEE 802.11	<ul style="list-style-type: none"> <li>○ Criado em 1994, foi o padrão original.</li> <li>○ Oferecia taxas de transmissão de 2 Mbps.</li> <li>○ Caiu em desuso com o surgimento de novos padrões.</li> </ul>
IEEE 802.11b	<ul style="list-style-type: none"> <li>○ Taxas de transmissão de 11Mbps.</li> <li>○ Largamente utilizada hoje em dia.</li> <li>○ Opera em 2.4Ghz</li> <li>○ Alcance de até 100m indoor e 300m outdoor</li> <li>○ Mais voltado para aplicações indoor</li> <li>○ Tende a cair em desuso com a popularização do 802.11g</li> </ul>



IEEE 802.11a	<ul style="list-style-type: none"> <li>○ Taxas de transmissão de 54Mbps.</li> <li>○ Alcance menor do que a 802.11b.</li> <li>○ Opera em 5Ghz</li> <li>○ Alcance de até 60m indoor e 100m outdoor</li> <li>○ Mais voltado para aplicações indoor</li> <li>○ Seu maior problema é a não compatibilidade com dispositivos do padrão b , o que prejudicou e muito sua aceitação no mercado.</li> </ul>
IEEE 802.11g	<ul style="list-style-type: none"> <li>○ Taxas de transmissão de 54Mbps podendo chegar em alguns casos a 108Mbps.</li> <li>○ Opera em 2.4Ghz</li> <li>○ Mais voltado para aplicações indoor.</li> <li>○ Reúne o melhor dos mundos a e b. (alcance x taxa)</li> </ul>
IEEE 802.16a	<ul style="list-style-type: none"> <li>○ Criado em 2003.</li> <li>○ Popularmente conhecido como Wi-Max</li> <li>○ Voltado exclusivamente para aplicações outdoor</li> <li>○ Alcance de até 50Km</li> <li>○ Taxas de transmissão de até 280Mbps</li> </ul>

## Técnicas de Transmissão

WLANs usam uma técnica de transmissão conhecida como difusão de espectro (Spread Spectrum). Essa técnica caracteriza-se pela grande largura de banda e baixa potência de sinal. São sinais difíceis de detetar e mesmo intercetar sem o equipamento adequado. Existem dois tipos de tecnologias de Spread Spectrum regulamentadas pelo FCC: Direct Sequence Spread Spectrum (DSSS) e Frequency Hopping Spread Spectrum (FHSS).

DSSS	<ul style="list-style-type: none"> <li>○ Menos resistente a interferência</li> <li>○ Compatibilidade com equipamentos de padrões anteriores</li> <li>○ Taxa de Transmissão de 11 Mbps</li> <li>○ Menor segurança</li> <li>○ Possui 11 canais, mas destes somente 3 são não-interferentes e os efetivamente usados para transmissão – Canais: 1, 6 e 11</li> </ul>
------	---



FHSS	<ul style="list-style-type: none"> <li>○ Mais resistente a interferência</li> <li>○ Não possui compatibilidade com equipamentos de padrões anteriores</li> <li>○ Taxa de transmissão de 2Mbps</li> <li>○ Maior segurança</li> <li>○ 79 Canais disponíveis para transmissão</li> </ul>
------	---

NOTA: No mundo das WLANs, o DSSS é a tecnologia utilizada.

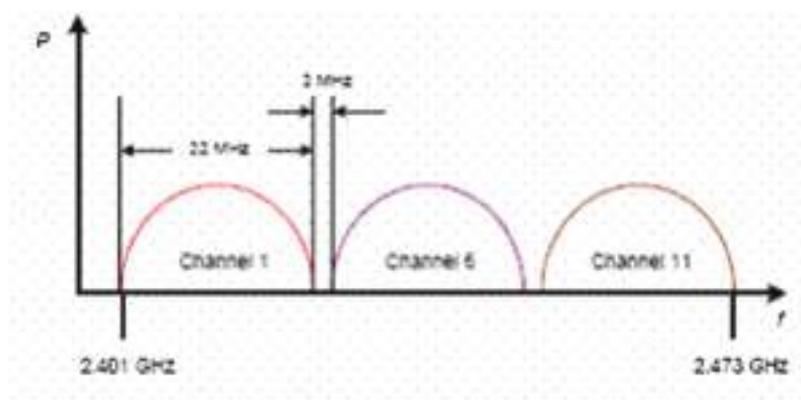


Figura 223: Canais não interferentes no DSSS

## Elementos de Hardware

Na tabela a seguir descrevemos os componentes de uma WLAN

 PC Card	<ul style="list-style-type: none"> <li>○ Usado somente em notebooks</li> <li>○ Serve para conectar o notebook a rede wireless</li> <li>○ Possui antena interna imbutida</li> </ul>
 Placas PCI	<ul style="list-style-type: none"> <li>○ Usado somente em desktops</li> <li>○ Serve para conectar o desktop a rede wireless</li> <li>○ Possui antena externa acoplada a saída da placa</li> </ul>
 Adaptadores USB	<ul style="list-style-type: none"> <li>○ Pode ser usado em notebooks ou desktops</li> <li>○ Serve para conectar o notebook ou desktop a rede wireless</li> <li>○ Possui antena interna embutida</li> </ul>



 <p>Pontos de Acesso</p>	<ul style="list-style-type: none"> <li>○ Concentra todo o tráfego da rede wireless além das conexões oriundas dos clientes.</li> <li>○ Possui um identificador que identifica a rede chamado SSID.</li> <li>○ Interface entre a rede wireless e a rede por cabo por possuir porta UTP 10 ou 100Mbps</li> <li>○ Possui antena interna embutida</li> <li>○ Suporta a conexão de antenas externas, na maioria dos casos</li> </ul>
 <p>Pontes Wireless Workgroup</p>	<ul style="list-style-type: none"> <li>○ Agrupa vários clientes LAN e transforma essa LAN em único cliente WLAN.</li> <li>○ Recomendado em situações em que um pequeno grupo de utilizadores precisa de acesso a rede principal.</li> <li>○ O número máximo de estações que pode ser conectado está compreendido entre 8 e 128, dependendo do fabricante.</li> </ul>
 <p>Pontes Wireless</p>	<ul style="list-style-type: none"> <li>○ Conecta duas ou mais redes</li> <li>○ Compreende 4 modos de operação: Root, Non-Root, Access Point e Repeater.</li> <li>○ Possui a capacidade de formação de backbone wireless através de 2 PC Cards.</li> </ul>
 <p>Gateways</p>	<ul style="list-style-type: none"> <li>○ Conecta um pequeno número de dispositivos wireless a internet ou outra rede</li> <li>○ Possui uma porta WAN e várias portas LAN. Geralmente tem um hub ou switch embutido e possui as funcionalidades de um Ponto de Acesso.</li> </ul>
 <p>Antenas</p>	<ul style="list-style-type: none"> <li>○ Podem ser conectadas a pontos de acesso ou a máquinas clientes para aumentar o ganho do sinal e assim melhorar a transmissão de dados.</li> <li>○ Podem ser direcionais ou omnidirecionais.</li> </ul>



## Tipos de WLAN

Uma WLAN pode ser utilizada tanto na forma Indoor quanto na forma Outdoor.

### Indoor

Dizemos que uma WLAN é indoor quando o sinal está a ser transmitido em ambiente fechado normalmente na presença de muitos obstáculos, um escritório é um bom exemplo.

Não há necessidade de vista direta entre as antenas para que haja comunicação. Alcance pequeno em torno de até 300 metros. Podem ter a presença de um Ponto de Acesso ou não.

### Rede AD-HOC

Dizemos que uma rede sem fio é “AD-HOC” quando não possui cabos de rede. Todos os computadores devem utilizar apenas placas de rede wireless. Cada computador é capaz de transmitir e receber informações para todos os demais que formam a rede.

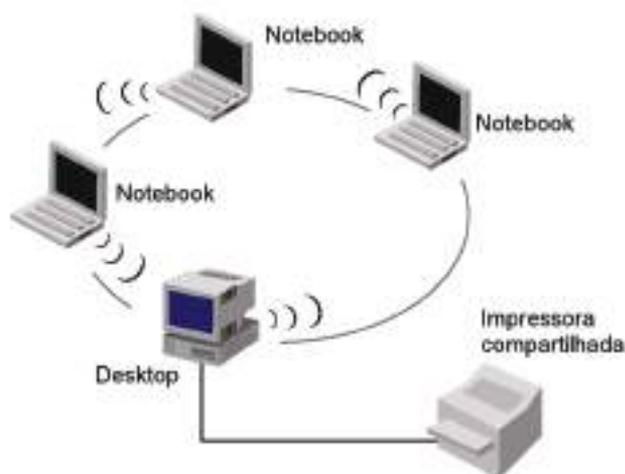


Figura 224: Exemplo de rede AF-HOC.

### Rede de infraestrutura

Este tipo de rede sem fio é integrada a uma rede por cabo através de aparelhos chamados “Access Points” (pontos de acesso).



Cada access point possui um conector RJ-45 para ligação com a rede por cabo, e cria ao seu redor, uma região que dá acesso sem fio a computadores equipados com placas apropriadas.

Podemos instalar vários access points para aumentara a área de cobertura da rede sem fio.

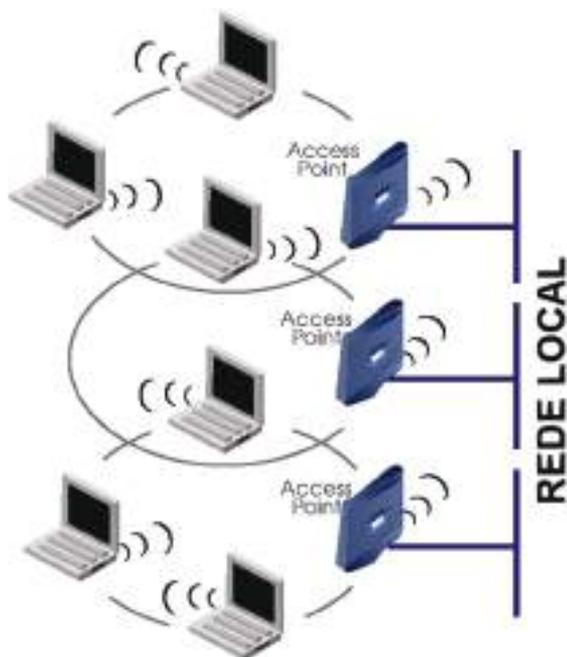


Figura 225: Exemplo de rede de infraestrutura.

A seguir são apresentadas as características mais comuns das redes Ad-HOC e das Redes de Infraestrutura.

AD-HOC	<ul style="list-style-type: none"> <li>○ Não existem Pontos de Acesso (AP)</li> <li>○ Comunicação feita cliente – cliente</li> <li>○ Não existe canalização do tráfego</li> <li>○ Performance diminui a medida que novos clientes são acrescentados</li> <li>○ Suporta no máximo 5 clientes para uma performance aceitável com tráfego leve</li> </ul>
Infraestrutura	<ul style="list-style-type: none"> <li>○ Necessidade de um Ponto de Acesso (AP)</li> <li>○ Comunicação cliente – cliente não é permitida. Toda a comunicação é feita com o AP.</li> <li>○ Centralização do tráfego. Todo o tráfego da Rede passa pelo AP.</li> <li>○ Compreende dois modos de operação: BSS (Basic Service Set), ESS (Extended Service Set)</li> </ul>



BSS – Consiste de um Ponto de Acesso ligado a rede por cabo e um ou mais clientes wireless. Quando um cliente quer comunicar com outro ou com algum dispositivo na rede por cabo deve usar o Ponto de Acesso para isso. O BSS compreende uma simples célula ou área de RF e tem somente um identificador (SSID). Para que um cliente possa fazer parte da célula ele deve estar configurado para usar o SSID do Ponto de Acesso.

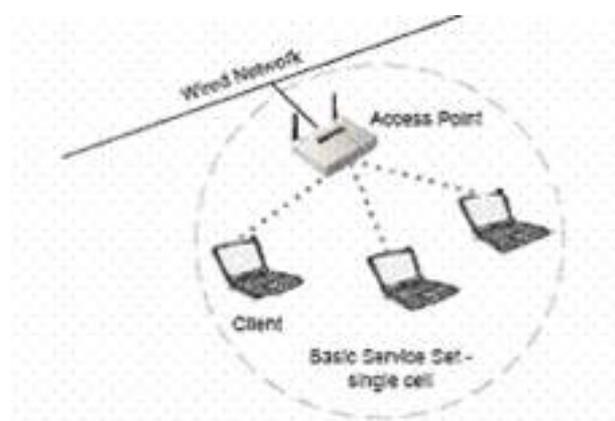


Figura 226: Sistema BSS

ESS – São 2 sistemas BSS conectados por um sistema de distribuição, seja ele LAN, WAN, Wireless ou qualquer outro. Necessita portanto de 2 Pontos de Acesso. Permite roaming entre as células. Não necessita do mesmo SSID em ambos os BSS.

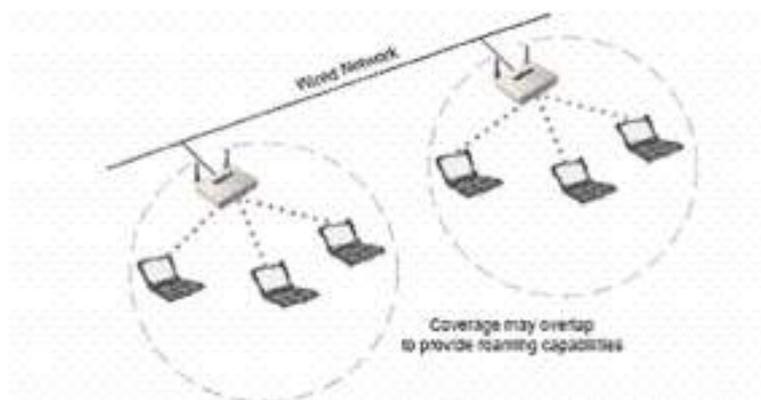


Figura 227: Sistema ESS

### Outdoor

Dizemos que uma WLAN é outdoor quando o sinal está a ser transmitido ao ar livre, uma comunicação entre dois prédios é um bom exemplo. As antenas ficam nos topos dos prédios e para que haja comunicação é necessário haver vista direta entre elas. Possui longo alcance podendo chegar a vários quilômetros.



## Instalação de uma rede wi-fi AD-HOC

Começamos com a instalação de uma placa de rede PCI wireless em cada computador da rede para o caso de ainda não a ter instalada. Os comandos de configuração para essas placas são similares, tanto em desktops quanto em notebooks. Usaremos como exemplo o Windows XP, que possui suporte a redes sem fio. Se usarmos uma versão mais antiga do Windows, é preciso instalar ainda o software de controle fornecido no CD-ROM que acompanha a placa.

Ao ser iniciado, o Windows XP detectará a placa e abrirá o assistente para adicionar novo hardware. O método exato dependerá do software de instalação de drivers fornecido pelo fabricante. Nos modelos que testamos, basta inserir o CD-ROM neste momento e a instalação prosseguirá automaticamente.

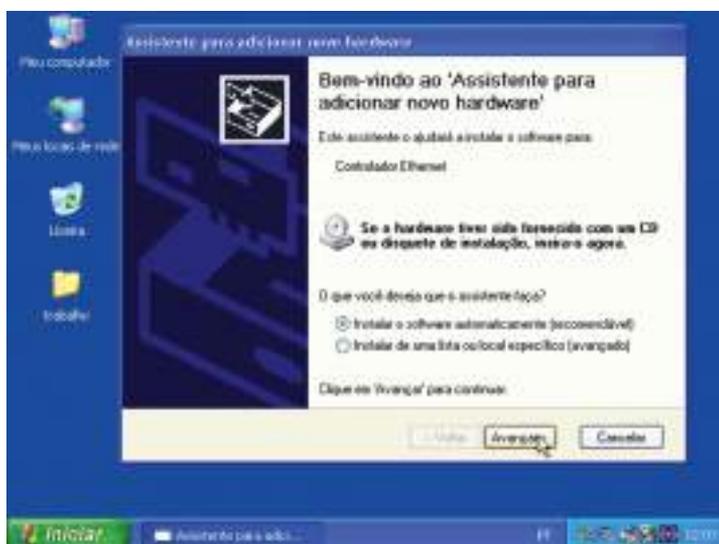


Figura 228: Assistente para adicionar hardware.

Os drivers serão localizados e instalados.



Figura 229: Instalação dos drivers em progresso.



Confirmamos a mensagem apresentada pelo assistente ao final da sua operação. No caso, temos:

O Assistente terminou de instalar o software para:

*IEEE 802.11b Wireless Cardbus/PCI Adapter*

Note que os mesmos drivers são utilizados tanto para a versão PCI quanto para a versão de cartão, usada em notebooks.



Figura 230: Finalização da instalação da placa.

Confirmamos agora no Gestor de dispositivos se a placa está realmente com os seus drivers instalados. Clicando em Adaptadores de rede, vemos a indicação da placa instalada:

IEEE 802.11b Wireless Cardbus/PCI Adapter

Damos agora um duplo clique no adaptador de rede wireless para alterar as suas propriedades.

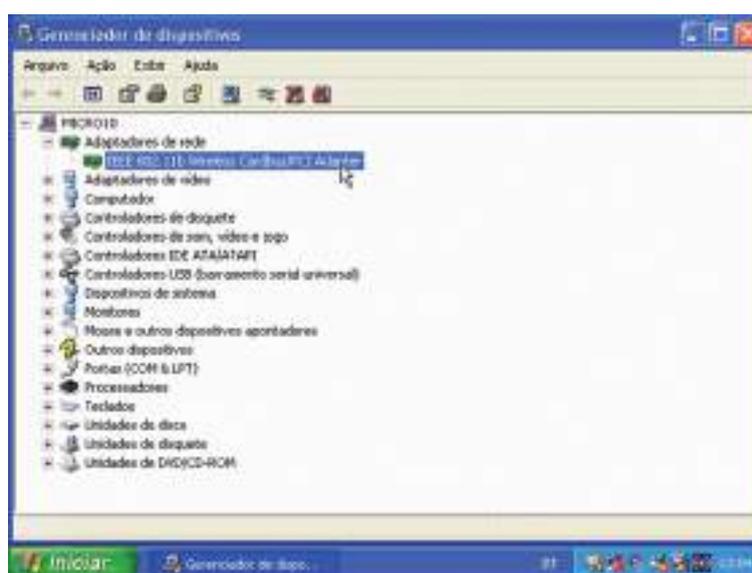


Figura 231: Gestor de dispositivos.



Na guia Avançado devemos programar:

Canal: As placas IEEE 802.11b usam canais de 1 a 11. Todas as placas da rede devem utilizar o mesmo canal.

Tipo: Ad-Hoc, no nosso caso

SSID: Nome da rede, deixamos na configuração de fábrica.



Figura 232: Propriedades de IEEE 802.11b.

A placa de rede aparecerá na janela de conexões de rede. No momento está indicada com um “X” vermelho, indicando que ainda não recebe sinal.

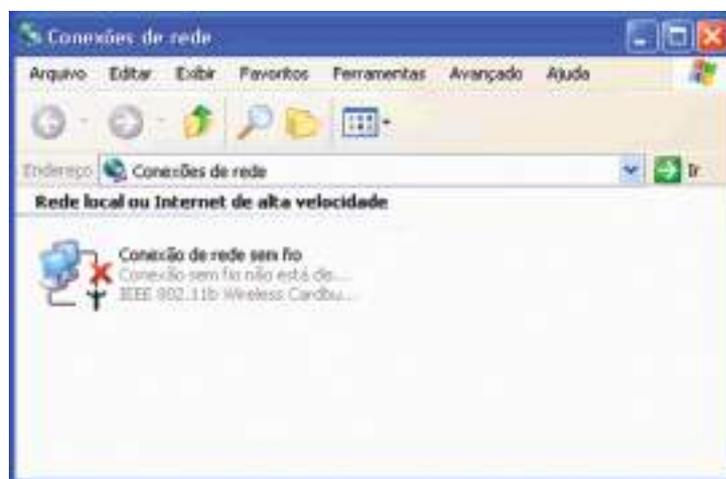


Figura 233: Janela das ligações de rede.

Clicando no ícone da ligação no canto inferior direito do ecrã temos o comando:

*Exibir redes sem fio disponíveis.*





Figura 234: Opção para mostrar redes sem fios.

De momento não existem redes sem fio disponíveis. Clicamos em Avançado para configurar a rede.



Figura 235: Menu de criação de redes sem fios.

Será apresentada a janela da figura 236, também sem redes disponíveis. Deixamos marcada a opção:

*Usar o Windows para definir as configurações da rede sem fio.*

Criamos a rede clicando em Adicionar, como mostra a figura.



Figura 236: Criar rede sem fio.



Será aberta uma janela para preenchimento das propriedades da rede. Devemos dar um nome para a rede (SSID). Neste exemplo ainda não usaremos as opções de proteção por criptografia (WEP). Marcamos a opção de rede computador a computador (AD-HOC).

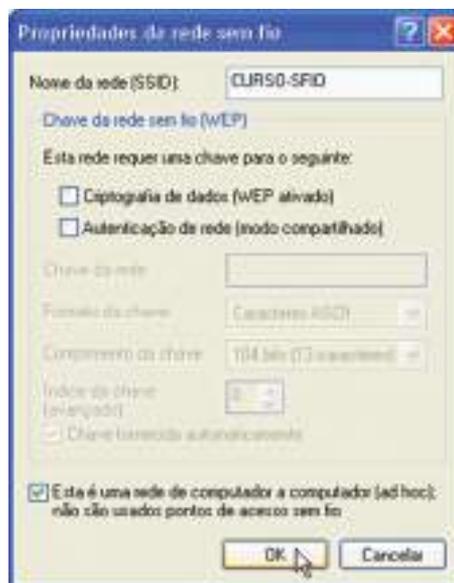


Figura 237: Propriedades da rede sem fio.

A rede estará criada, sendo gerada pelo seu primeiro computador. Os outros computadores irão “ver” esta rede e ligar-se na mesma. Fechamos todas as janelas e aguardamos até que o ícone da conexão de rede seja mostrado como na figura 238.

Não esquecer de ativar, nas propriedades da conexão, a opção “Mostrar ícone quando conectado”.

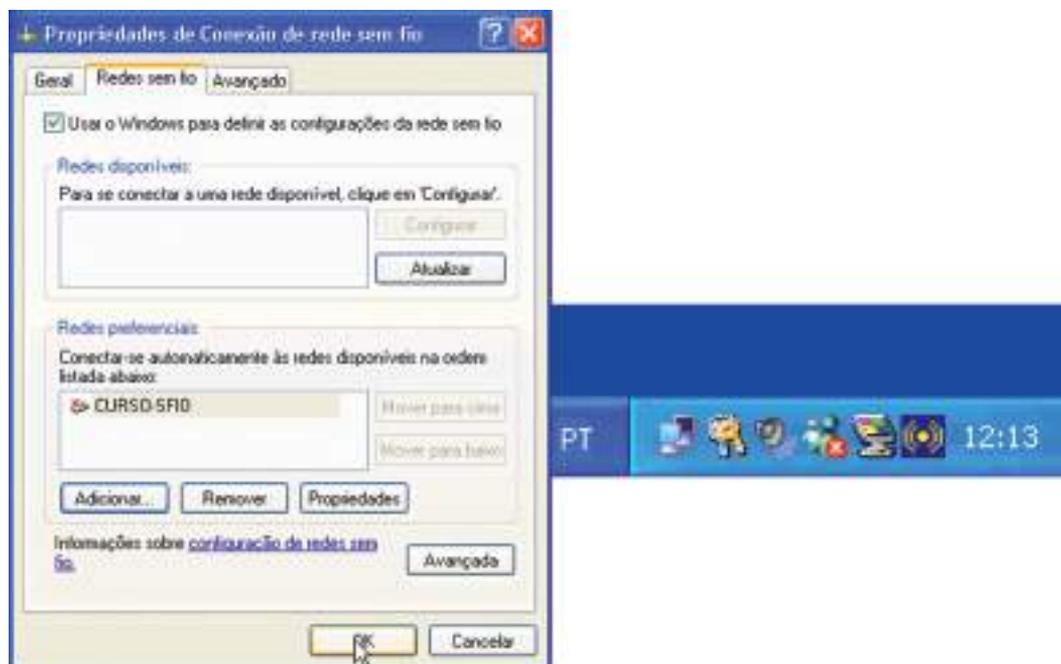


Figura 238: Rede sem fio criada e pronta a ligar.



Os outros computadores detectarão a presença de sinal de rádio e estarão aptos a entrar nesta rede. Usando o comando:

*Exibir redes sem fio disponíveis.*

Temos uma janela que mostra a rede recém-criada. Clicamos nesta rede e a seguir em Conectar.



Figura 239: Redes sem fio disponíveis.

Usamos também o comando Status da conexão de rede para fazer alguns testes importantes.

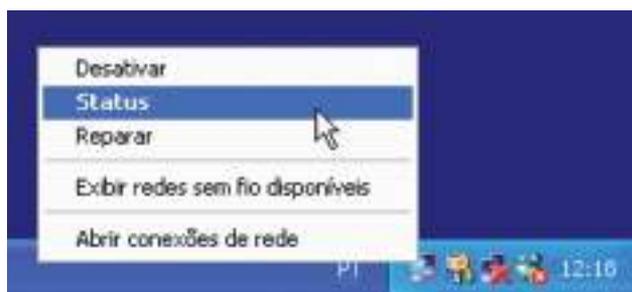


Figura 240: Verificação do status da nossa rede.



Verificamos o IP da ligação de rede. Como esta rede não possui DHCP, o IP será da forma: 169.254.xx.yy

Figura 241: Status da ligação de rede sem fios.



Clicamos agora na aba Geral para verificar a intensidade do sinal e a velocidade de comunicação. As placas reduzem automaticamente a velocidade quando o sinal é fraco.



Figura 242: Verificação da intensidade do sinal.

Abrimos agora a janela de conexões de rede sem fio, selecionamos a conexão desejada e clicamos em Conectar.

NOTA: O Windows XP pode ser configurado para entrar automaticamente na rede ao ser detectada, sem precisarmos usar este comando. Como ainda estamos a testar a rede, clicamos em Conectar para ter a certeza de que a rede irá funcionar.



Figura 243: Ligação à rede sem fios.



Uma vez feita a conexão, o uso da rede sem fio é idêntico ao de uma rede por cabo. É possível partilhar documentos e impressoras, aceder à Internet e usar todos os recursos da rede.

Clicamos em Meus locais de rede e no grupo de trabalho. No nosso exemplo são mostrados os dois computadores existentes na rede sem fio.

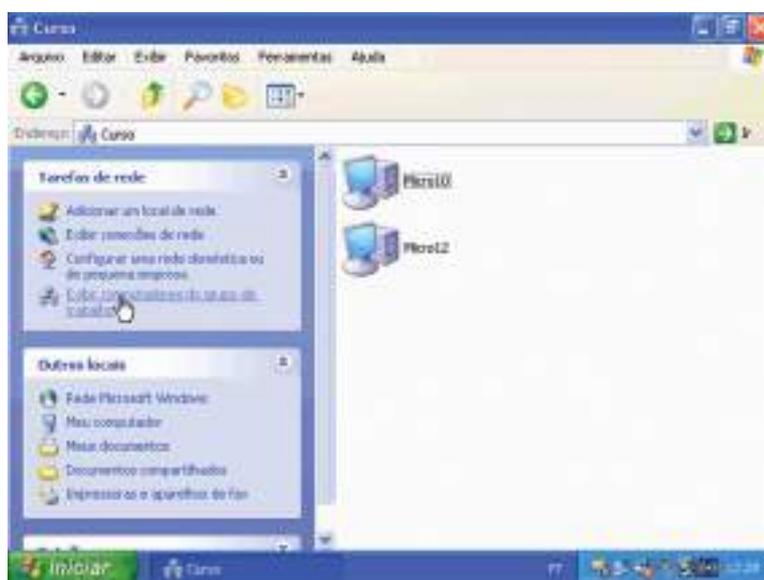


Figura 244: Grupo de trabalho da rede recém criada.

## Instalação de uma rede wi-fi AD-HOC com WEP

Uma rede sem fio desprotegida pode ser facilmente acedida por pessoas não autorizadas. Como o alcance é grande, vizinhos que possuam computadores com placas de rede wireless poderão descobrir a rede e entrar na mesma. Se na nossa rede existirem pastas partilhadas sem senha, esses vizinhos poderão ter acesso aos nossos documentos. Se a nossa rede tiver acesso à Internet, então o nosso vizinho poderá navegar gratuitamente. As placas de rede sem fio utilizam o recurso WEP, que é um conjunto de protocolos de segurança que impedirão o acesso de computadores não autorizados. Será preciso fornecer uma senha para entrar na rede.

Nas propriedades da conexão da rede sem fio (janela de conexões de rede), selecionamos a guia Redes sem fio.

Clicamos em Adicionar, para criar uma rede sem fio com proteção.





Figura 245: Propriedades de rede sem fios.

Marcamos a opção “Criptografia de dados – WEP Ativado”

A opção “Autenticação de rede” deve ficar marcada em todos os computadores, ou desmarcada em todos os computadores. Ela define um dos dois possíveis métodos para uso de chaves de criptografia.

Desmarcamos a opção “Chave fornecida automaticamente”. Seleccionamos o comprimento da chave de 104 bits e escrevemos uma chave de 13 caracteres ou 26 dígitos hexadecimais. Marcamos a opção “Esta é uma rede ad-hoc”.

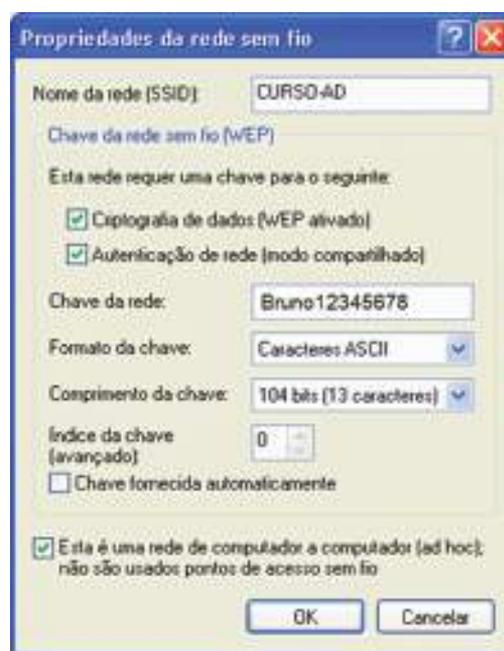


Figura 246: Propriedades de rede sem fios.



A conexão recém criada constará no quadro de redes preferenciais. Fechamos as janelas para finalizar.

Depois de fazer estas configurações num computador qualquer da rede, será preciso fazer configurações semelhantes em todos os restantes computadores.



Figura 247: Propriedades de rede sem fios.

Ao fazermos o mesmo num outro computador qualquer da rede, a ligação protegida recém-criada aparecerá na lista de Redes disponíveis.



Clicamos na rede que criamos e a seguir em Configurar. Poderemos então fornecer a mesma chave que usamos no primeiro computador.

Figura 248: Configuração da rede sem fios em outros computadores.



Usamos a mesma chave WEP e fazemos as mesmas configurações que foram usadas no primeiro computador. Todos os computadores da rede sem fio protegida devem usar configurações semelhantes.

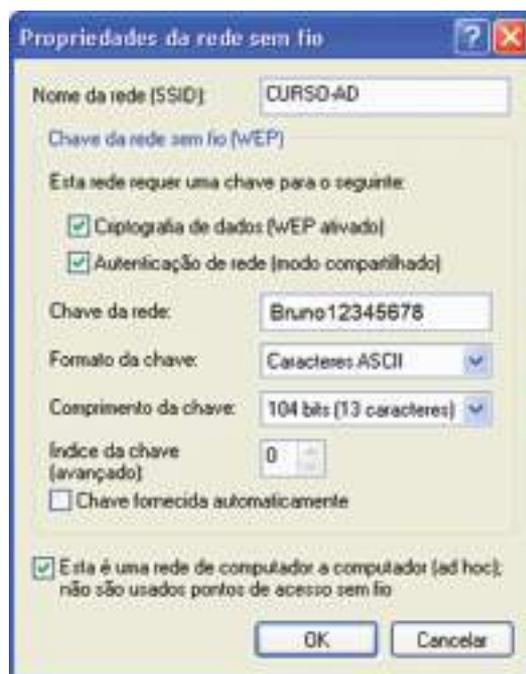


Figura 249: Propriedades da rede sem fios.

Usamos os comandos já apresentados na rede sem proteção. Verificamos a intensidade do sinal.

Note que computadores que não tenham o código, mesmo que recebam um sinal forte, não poderão entrar na rede.

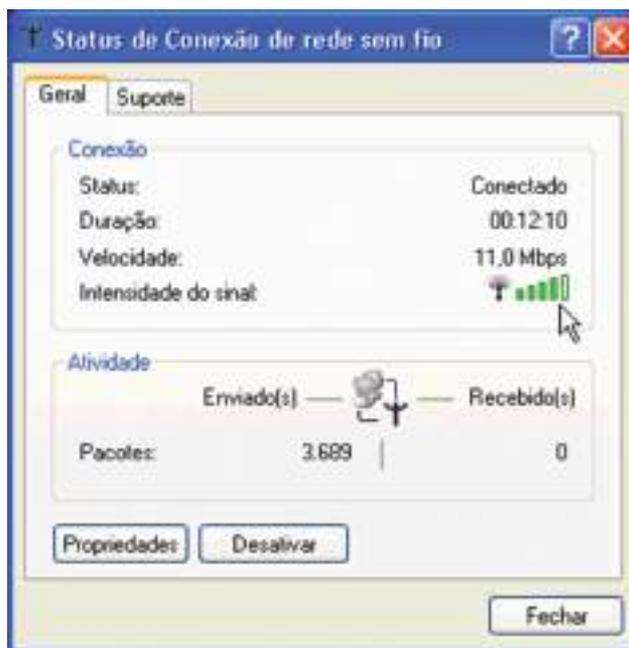


Figura 250: Status da rede sem fios.

Uma outra forma para programar a chave WEP numa rede já configurada é abrir a janela de conexões de rede sem fio, clicar na rede desejada e escrever a chave. O Windows irá memorizar automaticamente esta chave e o acesso à rede estará disponível. Não será mais preciso fornecer esta chave, já memorizada.

Se em um computador que ainda não teve a chave correta configurada, deixamos a chave em branco ou usamos uma chave errada, o acesso à rede não estará disponível.





Figura 251: Senha de rede errada.

Sem a chave correta, o computador não entra na rede. Não é possível exibir os computadores do grupo de trabalho. Nem podemos usar o comando PING, os computadores protegidos não responderão, mesmo que usemos os IPs corretos.

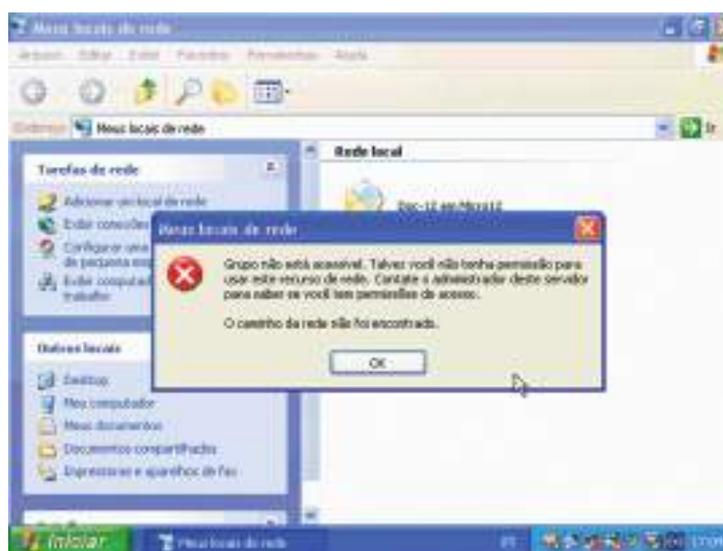


Figura 252: Acesso negado à rede sem fios.

## Instalação de uma rede wi-fi com Wireless Broadband Router

Uma aplicação interessante das redes sem fio é a partilha de ligação de banda larga. Para isto devemos usar um wireless broadband router.

O modelo que vamos usar como exemplo é fabricado pela LinkSys, que é uma divisão da CISCO, um dos maiores fabricantes de equipamentos para redes.



Devemos ligar este router ao modem de banda larga, seja ele ADSL ou a cabo. Para iniciarmos a configuração, devemos ligar um computador a este router, usando um cabo UTP/RJ-45.



Figura 253: Router de banda larga wireless.

Usamos o comando Status / Suporte da placa de rede (com fio) e clicamos em Reparar. Desta forma descobriremos o IP do router. No exemplo ao lado vemos que o IP deste router é:

192.168.1.1

Esta informação é necessária para usar o Setup do router, que é muito parecido com os de outros routers já mostrados anteriormente. No caso deste produto não será preciso usar o Setup, pois o software que o acompanha no seu CD-ROM faz a configuração automaticamente, exceto a criptografia. Começemos então sem criptografia.



Figura 254: Status da rede sem fios.



Depois de fazer as ligações no modem e no computador, usamos o CD que acompanha o produto. Entrará em execução o seu programa de configuração. Clicamos em Setup Wizard.

É preciso ainda ligar o computador à Internet. No caso de modems a cabo, a conexão já está feita.



Figura 255: Software de instalação LinkSys.

No caso de conexões ADSL, o procedimento é um pouco diferente. Ligamos o computador diretamente no modem (sem router) e fazemos a ligação (o modem deve operar no modo bridge). Depois de conetado, desconetamos o cabo que liga o modem ao computador. Ligamos o modem no router (porta WAN) e o computador no router (uma das portas WAN).



Figura 256: Ligação com o modem.



O router já estará então ligado à conexão de Internet (ativa) e ao computador. Podemos clicar agora em NEXT.



Figura 257: Ligação com o computador.

É preciso verificar se os LEDs do router estão acesos. Devem estar acesos os LEDs correspondentes à conexão WAN e à conexão LAN usada. Se os LEDs correspondentes não acenderem, então está a ser usado um cabo errado. O cabo que liga o router ao computador deve ser do tipo direto, e o que liga o router ao modem é normalmente do tipo crossover.



Figura 258: Verificação dos leds.



No nosso teste, o programa de instalação informa que não conseguiu estabelecer contato com o router, e pede que pressionemos o botão RESET na parte traseira do roteador durante 10 segundos. Devemos desligar o router antes de realizar esta operação. Depois de ligá-lo, clicamos mais uma vez em NEXT e o programa de instalação prosseguiu normalmente.

Podem ocorrer certos “desvios de percurso” como este, dependendo do produto que está a ser instalado.



Figura 259: Erro de ligação com o router.

Preenchemos o nome de utilizador e a senha. Neste caso usamos, os dados do nosso provedor de serviço.



Figura 260: Configuração PPPoE.

Este router vem configurado de fábrica com username admin e senha 1234. Podemos neste momento preencher algo diferente, o que é altamente recomendável (lembre-se dos vizinhos).





Figura 261: Atribuição de nova password ao router.

O programa de instalação chama a rede de LINKSYS e utiliza o canal 6. Podemos usar essas configurações, ou então escolher um nome ao nosso gosto. Se tivermos problemas com o sinal fraco mudamos depois para outro canal, usando o Setup do router.



Figura 262: Atribuição de SSID.

Terminada a instalação, podemos testar o acesso à Internet, primeiro através das conexões via cabo. Depois podemos fazer os testes com os computadores que usam placas de rede sem fio.





Figura 263: Finalização da instalação.

Usando o comando “Exibir redes sem fio disponíveis” vemos a rede criada pelo roteador (LINKSYS). Para entrar na rede basta selecioná-la e clicar em Conectar.

A partir daí podemos usar a rede sem fio e a rede por cabo (lembre-se que o router possui também conectores RJ-45). Podemos aceder aos documentos e impressoras e também aceder à Internet. Todos os computadores da rede, sejam ligados com fio ou sem fio, terão acesso a todos os recursos.



Figura 264: Redes disponíveis.

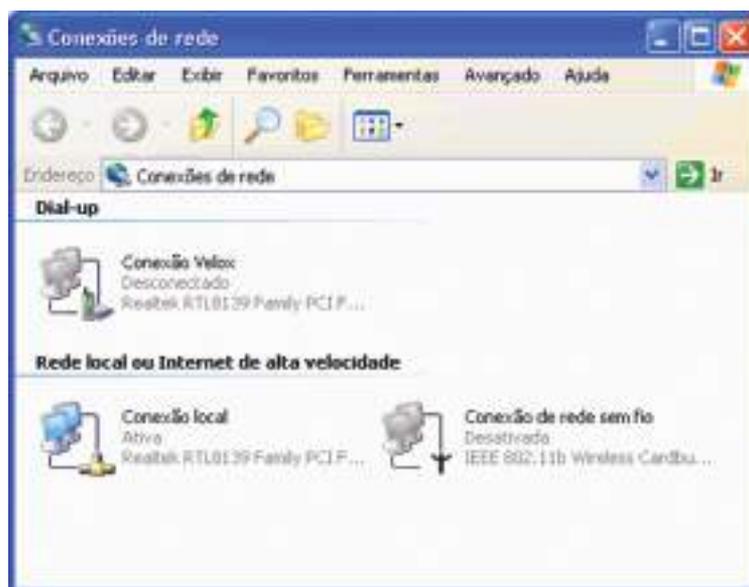


## Instalação de uma rede wi-fi com Wireless Broadband Router e WEP

Também no caso de routers de banda larga sem fio, não devemos deixar a rede desprotegida. É preciso ativar a proteção WEP no router e nos computadores que usam placas de rede sem fio.

Para fazer as configurações, usamos inicialmente uma placa de rede normal. No exemplo da figura 265 usamos um computador com duas placas de rede, sendo uma normal e outra sem fios. Desativamos a conexão sem fio para que o acesso seja feito apenas pelos conectores RJ-45.

Figura 265: Exemplo de ligações de rede disponíveis.



Mais uma vez usamos o comando Status / Suporte para descobrir o IP do router, pois será preciso usar o seu Setup. Clicamos em Reparar para obter o novo IP. Se for apresentada rapidamente uma mensagem de “operação concluída”, significa que a conexão entre o computador e o roteador está perfeita.

No exemplo, o IP do router é:

192.168.1.1

Figura 266: Status da ligação local.



Escrevemos então no navegador: *http://192.168.1.1*

O router será contactado e pedirá o preenchimento de username e password. Normalmente usamos aqui o nome e senha que vêm de fábrica, mas no nosso exemplo programamos um outro nome e senha quando executamos o software de configuração do router. Devemos escrever essas informações.

Não é aconselhável o uso de senhas fáceis de adivinhar, lembre-se dos vizinhos!

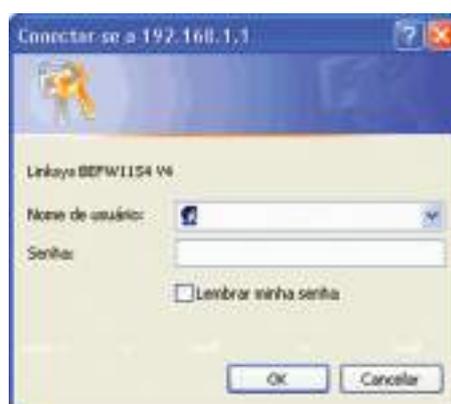


Figura 267: Menu de entrada no setup do router.

Depois de entrar, clicamos então em Wireless e a seguir em Wireless security.

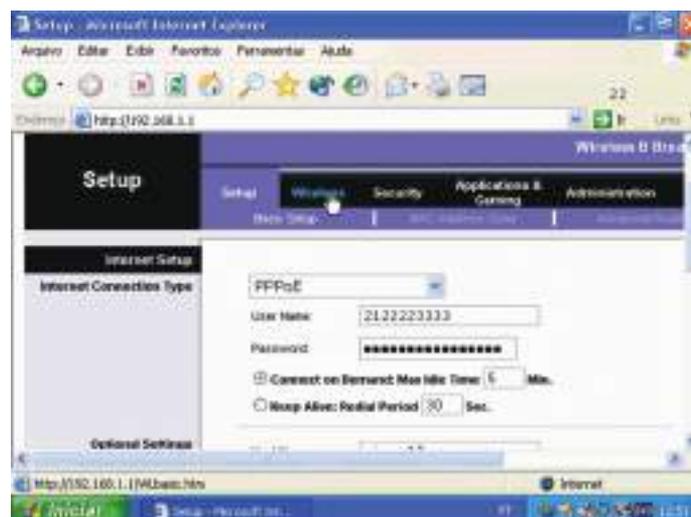


Figura 268: Menu de dados de segurança da rede sem fios.

Usamos então as seguintes configurações:

- Wireless Security: Enable
- Security Mode: WEP
- Wireless Encryption Level: 128 bits



Devemos agora escrever uma WEP Key com 26 dígitos hexadecimais. Podemos gerar esta chave de outra forma, escrevendo uma sequência de 13 caracteres e clicamos em Generate, assim uma chave será gerada em função desta sequência.



Figura 269: Menu para gerar e criar nossa password de entrada no router sem fios.

Clicamos em Save Settings no Setup do router e fechamos o navegador. Agora devemos ativar a conexão sem fios no computador que utilizamos e desativar a conexão com fio (ou desligar o cabo).

Para ativar a conexão sem fios, clicamos com o botão direito e escolhemos a opção Ativar.

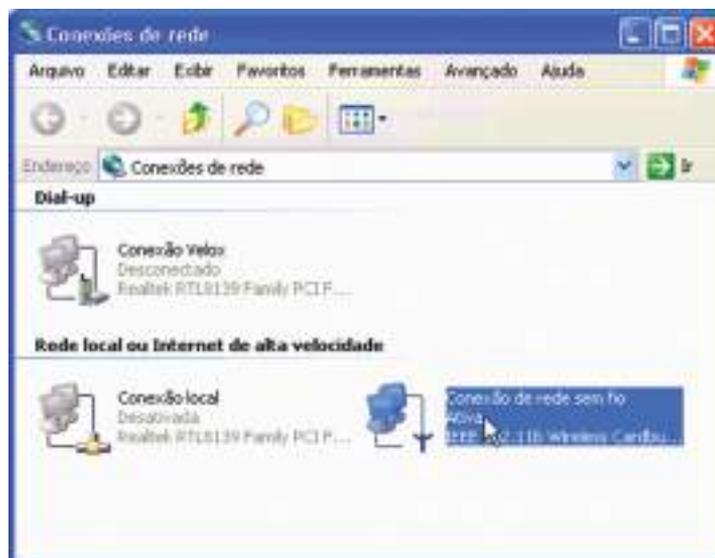


Figura 270: Ativação da ligação de rede sem fios.

Como sempre, verificamos o nível de intensidade do sinal recebido pela placa de rede sem fios. Se o nível estiver fraco, fazemos o reposicionamento da antena ou do router.





Figura 271: Verificação da intensidade de sinal.

Selecionamos a guia Suporte e clicamos em Reparar. Isto é necessário, pois o IP da conexão pode ainda estar válido, tendo sido obtido antes do WEP ser ativado no router.



Figura 272: Menu para renovar o IP.

Como esta ligação não está a usar WEP e o router está, ocorrerá uma falha na renovação do IP, como mostra a mensagem da figura 273. O IP atribuído à placa de rede sem fio será da forma

169.254.xx.yy

Que é o tipo de IP usado em redes Microsoft que não possuem DHCP. No caso, a rede possui sim um DHCP, que é o router, mas o computador não conseguiu contato pois não tem o código WEP. Isto mostra que a rede sem fios criada pelo nosso router está protegida.



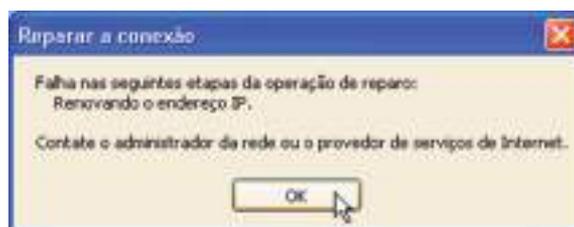


Figura 273: Mensagem de erro, de falha na renovação de IP.

A ligação de rede sem fios de cada computador deve ser agora configurada com a mesma chave WEP programada no router. Para isto abrimos as propriedades da ligação de rede sem fios e clicamos na guia Redes sem fios.

Clicamos na rede desejada (LINKSYS) e em Propriedades.



Figura 274: Ativação WEP no computador.



Marcamos a opção “Criptografia de dados – WEP ativado”. Desmarcamos a opção “Chave fornecida automaticamente” e escrevemos a mesma chave configurada no router. Clicamos em OK para finalizar.

Figura 275: Menu para inserir a nossa chave WEP.



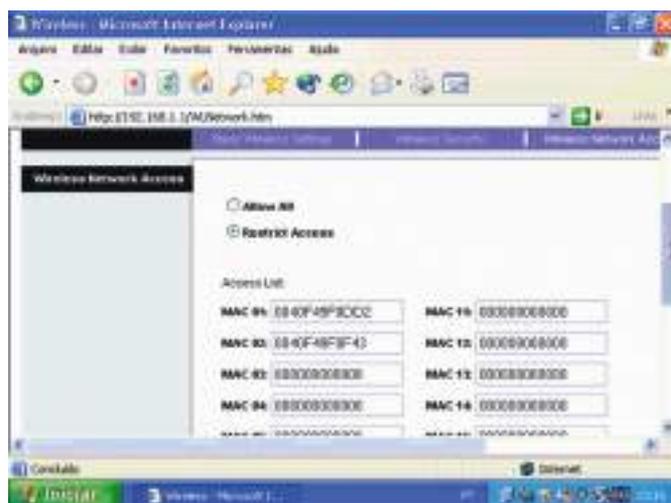
Para testar a comunicação entre o computador com placa de rede sem fios e o router, devemos inicialmente tentar receber um IP. Usamos então o Status da conexão, clicamos em Suporte e Reparar. Se a comunicação estiver perfeita, depois de alguns segundos será apresentada uma mensagem de “operação concluída”. A placa de rede receberá um IP (no exemplo da figura 278, 192.168.1.101) e será indicado o IP do router (Gateway padrão), que no exemplo é 192.168.1.1.



Figura 276: Status da nossa rede sem fios.

Podemos agora iniciar o navegador e navegar livremente pela internet. Podemos ainda fazer um teste à rede, fazendo o acesso a documentos e pastas partilhadas. A nossa conexão está perfeita e totalmente protegida do acesso de estranhos.

Um ultimo aspeto e não menos importante, é que os roteadores de banda larga permitem restringir ainda mais o acesso, fornecendo uma proteção adicional à rede, impedindo que computadores externos acedam indevidamente. No setup do router encontramos um comando onde indicamos os endereços MAC das placas de rede sem fio usadas na nossa rede. Neste menu inserimos o MAC address da placa que queremos bloquear, e assim mesmo tendo a senha de entrada na nossa rede sem fios estes computadores não



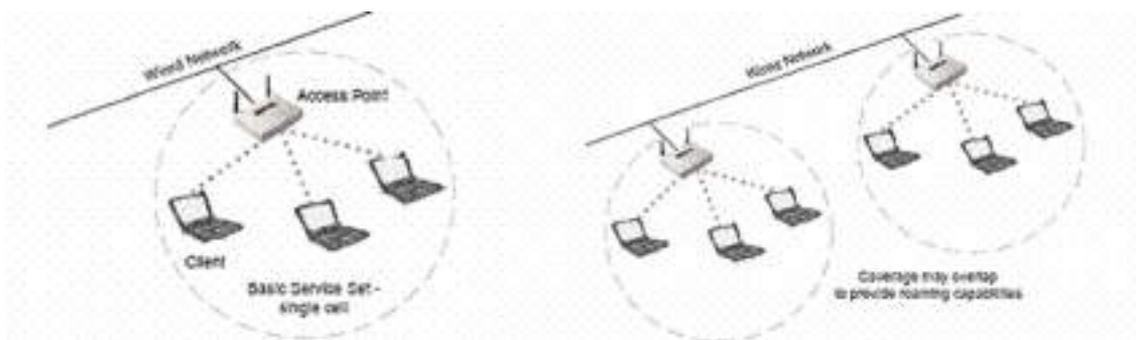
teram acesso a nenhum recurso da rede.

Figura 277: Menu de bloqueio por MAC address.



## Questionário

1. Qual é o significado das siglas FCC e IEEE?
2. Existem diversos padrões IEEE para as redes sem fios. Enuncie alguns dos mais conhecidos.
3. Qual é a técnica de transmissão utilizada pelas WAN's? Quais são as suas características?
4. As Wans podem ser utilizadas em duas formas, Indoor e Outdoor. O que é uma Wann Indoor?
5. Diga o que entende por redes AD-HOC.
6. Enuncie algumas das características de redes de infraestruturas.
7. Das seguintes figuras, diga qual é o sistema BSS e qual é o sistema ESSS.



(a)

(b)

8. Diga o que entende por WAN outdoor.



# Segurança em Redes

Imaginemos que resolvemos usar tudo o que aprendemos até agora para montar uma rede e conectá-la à Internet. Em poucas semanas todo o funcionamento da nossa empresa/escola passou a depender desta rede. Infelizmente, depois de muito trabalho e centenas de configurações detalhadas, um hacker Invadiu a nossa rede e apagou todos as configurações. Isso obrigar-nos-ia a perder horas e horas para colocar tudo como estava antes, especialmente se nos esquecemos de fazer backup dos dados das principais máquinas do sistema. Como tempo e dinheiro são irmãos muito próximos, um grande prejuízo foi o que sobrou dessa brincadeira.

A visão pessimista que demos acima serve para ilustrar o quanto pensar em segurança é fundamental. A segurança de redes é o principal capítulo da segurança digital. Não existe hoje uma rede profissional que não implemente mecanismos de segurança, qualquer um que seja, visando evitar incidentes que causem prejuízos.

Infelizmente, a segurança de redes normalmente está associada a jovens de 16 anos cheios de espinhas no rosto que ficam o dia todo a tentar invadir o Pentágono ou a NASA. Esta visão cinematográfica do assunto atrapalha ainda mais na quando se tem de falar seriamente sobre ele.

Em primeiro lugar, a segurança de redes não trata apenas de invasões e ataques externos. Pouco importa ao presidente de uma grande multinacional se a empresa ficou offline por causa de um hacker ou porque o administrador derramou café sobre o router.

Ao longo do curso, em módulos anteriores já mostramos um elemento necessário que está além da proteção contra invasões: o backup. Vamos aproveitar e aprender a primeira regra da segurança digital e, conseqüentemente, da segurança de redes: faça backup!

E já que falamos do assunto, a segunda regra é: quem tem só um backup não tem nada. Este capítulo não tem a intenção de criar alunos especialista em segurança de redes ou em segurança digital. Essas duas áreas são multidisciplinares e amplas o suficientes para preencherem vários módulos e até cursos. O objetivo com este capítulo é alertar para a real necessidade de segurança dentro da uma rede e dar a uma ideia geral de como implementar essa segurança.



### *Segurança Física da Rede*

De nada adianta começarmos a falar sobre métodos para impedir que um *hacker* entre no nosso sistema se não implementarmos na nossa rede processos de prevenção e controle.

Esses processos devem diminuir as vulnerabilidades ambientais e resguardar todo o sistema de uma fatalidade. No caso de uma fatalidade ocorrer, o retomo do sistema ao seu estado normal deve ser o mais rápido possível e a causa deve ser identificada imediatamente.

Em primeiro lugar, as máquinas vitais para a nossa rede devem ser colocadas num lugar seguro, longe de condições climatéricas e ambientais que possam danificá-la, reduzir a sua vida útil ou provocar problemas de interrupção do funcionamento a longo prazo.

Para isso, deve-se dispor de um CPD (Centro de processamento de Dados) bem equipado, dotado de sistema elétrico controlado (estabilizadores) e até mesmo de unidades alternativas de energia, no caso de falha da rede elétrica (no-breaks).

O acesso a esse CPD só deve ser permitido a pessoal autorizado, treinado para operar as máquinas que estão lá dentro e todo acesso deve ser identificado e arquivado. Isso quer dizer que todos os técnicos que entrarem no CPD devem deixar descrito os seus dados pessoais, a hora a que entrou, que trabalhos realizou e a que hora deixou o CPD.

Essas informações devem ser conferidas e validadas por um funcionário “fiscal”.

Deve haver um sistema anti incêndio não prejudicial aos equipamentos (normalmente é usado em Inundação de gás). Não deve ser permitido fumar nas instalações desse CPD e isso lembra separar o sistema de ar condicionado do CPD do sistema do resto da empresa. O ar refrigerado do CPD deve ser filtrado. Claro que isto em condições ideais, por vezes a realidade é bem diferente, e temos que nos adaptar ao meio em que estamos.

É preciso estabelecer uma periodicidade para fazer backup de todas as máquinas do CPD. O hardware de backup deve ser renovado constantemente, isto é, não se deve regravar sobre a mesma drive muitas vezes seguidas.

É claro que a Implementação de cada um dos processos acima depende do orçamento financeiro de cada um. Um CPD bem equipado pode passar de 1 milhão USD em gastos, fora os equipamentos! Com isto, queremos dar apenas uma ideia do que seria um ambiente próximo do ideal.



## *Segurança Preventiva de Dados*

A segurança preventiva implementa ações que procuram evitar que dados sejam danificados ou comprometidos sem que a ação direta de terceiros ou sem que a ação de pessoas mal-intencionadas criem o problema. Uma falha de um operador de computador que sem querer apague uma pasta importante do sistema, por exemplo, deve poder ser evitada ou reparada facilmente.

O principal elemento dessa parte da segurança é o antivírus. Se já é impensável ter um computador sem antivírus, imaginemos uma rede inteira! Além disso, a Internet acelerou ainda mais o tempo de distribuição dos vírus. Se há uns anos atrás os vírus levavam até 14 meses para se propagar em grande escala, hoje em dia apenas 30 minutos são mais do que suficientes para atingir milhões de computadores em todo o mundo. É inviável que um software antivírus funcione bem apenas com atualizações mensais ou semestrais como acontecia antigamente.

Atualmente a solução profissional adotada em redes de todos os tamanhos é a de antivírus distribuído. Nesta solução passa a residir na rede interna um servidor antivírus, responsável por procurar novas atualizações e “vacinas” de maneira a distribuir essas vacinas para os antivírus clientes, instalados nas estações de trabalho. Existem soluções que conseguem identificar vírus que não são conhecidos, guardá-los em quarentena, enviar uma cópia do vírus para um laboratório especializado e aguardar por uma vacina para que possa desinfetar o ficheiro. Tudo isso automaticamente e sem que o administrador tenha de intervir. Entretanto, os erros dos utilizadores não são considerados como vírus e a eliminação de uma pasta de sistema, continua a ser uma ameaça. Para estes casos existem soluções de “congelamento” do sistema que conseguem impedir que ações danosas ou não autorizadas pelo administrador sejam realizadas. Esses softwares monitorizam o funcionamento do sistema e verificam se a ação ou o comando que o utilizador ou programa está a executar é permitido pela política do administrador, caso contrário exibe uma mensagem onde informa que ocorreu um erro.

## *Sistemas Ativos de Segurança*

Os sistemas ativos de segurança visam evitar que ataques estruturados sejam feitos contra uma rede ou um sistema específico. Eles impedem que pessoas mal-intencionadas



consigam explorar fendas e vulnerabilidades com o objetivo de penetrar no sistema com objetivos duvidosos.

Como o nosso foco é em redes e não em sistemas de segurança de uma forma genérica, vamos analisar apenas o principal elemento responsável pela segurança de redes: a *firewall*.

### Firewall

Hoje em dia praticamente todas as estruturas de segurança de redes dependem do conceito de firewall. A ideia original da firewall era isolar a sua rede interna da Internet, por completo. Como a Internet é uma rede que respira TCP/IP, não existe melhor forma de fazer isso do que “escutar” todo o tráfego TCP/IP endereçado para a nossa rede interna, proveniente da Internet, e todo o tráfego para a Internet, proveniente da nossa rede interna. O objetivo destas “escutas” era o de filtrar o que era permitido do que não era. Como regra geral, praticamente tudo era proibido e, aos poucos, foram criadas regras que permitiam a passagem do tráfego essencial.

Uma firewall é, na realidade, um poderoso router que interliga duas redes e possui, pelo menos, duas placas de rede. Numa ponta temos sempre a rede pública, ou insegura e, na outra, temos a rede privada, ou segura.

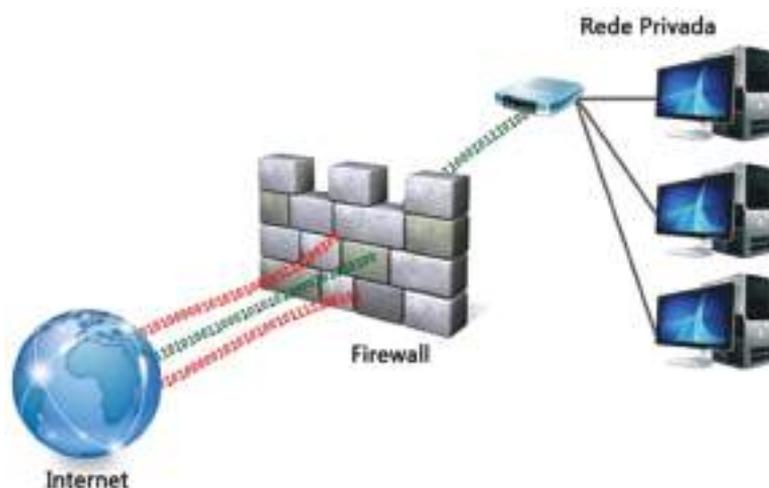
A firewall funciona analisando os cabeçalhos dos pacotes IP que passam através dela, com origem ou destino a uma das redes à qual quer proteger. Para facilitar as explicações, vamos supor que a rede de destino e de origem sejam sempre diferentes.

Ao analisar o cabeçalho dos pacotes, a firewall consegue saber os protocolos usados e as portas de origem e destino do pacote. Como informação adicional, a firewall pode ainda analisar os endereços IP de origem e destino. Depois disso, ela faz uma comparação numa tabela de regras, analisando se o pacote pode prosseguir ou não. No caso de o pacote estar permitido (ou “abençoado”, como alguns técnicos preferem dizer), a firewall passa a agir como um router normal. No caso de o pacote não se enquadrar em nenhuma regra, a firewall pode tomar duas decisões: recusar a receção do pacote (*deny*) ou descartá-lo (*drop*).

Quando um pacote é recusado, existe uma comunicação entre a firewall e o remetente do pacote, a informar que a conexão foi cortada. No caso de um pacote descartado, essa

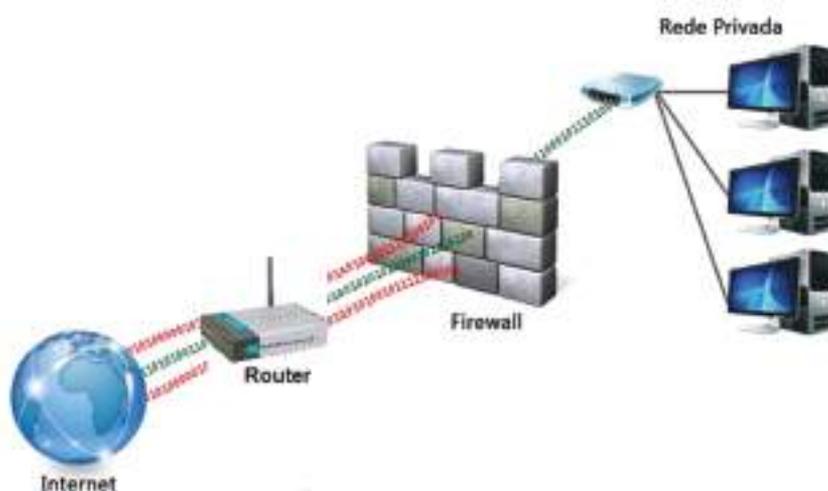


comunicação não existe e a firewall simplesmente ignora qualquer comunicação vinda do remetente do pacote, fazendo parecer que o pacote simplesmente se perdeu. Na figura 278 podemos observar o esquema básico de implementação da firewall numa estrutura de rede ligada à Internet.



*Figura 278: Ligação simples de uma firewall, a proteger uma rede ligada à Internet.*

A firewall pode ou não estar ligada diretamente ao seu backbone Internet. Normalmente existe um outro router na frente dela, já que usualmente as firewalls são PCs com duas placas de rede e o seu backbone Internet fornece um cabo do padrão V.35 (que é um conector de 34 pinos), não suportado pelas placas de rede Ethernet. Se o nosso orçamento de rede permitir, com certeza é melhor optar por ter um router na frente e deixar que a firewall faça apenas o seu trabalho de filtragem de pacotes, como mostramos na figura 279.



*Figura 279: Esquema preferível, utilizando uma firewall e um router para ligar a nossa rede à Internet.*

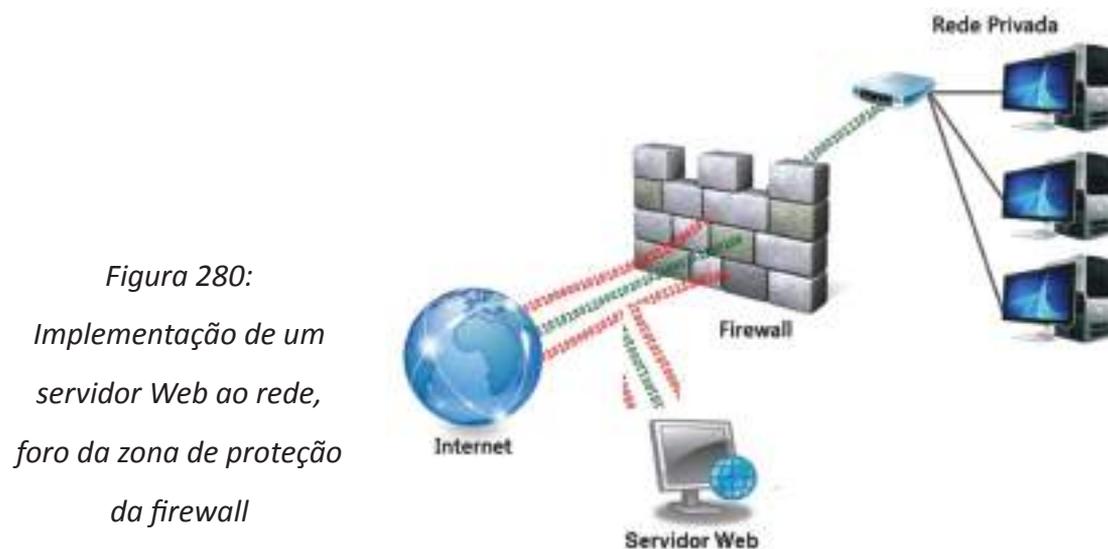


O conceito de firewall não é proprietário do mundo TCP/IP. Existem firewalls para outros tipos de rede, mas sem dúvida alguma a firewall é um organismo ideal para a comunicação de redes TCP/IP.

Vale a pena ressaltar que a firewall, como dissemos, analisa apenas os cabeçalhos dos pacotes IP e não os dados. Embora existam firewalls no mercado que hoje em dia façam esse tipo de análise, essa é uma tarefa que está além das obrigações de uma firewall normal. Se precisarmos que exista a análise do conteúdo dos pacotes IP na nossa rede, então o ideal é que sejam utilizadas ferramentas específicas de filtragem de conteúdo para trabalhar em conjunto com a firewall.

### *Colocar a nossa rede acessível*

Anteriormente dissemos que a função original da firewall é a de isolar completamente a nossa rede da Internet. Esse conceito, que era muito prático há alguns anos atrás, mudou completamente nos dias de hoje. Hoje em dia a ideia em vigor é a de permitir o acesso controlado aos recursos da nossa rede interna por utilizadores da rede externa. A arquitetura da firewall como um bloqueador geral começou a trazer problemas quando algumas empresas quiseram colocar servidores web para disponibilizar páginas www aos seus visitantes. Só que a segurança não podia ser esquecida em momento algum, e permitir o acesso externo a uma máquina da rede interna era, no mínimo, insano. Uma pessoa mal-intencionada que tivesse invadido um servidor web na rede interna poderia passar a fazer absolutamente tudo dentro da rede interna da empresa, como se ele fosse um utilizador de uma estação de trabalho presente na rede local dessa empresa.



*Figura 280:  
Implementação de um  
servidor Web ao rede,  
fora da zona de proteção  
da firewall*

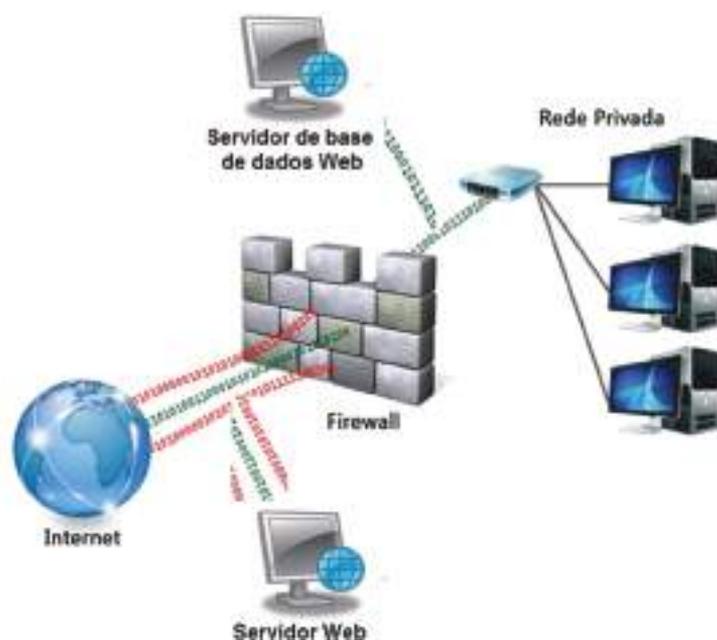


No princípio, a solução adotada é a apresentada na figura 280. Nela o servidor web fica fora da zona de proteção do firewall. Isso impedia que um utilizador externo no controlo do servidor web tomasse ações destrutivas na rede interna. Por outro lado, o próprio servidor web estava totalmente à mercê dos hackers para ser invadido.

Colocar o servidor web na rede interna dificultava o trabalho desses hackers, mas ao mesmo tempo dava todos os direitos aos hackers mais Inteligentes e perigosos. Colocar o servidor web na rede externa facilitava o trabalho dos hackers, mas impedia que um hacker, por mais esperto que fosse, acesse indiscriminadamente à rede interna

Além disso, o servidor web normalmente não guardava qualquer informação valiosa, principalmente porque a média de acessos na web era muito baixa e uma intrusão na página principal de uma empresa tinha pouco ou nenhum impacto. Com o passar dos anos e o crescimento do número de utilizadores (e hackers) na Internet, o valor das informações colocadas nas páginas principais das empresas subiu. Agora, os negócios passavam a ser feitos também através do servidor web, normalmente utilizando uma base de dados para armazenar pedidos e tudo o que fosse necessário. Se a página principal continuava valendo pouco, a base de dados valia muito e era vital para a empresa e não poderia nunca ficar na rede externa.

A solução encontrada e apresentada na figura 281, colocando a base de dados na rede Interna e abrindo uma regra na firewall a permitir ao servidor web acesso a essa base de dados. Parece seguro o bastante, certo? Mas não é, nem um pouco.



*Figura 281: Implementação de um servidor de base de dados Web.*



Apesar de o servidor de base de dados estar protegido, o servidor web não está e, além disso, esse servidor tem poderes sobre o servidor de base de dados. Assim, um hacker que tivesse a apoderar-se do servidor web poderia fazer acessos ao servidor de base de dados para copiar os seus dados ou alterá-los ou até mesmo obter acesso à máquina onde a base de dados se encontrava e, assim, agir na rede interna como se fosse um utilizador de uma estação de trabalho interna, podendo fazer o que bem entender.

Esse tipo de ataque exigia muito mais conhecimento técnico, mas normalmente o retorno financeiro proporcionado por ele era alto (roubando a base de dados da empresa, que contém dados pessoais dos clientes, incluindo os números de cartões de crédito, tornando qualquer arquitetura baseada no conceito da Figura 281 um bom alvo para a ação de hackers.

A melhor solução é separar o servidor de base de dados da rede interna, sem colocá-lo na rede externa, e, ao mesmo tempo, aumentar a segurança do servidor web. Como fazer Isso?

A melhor maneira é criar uma rede intermediária, entre a rede externa e a rede interna, que passou a ser conhecida como Rede Desmilitarizada, ou simplesmente DMZ (DeMilitarized Zone NetWork).

### *DMZ (DeMilitarized Zone Network)*

A Rede Desmilitarizada (DMZ) requer duas firewalls para ser implementada. Entre essas duas firewalls a rede abriga o servidor web e o servidor de base de dados. A figura 282 ilustra o conceito inicial de DMZ.



Figura 282: Conceito inicial de DMZ.



Na firewall externa (firewall 1) eram criadas regras que permitiam o acesso ao servidor web e bloqueavam o acesso a qualquer outra coisa. Já a firewall interna (firewall 2) tinha a função de bloquear o acesso à rede Interna.

Como não havia mais firewalls entre o servidor web e a base de dados, a relação de confiança entre eles passava a ser ainda mais forte. No mundo da segurança, as principais falhas de segurança (buracos) têm origem nas relações de confiança.

Agora a rede interna estava bastante protegida, o servidor web estava protegido e a base de dados estava levemente protegida. Apesar de não ser possível aceder à base de dados diretamente, vindo da Internet, continuava a ser possível fazer investidas contra o servidor web e, uma vez dentro dele, podia-se fazer muito mais coisas contra a base de dados do que antes. O acesso à rede interna era completamente negado, mas quem precisa de acesso á rede interna quando se pode fazer o que quiser na base de dados de um home banking por exemplo?

Rapidamente os administradores de rede deram conta disso, especialmente depois de dois famosos incidentes que envolveram bancos que usavam esta arquitetura. A solução para esse problema é apresentada na Figura 283.



*Figura 283: Solução para a falha de segurança apresentada pela arquitetura DMZ tradicional.*

Agora o servidor web passa a residir sozinho na DMZ e a firewall interna (firewall 2) permite apenas o acesso necessário à base de dados, evitando muitas das alterações que um acesso total à máquina permitiria.

Esta solução, desde que seja corretamente configurada, é segura o suficiente para fazer qualquer administrador de rede dormir tranquilo.



O único detalhe dela é que o preço de implementação de duas firewalls é muito alto e em geral os benefícios não compensavam o investimento. Como contornar essa questão financeira?

A ideia que surgiu é a de colocar uma terceira placa de rede numa firewall única, criando nessa placa a DMZ, como mostra a Figura 284. As regras nela devem ser melhor detalhadas e deve-se tratar a DMZ como uma rede insegura, mas na prática o efeito é exatamente o mesmo da solução com duas firewalls.

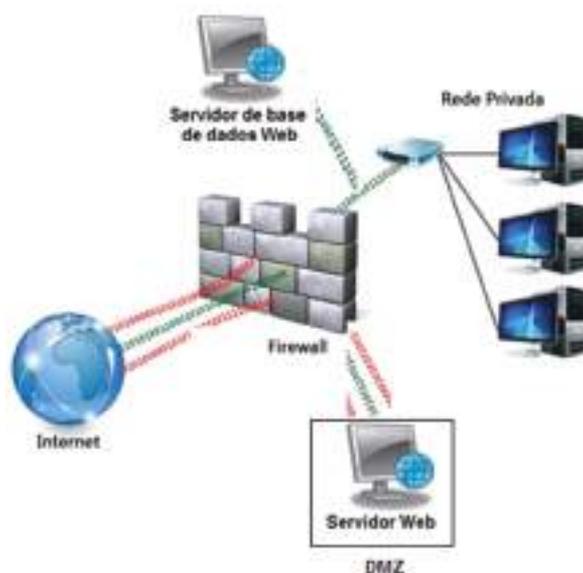


Figura 284: Solução mais barata da DMZ utilizando apenas uma Firewall.

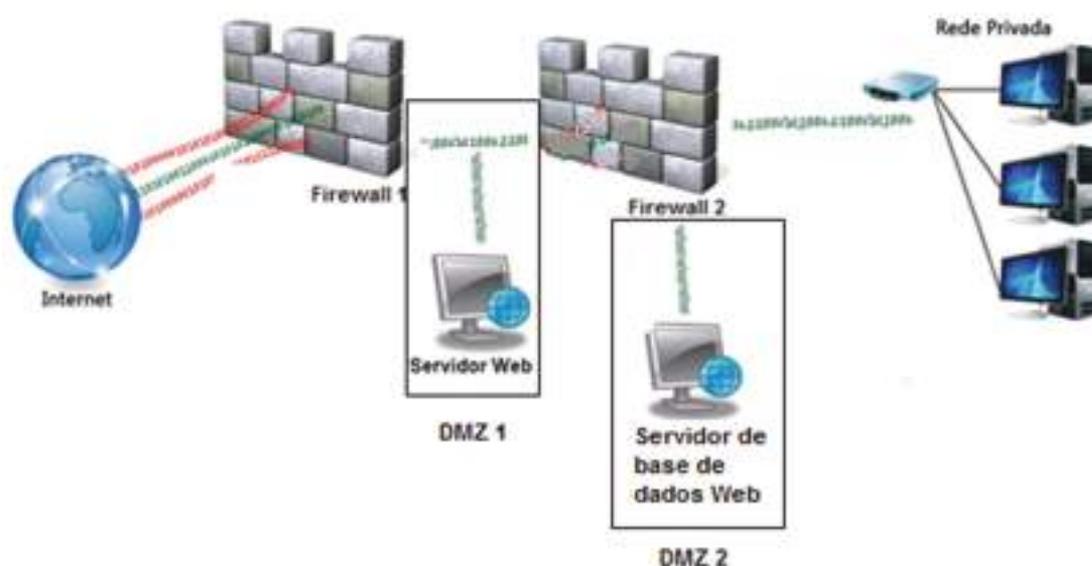
A firewall permite o acesso vindo de qualquer máquina para o servidor web na DMZ e permite o acesso apenas do server web na DMZ à porta correta do servidor da base de dados na rede Interna.

Esta solução é a mais adotada hoje em dia por empresas que precisam de acesso web à base de dados e é tão segura quanto a solução com duas firewalls.

Ainda assim o único se não desta solução é que o seu servidor de base de dados continua na rede interna e, no caso de nos depararmos com um hacker tecnicamente muito bom, os prejuízos causados por acesso não autorizado a dados confidenciais existentes no nosso servidor de disco, por exemplo, podem ser incalculáveis.

A maneira ideal de se proteger por completo desse tipo de ameaça é voltar á arquitetura com duas firewalls, porém acrescentando uma terceira placa à firewall interna (Firewall 2) e, nessa segunda DMZ criada na firewall interna, colocar o servidor de base de dados, como mostra a figura 285.





Acrescentar uma segunda placa de rede à firewall externa (firewall 1) e colocar o servidor de base de dados na DMZ principal entre as duas firewalls têm o mesmo efeito e é a solução preferida pelos administradores que usam esta arquitetura por evitar mais regras na firewall interna, que normalmente possui mais regras do que a externa.

### *Filtragem de Conteúdo*

Como já referimos anteriormente a firewall não analisa os dados dos pacotes IP que passam por ele. Este detalhe técnico é fundamental nos dias de hoje quando queremos dar o maior acesso possível com o maior controlo e segurança.

É impossível numa firewall controlar se estão a entrar vírus através de e-mails ou se os nossos funcionários estão a usar quatro horas do expediente para aceder a páginas indevidas.

A análise e o controlo desse tipo de tráfego é atualmente uma das áreas mais interessantes da segurança digital e é chamada *filtragem e conteúdo*.

### *Filtragem de E-Mail*

A maioria das ameaças de segurança que existem hoje chega através de e-mail. Se pensarmos que uma boa solução é ter um antivírus, o que nos pode manter longe delas, estamos muito enganados.



Normalmente quando falamos de vírus por e-mail, estamos a falar de cavalos de troia. Só que, quando esse tipo de ameaça aparece, demora mais tempo para ser catalogada pelos fabricantes de antivírus do que para chegar até nos. Se nós fizermos um arquivo executável com a linha “Format c:” e enviarmos para alguém via e-mail, o nosso antivírus, por mais poderoso que seja, não fará nada.

Juntando a isso o recurso de que alguns programas para leitura de e-mail têm de executar ou abrir ficheiros anexos simplesmente ao receber o e-mail, sem esperar qualquer comando do utilizador. Já dá para imaginar quão grande poderá ser o prejuízo mesmo depois de ter tanto dinheiro investido numa mega solução de firewalls.

Filtrar o e-mail para o uso adequado pelos empregados de uma empresa é fundamental para o bom funcionamento da nossa rede interna e a manutenção da sua produtividade. Existem hoje no mercado diversos softwares poderosíssimos para esse tipo de controlo. Eles podem filtrar até mesmo o conteúdo da mensagem baseado em padrões pré-estabelecidos por nós, de acordo com uma listagem de assuntos proibidos. Alguns chegam ao ponto de bloquear qualquer e-mail que possua um ficheiro executável anexado (assim, mesmo que ele contenha um vírus desconhecido, o software é capaz de preveni-lo contra).

Podemos usar os recursos desse tipo de programa para controlar todo o tráfego de e-mail de uma empresa e saber quando um funcionário envia informações confidenciais para fora ou quando está a enviar o currículo para uma empresa concorrente, por exemplo.

### *Filtragem Web*

Assim como o e-mail, a web também é uma fonte de perigos. Talvez seja pior do que o e-mail em muitos casos, principalmente porque através dela trabalham programas em Java, JavaScript, ActiveX e VBScript, que podem escrever e ler dados no nosso disco rígido e até mesmo em toda uma rede interna.

Entrar numa página e receber um “escuta virtual” que captura todas as senhas que trafegam na nossa rede local é tão fácil quanto beber uma Coca-Cola e o detalhe é que nós nem sequer vamos perceber que estamos a ser escutados.

Existem soluções para filtragem de conteúdo web tão poderosas quanto as de e-mail e também com recursos de filtragem web no sentido de saída (um funcionário a enviar



dados confidenciais através do webmail, por exemplo), coisa que até pouco tempo atrás parecia impossível.

Filtrar o conteúdo web que entra numa empresa através da navegação web dos funcionários também é uma maneira de manter a produtividade, evitando que eles acessem as páginas com conteúdo incompatível com o horário de expediente.

### Questionário

1. Para que serve um CPD?
2. Diga o que entende por segurança preventiva de dados.
3. Complete a seguinte afirmação:  
“Atualmente a solução profissional adotada em redes de todos os tamanhos é a de \_\_\_\_\_ distribuído. Nesta solução passa a residir na rede interna um \_\_\_\_\_ antivírus, responsável por procurar novas atualizações e “\_\_\_\_\_” de maneira a distribuir essas vacinas para os antivírus clientes, instalados nas \_\_\_\_\_ de trabalho.”
4. O que são sistemas ativos de segurança?
5. Diga como funciona uma Firewall.
6. O que é uma DMZ e em que consiste?



## Bibliografia

Baptista, Carlos Pedro Zaragoza, *Fundamental dos Sistemas Digitais*. Lisboa: FCA – Editora Informática, 2003.

Gouveia, José; Magalhães, Alberto, *Curso Técnico de Hardware*. Lisboa: FCA – Editora Informática, 2003.

Gouveia, José; Magalhães, Alberto, *Hardware Montagem, Atualização, Detecção e Reparação de Avarias em PCs e Periféricos* 4ª ed.. Lisboa: FCA – Editora Informática, 2004.

Gouveia, José; Magalhães, Alberto. *Hardware para PC's e Redes*. Lisboa: FCA – Editora Informática, 2004.

Loureiro, Paulo, *TCP / IP em Redes Microsoft – Para Profissionais*. Lisboa: FCA – Editora Informática, 2004.

Marques, José Alves; Guedes, Paulo, *Tecnologia de Sistemas Distribuídos*. Lisboa: FCA – Editora Informática, 2004.

Monteiro, Edmundo; Boavista, Fernando, *Engenharia de Redes Informáticas*. Lisboa: FCA – Editora Informática, 2005.

Monteiro, Rui Vasco *et al.*, *Tecnologia dos Equipamentos Informáticos*. Lisboa: FCA – Editora Informática, 2005.

Nunes, Mário Serafim; Casaca, Augusto Júlio, *Redes Digitais Com Integração de Serviços*. Editorial Presença, 2001.

VASCONCELOS, LAÉRCIO. *Como montar e configurar sua rede de PCs; rápido e fácil*. São Paulo: Makron Books: Pearson Education, 2003.

Rodrigues, Luís Silva, *Arquiteturas dos Sistemas de Informação*. Lisboa: FCA – Editora Informática, 2003.

Sousa, Sérgio, *Tecnologias de Informação - O que são? Para que Servem?* - 4ª ed.. Lisboa: FCA – Editora Informática, 2005.

