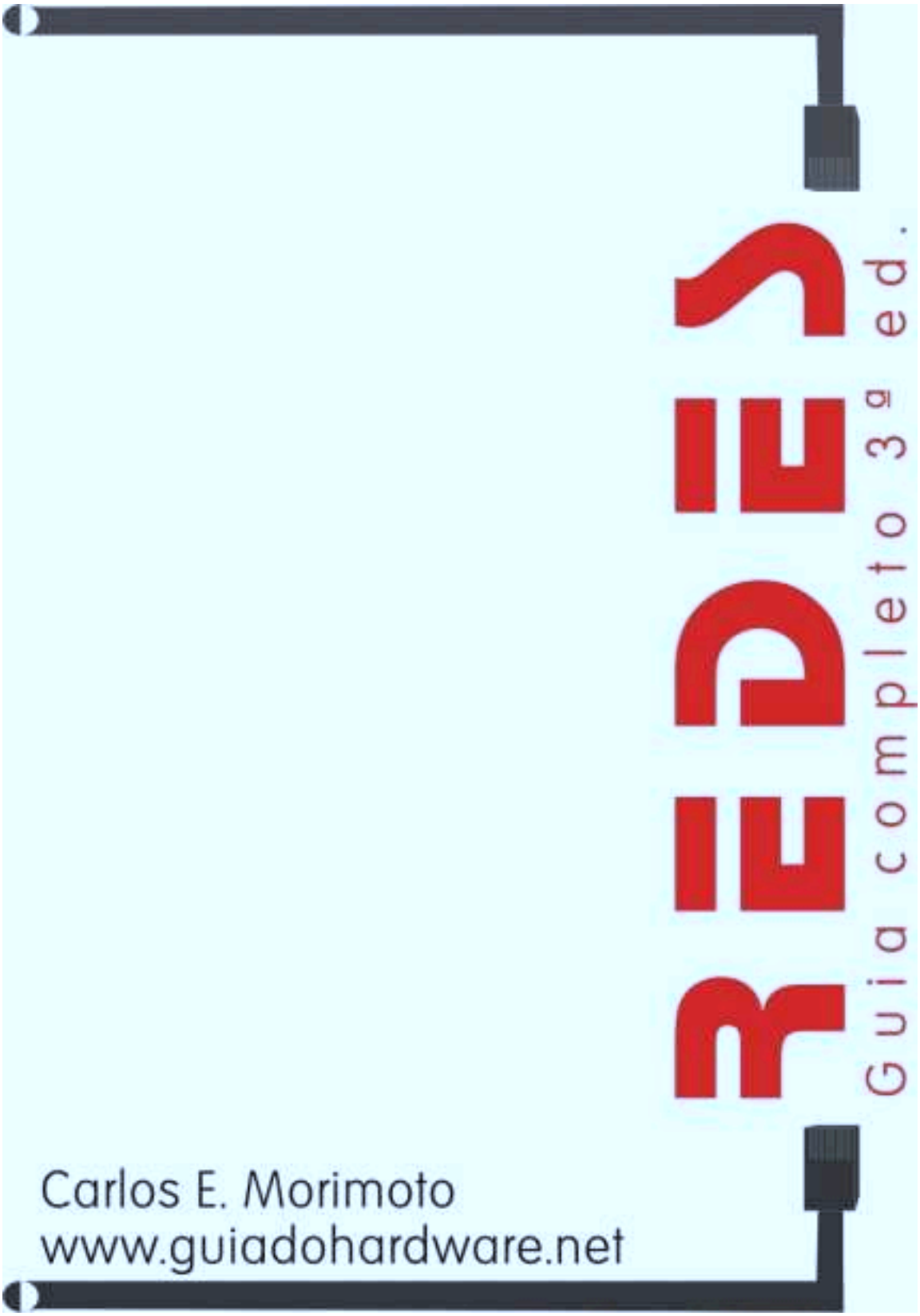

REDES
Guia completo 3ª ed.
Carlos E. Morimoto
www.guiadohardware.net

:. Novo sistema de distribuição:

Antigamente meus e-books eram comercializados de uma forma tradicional, você depositava o valor e ao confirmar o depósito recebia os links para baixar os e-books. O preço reduzido permitia que muito mais pessoas tivessem acesso ao conteúdo do que seria possível com livros impressos vendidos a 50 ou 100 reais em livrarias.

Como a idéia dos e-books é justamente permitir que mais pessoas tenham acesso ao conteúdo, estou agora passando a utilizar um sistema de distribuição diferente. Os links para baixar os e-books estão disponíveis para todos, você pode baixar os e-books e inclusive distribuir os arquivos para outras pessoas, colocar links no seu site, sugerir a publicação na sua revista com CD-ROM favorita, etc. Eles estão aqui justamente para serem distribuídos.

Depois que você ler e comprovar a qualidade dos e-books você pode optar por depositar os **R$ 8,00** que é um valor bem razoável se comparado com o que estes livros custariam em formato impresso ou, se não gostar do material, simplesmente deletar os arquivos.

Os livros continuam sendo vendidos, mas estou dando um voto de confiança, acreditando na sua honestidade e na dos seus amigos :-)

Como disse, sinta-se à vontade para distribuir os arquivos e divulgar estes links, mas explique sobre a forma como eles são distribuídos. Embora **R$ 8,00** seja um valor pequeno, como várias pessoas adiquirem os e-books a renda tem sido suficiente para justificar o trabalho de atualiza-los.

Lembre-se que este valor de R$ 8,00 é por TODA a coleção dos meus e-books, então depois de pagar, sinta-se à vontade para baixar os outros.

O pagamento pode ser feito via depósito bancário, numa das contas abaixo:

- Conta A:
Banco Real (banco nº 275)
Agência: 0544 (PAB UNG - Guarulhos)
C. Corrente: 2713476
Carlos Eduardo Morimoto da Silva

- Conta B:
Banco Itaú (banco nº 341)
Agência: 3150
C. Poupança: 04634-4 / 500
(o /500 é complemento para depósitos feitos no caixa eletrônico)
Carlos Eduardo Morimoto da Silva

- Conta C
Banco Bradesco (banco nº 237)
Agencia - 2304 - 3
C. Poupança - 1003036 - 6
Carlos Eduardo Morimoto da Silva

- Conta D
Banco Banespa (banco nº 33)
Agência: 0110
C. Corrente: 01054925-4
Cristiane Suzukayama

- Conta E
Banco do Brasil (banco nº 001)
Agência: 3435-5
C. Poupança: 803 206-8
(o dígito de variação, necessário para transferências via caixa eletrônico é 1)
Cristiane Suzukayama

Se preferir você pode enviar um vale-postal, cheque, etc. Para:

Carlos Eduardo Morimoto
Caixa Postal 3532
Guarulhos - SP
CEP: 07097-990

Índice geral

Prefácio

As redes vem sendo cada vez mais utilizadas, não apenas em grandes empresas, mas em pequenos escritórios, ou mesmo em casa. A demanda por profissionais qualificados neste mercado vem tornando-se cada vez maior, e as remunerações não são nada ruins. Mesmo que você não pretenda tornar-se um especialista em redes, possuir pelo menos os conhecimentos básicos irá ajudar bastante sua carreira profissional. Se você já trabalha como técnico poderá agora oferecer mais um serviço a seus clientes.

Montar e configurar redes pequenas e médias é uma tarefa surpreendentemente simples. O objetivo deste livro é lhe dar todo o conhecimento necessário para montar redes de pequeno porte, como as usadas em casas e escritórios, incluindo compartilhamento da mesma conexão à Internet, configuração de endereços IP, etc. Porém, também são abordados tópicos mais avançados, como a configuração de máscaras de sub-rede complexas, criação de redes virtuais, etc. que lhe darão uma boa idéia de como montar redes mais complexas. Apesar do assunto parecer bastante técnico, procurei usar uma linguagem os mais didática possível, abordando todos os detalhes, porém sem cair no tecnismo, a mesma linguagem que uso em meus outros livros

Porque ligar micros em rede?

A partir do momento em que passamos a usar mais de um micro, seja dentro de uma empresa, escritório, ou mesmo em casa, fatalmente surge a necessidade de transferir arquivos e programas, compartilhar a conexão com a Internet e compartilhar periféricos de uso comum entre os micros. Certamente, comprar uma impressora, um modem e um drive de CD-ROM para cada micro e ainda por cima, usar disquetes, ou mesmo CDs gravados para trocar arquivos, não é a maneira mais produtiva, nem a mais barata de se fazer isso.

A melhor solução na grande maioria dos casos é também a mais simples: ligar todos os micros em rede. Montar e manter uma rede funcionando, tem se tornado cada vez mais fácil e barato. Cada placa de rede custa apartir de 35 reais, um Hub simples, 10/10 pode ser encontrado por 100 reais, ou até um pouco menos, enquanto 10 metros de cabo de par trançado não custam mais do que 6 ou 8 reais.

Se você mesmo for fazer o trabalho, ligar 10 micros em rede, custaria entre 500 e 800 reais, usando cabos de par trançado e um hub e placas 10/100 em todos os micros.

Com a rede funcionando, você poderá compartilhar e transferir arquivos, compartilhar a conexão com a Internet, assim como compartilhar impressoras, CD-ROMs e outros periféricos, melhorar a comunicação entre os usuários da rede através de um sistema de mensagens ou de uma agenda de grupo, jogar jogos em rede, entre várias outras possibilidades.

Compartilhando arquivos

Num grupo onde várias pessoas necessitem trabalhar nos mesmos arquivos (dentro de um escritório de arquitetura, por exemplo, onde normalmente várias pessoas trabalham no mesmo desenho), seria muito útil centralizar os arquivos em um só lugar, pois assim teríamos apenas uma versão do arquivo circulando pela rede e ao abri-lo, os usuários estariam sempre trabalhando com a versão mais recente.

Centralizar e compartilhar arquivos também permite economizar espaço em disco, já que ao invés de termos uma cópia do arquivo em cada máquina, teríamos uma única cópia localizada no servidor de arquivos. Com todos os arquivos no mesmo local, manter um backup de tudo também torna-se muito mais simples.

Simplesmente ligar os micros em rede, não significa que todos terão acesso a todos os arquivos de todos os micros; apenas arquivos que tenham sido compartilhados, poderão ser acessados. E se por acaso apenas algumas pessoas devam ter acesso, ou permissão para alterar o arquivo, basta protegê-lo com uma senha (caso esteja sendo usado o Windows 95/98) ou estabelecer permissões de acesso, configurando exatamente o que cada usuário poderá fazer (caso esteja usando Windows 2000, XP, Linux, Netware, ou outro sistema com este recurso).

Além de arquivos individuais, é possível compartilhar pastas ou mesmo, uma unidade de disco inteira, sempre com o recurso de estabelecer senhas e permissões de acesso.

A sofisticação dos recursos de segurança variam de acordo com o sistema operacional utilizado. No Windows 98 as únicas formas de segurança são pastas ocultas e senhas. Usando um servidor Windows NT, 2000 ou Linux você terá à disposição configurações muito mais complexas, como grupos de usuários ou de domínios, vários níveis de acesso, etc., mas em compensação terá em mãos um sistema muito mais difícil de configurar. Ao longo deste livro iremos analisar os pontos fortes e fracos dos principais sistemas de rede.


A Internet nada mais é do que uma rede em escala mundial. Se por exemplo você abrir o ícone "redes" no painel de controle, instalar o "compartilhamento de arquivos e impressoras para redes Microsoft" e compartilhar suas unidades de disco, sem estabelecer uma senha de acesso, qualquer um que saiba localizar seu micro enquanto estiver conectado, terá acesso irrestrito a todos os seus arquivos, já que eles estão compartilhados com a rede (no caso a Internet inteira).

Compartilhando periféricos

Da mesma maneira que compartilhamos arquivos, podemos também compartilhar periféricos, permitindo a qualquer micro da rede imprimir na impressora ligada ao micro 2, ler um CD que está no drive do micro 4, ou mesmo compartilhar a mesma conexão à Internet estabelecida através do modem instalado no micro 7.

Como no caso dos arquivos, é possível estabelecer senhas e permissões de acesso para evitar, por exemplo, que a Maria do micro 5 use a impressora Laser para imprimir seus rascunhos, ao invés de usar a matricial.

Sistema de mensagens e agenda de grupo

Um sistema que permita enviar mensagens a outros usuários da rede, pode parecer inútil numa pequena rede, mas numa empresa com várias centenas de micros, divididos entre vários andares de um prédio, ou mesmo entre cidades ou países diferentes, pode ser muito útil para melhorar a comunicação entre os funcionários. Além de texto (que afinal de contas pode ser transmitido através de um e-mail comum) é possível montar um sistema de comunicação viva voz, ou mesmo de vídeo conferência, economizando o dinheiro que seria gasto com chamadas telefônicas.

Estas chamadas podem ser feitas tanto dentro da rede interna da empresa, quanto a outras filiais, localizadas em outras cidades ou mesmo outros países, via Internet. Este é um recurso em moda atualmente, o famoso voz sobre IP, que vem atraindo a atenção até mesmo da empresas de telefonia, pois torna as chamadas muito mais baratas do que são através do sistema comutado atual.

Via Internet, uma chamada para o Japão não custaria mais do que uma chamada local comum, muito pouco. O maior problema é estabelecer links rápidos o suficiente para manter uma boa qualidade.

Outro recurso útil seria uma agenda de grupo, um programa que mantém a agenda de todos ou

usuários e pode cruzar os dados sempre que preciso; descobrindo por exemplo um horário em que todos estejam livres para que uma reunião seja marcada.

Jogos em Rede

Mais um recurso que vem sendo cada vez mais utilizado, são os jogos multiplayer como Quake 3 e Diablo II que podem ser jogados através da rede. A maior vantagem neste caso, é que a comunicação permitida pela rede é muito mais rápida que uma ligação via modem, evitando o famoso LAG, ou lentidão, que tanto atrapalha quando jogamos os mesmos jogos via Internet.

Em geral, depois de configurada a rede, a configuração dentro do jogo é bastante simples, basta verificar quais protocolos de rede são suportados. Atualmente, a maioria dos jogos suporta multiplayer via TCP/IP. Não apenas os jogos, mas vários outros recursos, como o compartilhamento de conexão só funcionarão com este protocolo. Apenas alguns jogos antigos, como o Warcraft II exigem IPX/SPX, ou mesmo o uso de um cabo serial.

No Diablo II por exemplo, basta acessar a opção Multiplayer Game. Configure o PC mais rápido como host, ou seja, quem irá sediar o jogo e permitir a conexão dos outros PCs. Nos demais, basta escolher a opção de conectar-se ao host e fornecer seu (do host) endereço IP, configurado nas propriedades da conexão de rede, como por exemplo 192.168.0.1

Compartilhando a conexão com a Internet

Este é provavelmente o uso mais comum para as redes hoje em dia. Antigamente se falava em uma proporção de 80/20 entre os dados que trafegam entre os micros da rede local e os dados que vão para a Internet. Hoje em dia esta proporção é muito diferente, a maior parte dos dados vai para a Internet.

Muita gente trabalha apenas usando o navegador e o cliente de e-mails e cada vez mais as redes das empresas estão se integrando à Web para permitir que clientes e os próprios funcionários tenham acesso às informações em qualquer lugar.

Hoje em dia é muito simples compartilhar a conexão com a Internet e veremos ao longo do livro tanto como compartilhar a conexão a partir de um servidor Windows quanto a partir de um servidor linux. Afinal, pra quê ter um modem e uma linha telefônica para cada micro se você pode ter uma conexão de alta velocidade compartilhada entre todos a um custo muito mais baixo?

Terminais leves

Este é mais uma possibilidade interessante. Por que sofrer com a lentidão dos 486, ou gastar rios de dinheiro para substituí-los por micros novos se você pode interliga-los a um micro mais rápido e rodar os aplicativos a partir do servidor, apenas direcionando a saída de tela para os terminais 486? Com um Pentium III ou Duron como servidor você terá potência de sobra para 10 ou até mesmo 20 terminais. Veremos como colocar esta idéia em prática no final do livro.

Como as redes funcionam

Genericamente falando, existem dois tipos de rede, chamadas LAN e WAN. A diferença é que enquanto uma LAN (local area network, ou rede local) é uma rede que une os micros de um escritório, prédio, ou mesmo um conjunto de prédios próximos, usando cabos ou ondas de rádio, uma WAN (wide area network, ou rede de longa distância) interliga micros situados em cidades, países ou mesmo continentes diferentes, usando links de fibra óptica, microondas ou mesmo satélites. Geralmente uma WAN é formada por várias LANs interligadas: as várias filiais de uma grande empresa por exemplo.

Placas de Rede

O primeiro componente de uma rede é justamente a placa de rede. Além de funcionar como um meio de comunicação, a placa de rede desempenha várias funções essenciais, como a verificação da integridade dos dados recebidos e a correção de erros. A placa de rede deverá ser escolhida de acordo com a arquitetura de rede escolhida (Ethernet ou Token Ring) e também de acordo com o tipo de cabo que será usado.

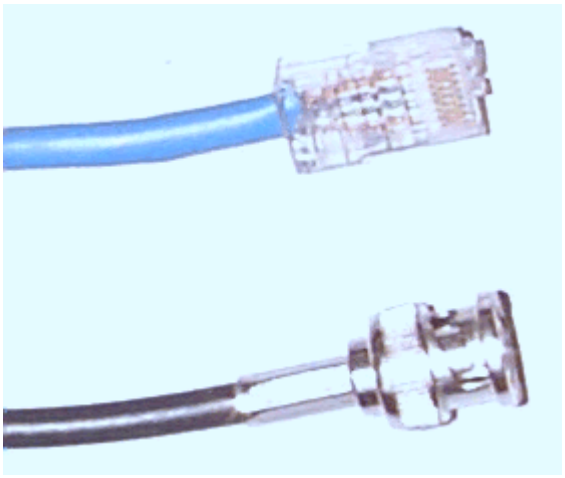
Atualmente, as placas mais comuns são as placas Ethernet 10/100, que utilizam cabos de par trançado e vem em versão PCI:


Placa de rede Fast Ethernet (cortesia da 3com)

Cabos

Para haver comunicação entre as placas de rede é necessário algum meio físico de comunicação. Apesar dos cabos de cobre serem de longe os mais utilizados, podemos também usar fibra óptica ou mesmo ondas de rádio. Em matéria de cabos, os mais utilizados são os cabos de par trançado, cabos coaxiais e cabos de fibra óptica. Cada categoria tem suas próprias vantagens e limitações, sendo mais adequado para um tipo específico de rede. Os cabos coaxiais permitem que os dados sejam transmitidos através de uma distância maior que a permitida pelos cabos de par trançado sem blindagem (UTP), mas por outro, lado não são tão flexíveis e são mais caros que eles. Os cabos de fibra óptica permitem transmissões de dados a velocidades muito maiores e são completamente imunes a qualquer tipo de interferência eletromagnética, porém, são muito mais caros e difíceis de instalar, demandando equipamentos mais caros e mão de obra mais especializada. Apesar da alta velocidade de transferência, as fibras ainda não são uma boa opção

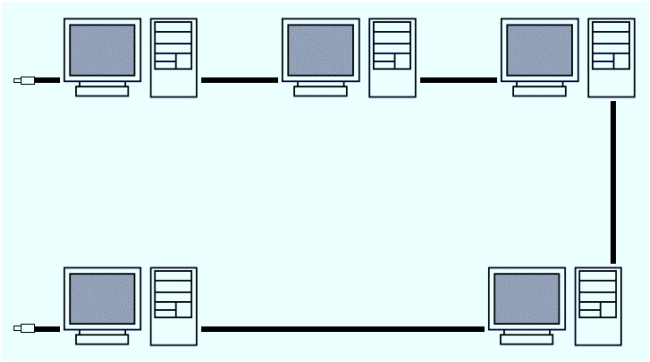
para pequenas redes devido ao custo.

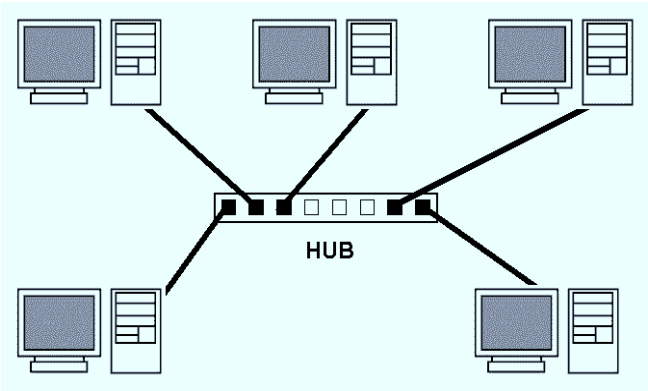

Cabo de par trançado e cabo coaxial

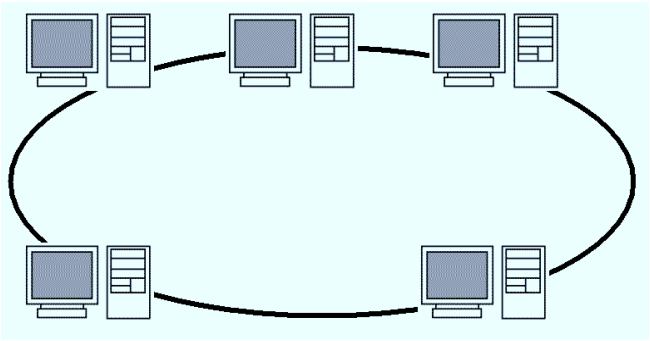
Topologias

Temos em seguida, a topologia da rede, ou seja, de que forma os micros são interligados. Como quase tudo em computação, temos aqui uma divisão entre topologias físicas e topologias lógicas. A topologia física é a maneira como os cabos conectam **fisicamente** os micros. A topologia lógica, por sua vez, é a maneira como os sinais trafegam através dos cabos e placas de rede. As redes Ethernet, por exemplo, usam uma topologia lógica de barramento, mas podem usar topologias físicas de estrela ou de barramento. As redes Token Ring, por sua vez, usam uma topologia lógica de anel, mas usam topologia física de estrela. Não se preocupe pois vamos ver tudo com detalhes mais adiante :-)

Temos três tipos de topologia física, conhecidas como topologia de barramento, de estrela e de anel. A topologia de barramento é a mais simples das três, pois nela um PC é ligado ao outro, usando cabos coaxiais. Na topologia de estrela, os micros não são ligados entre sí, mas sim a um hub, usando cabos de par trançado. O Hub permite que todos os micros conectados se vejam mutuamente. Finalmente temos a topologia de anel, onde apenas um cabo passa por todos os micros e volta ao primeiro, formando um anel fechado. A topologia de anel físico é praticamente apenas uma teoria, pois seria complicado e problemático demais montar uma rede deste tipo na prática. Sempre que ouvir falar em uma rede com topologia de anel, pode ter certeza que na verdade se trata de uma rede Token Ring, que usa uma topologia de anel lógico, mas que ao mesmo tempo usa topologia física de estrela.







Topologias físicas de barramento (acima à esquerda), de estrela (acima) e de anel (ao lado).

Arquiteturas

Ethernet, Token Ring e Arcnet são três arquiteturas de rede diferentes, que exigem placas de rede diferentes, e possuem exigências diferentes a nível de cabeamento, que iremos examinar mais adiante.

Uma arquitetura de rede define como os sinais irão trafegar através da rede. Todo o trabalho é feito de maneira transparente pela placa de rede, que funciona de maneira diferente de acordo com a arquitetura para a qual tenha sido construída.

Por isso, existem tanto placas de rede padrão Ethernet, quanto padrão Token Ring e Arcnet. Uma vez que decida qual arquitetura de rede irá utilizar, você terá que usar apenas placas compatíveis com a arquitetura: 30 placas Ethernet para os 30 micros da rede, por exemplo.

Claro que atualmente as redes Ethernet são de longe as mais usadas, mas nem por isso vamos deixar de conhecer as opções.

Protocolos

Cabos e placas de rede servem para estabelecer uma ligação física entre os micros, a fim de permitir a transmissão de dados. Os protocolos, por sua vez, constituem um conjunto de padrões usados para permitir que os micros “falem a mesma língua” e possam se entender. Os protocolos

mais usados atualmente são o TPC/IP (protocolo padrão na Internet), NetBEUI e IPX/SPX.

Podemos fazer uma analogia com o sistema telefônico: veja que as linhas, centrais, aparelhos, etc. servem para criar uma ligação que permite a transmissão de voz. Mas, para que duas pessoas possam se comunicar usando o telefone, existem vários padrões. Por exemplo, para falar com um amigo você discará seu número, ele atenderá e dirá "alô" para mostrar que está na linha. Vocês se comunicarão usando a língua Portuguesa, que também é um conjunto de códigos e convenções e, finalmente, quando quiser terminar a conversa, você irá despedir-se e desligar o telefone.

Os protocolos de rede têm a mesma função: permitir que um pacote de dados realmente chegue ao micro destino, e que os dados sejam inteligíveis para ele. Para existir comunicação, é preciso que todos os micros da rede utilizem o mesmo protocolo (você nunca conseguiria comunicar-se com alguém que falasse Chinês, caso conhecesse apenas o Português, por exemplo).

É possível instalar vários protocolos no mesmo micro, para que ele torne-se um "poliglota" e possa se entender com micros usuários de vários protocolos diferentes. Se você usa o protocolo NetBEUI em sua rede, mas precisa que um dos micros acesse a Internet (onde e utilizado o protocolo TCP/IP), basta instalar nele os dois protocolos. Assim ele usará o TCP/IP para acessar a Internet e o NetBEUI para comunicar-se com os outros micros da rede. Dentro do Windows 98, você pode instalar e desinstalar protocolos através do ícone "redes" no painel de controle.

Existe apenas um pequeno problema em usar vários periféricos no mesmo micro que é uma pequena perda de desempenho, já que ele terá de lidar com mais solicitações simultâneas, por isso é recomendável manter instalados apenas os protocolos que forem ser usados. De qualquer forma, conforme os PCs vem tornando-se mais rápidos, esta queda vem tornando-se cada vez menos perceptível.

Recursos

Tudo que é compartilhado através da rede, seja um arquivo, um CD-ROM, disco rígido ou impressora, é chamado de recurso. O micro que disponibiliza o recurso é chamado de servidor ou host, enquanto os micros que usam tal recurso são chamados de clientes, ou guests. Talvez o tipo mais conhecido (e mais obsoleto) de rede cliente-servidor, sejam as antigas redes baseadas em mainframes e terminais burros, onde todo o processamento era feito no servidor, enquanto os terminais funcionavam apenas como interfaces de entrada e saída de dados.

Num conceito mais moderno, existem vários tipos de servidores: servidores de disco (que disponibilizam seu disco rígido para ser usado por estações sem disco rígido, mas com poder de processamento), servidores de arquivos (que centralizam e disponibilizam arquivos que podem ser acessados por outros micros da rede), servidores de fax (que cuidam da emissão e recepção de faxes através da rede), servidores de impressão (que disponibilizam uma impressora) e assim por diante. Dependendo do seu poder de processamento e de como estiver configurado, um único micro pode acumular várias funções, servindo arquivos e impressoras ao mesmo tempo, por exemplo.

Existem também servidores dedicados e servidores não-dedicados. A diferença é que enquanto um servidor dedicado é um micro reservado, um servidor não dedicado é um micro qualquer, que é usado normalmente, mas que ao mesmo tempo disponibiliza algum recurso. Se você tem 5 micros

numa rede, todos são usados por alguém, mas um deles compartilha uma impressora e outro disponibiliza arquivos, temos dois servidores não dedicados, respectivamente de impressão e de arquivos.

Outro vocábulo bastante usado no ambiente de redes é o termo "estação de trabalho". Qualquer micro conectado à rede, e que tenha acesso aos recursos compartilhados por outros micros da rede, recebe o nome de estação de trabalho. Você também ouvirá muito o termo "nó de rede". Um nó é qualquer aparelho conectado à rede, seja um micro, uma impressora de rede, um servidor ou qualquer outra coisa que tenha um endereço na rede.

N.O.S.

Finalmente chegamos ao último componente da rede, o NOS, ou "Network Operational System". Qualquer sistema operacional que possa ser usado numa rede, ou seja, que ofereça suporte à redes pode ser chamado de NOS. Temos nesta lista o Windows 3.11 for Workgroups, o Windows 95/98, Windows NT, Windows 2000, Novell Netware, Linux, Solaris, entre vários outros. Cada sistema possui seus próprios recursos e limitações, sendo mais adequado para um tipo específico de rede.

Hoje em dia, os sistemas mais usados como servidores domésticos ou em pequenas empresas são o Windows 2000 Server (ou NT Server) e o Linux, que vem ganhando espaço. O mais interessante é que é possível misturar PCs rodando os dois sistemas na mesma rede, usando o Samba, um software que acompanha a maior parte das distribuições do Linux que permite que tanto uma máquina Linux acesse impressoras ou arquivos de um servidor Windows, quanto que um servidor Linux substitua um servidor Windows, disponibilizando arquivos e impressoras para clientes rodando Windows.

O Samba não é tão fácil de configurar quanto os compartilhamentos e permissões de acesso do Windows, mas em termos de funcionalidade e desempenho não deixa nada a desejar. Você pode encontrar maiores informações sobre ele no http://www.samba.org/

Cabeamento

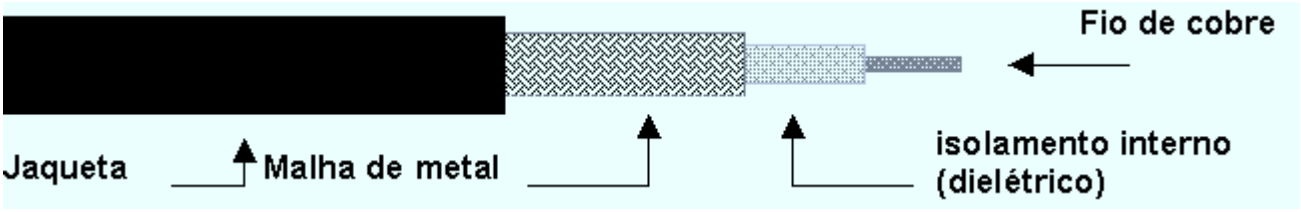
Até agora tivemos apenas uma visão geral sobre os componentes e funcionamento das redes. Vamos agora estudar tudo com mais detalhes, começando com os sistemas de cabeamento que você pode utilizar em sua rede.

Como já vimos, existem três tipos diferentes de cabos de rede: os cabos coaxiais, cabos de par trançado e os cabos de fibra óptica.

Cabo coaxial

Os cabos coaxiais são cabos constituídos de 4 camadas: um condutor interno, o fio de cobre que

transmite os dados; uma camada isolante de plástico, chamada de dielétrico que envolve o cabo interno; uma malha de metal que protege as duas camadas internas e, finalmente, uma nova camada de revestimento, chamada de jaqueta.

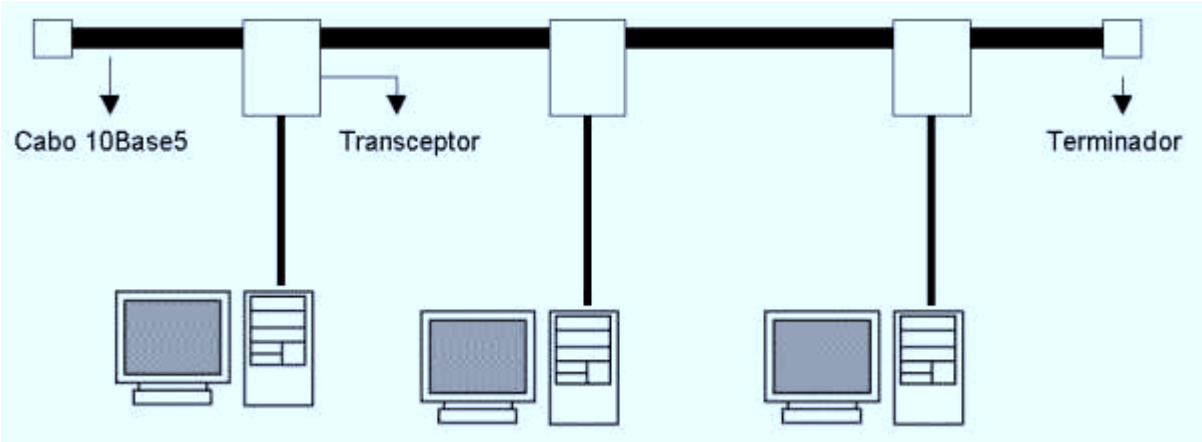


Se você envolver um fio condutor com uma segunda camada de material condutor, a camada externa protegerá a primeira da interferência externa. Devido a esta blindagem, os cabos coaxiais (apesar de ligeiramente mais caros que os de par trançado) podem transmitir dados a distâncias maiores, sem que haja degradação do sinal. Existem 4 tipos diferentes de cabos coaxiais, chamados de 10Base5, 10Base2, RG-59/U e RG-62/U

O cabo **10Base5** é um tipo mais antigo, usado geralmente em redes baseadas em mainframes. Esta cabo é muito grosso, tem cerca de 0.4 polegadas, ou quase 1 cm de diâmetro e por isso é muito caro e difícil de instalar devido à baixa flexibilidade. Outro tipo de cabo coaxial pouco usado atualmente é o **RG62/U**, usado em redes Arcnet. Temos também o cabo **RG-59/U**, usado na fiação de antenas de TV.

Além da baixa flexibilidade e alto custo, os cabos 10Base5 exigem uma topologia de rede bem mais cara e complicada. Temos o cabo coaxial 10base5 numa posição central, como um backbone, sendo as estações conectadas usando um segundo dispositivo, chamado transceptor, que atua como um meio de ligação entre elas e o cabo principal.

Os transceptores perfuram o cabo 10Base5, alcançando o cabo central que transmite os dados, sendo por isso também chamados de "derivadores vampiros". Os transceptores são conectados aos encaixes AUI das placas de rede (um tipo de encaixe parecido com a porta de joystick da placa de som, encontrado principalmente em placas antigas) através de um cabo mais fino, chamado cabo transceptor. Além de antiquada, esta arquitetura é muito cara, tanto a nível de cabos e equipamentos, quanto em termos de mão de obra.



Os cabos 10Base5 foram praticamente os únicos utilizados em redes de mainframes no inicio da

década de 80, mas sua popularidade foi diminuindo com o passar do tempo por motivos óbvios.

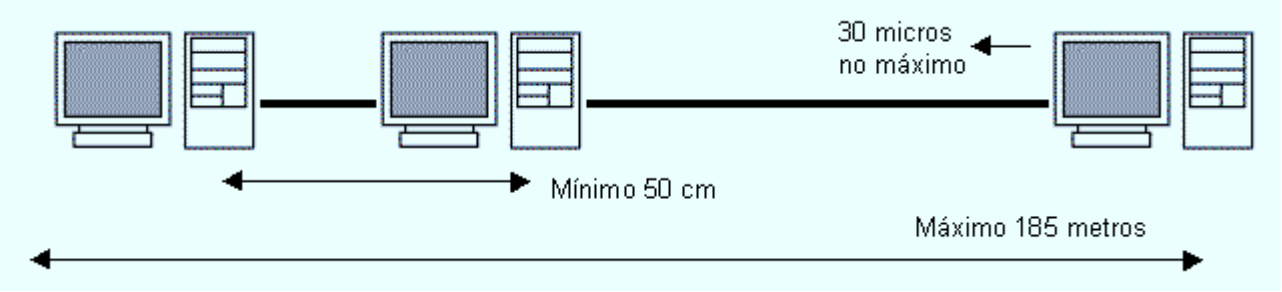
Atualmente você só se deparará com este tipo de cabo em instalações bem antigas ou, quem sabe, em museus ;-)

Finalmente, os cabos **10Base2**, também chamados de cabos coaxiais finos, ou cabos Thinnet, são os cabos coaxiais usados atualmente em redes Ethernet, e por isso, são os cabos que você receberá quando pedir por "cabos coaxiais de rede". Seu diâmetro é de apenas 0.18 polegadas, cerca de 4.7 milímetros, o que os torna razoavelmente flexíveis.

Os cabos 10Base2 são bem parecidos com os cabos usados em instalações de antenas de TV, a diferença é que, enquanto os cabos RG-59/U usados nas fiações de antena possuem impedância de 75 ohms, os cabos 10Base2 possuem impedância de apenas 50 ohms. Por isso, apesar dos cabos serem parecidos, nunca tente usar cabos de antena em redes de micros. É fácil diferenciar os dois tipos de cabo, pois os de redes são pretos enquanto os para antenas são brancos.

O "10" na sigla 10Base2, significa que os cabos podem transmitir dados a uma velocidade de até 10 megabits por segundo, "Base" significa "banda base" e se refere à distância máxima para que o sinal pode percorrer através do cabo, no caso o "2" que teoricamente significaria 200 metros, mas que na prática é apenas um arredondamento, pois nos cabos 10Base2 a distância máxima utilizável é de 185 metros.

Usando cabos 10Base2, o comprimento do cabo que liga um micro ao outro deve ser de no mínimo 50 centímetros, e o comprimento total do cabo (do primeiro ao último micro) não pode superar os 185 metros. É permitido ligar até 30 micros no mesmo cabo, pois acima disso, o grande número de colisões de pacotes irá prejudicar o desempenho da rede, chegando ao ponto de praticamente impedir a comunicação entre os micros em casos extremos.

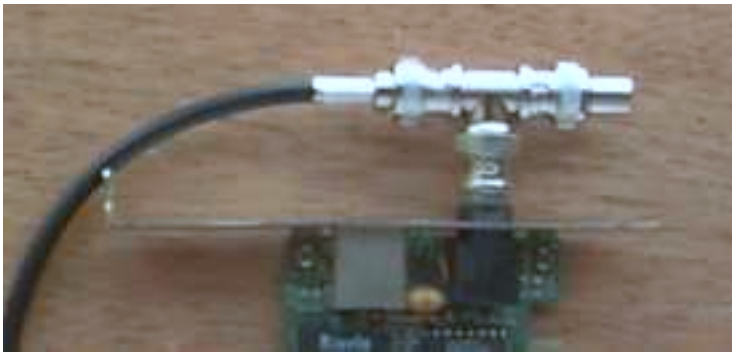


Conectamos o cabo coaxial fino à placa de rede usando conectores BCN, que por sua vez são ligados a conectores T ligados na placa de rede. Usando cabos coaxiais os micros são ligados uns aos outros, com um cabo em cada ponta do conector T.


Conector BCN desmontado


Conector T na placa de rede

São necessários dois terminadores para fechar o circuito. Os terminadores são encaixados diretamente nos conectores T do primeiro e último micro da rede. Pelo menos um dos terminadores, deverá ser aterrado.


Terminador

Se você não instalar um terminador em cada ponta da rede, quando os sinais chegarem às pontas do cabo, retornarão, embora um pouco mais fracos, formando os chamados pacotes sombra. Estes pacotes atrapalham o tráfego e corrompem pacotes bons que estejam trafegando, praticamente inutilizando a rede.

Em redes Ethernet os terminadores devem ter impedância de 50 ohms (a mesma dos cabos), valor que geralmente vem estampado na ponta do terminador.

Para prender o cabo ao conector BCN, precisamos de duas ferramentas: um descascador de cabo

coaxial e um alicate de crimpagem. O descascador serve para retirar o dielétrico do cabo, deixando exposto o fio de cobre (você pode fazer este trabalho com algum outro instrumento cortante, como um estilete, mas usando o descascador o resultado será bem melhor). O alicate para crimpagem serve para prender o cabo ao conector, impedindo que ele se solte facilmente. O alicate de crimpagem possuirá sempre pelo menos dois orifícios, o menor, com cerca de 1 mm de diâmetro serve para prender o pino central do conector BCN ao fio central do cabo. A maior serve para prender o anel de metal.

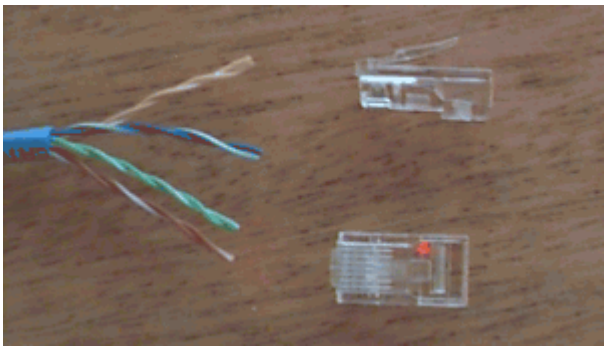
Para crimpar os cabos coaxiais é indispensável ter o alicate de crimpagem. Não dá para fazer o serviço com um alicate comum pois ele não oferece pressão suficiente. Um alicate de crimpagem de cabos coaxiais custa à partir de 45 reais; entretanto, a maioria das lojas que vendem cabos também os crimpam de acordo com a necessidade do cliente.

Descascador de cabos coaxiais (à esquerda) e alicate de crimpagem.

Cabo de par trançado

Os cabos de par trançados vem substituindo os cabos coaxiais desde o início da década de 90. Hoje em dia é muito raro alguém ainda utilizar cabos coaxiais em novas instalações de rede, o mais comum é apenas reparar ou expandir redes que já existem. Mais adiante teremos um comparativo entre os dois tipos de cabos.

O nome “par trançado” é muito conveniente, pois estes cabos são constituídos justamente por 4 pares de cabos entrelaçados. Veja que os cabos coaxiais usam uma malha de metal que protege o cabo de dados contra interferências externas; os cabos de par trançado por sua vez, usam um tipo de proteção mais sutil: o entrelaçamento dos cabos cria um campo eletromagnético que oferece uma razoável proteção contra interferências externas.


Cabo de par Trançado

Além dos cabos sem blindagem (como o da foto) conhecidos como **UTP** (Unshielded Twisted Pair), existem os cabos blindados conhecidos como **STP** (Shielded Twisted Pair). A única diferença entre eles é que os cabos blindados além de contarem com a proteção do entrelaçamento dos fios, possuem uma blindagem externa (assim como os cabos coaxiais), sendo mais adequados a ambientes com fortes fontes de interferências, como grandes motores elétricos e estações de rádio que estejam muito próximas. Outras fontes menores de interferências são as lâmpadas fluorescentes (principalmente lâmpadas cansadas que ficam piscando), cabos elétricos quando colocados lado a lado com os cabos de rede e mesmo telefones celulares muito próximos dos cabos.

Quanto maior for o nível de interferência, menor será o desempenho da rede, menor será a distância que poderá ser usada entre os micros e mais vantajosa será a instalação de cabos blindados. Em ambientes normais porém os cabos sem blindagem costumam funcionar bem.

Existem no total, 5 categorias de cabos de par trançado. Em todas as categorias a distância máxima permitida é de 100 metros. O que muda é a taxa máxima de transferência de dados e o nível de imunidade a interferências .

Categoria 1: Este tipo de cabo foi muito usado em instalações telefônicas antigas, porem não é mais utilizado.

Categoria 2: Outro tipo de cabo obsoleto. Permite transmissão de dados a até 4 mbps.

Categoria 3: Era o cabo de par trançado sem blindagem usado em redes até alguns anos atrás. Pode se estender por até 100 metros e permite transmissão de dados a até 10 Mbps. A diferença do cabo de categoria 3 para os obsoletos cabos de categoria 1 e 2 é o numero de tranças. Enquanto nos cabos 1 e 2 não existe um padrão definido, os cabos de categoria 3 (assim como os de categoria 4 e 5) possuem atualmente de 24 a 45 tranças por metro, sendo muito mais resistente a ruídos externos. Cada par de cabos tem um número diferente de tranças por metro, o que atenua as interferências entre os cabos. Praticamente não existe a possibilidade de dois pares de cabos terem exatamente a mesma disposição de tranças.

Categoria 4: Por serem blindados, estes cabos já permitem transferências de dados a até 16 mbps, e são o requisito mínimo para redes Token Ring de 16 mbps, podendo ser usados também em redes Ethernet de 10 mbps no lugar dos cabos sem blindagem.

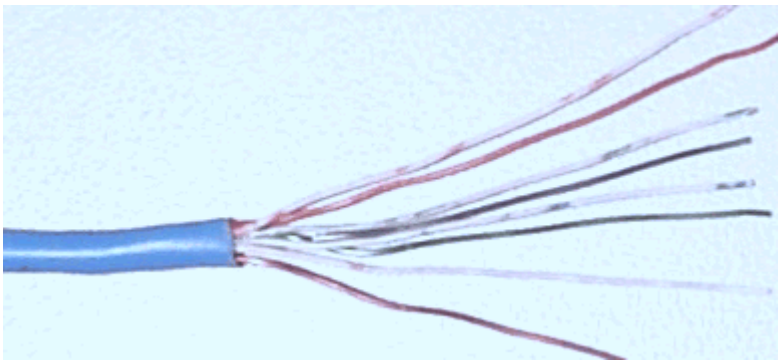
Categoria 5: Este é o tipo de cabo de par trançado usado atualmente, que existe tanto em versão blindada quanto em versão sem blindagem, a mais comum. A grande vantagem sobre esta categoria de cabo sobre as anteriores é a taxa de transferência, até 100 mbps.

Os cabos de categoria 5 são praticamente os únicos que ainda podem ser encontrados à venda, mas em caso de dúvida basta checas as inscrições decalcadas no cabo, entre elas está a categoria do cabo, como na foto abaixo:

"Category 5e"

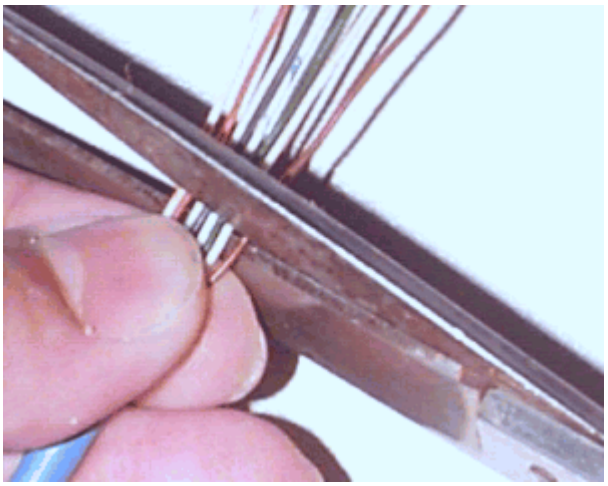
Independentemente da categoria, todos os cabos de par trançado usam o mesmo conector, chamado RJ-45. Este conector é parecido com os conectores de cabos telefônicos, mas é bem maior por acomodar mais fios. Uma ponta do cabo é ligada na placa de rede e a outra no hub.

Para crimpar o cabo, ou seja, para prender o cabo ao conector, usamos um alicate de crimpagem. Após retirar a capa protetora, você precisará tirar as tranças dos cabos e em seguida "arruma-los" na ordem correta para o tipo de cabo que estiver construindo (veremos logo adiante)

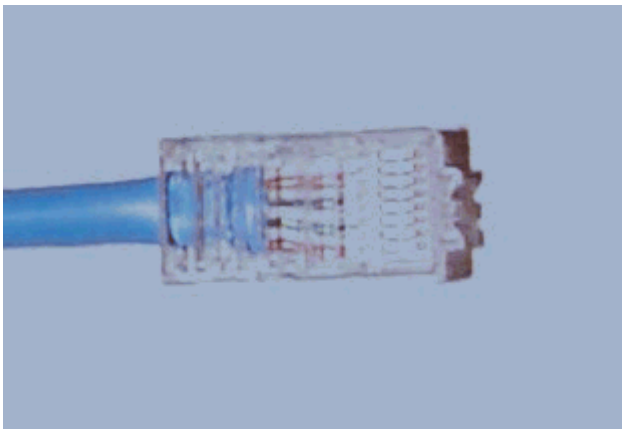


Veja que o que protege os cabos contra as interferências externas é são justamente as tranças. A parte destrançada que entra no conector é o ponto fraco do cabo, onde ele é mail vulnerável a todo tipo de interferência. Por isso, é recomendável deixar um espaço menor possível sem as tranças, se possível menos de 2,5 centímetros.

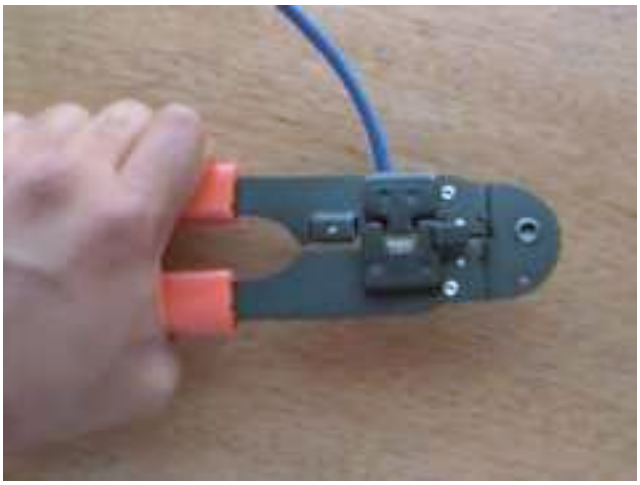
Para isso, uma sugestão é que você destrance um pedaço suficiente do fio, para ordena-los confortavelmente e depois corte o excesso, deixando apenas os 2 centímetros que entrarão dentro do conector:



Finalmente, basta colocar os fios dentro do conector e pressiona-lo usando um alicate de crimpagem.



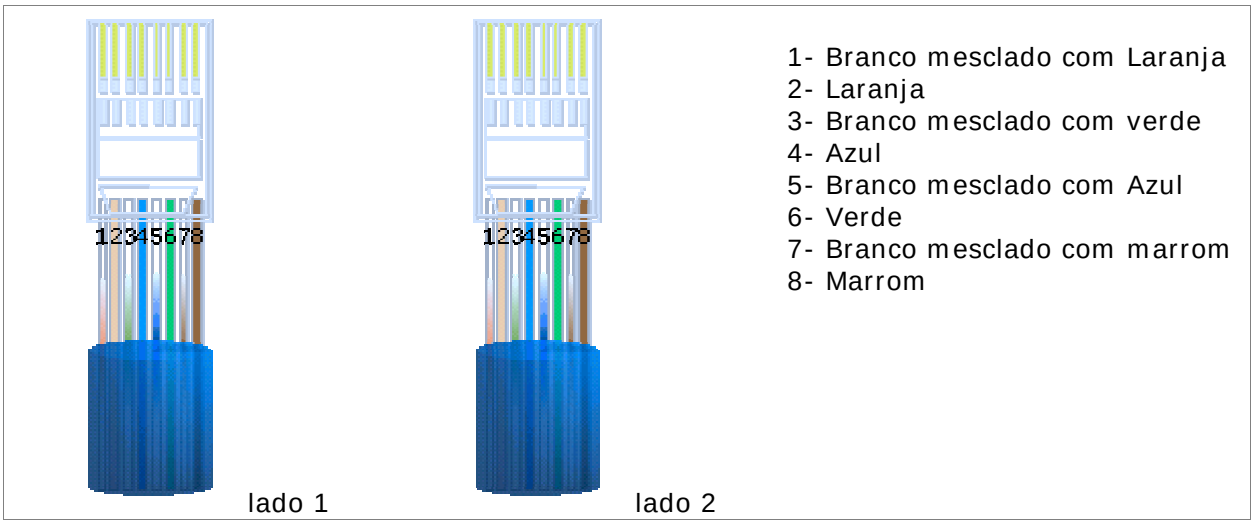
A função do alicate é fornecer pressão suficiente para que os pinos do conector RJ-45, que internamente possuem a forma de lâminas, esmaguem os fios do cabo, alcançando o fio de cobre e criando o contato. Você deve retirar apenas a capa externa do cabo e não descascar individualmente os fios, pois isto ao invés de ajudar, serviria apenas para causar mau contato, deixado o encaixe com os pinos do conector “frouxo”.



Os alicates para crimpar cabos de par trançado são um pouco mais baratos que os usados para crimpar cabos coaxiais. Os alicates mais simples custam a partir de 40 reais, mas os bons alicates custam bem mais. Existem alguns modelos de alicates feitos de plástico, com apenas as pontas de metal. Estes custam bem menos, na faixa de 15 reais, mas são muito ruins, pois quebram muito facilmente e não oferecem a pressão adequada. Como no caso dos coaxiais, existe também a opção de comprar os cabos já crimpados, o ideal caso você não pretenda montar apenas sua rede doméstica ou da empresa, e não trabalhar profissionalmente com redes.

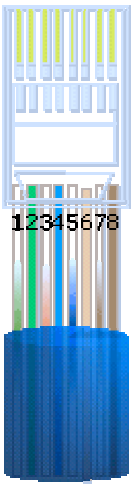
Um problema óbvio em trabalhar com cabos já crimpados é que será quase impossível passa-los através das paredes, como seria possível fazer com cabos ainda sem os conectores.

Existe uma posição certa para os cabos dentro do conector. Note que cada um dos fios do cabo possui uma cor diferente. Metade tem uma cor sólida enquanto a outra metade tem uma cor mesclada com branco. Para criar um cabo destinado a conectar os micros ao hub, a seqüência tanto no conector do micro quanto no conector do hub será o seguinte:



É possível também criar um cabo para ligar diretamente dois micros, sem usar um hub, chamado de cabo cross-over. Logicamente este cabo só poderá ser usado caso a sua rede tenha apenas dois

micros. Neste tipo de cabo a posição dos fios é diferente nos dois conectores, de um dos lados a pinagem é a mesma de um cabo de rede normal, enquanto no outro a posição dos pares verde e laranja são trocados. Daí vem o nome cross-over, que significa, literalmente, cruzado na ponta:

 lado 1	Conector da esquerda: 1- Branco com Laranja 2- Laranja 3- Branco com Verde 4- Azul 5- Branco com Azul 6- Verde 7- Branco com Marrom 8- Marrom	 lado 2	Conector da direita: 1- Branco com Verde 2- Verde 3- Branco com Laranja 4- Azul 5- Branco com Azul 6- Laranja 7- Branco com Marrom 8- Marrom

Existe um teste simples para saber se o cabo foi crimpado corretamente: basta conectar o cabo à placa de rede do micro e ao hub. Tanto o LED da placa quanto o do hub deverão acender. Naturalmente, tanto o micro quanto o hub deverão estar ligados.

Existem também aparelhos testadores de cabos, que oferecem um diagnóstico muito mais sofisticado, dizendo por exemplo se os cabos são adequados para transmissões a 10 ou a 100 megabits. Estes aparelhos serão bastante úteis caso você vá crimpar muitos cabos, mas são dispensáveis para trabalhos esporádicos. Custam apartir de 100 dólares.

Os cabos de rede são um artigo bem barato, que representam apenas uma pequena porcentagem do custo total da rede. Os cabos de par trançado podem ser comprados por até 60 centavos o metro, e centavos de real, não de dólar, enquanto os conectores custam 50 ou 60 centavos cada. O único artigo relativamente caro é o alicate de crimpagem.

Par trançado x Coaxial

Disse anteriormente que cada uma destas categorias de cabos possui algumas vantagens e desvantagens. Na verdade, o coaxial possui bem mais desvantagens do que vantagens em relação aos cabos de par trançado, o que explica o fato dos cabos coaxiais virem tornando-se cada vez mais raros. Numa comparação direta entre os dois tipos de cabos teremos:

Distância máxima: o cabo coaxial permite uma distância máxima entre os pontos de até 185 metros, enquanto os cabos de par trançado permitem apenas 100 metros.

Resistência a interferências: Os cabos de par trançado sem blindagem são muito mais sensíveis à interferências do que os cabos coaxiais, mas os cabos blindados por sua vez

apresentam uma resistência equivalente ou até superior.

Mau contato: Usando cabo coaxial, a tendência a ter problemas na rede é muito maior, pois este tipo de cabo costuma ser mais suscetível a mau contato do que os cabos de par trançado. Outra desvantagem é que usando o coaxial, quando temos problemas de mau contato no conector de uma das estações, a rede toda cai, pois as duas "metades" não contam com terminadores nas duas extremidades. Para complicar, você terá que checar PC por PC até encontrar o conector com problemas, imagine fazer isso numa rede com 20 micros...

Usando par trançado, por outro lado, apenas o micro problemático ficaria isolado da rede, pois todos os PCs estão ligados ao hub e não uns aos outros. Este já é uma argumento forte o suficiente para explicar a predominância das redes com cabo de par trançado.

Custo: Os cabos coaxiais são mais caros que os cabos de par trançado sem blindagem, mas normalmente são mais baratos que os cabos blindado. Por outro lado, usando cabos coaxiais você não precisará de um hub. Atualmente já existem hubs de 8 portas por menos de 100 reais, não é mais um artigo caro como no passado.

Velocidade máxima: Se você pretende montar uma rede que permita o tráfego de dados a 100 mbps, então a única opção é usar cabos de par trançado categoria 5, pois os cabos coaxiais são limitados apenas 10 mbps. Atualmente é complicado até mesmo encontrar placas de rede com conectores para cabo coaxial, pois apenas as placas antigas, ISA de 10 megabits possuem os dois tipos de conector. As placas PCI 10/100 possuem apenas o conector para cabo de par trançado.

Fibra óptica

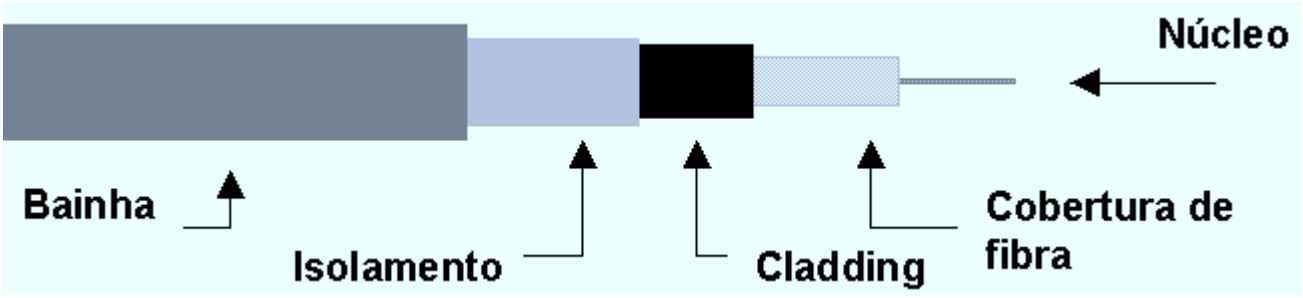
Ao contrário dos cabos coaxiais e de par trançado, que nada mais são do que fios de cobre que transportam sinais elétricos, a fibra óptica transmite luz e por isso é totalmente imune a qualquer tipo de interferência eletromagnética. Além disso, como os cabos são feitos de plástico e fibra de vidro (ao invés de metal), são resistentes à corrosão.

A distância permitida pela fibra também é bem maior: os cabos usados em redes permitem segmentos de até 1 KM, enquanto alguns tipos de cabos especiais podem conservar o sinal por até 5 KM (distâncias maiores são obtidas usando repetidores). Mesmo permitindo distâncias tão grandes, os cabos de fibra óptica permitem taxas de transferências de até 155 mbps, sendo especialmente úteis em ambientes que demandam uma grande transferência de dados. Como não soltam faíscas, os cabos de fibra óptica são mais seguros em ambientes onde existe perigo de incêndio ou explosões. E para completar, o sinal transmitido através dos cabos de fibra é mais difícil de interceptar, sendo os cabos mais seguros para transmissões sigilosas.

As desvantagens da fibra residem no alto custo tanto dos cabos quanto das placas de rede e instalação que é mais complicada e exige mais material. Por isso, normalmente usamos cabos de par trançado ou coaxiais para fazer a interligação local dos micros e um cabo de fibra óptica para servir como backbone, unindo duas ou mais redes ou mesmo unindo segmentos da mesma rede que estejam distantes.

O cabo de fibra óptica é formado por um núcleo extremamente fino de vidro, ou mesmo de um tipo especial de plástico. Uma nova cobertura de fibra de vidro, bem mais grossa envolve e

protege o núcleo. Em seguida temos uma camada de plástico protetor chamada de cladding, uma nova camada de isolamento e finalmente uma capa externa chamada bainha.



A luz a ser transmitida pelo cabo é gerada por um LED, ou diodo emissor de luz. Chegando ao destino, o sinal luminoso é decodificado em sinais digitais por um segundo circuito chamado de foto-diodo. O conjunto dos dois circuitos é chamado de CODEC, abreviação de codificador/decodificador.

Existem dois tipos de cabos de fibra óptica, chamados de cabos monomodo e multimodo, ou simplesmente de modo simples e modo múltiplo. Enquanto o cabo de modo simples transmite apenas um sinal de luz, os cabos multimodo contém vários sinais que se movem dentro do cabo. Ao contrário do que pode parecer à primeira vista, os cabos monomodo transmitem mais rápido do que os cabos multimodo, pois neles a luz viaja em linha reta, fazendo o caminho mais curto. Nos cabos multimodo o sinal viaja batendo continuamente mas paredes do cabo, tornando-se mais lento e perdendo a intensidade mais rapidamente.

Ao contrário do que costuma-se pensar, os cabos de fibra óptica são bastante flexíveis e podem ser passados dentro de conduítes, sem problemas. Onde um cabo coaxial entra, pode ter certeza que um cabo de fibra também vai entrar. Não é necessário em absoluto que os cabos fiquem em linha reta, e devido às camadas de proteção, os cabos de fibra também apresentam uma boa resistência mecânica.

A velocidade de 155 mbps que citei a pouco, assim como as distâncias máximas dos cabos de fibra, referem-se às tecnologias disponíveis para o uso em pequenas redes, cujas placas e demais componentes podem ser facilmente encontrados. Tecnologias mais caras e modernas podem atingir velocidades de transmissão na casa dos Terabits por segundo, atingindo distância de vários quilômetros. Aliás, a velocidade de transmissão nas fibras ópticas vem evoluindo bem mais rápido que os processadores, ou outros componentes, por isso é difícil encontrar material atualizado sobre as tecnologias mais recentes.

Placas de Rede

A placa de rede é o hardware que permite aos micros conversarem entre sí através da rede. Sua função é controlar todo o envio e recebimento de dados através da rede. Cada arquitetura de rede exige um tipo específico de placa de rede; você jamais poderá usar uma placa de rede Token Ring em uma rede Ethernet, pois ela simplesmente não conseguirá comunicar-se com as demais.

Além da arquitetura usada, as placas de rede à venda no mercado diferenciam-se também pela taxa de transmissão, cabos de rede suportados e barramento utilizado.

Quanto à taxa de transmissão, temos placas Ethernet de 10 mbps e 100 mbps e placas Token Ring de 4 mbps e 16 mbps. Como vimos na trecho anterior, devemos utilizar cabos adequados à velocidade da placa de rede. Usando placas Ethernet de 10 mbps por exemplo, devemos utilizar cabos de par trançado de categoria 3 ou 5, ou então cabos coaxiais. Usando uma placas de 100 mbps o requisito mínimo a nível de cabeamento são cabos de par trançado blindados nível 5.

No caso de redes Token Ring, os requisitos são cabos de par trançado categoria 2 (recomendável o uso de cabos categoria 3) para placas de rede de 4 Mbps, e cabos de par trançado blindado categoria 4 para placas de 16 mbps. Devido às exigência de uma topologia em estrela das redes Token Ring, nenhuma placa de rede Token Ring suporta o uso de cabos coaxiais.

Cabos diferentes exigem encaixes diferentes na placa de rede. O mais comum em placas Ethernet, é a existência de dois encaixes, uma para cabos de par trançado e outro para cabos coaxiais. Muitas placas mais antigas, também trazem encaixes para cabos coaxiais do tipo grosso (10Base5), conector com um encaixe bastante parecido com o conector para joysticks da placa de som.

Placas que trazem encaixes para mais de um tipo de cabo são chamadas placas combo. A existência de 2 ou 3 conectores serve apenas para assegurar a compatibilidade da placa com vários cabos de rede diferentes. Naturalmente, você só poderá utilizar um conector de cada vez.


Placa combo

As placas de rede que suportam cabos de fibra óptica, são uma exceção, pois possuem encaixes apenas para cabos de fibra. Estas placas também são bem mais caras, de 5 a 8 vezes mais do que as placas convencionais por causa do CODEC, o circuito que converte os impulsos elétricos recebidos em luz e vice-versa que ainda é extremamente caro.

Finalmente, as placas de rede diferenciam-se pelo barramento utilizado. Atualmente você encontrará no mercado placas de rede ISA e PCI usadas em computadores de mesa e placas PCMCIA, usadas em notebooks e handhelds. Existem também placas de rede USB que vem sendo cada vez mais utilizadas, apesar de ainda serem bastante raras devido ao preço salgado.

Naturalmente, caso seu PC possua slots PCI, é recomendável comprar placas de rede PCI pois além de praticamente todas as placas PCI suportarem transmissão de dados a 100 mbps (todas as placas de rede ISA estão limitadas a 10 mbps devido à baixa velocidade permitida por este barramento), você poderá usá-las por muito mais tempo, já que o barramento ISA vem sendo cada vez menos usado em placas mãe mais modernas e deve gradualmente desaparecer das

placas mãe novas.

A nível de recursos do sistema, todas as placas de rede são parecidas: precisam de um endereço de IRQ, um canal de DMA e um endereço de I/O. Bastando configurar os recursos corretamente.

O canal de IRQ é necessário para que a placa de rede possa chamar o processador quando tiver dados a entregar. O canal de DMA é usado para transferir os dados diretamente à memória, diminuindo a carga sobre o processador. Finalmente, o endereço de I/O informa ao sistema aonde estão as informações que devem ser movidas. Ao contrário dos endereços de IRQ e DMA que são escassos, existem muitos endereços de I/O e por isso a possibilidade de conflitos é bem menor, especialmente no caso de placas PnP. De qualquer forma, mudar o endereço de I/O usado pela placa de rede (isso pode ser feito através do gerenciador de dispositivos do Windows) é uma coisa a ser tentada caso a placa de rede misteriosamente não funcione, mesmo não havendo conflitos de IRQ e DMA.

Todas as placas de rede atuais são PnP, tendo seus endereços configurados automaticamente pelo sistema. Placas mais antigas por sua vez, trazem jumpers ou DIP switches que permitem configurar os endereços a serem usados pela placa. Existem também casos de placas de rede de legado que são configuráveis via software, sendo sua configuração feita através de um programa fornecido junto com a placa.

Para que as placas possam "se encontrar" dentro da rede, cada placa possui também um endereço de nó. Este endereço de 48 bits é único e estabelecido durante o processo de fabricação da placa, sendo inalterável. O endereço físico é relacionado com o endereço lógico do micro na rede. Se por exemplo na sua rede existe um outro micro chamado "Micro 2", e o "Micro 1" precisa transmitir dados para ele, o sistema operacional de rede ordenará à placa de rede que transmita os dados ao "Micro 2", porém, a placa usará o endereço de nó e não o endereço de fantasia "Micro 2" como endereço. Os dados trafegarão através da rede e será acessível a todas as os micros, porém, apenas a placa do "Micro 2" lerá os dados, pois apenas ela terá o endereço de nó indicado no pacote.

Sempre existe a possibilidade de alterar o endereço de nó de uma placa de rede, substituindo o chip onde ele é gravado. Este recurso é usado algumas vezes para fazer espionagem, já que o endereço de nó da rede poderá ser alterado para o endereço de nó de outra placa da rede, fazendo com que a placa clonada, instalada no micro do espião também receba todos os dados endereçados ao outro micro.

Hubs

Numa rede com topologia de estrela, o Hub funciona como a peça central, que recebe os sinais transmitidos pelas estações e os retransmite para todas as demais. Existem dois tipos de hubs, os hubs passivos e os hubs ativos.

Os hubs passivos limitam-se a funcionar como um espelho, refletindo os sinais recebidos para todas as estações a ele conectadas. Como ele apenas distribui o sinal, sem fazer qualquer tipo de amplificação, o comprimento total dos dois trechos de cabo entre um micro e outro, passando pelo hub, não pode exceder os 100 metros permitidos pelos cabos de par trançado.

Um Hub ativo por sua vez, além de distribuir o sinal, serve como um repetidor, reconstituindo o sinal enfraquecido e retransmitindo-o. Enquanto usando um Hub passivo o sinal pode trafegar apenas 100 metros somados os dois trechos de cabos entre as estações, usando um hub ativo o sinal pode trafegar por 100 metros até o hub, e após ser retransmitido por ele trafegar mais 100 metros completos. Apesar de mais caro, este tipo de hub permite estender a rede por distâncias maiores.

Hubs Inteligentes

Além dos hubs comuns, que apenas distribuem os sinais da rede para os demais micros conectados a ele, existe uma categoria especial de hubs, chamados de smart hubs, ou hubs inteligentes. Este tipo de hub incorpora um processador e softwares de diagnóstico, sendo capaz de detectar e se preciso desconectar da rede estações com problemas, evitando que uma estação faladora prejudique o tráfego ou mesmo derrube a rede inteira; detectar pontos de congestionamento na rede, fazendo o possível para normalizar o tráfego; detectar e impedir tentativas de invasão ou acesso não autorizado à rede e outros problemas em potencial entre outras funções, que variam de acordo com a sofisticação do Hub. O SuperStak II da 3Com por exemplo, traz um software que baseado em informações recebidas do hub, mostra um gráfico da rede, mostrando as estações que estão ou não funcionando, pontos de tráfego intenso etc.

Usando um hub inteligente a manutenção da rede torna-se bem mais simples, pois o hub fará a maior parte do trabalho. Isto é especialmente necessário em redes médias e grandes.

Switchs

Um Hub simplesmente retransmite todos os dados que chegam para todas as estações conectadas a ele, como um espelho. Isso faz com que o barramento de dados disponível seja compartilhado entre todas as estações e que apenas uma possa transmitir de cada vez.

Um switch também pode ser usado para interligar vários hubs, ou mesmo para interligar diretamente as estações, substituindo o hub. Mas, o switch é mais esperto, pois ao invés de simplesmente encaminhar os pacotes para todas as estações, encaminha apenas para o destinatário correto. Isto traz uma vantagem considerável em termos desempenho para redes congestionadas, além de permitir que, em casos de redes, onde são misturadas placas 10/10 e 10/100, as comunicações possam ser feitas na velocidade das placas envolvidas. Ou seja, quando duas placas 10/100 trocarem dados, a comunicação será feita a 100 megabits. Quando uma das placas de 10 megabits estiver envolvida, será feita a 10 megabits. Os switchs mais baratos, destinados a substituir os hubs são também chamados de hub-switchs.

De maneira geral a função do switch é muito parecida com a de um bridge, com a excessão que um switch tem mais portas e um melhor desempenho. Usando bridges ou switches todos os segmentos interligados continuam fazendo parte da mesma rede. As vantagens são apenas a melhora no desempenho e a possibilidade de adicionar mais nós do que seria possível unindo os hubs diretamente. Os roteadores por sua vez são ainda mais avançados, pois permitem interligar várias redes diferentes, criando a comunicação, mas mantendo-as como redes distintas.

Conectando Hubs

A maioria dos hubs possuem apenas 8 portas, alguns permitem a conexão de mais micros, mas sempre existe um limite. E se este limite não for suficiente para conectar todos os micros de sua rede?

Para quebrar esta limitação, existe a possibilidade de conectar dois ou mais hubs entre sí. Quase todos os hubs possuem uma porta chamada "Up Link" que se destina justamente a esta conexão. Basta ligar as portas Up Link de ambos os hubs, usando um cabo de rede normal para que os hubs passem a se enxergar.

Como para toda a regra existe uma exceção, alguns hubs mais baratos não possuem a porta Up Link, mas nem tudo está perdido, lembra-se do cabo cross-over que serve para ligar diretamente dois micros sem usar um hub? Ele também serve para conectar dois hubs. A única diferença neste caso é que ao invés de usar as portas Up Link, usaremos duas portas comuns.

Note que caso você esteja interligando hubs passivos, a distância total entre dois micros da rede, incluindo o trecho entre os hubs, não poderá ser maior que 100 metros, o que é bem pouco no caso de uma rede grande. Neste caso, seria mais recomendável usar hubs ativos, que amplificam o sinal.

Repetidores

Caso você precise unir dois hubs que estejam muito distantes, você poderá usar um repetidor. Se você tem, por exemplo, dois hubs distantes 150 metros um do outro, um repetidor estrategicamente colocado no meio do caminho servirá para viabilizar a comunicação entre eles.

Crescendo junto com a rede

O recurso de conectar hubs usando a porta Up Link, ou usando cabos cross-over, é utilizável apenas em redes pequenas, pois qualquer sinal transmitido por um micro da rede será retransmitido para todos os outros. Quanto mais micros tivermos na rede, maior será o tráfego e mais lenta a rede será.

Para resolver este problema, existem dois tipos de hubs especiais: os hubs empilháveis e os concentradores (também chamados de hubs de gabinete).

Os hubs empilháveis são a solução mais barata; inicialmente produzidos pela 3Com, são hubs "normais" que podem ser conectados entre sí através de um barramento especial, que aparece na forma de dois conectores encontrados na parte traseira do Hub. Temos então, dois barramentos de comunicação, um entre cada hub e os micros a ele conectados, e outro barramento de comunicação entre os hubs. Caso o micro 1 conectado ao hub A, precise transmitir um dado para o micro 22 conectado ao hub C, por exemplo, o sinal irá do Hub A diretamente para o Hub C

usando o barramento especial, e em seguida para o micro 22, sem ser transmitido aos demais hubs e micros da rede.
Os hubs empilháveis são conectados entre sí através de conectores localizados em sua parte traseira. Como um hub é conectado ao outro, você poderá ir interligando mais hubs conforme a rede for crescendo.


Hubs empilháveis da 3com

Os concentradores por sua vez, são grandes caixas com vários slots de barramento. Da mesma maneira que conectamos placas de expansão à placa mãe do micro, conectamos placas de porta aos slots do concentrador. Cada placa de porta é na verdade um hub completo, com 8 ou 16 portas. O barramento principal serve para conectar as placas. Você pode começar com apenas algumas placas, e ir adicionando mais placas conforme necessário.

Um concentrador pode trazer até 16 slots de conexão, o que permite a conexão de até 256 micros (usando placas de 16 portas). Mas se este número ainda não for suficiente, é possível interligar dois ou mais concentradores usando placas de backbone, que são conectadas ao último slot de cada concentrador, permitindo que eles sejam interligados, formando um grande concentrador. Neste último caso é possível conectar um número virtualmente ilimitado de micros.

10 ou 100?

Para que a sua rede possa transmitir a 100 mbps, além de usar placas de rede Ethernet PCI de 100 mbps e cabos de par trançado categoria 5, é preciso também comprar um hub que transmita a esta velocidade. A maioria dos hubs à venda atualmente no mercado, podem funcionar tanto a 10 quanto a 100 mbps, enquanto alguns mais simples funcionam a apenas 10 mbps. No caso dos hubs 10/100 mais simples, é possível configurar a velocidade de operação através de uma chave, enquanto hubs 10/100 inteligentes freqüentemente são capazes de detectar se a placa de rede da estação e o cabo são adequados para as transmissões a 100 mbps sendo a configuração automática.

Bridges, Roteadores e Gateways

Montar uma rede de 3 ou 4 micros é bem fácil. Mas, e se ao invés de apenas 4 PCs, forem um

contingente de centenas de PCs divididos em vários prédios diferentes, algumas dezenas de Macs, e de brinde, meia dúzia de velhos mainframes, todos esperando alguém (no caso você ;-) conseguir realizar o milagre de colocá-los para conversar?

Em redes maiores, além de cabos e hubs, usamos mais alguns dispositivos, um pouco mais caros: bridges (pontes) e Roteadores (routers). Todos estes podem ser tanto componentes dedicados, construídos especialmente para esta função, ou PCs comuns, com duas placas de rede e o software adequado para executar a função.

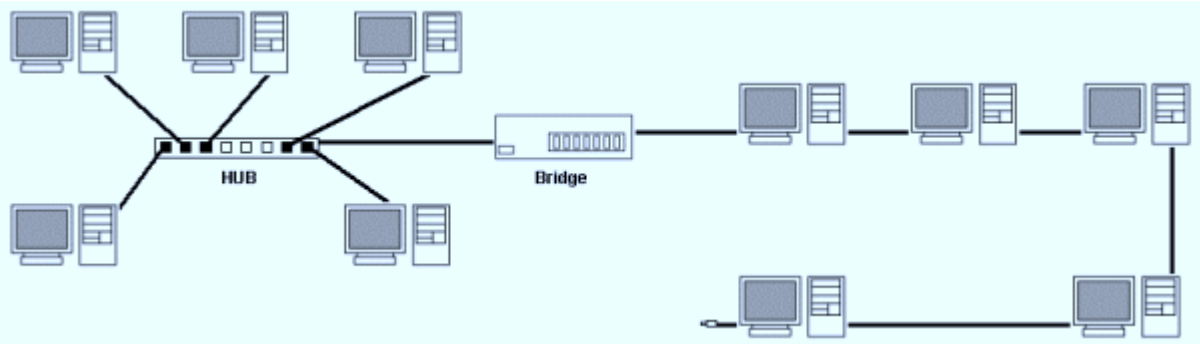
Bridges (pontes)

Imagine que em sua empresa existam duas redes; uma rede Ethernet, e outra rede Token Ring. Veja que apesar das duas redes possuírem arquiteturas diferentes e incompatíveis entre sí, é possível instalar nos PCs de ambas um protocolo comum, como o TCP/IP por exemplo. Com todos os micros de ambas as redes falando a mesma língua, resta apenas quebrar a barreira física das arquiteturas de rede diferentes, para que todos possam se comunicar. É justamente isso que um bridge faz. É possível interligar todo o tipo de redes usando bridges, mesmo que os micros sejam de arquiteturas diferentes, Macs de um lado e PCs do outro, por exemplo, contanto que todos os micros a serem conectados utilizem um protocolo comum. Antigamente este era um dilema difícil, mas atualmente isto pode ser resolvido usando o TCP/IP, que estudaremos à fundo mais adiante.

Como funcionam os Bridges?

Imagine que você tenha duas redes, uma Ethernet e outra Token Ring, interligadas por um bridge. O bridge ficará entre as duas, escutando qualquer transmissão de dados que seja feita em qualquer uma das duas redes. Se um micro da rede A transmitir algo para outro micro da rede A, o bridge ao ler os endereços de fonte e destino no pacote, perceberá que o pacote se destina ao mesmo segmento da rede e simplesmente ignorará a transmissão, deixando que ela chegue ao destinatário através dos meios normais. Se, porém, um micro da rede A transmitir algo para o micro da rede B, o bridge detectará ao ler o pacote que o endereço destino pertence ao outro segmento, e encaminhará o pacote.

Caso você tenha uma rede muito grande, que esteja tornando-se lenta devido ao tráfego intenso, você também pode utilizar um bridge para dividir a rede em duas, dividindo o tráfego pela metade.



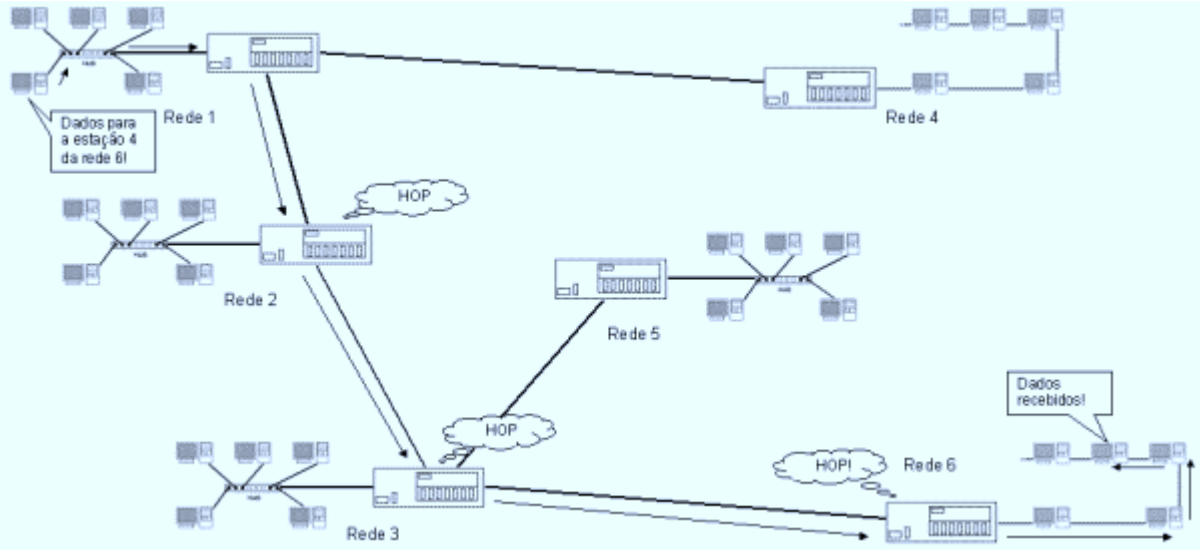
Existem também alguns bridges mais simples (e mais baratos) que não são capazes de distinguir se um pacote se destina ou não ao outro lado da rede. Eles simplesmente encaminham tudo, aumentando desnecessariamente o tráfego na rede. Estes bridges são chamados de bridges de encaminhamento, servem para conectar redes diferentes, mas não para diminuir o tráfego de dados. A função de bridge também pode ser executada por um PC com duas placas de rede, corretamente configurado.

Roteadores (routers)

Os bridges servem para conectar dois segmentos de rede distintos, transformando-os numa única rede. Os roteadores por sua vez, servem para interligar duas redes separadas. A diferença é que usando roteadores, é possível interligar um número enorme de redes diferentes, mesmo que situadas em países ou mesmo continentes diferentes. Note que cada rede possui seu próprio roteador e os vários roteadores são interligados entre sí.

Os roteadores são mais espertos que os bridges, pois não lêem todos os pacotes que são transmitidos através da rede, mas apenas os pacotes que precisam ser roteados, ou seja, que destinam-se à outra rede. Por este motivo, não basta que todos os micros usem o mesmo protocolo, é preciso que o protocolo seja roteável. Apenas o TCP/IP e o IPX/SPX são roteáveis, ou seja, permitem que os pacotes sejam endereçados à outra rede. Portanto, esqueça o NetBEUI caso pretenda usar roteadores.

Como vimos, é possível interligar inúmeras redes diferentes usando roteadores e não seria de se esperar que todos os roteadores tivessem acesso direto a todos os outros roteadores a que estivesse conectado. Pode ser que por exemplo, o roteador 4 esteja ligado apenas ao roteador 1, que esteja ligado ao roteador 2, que por sua vez seja ligado ao roteador 3, que esteja ligado aos roteadores 5 e 6. Se um micro da rede 1 precisar enviar dados para um dos micros da rede 6, então o pacote passará primeiro pelo roteador 2 sendo então encaminhado ao roteador 3 e então finalmente ao roteador 6. Cada vez que o dado é transmitido de um roteador para outro, temos um **hop**.



Os roteadores também são inteligentes o suficiente para determinar o melhor caminho a seguir. Inicialmente o roteador procurará o caminho com o menor número de hops: o caminho mais curto. Mas se por acaso perceber que um dos roteadores desta rota está ocupado demais, o que pode ser medido pelo tempo de resposta, então ele procurará caminhos alternativos para desviar deste roteador congestionado, mesmo que para isso o sinal tenha que passar por mais roteadores. No final, apesar do sinal ter percorrido o caminho mais longo, chegará mais rápido, pois não precisará ficar esperando na fila do roteador congestionado.

A Internet é na verdade uma rede gigantesca, formada por várias sub-redes interligadas por roteadores. Todos os usuários de um pequeno provedor, por exemplo, podem ser conectados à Internet por meio do mesmo roteador. Para baixar uma página do Yahoo por exemplo, o sinal deverá passar por vários roteadores, várias dezenas em alguns casos. Se todos estiverem livres, a página será carregada rapidamente. Porém, se alguns estiverem congestionados pode ser que a página demore vários segundos, ou mesmo minutos antes de começar a carregar.

O tempo que um pedido de conexão demora para ir até o servidor destino e ser respondido é chamado de "Ping". Você pode medir os pings de vários servidores diferentes usando o prompt do MS-DOS. Estando conectado à Internet basta digitar:
ping endereço_destino, como em: **ping** www.uol.com.br ou **ping** 207.167.207.78

Outra ferramenta útil tanto para medir o tempo de resposta de um servidor qualquer, quanto para verificar por quantos e quais roteadores o sinal está passando até chegar lá é o **NeoTrace**, um freeware que pode ser baixado na área e download do Guia do Hardware:
http://www.guiadohardware.net/download/

Nós de interconexão

Os bridges trabalham apenas checando o endereço destino dos pacotes transmitidos através da rede e os encaminhando quando necessário, para o outro segmento. Os roteadores são bem mais sofisticados, mas no fundo fazem a mesma tarefa básica: encaminhar os pacotes de dados. Tanto

os bridges quanto os roteadores trabalham lendo e transmitindo os pacotes, sem alterar absolutamente nada da mensagem, por isso que é necessário que todos os micros ligados a eles utilizem o mesmo protocolo.

Mas, e se você precisar interligar máquinas que não suportem o mesmo protocolo: interligar PCs a um mainframe projetado para se comunicar apenas com terminais burros, por exemplo?

O trabalho dos nós de interconexão é justamente este, trabalhar como tradutores, convertendo as informações de um protocolo para outro protocolo inteligível ao destinatário. Para cumprir esta tarefa são utilizáveis dois artifícios: o tunnelling e a emulação de terminal.

O tunnelling é o método mais simples e por isso mais usado. Ele consiste em converter a informação para um protocolo mutuamente inteligível, que possa ser transportado através da rede, e em seguida novamente converter o pacote para o protocolo usado na rede destino.

Se, por exemplo, é preciso transmitir um pacote de dados Novell IPX de uma rede de PCs para um Macintosh conectado a uma rede AppleTalk, podemos do lado da Rede Novell "envelopar" os dados usando o protocolo TPC/IP que é inteligível para ambas as redes, para que ele possa chegar ao destino, e do lado da rede AppleTalk "retirar o envelope" para obter os dados reais.

A emulação de terminal já é um processo um pouco mais trabalhoso e se destina a permitir a conexão de PCs com mainframes antigos, como os ainda muito utilizados em bancos. Como os mainframes são capazes de se comunicar apenas com terminais burros e não com PCs, é preciso fazer com que o PC finja ser um terminal burro durante a conversação. O "fingimento" é feito através de um programa de emulação de terminal, instalado em cada PC usuário do mainframe.

Para conectar vários PCs ligados em rede a um mainframe, é preciso instalar uma placa de interconexão em um dos PCs da rede (para poder conectá-lo fisicamente ao mainframe), esta placa contém a interface que permitirá a conexão. Este PC passará a ser o servidor do nó de interconexão.

Após estabelecer a conexão da rede com o mainframe, o acesso é feito usando o programa de emulação instalado em cada PC da rede, sendo a comunicação feita através do micro que está atuando como nó de interconexão. Note que por ser realizado via software, o processo de emulação é relativamente lento, o que era um problema em micros 286 ou 386 usados antigamente, mas não nos PCs modernos, muitas vezes mais rápidos que o próprio mainframe :-).

Arquiteturas de rede

Como vimos no início deste capítulo, temos uma divisão entre topologias físicas de rede (a forma como os micros são interligados) e as topologias lógicas (a forma como os dados são transmitidos).

Quanto à topologia física, temos topologias de barramento, onde usamos um único cabo coaxial para interligar todos os micros, e topologias de estrela, onde usamos cabos de par trançado e um hub.

As redes com topologia de estrela são as mais usadas atualmente, pois nelas a solução de

problemas é muito mais simples. Se uma estação não funciona, temos o problema isolado à própria estação. Basta então verificar se a estação está corretamente configurada e se a placa de rede está funcionando, se o cabo que liga o micro ao hub está intacto, não existe mau contato e se a porta do hub à qual o micro está conectado está funcionando.

As únicas vantagens da topologia de barramento físico residem no custo, já que geralmente usamos menos cabo para interligar os micros e não precisamos de um hub. As desvantagens por sua vez são muitas: como um único cabo interliga todos os micros, uma única estação com problemas será capaz de derrubar toda a rede. A solução de problemas também é mais difícil, pois você terá que examinar micro por micro até descobrir qual está derrubando a rede. A possibilidade de mau contato nos cabos também é maior, e novamente, um único encaixe com mau contato pode derrubar toda a rede (e lá vai você novamente checando micro por micro...). Finalmente, usando cabo coaxial, sua rede ficará limitada a 10 mbps, enquanto usando cabos de par trançado categoria 5 numa topologia de estrela, podemos chegar a 100 mbps.

Por causa destas desvantagens, a topologia de barramento pode ser utilizável em redes de no máximo 5 ou 10 micros, acima disto você deve considerar apenas a topologia de estrela. Caso você não se importe de gastar alguns reais a mais num hub, é aconselhável já começar logo com uma rede com cabos de par trançado, que lhe dará menos dor de cabeça mais tarde.

Citei no início a topologia física de anel, onde um único cabo interligaria todos os micros e voltaria ao primeiro formando um anel. Esta topologia porém é apenas uma teoria, já que o cabeamento seria muito mais difícil e não teríamos vantagens sobre a redes em barramento e estrela.

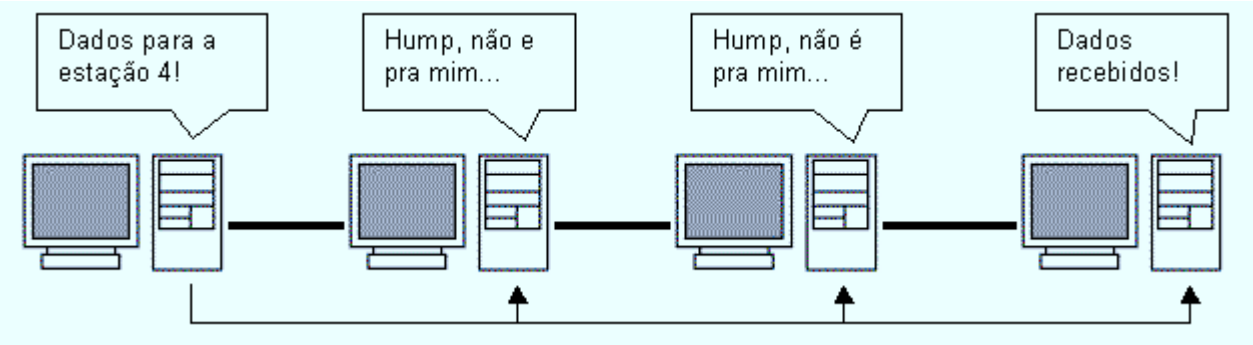
Topologias Lógicas

A topologia lógica da rede, determina como os dados são transmitidos através da rede. Não existe necessariamente uma ligação entre a topologia física e lógica; podemos ter uma estrela física e um barramento lógico, por exemplo.

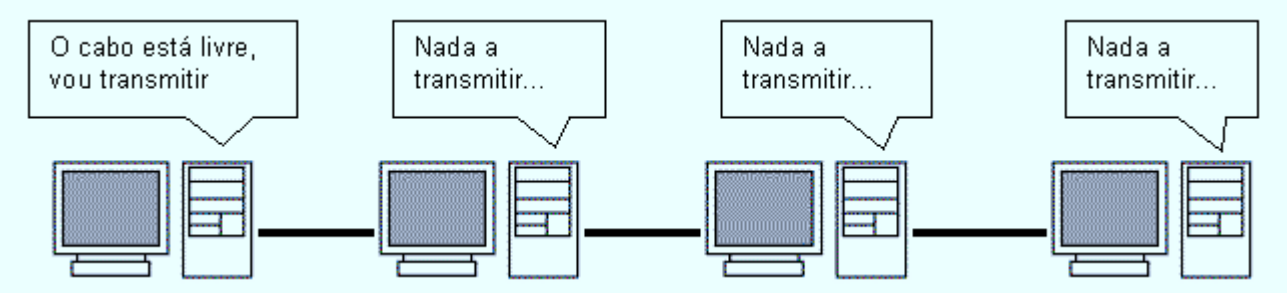
Existem três topologias lógicas de rede: Ethernet, Token Ring e Arcnet. Como a topologia lógica determina diretamente o modo de funcionamento da placa de rede, esta será específica para um tipo de rede. Não é possível usar placas Token Ring em Redes Ethernet, ou placas Ethernet em Redes Arcnet, por exemplo.

Redes Ethernet

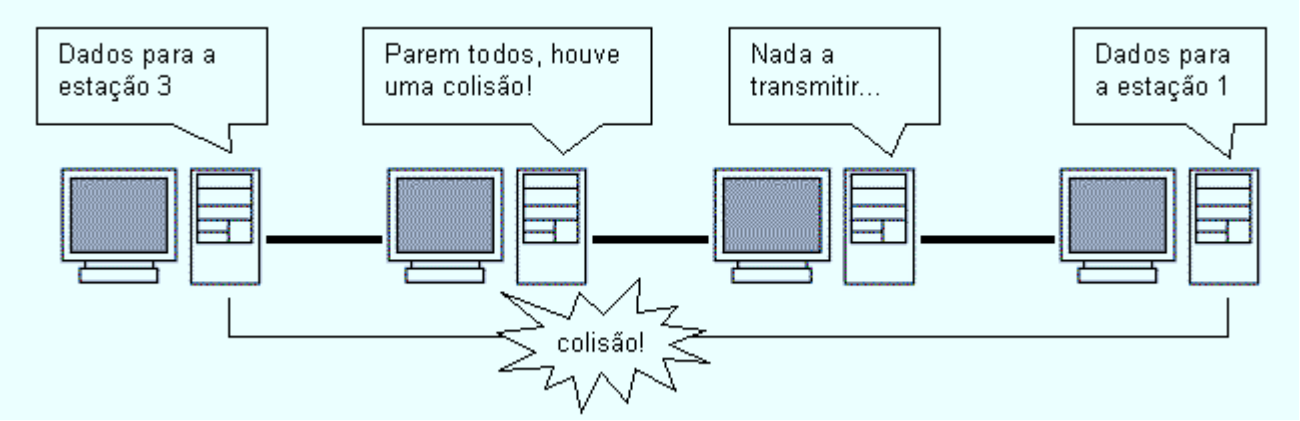
As placas de rede Ethernet são de longe as mais utilizadas atualmente, sobretudo em redes pequenas e médias e provavelmente a única arquitetura de rede com a qual você irá trabalhar. Numa rede Ethernet, temos uma topologia lógica de barramento. Isto significa que quando uma estação precisar transmitir dados, ela irradiará o sinal para toda a rede. Todas as demais estações ouvirão a transmissão, mas apenas a placa de rede que tiver o endereço indicado no pacote de dados receberá os dados. As demais estações simplesmente ignorarão a transmissão. Mais uma vez vale lembrar que apesar de utilizar uma topologia lógica de barramento, as redes Ethernet podem utilizar topologias físicas de estrela ou de barramento.



Como apenas uma estação pode falar de cada vez, antes de transmitir dados a estação irá "ouvir" o cabo. Se perceber que nenhuma estação está transmitindo, enviará seu pacote, caso contrário, esperará até que o cabo esteja livre. Este processo é chamado de "Carrier Sense" ou sensor mensageiro.

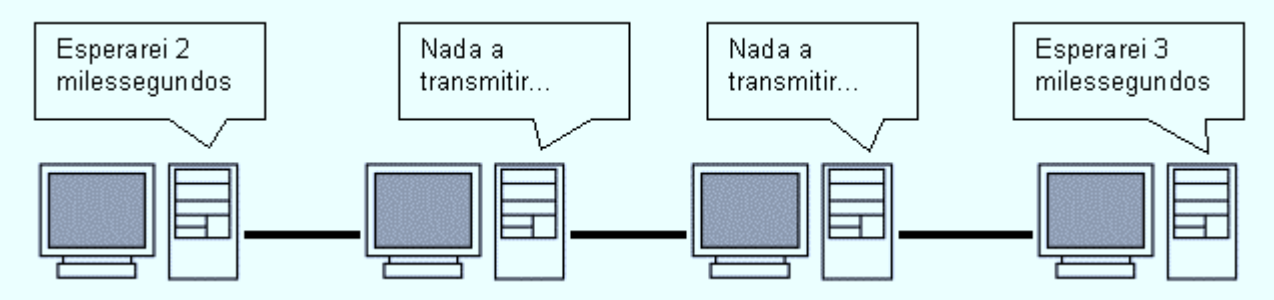


Mas, caso duas estações ouçam o cabo ao mesmo tempo, ambas perceberão que o cabo está livre e acabarão enviando seus pacotes ao mesmo tempo. Teremos então uma colisão de dados.
Dois pacotes sendo enviados ao mesmo tempo geram um sinal elétrico mais forte, que pode ser facilmente percebido pelas placas de rede. A primeira estação que perceber esta colisão irradiará para toda a rede um sinal especial de alta freqüência que cancelará todos os outros sinais que estejam trafegando através do cabo e alertará as demais placas que ocorreu uma colisão.



Sendo avisadas de que a colisão ocorreu, as duas placas "faladoras" esperarão um número aleatório de milessegundos antes de tentarem transmitir novamente. Este processo é chamado de TBEB "truncated exponencial backof". Inicialmente as placas escolherão entre 1 ou 2, se houver

outra colisão escolherão entre 1 e 4, em seguida entre 1 e 8 milessegundos, sempre dobrando os números possíveis até que consigam transmitir os dados. Apesar de as placas poderem fazer até 16 tentativas antes de desistirem, normalmente os dados são transmitidos no máximo na 3º tentativa.



Veja que apesar de não causarem perda ou corrupção de dados, as colisões causam uma grande perda de tempo, resultando na diminuição do desempenho da rede. Quanto maior for o número de estações, maior será a quantidade de colisões e menor será o desempenho da rede. Por isso existe o limite de 30 micros por segmento numa rede de cabo coaxial, e é recomendável usar bridges para diminuir o tráfego na rede caso estejamos usando topologia em estrela, com vários hubs interligados (e muitas estações).

Outro fator que contribui para as colisões é o comprimento do cabo. Quanto maior for o cabo (isso tanto para cabos de par trançado quanto coaxial) mais fraco chegará o sinal e será mais difícil para a placa de rede escutar o cabo antes de enviar seus pacotes, sendo maior a possibilidade de erro.

Usar poucas estações por segmento e usar cabos mais curtos do que a distância máxima permitida, reduzem o número de colisões e aumentam o desempenho da rede. O ideal no caso de uma rede com mais de 20 ou 30 micros, é dividir a rede em dois ou mais segmentos usando bridges, pois como vimos anteriormente, isto servirá para dividir o tráfego na rede.

Veja que todo este controle é feito pelas placas de rede Ethernet. Não tem nada a ver com o sistema operacional de rede ou com os protocolos de rede usados.

Pacotes

Todos os dados transmitidos através da rede, são divididos em pacotes. Em redes Ethernet, cada pacote pode ter até 1550 bytes de dados. A estação emissora escuta o cabo, transmite um pacote, escuta o cabo novamente, transmite outro pacote e assim por diante. A estação receptora por sua vez, vai juntando os pacotes até ter o arquivo completo.

O uso de pacotes evita que uma única estação monopolize a rede por muito tempo, e torna mais fácil a correção de erros. Se por acaso um pacote chegar corrompido, devido a interferências no cabo, ou qualquer outro motivo, será solicitada uma retransmissão do pacote. Quanto pior for a qualidade do cabo e maior for o nível de interferências, mais pacotes chegarão corrompidos e terão que ser retransmitidos e, consequentemente, pior será o desempenho da rede. Os pacotes Ethernet são divididos em 7 partes:

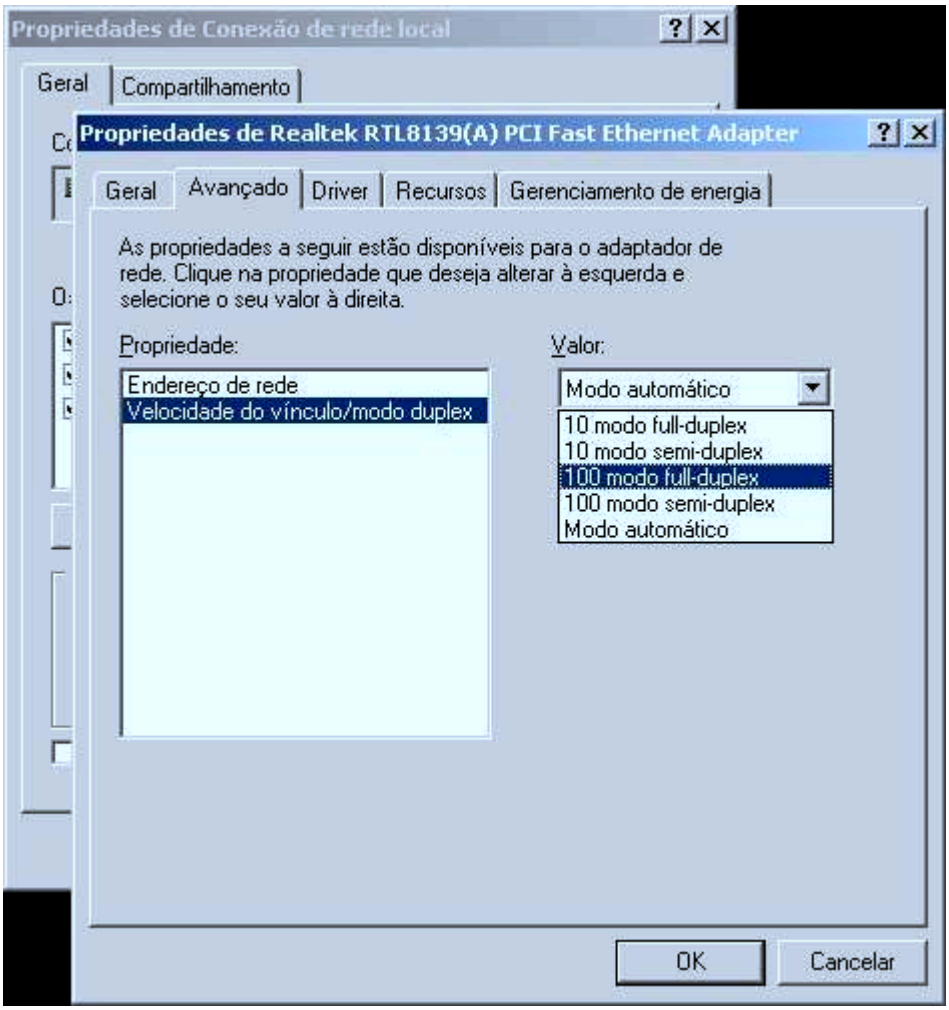
Preâmbulo (7 bytes)	Inicio (1 byte)	Endereço destino (6 bytes)	Endereço de origem (6 bytes)	Tipo de dados (2 bytes)	Dados (até 1550 bytes)	Verificação (4 bytes)

O **preâmbulo** serve para coordenar o envio dos demais dados do pacote, servindo como um sinal de sincronismo. O **byte de início** avisa as estações recebedoras que a transmissão irá começar (até aqui todas as estações da rede estão lendo o pacote). O **endereço de destino** indica a qual estação o pacote está endereçado. Apenas a placa de rede que possuir o endereço indicado irá ler o restante do pacote, as demais ignorarão o restante da transmissão. O **endereço de origem** indica qual estação está enviando os dados.

Antes de começar o envio dos dados em sí, temos mais um campo de 16 bits (2 bytes) que indica o **tipo de dados** que será transmitido, alguns dos atributos são: imagem, texto ASCII e binário. Finalmente temos enviados os **dados**, sendo que cada pacote pode conter até 1550 bytes de dados. Caso o arquivo seja maior que isso, será dividido em vários pacotes. Finalizando o pacote temos mais 32 bits de **verificação** que servem para a estação receptora checar se os dados do pacote chegaram intactos, através de um processo de paridade. Caso o pacote chegue corrompido será solicitada sua retransmissão.

Modo Full-Duplex

Para ativar o modo full duplex da placa, você precisa apenas acessar as propriedades da conexão de rede e clicar em “configurar” para abrir a janela de opções da placa de rede. Você encontrará a opção de ativar o Full-Duplex na sessão “Avançado”.



Mas, existe uma pequena regra para ativar o full duplex.

Numa rede de 10 megabits 10Base-T ou de 100 megabits 100Base-TX, os dois padrões mais comuns, você só pode usar o modo full duplex se estiver usando um cabo cross over, apenas entre dois micros, ou então se estiver usando um switch.

As duas arquiteturas utilizam apenas dois pares dos 4 do cabo de par trançado. Um par transmite dados e o outro transmite as notificações de colisões de pacotes. No full duplex são utilizados os dois pares, um para enviar e outro para receber, por isso não existe mais a detecção de colisão de pacotes.

Se você ativar o full duplex com mais de 2 PCs por segmento de rede (usando um hub) o desempenho da rede vai diminuir ao invés de aumentar, pois o número de colisões de pacotes vai aumentar muito e as placas serão obrigadas a fazer muitas retransmissões.

Mas, não existe um ganho de desempenho muito grande ao usar o full duplex ao invés do half-duplex (ou semi-duplex), pois só haverá ganho quando as duas estações precisarem transmitir grandes quantidades de dados aos mesmo tempo. O cenário mais comum é uma das estações

transmitindo dados e a outra apenas confirmando o recebimento dos pacotes, onde o modo full-duplex não faz diferença.

As placas 10Base-2, as antigas, que utilizam cabo coaxial, não suportam full duplex. Isso é uma exclusividade das placas que utilizam par trançado ou fibra óptica. As redes gigabit-over-cooper, que também utilizam cabos de par trançado suportam um modo full duplex, que também pode ser ativado apenas ao ligar diretamente dois PCs ou utilizar um switch.

Tecnologias antigas de rede

As redes Token Ring e mesmo as Arcnet já tiveram seus dias de glória, mas acabaram caindo em desuso com a popularização das redes Ethernet. Ainda é possível encontrar algumas redes Token Ring, sobretudo em grandes empresas e ainda é possível comprar placas e hubs, mas estamos vendo uma curva descendente, onde não são montadas novas redes e as antigas são apenas reparadas, não expandidas. São as Brasílias e Fuscas entre as redes.

Redes Token Ring

Diferentemente das redes Ethernet que usam uma topologia lógica de barramento, as redes Token Ring utilizam uma topologia lógica de anel. Quanto à topologia física, é utilizado um sistema de estrela parecido com o 10BaseT, onde temos hubs inteligentes com 8 portas cada ligados entre sí. Tanto os hubs quanto as placas de rede e até mesmo os conectores dos cabos têm que ser próprios para redes Token Ring. Existem alguns hubs combo, que podem ser utilizados tanto em redes Token Ring quanto em redes Ethernet.

O custo de montar uma rede Token Ring é muito maior que o de uma rede Ethernet, e sua velocidade de transmissão está limitada a 16 mbps, contra os 100 mbps permitidos pelas redes Ethernet. Porém, as redes Token Ring trazem algumas vantagens sobre sua concorrente: a topologia lógica em anel é quase imune a colisões de pacote, e pelas redes Token Ring obrigatoriamente utilizarem hubs inteligentes, o diagnóstico e solução de problemas é mais simples.

Devido a estas vantagens, as redes Token Ring ainda são razoavelmente utilizadas em redes de médio a grande porte. Contudo, não é recomendável pensar em montar uma rede Token Ring para seu escritório, pois os hubs são muito caros e a velocidade de transmissão em pequenas redes é bem mais baixa que nas redes Ethernet.

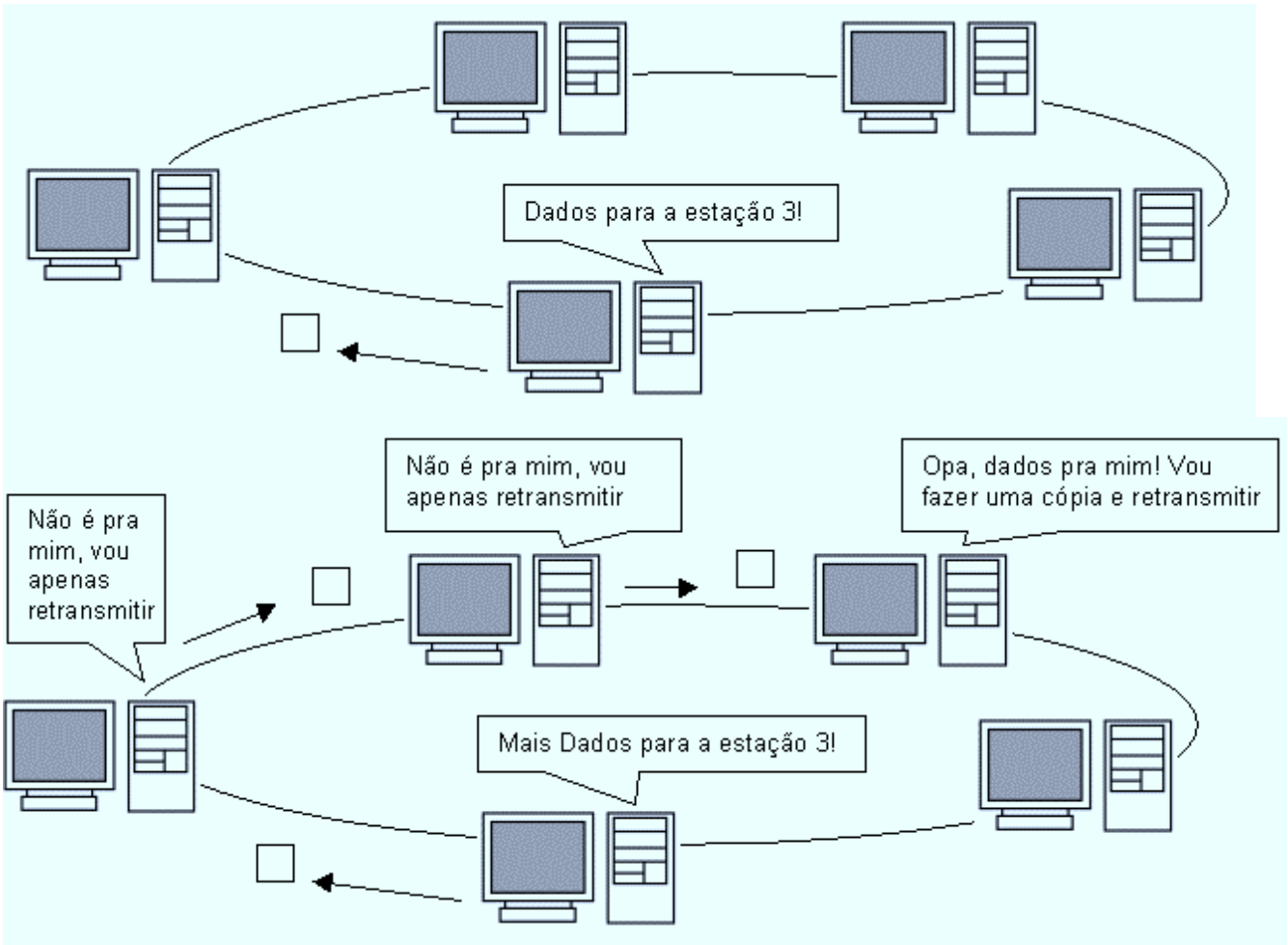
Como disse, as redes Token Ring utilizam uma topologia lógica de anel. Apesar de estarem fisicamente conectadas a um hub, as estações agem como se estivessem num grande anel. Disse anteriormente que as redes Token Ring são praticamente imunes a colisões, curioso em saber como este sistema funciona?

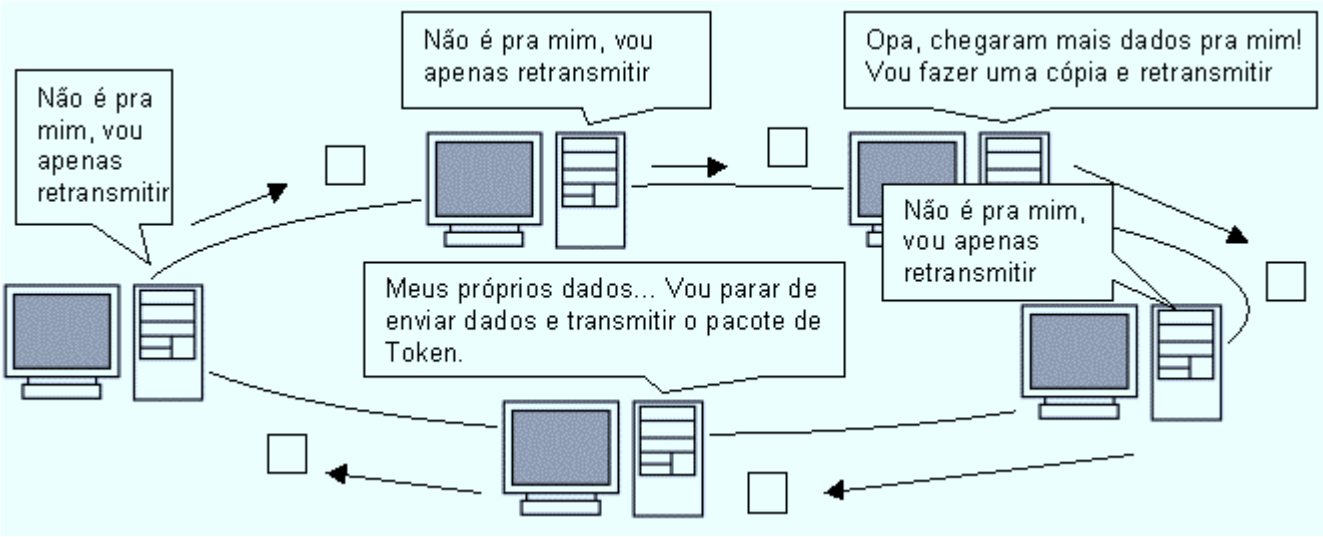
Se você tem uma grande quantidade de pessoas querendo falar (numa reunião por exemplo), como fazer para que apenas uma fale de cada vez? Uma solução seria usar um bastão de falar: quem estivesse com o bastão (e somente ele) poderia falar por um tempo determinado, ao final do qual deveria passar o bastão para outro que quisesse falar e esperar até que o bastão volte,

caso queira falar mais.

É justamente este o sistema usado em redes Token Ring. Um pacote especial, chamado pacote de Token circula pela rede, sendo transmitido de estação para estação. Quando uma estação precisa transmitir dados, ela espera até que o pacote de Token chegue e, em seguida, começa a transmitir seus dados.

A transmissão de dados em redes Token também é diferente. Ao invés de serem irradiados para toda a rede, os pacotes são transmitidos de estação para estação (daí a topologia lógica de anel). A primeira estação transmite para a segunda, que transmite para a terceira, etc. Quando os dados chegam à estação de destino, ela faz uma cópia dos dados para sí, porém, continua a transmissão dos dados. A estação emissora continuará enviando pacotes, até que o primeiro pacote enviado dê uma volta completa no anel lógico e volte para ela. Quando isto acontece, a estação pára de transmitir e envia o pacote de Token, voltando a transmitir apenas quando receber novamente o Token.





O sistema de Token é mais eficiente em redes grandes e congestionadas, onde a diminuição do número de colisões resulta em um maior desempenho em comparação com redes Ethernet semelhantes. Porém, em redes pequenas e médias, o sistema de Token é bem menos eficiente do que o sistema de barramento lógico das redes Ethernet, pois as estações têm de esperar bem mais tempo antes de poder transmitir.

Redes Arcnet

Das três topologias, a Arcnet é a mais antiga, existindo desde a década de 70. É claro que de lá pra cá tivemos muitos avanços, mas não o suficiente para manter as redes Arcnet competitivas frente às redes Token Ring e Ethernet. Para você ter uma idéia, as redes Arcnet são capazes de transmitir a apenas 2.5 mbps e quase não existem drivers for Windows para as placas de rede. Os poucos que se aventuram a usá-las atualmente normalmente as utilizam em modo de compatibilidade, usando drivers MS-DOS antigos.

Atualmente as redes Arcnet estão em vias de extinção, você dificilmente encontrará placas Arcnet à venda e mesmo que as consiga, enfrentará uma via sacra atrás de drivers para conseguir fazê-las funcionar.

Apesar de suas limitações, o funcionamento de rede Arcnet é bem interessante por causa de sua flexibilidade. Como a velocidade de transmissão dos dados é bem mais baixa, é possível usar cabos coaxiais de até 600 metros, ou cabos UTP de até 120 metros. Por serem bastante simples, os hubs Arcnet também são baratos.

O funcionamento lógico de uma rede Arcnet também se baseia num pacote de Token, a diferença é que ao invés do pacote ficar circulando pela rede, é eleita uma estação controladora da rede, que envia o pacote de Token para uma estação de cada vez.

Não há nenhum motivo especial para uma estação ser escolhida como controladora, geralmente é escolhida a estação com o endereço de nó formado por um número mais baixo.

Apesar de completamente obsoletas, muitos dos conceitos usados nas redes Arcnet foram usados para estabelecer os padrões atuais de rede.

Novas tecnologias de rede

As redes Ethernet são extremamente acessíveis, com placas de rede que chegam a custar 30 ou 35 reais, hubs de menos de 100 reais e cabos de rede com preços simplesmente irrisórios. A velocidade também é muito boa: 100 megabits são suficientes para quase todo tipo de aplicação, com exceção de redes muito congestionadas ou servidores de arquivos de alto desempenho.

Excluindo apenas as limitações em termos de flexibilidade, já que ainda é preciso sair passando cabos de rede pela casa, as redes Ethernet têm hoje um custo-benefício simplesmente imbatível.

Mas, atualmente, as opções de redes vão muito além das redes Ethernet. Padrões de redes sem fio como o IEEE 802.11b e o IEEE 802.11atrazem uma comodidade e facilidade de instalação atrativa principalmente em ambientes onde predominam os notebooks e portáteis em geral. O bluetooth é mais um padrão de rede sem fio que promete servir como complemento para as demais arquiteturas, permitindo interligar em rede pequenos aparelhos, como Palms, câmeras digitais, celulares, etc. Isso sem falar nos padrões Home PNA e HomePlug Powerline, que utilizam como mídia as extensões telefônicas e tomadas elétricas que todos temos em casa, facilitando a instalação da rede.

Além destes padrões, destinados ao mercado doméstico, temos padrões de rede muito mais rápidos que as redes Fast-Ethernet (100 megabits), destinadas principalmente a interligar servidores de arquivos de alto desempenho.

Claro, você não pode deixar de conhecer em primeira mão todas estas tecnologias. Vamos então analisar as características de cada opção:

IEEE 802.11b

Esta é a tecnologia de rede sem fio mais difundida atualmente e a que tem maiores chances de tornar-se padrão nos próximos um ou dois anos, passando a rivalizar com as redes Ethernet que já estão tão bem estabelecidas.

A topologia das redes 802.11b é semelhante a das redes de par trançado, com um Hub central. A diferença no caso é que simplesmente não existem os fios ;-) Existem tanto placas PC-Card, que podem ser utilizadas em notebooks e em alguns handhelds, quanto placas para micros de mesa.

Não existe mistério na instalação das placas. Basta deixar que o Windows detecte o novo hardware e fornecer os drivers da placa, ou executar o utilitário de configuração. O Windows XP possui drivers para algumas placas, facilitando a tarefa. As placas 802.11b são detectadas como placas Ethernet, apenas uma forma que os fabricantes encontraram para facilitar a compatibilidade com os vários sistemas operacionais.

Existem muitos casos de fabricantes que optaram por produzir apenas placas PC-Card (presumindo que a maior parte das vendas seria feita para usuários de notebooks) e que oferecem como complemento um adaptador opcional que pode ser usado para encaixar os cartões em micros de mesa. Lembre-se que o padrão PC-Card dos notebooks e o barramento PCI dos desktops são muito semelhantes, por isso basta um adaptador simples.

O Hub é chamado de ponto de acesso e tem a mesma função que desempenha nas redes Ethernet: retransmitir os pacotes de dados, de forma que todos os micros da rede os recebam.


Placa de rede 802.11b

Ponto de acesso

Não existe limite no número de estações que podem ser conectadas a cada ponto de acesso mas, assim como nas redes Ethernet, a velocidade da rede decai conforme aumenta o número de estações, já que apenas uma pode transmitir de cada vez.

A maior arma do 802.11b contra as redes cabeadas é a versatilidade. O simples fato de poder interligar os PCs sem precisar passar cabos pelas paredes já é o suficiente para convencer algumas pessoas, mas existem mais alguns recursos interessantes que podem ser explorados.

Sem dúvidas, a possibilidade mais interessante é a mobilidade para os portáteis. Tanto os notebooks quanto handhelds e as futuras webpads podem ser movidos livremente dentro da área coberta pelos pontos de acesso sem que seja perdido o acesso à rede.

Esta possibilidade lhe dará alguma mobilidade dentro de casa para levar o notebook para onde quiser, sem perder o acesso à Web, mas é ainda mais interessante para empresas e escolas. No caso das empresas a rede permitiria que os funcionários pudessem se deslocar pela empresa sem perder a conectividade com a rede e bastaria entrar pela porta para que o notebook

automaticamente se conectasse à rede e sincronizasse os dados necessários. No caso das escolas a principal utilidade seria fornecer acesso à Web aos alunos. Esta já é uma realidade em algumas universidades e pode tornar-se algo muito comum dentro dos próximos anos.

Vamos então às especificações e aos recursos desta arquitetura.

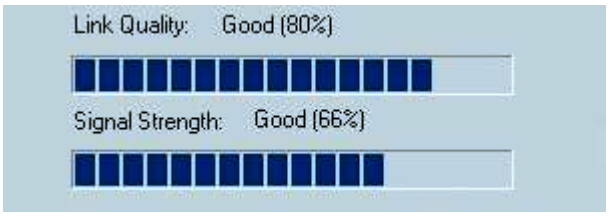
A velocidade das redes 802.11b é de **11 megabits**, comparável à das redes Ethernet de 10 megabits, mas muito atrás da velocidade das redes de 100 megabits. Estes 11 megabits não são adequados para redes com um tráfego muito pesado, mas são mais do que suficientes para compartilhar o acesso à web, trocar pequenos arquivos, jogar games multiplayer, etc. Note que os 11 megabits são a taxa bruta de transmissão de dados, que incluem modulação, códigos de correção de erro, retransmissões de pacotes, etc., como em outras arquiteturas de rede. A velocidade real de conexão fica em torno de 6 megabits, o suficiente para transmitir arquivos a 750 KB/s, uma velocidade real semelhante à das redes Ethernet de 10 megabits.

Mas, existe a possibilidade de combinar o melhor dos dois mundos, conectando um ponto de acesso 802.11b a uma rede Ethernet já existente. No ponto de acesso da foto acima você pode notar que existe um conector RJ-45:

Isto adiciona uma grande versatilidade à rede e permite diminuir os custos. Você pode interligar os PCs através de cabos de par trançado e placas Ethernet que são baratos e usar as placas 802.11b apenas nos notebooks e aparelhos onde for necessário ter mobilidade. Não existe mistério aqui, basta conectar o ponto de acesso ao Hub usando um cabo de par trançado comum para interligar as duas redes. O próprio Hub 802.11b passará a trabalhar como um switch, gerenciando o tráfego entre as duas redes.

O alcance do sinal varia entre 15 e 100 metros, dependendo da quantidade de obstáculos entre o ponto de acesso e cada uma das placas. Paredes, portas e até mesmo pessoas atrapalham a propagação do sinal. Numa construção com muitas paredes, ou paredes muito grossas, o alcance pode se aproximar dos 15 metros mínimos, enquanto num ambiente aberto, como o pátio de uma escola o alcance vai se aproximar dos 100 metros máximos. Se você colocar o ponto de acesso próximo da janela da frente da sua casa por exemplo, provavelmente um vizinho distante dois quarteirões ainda vai conseguir se conectar à sua rede.

Você pode utilizar o utilitário que acompanha a placa de rede para verificar a qualidade do sinal em cada parte do ambiente onde a rede deverá estar disponível. O utilitário lhe fornecerá um gráfico com a potência e a qualidade do sinal, como abaixo:



A potência do sinal decai conforme aumenta a distância, enquanto a qualidade decai pela combinação do aumento da distância e dos obstáculos pelo caminho. É por isso que num campo aberto o alcance será muito maior do que dentro de um prédio por exemplo.

Conforme a potência e qualidade do sinal se degrada, o ponto de acesso pode diminuir a velocidade de transmissão a fim de melhorar a confiabilidade da transmissão. A velocidade pode cair para 5.5 megabits, 2 megabits ou chegar a apenas 1 megabit por segundo antes do sinal se perder completamente. Algumas placas e pontos de acesso são capazes de negociar velocidades ainda mais baixas, possibilitando a conexão a distâncias ainda maiores. Nestes casos extremos o acesso à rede pode se parecer mais com uma conexão via modem do que via rede local.

As redes sem fio, sejam baseadas no 802.11b ou em qualquer outro padrão, apresentam um grande potencial para o futuro. Uma mudança mais interessante que eu vejo é o estabelecimento de pontos de acesso à Web em lojas, supermercados, shoppings, restaurantes, escolas, etc. onde o acesso à Web será oferecido como conveniência aos clientes armados com notebooks e palmtops, que dentro dos próximos anos se tornarão muito mais populares e já virão com interfaces de rede sem fio. Será uma forma de acesso muito mais barata (e mais rápida) que a através dos celulares 2.5G ou mesmo 3G e ao mesmo tempo será algo muito barato de implantar para os comerciantes que já tiverem um PC com acesso à Web.

Já que na maior parte do tempo em que não estamos em casa ou no trabalho estamos em algum destes lugares, estas pequenas redes públicas diminuirão muito a necessidade de usar o acesso via celular, que mesmo com o 2.5G continuará sendo caro, já que não haverá mais cobrança por minuto, mas em compensação haverá tarifação pela quantidade de dados transferidos. Será uma grande conveniência, já que você poderá acessar a Web em praticamente qualquer lugar. O velho sonho de muitos educadores de escolas onde cada aluno tem um computador conectado à rede da escola também poderá tornar-se realidade mais facilmente.

O alcance de 15 a 100 metros do 802.11b é mais do que suficiente para uma loja, escritório ou restaurante. No caso de locais maiores, bastaria combinar vários pontos de acesso para cobrir toda a área. Estes pontos podem ser configurados para automaticamente dar acesso a todos os aparelhos dentro da área de cobertura. Neste caso não haveria maiores preocupações quanto à segurança, já que estará sendo compartilhado apenas acesso à web.

Segurança

A maior dúvida sobre o uso de redes sem fio recai sobre o fator segurança. Com um transmissor irradiando os dados transmitidos através da rede em todas as direções, como impedir que qualquer um possa se conectar a ela e roubar seus dados? Como disse acima, um ponto de acesso instalado próximo à janela da sala provavelmente permitirá que um vizinho a dois quarteirões da sua casa consiga captar o sinal da sua rede, uma preocupação agravada pela popularidade que as

redes sem fio vêm ganhando.

Alguns kits permitem ainda conectar antenas Yagi, ou outras antenas de longo alcance nas interfaces de rede, o que aumenta ainda mais o alcance dos sinais, que com as antenas especiais pode chegar a mais de 500 metros. Veremos isto com mais detalhes logo adiante.

Para garantir a segurança, existem vários sistemas que podem ser implementados, apesar de nem sempre eles virem ativados por default nos pontos de acesso.

Todo ponto de acesso 802.11b, mesmo os de baixo custo, oferece algum tipo de ferramenta de administração. Alguns podem ser acessados via web, como alguns modems ADSL e switches, onde basta digitar no browser de uma das máquinas da rede o endereço IP do ponto de acesso e a porta do serviço.

Neste caso, qualquer PC da rede (um um intruso que se conecte a ela) pode acessar a ferramenta de configuração. Para se proteger você deve alterar a senha de acesso default e se possível também alterar a porta usada pelo serviço. Assim você terá duas linhas de proteção. Mesmo que alguém descubra a senha ainda precisará descobrir qual porta o utilitário está escutando e assim por diante.

Em outros casos será necessário instalar um programa num dos micros da rede para configurar o ponto de acesso, mas valem as mesmas medidas de alterar a senha default e se possível a porta TCP utilizada pelo serviço.

Dentro do utilitário de configuração você poderá habilitar os recursos de segurança. Na maioria dos casos todos os recursos abaixo vem desativados por default a fim de que a rede funcione imediatamente, mesmo antes de qualquer coisa ser configurada. Para os fabricantes, quanto mais simples for a instalação da rede, melhor, pois haverá um número menor de usuários insatisfeitos por não conseguir fazer a coisa funcionar. Mas, você não é qualquer um. Vamos então às configurações:

ESSID

A primeira linha de defesa é o **ESSID** (Extended Service Set ID), um código alfanumérico que identifica os computadores e pontos de acesso que fazem parte da rede. Cada fabricante utiliza um valor default para esta opção, mas você deve alterá-la para um valor alfanumérico qualquer que seja difícil de adivinhar.

Geralmente estará disponível no utilitário de configuração do ponto de acesso a opção "**broadcast ESSID**". Ao ativar esta opção o ponto de acesso envia periodicamente o código ESSID da rede, permitindo que todos os clientes próximos possam conectar-se na rede sem saber préviamente o código. Ativar esta opção significa abrir mão desta camada de segurança, em troca de tornar a rede mais "plug-and-play". Você não precisará mais configurar manualmente o código ESSID em todos os micros.

Esta é uma opção desejável em redes de acesso público, como muitas redes implantadas em escolas, aeroportos, etc. mas caso a sua preocupação maior seja a segurança, o melhor é desativar a opção. Desta forma, apenas quem souber o valor ESSID poderá acessar a rede.

WEP

Apenas o ESSID, oferece uma proteção muito fraca. Mesmo que a opção broadcast ESSID esteja desativada, já existem sniffers que podem descobrir rapidamente o ESSID da rede monitorando o tráfego de dados.

Heis que surge o WEP, abreviação de Wired-Equivalent Privacy, que como o nome sugere traz como promessa um nível de segurança equivalente à das redes cabeadas. Na prática o WEP também tem suas falhas, mas não deixa de ser uma camada de proteção essencial, muito mais difícil de penetrar que o ESSID sozinho.

O WEP se encarrega de encriptar os dados transmitidos através da rede. Existem dois padrões WEP, de 64 e de 128 bits. O padrão de 64 bits é suportado por qualquer ponto de acesso ou interface que siga o padrão WI-FI, o que engloba todos os produtos comercializados atualmente. O padrão de 128 bits por sua vez não é suportado por todos os produtos. Para habilitá-lo será preciso que todos os componentes usados na sua rede suportem o padrão, caso contrário os nós que suportarem apenas o padrão de 64 bits ficarão fora da rede.

Na verdade, o WEP é composto de duas chaves distintas, de 40 e 24 bits no padrão de 64 bits e de 104 e 24 bits no padrão de 128. Por isso, a complexidade encriptação usada nos dois padrões não é a mesma que seria em padrões de 64 e 128 de verdade.

Além do detalhe do número de bits nas chaves de encriptação, o WEP possui outras vulnerabilidades. Alguns programas já largamente disponíveis são capazes de quebrar as chaves de encriptação caso seja possível monitorar o tráfego da rede durante algumas horas e a tendência é que estas ferramentas se tornem ainda mais sofisticadas com o tempo. Como disse, o WEP não é perfeito, mas já garante um nível básico de proteção.

O WEP vem desativado na grande maioria dos pontos de acesso, mas pode ser facilmente ativado através do utilitário de configuração. O mais complicado é que você precisará definir manualmente uma chave de encriptação (um valor alfanumérico ou hexadecimal, dependendo do utilitário) que deverá ser a mesma em todos os pontos de acesso e estações da rede. Nas estações a chave, assim como o endereço ESSID e outras configurações de rede podem ser definidas através de outro utilitário, fornecido pelo fabricante da placa.

Um detalhe interessante é que apartir do início de 2002 os pontos de acesso devem começar a suportar o uso de chaves de encriptação dinâmicas, que não exigirão configuração manual. Ao adquirir um ponto de acesso agora é importante verificar se ele pode ser atualizado via software, para que mais tarde você possa instalar correções e suporte a novos padrões e tecnologias.

RADIUS

Este é um padrão de encriptação proprietário que utiliza chaves de encriptação de 128 bits reais, o que o torna muito mais seguro que o WEP. Infelizmente este padrão é suportado apenas por alguns produtos. Se estiver interessado nesta camada extra de proteção, você precisará pesquisar

quais modelos suportam o padrão e selecionar suas placas e pontos de acesso dentro desse círculo restrito. Os componentes geralmente serão um pouco mais caro, já que você estará pagando também pela camada extra de encriptação.

Permissões de acesso

Além da encriptação você pode considerar implantar também um sistema de segurança baseado em permissões de acesso. O Windows 95/98/ME permite colocar senhas nos compartilhamentos, enquanto o Windows NT, 2000 Server ou ainda o Linux, via Samba, já permitem uma segurança mais refinada, baseada em permissões de acesso por endereço IP, por usuário, por grupo, etc.

Usando estes recursos, mesmo que alguém consiga penetrar na sua rede, ainda terá que quebrar a segurança do sistema operacional para conseguir chegar aos seus arquivos. Isso vale não apenas para redes sem fio, mas também para redes cabeadas, onde qualquer um que tenha acesso a um dos cabos ou a um PC conectado à rede é um invasor em potencial.

Alguns pontos de acesso oferecem a possibilidade de estabelecer uma lista com as placas que têm permissão para utilizar a rede e rejeitar qualquer tentativa de conexão de placas não autorizadas. O controle é feito através dos endereços MAC das placas, que precisam ser incluídos um a um na lista de permissões, através do utilitário do ponto de acesso. Muitos oferecem ainda a possibilidade de estabelecer senhas de acesso.

Somando o uso de todos os recursos acima, a rede sem fio pode tornar-se até mais segura do que uma rede cabeada, embora implantar tantas camadas de proteção torne a implantação da rede muito mais trabalhosa.

Como so dados são transmitidos e interferência

As redes 802.11b transmitem sinais de rádio na faixa dos 2.4 GHz utilizando um modo de transmissão chamado Direct Sequence Spread Spectrum, onde o transmissor escolhe uma frequência onde não existam outras transmissões e se mantém nela durante o período de operação, a menos que o nível de interferência atinja um ponto crítico. Neste caso os transmissores procurarão outra frequência disponível. O padrão 802.11b utiliza frequências entre 2.4 e 2.48 GHz, com um total de 11 canais disponíveis (2.412, 2.417, 2.422, 2.427, 2.432, 2.437, 2.442, 2.447, 2.452, 2.457 e 2.462 GHz).

Os transmissores podem utilizar qualquer uma das faixas em busca da banda mais limpa, o que já garante alguma flexibilidade contra interferências. Apesar disso, as redes 802.11b possuem pelo menos quatro inimigos importantes: os transmissores bluetooth, telefones sem fio que operam na faixa dos 2.4 GHz, aparelhos de microondas e outros pontos de acesso 802.11b próximos.

Em nenhum dos quatro casos existe o risco da rede chegar a sair fora do ar (mesmo em casos extremos), mas existe a possibilidade de haver uma degradação de desempenho considerável.

O Bluetooth costuma ser o mais temido, pois também é um padrão de redes sem fio e também opera na faixa dos 2.4 GHz. Mas, na prática, o Bluetooth é o menos perigoso dos quatro, pois

utiliza um modo de transmissão diferente do 802.11b, chamado Frequency Hop Spread Spectrum, onde os transmissores mudam constantemente de frequência, dentro do conjunto de 79 canais permitido pelo padrão. Esta é uma forma de evitar interferência com outros transmissores Bluetooth próximos, já que a sequência é conhecida apenas pelos dispositivos envolvidos e, em consequência, também evita uma interferência direta com transmissores 802.11b.

Na prática, os transmissores Bluetooth podem causar uma pequena perda de desempenho nos momentos em que tentarem transmitir na mesma frequência dos transmissores 802.11b. Mas, como o chaveamento é muito rápido, isto só chega a ser um problema nas transmissões de vídeo ou outros tipos de mídia via streaming, onde qualquer pequena pausa já atrapalha a visualização.

Os modelos de telefone sem fio que operam na faixa dos 2.4 GHz são um pouco mais perigosos, já que ao contrário do bluetooth operam a uma frequência fixa. Neste caso o telefone pode invadir a frequência utilizada pela rede, prejudicando a velocidade de transmissão enquanto estiver sendo usado.

Os aparelhos de microondas também utilizam ondas de rádio nesta mesma faixa de frequência e por isso também podem atrapalhar, embora apenas caso fiquem muito próximos dos transmissores. Caso o microondas fique a pelo menos 6 metros, não haverá maiores problemas.

Finalmente, chegamos ao problema final. O que acontece caso todos os seus vizinhos resolvam utilizar redes 802.11b, ou caso você precise utilizar vários pontos de acesso na mesma rede?

Como disse acima, os dispositivos de cada rede podem utilizar qualquer um dos 11 canais permitidos pelo padrão. Mas existe um porém: dos 11, apenas 3 canais podem ser utilizados simultâneamente, pois os transmissores precisam de uma faixa de 22 MHz para operar.

Se existirem até 3 transmissores na mesma área, não haverá problemas, pois cada um poderá utilizar um canal diferente. Com 4 ou mais pontos de acesso você terá perda de desempenho sempre que dois tentarem transmitir dados simultâneamente.

Na prática, o cenário é parecido com o que temos numa rede Ethernet. Como o Hub encaminha todos os pacotes para todas as estações, apenas uma estação pode transmitir de cada vez. Sempre que duas estações tentam transmitir ao mesmo tempo, temos uma colisão de pacotes e a rede fica paralisada por alguns milessegundos, até que as estações possam voltar a retransmitir, uma de cada vez.

No 802.11b temos um cenário parecido. Com vários pontos de acesso operando no mesmo canal, as transmissões precisam ser feitas de forma alternada. Na melhor das hipóteses, você não terá 11 megabits para cada um, mas 11 megabits para todos. Naturalmente isso só se aplica nos momentos em que ambos transmitirem ao mesmo tempo.

Mais uma curiosidade é que é possível aproveitar os três canais simultâneos para utilizar dois ou três pontos de acesso no mesmo local, como uma forma de aumentar a performance da rede (no caso de redes muito movimentadas, com muitas estações), dividindo os usuários entre os pontos de acesso disponíveis. Existem alguns casos de pontos de acesso que trabalham simultâneamente nas três frequências, como se fosse três pontos de acesso distintos.

Aumentando o alcance

Assim como em outras tecnologias de transmissão via rádio, a distância que o sinal é capaz de percorrer depende também da qualidade da antena usada. As antenas padrão utilizadas nos pontos de acesso, geralmente de 2 dBi são pequenas e práticas, além de relativamente baratas, mas existe a opção de utilizar antenas mais sofisticadas para aumentar o alcance da rede.


Ponto de acesso com as antenas padrão.

Alguns fabricantes chegam a dizer que o alcance dos seus pontos de acesso chega a 300 metros, usando as pequenas antenas padrão. Isto está um pouco longe da realidade, pois só pode ser obtido em campos abertos, livres de qualquer obstáculo e mesmo assim o sinal ficaria tão fraco que a velocidade de transmissão mal chegaria a 1 megabit.

Mesmo assim, a distância máxima e a qualidade do sinal (e consequentemente a velocidade de transmissão) pode variar bastante de um modelo de ponto de acesso para outro, de acordo com a qualidade do transmissor e da antena usada pelo fabricante.

Existem basicamente três tipos de antenas que podem ser utilizadas para aumentar o alcance da rede.

As antenas Yagi, são as que oferecem um maior alcance, mas em compensação são capazes de cobrir apenas a área para onde são apontadas. Estas antenas são mais úteis para cobrir alguma área específica, longe do ponto de acesso, ou então para um usuário em trânsito, que precisa se conectar à rede. Em ambos os casos, o alcance utilizando uma antena Yagi pode passar dos 500 metros.


Antena Yagi

A segunda opção são as antenas ominidirecionais, que, assim como as antenas padrão dos pontos de acesso, cobrem uma área circular (ou esférica, caso o ponto de acesso esteja instalado acima do solo) em torno da antena. A vantagem é a possibilidade de utilizar uma antena com uma maior potência. Existem modelos de antenas ominidirecionais de 3dbi, 5 dBi, 10 dBi ou até mesmo 15 dBi, um grande avanço sobre as antenas de 2 dBi que acompanham a maioria dos pontos de

acesso.

  Antenas ominidirecionais

Assim como as Yagi, as antenas ominidirecionais podem ser usadas tanto para aumentar a área de cobertura do ponto de acesso, quanto serem instaladas numa interface de rede, em substituição à antena que a acompanha, permitindo captar o sinal do ponto de acesso de uma distância maior.

Mais uma opção de antena são as mini-parabólicas, que também captam o sinal em apenas uma direção, como as Yagi, mas em compensação podem ter uma potência ainda maior, dependendo do modelo usado.

 Mini-Parabólica

Estas antenas podem custar de 30 a mais de 200 dólares, dependendo da potência. As antenas Yagi estão entre as mais caras, vendidas por US$ 150 ou mais. Além do problema do preço, existe um aumento no risco de uso indevido na rede, já que o sinal irá propagar-se por uma distância maior, mais uma razão para reforçar a segurança.

Modo Ad-hoc

Assim como é possível ligar dois micros diretamente usando duas placas Ethernet e um cabo cross-over, sem usar hub, também é possível criar uma rede Wireless entre dois PCs sem usar um ponto de acesso. Basta configurar ambas as placas para operar em modo Ad-hoc (através do utilitário de configuração). A velocidade de transmissão é a mesma, mas o alcance do sinal é bem menor, já que os transmissores e antenas das interfaces não possuem a mesma potência do ponto de acesso.

Este modo pode servir para pequenas redes domésticas, com dois PCs próximos, embora mesmo neste caso seja mais recomendável utilizar um ponto de acesso, interligado ao primeiro PC através

de uma placa Ethernet e usar uma placa wireless no segundo PC ou notebook, já que a diferenças entre o custo das placas e pontos de acesso não é muito grande.

A questão do custo

O custo ainda é uma questão delicada em se tratando de redes sem fio. Mais delicada ainda para tratar aqui, já que vou ter que usar minhas capacidades mediúnicas e tentar fazer um exercício de futurologia :-)

Mas falando sério, o mercado de redes sem fio ainda está em expansão. Existe um grande interesse por parte dos fabricantes em popularizar a tecnologia pois os periféricos para redes Ethernet já estão tão baratos que a margem de lucro dos fabricantes, mesmo dos que vendem soluções mais caras, como a Intel e 3Com é irrisória. Além disso, eles só conseguem vender novos componentes para quem ainda não tem redes, já que placas de rede e Hubs são componentes bastante duráveis, na maioria das vezes aproveitados em vários upgrades.

As redes sem fio são a chance de conseguir convencer os usuários a trocar boa parte da base instalada.

Enquanto escrevo (Dezembro de 2001) os pontos de acesso ainda custam de 150 e 250 dólares e as interfaces de rede custam de 100 a 150 dólares, em média. Nos EUA os valores já estão um pouco mais baixos que isto e no Japão os pontos de acesso e interfaces chegam a ser vendidas por 100 e 60 dólares respectivamente.

Sem dúvida, os componentes para redes sem fio vão continuar sendo mais caros que os para redes Ethernet por muito tempo. Além dos controladores existem os transmissores e as antenas, que aumentam bastante o custo total do conjunto. Mas o futuro parece promissor.

Conforme a tecnologia for se popularizando e os fabricantes começarem a produzir os componentes em maior quantidade, os preços devem cair para algo próximo de 70 dólares pelos pontos de acesso e 50 dólares pelas interfaces de rede ao longo de 2002.

Outro detalhe importante é que vários fabricantes de placas mãe vêm apresentando projetos de placas com interfaces 802.11b onboard. A primeira foi a Intel, com uma placa de referência apresentada durante a Comdex (a Americana) em Novembro de 2001.

As placas com interfaces onboard serão sem dúvidas muito mais baratas do que o conjunto de placas mãe e uma placa 802.11b separada e passarão a representar uma percentagem considerável do total de placas vendidas até a segunda metade de 2002, o que poderá ser decisivo para a popularização da tecnologia.

Mas, como vimos, as redes sem fio podem ser usadas como complemento para as redes cabeadas que já existem. Esta é a aplicação ideal, considerando que a velocidade é mais baixa e o custo é mais alto. O melhor custo benefício seria então usar uma rede cabeada para interligar todos os desktops, ligar um ponto de acesso ao hub e usar placas wireless apenas nos notebooks e outros aparelhos portáteis. Se a preocupação for a segurança, é possível incluir ainda um firewall entre a rede cabeada e a rede sem fio.

Mas, não existe garantia que o 802.11b seja mesmo o padrão definitivo. O maior concorrente é o 802.11a, que é menos susceptível a interferências é mais rápido.

IEEE 802.11a

O 802.11b utiliza a frequência de 2.4 GHz, a mesma utilizada por outros padrões de rede sem fio e pelos microondas, todos potenciais causadores de interferência. O 802.11a por sua vez utiliza a frequência de 5 GHz, onde a interferência não é problema. Graças à frequência mais alta, o padrão também é quase cinco vezes mais rápido, atingindo respeitáveis 54 megabits.

Note que esta é a velocidade de transmissão "bruta" que inclui todos os sinais de modulação, cabeçalhos de pacotes, correção de erros, etc. a velocidade real das redes 802.11a é de 24 a 27 megabits por segundo, pouco mais de 4 vezes mais rápido que no 802.11b.

Outra vantagem é que o 802.11a permite um total de 8 canais simultâneos, contra apenas 3 canais no 802.11b. Isso permite que mais pontos de acesso sejam utilizados no mesmo ambiente, sem que haja perda de desempenho.

O grande problema é que o padrão também é mais caro, por isso a primeira leva de produtos vai ser destinada ao mercado corporativo, onde existe mais dinheiro e mais necessidade de redes mais rápidas.

Além disso, por utilizarem uma frequência mais alta, os transmissores 8021.11a também possuem um alcance mais curto, teoricamente metade do alcance dos transmissores 802.11b, o que torna necessário usar mais pontos de acesso para cobrir a mesma área, o que contribui para aumentar ainda mais os custos.

A diferença de custo vai se manter por um ou dois anos. É de se esperar então que as redes de 11 megabits continuem se popularizando no mercado doméstico, enquanto as de 54 megabits ganhem terreno no mercado corporativo, até que um dia o preço dos dois padrões se nivele e tenhamos uma transição semelhante à das redes Ethernet de 10 para 100 megabits.

Ao contrário do que o nome sugere, o 802.11a é um padrão mais recente do que o 802.11b. Na verdade, os dois padrões foram propostos pelo IEEE na mesma época, mas o 802.11b foi finalizado antes e por isso chegou ao mercado com mais de 6 meses de antecedência. Os primeiros periféricos 802.11a foram lançados em Novembro de 2001.

IEEE 802.11g

Este é um padrão recentemente aprovado pelo IEEE, que é capaz de transmitir dados a 54 megabits, assim como o 802.11a.

A principal novidade é que este padrão utiliza a mesma faixa de frequência do 802.11b atual: 2.4 GHz. Isso permite que os dois padrões sejam intercompatíveis. A idéia é que você possa montar uma rede 802.11b agora e mais pra frente adicionar placas e pontos de acesso 802.11g,

mantendo os componentes antigos, assim como hoje em dia temos liberdade para adicionar placas e hubs de 100 megabits a uma rede já existente de 10 megabits.

A velocidade de transferência nas redes mistas pode ou ser de 54 megabits ao serem feitas transferências entre pontos 802.11g e de 11 megabits quando um dos pontos 801.11b estiver envolvido, ou então ser de 11 megabits em toda a rede, dependendo dos componentes que forem utilizados. Esta é uma grande vantagem sobre o 802.11a, que também transmite a 54 megabits, mas é incompatível com os outros dois padrões.

Os primeiros produtos baseados no 802.11g devem chegar ao mercado apartir do final de 2002, um ano depois da primeira leva do 802.11a, que é o concorrente direto. Isso significa que a popularidade do 802.11g será determinada pelo sucesso do concorrente. Se o 802.11a for rapidamente adotado e chegar a substituir o 802.11b até lá, os periféricos 802.11g terão pouca chance e talvez nem cheguem a ser lançados, já que seria uma guerra perdida.

Se por outro lado a maioria dos usuários preferir os dispositivos 802.11b, então o 802.11g terá chances de dominar o mercado.

Home PNA

Este é um padrão para transmissão de dados através de cabos telefônicos comuns a curtas distâncias. A idéia é que os usuários interessados em montar uma rede doméstica mas que não tenham como passar cabos de rede pela casa, possam aproveitar as extensões telefônicas já existentes para ligar seus micros em rede. Existem duas versões deste padrão: a versão 1.0, já obsoleta, transmite a apenas 1 mbps, muito pouco se comparado às redes Ethernet, enquanto a versão 2.0 já transmite a 10 mbps, uma velocidade próxima à das redes 802.11b.

Os dispositivos Home PNA utilizam uma arquitetura de rede ponto a ponto, sem a necessidade de usar nenhum tipo de hub ou concentrador e os sinais não interferem com as ligações de voz, nem com os serviços de acesso via ADSL, já que ambos utilizam frequências diferentes.

A distância máxima entre os pontos é de 330 metros e é possível utilizar montar redes de até 50 PCs. É possível conectar mais PCs caso necessário, mais quanto maior o número de PCs, maior o número de colisões de pacotes e pior o desempenho.

O uso do Home PNA só é viável caso você já possua extensões telefônicas para todos os PCs, caso contrário, fio por fio seria mais vantajoso usar as velhas redes Ethernet, que são mais rápidas e mais baratas.

Em termos de custo, temos uma faixa intermediária entre as redes Ethernet e as redes Wireless. Nos EUA cada placa PCI custa de 40 a 60 dólares, dependendo do modelo, menos da metade do preço das placas 802.11b, mas ainda um pouco salgado. Aqui no Brasil estes produtos ainda não são muito comuns, mas os preços não são muito mais altos que isto. Além dos PCI, existem também alguns modelos USB, que são um pouco mais caros.

Como esta é uma tecnologia destinada a usuário domésticos, o mais comum é os fabricantes oferecerem os produtos na forma de kits, com duas placas de rede, ao invés de vendê-los de forma unitária:

Kit com placas Home PNA

Fora a praticidade de poder utilizar as extensões telefônicas, as redes Home PNA não oferecem vantagens sobre as redes Ethernet e por isso não são difundidas quanto as redes sem fio. Apesar disso, as placas são relativamente baratas, o que deve garantir a sobrevivência do padrão pelo menos até que as redes sem fio tornem-se mais acessíveis.

Caso você se decida por este padrão, não deixe de prestar atenção se está comprando placas de 1 ou de 10 megabits. Apesar de não serem mais produzidas, ainda existe oferta de placas de 1 megabit, que são suficientes apenas para compartilhar a conexão com a Internet e transferir pequenos arquivos, caso você não tenha pressa. É possível misturar placas de 1 e 10 megabits na mesma rede mas, neste caso, as placas de 10 megabits passarão a trabalhar a apenas 1 megabit para manter compatibilidade com as placas mais lentas.

HomePlug Powerline

Este é mais uma tecnologia que segue a idéia de utilizar os cabos que já temos em casa ao invés de instalar mais cabos para a rede.

Mas, enquanto o HomePNA permite usar as extensões telefônicas, o HomePlug permite utilizar a própria fiação elétrica da casa, algo ainda mais prático.

Apesar dos cabos elétricos não serem exatamente um meio adequado para a transmissão de dados, o HomePlug permite velocidades mais altas que o 802.11b e o HomePNA, 20 megabits no total ou 14 megabits reais, descontando o protocolo de correção de erros utilizado para garantir a confiabilidade das transmissões através de um meio tão hostil quanto os cabos elétricos.

Descontando todas as perdas com as várias camadas de modulação e protocolos, temos velocidades de transmissão de dados de 8 a 9 megabits, uma marca respeitável, que supera por uma boa margem os 7 megabits reais das redes Ethernet de 10 megabits.

O padrão HomePlug 1.0 foi estabelecido em Julho de 2001 e os primeiros produtos começaram a ser lançados em Novembro ou seja, estamos falando de um padrão bastante novo.

Não existe um número máximo de dispositivos que podem ser adicionados à rede, mas a banda é compartilhada entre todos os dispositivos. Quanto mais dispositivos, pior será o desempenho.

O maior problema do HomePlug é que os sinais da rede se propagam por toda a instalação elétrica até o transformador da rua. Isto é um problema sobretudo em apartamentos e conjuntos residenciais, onde é comum cada prédio ou bloco compartilhar o mesmo transformador. Caso um número grande de moradores resolvesse usar redes HomePlug, sem dúvida a velocidade de transmissão decairia bastante.

Para garantir pelo menos a privacidade dos usuários, o padrão utiliza o algoritmo de encriptação DES, que utiliza chaves de 56 bits, razoavelmente seguras para os padrões atuais.

Cada interface HomePlug custa em média 100 dólares, apesar de haver perspectiva de queda para os próximos meses, já que o padrão ainda é muito novo. A tendência é que o sistema se mantenha mais barato que o 802.11b, já que não é necessário utilizar pontos de acesso, os transmissores são mais baratos e não é necessário usar a antena que responde por boa parte dos custo das placas 802.11b

Ainda é muito cedo para dizer se o HomePlug será capaz de conquistar seu espaço competindo diretamente com as redes sem fio, mas sem dúvida o padrão tem potencial para tornar-se uma alternativa viável, principalmente considerando que já está em desenvolvimento o padrão 2.0, que aumentará a velocidade de transmissão para 100 megabits.

HomeRF

O HomeRF é mais um padrão de redes sem fio que utiliza a faixa dos 2.4 GHz, mas que acabou levando a pior com o lançamento do 802.11b.

O Home RF utiliza um protocolo chamado Shared Wireless Access Protocol, onde as interfaces de rede se comunicam diretamente, sem o uso de um ponto de acesso. Isto diminui o custo da rede, mas também compromete o alcance do sinal, que é de (em condições ideais) apenas 50 metros. É possível criar redes HomeRF com até 127 nós, mas como o mesmo canal é compartilhado por todos, quanto mais nós mais baixa será a velocidade. O ideal seria criar redes com no máximo 10 nós, segundo o recomendado pelos próprios fabricantes.

A idéia original era que o HomeRF fosse um padrão de redes sem fio de baixo custo, o que não se concretizou, já que no auge do padrão as placas não custavam menos de 100 dólares a unidade. Até aí não temos nenhuma grande desvantagem, já que mesmo hoje em dias as interfaces 802.11b custam nesta faixa de preço (sem incluir o ponto de acesso), o grande problema é que além de tudo o padrão HomeRF também é mais lento. Apenas 1.6 megabits.

Na época em que foi lançado esta era uma boa marca, já que a versão original do IEEE 802.11 transmitia a apenas 1 megabit e a segunda versão, que já utilizava modo DSSS atingia apenas 2 megabits. Como o preço das placas 802.11 era mais alto na época, o HomeRF tinha tudo para conquistar seu espaço. Foi então que surgiu o padrão 802.11b, que além de ser mais rápido,

conseguiu uma razoável aceitação, permitindo que os fabricantes produzissem os componentes em maior quantidade e baixassem os preços.

O HomeRF é um padrão quase esquecido, mas que pode voltar a ser usado em aparelhos de telefone sem fio e outros dispositivos de comunicação, já que o padrão permite a transmissão de 4 chamadas de voz simultâneas

Bluetooth

O Bluetooth é uma tecnologia de transmissão de dados via sinais de rádio de alta freqüência, entre dispositivos eletrônicos próximos, que vem sendo desenvolvida num consórcio, que originalmente incluía a Ericsson, IBM, Nokia, Toshiba e Intel.

A distância ideal é de no máximo 10 metros e a distância máxima é de 100 metros. Um dos trunfos da é a promessa de transmissores baratos e pequenos o suficiente para serem incluídos em praticamente qualquer tipo de dispositivo, começando por notebooks, celulares e micros de mão, passando depois para micros de mesa, mouses, teclados, joysticks, fones de ouvido, etc. Já tem gente imaginando um "admirável mundo novo Bluetooth" onde tudo estaria ligado entre sí e à Internet, onde a cafeteira poderia ligar para o seu celular para avisar que o café acabou, ou a geladeira te mandar um mail avisando que está sem gelo... sinceramente acho que existem usos mais úteis para essa tecnologia, mas tem louco pra tudo... :-)

A grande vantagem do Bluetooth é o fato de ser um padrão aberto e livre de pagamento de royalties, o que vem levando muitos fabricantes a se interessar pela tecnologia.

As especificações técnicas do padrão são as seguintes:

Alcance ideal: 10 metros
Alcance máximo: 100 metros (em condições ideais e com ambos os transmissores operado com potência máxima)
Freqüência de operação: 2.4 GHz
Velocidade máxima de transmissão: 1 Mbps
Potência da transmissão: 1 mW a 100 mW

A demora

O Bluetooth foi originalmente anunciado em 1998, como um padrão de transmissão sem fio que poderia ser usado universalmente. De fato, o padrão oferece grandes possibilidades, o problema é que, três anos depois do lançamento do padrão, os dispositivos bluetooth não chegaram às lojas. Afinal, o que houve com o Bluetooth?

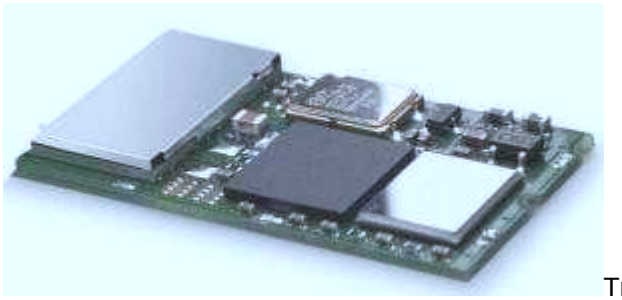
Inicialmente imaginava-se que o Bluetooth poderia ser usado para quase tudo, desde redes sem fio até para conectar periféricos como mouses, teclados, e até mesmo eletrodomésticos entre sí.

Mas, atualmente os fabricantes vêm considerando seu uso para tarefas um pouco mais modestas. A probabilidade de utilizar o Bluetooth como um padrão universal para redes sem fio caiu por terra

com o IEEE 802.11b, que é capaz de manter taxas de transferência de 11 megabits e é capaz de cobrir distâncias maiores, sem falar nos dois sucessores, o 802.11a e o 802.11g

O 802.11b pode ser utilizado para conectar PCs, notebooks e também outros dispositivos de médio porte. O problema fica por conta dos Handhelds, celulares e outros aparelhos pequenos, alimentados por baterias. Os transmissores 802.11b trabalham com um sinal bastante intenso e por isso também consomem muita energia.

O Bluetooth perde feio para o trio em termos de velocidade, pois o padrão é capaz de transmitir a apenas 1 megabit, isto em teoria, já que a velocidade prática cai para apenas 700 Kbits graças aos sinais de controle e modulação. Em compensação, o Bluetooth é uma tecnologia mais barata que o 802.11b. Atualmente os transmissores já custam, para os fabricantes, cerca de 20 dólares por unidade, um quinto do preço de uma placa de rede 802.11b. Outra diferença é que os transmissores bluetooth trabalham com uma potência mais baixa e são menores. Isso permite que eles consumam menos energia, permitindo que sejam usados também em pequenos aparelhos. Os transmissores são bastante compactos, o da foto abaixo por exemplo têm o comprimento de um palito de fósforos. Atualmente existem transmissores ainda menores, com menos de 1 centímetro quadrado.


Transmissor Bluetooth

Com estes dados ja dá para entender por que os fabricantes não estão mais citando o uso do bluetooth em redes sem fio, simplesmente o padrão não tem condições de competir neste segmento. A idéia agora é usar as redes Ethernet ou o 802.11b para ligar os PCs e notebooks em rede e o bluetooth como um complemento para conectar periféricos menores, como Handhelds, celulares, e até mesmo periféricos de uso pessoal, como teclados, mouses, fones de ouvido, etc.

O Bluetooth serviria então como uma opção às interfaces USB, seriais e paralelas para a conexão de periféricos. De fato, a velocidade permitida pelo Bluetooth é bem mais baixa que a das interfaces USB, estamos falando de 12 megabits contra apenas 1 megabit.

Mais um dado interessante é que a Intel vem tentando incentivar os fabricantes a abandonar o uso das interfaces seriais, paralelas, PS/2 e até mesmo do bom e velho drive de disquetes, substituindo todos estes periféricos por similares USB ou bluetooth. Esta mudança poderia finalmente possibilitar a adoção em massa do bluetooth, o que de certa forma seria bem vindo já que seria um meio muito mais simples de sincronizar dados com o palm, transferir as fotos da câmera digital, etc. não seria mais preciso instalar cabos, apenas deixar o periférico próximo do PC.

Mas, para isso ainda faltam resolver dois problemas.

Em primeiro lugar, falta a padronização definitiva do Bluetooth. O padrão 1.0 possuía vários

problemas o que levou os fabricantes a trabalharem no padrão 1.1, que promete ser o definitivo. O padrão 1.1 foi estabelecido recentemente e não oferece compatibilidade com periféricos do padrão antigo. Para complicar, não existe a certeza de que não haverão novas mudanças no padrão.

Além disso, existe o problema do preço. Atualmente os transmissores bluetooth ainda custam na casa dos 20 dólares. Segundo os fabricantes, seria necessário que o valor caísse para algo próximo de 5 dólares por transmissor para que fosse viável incluir transmissores bluetooth em todos os periféricos. O valor vai continuar caindo conforme a tecnologia avança, mas pode demorar mais dois anos até que chegue até este patamar.

Usos para o Bluetooth

Esta é a parte futurista deste tópico. Imagine que aplicações poderão surgir ao combinarmos a natural miniaturização dos componentes e a possibilidade de conectá-los sem fios uns aos outros.

Cada aparelho têm uma certa função, mas ao interligá-los novas utilidades podem surgir, da mesma forma que novas idéias surgem quando várias pessoas trabalham em conjunto.

O celular permite realizar chamadas de voz e acessar a Internet. Mas, sua funcionalidade não é perfeita. Para atender uma chamada é necessário tirá-lo do bolso e o acesso à Web é extremamente limitado, graças ao pequeno tamanho da tela e da pequena capacidade de processamento do aparelho.

Um Palm (ou outro Handheld qualquer) tem bem mais recursos que o celular, mas ao mesmo tempo não tem acesso à Web. Existem alguns aparelhos que tentam juntar as duas coisas, o que acaba resultando num celular bem maior que o habitual que traz um Palm embutido.

Mas, caso os dois aparelhos viessem equipados com transmissores bluetooth seria possível acessar a Web através do Palm, com muito mais recursos que no celular, utilizando sem precisar tirar o celular do bolso. Como apartir dos próximos meses teremos celulares 2.5G (e no futuro os 3G) que ficarão continuamente conectados à Web, a parceria seria muito bem vinda.

Imaginando que este Palm do futuro tivesse memória suficiente, ele poderia ser usado também para gravar as chamadas de voz, servir como secretária eletrônica e outros recursos semelhantes.

Podemos agora adicionar um terceiro dispositivo, um fone de ouvido. Este fone, estaria ligado tanto ao celular quando ao Palm. Existem transmissores bluetooth pequenos o suficientes para serem usados num fone de ouvido sem fio. Já existem até alguns produtos, como o da foto:

Fone de ouvido Bluetooth

Este fone de ouvido com microfone permitiria adicionar mais recursos aos outros dois aparelhos. Seria possível tanto ouvir músicas em MP3 e gravar notas de voz através da conexão com o Palm, quanto usá-lo para atender as chamadas no celular. É possível imaginar mais funções, como por exemplo acessar dados na agenda de compromissos do Palm através de comandos de voz. Seria estranho sair falando sozinho no meio da rua, mas é mais uma possibilidade, enfim.

Temos aqui o que pode ser chamada de PAN ou Personal Area Network, uma rede pessoal, entre os dispositivos que carrega nos bolsos.

Ao chegar em casa, o Palm automaticamente formaria uma rede com o PC. Isso permitiria configurá-lo para automaticamente fazer o sincronismo periodicamente, sem a necessidade do velho ritual de colocá-lo no cradle, apertar o botão e esperar. Seria possível também programar outros tipos de tarefas.

Se você tivesse uma câmera digital existiria a possibilidade de transferir automaticamente as fotos para o PC ou o Palm, ou mesmo enviá-las via e-mail ou salvá-las num disco virtual usando a conexão do celular.

Estes claro são alguns exemplos, existem muitas outras aplicações possíveis aqui. A idéia seria fazer todas as conexões que seriam possíveis utilizando fios mas de uma forma bem mais prática. Se realmente conseguirem produzir transmissores bluetooth por 5 dólares cada um, isto tem uma grande possibilidade de acontecer.

Veja que entre as aplicações que citei, não estão planos de criar redes usando apenas o bluetooth, o padrão é muito lento para isto. Ele serviria no máximo para compartilhar a conexão com a Web entre dois PCs próximos e compartilhar pequenos arquivos. Para uma rede mais funcional seria preciso apelar para os cabos de rede ou um dos padrões de rede sem fio que citei há pouco, que são mais rápidos e têm um alcance maior que o bluetooth.

Finalmente, outra área em que o Bluetooth será muito útil é nas Internet Appliances. Se você nunca ouviu o termo, estes são periféricos que oferecem alguma funcionalidade relacionada à Web. O conceito pode ser usado para adicionar recursos à maioria dos eletrodomésticos, mas algum tipo de conexão sem fio é essencial para tudo funcionar.

Na casa do futuro é fácil imaginar um PC servindo como servidor central, concentrando recursos que vão desde espaço em disco e conexão à web até poder de processamento. Todos os outros dispositivos podem utilizar os recursos do servidor.

Veja o caso do aparelho de som por exemplo. Ao ser conectado ao PC passa a ser possível reproduzir as músicas em MP3 armazenadas nele, sem a necessidade de transferi-las antes para o aparelho. Com isso, cortamos custos, já que o aparelho de som não precisará de memória flash ou muito menos de um HD para armazenar as músicas. Com a centralização, todos os eletrodomésticos poderão ser controlados remotamente. Se o PC ficar conectado continuamente à Web (quem sabe via fibra óptica, já que estamos imaginando alguns anos à frente) será possível controlar tudo de qualquer lugar, usando o celular ou outro dispositivo com conexão à web.

O interessante é que não estamos falando de um grande aumento no custo do aparelhos. Como eles não precisarão nem de muita memória nem de um processador sofisticado, já que tudo será processado pelo PC central, bastarão os sensores necessários, um chip de controle simples e o transmissor bluetooth. Presumindo que o transmissor custe os 5 dólares prometidos pelos fabricantes, teríamos um aumento de preço em torno de 15 dólares por aparelho, algo aceitável se alguém tiver boas idéia para adicionar funcionalidade à cada um.

Como funciona o Bluetooth

Numa rede Bluetooth, a transmissão de dados é feita através de pacotes, como na Internet. Para evitar interferências e aumentar a segurança, existem 79 canais possíveis (23 em alguns países onde o governo reservou parte das freqüências usadas). Os dispositivos Bluetooth têm capacidade de localizar dispositivos próximos, formando as redes de transmissão, chamadas de piconet. Uma vez estabelecida a rede, os dispositivos determinam um padrão de transmissão, usando os canais possíveis. Isto significa que os pacotes de dados serão transmitidos cada um em um canal diferente, numa ordem que apenas os dispositivos da rede conhecem.

Isto anula as possibilidades de interferência com outros dispositivos Bluetooth próximos (assim como qualquer outro aparelho que trabalhe na mesma freqüência) e torna a transmissão de dados mais segura, já que um dispositivo "intruso", que estivesse próximo, mas não fizesse parte da rede simplesmente não compreenderia a transmissão. Naturalmente existe também um sistema de verificação e correção de erros, um pacote que se perca ou chegue corrompido ao destino será retransmitido, assim como acontece em outras arquiteturas de rede.

Para tornar as transmissões ainda mais seguras, o padrão inclui também um sistema de criptografia. Existe também a possibilidade de acrescentar camadas de segurança via software, como novas camadas de criptografia, autenticação, etc.

Consumo elétrico

Os dispositivos Bluetooth possuem um sistema de uso inteligente da potência do sinal. Se dois dispositivos estão próximos, é usado um sinal mais fraco, com o objetivo de diminuir o consumo elétrico, se por outro lado eles estão distantes, o sinal vai ficando mais forte, até atingir a potência máxima.

Dentro do limite dos 10 metros ideais, o consumo de cada transmissor fica em torno de 50 micro ampères, algo em torno de 3% do que um celular atual, bem menos do que outras tecnologias

sem fio atuais. O baixo consumo permite incluir os transmissores em notebooks, celulares e handhelds sem comprometer muito a autonomia das baterias.

Gigabit Ethernet

Depois dos padrões de 10 e 100 megabits, o passo natural para as redes Ethernet seria novamente multiplicar por 10 a taxa de transmissão, atingindo 1000 megabits. E foi justamente o que fizeram :-)

O padrão Gigabit Ethernet começou a ser desenvolvido pelo IEEE em 1997 e acabou se ramificando em quatro padrões diferentes.

O **1000BaseLX** é o padrão mais caro, que suporta apenas cabos de fibra óptica e utiliza a tecnologia long-wave laser, com laseres de 1300 nanômetros. Apesar de, em todos os quatro padrões a velocidade de transmissão ser a mesma, 1 gigabit, o padrão 1000Base-LX é o que atinge distâncias maiores. Usando cabos de fibra óptica com núcleo de 9 mícrons o sinal é capaz de percorrer distâncias de até 5 KM, enquanto utilizando cabos com núcleo de 50 ou 62.5 mícrons, com frequências de respectivamente 400 e 500 MHz, que são os padrões mais baratos, o sinal percorre 550 metros.

O segundo padrão é o **1000BaseSX** que também utiliza cabos de fibra óptica, mas utiliza uma tecnologia de transmissão mais barata, chamada short-wave laser, que é uma derivação da mesma tecnologia usada em CD-ROMs, com feixes de curta distância. Justamente por já ser utiliza em diversos dispositivos, esta tecnologia é mais barata, mas em em compensação o sinal também é capaz de atingir distâncias menores.

Existem quatro padrões de laseres para o 1000BaseSX. Com laseres de 50 mícrons e frequência de 500 MHz, o padrão mais caro, o sinal é capaz de percorrer os mesmos 550 metros dos padrões mais baratos do 1000BaseLX. O segundo padrão também utiliza laseres de 50 mícrons, mas a frequência cai para 400 MHz e a distância para apenas 500 metros.

Os outros dois padrões utilizam laseres de 62.5 mícrons e frequências de 200 e 160 MHz, por isso são capazes de atingir apenas 275 e 220 metros, respectivamente.

Para distâncias mais curtas existe o **1000BaseCX**, que ao invés de fibra óptica utiliza cabos twiaxiais, um tipo de cabo coaxial com dois fios, que tem a aparência de dois cabos coaxiais grudados. Este padrão é mais barato que os dois anteriores, mas em compensação o alcance é de apenas 25 metros. A idéia é que ele servisse para interligar servidores em data centers, que estivessem no mesmo rack, ou em racks próximos.

Mas, o padrão que está crescendo mais rapidamente, a ponto de quase condenar os demais ao desuso é o **1000BaseT**, também chamado de Gigabit over copper, por utilizar os mesmos cabos de par trançado categoria 5 que as redes de 100 megabits atuais. Isto representa uma enorme economia, não apenas por eliminar a necessidade de trocar os cabos atuais por cabos muito mais caros, mas também nas próprias placas de rede, que passam a ser uma evolução das atuais e não uma tecnologia nova. O alcance continua sendo de 100 metros e os switchs compatíveis com o padrão são capazes de combinar nós de 10, 100 e 1000 megabits, sem que os mais lentos atrapalhem os demais.

Toda esta flexibilidade torna uma eventual migração para o 1000BaseT relativamente simples, já que você pode aproveitar o cabeamento já existente. Na verdade, muita pouca coisa muda. Note que apesar dos cabos serem os mesmos, o 1000BaseT faz um uso muito mais intensivo da capacidade de transmissão e por isso detalhes como o comprimento da parte destrançada do cabo para o encaixe do conector, o nível de interferência no ambiente, cabos muito longos, etc. são mais críticos. Com um cabeamento ruim, o índice de pacotes perdidos será muito maior do que numa rede de 100 megabits.

Todos estes padrões de Gigabit Ethernet são intercompatíveis apartir da camada Data Link do modelo OSI. Abaixo da Data Link está apenas a camada física da rede, que inclui o tipo de cabos e o tipo de modulação usado para transmitir dados através deles. Os dados transmitidos, incluindo camadas de correção de erro, endereçamento, etc. são idênticos em qualquer um dos padrões. Assim como muitos hubs, inclusive modelos baratos permitem juntar redes que utilizam cabos de par trançado e cabo coaxial, é muito simples construir dispositivos que permitam interligar estes diferentes padrões.

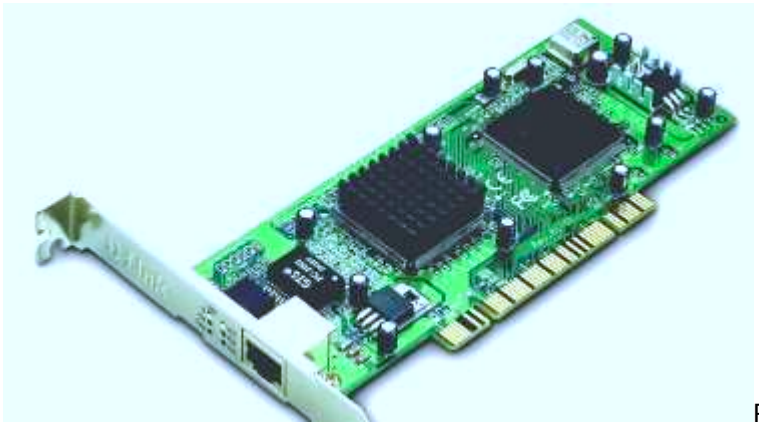
Isto permite interligar facilmente seguimentos de rede com cabeamento e cobre e de fibra óptica, que podem ser usados nos locais onde os 100 metros dos cabos cat 5 não são suficientes.

As placas Gigabit Ethernet já estão relativamente acessíveis, custando entre 150 e 500 dólares. Existe um modelo da DLink, o DGE550T (Gigabit over copper). que já custa abaixo dos 100 dólares, mas naturalmente tudo nos EUA. Os switchs continuam sendo o equipamento mais caro, custando na casa dos 1000 dólares (Janeiro de 2001).

Naturalmente não é uma tecnologia que você utilizaria na sua rede doméstica, até por que existiriam poucas vantagens sobre uma rede tradicional de 100 megabits, mas o ganho de velocidade faz muita diferença nos pontos centrais de grandes redes, interligando os principais servidores, criando sistemas de balanceamento de carga, backup, etc. Outro uso são os clusters de computadores, onde é preciso um link muito rápido para obter o melhor desempenho.

As placas Gigabit Ethernet podem operar tanto no modo full-duplex, onde os dois lados podem transmitir dados simultâneamente, quanto no modo half-duplex. O que determina o uso de um modo ou de outro é novamente o uso de um hub ou de um switch.

Você verá muitas placas anunciadas como capazes de operar a 2 Gigabits, o que nada mais é do que uma alusão ao uso do modo full-duplex. Já que temos 1 Gigabit em cada sentido, naturalmente a velocidade total é de 2 Gigabits. Mas, na prática não funciona bem assim pois raramente ambas as estações precisarão transmitir grandes quantidades de dados. O mais comum é uma relação assimétrica, com uma falando e a outra apenas enviando os pacotes de confirmação, onde o uso do full-duplex traz um ganho marginal.


Placa Gigabit Ethernet, cortesia da DLink

Assim como as placas de 100 megabits, as placas gigabit são completamente compatíveis com os padrões anteriores. Você pode até mesmo ligar uma placa Gigabit Ethernet a um hub 10/100 se quiser, mas a velocidade terá de ser nivelada por baixo, respeitando a do ponto mais lento. Considerando o custo o mais inteligente é naturalmente usar um switch, ou um PC com várias placas de rede para que cada ponto da rede possa trabalhar na sua velocidade máxima.

10 Gigabit Ethernet

O primeiro padrão de redes 10 Gigabit Ethernet, novamente 10 vezes mais rápido que o anterior, está em desenvolvimento desde 1999 e chama-se 10GBaseX. O padrão ainda está em fase de testes, mas deverá ser finalizado ainda na primeira metade de 2002. Daí podemos contar pelo menos mais 4 ou 6 meses até que os primeiros produtos cheguem ao mercado e outros tantos até que comecem a se popularizar.

Este padrão é bastante interessante do ponto de vista técnico, pois além da velocidade, o alcance máximo é de nada menos que 40 KM, utilizando cabos de fibra óptica monomodo. Existe ainda uma opção de baixo custo, utilizando cabos multimodo, mas que em compensação tem um alcance de apenas 300 metros.

O 10 Gigabit Ethernet também representa o fim dos hubs. O padrão permite apenas o modo de operação full-duplex, onde ambas as estações podem enviar e receber dados simultâneamente, o que só é possível através do uso de switchs. Isto encarece mais ainda o novo padrão, mas trás ganhos de desempenho consideráveis, já que além de permitir o uso do modo full-duplex, o uso de um switch acaba com as colisões de pacotes.

Outra mudança importante é que, pelo menos por enquanto, sequer é cogitado o desenvolvimento de um padrão que utilize cabos de cobre, sequer sabe-se se seria possível. Mas, isto não é conclusivo, pois os padrões iniciais do Gigabit também traziam como opções apenas os cabos de fibra óptica. O par trançado veio apenas em 99, dois anos depois.


Placa 10 Gigabit, cortesia da Cisco

O 10 Gigabit não se destina a substituir os padrões anteriores, pelo menos a médio prazo. A idéia é complementar os padrões de 10, 100 e 1000 megabits, oferecendo uma solução capaz e interligar redes distantes com uma velocidade comparável aos backbones DWDM, uma tecnologia muito mais cara, utilizada atualmente nos backbones da Internet.

Suponha por exemplo que você precise interligar 5.000 PCs, divididos entre a universidade, o parque industrial e a prefeitura de uma grande cidade. Você poderia utilizar um backbone 10 Gigabit Ethernet para os backbones principais, unindo os servidores dentro dos três blocos e os interligando à Internet, usar uma malha de switchs Gigabit Ethernet para levar a rede até as salas, linhas de produção e salas de aula e usar hubs 10/100 para levar a rede até os alunos e funcionários, talvez complementando com alguns pontos de acesso 802.11b para oferecer também uma opção de rede sem fio.

Isto estabelece uma pirâmide, onde os usuários individuais possuem conexões relativamente lentas, de 10 ou 100 megabits, interligadas entre sí e entre os servidores pelas conexões mais rápidas e caras, um sistema capaz de absorver várias chamadas de videoconferência simultâneas por exemplo.

Tanto o Gigabit quanto o 10 Gigabit sinalizam que as redes continuarão a ficar cada vez mais rápidas e mais acessíveis. Hoje em dia é possível comprar uma placa 10/100 por menos de 30 reais e, com o barateamento dos novos padrões, estes preços não voltarão a subir. Com as redes tão baratas, aplicações que estavam fora de moda, como os terminais diskless, terminais gráficos, etc. voltaram a ser atrativas.

Os PCs continuam relativamente caros, mas a banda de rede está muito barata. Com isto, começa a fazer sentido aproveitar PCs antigos, transformando-os em terminais de PCs mais rápidos. Um único Pentium III ou Duron pode servir 5, 10 ou até mesmo 20 terminais 486 e com um desempenho muito bom, já que os aplicativos rodam no servidor, não nos terminais. Veremos como colocar esta idéia em prática mais adiante.

Ponto a ponto x cliente - servidor

Seguramente, a polêmica em torno de qual destas arquiteturas de rede é melhor, irá continuar durante um bom tempo. Centralizar os recursos da rede em um servidor dedicado, rodando um sistema operacional de rede, como um Windows NT Server ou Novell Netware, garante uma maior segurança para a rede, garante um ponto central para arquivos; e ao mesmo tempo, oferece uma proteção maior contra quedas da rede, pois é muito mais difícil um servidor dedicado travar ou ter algum problema que o deixe fora do ar, do que um servidor de arquivos não dedicado, rodando o Windows 95, e operado por alguém que mal sabe o efeito de apertar “Ctrl+Alt+Del” :)

Por outro lado, uma rede cliente - servidor é mais difícil de montar e configurar (certamente é muito mais fácil compartilhar arquivos e impressoras no Windows 98 do que configurar permissões de acesso no Novell Netware...) e, na ponta do lápis, acaba saindo muito mais cara, pois além das estações de trabalho, teremos que montar um servidor, que por exigir um bom poder de processamento não sairá muito barato.

Um consenso geral é que para redes pequenas e médias, de até 40 ou 50 micros, onde a segurança não seja exatamente uma questão vital, uma rede ponto a ponto é geralmente a melhor escolha. Em redes maiores, o uso de servidores começa a tornar-se vantajoso.

Cliente - servidor

Montando uma rede cliente-servidor, concentraremos todos os recursos da rede no ou nos servidores. Arquivos, impressoras, serviços de fax e acesso à Internet, etc. tudo será controlado pelos servidores. Para isso, teremos que instalar um sistema operacional de rede no servidor. Existem vários sistemas no mercado, sendo os mais usados atualmente o Windows 2000 Server, Windows NT 4 Server, Novell Netware e versões do Linux.

Em todos os sistemas é preciso um pouco de tempo para configurar as permissões de acesso aos recursos, senhas, atributos, etc. mas, em compensação, uma vez que tudo estiver funcionando você terá uma rede muito mais resistente à tentativas de acesso não autorizado.

Como já vimos, existem vários tipos de servidores, classificados de acordo com o tipo de recurso que controlam. Temos servidores de disco, servidores de arquivos, servidores de impressão, servidores de acesso à Internet., etc.

Servidores de disco

Os servidores de disco foram bastante utilizados em redes mais antigas, onde (para cortar custos) eram utilizadas estações de trabalho sem disco rígido. O disco rígido do servidor era então disponibilizado através da rede e utilizado pelas estações. Todos os programas e dados usados pelos micros da rede, incluindo o próprio sistema operacional de cada estação, eram armazenados no servidor e acessados através da rede.

Neste tipo de rede, instalamos placas de rede com chips de boot nas estações. Nestes chips de memória EPROM, ficam armazenadas todas as informações necessárias para que o micro inicialize e ganhe acesso à rede, tornando-se capaz de acessar o disco do servidor e, a partir dele carregar o sistema operacional e os programas. Veja que a estação não solicita os arquivos ao servidor, ela simplesmente solicita uma cópia da FAT e acessa diretamente o disco. Veja o problema em potencial: a cópia da FAT é recebida durante o processo de boot de cada estação, mas durante o dia, vários arquivos do disco serão renomeados, deletados, movidos, novos arquivos serão criados, etc., e a cópia da FAT, de posse da estação, tornar-se-á desatualizada. Se cada vez que houvessem alterações nos arquivos do disco, o servidor tivesse que transmitir uma nova cópia da FAT para todas as estações, o tráfego seria tão intenso que não conseguiríamos fazer mais nada através da rede.

A solução mais usada neste caso era particionar o disco rígido do servidor em vários volumes, um para cada estação. Para armazenar dados que serão acessados por todas as estações, mas não alterados, pode ser criado um volume público apenas para leitura.

Redes baseadas em servidores de disco e estações diskless (sem disco rígido), são utilizáveis apenas em conjunto com sistemas operacionais e programas somente-texto (como no MS-DOS), pois neles é preciso transmitir uma quantidade pequena de dados através da rede. Se fossemos querer rodar um sistema operacional gráfico como o Windows, a rede tornar-se-ia extremamente lenta, pois o tráfego de dados seria gigantesco, congestionando tanto o servidor quanto a rede em sí.

Servidores de arquivos

Muito mais utilizados atualmente, os servidores de arquivos disponibilizam apenas arquivos através da rede e não o disco rígido em sí. A diferença é que cada estação deverá ter seu próprio disco rígido, onde estará instalado seu sistema operacional, e acessará o servidor apenas para buscar arquivos.

Enquanto um servidor de disco simplesmente disponibiliza seu disco rígido dizendo: “Vão, usem a cópia da FAT que dei a vocês e peguem o que quiserem”, num servidor de arquivos a estação dirá qual arquivo quer e o servidor irá busca-lo em seu disco rígido e em seguida transmiti-lo para a estação. Veja que enquanto no primeiro caso a estação acessa diretamente o disco do servidor para pegar o arquivo, no segundo o próprio servidor pega o arquivo e o transmite para a estação.

Como o sistema operacional e a maioria dos programas estarão localizados nos discos rígidos das estações, o tráfego na rede será bem menor e não existirá problema em rodar sistemas operacionais e programas pesados.

Ponto a ponto

Enquanto nas redes cliente - servidor temos o servidor como o ponto central da rede, de onde todos os recursos são acessados, numa rede ponto a ponto todas as estações dividem os recursos e estão no mesmo nível hierárquico, ou seja, todos os micros são ao mesmo tempo estações de trabalho e servidores.

Praticamente qualquer recurso de uma estação de trabalho, arquivos, impressoras, etc. podem ser compartilhados com a rede e acessados a partir de outras estações. A diferença é que não é preciso reservar uma máquina para a tarefa de servidor, a configuração da rede é muito mais simples e rápida e, se por acaso a rede cai, todos os computadores continuam operacionais, apesar de separados. A desvantagens, como vimos, são uma segurança mais frágil contra acesso não autorizado e contra panes nos micros que disponibilizam os recursos.

Servidores não dedicados

Imagine uma rede com 4 micros: O micro 1, operado pelo João que disponibiliza a única impressora da rede, o micro 2, operado pela Renata, que serve como um ponto central de armazenamento dos arquivos na rede, o micro 3, operado pelo Rodrigo, que disponibiliza um CD-ROM (também o único da rede) e o micro 4, operado pelo Rafael, onde está instalado o modem que compartilha sua conexão à Internet.

Todos os micros são servidores, respectivamente de impressão, arquivos, CD-ROM e acesso à Internet. Porém, ao mesmo tempo, todos estão sendo usados por alguém como estação de trabalho. Dizemos então que os 4 micros são servidores não dedicados. Sua vantagem é que (como no exemplo), não precisamos sacrificar uma estação de trabalho, mas em compensação, temos um sistema mais vulnerável. Outro inconveniente é que é preciso manter o micro ligado (mesmo que ninguém o esteja usando), para que seus recursos continuem disponíveis para a rede.

Impressoras de rede

Simplesmente disponibilizar uma impressora a partir de uma estação de trabalho é a forma mais simples e barata de coloca-la à disposição da rede. Este arranjo funciona bem em redes pequenas, onde a impressora não é tão utilizada. Mas, se a impressora precisar ficar imprimindo a maior parte do tempo, será difícil para quem está usando o micro da impressora conseguir produzir alguma coisa, já que usando o Windows 95/98 o micro fica bastante lento enquanto está imprimindo.

Neste caso, talvez fosse melhor abandonar a idéia de um servidor de impressão não dedicado, e reservar um micro para ser um servidor dedicado de impressão. Neste caso, o micro não precisa ser lá grande coisa, qualquer 486 com espaço em disco suficiente para instalar o Windows 95 (e mais uns 80 ou 100 MB livres para armazenar os arquivos temporários do spooler de impressão) dará conta do recado. Coloque nele um monitor monocromático, deixe-o num canto da sala sempre ligado e esqueça que ele existe :-)

Outra opção seria usar um dispositivo servidor de impressão. Estas pequenas caixas possuem seu próprio processador, memórias e placa de rede, substituindo um servidor de impressão. As vantagens deste sistema são a praticidade e o custo, já que os modelos mais simples custam em torno de 200 - 250 dólares. Um bom exemplo de dispositivos servidores de impressão são os JetDirect da HP. Basta conectar o dispositivo à rede, conectá-lo à impressora e instalar o programa cliente nos micros da rede que utilizarão a impressora. Para maiores informações sobre os JetDirect, consulte o site da HP, http://www.hp.com/net_printing

Finalmente, você poderá utilizar uma impressora de rede. Existem vários modelos de impressoras especiais para este fim, que tem embutida uma placa de rede, processador e memória RAM, ou seja, “vem com um JetDirect embutido”. Normalmente apenas as impressoras a Laser mais caras (a HP Laser Jet 8500 N por exemplo) possuem este recurso, por isso, na maioria dos casos as duas primeiras opções são mais viáveis para a sua pequena rede.

Protocolos

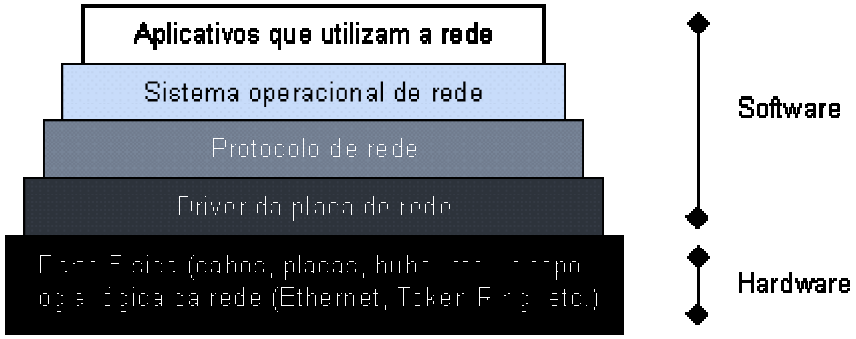
Toda a parte física da rede: cabos, placas, hubs, etc., serve para criar um meio de comunicação entre os micros da rede, como o sistema telefônico ou os correios, que permitem que você comunique-se com outras pessoas. Porém, assim como para que duas pessoas possam falar pelo telefone é preciso que ambas falem a mesma língua, uma saiba o número da outra, etc. para que dois computadores possam se comunicar através da rede, é preciso que ambos usem o mesmo protocolo de rede.

Um protocolo é um conjunto de regras que definem como os dados serão transmitidos; como será feito o controle de erros e retransmissão de dados; como os computadores serão endereçados dentro da rede etc. Um micro com o protocolo NetBEUI instalado, só será capaz de se comunicar através da rede com outros micros que também tenham o protocolo NetBEUI, por exemplo. É possível que um mesmo micro tenha instalados vários protocolos diferentes, tornando-se assim um "poliglota". Graças aos protocolos, também é possível que computadores rodando diferentes sistemas operacionais de rede, ou mesmo computadores de arquiteturas diferentes se comuniquem, basta apenas que todos tenham um protocolo em comum.

O TCP/IP, por exemplo, é um protocolo suportado por praticamente todos os sistemas operacionais. O uso do TCP/IP é que permite o milagre de computadores de arquiteturas totalmente diferentes, como PCs, Macs, Mainframes e até mesmo, telefones celulares e micros de bolso poderem comunicar-se livremente através da Internet.

Camadas da rede

Uma rede é formada por várias camadas. Primeiro temos toda a parte física da rede, incluindo os cabos, hubs e placas de rede. Sobre a parte física temos primeiramente a topologia lógica da rede que, como vimos, é determinada pela própria placa de rede. Em seguida, temos o driver da placa rede que é fornecido pelo fabricante e permite que o sistema operacional possa acessar a placa de rede, atendendo às solicitações do protocolo de rede, o sistema operacional de rede e finalmente os programas. A primeira camada é física, e as demais são lógicas.



Atualmente são usados basicamente 3 protocolos de rede: o NetBEUI, o IPX/SPX e o TCP/IP. Cada um com suas características próprias:

NetBEUI

O NetBEUI é uma espécie de "vovô protocolo", pois foi lançado pela IBM no início da década de 80 para ser usado junto com o IBM PC Network, um micro com configuração semelhante à do PC XT, mas que podia ser ligado em rede. Naquela época, o protocolo possuía bem menos recursos e era chamado de NetBIOS. O nome NetBEUI passou a ser usado quando a IBM estendeu os recursos do NetBIOS, formando o protocolo complexo que é usado atualmente.

No jargão técnico atual, usamos o termo "NetBEUI" quando nos referimos ao protocolo de rede em sí e o termo "NetBIOS" quando queremos nos referir aos comandos deste mesmo protocolo usado pelos programas para acessar a rede.

Ao contrário do IPX/SPX e do TPC/IP, o NetBEUI foi concebido para ser usado apenas em pequenas redes, e por isso acabou tornando-se um protocolo extremamente simples. Por um lado, isto fez que ele se tornasse bastante ágil e rápido e fosse considerado o mais rápido protocolo de rede durante muito tempo. Para você ter uma idéia, apenas as versões mais recentes do IPX/SPX e TCP/IP conseguiram superar o NetBEUI em velocidade.

Mas, esta simplicidade toda tem um custo: devido ao método simples de endereçamento usado pelo NetBEUI, podemos usa-lo em redes de no máximo 255 micros. Além disso, o NetBEUI não suporta enumeração de redes (para ele todos os micros estão ligados na mesma rede). Isto significa, que se você tiver uma grande Intranet, composta por várias redes interligadas por roteadores, os micros que usarem o NetBEUI simplesmente não serão capazes de enxergar micros conectados às outras redes, mas apenas os micros a que estiverem conectados diretamente. Devido a esta limitação, dizemos que o NetBEUI é um protocolo "não roteável"

Apesar de suas limitações, o NetBEUI ainda é bastante usado em redes pequenas, por ser fácil de instalar e usar, e ser razoavelmente rápido. Porém, para redes maiores e Intranets de qualquer tamanho, o uso do TCP/IP é muito mais recomendável.

IPX/ SPX

Este protocolo foi desenvolvido pela Novell, para ser usado em seu Novell Netware. Como o Netware acabou tornando-se muito popular, outros sistemas operacionais de rede, incluindo o Windows passaram a suportar este protocolo. O IPX/SPX é tão rápido quanto o TPC/IP (apesar de não ser tão versátil) e suporta roteamento, o que permite seu uso em redes médias e grandes.

Apesar do Netware suportar o uso de outros protocolos, incluindo o TPC/IP, o IPX/SPX é seu protocolo preferido e o mais fácil de usar e configurar dentro de redes Novell.

Você já deve ter ouvido muito a respeito do Netware, que é o sistema operacional de rede cliente - servidor mais utilizado atualmente.

Além do módulo principal, que é instalado no servidor, é fornecido um módulo cliente, que deve ser instalado em todas as estações de trabalho, para que elas ganhem acesso ao servidor.

Além da versão principal do Netware, existe a versão Personal, que é um sistema de rede ponto a

ponto, que novamente roda sobre o sistema operacional. Esta versão do Netware é bem fácil de usar, porém não é muito popular, pois o Windows sozinho já permite a criação de redes ponto a ponto muito facilmente.

DLC

O DLC é um protocolo usado por muitas instalações Token Ring para permitir a comunicação de PCs com nós de interconexão de mainframe. Alguns modelos antigos de JetDirects da HP, assim como alguns poucos modelos de impressoras de rede também só podem ser acessados usando este protocolo. Apesar de ser necessário instala-lo apenas nestes dois casos, o Windows oferece suporte ao DLC, bastando instala-lo junto com o protocolo principal da rede.

TCP/IP

Uma das principais prioridades dentro de uma força militar é a comunicação, certo? No final da década de 60, esta era uma grande preocupação do DOD, Departamento de Defesa do Exército Americano: como interligar computadores de arquiteturas completamente diferentes, e que ainda por cima estavam muito distantes um do outro, ou mesmo em alto mar, dentro de um porta aviões ou submarino?

Após alguns anos de pesquisa, surgiu o TCP/IP, abreviação de "Transmission Control Protocol/Internet Protocol" ou Protocolo de Controle de Transmissão/Protocolo Internet. O TPC/IP permitiu que as várias pequenas redes de computadores do exército Americano fossem interligadas, formando uma grande rede, embrião do que hoje conhecemos como Internet.

O segredo do TCP/IP é dividir a grande rede em pequenas redes independentes, interligadas por roteadores. Como apesar de poderem comunicar-se entre sí, uma rede é independente da outra; caso uma das redes parasse, apenas aquele segmento ficaria fora do ar, não afetando a rede como um todo. No caso do DOD, este era um recurso fundamental, pois durante uma guerra ou durante um ataque nuclear, vários dos segmentos da rede seriam destruídos, junto com suas respectivas bases, navios, submarinos, etc., e era crucial que o que sobrasse da rede continuasse no ar, permitindo ao comando coordenar um contra ataque. Veja que mesmo atualmente este recurso continua sedo fundamental na Internet, se por exemplo o servidor do Geocities cair, apenas ele ficará inacessível.

Apesar de inicialmente o uso do TPC/IP ter sido restrito a aplicações militares, com o passar do tempo acabou tornando-se de domínio público, o que permitiu aos fabricantes de software adicionar suporte ao TCP/IP aos seus sistemas operacionais de rede. Atualmente, o TPC/IP é suportado por todos os principais sistemas operacionais, não apenas os destinados a PCs, mas a todas as arquiteturas, inclusive mainframes, minicomputadores e até mesmo celulares e handhelds. Qualquer sistema com um mínimo de poder de processamento, pode conectar-se à Internet, desde que alguém crie para ele um protocolo compatível com o TCP/IP e aplicativos www, correio eletrônico etc. Já tive notícias de um grupo de aficcionados que criou um aplicativo de correio eletrônico e browser para MSX.

Alguns exemplos de sistemas operacionais que suportam o TCP/IP são: o MS-DOS, Windows 3.11,

Windows 95/98/NT/2000/CE, Netware, MacOS, OS/2, Linux, Solaris, a maioria das versões do Unix, BeOS e vários outros.

Voltando à história da Internet, pouco depois de conseguir interligar seus computadores com sucesso, o DOD interligou alguns de seus computadores às redes de algumas universidades e centros de pesquisa, formando uma inter-rede, ou Internet. Logo a seguir, no início dos anos 80, a NFS (National Science Foundation) dos EUA, construiu uma rede de fibra ótica de alta velocidade, conectando centros de supercomputação localizados em pontos chave nos EUA e interligando-os também à rede do DOD. Essa rede da NSF, teve um papel fundamental no desenvolvimento da Internet, por reduzir substancialmente o custo da comunicação de dados para as redes de computadores existentes, que foram amplamente estimuladas a conectar-se ao backbone da NSF, e consequentemente, à Internet. A partir de abril de 1995, o controle do backbone (que já havia se tornado muito maior, abrangendo quase todo o mundo através de cabos submarinos e satélites) foi passado para o controle privado. Além do uso acadêmico, o interesse comercial pela Internet impulsionou seu crescimento, chegando ao que temos hoje.

Endereçamento IP

Dentro de uma rede TCP/IP, cada micro recebe um endereço IP único que o identifica na rede. Um endereço IP é composto de uma seqüência de 32 bits, divididos em 4 grupos de 8 bits cada. Cada grupo de 8 bits recebe o nome de **octeto**.

Veja que 8 bits permitem 256 combinações diferentes. Para facilitar a configuração dos endereços, usamos então números de 0 a 255 para representar cada octeto, formando endereços como 220.45.100.222, 131.175.34.7 etc. Muito mais fácil do que ficar decorando binários.

O endereço IP é dividido em duas partes. A primeira identifica a rede à qual o computador está conectado (necessário, pois numa rede TCP/IP podemos ter várias redes conectadas entre sí, veja o caso da Internet) e a segunda identifica o computador (chamado de host) dentro da rede.

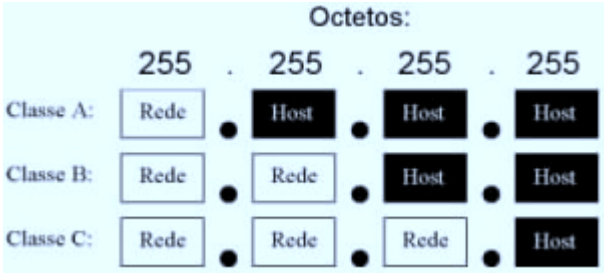
Obrigatoriamente, os primeiros octetos servirão para identificar a rede e os últimos servirão para identificar o computador em sí. Como temos apenas 4 octetos, esta divisão limitaria bastante o número de endereços possíveis. Se fosse reservado apenas o primeiro octeto do endereço por exemplo, teríamos um grande número de hosts, mas em compensação poderíamos ter apenas 256 sub-redes. Mesmo se reservássemos dois octetos para a identificação da rede e dois para a identificação do host, os endereços possíveis seriam insuficientes.

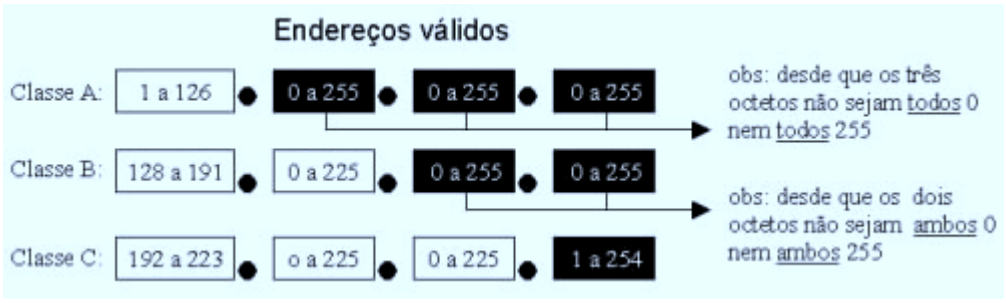
Para permitir uma gama maior de endereços, os desenvolvedores do TPC/IP dividiram o endereçamento IP em cinco classes, denominadas A, B, C, D, e E, sendo que apenas as três primeiras são usadas para fins de endereçamento. Cada classe reserva um número diferente de octetos para o endereçamento da rede:

Na classe A, apenas o primeiro octeto identifica a rede, na classe B são usados os dois primeiros octetos e na classe C temos os três primeiros octetos reservados para a rede e apenas o último reservado para a identificação dos hosts.

O que diferencia uma classe de endereços da outra, é o valor do primeiro octeto. Se for um número entre 1 e 126 (como em 113.221.34.57) temos um endereço de classe A. Se o valor do

primeiro octeto for um número entre 128 e 191, então temos um endereço de classe B (como em 167.27.135.203) e, finalmente, caso o primeiro octeto seja um número entre 192 e 223 teremos um endereço de classe C:





Ao implantar uma rede TCP/IP você deverá analisar qual classe de endereços é mais adequada, baseado no número de nós da rede. Veja que, com um endereço classe C, é possível endereçar apenas 254 nós de rede; com um endereço B já é possível endereçar até 65,534 nós, sendo permitidos até 16,777,214 nós usando endereços classe A. Claro que os endereços de classe C são muito mais comuns. Se você alugar um backbone para conectar a rede de sua empresa à Internet, muito provavelmente irá receber um endereço IP classe C, como 203.107.171.x, onde 203.107.171 é o endereço de sua rede dentro da Internet, e o "x" é a faixa de 254 endereços que você pode usar para identificar seus hosts. Veja alguns exemplos de endereços TCP/IP válidos:

Classe A	105.216.56.185	45.210.173.98	124.186.45.190	89.42.140.202	34.76.104.205	98.65.108.46
Classe B	134.65.108.207	189.218.34.100	156.23.219.45	167.45.208.99	131.22.209.198	190.22.107.34
Classe C	222.45.198.205	196.45.32.145	218.23.108.45	212.23.187.98	220.209.198.56	198.54.89.3

Como você deve ter notado, nem todas as combinações de valores são permitidas. Alguns números são reservados e não podem ser usados em sua rede. Veja agora os endereços IPs inválidos:

Endereço inválido	Por que?
0.xxx.xxx.xxx	Nenhum endereço IP pode começar com zero, pois o identificador de rede 0 é utilizado para indicar que se está na mesma rede, a chamada rota padrão.

127.xxx.xxx.xxx	Nenhum endereço IP pode começar com o número 127, pois este número é reservado para testes internos, ou seja, são destinados à própria máquina que enviou o pacote. Se por exemplo você tiver um servidor de SMTP e configurar seu programa de e-mail para usar o servidor 127.0.0.1 ele acabará usando o próprio servidor instalado máquina :-)
255.xxx.xxx.xxx xxx.255.255.255 xxx.xxx.255.255	Nenhum identificador de rede pode ser 255 e nenhum identificador de host pode ser composto apenas de endereços 255, seja qual for a classe do endereço. Outras combinações são permitidas, como em 65.34.255.197 (num endereço de classe A) ou em 165.32.255.78 (num endereço de classe B).
xxx.0.0.0 xxx.xxx.0.0	Nenhum identificador de host pode ser composto apenas de zeros, seja qual for a classe do endereço. Como no exemplo anterior, são permitidas outras combinações como 69.89.0.129 (classe A) ou 149.34.0.95 (classe B)
xxx.xxx.xxx.255 xxx.xxx.xxx.0	Nenhum endereço de classe C pode terminar com 0 ou com 255, pois como já vimos, um host não pode ser representado apenas por valores 0 ou 255. Os endereços **xxx.255.255.255 xxx.xxx.255.255 e xxx.xxx.xxx.255** são sinais de broadcast que são destinados simultâneamente à todos os computadores da rede. Estes endereços são usados por exemplo numa rede onde existe um servidor DHCP, para que as estações possam receber seus endereços IP cada vez que se conectam à rede.

Se você não pretender conectar sua rede à Internet, você pode utilizar qualquer faixa de endereços IP válidos e tudo irá funcionar sem problemas. Mas, apartir do momento em que você resolver conecta-los à Web os endereços da sua rede poderá entrar em conflito com endereços já usados na Web.

Para resolver este problema, basta utilizar uma das faixas de endereços reservados. Estas faixas são reservadas justamente ao uso em redes internas, por isso não são roteadas na Internet.

As faixas de endereços reservados mais comuns são 10.x.x.x e 192.168.x.x, onde respectivamente o 10 e o 192.168 são os endereços da rede e o endereço de host pode ser configurado da forma que desejar.

O ICS do Windows usa a faixa de endereços 192.168.0.x. Ao compartilhar a conexão com a Web utilizando este recurso, você simplesmente não terá escolha. O servidor de conexão passa a usar o endereço 192.168.0.1 e todos os demais micros que forem ter acesso à Web devem usar endereços de 192.168.0.2 a 192.168.0.254, já que o ICS permite compartilhar a conexão entre apenas 254 PCs.

O default em muitos sistemas é 192.168.1.x, mas você pode usar os endereços que quiser. Se você quiser uma faixa ainda maior de endereços para a sua rede interna, é só apelar para a faixa 10.x.x.x, onde você terá à sua disposição mais de 12 milhões de endereços diferentes.

Veja que usar uma destas faixas de endereços reservados não impede que os PCs da sua rede possam acessar a Internet, todos podem acessar através de um servidor proxy.

Máscara de sub-rede

Ao configurar o protocolo TPC/IP, seja qual for o sistema operacional usado, além do endereço IP é preciso informar também o parâmetro da máscara de sub-rede, ou "subnet mask". Ao contrário do endereço IP, que é formado por valores entre 0 e 255, a máscara de sub-rede é formada por apenas dois valores: 0 e 255, como em 255.255.0.0 ou 255.0.0.0. onde um valor 255 indica a parte endereço IP referente à rede, e um valor 0 indica a parte endereço IP referente ao host.

A máscara de rede padrão acompanha a classe do endereço IP: num endereço de classe A, a máscara será 255.0.0.0, indicando que o primeiro octeto se refere à rede e os três últimos ao host. Num endereço classe B, a máscara padrão será 255.255.0.0, onde os dois primeiros octetos referem-se à rede e os dois últimos ao host, e num endereço classe C, a máscara padrão será 255.255.255.0 onde apenas o último octeto refere-se ao host.

Ex. de endereço IP	Classe do Endereço	Parte referente à rede	Parte referente ao host	Mascara de sub-rede padrão
98.158.201.128	Classe A	98.	158.201.128	255.0.0.0 (rede.host.host.host)
158.208.189.45	Classe B	158.208.	189.45	255.255.0.0 (rede.rede.host.host)
208.183.34.89	Classe C	208.183.34.	89	255.255.255.0 (rede.rede.rede.host)

Mas, afinal, para que servem as máscaras de sub-rede então? Apesar das máscaras padrão acompanharem a classe do endereço IP, é possível "mascarar" um endereço IP, mudando as faixas do endereço que serão usadas para endereçar a rede e o host. O termo "máscara de sub-rede" é muito apropriado neste caso, pois a "máscara" é usada apenas dentro da sub-rede.

Veja por exemplo o endereço 208.137.106.103. Por ser um endereço de classe C, sua máscara padrão seria 255.255.255.0, indicando que o último octeto refere-se ao host, e os demais à rede. Porém, se mantivéssemos o mesmo endereço, mas alterássemos a máscara para 255.255.0.0 apenas os dois primeiros octetos (208.137) continuariam representando a rede, enquanto o host passaria a ser representado pelos dois últimos (e não apenas pelo último).

Ex. de endereço IP	Máscara de sub-rede	Parte referente à rede	Parte referente ao host
208.137.106.103	255.255.255.0 (padrão)	208.137.106.	103
208.137.106.103	255.255.0.0	208.137.	106.103
208.137.106.103	255.0.0.0	208.	137.106.103

Veja que 208.137.106.103 com máscara 255.255.255.0 é diferente de 208.137.106.103 com máscara 255.255.0.0: enquanto no primeiro caso temos o host 103 dentro da rede 208.137.106, no segundo caso temos o host 106.103 dentro da rede 208.137.

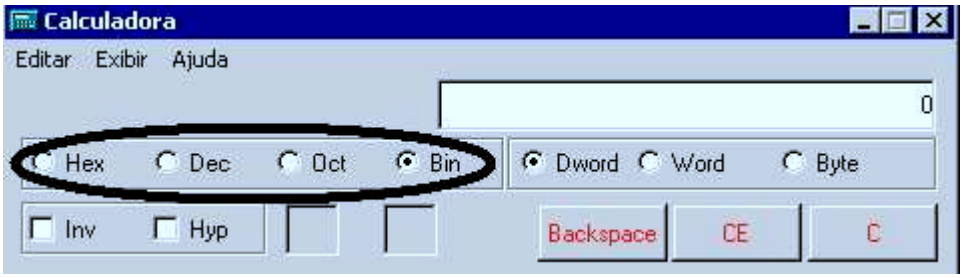
Dentro de uma mesma sub-rede, todos os hosts deverão ser configurados com a mesma máscara de sub-rede, caso contrário poderão não conseguir comunicar-se, pois pensarão estar conectados a redes diferentes. Se, por exemplo, houverem dois micros dentro de uma mesma sub-rede, configurados com os endereços 200.133.103.1 e 200.133.103.2 mas configurados com máscaras diferentes, 255.255.255.0 para o primeiro e 255.255.0.0 para o segundo, teremos um erro de configuração.

Máscaras complexas

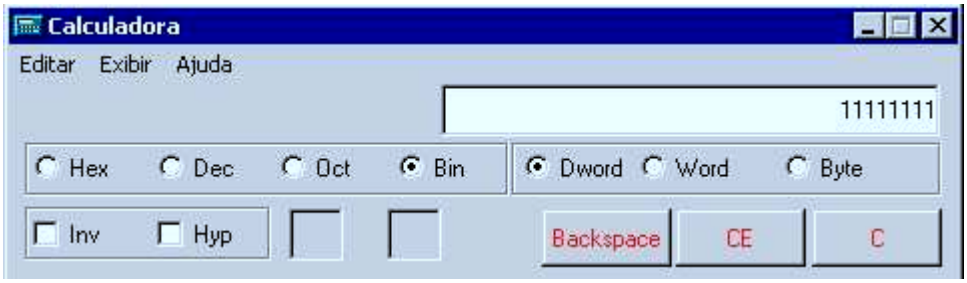
Até agora vimos apenas máscaras de sub-rede simples. Porém o recurso mais refinado das máscaras de sub-rede é quebrar um octeto do endereço IP em duas partes, fazendo com que dentro de um mesmo octeto, tenhamos uma parte que representa a rede e outra que representa o host.

Este conceito é um pouco complicado, mas em compensação, pouca gente sabe usar este recurso, por isso vele à pena fazer um certo esforço para aprender.

Configurando uma máscara complexa, precisaremos configurar o endereço IP usando números binários e não decimais. Para converter um número decimal em um número binário, você pode usar a calculadora do Windows. Configure a calculadora para o modo científico (exibir/científica) e verá que do lado esquerdo aparecerá um menu de seleção permitindo (entre outros) encolher entre decimal (dec) e binário (bin).



Configure a calculadora para binário e digite o número 11111111, mude a opção da calculadora para decimal (dec) e a calculadora mostrará o número 255, que é o seu correspondente em decimal. Tente de novo agora com o binário 00000000 e terá o número decimal 0.



Veja que 0 e 255 são exatamente os números que usamos nas máscaras de sub-rede simples. O número decimal 255 (equivalente a 11111111) indica que todos os 8 números binários do octeto se referem ao host, enquanto o decimal 0 (correspondente a 00000000) indica que todos os 8 binários do octeto se referem ao host.

Mascara de sub-rede simples:

Decimal:	**255**	**255**	**255**	**0**
Binário:	**11111111**	**11111111**	**11111111**	**00000000**
	rede	**rede**	**rede**	**host**

Porém, imagine que você alugou um backbone para conectar a rede de sua empresa à Internet e recebeu um endereço de classe C, 203.107.171.x onde o 203.107.171 é o endereço de sua rede na Internet e o "x" é a faixa de endereços de que você dispõe para endereçar seus micros. Você pensa: "ótimo, só tenho 15 micros na minha rede mesmo, 254 endereços são mais do que suficientes". Mas logo depois surge um novo problema: "droga, esqueci que a minha rede é composta por dois segmentos ligados por um roteador".

Veja a dimensão do problema: você tem apenas 15 micros, e um endereço de classe C permite endereçar até 254 micros, até aqui tudo bem, o problema é que por usar um roteador, você tem na verdade duas redes distintas. Como endereçar ambas as redes, se você não pode alterar o 203.107.171 que é a parte do seu endereço que se refere à sua rede? Mais uma vez, veja que o "203.107.171" é fixo, você não pode alterá-lo, pode apenas dispor do último octeto do endereço.

Este problema poderia ser resolvido usando uma máscara de sub-rede complexa. Veja que dispomos apenas dos últimos 8 bits do endereço IP:

Decimal:	**203**	**107**	**171**	**x**
Binário:	**11001011**	**11010110**	**10101011**	**????????**

Usando uma máscara 255.255.255.0 reservaríamos todos os 8 bits de que dispomos para o endereçamento dos hosts, e não sobraria nada para diferenciar as duas redes que temos.

Mas, se por outro lado usássemos uma máscara complexa, poderíamos "quebrar" os 8 bits do octeto em duas partes. Poderíamos então usar a primeira para endereçar as duas redes, e a segunda parte para endereçar os Hosts:

Decimal:	**203**	**107**	**171**	**x**
Binário:	**11001011**	**11010110**	**10101011**	**???? ????**
	rede	**rede**	**rede**	**rede host**

Para tanto, ao invés de usar a máscara de sub-rede 255.255.255.0 (converta para binário usando a calculadora do Windows e terá 11111111.11111111.11111111.00000000) que, como vimos, reservaria todos os 8 bits para o endereçamento do host, usaremos uma máscara 255.255.255.240 (corresponde ao binário 11111111.111111.11111111.11110000). Veja que numa máscara de sub-rede os números binários "1" referem-se à rede e os números "0" referem-se ao host. Veja que na máscara 255.255.255.240 temos exatamente esta divisão, os 4 primeiros binários do último octeto são positivos e os quatro últimos são negativos.

Máscara de sub-rede:

Decimal:	**255**	**255**	**255**	**240**
Binário:	**11111111**	**11111111**	**11111111**	**1111 0000**
	rede	**rede**	**rede**	**rede host**

Temos agora o último octeto dividido em dois endereços binários de 4 bits cada. Cada um dos dois grupos, agora representa um endereço distinto, e deve ser configurado independentemente. Como fazer isso? Veja que 4 bits permitem 16 combinações diferentes. Se você converter o número 15 em binário terá "1111" e se converter o decimal 0, terá "0000". Se converter o decimal 11 terá "1011" e assim por diante.

Use então endereços de 0 a 15 para identificar os hosts, e endereços de 1 a 14 para identificar a rede. Veja que os endereços 0 e 15 não podem ser usados para identificar o host, pois assim como os endereços 0 e 255, eles são reservados.

Endereço IP:

Decimal	**203**	**107**	**171**	**12 _ 14**
Binário	**11111111**	**11111111**	**11111111**	**1100 1110**
	rede	**rede**	**rede**	**rede host**

Estabeleça um endereço de rede para cada uma das duas sub-redes que temos, e em seguida, estabeleça um endereço diferente para cada micro da rede, mantendo a formatação do exemplo anterior. Por enquanto, apenas anote num papel os endereços escolhidos, junto como seu correspondente em binários.

Quando for configurar o endereço IP nas estações, primeiro configure a máscara de sub-rede como 255.255.255.240 e, em seguida, converta os binários dos endereços que você anotou no papel, em decimais, para ter o endereço IP de cada estação. No exemplo da ilustração anterior, havíamos estabelecido o endereço 12 para a rede e o endereço 14 para a estação; 12 corresponde a "1100" e 14 corresponde a "1110". Juntando os dois temos "11001110" que corresponde ao decimal "206". O endereço IP da estação será então 203.107.171.206.

Se você tivesse escolhido o endereço 10 para a rede a o endereço 8 para a estação, teríamos

"10101000" que corresponde ao decimal 168. Neste caso, o endereço IP da estação seria 203.107.171.168

Caso você queira reservar mais bits do último endereço para o endereço do host (caso tenha mais de 16 hosts e menos de 6 redes), ou então mais bits para o endereço da rede (caso tenha mais de 14 redes e menos de 8 hosts em cada rede).

Máscara de sub-rede	Bits da rede	Bits do host	Número máximo de redes	Número máximo de hosts
240	1111	0000	14 endereços (de 1 a 14)	16 (endereços de 0 a 15)
192	11	000000	2 endereços (2 e 3)	64 (endereços de 0 a 63)
224	111	00000	6 endereços (de 1 a 6)	32 (endereços de 0 a 31)
248	11111	000	30 endereços (de 1 a 30)	8 endereços (de 0 a 7)
252	111111	00	62 endereços (de 1 a 62)	4 endereços (de 0 a 3)

Em qualquer um dos casos, para obter o endereço IP basta converter os dois endereços (rede e estação) para binário, "juntar" os bits e converter o octeto para decimal.

Usando uma máscara de sub-rede 192, por exemplo, e estabelecendo o endereço 2 (ou "10" em binário) para a rede e 47 (ou "101111" em binário) para o host, juntaríamos ambos os binários obtendo o octeto "10101111" que corresponde ao decimal "175".

Se usássemos a máscara de sub-rede 248, estabelecendo o endereço 17 (binário "10001") para a rede e o endereço 5 (binário "101") para o host, obteríamos o octeto "10001101" que corresponde ao decimal "141"

Claro que as instruções acima valem apenas para quando você quiser conectar vários micros à Web, usando uma faixa de endereços válidos. Caso você queira apenas compartilhar a conexão entre vários PCs, você precisará de apenas um endereços IP válido. Neste caso, o PC que está conectado à Web pode ser configurado (usando um Proxy) para servir como portão de acesso para os demais.

Usando o DHCP

Ao invés de configurar manualmente os endereços IP usados por cada máquina, é possível fazer com que os hosts da rede obtenham automaticamente seus endereços IP, assim como sua configuração de máscara de sub-rede e defaut gateway. Isto torna mais fácil a tarefa de manter a rede e acaba com a possibilidade de erros na configuração manual dos endereços IP.

Para utilizar este recurso, é preciso implantar um servidor de DHCP na rede. A menos que sua rede seja muito grande, não é preciso usar um servidor dedicado só para isso: você pode outorgar mais esta tarefa para um servidor de arquivos, por exemplo. O serviço de servidor DHCP pode ser

instalado apenas em sistemas destinados a servidores de rede, como o Windows NT Server, Windows 2000 Server, Novell Netware 4.11 (ou superior) além claro do Linux e das várias versões do Unix.

Do lado dos clientes, é preciso configurar o TCP/IP para obter seu endereço DHCP a partir do servidor. Para fazer isso, no Windows 98 por exemplo, basta abrir o ícone redes do painel de controle, acessar as propriedades do TCP/IP e na guia "IP Address" escolher a opção "Obter um endereço IP automaticamente".

Cada vez que o micro cliente é ligado, carrega o protocolo TCP/IP e em seguida envia um pacote de broadcast para toda a rede, perguntando quem é o servidor DHCP. Este pacote especial é endereçado como 255.255.255.255, ou seja, para toda a rede. Junto com o pacote, o cliente enviará o endereço físico de sua placa de rede.

Ao receber o pacote, o servidor DHPC usa o endereço físico do cliente para enviar para ele um pacote especial, contendo seu endereço IP. Este endereço é temporário, não é da estação, mas simplesmente é "emprestado" pelo servidor DHCP para que seja usado durante um certo tempo. Uma configuração importante é justamente o tempo do empréstimo do endereço. A configuração do "Lease Duration" muda de sistema para sistema. No Windows NT Server por exemplo, pode ser configurado através do utilitário "DHCP Manager".

Depois de decorrido metade do tempo de empréstimo, a estação tentará contatar o servidor DHCP para renovar o empréstimo. Se o servidor DHCP estiver fora do ar, ou não puder ser contatado por qualquer outro motivo, a estação esperará até que tenha se passado 87.5% do tempo total, tentando várias vezes em seguida. Se terminado o tempo do empréstimo o servidor DHCP ainda não estiver disponível, a estação abandonará o endereço e ficará tentando contatar qualquer servidor DHCP disponível, repetindo a tentativa a cada 5 minutos. Porém, por não ter mais um endereço IP, a estação ficará fora da rede até que o servidor DHPC volte.

Veja que uma vez instalado, o servidor DHCP passa a ser essencial para o funcionamento da rede. Se ele estiver travado ou desligado, as estações não terão como obter seus endereços IP e não conseguirão entrar na rede.

Você pode configurar o tempo do empréstimo como sendo de 12 ou 24 horas, ou mesmo estabelecer o tempo como ilimitado, assim a estação poderá usar o endereço até que seja desligada no final do dia, minimizando a possibilidade de problemas, caso o servidor caia durante o dia.

Todos os provedores de acesso à Internet usam servidores DHCP para fornecer dinâmicamente endereços IP aos usuários. No caso deles, esta é uma necessidade, pois o provedor possui uma faixa de endereços IP, assim como um número de linhas bem menor do que a quantidade total de assinantes, pois trabalham sobre a perspectiva de que nem todos acessarão ao mesmo tempo.

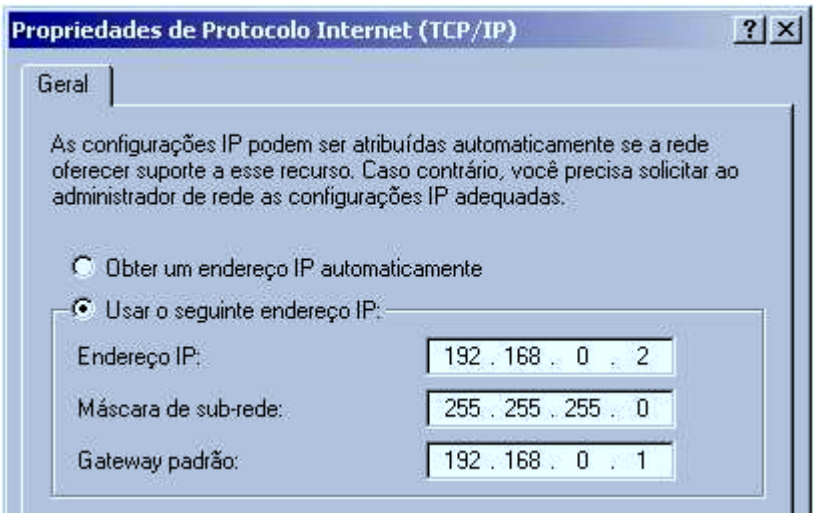
Defaut Gateway

Um rede TCP/IP pode ser formada por várias redes interligadas entre sí por roteadores. Neste caso, quando uma estação precisar transmitir algo a outra que esteja situada em uma rede diferente (isso é facilmente detectado através do endereço IP), deverá contatar o roteador de sua

rede para que ele possa encaminhar os pacotes. Como todo nó da rede, o roteador possui seu próprio endereço IP. É preciso informar o endereço do roteador nas configurações do TCP/IP de cada estação, no campo "defaut gateway", pois sem esta informação as estações simplesmente não conseguirão acessar o roteador e consequentemente as outras redes.

Caso a sua rede seja suficientemente grande, provavelmente também terá um servidor DHCP. Neste caso, você poderá configurar o servidor DHCP para fornecer o endereço do roteador às estações junto com o endereço IP.

Por exemplo, se você montar uma rede domésticas com 4 PCs, usando os endereços IP **192.168.0.1**, **192.168.0.2**, **192.168.0.3** e **192.168.0.4**, e o PC 192.168.0.1 estiver compartilhando o acesso à Web, seja através do ICS do Windows ou outro programa qualquer, as outras três estações deverão ser configuradas para utilizar o Default Gateway 192.168.0.1. Assim, qualquer solicitação fora da rede 192.168.0 será encaminhada ao PC com a conexão, que se encarregará de enviá-la através da Web e devolver a resposta:



Servidor DNS

O DNS (domain name system) permite usar nomes amigáveis ao invés de endereços IP para acessar servidores. Quando você se conecta à Internet e acessa o endereço http://www.guiadohardware.net usando o browser é um servidor DNS que converte o "nome fantasia" no endereço IP real do servidor, permitindo ao browser acessá-lo.

Para tanto, o servidor DNS mantém uma tabela com todos os nomes fantasia, relacionados com os respectivos endereços IP. A maior dificuldade em manter um servidor DNS é justamente manter esta tabela atualizada, pois o serviço tem que ser feito manualmente. Dentro da Internet, temos várias instituições que cuidam desta tarefa. No Brasil, por exemplo, temos a FAPESP. Para registrar um domínio é preciso fornecer à FAPESP o endereço IP real do servidor onde a página ficará hospedada. A FAPESP cobra uma taxa de manutenção anual de R$ 50 por este serviço.

Servidores DNS também são muito usados em Intranets, para tornar os endereços mais amigáveis e fáceis de guardar.

A configuração do servidor DNS pode ser feita tanto manualmente em cada estação, quanto automaticamente através do servidor DHCP. Veja que quanto mais recursos são incorporados à rede, mais necessário torna-se o servidor DHCP.

Servidor WINS

O WINS (Windows Internet Naming Service) tem a mesma função do DNS, a única diferença é que enquanto um servidor DNS pode ser acessado por praticamente qualquer sistema operacional que suporte o TCP/IP, o WINS é usado apenas pela família Windows. Isto significa ter obrigatoriamente um servidor NT e estações rodando o Windows 98 para usar este recurso.

O WINS é pouco usado por provedores de acesso à Internet, pois neste caso um usuário usando o Linux, por exemplo, simplesmente não conseguiria acesso. Normalmente ele é utilizado apenas em Intranets onde os sistemas Windows são predominantes.

Como no caso do DNS, você pode configurar o servidor DHCP para fornecer o endereço do servidor WINS automaticamente.

Redes Virtuais Privadas

Mais um recurso permitido pela Internet são as redes virtuais. Imagine uma empresa que é composta por um escritório central e vários vendedores espalhados pelo país, onde os vendedores precisam conectar-se diariamente à rede do escritório central para atualizar seus dados, trocar arquivos etc. Como fazer esta conexão?

Uma idéia poderia ser usar linhas telefônicas e modems. Mas, para isto precisaríamos conectar vários modems (cada um com uma linha telefônica) ao servidor da rede central, um custo bastante alto, e, dependendo do tempo das conexões, o custo dos interurbanos poderia tornar a idéia inviável. Uma VPN porém, serviria como uma luva neste caso, pois usa a Internet como meio de comunicação.

Para construir uma VPN, é necessário um servidor rodando um sistema operacional compatível com o protocolo PPTP (como o Windows NT 4 Server e o Windows 2000 Server), conectado à Internet através de uma linha dedicada. Para acessar o servidor, os clientes precisarão apenas conectar-se à Internet através de um provedor de acesso qualquer. Neste caso, os clientes podem usar provedores de acesso da cidade aonde estejam, pagando apenas ligações locais para se conectar à rede central.

Também é possível usar uma VPN para interligar várias redes remotas, bastando para isso criar um servidor VPN com uma conexão dedicada à Internet em cada rede.

À princípio, usar a Internet para transmitir os dados da rede pode parecer inseguro, mas os dados transmitidos através da VPN são encriptados, e por isso, mesmo se alguém conseguir interceptar a

transmissão, muito dificilmente conseguirá decifrar os pacotes, mesmo que tente durante vários meses.

Embora seja necessário que o servidor VPN esteja rodando o Windows NT 4 Server, ou o Windows 2000 Server, as estações cliente podem usar o Windows 98, ou mesmo o Windows 95. Uma vez conectado à VPN, o micro cliente pode acessar qualquer recurso da rede, independentemente do protocolo: poderá acessar um servidor Netware usando o IPX/SPX ou um mainframe usando o DLC, por exemplo.

Configurar a rede e compartilhar a conexão

Depois de todas estas páginas de teoria, finalmente chegou a hora de colocar a mão na massa e montar nossa primeira rede. O restante deste livro será dedicado a conhecer as configurações de rede do Windows 95, 98 e 2000, aprender sobre segurança de rede, com algumas dicas práticas e exercitar um pouco nosso poder criativo com alguns exercícios práticos. Uma coisa de cada vez :-)

O primeiro passo para montar uma rede é escolher os componentes físicos: placas de rede, hub e cabos de rede. Atualmente você deve considerar apenas a compra de placas de rede Ethernet 10/100 em versão PCI, a menos claro que pretenda ligar à algum 486 que não tenha slots PCI, neste caso você ainda poderá encontrar algumas placas ISA à venda. Prefira comprar uma placa de rede nova, pois atualmente as placas de rede são um periférico muito barato. Não vale à pena correr o risco de levar pra casa uma placa com defeito ou sem drivers para economizar 10 reais.

No caso das placas ISA existe mais um problema em potencial. As placas antigas, sem suporte a plug-and-play são mais complicadas de instalar que as atuais. Ao invés de simplesmente espetar a placa e fornecer o driver você precisará utilizar primeiro o utilitário DOS, presente no disquete que acompanha a placa para configurar seus endereços e em seguida instala-la manualmente, através do "adicionar novo Hardware" do Windows, fornecendo os endereços que escolheu anteriormente.

A instalação das placas de rede PCI não é simples apenas no Windows. Qualquer distribuição Linux atual também será capaz de reconhecer e instalar a placa logo na instalação. Em alguns pontos, a configuração da rede numa distribuição atual do Linux é mais simples até que no Windows 98 ou 2000. O Linux Mandrake, apartir da versão 8.0 chega ao cúmulo de configurar o Samba para integrar a estação Linux a uma rede Windows já existente de forma automática.

Se você optar por utilizar uma rede sem fio 802.11b ou HomeRF os procedimentos não mudam. As placas de rede ou cartões PC-Card são instalados nos PCs e Notebooks como uma placa de rede normal e o ponto de acesso (no caso de uma rede 802.11b) deve ser posicionado num ponto central do ambiente, para permitir que todos os micros fiquem o mais próximos possível dele. Lembre-se que quanto menos obstáculos houver entre os PCs e o ponto de acesso, maior será o alcance do sinal:

Colocar o ponto de acesso no meio da instalação ao invés de próximo da porta da frente ou de uma janela, também diminui a possibilidade de alguém captar (acidentalmente ou não) os sinais da sua rede. Um procedimento importante é escolher um código SSID para o seu ponto de acesso, o que pode ser feito através do software que o acompanha. Este código é o que impedirá que qualquer um possa se conectar à sua rede. Escolha um código difícil de adivinhar e configure todas as placas de rede para utilizarem o mesmo código que o servidor. Como disso, isto pode ser feito através do utilitário que acompanha cada componente.

Se possível, compre placas e pontos de acesso do mesmo fabricante. Apesar de pontos de acesso e placas do mesmo padrão serem intercompatíveis, você pode ter um pouco mais de dificuldade para por a rede para funcionar caso cada placa venha com um software diferente.

Mas, Voltando para as boas e velhas redes com fio (que presumo, ainda seja as mais comuns dentro dos próximos dois ou três anos), precisamos agora escolher o Hub e os cabos a utilizar.

Eu não recomendo mais utilizar cabos coaxiais em hipótese alguma. Eles são mais caros, mais difíceis de achar (incluindo o alicate de crimpagem), a velocidade fica limitada a 10 megabits etc. Simplesmente estamos falando de um padrão que já faz parte do passado. Você teria interesse em comprar um PC com monitor monocromático? É um caso parecido :-)

Já que (por simples imposição do autor :-)) vamos utilizar um hub e cabos de par trançado, resta escolher qual hub utilizar. Esta é a escolha mais difícil, pois além das diferenças de recursos, os preços variam muito. Se esta é a sua primeira rede, eu recomendo começar por um hub 10/100 simples, com 8 portas. Os mais baratos custam na faixa dos 50 dólares e você poderá conectar a ele tanto placas de rede de 10 quanto de 100 megabits. Lembre-se porém que caso apenas uma placa de 10 megabits esteja conectada, toda a rede passará a operar a 10 megabits. Este é o significado de 10/100.

Existe uma forma de combinar placas de 10 e de 100 megabits na mesma rede, que é utilizar um hub-switch ao invés de um hub simples. O problema neste caso é o preço, já que um bom hub-switch não sairá por menos de 120 dólares.

Você também poderá encontrar alguns hubs 10/10 por um preço camarada. Dependendo do preço e do uso da rede, não deixa de ser uma opção, já que mais tarde você poderá troca-lo por um hub 10/100 mantendo os demais componentes da rede.

Não existe muito mistério quanto aos cabos. Basta comprar os cabos de categoria 5e, que são

praticamente os únicos que você encontrará à venda, além dos conectores e um alicate de crimpagem, ou, se preferir, comprar os cabos já crimpados.

A parte mais complicada pode ser passar os cabos através das paredes ou do forro do teto. O negócio aqui é pensar com calma a melhor forma de passa-los. Uma opção é comprar canaletas e fazer uma instalação aparente. Para passar os cabos pelas paredes não há outra alternativa senão crimpá-los você mesmo.

Esta relativa dificuldade na instalação dos cabos é o que vem levando algumas pessoas a investir numa rede sem fio. Pessoalmente eu acho que os componentes ainda estão muito caros. Ainda sairá muito mais barato comprar um alicate de crimpagem e contratar um eletricista para passar os cabos se for o caso.

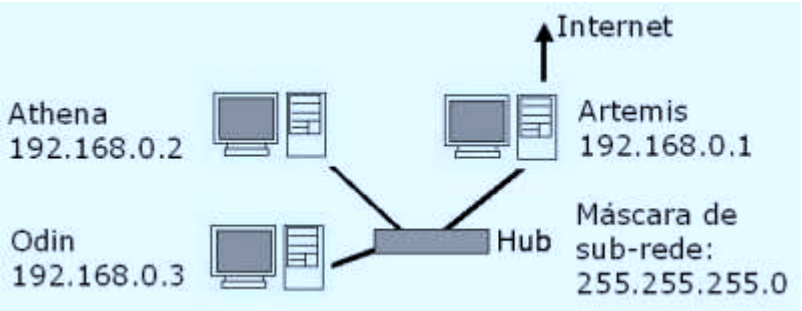
Planejando a rede

Depois de resolvida a instalação física da rede, planeje a configuração lógica da rede. Ou seja, se você pretende compartilhar a conexão com a Web, quais micros compartilharão arquivos, impressoras e outros recursos, qual será o endereço IP de cada micro e assim por diante.

Vamos exercitar um pouco a imaginação. Imagine que você tenha três micros. Um deles (vamos chamar de Artemis) têm uma conexão via cabo, que você quer compartilhar com os outros dois PCs (Athena e Odin).

Como o cable modem é ligado ao Artemis através de uma placa de rede, você precisará instalar uma segunda placa para liga-lo à rede. Ele passará a ter então dois endereços IP, o da internet, fornecido pelo seu provedor ou obtido automaticamente e um segundo IP para a sua rede interna.

Você pode usar por exemplo o endereço 192.168.0.1 para o Artemis (o defaut ao compartilhar a conexão através do ICS do Windows) e IPs sequenciais para os outros dois micros: 192.168.0.2 e 192.168.0.3. A máscara de sub-rede será 255.255.255.0 em todos os micros:



Neste caso o Artemis passa a ser também o Gateway da rede ou seja, o PC que os outros dois irão consultar sempre que for solicitado qualquer endereço que não faça parte da sua rede local. O Artemis se encarregará então de enviar os pedidos através da Internet e devolver as respostas. É assim que funciona o acesso compartilhado. Na verdade o Artemis continua sendo o único conectado à Web, mas graças a este trabalho de garoto de recados, todos passam a ter acesso.

Para compartilhar o Acesso você pode tanto utilizar o ICS do Windows, presente no Windows 98 SE, ME, 2000 e XP ou utilizar um servidor proxy. Mais adiante veremos como compartilhar o acesso tanto usando o ICS quanto utilizando o AnalogX Proxy, um freeware bastante competente. Outra boa opção é o Wingate, que têm mais recursos que o ICS, mas em compensação custa US$ 69 para até 6 usuários. A página é http://www.wingate.com/

Também é possível compartilhar uma conexão via modem. Neste caso existe a opção de ativar a discagem por demanda, onde o servidor estabelece a conexão automaticamente sempre que um dos clientes solicita uma página qualquer e encerra a conexão depois de algum tempo de inatividade. Claro que o ideal é ter algum tipo de conexão contínua, seja via cabo, ADSL, Satélite, etc.

Além de compartilhar a conexão com a Web, você pode compartilhar pastas, impressoras, drives de CD-ROM, etc. Você pode por exemplo adicionar mais um micro na rede, um 486 velho por exemplo e usa-lo como um servidor de back-up, para não correr o risco de perder seus arquivos no caso de qualquer desaste.

Configuração de rede no Win 98

Depois de montar a parte física da rede, vamos agora para a configuração lógica das estações. Este trecho explica como instalar a placa de rede e fazer a configuração lógica da rede em micros rodando o Windows 95 ou 98:

Instalando a placa de rede

Todas as placas de rede à venda atualmente são plug-and-play, isto torna sua instalação extremamente fácil. Basta espetar a placa em um slot disponível da placa mãe, inicializar o micro para que o Windows a detecte e se necessário, fornecer os drivers que vêm junto com a placa. Para instalar uma placa não plug-and-play, abra o ícone “rede” do painel de controle, clique em “adicionar”, em seguida em “adaptador” e finalmente em “com disco”.

Depois de instalada a placa, acesse o gerenciador de dispositivos e cheque as configurações da placa para ter certeza de que ela está funcionando corretamente. Placas plug-and-play não costumam dar muita dor de cabeça, mas é comum placas antigas, de legado, entrarem em conflito com outros dispositivos. Se for o seu caso, altere o endereço usado pela placa, ou então reserve o endereço de IRQ usado pela placa na sessão “PCI/plug-and-play” do Setup, para que não seja usado por outros dispositivos.

Configurando uma rede ponto a ponto

Tanto o Windows 95, quanto o Windows 98, oferecem recursos que permitem montar uma rede ponto a ponto entre vários micros rodando o Windows com facilidade. Você deverá instalar o “Cliente para redes Microsoft”, o “Compartilhamento de arquivos e impressoras para redes

Microsoft" e um protocolo de comunicação dentro do ícone "Redes" do painel de controle.

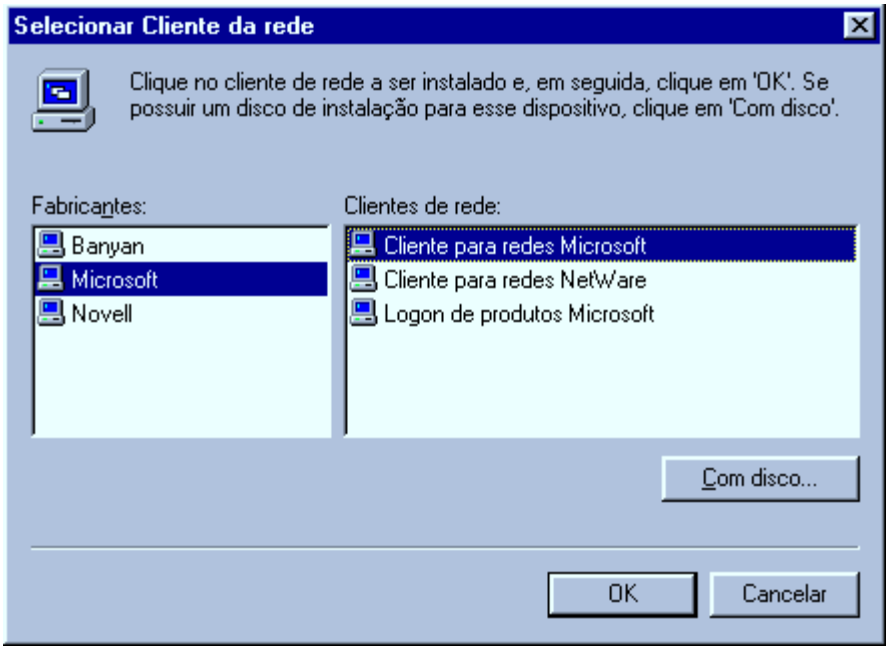
Você poderá instalar basicamente três protocolos: TCP/IP, NetBEUI e IPX/SPX. O TCP/IP é praticamente obrigatório, pois é necessário para compartilhar o acesso à Web, mas você pode manter os outros dois instalados se desejar. O NetBEUI permite compartilhar recursos com os outros micros da rede sem necessidade de configurar manualmente um endereço, como no TCP/IP e o IPX/SPX permite a conexão com redes Novel.

É recomendável, sempre que possível, manter apenas o TCP/IP instalado, pois ao instalar vários protocolos, mais clientes de rede etc., o Windows sempre manterá todos eles carregados, tornando o sistema um pouco mais lento.

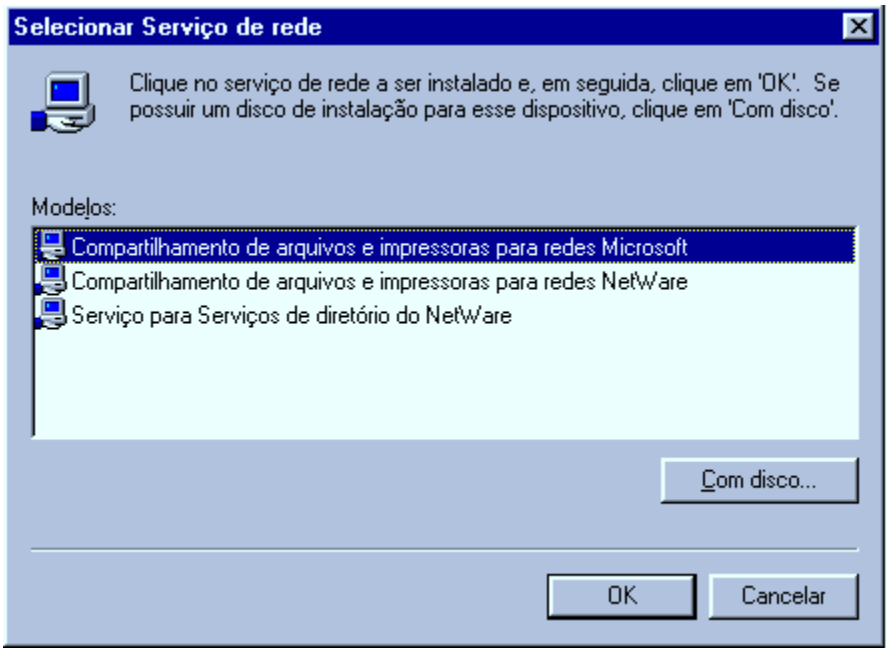
Para instalar o protocolo basta escolher "protocolo" e clicar em "adicionar". Na tela seguinte escolha "Microsoft" no menu do lado esquerdo para que os protocolos disponíveis sejam exibidos. Também estão disponíveis protocolos de outros fabricantes, como o Banyan VINES e o IBM DLC (caso precise).

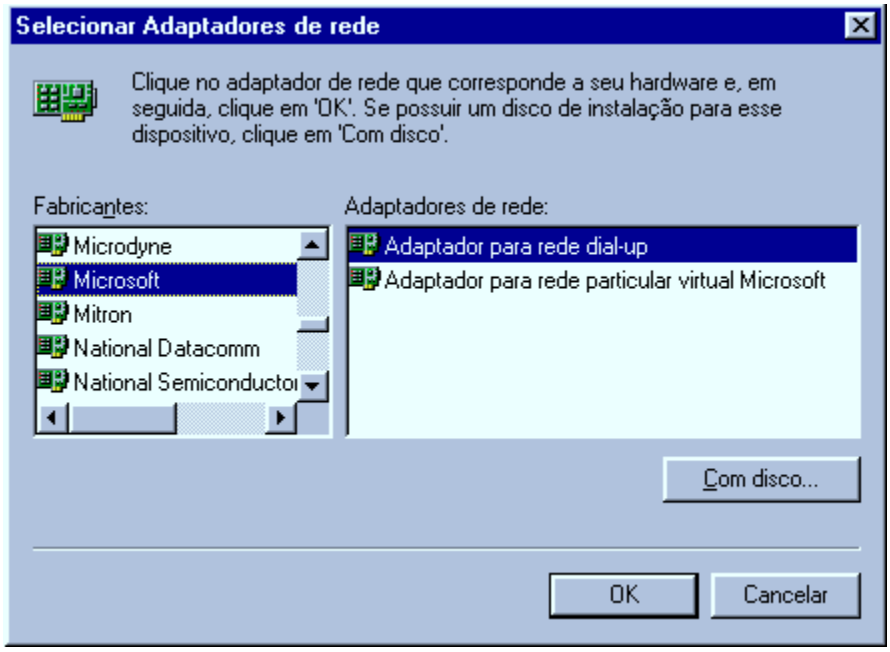
Depois de instalar os protocolos, você deve instalar também o "Cliente para redes Microsoft", para que possa acessar os recursos da rede. Basta escolher "Cliente" e clicar em "Adicionar" na janela de instalação dos componentes da rede. Sem instalar o cliente para redes Microsoft o micro não será capaz de acessar os recursos da rede.

Para finalizar, volte à janela de instalação de componentes, clique em "serviço" e "adicionar", e instale o "Compartilhamento de arquivos e impressoras para redes Microsoft", que permitirá a você compartilhar recursos como arquivos e impressoras com outros micros da rede.



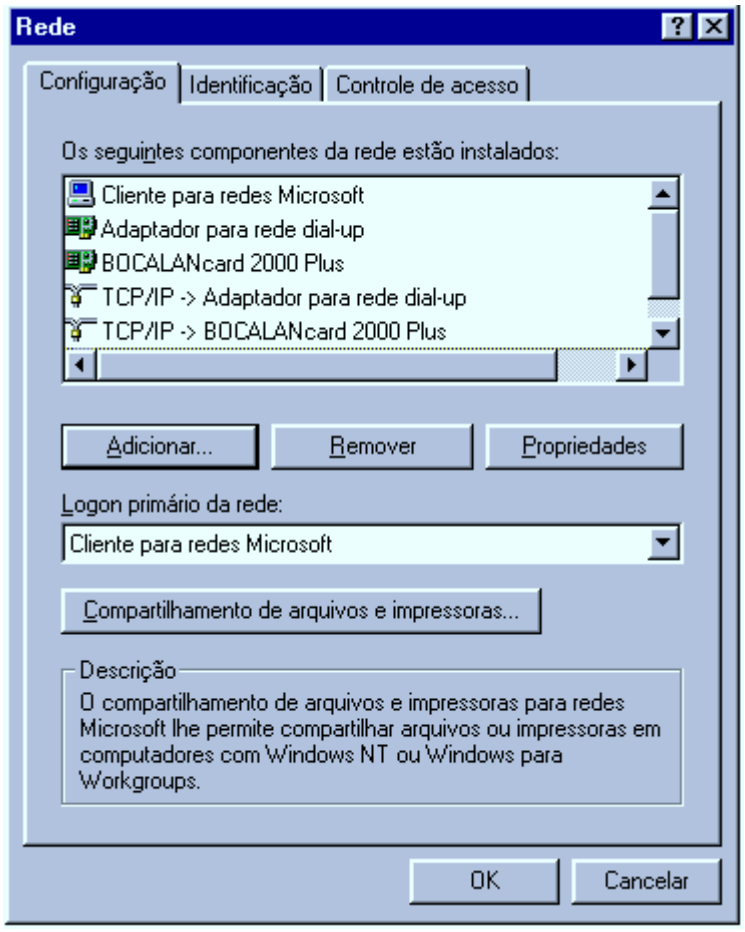
Para que o micro possa acessar a Internet, você deverá instalar também o “Adaptador para redes dial-up”. Para isto, clique em “adaptador” na janela de instalação de componentes, e no menu que surgirá, escolha “Microsoft” no menu da esquerda, e em seguida, “Adaptador para redes dial-up” no menu da direita.

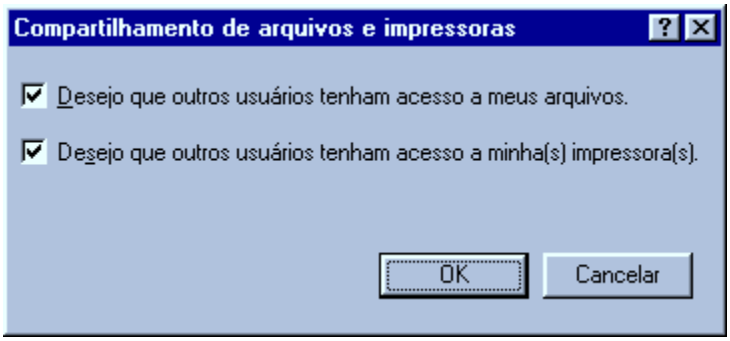




Configurações

Após instalar os itens anteriores, seu ambiente de rede deverá estar como o exemplo da figura ao abaixo. Clique no botão "Compartilhamento de arquivos e impressoras" e surgirá um menu com duas seleções: "desejo que outros usuários tenham acesso aos meus arquivos" e "desejo que outros usuários tenham acesso às minhas impressoras". Por enquanto, mantenha marcados ambos os campos.



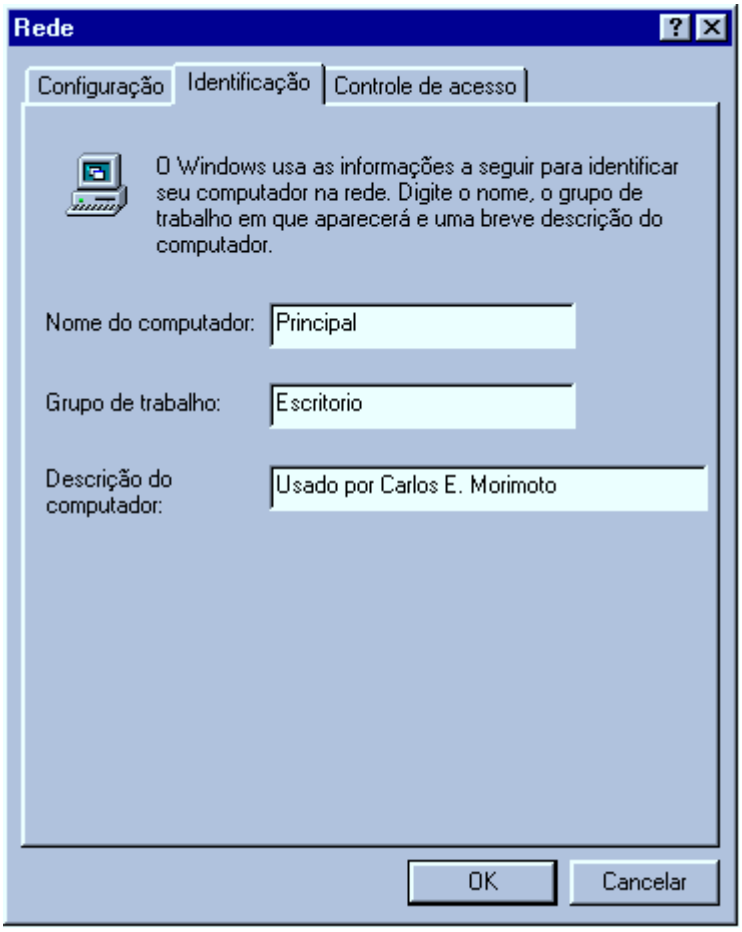


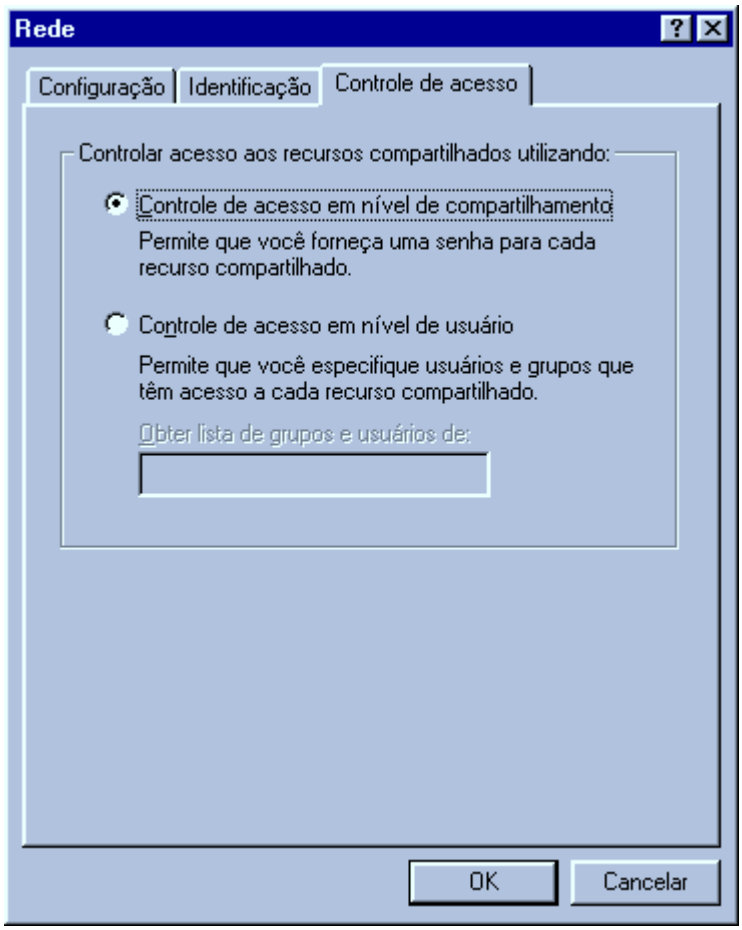
Voltando à janela principal, acesse agora a guia "Identificação". Nos campos, você deve dar um

nome ao micro. Este nome será a identificação do micro dentro da rede Microsoft, e deverá ser diferente em cada micro da rede. Este nome poderá ter até 15 caracteres. São permitidos apenas caracteres alfanuméricos e os caracteres ! @ # $ % ^ & ( ) - _ { } ‘ . ~ e não são permitidos espaços em branco. Na mesma janela você deverá digitar o nome do grupo de trabalho do qual o computador faz parte. Todos os micros de uma mesma sessão deverão fazer parte do mesmo grupo de trabalho, isto facilitará o acesso aos recursos, pois fará com que todos apareçam na mesma janela, quando você localizar um micro na rede, e dentro na mesma pasta, quando abrir o ícone “ambiente de redes”

Finalmente, digite algo que descreva o micro no campo “Descrição do computador”, este campo não altera em nada a configuração ou o funcionamento da rede, mas será visto por outros usuários que acessarem recursos compartilhados pelo seu micro. Você pode digitar, por exemplo, o nome do usuário do micro, ou então alguma observação como “Micro do chefe”.

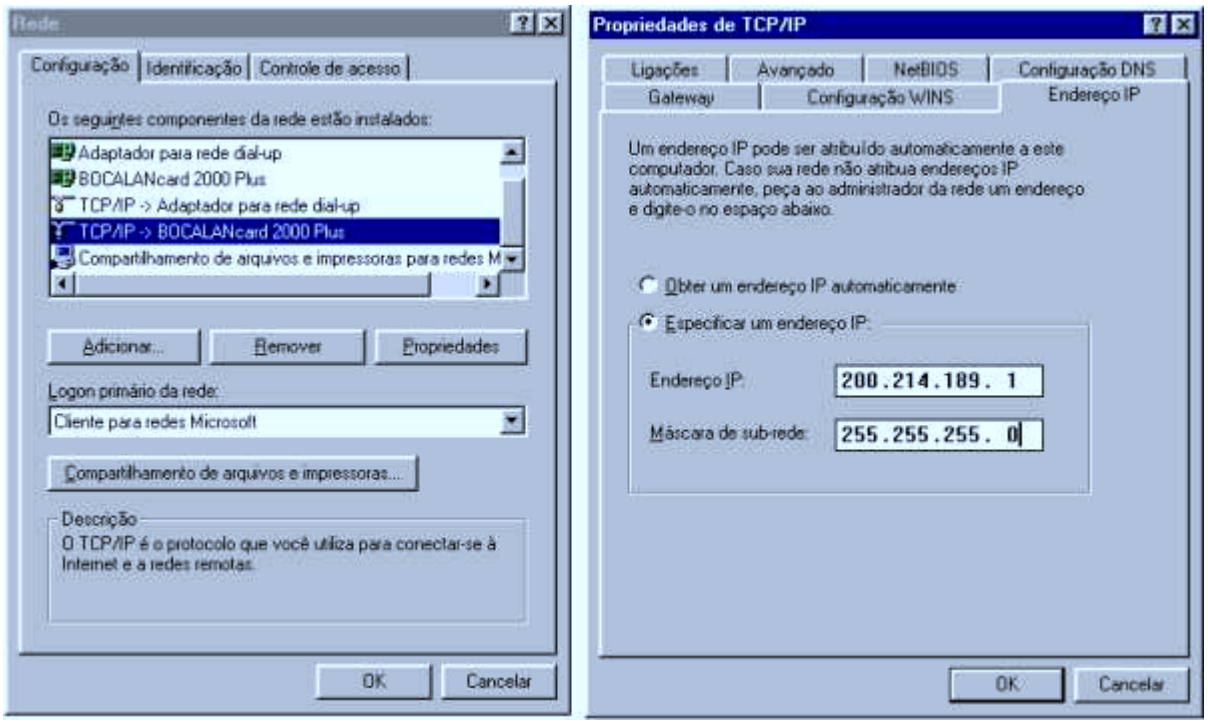
Acesse agora a guia “Controle de acesso”. Aqui você poderá escolher entre “Controle de acesso em nível de compartilhamento” e “controle de acesso em nível de usuário”. A primeira opção se destina a compartilhar recursos numa rede ponto a ponto, onde um recurso compartilhado fica acessível a todos os demais micros da rede, podendo ser protegido apenas com uma senha. A opção de controle de acesso a nível de usuário pode ser usada apenas em redes cliente – servidor; selecionando esta opção, você deverá configurar as permissões de acesso aos recursos da rede no servidor e informar no campo, o endereço do servidor onde estão estas informações.





Finalmente, precisamos acertar as configurações do TCP/IP. Veja que no gerenciador de rede aparecerão duas entradas para o TCP/IP, uma relacionada com a placa de rede e outra relacionada com o adaptador de rede dial-up. A entrada relacionada com a dial-up é a entrada usada para acessar a Internet via modem, e deve ser configurada (se necessário) de acordo com as configurações fornecidas pelo seu provedor de acesso. A entrada relacionada com a placa de rede por sua vez, é a utilizada pela rede. É ela que devemos configurar.

Clique sobre ela e, em seguida, sobre o botão "propriedades"; surgirá então uma nova janela com as propriedades do TPC/IP. No campo "endereço IP" escolha a opção "Especificar um endereço IP" e forneça o endereço IP do micro, assim como sua máscara de sub-rede. O Campo "Obter um endereço automaticamente" deve ser escolhido apenas no caso de você possuir um servidor DHCP corretamente configurado em sua rede.



Logando-se na rede

Após instalar o cliente para redes Microsoft, toda vez que inicializar o micro o Windows pedirá seu nome de usuário e senha. É obrigatório logar-se para poder acessar os recursos da rede. Se você pressionar a tecla "Esc", a janela de logon desaparecerá e o sistema inicializará normalmente, porém todos os recursos de rede estarão indisponíveis.

Se a tela de logon não aparecer, significa que o Windows está tendo problemas para acessar a placa de rede, e consequentemente a rede está indisponível. Neste caso, verifique se a placa de rede realmente funciona, se não está com nenhum tipo de conflito e se os drivers que você usou são os corretos.

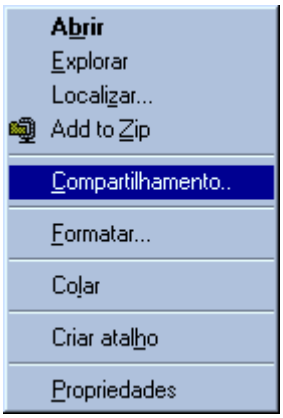
Lembre-se que muitas placas de rede mais antigas (não PnP) precisam ter seus endereços de IRQ, I/O e DMA configurados através de um programa que acompanha a placa antes de serem instaladas. Este programa, geralmente "Setup.exe" vem no disquete que acompanha a placa; basta executá-lo pelo DOS.

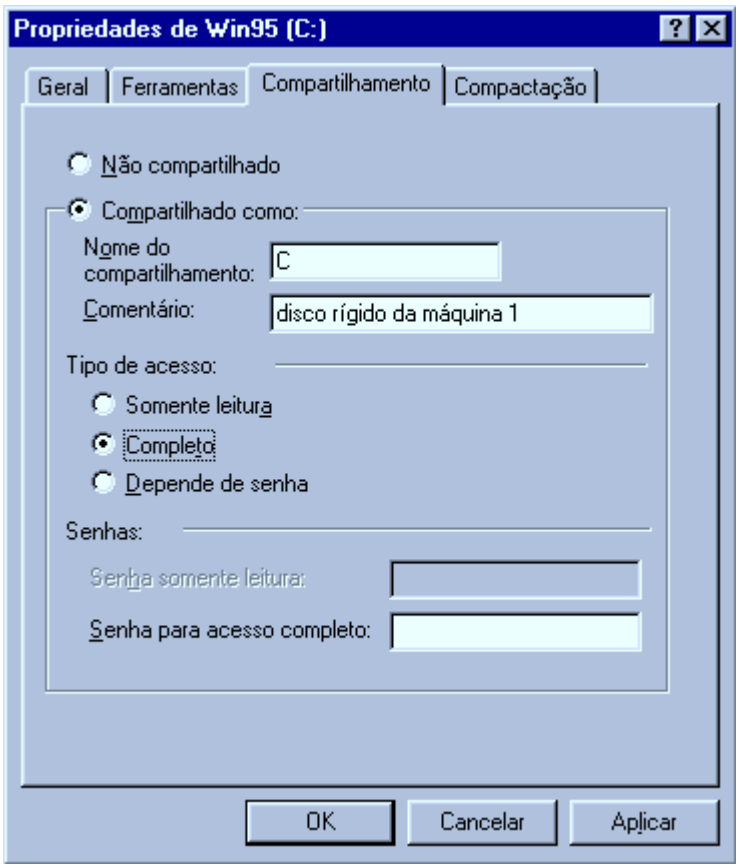
Compartilhando recursos

Vamos agora à parte mais importante da configuração de rede, pois afinal o objetivo de uma rede ponto a ponto é justamente compartilhar e acessar recursos através da rede, não é? ;-)

O Serviço de compartilhamento usado pelo Windows 98 permite compartilhar drivers de disquete,

drivers de CD-ROM, impressoras, pastas e mesmo uma unidade de disco inteira. Para compartilhar um recurso, basta abrir o ícone "Meu Computador", clicar com o botão direito sobre o ícone do disco rígido, CD-ROM, drive de disquetes, etc., e escolher "compartilhamento" no menu que surgirá.





Mude a opção de "Não compartilhado" para "Compartilhado como". No campo "Nome do Compartilhamento" dê o nome que identificará o compartilhamento na rede. Você pode, por exemplo, dar o nome "C:" para o disco rígido, "CD-ROM" para o CD-ROM, "Documentos" para uma pasta com arquivos do Word, etc. Veja que independentemente de ser um disco rígido inteiro, um CD-ROM, uma impressora, ou uma pasta, cada compartilhamento possui um nome exclusivo pelo qual será acessado através da rede. Na mesma janela você poderá configurar o tipo de acesso permitido para o compartilhamento. As opções são:

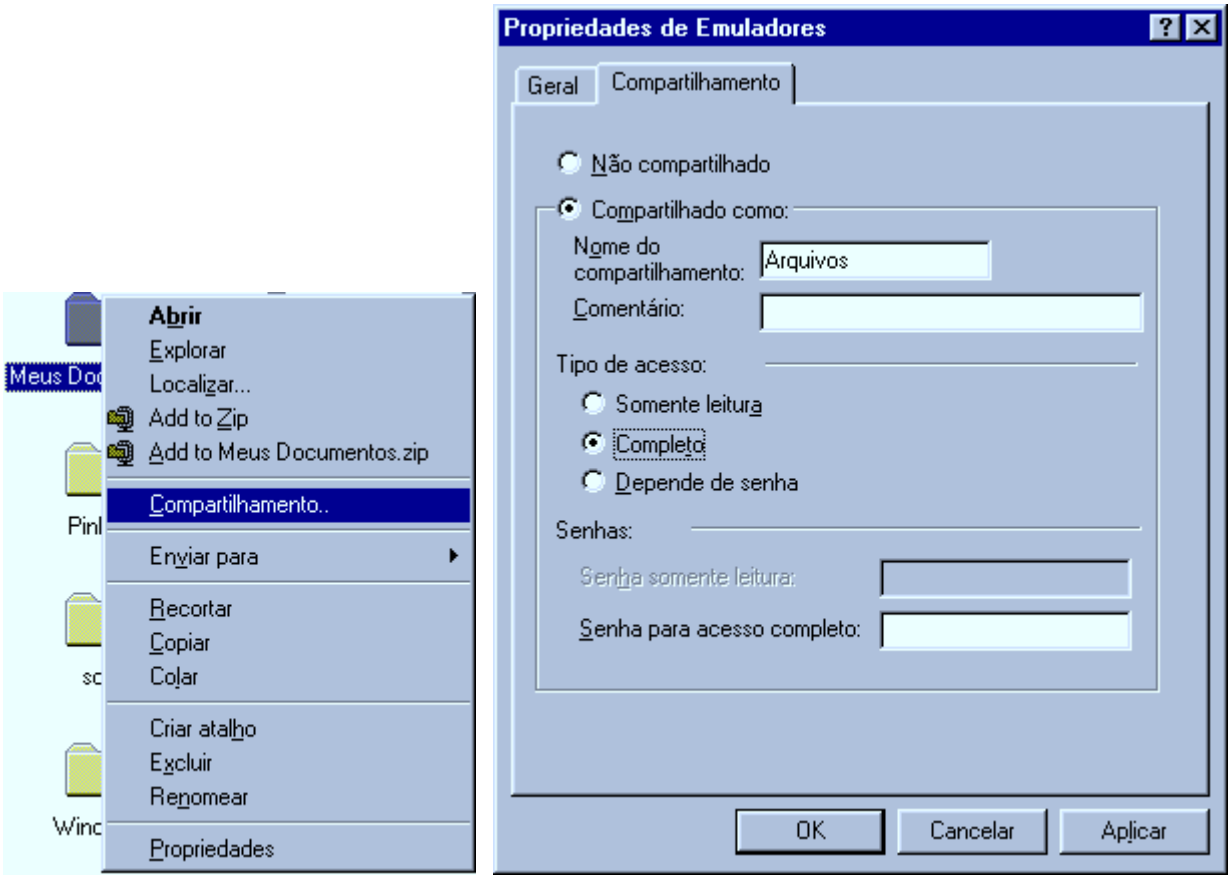
Somente leitura : Os outros usuários poderão apenas ler os arquivos do disco, mas não poderão alterar os arquivos, ou copiar nada para o disco. Você pode usar este tipo de compartilhamento para proteger, por exemplo, arquivos de programas que são acessados por vários usuários, mas que não devem ser alterados.

Completo : Determina que os outros usuários poderão ter acesso total à pasta ou disco compartilhado: copiar, alterar ou deletar, exatamente como se fosse um disco local.

Depende da senha : Permite que você estabeleça senhas de acesso. Assim o recurso só poderá ser acessado caso o usuário do outro micro tenha a senha de acesso. Você poderá escolher senhas

diferentes para acesso completo e somente leitura.

Ao invés de compartilhar todo o disco rígido, você poderá compartilhar apenas algumas pastas. Para isso, deixe o disco rígido como "Não Compartilhado", e compartilhe apenas as pastas desejadas, clicando sobre elas com o botão direito e escolhendo "compartilhamento". Compartilhar uma pasta significa compartilhar todos os arquivos e sub-pastas que estejam dentro. Infelizmente o Windows 98 não permite compartilhar arquivos individualmente.



Para compartilhar a impressora, acesse o ícone "Impressoras", clique com o botão direito sobre ela e novamente escolha "compartilhamento". Compartilhe-a, dê um nome para ela e se quiser, estabeleça uma senha de acesso.

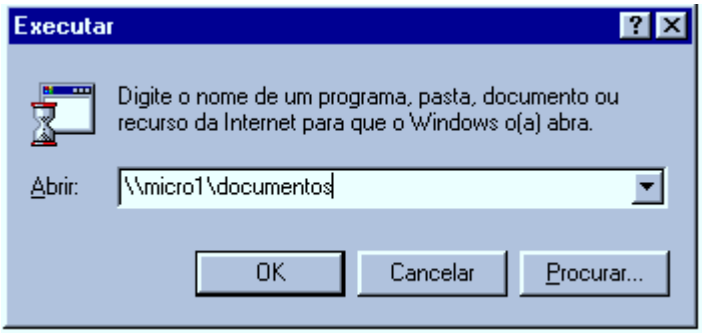
Tudo pronto, agora basta ligar todos os micros e os recursos compartilhados aparecerão através do Windows Explorer, ou abrindo o ícone "Ambiente de Rede" que está na mesa de trabalho. Tudo que estiver compartilhado poderá ser acessado como se fizesse parte de cada um dos micros.

Acessando discos e pastas compartilhados

Existem 4 maneiras de acessar um disco rígido, CD-ROM ou pasta compartilhados. A primeira maneira, e a mais simples, é usar o ícone "Ambiente de Rede" que está na área de trabalho.

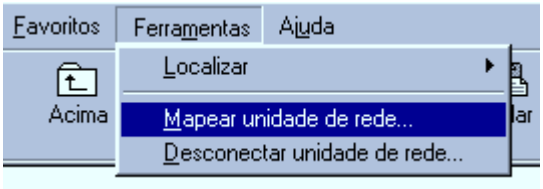
Clicando sobre ele, surgirá uma janela mostrando todos os micros da rede que estão compartilhando algo, bastando clicar sobre cada um para acessar os compartilhamentos.

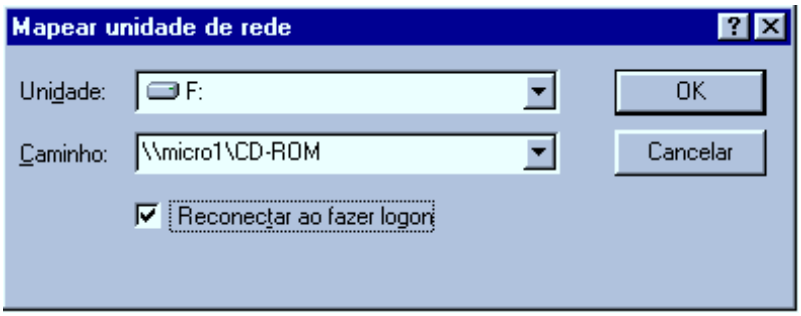
A segunda maneira é semelhante à primeira, porém é mais rápida. Se por exemplo você quer acessar a pasta de documentos do micro 1, que está compartilhada como "documentos", basta usar o comando "Executar..." do menu iniciar. A sintaxe da linha de comandos é \\nome_do_micro\nome_do_compartilhamento como em \\micro1\documentos. Isto abrirá uma janela mostrando todo o conteúdo da pasta compartilhada. Outras sintaxes para este comando são:
\\micro1 : para mostrar todos os compartilhamentos do micro indicado
\\micro1\documentos\maria : mostra o conteúdo da pasta "maria" que está dentro do compartilhamento "documentos" que está no micro 1.



A terceira maneira é mapear uma unidade de rede através do Windows Explorer. Uma unidade de rede é um compartilhamento que é usado com se fosse uma unidade de disco local, recebendo uma letra, e aparecendo no Windows Explorer junto com as unidades de disco local. Mapear uma pasta ou disco compartilhado torna o acesso mais fácil e rápido.

Para mapear uma unidade de rede, abra o Windows Explorer, clique em "Ferramentas" e, em seguida, em "Mapear unidade de Rede". Na janela que surgirá, você deverá digitar o endereço de rede do recurso compartilhado, como em \\micro1\CD-ROM





No campo “unidade”, você deverá escolher a letra que a unidade compartilhada receberá. Não é preciso escolher uma letra seqüencial, pode ser qualquer uma das que aparecerão ao clicar sobre a seta.

A opção “reconectar ao fazer logon”, quando marcada, fará com que seu micro tente recriar a unidade toda vez que você se logar na rede. Se por acaso, ao ligar seu micro, o micro que está disponibilizando o compartilhamento não estiver disponível, será exibida uma mensagem de erro, perguntando se você deseja que o Windows tente restaurar a conexão da próxima vez que você se logar na rede. Você também pode desconectar uma unidade de rede, basta clicar com o botão direito sobre ela (através do Windows Explorer ou do ícone “Meu computador”) e escolher “Desconectar” no menu que surgirá.

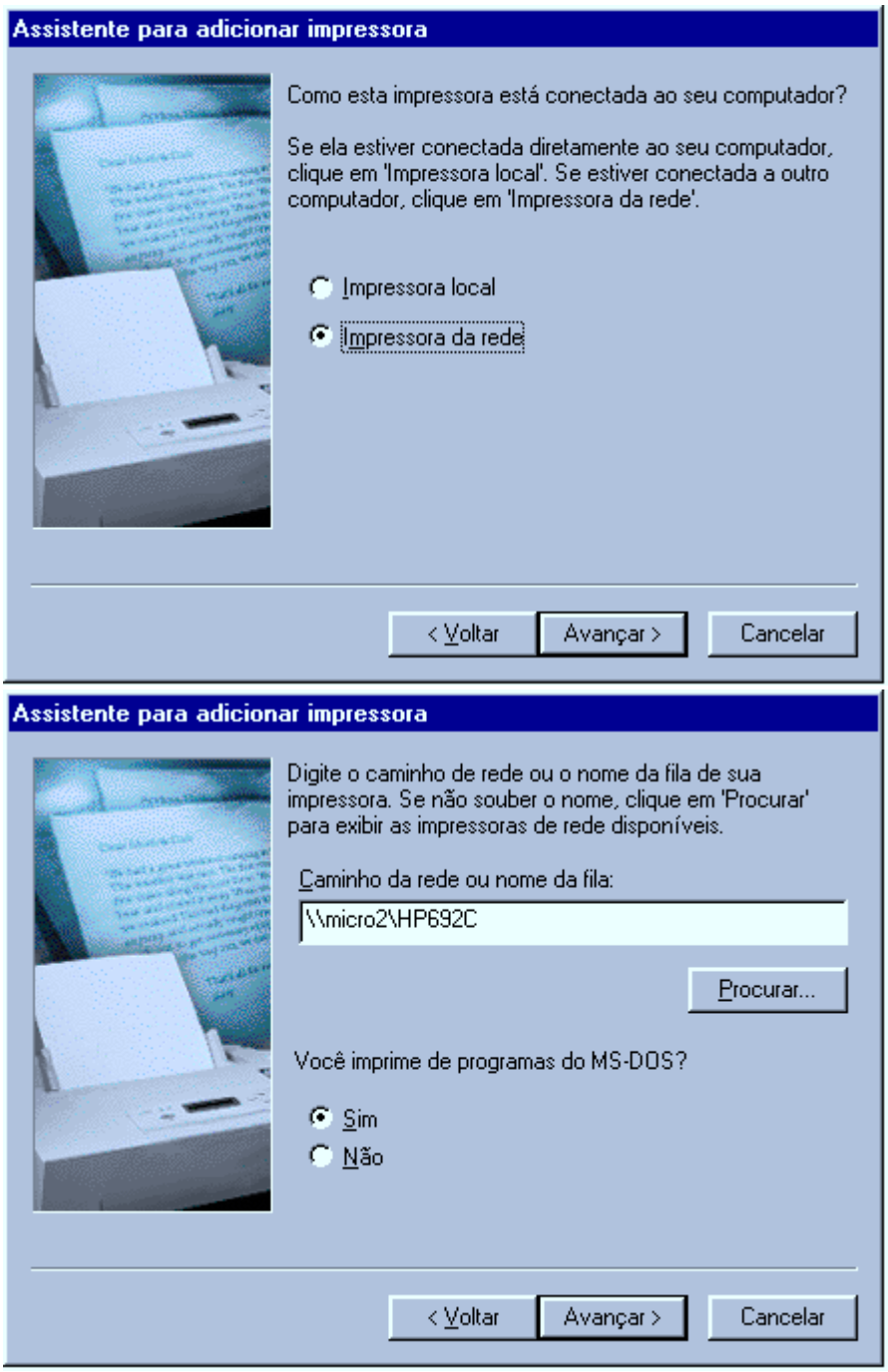
Uma unidade compartilhada também pode ser acessada através dos aplicativos, usando os comandos de abrir arquivo, salvar arquivo, inserir arquivo, etc. Esta é a quarta maneira de acessar os recursos da rede.

Acessando impressoras de rede

Para imprimir em uma impressora de rede, você deverá primeiro instalá-la na estação cliente. A instalação de uma impressora de rede não é muito diferente da instalação de uma impressora local, na verdade é até mais simples.

Abra o ícone “Meu computador” e em seguida o ícone “impressoras”. Clique agora em “adicionar impressora” e em seguida no botão “avançar”. Surgirá uma nova janela, perguntando se você está instalando uma impressora local ou uma impressora de rede. Escolha “impressora de rede” e novamente em “avançar”.

Na janela que surgirá a seguir, você deverá informar o caminho de rede da impressora. Lembre-se que como qualquer outro compartilhamento, uma impressora de rede tem seu nome de compartilhamento. O endereço da impressora é composto por duas barras invertidas, o nome do micro à qual ela está conectada, barra invertida, o nome da impressora na rede, como em \\micro2\HP692C



Você deverá informar também se precisará usar a impressora de rede para imprimir a partir de programas do MS-DOS. Caso escolha "sim", o Windows fará as alterações necessárias nos arquivos de inicialização para que a impressora funcione a partir do MS-DOS.

Como estamos instalando uma impressora de rede, não será necessário fornecer os drivers da impressora, pois o Windows os copiará a partir do micro aonde ela está conectada. Depois de terminada a instalação, o Windows permitirá que você dê um nome à impressora (o nome dado

aqui se refere apenas ao ícone da impressora), perguntando também se você deseja que seus aplicativos usem a impressora como padrão. Como de praxe, o Windows lhe dará a opção de imprimir uma página de teste; faça como quiser e clique em “concluir” para finalizar a instalação.

O ícone referente à impressora de rede aparecerá na pasta de impressoras, e você poderá utiliza-la da mesma maneira que utilizaria uma impressora local. Usar uma impressora de rede traz a vantagem do micro não ficar lento enquanto a impressora estiver imprimindo, pois os trabalhos de impressão são transferidos diretamente para o spooler de impressão do micro que está disponibilizando a impressora, e ele próprio (o servidor de impressão) deverá cuidar da tarefa de alimentar a impressora com dados.

O spooler de impressão nada mais é do que um arquivo temporário criado dentro da pasta \Windows\Spool\Printers do disco do servidor de impressão. Nesta pasta serão gravados todos os arquivos a serem impressos, organizados na forma de uma fila de impressão. Usamos o termo “fila” pois os arquivos vão sendo impressos na ordem de chegada.

Dependendo do número e tamanho dos arquivos a serem impressos, o spooler pode vir a consumir um espaço em disco considerável. O servidor de impressão também ficará lento enquanto a impressora estiver imprimindo, por isso, se a quantidade de documentos impressos for grande, você deve considerar a idéia de um servidor de impressão dedicado.

Compartilhamentos ocultos

Usando o Windows 98, também e possível criar compartilhamentos ocultos. Um compartilhamento oculto possui as mesmas características dos compartilhamentos normais, a única diferença é que ele não aparecerá junto com os outros quando for aberto o ícone “Ambiente de redes”; apenas quem souber o nome do compartilhamento poderá acessá-lo.

Para criar um compartilhamento oculto, basta acrescentar um “$” no final do seu nome, como por exemplo, documentos$, CD-ROM$, C:$ etc. Como o compartilhamento oculto não aparecerá usando o ícone ambiente de rede, só será possível acessá-lo usando o comando “Executar” do menu iniciar, digitando diretamente o nome do compartilhamento (como em \\micro1\CD-ROM$) ou então mapeando o compartilhamento como unidade de rede através do Windows Explorer.

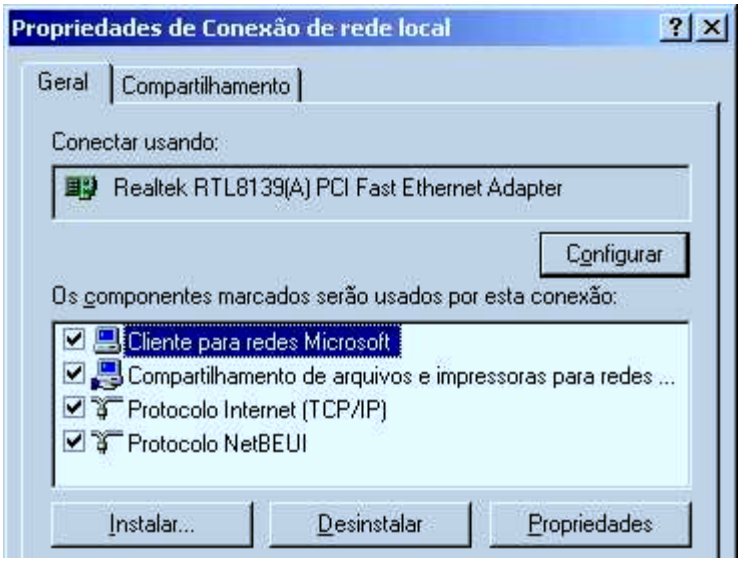
Em qualquer um dos casos, apenas quem souber o nome do compartilhamento poderá acessá-lo, isto pode ser útil para melhorar a segurança da rede.

Configuração de rede no Windows 2000

Após instalar a placa de rede, abra o ícone "conexões dial-up e de rede" do painel de controle. Você notará que além das conexões de acesso à Internet apareceu uma nova conexão (com um ícone diferente das demais) que representa a conexão da sua placa de rede.

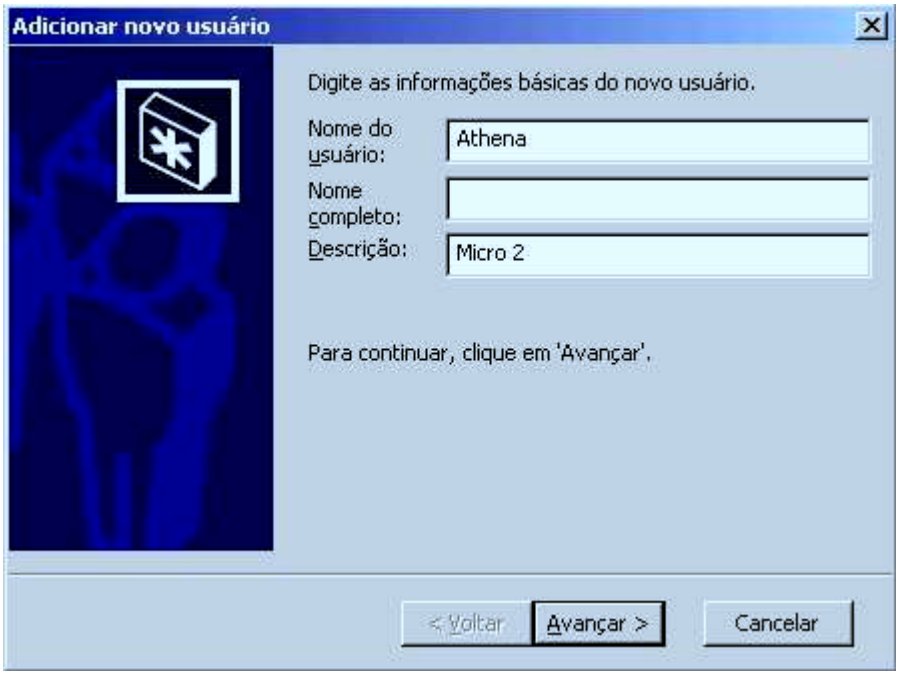
Abra o ícone correspondente à placa de rede e (caso já não estejam instalados) Instale o protocolo

"TCP/IP", o "Cliente para redes Microsoft" e em seguida o "Compartilhamento de arquivos e impressoras para redes Microsoft", como no caso anterior, você pode instalar também o NetBEUI e outros protocolos que desejar. Não se esqueça de acessar as propriedades do TCP/IP e configure o endereço IP como explicado anteriormente.



Agora vai uma parte da configuração que é necessária apenas no Windows 2000:

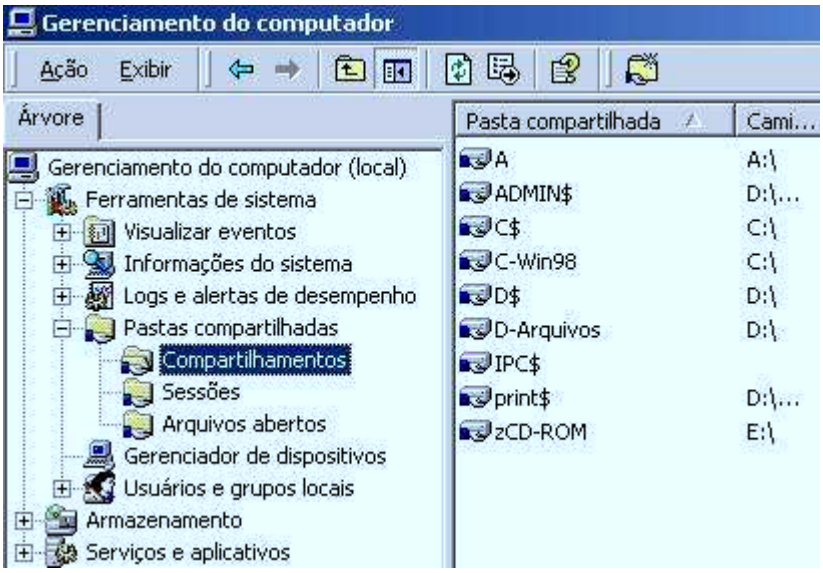
1- Ainda no painel de controle, acesse "usuários e senhas". Adicione na lista o login e senha de rede que está usando nas outras máquinas da rede, incluindo naturalmente as máquinas com o Windows 95/98. Caso contrário as outras máquinas não terão acesso à máquina com o Windows 2000. Se o objetivo for apenas compartilhar o acesso à Internet, você pode apenas ativar a conta "guest" que vem desabilitada por default:



Esta forma de controle do Windows 2000 é mais complicada de configurar, mas oferece uma segurança de rede muito maior. É fácil especificar o que cada usuário da rede poderá fazer. Numa empresa isso é extremamente útil, pois permitirá ter uma segurança de rede muito boa, mesmo sem usar um servidor dedicado.

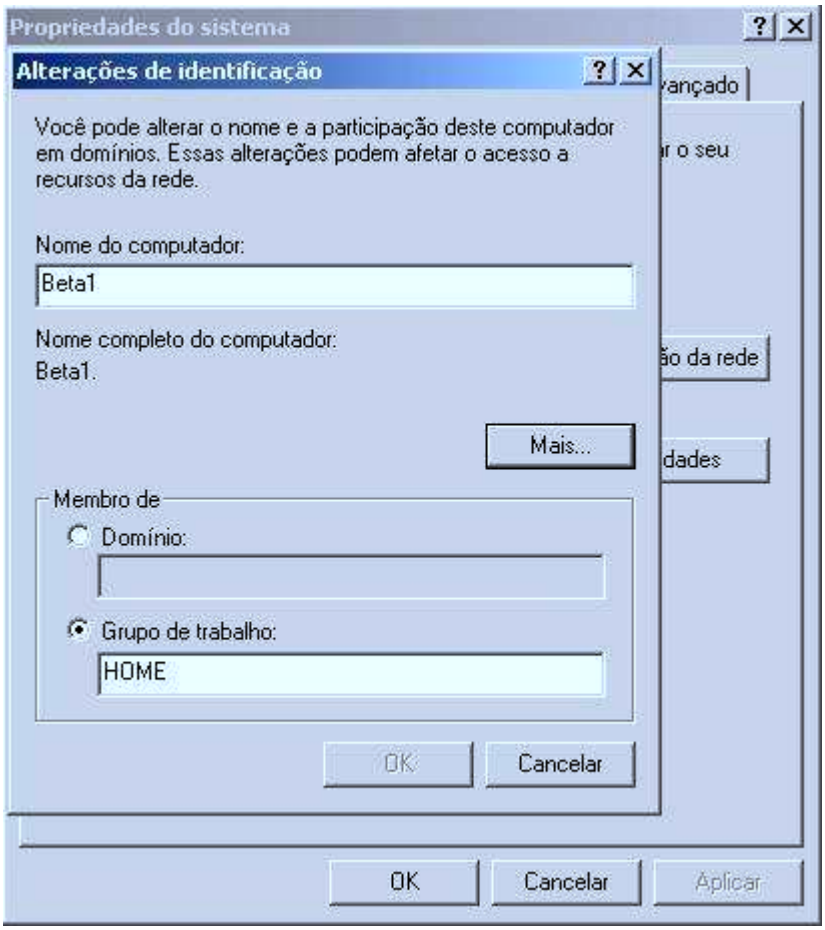
2- Acesse: Painel de controle/Ferramentas administrativas/Gerenciamento do computador, abra a Sessão Pastas compartilhadas/Compartilhamentos.

3- Adicione na lista de compartilhamentos as pastas que deseja acessar no outro micro. Não esqueça de colocar na lista dos que terão acesso à pasta os logins de usuário que estão sendo utilizados nos demais micros da rede:



Para compartilhar também a impressora, acesse painel de controle/impressoras. Um detalhe é que para compartilhar a impressora com micros rodando o Windows 95/98 ou outras versões antigas do Windows, você precisará fornecer também os drivers de impressoras para estes sistemas. Com certeza os drivers vieram junto com a impressora, mas caso você tenha perdido o CD, procure no site do fabricante.

4- Acesse Painel de controle/Sistema e em "Identificação de rede" clique no botão "Propriedades". Defina um nome para o computador (o Win 2K já cria um nome durante a instalação, mas você pode querer altera-lo). O grupo de trabalho deve ser o mesmo usado nos demais micros da rede.



Para instalar uma impressora de rede, ou seja acessar uma impressora compartilhada em outro micro da rede, acesse o Painel de controle/impressoras, clique em adicionar nova impressora e escolha "impressora de rede".

Compartilhar a conexão com a Internet usando o ICS

O ICS, ou Internet Conection Sharing é o recurso nativo do Windows que permite compartilhar a conexão com a Internet entre vários PCs, tanto rodando Windows, quanto rodando Linux ou outros sistemas operacionais. O ICS é encontrado no Windows 98 SE, Windows ME, Windows 2000 e Windows XP. Ele não está disponível no Windows 98 antigo, nem no Windows 95.

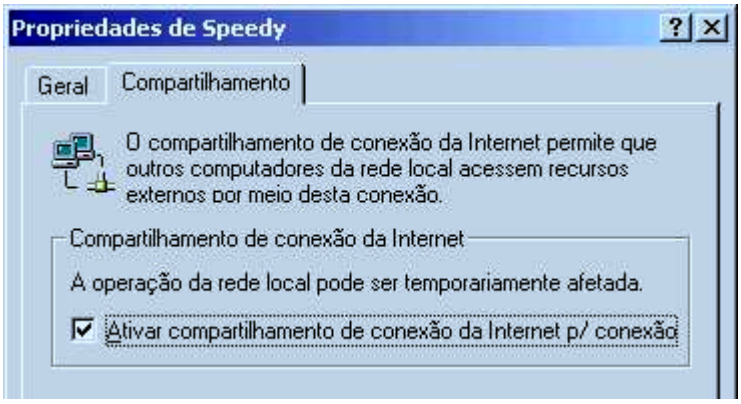
Vamos ver agora como configurar este recurso para compartilhar a conexão entre máquinas rodando o Windows 98 SS, Windows 2000 e Linux.

Para usar o ICS, você precisa estar com a sua rede já montada e com o protocolo TCP/IP instalado em todos os micros.

Um dos principais motivos para ligar micros em rede hoje em dia é compartilhar a mesma conexão com a Internet. Afinal, por que colocar um modem em cada máquina, possuir mais de uma linha telefônica, pagar mais pulsos telefônicos etc. se é possível ter apenas uma conexão, seja via modem, seja uma conexão rápida qualquer e compartilha-la com os demais micros da rede?

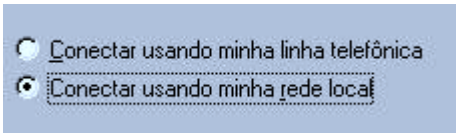
Compartilhar a conexão no Windows 2000 Professional

1 - Abra o painel de controle/Conexões dial-up e rede. Acesse as propriedades da conexão com a Internet (e não a configuração da rede local), seja via modem, ADSL etc. acesse as propriedades, compartilhamento, e marque a opção "Ativar compartilhamento de conexão com a Internet".



2 - Acesse as configurações de TCP/IP de todas as demais máquinas da rede mude a configuração para "obter automaticamente um endereço IP". Esta é a configuração recomendada pela Microsoft, que faz com que todos os PCs obtenham seus endereços IP automaticamente, apartir da máquina que está compartilhando a conexão, via DHCP.

3 - Este compartilhamento funciona automaticamente em máquinas rodando o Windows 2000 ou 98 SE, basta configurar o TCP/IP para obter seus endereços automaticamente. Caso você tenha PCs na rede rodando o Windows 98 ou Win 95, acesse (no cliente), iniciar > programas > acessórios > ferramentas para a Internet > entrar na Internet. Escolha "configuração manual" na primeira pergunta do assistente, e na segunda responda que deseja conectar-se através de uma rede local.



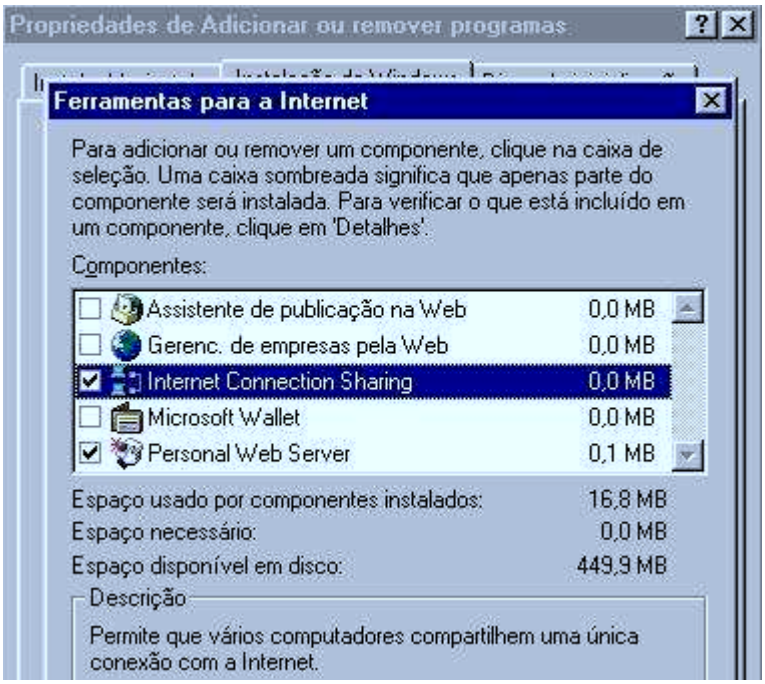
A seguir, deixe **desmarcada** a opção de acessar via proxy. Terminando, bastará reiniciar o micro.

Compartilhar a conexão no Windows 98 SE

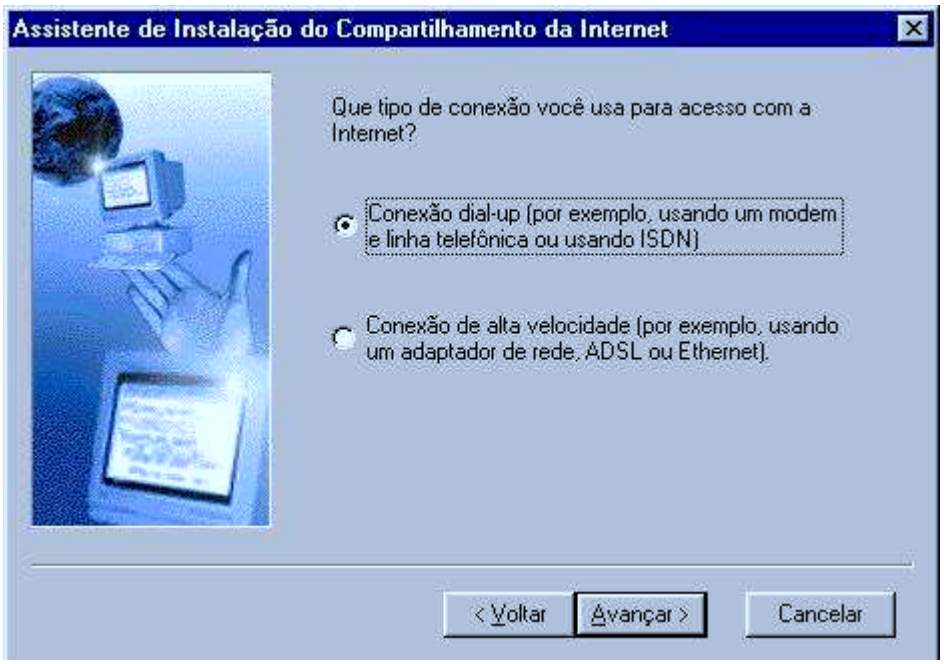
Infelizmente o Windows só incorporou um serviço de compartilhamento de conexão apartir do Windows 98 SE. Caso você esteja utilizando o Windows 98 antigo, ou o Windows 95, e por qualquer motivo não puder atualizar o sistema, a única solução seria utilizar um programa de proxy, como o Wingate, entre vários outros, inclusive gratuítos que já existem.

Presumindo que a máquina que detenha a conexão esteja rodando o Win 98 SE e que você já tenha configurado corretamente a rede, vamos aos passos para compartilhar a conexão:

1 - Abra o painel de controle/adicionar remover programas e abra a aba "instalação do Windows". Acesse as Ferramentas para a Internet e instale o Internet Conection Sharing.



2 - Logo depois de instalado o serviço, será aberto um assistente, que lhe perguntará sobre o tipo de conexão que possui. Sem mistério, basta escolher entre conexão dial-up, ou seja, uma conexão discada qualquer, seja via modem ou ISDN, ou mesmo cabo unidirecional, ou então Conexão de alta velocidade, caso esteja acessando via ADSL ou cabo bidirecional.



3 - Terminado, será gerado um disquete, com um outro assistente, que deverá ser executado nos outros micros da rede, rodando o Windows 98 antigo ou Windows 95, que se encarregará de fazer as configurações necessárias. Caso as outras máquinas da rede estejam rodando o Windows 98 SE, não será necessário instalar o disquete.

4 - Como no caso do Windows 2000, para que o compartilhamento funcione, você deverá configurar o TCP/IP em todas as máquinas, com exceção do servidor de conexão claro, para obter seus IP's automaticamente (como quando se disca para um provedor de acesso), e não utilizar IP's estáticos, como seria usado numa rede clássica.

As demais máquinas da rede obterão seus endereços apartir da máquina que está compartilhando a conexão, que passará a atuar como um mini-servidor DHCP.

É mais um motivo para manter o NetBEUI instalado junto com o TCP/IP, ele fará com que a rede funcione mesmo que a máquina que compartilha a conexão esteja desligada.

ICS com IP fixo

Apesar de toda a documentação da Microsoft dizer que ao usar o ICS deve-se usar endereço IP dinâmico nas estações, isso não é obrigatório, você pode usar endereços IP fixos nas estações se preferir.

Ao ativar o compartilhamento da conexão no servidor, o ICS configura a sua placa de rede interna com o endereço "192.168.0.1", este IP vale apenas para a sua rede interna, é claro diferente do endereço usado na internet.

Para que as estações tenham IP fixo, basta configura-las com endereços dentro deste escopo:

192.168.0.2, 192.168.0.3, etc. e mascara de sub-rede 255.255.255.0. Nos campos de "defaut gateway" e "servidor DNS preferencial" coloque o endereço do servidor, no caso 192.168.0.1. Prontinho.

O uso de endereços IP fixos na estações derruba boa parte das críticas feitas ao ICS do Windows, realmente muita gente não gosta do sistema de IPs dinâmicos, pois dificulta o uso da rede caso o servidor de conexão não esteja ligado para fornecer os endereços a serem usados pelas estações. Eu também prefiro usar minha rede com IPs fixos.

Detalhes sobre o ICS

"Estou começando a mexer com redes a pouco e estou com algumas dúvidas:
Com apenas uma máquina tendo speed (home) posso conectar 10 micros em rede (de Windows 98), tendo em um servidor win 98 SE? Hoje utilizamos em nossa empresa conexão Web via modem para cada micro, ainda usando pabx. Com uma rede de 10 micros, você acha que a conexão com speed compartilhado será mais rápida do que com modem em pabx? Compensa mudar o sistema em relação a velocidade de informações(a rede não é usada por todos a todo tempo....geralmente é só utilizada para enviar backups para o servidor a cada fim de turno)?

O compartilhamento de conexão oferecido pelo Windows vem se tornando bem popular. Como muita gente vem usando este recurso, também surgem várias dúvidas. Vou tentar dar uma explicação cuidadosa sobre como tudo funciona.

O ICS (Internet Conection Sharing, é o recurso do qual estamos falando :-) do Windows é na verdade um Proxy com suporte a NAT, que significa "Network Address Translation". O NAT é um recurso que permite converter endereços da rede interna em endereços a serem enviados. A "rede interna" neste caso nada mais é do que a rede da sua casa ou empresa, enquanto a rede externa é a Internet.

Imagine uma rede simples, com 3 PCs. O PC 1 é o que tem a conexão via Speedy, de 256k. Este PC precisa ter duas placas de rede, uma onde será ligado o modem ADSL e outra para liga-lo em rede com os outros dois PCs. Ao habilitar o compartilhamento de conexão, este PC passa a ser o servidor, fornecendo acesso para os outros dois PCs.

Como tem duas placas de rede, ele passará a ter dois endereços IP. O seu endereço IP na Internet, 200.183.57.176 (por exemplo) e seu endereço IP na rede, que por defaut será 192.168.0.1.

Segundo as instruções dadas pelo Windows, você deverá configurar os outros dois PCs para obterem seus endereços IP automaticamente, mas você pode configurar os IPs manualmente se quiser. Eu pessoalmente recomendo a segunda opção, pois tornará a rede mais flexível. Para isso, abra a configuração do protocolo TCP/IP e dê endereços IP para as duas estações, podem ser por exemplo 192.168.0.2 e 192.168.0.3. Em seguida, coloque o endereço do servidor, no caso 192.168.0.1 nos campos "Defaut Gateway" e "DNS primário". A máscara de sub-rede neste caso é 255.255.255.0. Rode o "Assistente para conexão com a Internet" do Windows (Iniciar > Programas > Acessórios > comunicações) e marque a opção de acessar através da rede local (creio que já expliquei isso em outros artigos)

Com isto, você configurou as duas estações para enviarem todos os pedidos para o PC 1, que é o único que está diretamente conectado à internet.

Ao abrir uma página, baixar um e-mail, abrir o ICQ, etc. em qualquer um dos dois PCs, o pedido de conexão será enviado para o PC 1, que por sua vez se encarregará de envia-los ao endereço correto na Internet, aguardar a resposta, e em seguida devolver os dados ao cliente.

Esta é justamente a função do NAT, tornar esta troca de dados transparente. Você não precisará configurar os programas para acessar a Internet via proxy, pois graças ao trabalho do PC 1, eles "pensarão" que estão diretamente conectados. Esta é a grande diferença entre o ICS e outros proxys que suportam Nat (o Wingate por exemplo) e proxys manuais, como por exemplo o Analog-X

A conexão com a Internet ficará disponível para os três PCs. Caso apenas um acesse, terá toda a conexão para si. Caso os três acessem ao mesmo tempo, a banda será dividida. Você vai perceber a conexão ficar mais lenta no PC 1 se estiver baixando arquivos no segundo, etc. Mas realmente, se comparada com uma conexão via modem, e ainda por cima via PABX, mesmo compartilhando a conexão entre 10 micros o acesso deverá ficar bem mais rápido. Se for o caso, pegue um Speedy de 2 megabits, provavelmente ainda vai sair mais barato que 10 contas de telefone :-).

O fato de compartilhar a conexão, não vai tornar sua rede mais lenta, pois a velocidade da conexão é muito pequena se comparado com os 10 ou 100 megabits que podem ser transportados através da rede.

Uma observação é que o ICS do Windows pode ser usado para compartilhar a conexão com PCs rodando outros sistemas operacionais. Basta configurar corretamente a rede, de preferencia com endereços IP fixos para que PCs com Linux, Free BSD, Windows 95, etc. acessem perfeitamente.

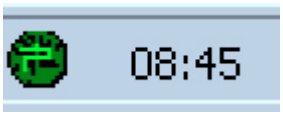
Compartilhar a conexão usando o Analog-X Proxy

O Analog-X Proxy, que pode ser encontrado na sessão de download, é um proxy bastante leve e fácil de usar que pode ser usado no caso de você não estar usando uma versão do Windows que já possua o Internet Conection Sharing, ou caso você não esteja conseguindo compartilhar a conexão através dele.

Você pode baixar o Analog-X Proxy pelo link: http://www.guiadohardware.net/download

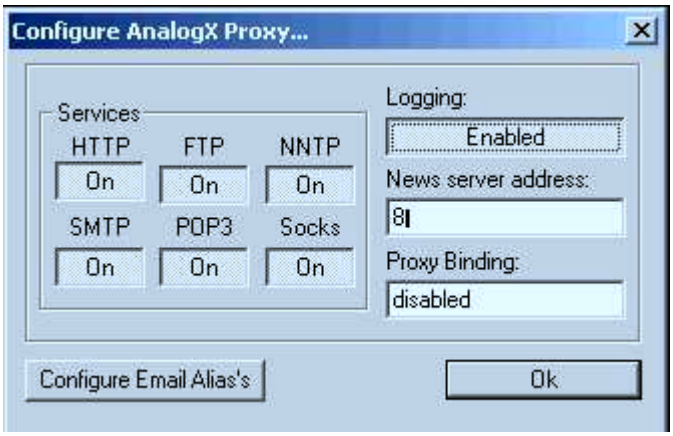
O programa é gratuíto e pode ser usado para compartilhar a conexão com um número ilimitado de estações. Claro que você deve limitar esse número de acordo com a velocidade de conexão, mas não existe limitação por parte do programa, ao contrário de alguns proxy's comerciais.

O proxy deve ser instalado apenas no PC com a conexão, surgirá um grupo no menu iniciar, com o atalho para inicializar o programa. Eu sugiro que você arraste o ícone para a pasta "Inicializar" para que você não precise ficar abrindo-o manualmente toda vez que ligar o micro. Ao ser aberto surgirá um ícone verde ao lado do relógio, indicando que o proxy está ativo.



Se o ícone estiver vermelho, significa que o proxy não está funcionando. Isso costuma acontecer caso você tenha algum outro programa servidor rodando na máquina, como por exemplo um servidor de SMTP (como o ArgoSoft Mail Server), um servidor de FTP, etc. Assim como outros proxy's, o AnalogX não custuma se entender muito bem com esses programas. Basta desativar o programa que estiver em conflito com ele e reinicializar o micro para que tudo volta à normalidade.

Com o proxy funcionando, abra a janela de configurações. Não existe muito a se configurar por aqui. você deve basicamente escolher quais protocolos devem ficar ativos, se você não for maníaco por segurança, deixe todos ativados. Se preferir, ative também o log, que será armazenado no arquivo "proxy.log", dentro da pasta onde o Proxy foi instalado



Nas estações, você precisará configurar os programas para acessar a Internet através do Proxy, programa por programa. Esta é a parte mais chata. Note também que alguns programas simplesmente não conseguirão acessar através do Analog-X, mesmo com configuração manual. A falha mais grave é o ICQ, apesar do AIM e o MS Messager, que usam um método de acesso mais simples funcionarem sem maiores problemas.

Outro problema grave é o acesso a e-mail via POP3. Você poderá usar Webmails, via browser, sem problema algum, mas existem várias limitações para baixar os e-mail apartir de um servidor de POP3. Vou explicar o que se pode fazer quanto a isso no final do tutorial.

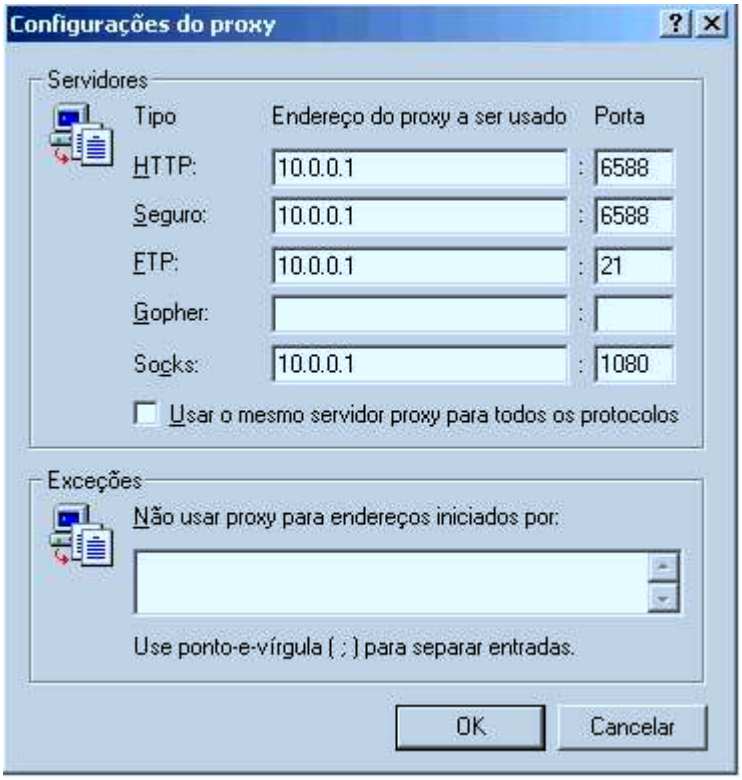
Por causa das limitações, é recomendável usar o Analog-X se a idéia for basicamente navegar através do Browser. Se você realmente precisar do ICQ e de e-mail via Pop3 em todas as estações, o mais recomendável é usar um proxy com suporte a Nat, como o Wingate, ou usar o Internet Conection Sharing do Windows.

Voltando à configuração nas estações, comece configurando o Browser. No IE 5, clique em Ferramentas > Opções da Internet > Conexões > Configurações da Lan

Marque a opção "Usar um servidor Proxy" e clique em "Avançado". Nos campos coloque o endereço IP do micro que está com a conexão, como por exemplo "10.0.0.1" e a porta a serr

usada para cada protocolo. As portas usadas pelo Analog-X são as seguintes:

HTTP:	porta 6588
HTTP Seguro:	porta 6588
SOCKS:	porta 1080
FTP:	porta 21
NNTP (news):	porta 119
POP3:	porta 110
SMTP:	porta 25



Deixe o campo “Gopher” em branco, pois o Analog-X não suporta este protocolo. O Gopher é um protocolo para buscas de arquivos, mas muito pouco usado atualmente. Creio que por isso o criador do Proxy nem se preocupou em adicionar suporte a ele.

Terminada a configuração, você já deve ser capaz de navegar normalmente através do Browser.

Se estiver usando o Opera 5, clique em File > Preferences > Connections > Proxy Servers. Surgirá uma janela parecida com a do IE. A configuração dos endereços é a mesma.

No Netscape clique em Edit > Preferences > Advanced > Proxys > Manual Proxy Configuration > View

Estas configurações valem caso você prefira usar outro proxy qualquer, que também exija configuração manual nas estações. Basta verificar quais são as portas usadas pelo proxy para cada protocolo. Outro comentário importante é que ao contrário do ICS do Windows, o Analog-X pode ser usado para compartilhar a conexão com estações rodando outros sistemas operacionais,

Linux, Free BSD, Mas OS, etc. sem problemas. Basta configurar a rede e configurar o browser para acessar através do proxy.

Para que outros programas possam acessar a Internet, novamente você deverá procurar nas configurações do programa a opção de acessar via proxy e configurar a porta. No FlashFXP (cliente de FTP) por exemplo, a configuração do proxy fica em: Options > Preferences > Proxy Firewall Ident. Na janela de configuração a opção "Proxy Server" fica como "Open (Host:Port)". No Babylon entre em Configuração > Conexão. Estes são apenas dois exemplos, o chato é que você precisará fazer o mesmo em todos os programas que forem acessar a Internet, em todas as estações.

Terminando a configuração, vem a parte mais complicada que é configurar o recebimento de e-mails via POP3. Como disse, você poderá acessar Webmails sem problema algum, já que eles são acessados pelo Browser.

No servidor, abra a janela de configuração do Analog-X e clique em "configure e-mail alia's". Clique em "add". Preencha os campos com o endereço de e-mail que será acessado e os servidores POP3 e SMTP:

Nas estações, abra o programa de e-mail e nos campos dos servidores POP e SMTP, coloque o endereço IP do servidor, 10.0.0.1 por exemplo. A estação enviará o pedido ao proxy que se encarregará de baixar os e-mails nos endereços indicados nos alias. Você pode adicionar mais de um alias, mas existe uma limitação quanto a isso que é o fato de não ser possível acessar duas contas de e-mail, como o mesmo login em servidores diferentes. Por exemplo, você pode acessar as contas visitante@guiadohardware.net e voce@seuprovedor.com.br, mas não poderá acessar voce@seuprovedor.com.br e voce@outroprovedor.com.br, a menos que fique toda hora mudando o alias no servidor. O Analog-X é bem deficitário nesse aspecto.

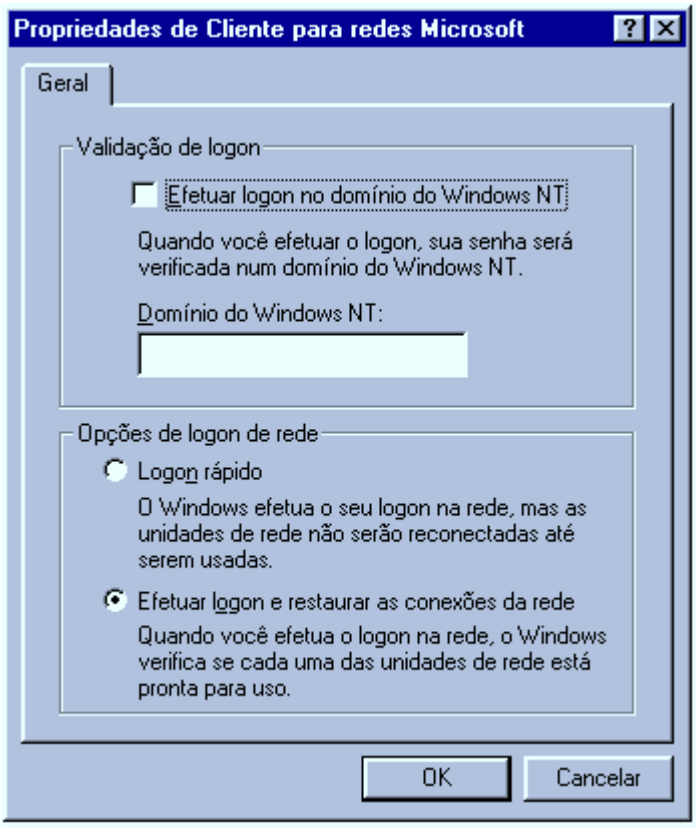
Comparado com outros proxys, a configuração do Analog-X é bastante simples e ele tem a grande vantagem de ser gratuíto. Porém, o programa também tem suas limitações. Ele pode ser quase ideal para alguns usuários e ser inusável para outros, depende do que você precisar usar através da rede e do que esperar do programa.

Acessando um Servidor Windows 2000 ou Windows NT

Além de ser usado em redes ponto a ponto, o Windows 98 pode atuar como cliente de um servidor rodando o Windows 2000 Server, ou o Windows NT Server. Estes sistemas oferecem total compatibilidade com o Windows 98. Você poderá visualizar computadores e domínios, acessar recursos compartilhados, e se beneficiar do sistema de segurança do Windows 2000 e NT Server, usando o servidor para controlar o acesso aos recursos compartilhados pela estação rodando o Windows 98.

Usando o Windows 98 como cliente de um servidor NT ou Windows 2000 (a configuração da estação é a mesma para os dois), a configuração dos serviços de rede e protocolos são parecidos com os de uma rede ponto a ponto, que vimos até agora, porém, temos à disposição alguns recursos novos, principalmente a nível de segurança. Vamos às configurações:

Depois de ter instalado a placa de rede, instalado o, ou os protocolos de rede, o cliente para redes Microsoft e o compartilhamento de arquivos e impressoras, volte à janela de configuração da rede, selecione o "cliente para redes Microsoft" e clique no botão "propriedades.



O campo de validação de logon, permite configurar a estação Windows 98 para efetuar logon no domínio NT, passando pelo processo de autenticação imposto pelo servidor. Para isso marque a opção "efetuar logon no domínio do Windows NT", e no campo "Domínio do Windows NT" escreva

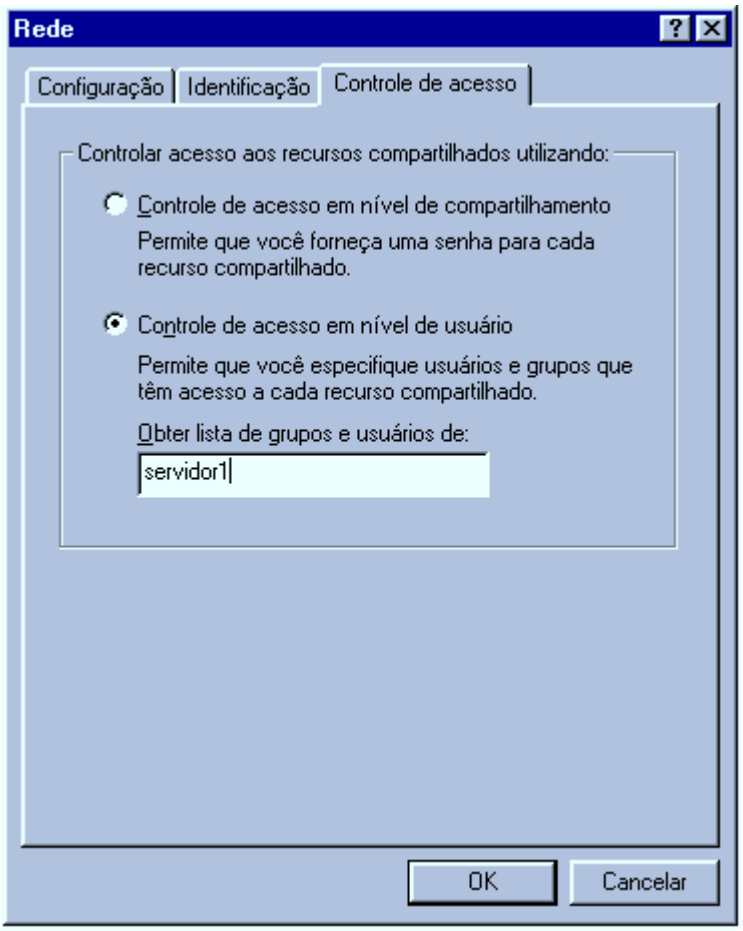
o nome do domínio NT. Obviamente, para que a estação possa logar-se é preciso antes cadastrar uma conta no servidor.

É preciso ativar esta opção para poder utilizar os recursos de perfis do usuário, scripts de logon e diretrizes de sistema permitidos pelo Windows NT e Windows 2000 Server. Ativando a opção de logar-se no servidor NT, a janela de logon que aparece quando o micro é inicializado terá, além dos campos "Nome do usuário" e "senha", um terceiro campo onde deverá ser escrito o nome do domínio NT no qual a estação irá logar-se

No campo de opções de logon de rede, você poderá escolher entre "Logon rápido" e "Efetuar logon e restaurar as conexões da rede". Esta opção aplica-se às unidades de rede que aprendemos a mapear no tópico anterior, e a qualquer tipo de rede. Escolhendo a Segunda opção, de restaurar as conexões de rede, o Windows tentará reestabelecer todas as unidades de rede, assim que você logar-se na rede. Isto traz um pequeno inconveniente: caso você tenha mapeado o CD-ROM do micro 3 por exemplo, e se por acaso quando logar-se na rede ele estiver desligado, o Windows exibirá uma mensagem de erro, que será exibida toda vez que algum recurso mapeado esteja indisponível, o que pode tornar-se inconveniente.

Escolhendo a opção de logon rápido, o Windows tentará reestabelecer a conexão com as estações que estiverem compartilhando as unidades de rede mapeadas apenas quando você for acessar cada uma. Isto torna a inicialização do micro mais rápida, diminui um pouco o tráfego na rede, economiza recursos de sistema e acaba com as mensagens chatas durante a inicialização.

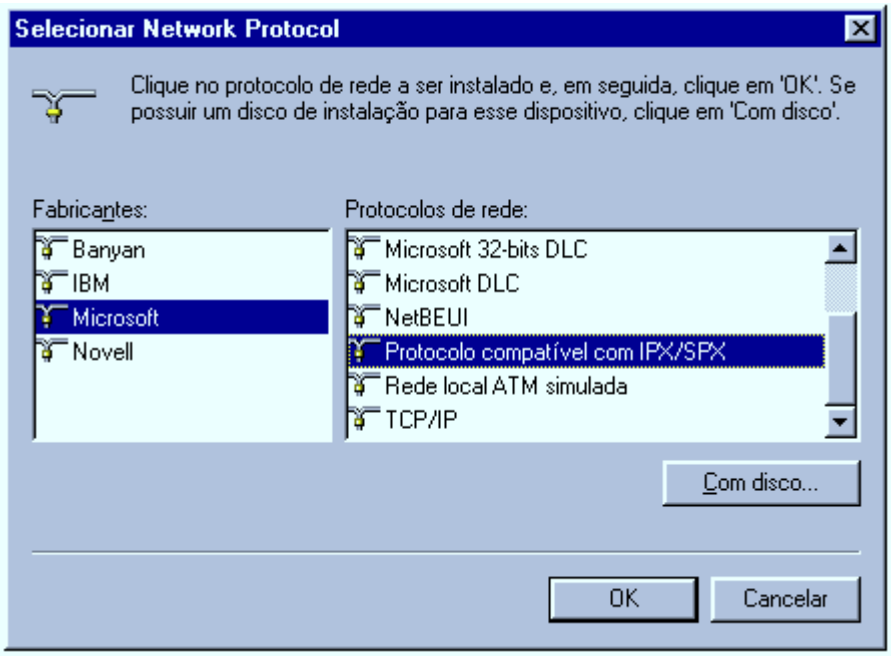
Voltando à janela principal, acesse agora a guia "controle de acesso". Lembra-se que usando uma rede não hierárquica podíamos apenas usar a primeira opção? Pois bem, logando-se em um servidor podemos agora usar a segunda opção, "Controle de acesso a nível de usuário", que permite especificar quais usuários poderão acessar os recursos compartilhados (ao invés de apenas estabelecer senhas). Ativando esta opção, o Windows abrirá o banco de dados com as contas de usuários do servidor toda vez que você compartilhar algo, permitindo que você especifique quais usuários poderão acessar o recurso. Para ativar estes recursos, basta escolher a opção de controle de acesso a nível de usuário, e fornecer o nome do servidor que armazena o banco de dados de contas dos usuários.

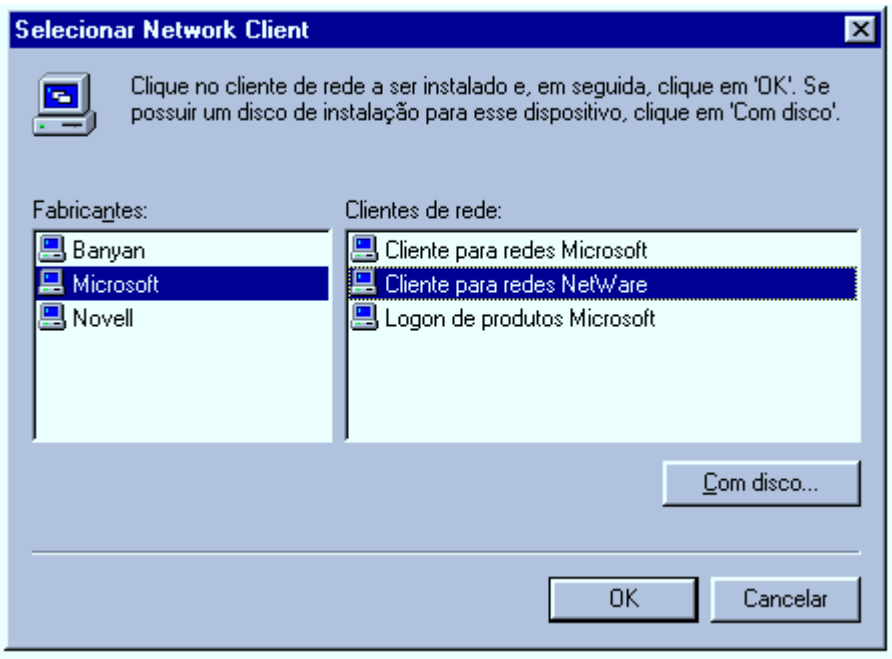


Acessando um Servidor Novell NetWare

Também é perfeitamente possível usar estações com o Windows 98 para acessar servidores Novell NetWare. Para isto é necessário ter instalado o protocolo IPX/SPX e também um cliente para redes NetWare. O cliente para redes Microsoft, que usamos até agora, permite apenas acessar outras estações Windows 95/98 ou servidores Windows NT/2000. Para instalar o protocolo IPX/SPX basta abrir o ícone de configuração da rede, clicar e "Adicionar...", "Protocolo", "Microsoft" e em seguida escolher "Protocolo compatível com IPX/SPX".

Quanto ao cliente para redes NetWare, o Windows 95/98 traz um cliente de modo protegido, que permite acessar servidores NetWare versão 3, 4 ou 5. Para instalá-lo, basta clicar em "Adicionar...", "Cliente", "Microsoft" e finalmente em "Ciente para redes NetWare".

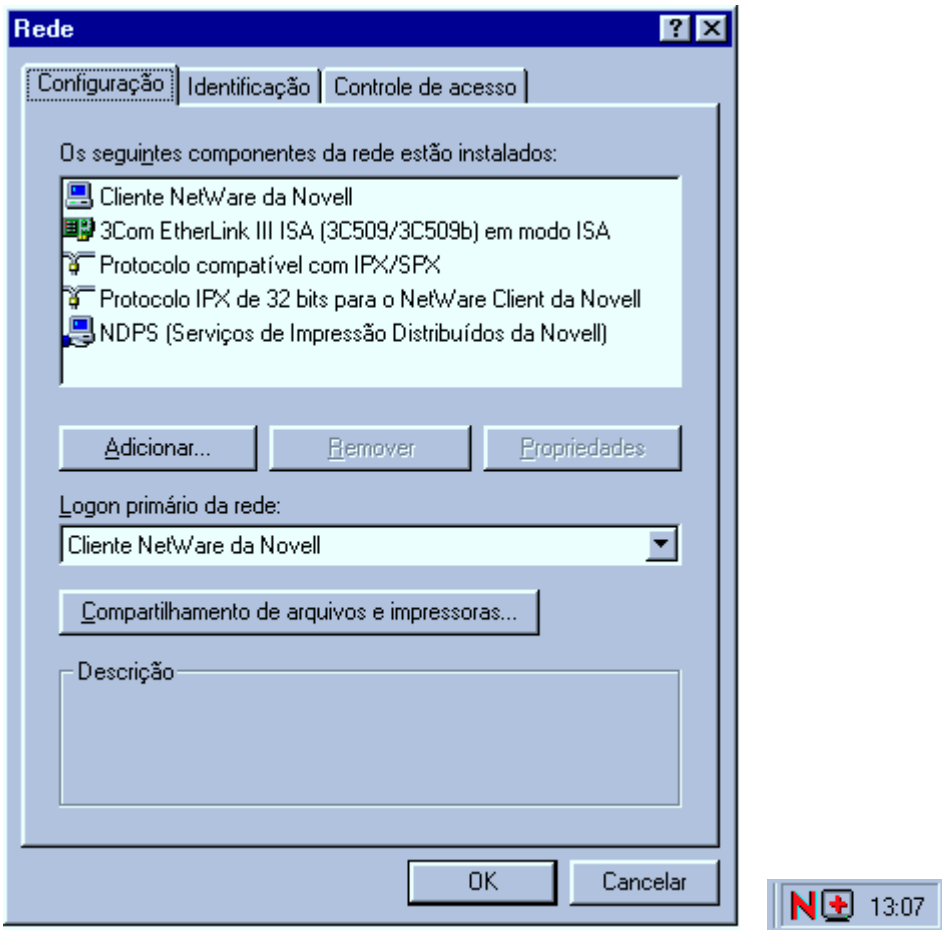




Apesar do cliente fornecido com o Windows 98 não ficar devendo muito em termos de recursos, é preferível usar o cliente fornecido pela própria Novell, que traz alguns recursos únicos, além de ser mais rápido. O programa cliente da Novell é fornecido junto com o módulo servidor, mas você também poderá baixa-lo gratuitamente (12 MB) do site da Novell: http://www.novell.com.br . Após baixar o arquivo, execute-o para que ele se descompacte automaticamente e, em seguida, execute o arquivo "setup.exe" para instalar o cliente.

O programa de instalação adicionará o "Cliente NetWare da Novell" e o "Protocolo IPX de 32 Bits para o NetWare Client da Novell" que aparecerão na janela de configuração da rede, e ficará

residente (já que você depende do programa para ter acesso ao servidor). Como no caso dos servidores NT, você deverá criar uma conta de usuário no servidor Novell e logar-se na rede infirmando no nome de usuário e senha estabelecidos.



Conectando-se a uma VPN

A pouco, vimos que uma VPN, ou rede privada virtual é uma rede de longa distância que usa a Internet como meio de comunicação. Numa VPN o servidor só precisa ter um link dedicado para que qualquer usuário da rede possa acessá-lo de qualquer parte do mundo usando a Internet. O Windows 98 pode atuar apenas como cliente de uma VPN, o servidor obrigatoriamente deve estar rodando o Windows NT 4 server, ou Windows 2000 server.

Para conectar-se a uma VPN basta marcar a "Rede Particular Virtual" que aparece dentro da pasta "Comunicações" durante a instalação do Windows. Você também pode instalar depois abrindo o ícone "adicionar/remover" do painel de controle e acessando a guia "Instalação do Windows".

Com o programa cliente instalado, abra a janela de acesso à rede dial-up e clique em "fazer nova conexão". Digite o nome do servidor VPN e no campo "selecionar um dispositivo" escolha "Microsoft VPN Adapter". Na janela seguinte digite o endereço IP do servidor VNP, clique novamente em "avançar" e em seguida em "concluir".

Para conectar-se à VPN, primeiro você deverá conectar-se à Internet usando um provedor

qualquer. Depois de conectado, abra novamente o ícone de acesso à rede dial-up e clique sobre o ícone do servidor VPN que foi criado. Na janela que surgirá digite seu nome de usuário, senha e confirme o endereço IP do servidor. Se tudo estiver correto você se conectará ao servidor e poderá acessar todos os recursos da rede remotamente. O único inconveniente será a velocidade do acesso, pois como estamos usando a Internet, e não cabos e placas de rede, teremos a velocidade de acesso limitada à velocidade do modem.

Segurança na Internet

De qualquer ponto podemos ter acesso a qualquer outro computador conectado à Internet, que esteja disponibilizando algum recurso, existe inclusive a possibilidade de invadir outros micros ou mesmo grandes servidores que não estejam protegidos adequadamente, mesmo usando como base um simples 486 ligado à Internet via acesso discado.

O protocolo TCP/IP foi concebido para ser tolerante a falhas de hardware, mas não a ataques intencionais. O principal risco é o fato dele permitir que usuários remotos acessem dados e arquivos de outros equipamentos conectados à rede. Como a Internet inteira funciona como uma grande rede TCP/IP, é possível ganhar acesso à qualquer máquina localizada em qualquer ponto do globo.

Já que o protocolo em sí não oferece grande proteção contra ataques externos, a segurança fica a cargo do sistema operacional de rede, e de outros programas, como os firewalls. Para proteger os dados que serão enviados através da rede, é possível usar um método de encriptação, para que mesmo interceptados, eles não tenham utilidade alguma. Atualmente são usados dois tipos de criptografia, de 40 bits e de 128 bits. Dados criptografados com algoritmos de 40 bits podem ser desencriptados em cerca de uma semana por alguém competente, porém a desencriptação de dados encriptados com um algoritmo de 128 bits é virtualmente impossível.

Dizemos que um sistema é perfeito apenas até alguém descobrir uma falha. Existem vários exemplos de falhas de segurança no Windows NT, em Browsers, em programas de criação e manutenção de sites Web, como o MS Front Page 2000 e até mesmo em programas como o VDO Live. Logicamente, após se darem conta da brecha, os criadores do programa se apressam em disponibilizar uma correção, mas nem todos os usuário instalam as correções e com o tempo outras falhas acabam sendo descobertas.

Por que o Unix é em geral considerado um sistema mais seguro do que o Windows NT, por exemplo? Por que por ser mais velho, as várias versões do Unix já tiveram a maioria de suas falhas descobertas e corrigidas, ao contrário de sistemas mais novos. Porém, a cada dia surgem novos softwares, com novas brechas de segurança, e além disso, cada vez mais máquinas são conectadas, ampliando a possível área de ataque.

Como são feitas as invasões

Muitas vezes os chamados Hackers são vistos pelos leigos quase como seres sobrenaturais, uma

espécie de mistura de Mac-Giver com Mister M, mas veja uma frase postada em um grande grupo de discussão sobre Hacking:.
"You may wonder whether Hackers need expensive computer equipment and a shelf full of technical manuals. The answer is NO! Hacking can be surprisingly easy!" numa tradução livre: "Você pode achar que os Hackers precisam de computadores caros e uma estante cheia de manuais técnicos. A resposta é NÃO! Hackear pode ser surpreendentemente fácil".

Frases como esta não são de se admirar, pois na verdade, a maioria dos ataques exploram falhas bobas de segurança ou mesmo a ingenuidade dos usuários, não exigindo que o agressor tenha grandes conhecimentos. Pelo contrário, a maioria dos ataques são feitos por pessoas com pouco conhecimento, muitas vezes lançando os ataques a partir do micro de casa.

Ultimamente têm sido descobertos vários ataques a sites, como por exemplo, o do Instituto de Previdência dos Servidores Militares do Estado de Minas Gerais, da Escola de Equitação do Exército, Faculdade Santa Marta e até mesmo do Ministério do Trabalho, onde as páginas principais eram substituídas por outras contendo o nome do invasor e alguns palavrões. Muitas destas invasões foram feitas aproveitando uma falha de segurança (já corrigida) do Front Page 2000, que sob certas condições permite a qualquer pessoa alterar as páginas mesmo sem a senha de acesso.

Outro caso famoso foi o de um site pornográfico Americano, que apesar de ser anunciado como um site gratuito, pedia o número do cartão de crédito do visitante "apenas como uma comprovação" de que ele era maior de 18 anos. Não é preciso dizer o que faziam com os números não é? ;-)

Hackers de verdade são capazes de lançar ataques reais a servidores aparentemente protegidos, mas sempre lançando ataques baseados em falhas de segurança dos sistemas, ou então, tentando adivinhar senhas de acesso. Uma vez dentro do sistema, a primeira preocupação é apagar evidências da invasão gravadas nos arquivos de log do sistema. Estes arquivos são alterados ou mesmo apagados, evitando que o administrador possa localizar o invasor. Em seguida, o atacante tenta conseguir mais senhas de aceso ao sistema, abrindo os arquivos do servidor que as armazenam. Caso consiga descobrir a senha do administrador, ou conseguir acesso completo explorando uma falha de segurança, pode até mesmo se fazer passar pelo administrador e atacar outras máquinas às quais a primeira tenha acesso. Para se proteger deste tipo de invasão, basta criar senhas difíceis de serem adivinhadas, se possível misturando letras e números com caracteres especiais, como @$#%& etc. e usar um sistema seguro, com todas as correções de segurança instaladas. Um bom programa de firewall completa o time.

Outras estratégias de invasão e roubo de dados, são usar programas keytrap (rastreadores de teclado que armazenam tudo que é digitado, inclusive senhas, em um arquivo que pode ser recuperado pelo invasor), cavalos de Tróia, monitores de rede, ou outros programas que permitam ao invasor ter acesso à maquina invadida. Para isto, basta enviar o arquivo ao usuário junto com algum artifício que possa convencê-lo a executar o programa que abrirá as portas do sistema, permitindo seu acesso remoto. Um bom exemplo deste tipo de programa é o back orifice.

Veja que neste caso não é preciso nenhum conhecimento em especial, apenas lábia suficiente para convencer o usuário a executar o programa, que pode ser camuflado na forma de um jogo ou algo parecido.

Caso o invasor tenha acesso físico à máquina que pretende invadir (o micro de um colega de trabalho por exemplo), fica ainda mais fácil. Um caso real foi o de um auxiliar de escritório que

instalou um keytrap no micro do chefe e depois limpou sua conta usado a senha do home banking que havia conseguido com a ajuda do programa.

Como se proteger

Hoje em dia, "Segurança na Internet" parece ser um tema de grande interesse, talvez pela complexidade (ou simplicidade, dependendo do ponto de vista :-) ou talvez pela pouca quantidade de informações disponíveis sobre o tema. Tanto que entre os 10 livros de informática mais vendidos, 3 tem como tema os "Hackers". O meu objetivo neste artigo é passar um pouco da minha experiência pessoal sobre o assunto.

Existem várias formas de se roubar dados ou invadir computadores. 99% das invasões se dá devido a um (ou vários) dos seguintes fatores:

1- Trojans como o Back-orifice instalados no micro

2- Bugs de segurança do Windows, IE, Netscape, ICQ ou de qualquer programa que estiver instalado no micro.

3- Portas TCP abertas

4- Descuido ou ingenuidade do usuário.

Trojans

Em primeiro lugar, vem os trojans. Os trojans, como o Back-orifice, Netbus e outros, nada mais são do que programas que uma vez instalados transformam seu computador num servidor, que pode ser acessado por qualquer um que tenha o módulo cliente do mesmo programa. Estes programas ficam quase invisíveis depois de instalados, dificultando sua identificação. De qualquer forma, como qualquer outro programa, estes precisam ser instalados. Ninguém é contaminado pelo BO de graça, sempre a contaminação surge devido a algum descuido.

Para isso pode-se usar de vários artifícios. Pode-se enviar o trojam disfarçado de um jogo ou qualquer outra coisa, fazendo com que o usuário execute o arquivo e se contamine (opção 4, ingenuidade do usuário...); o arquivo pode ser instalado quando você for ao banheiro por um "amigo" visitando sua casa...; ou finalmente, pode ser instalado sem que você perceba aproveitando-se de alguma vulnerabilidade em um dos programas que você tenha instalado.

Qualquer antivírus atualizado vai ser capaz de detectar estes programas e elimina-los, porém para isto é preciso que você atualize seu antivírus sempre, pois praticamente a cada dia surgem novos programas, ou versões aperfeiçoadas, capazes de enganar as atualizações anteriores. Não adianta nada manter o antivírus ativo caso você não baixe as atualizações. Pensando nisso, alguns programas, como o AVP avisam irritantemente sobre novas atualizações disponíveis

Bugs

Quanto aos bugs nos programas, estes costumam ser os mais simples de se resolver, pois assim que um bug se torna público o fabricante se apressa em lançar uma correção para ele. No caso do Windows e do Internet Explorer, as correções podem ser baixadas usando o Windows Update ou então ser baixadas manualmente apartir do site da Microsoft. Falando em correções, lançaram algumas esta semana, aproveite a deixa para ir baixá-las.

No caso de outros programas, como o Netscape por exemplo, você pode baixar as atualizações disponíveis apartir da página do fabricante. Em muitos casos os bugs são corrigidos apenas ao ser lançada uma nova versão do programa. Por exemplo, as versões antigas do ICQ tinham um bug que mostrava o endereço IP dos contatos da sua lista mesmo que ele estivesse escondido (como N/A) caso você desconectasse o ICQ e checasse novamente o Info do contato. Isto foi corrigido apartir do ICQ 98a.

Quem acessa a Net a mais de um ou dois anos, deve se lembrar que até algum tempo atrás, existiam vários programas de Nuke, que derrubavam a conexão e travavam o micro da vítima. Atualmente a grande maioria destes programas não funciona, justamente por que o Bug do Windows 95a que o tornava vulnerável a este tipo de ataque foi corrigido apartir do Windows 95 OSR/2.

Outra safra de vulnerabilidades comuns, são as de buffer overflow, que atingem um número muito grande de programas.

Os Buffers são áreas de memória criadas pelos programas para armazenar dados que estão sendo processados. Cada buffer tem um certo tamanho, dependendo do tipo de dados que ele irá armazenar. Um buffer overflow ocorre quando o programa recebe mais dados do que está preparado para armazenar no buffer. Se o programa não foi adequadamente escrito, este excesso de dados pode acabar sendo armazenado em áreas de memória próximas, corrompendo dados ou travando o programa, ou mesmo ser executada, que é a possibilidade mais perigosa.

Se um programa qualquer tivesse uma vulnerabilidade no sistema de login por exemplo, você poderia criar um programa que fornecesse caracteres de texto até completar o buffer e depois enviasse um executável, que acabaria rodando graças à vulnerabilidade.

Um caso famoso foi descoberto ano passado (2000) no Outlook Express. Graças à uma vulnerabilidade, era possível fazer com que um e-mail executasse arquivos apenas por ser aberto! Bastava anexar um arquivo com um certo número de caracteres no nome, que ele seria executado ao ser aberta a mensagem. Naturalmente, a Microsoft se apressou em lançar um patch e alertar os usuários para o problema. Felizmente, pelo menos por enquanto, não foi descoberta mais nenhuma vulnerabilidade tão perigosa no Outlook.

Semanalmente são descobertas vulnerabilidades de buffer overflow em vários programas. Algumas são quase inofensivas, enquanto outras podem causar problemas sérios. O próprio codered se espalhou tão rapidamente explorando uma vulnerabilidade do IIS da Microsoft. Com isto, o worm podia contaminar servidores desprotegidos simplesmente enviando o código que explora o bug, sem que ninguém executasse nenhum arquivo.

Portas TCP abertas

O terceiro problema, as portas TCP abertas é um pouco mais complicado de detectar. O protocolo TPC/IP que usamos na Internet é composto por uma série de portas lógicas. É mais um menos como um número de telefone com vários ramais.

Existem no total 65.535 portas TCP. Como no exemplo do ramal, não basta que exista um ramal, é preciso que exista alguém para atendê-lo, caso contrário ele não servirá para nada. Para que uma porta TCP esteja ativa, é preciso que algum programa esteja "escutando" a porta, ou seja, esteja esperando receber dados através dela. Por exemplo, a porta 21 serve para transferir arquivos via FTP, a porta 80 serve para acessar páginas Web e assim por diante.

Existem dois modos de acesso, como servidor e como host. Servidor é quem disponibiliza dados e host é quem acessa os dados. Ao abrir o www.guiadohardware.net, o servidor onde o site está hospedado é o servidor e você é o host. Excluindo-se algum eventual bug do navegador, não existe qualquer perigo em acessar uma página ou qualquer outra coisa como simples host, já que o seu papel será simplesmente receber dados e não transmitir qualquer coisa.

O perigo é justamente quando um programa qualquer que você tenha instalado no micro abra qualquer uma das portas TCP, transformando seu micro num servidor. Como citei no início do artigo, é justamente o que os trojans fazem.

Além dos trojans, existem várias outras formas de ficar com portas TCP abertas, como por exemplo manter um servidor de FTP, manter o Napster ou qualquer outro programa que compartilhe arquivos aberto, ou mesmo manter seu ICQ online. Nestes casos porém o aplicativo se encarrega de oferecer segurança, bloqueando a porta aberta, mas um bom programa de firewall completará o time, oferecendo uma proteção adicional.

Um erro comum neste caso é manter o "compartilhamento de arquivos e impressoras" habilitado na conexão com a Net. Como o nome sugere, este serviço serve para compartilhar seus arquivos e impressoras com a rede onde você estiver conectado, ou seja, com a Internet Inteira! Qualquer um com um scanner de portas pode achar rapidamente dezenas de "patos" com o compartilhamento habilitado e invadi-los facilmente, sem sequer precisar usar o back-orifice ou qualquer outro programa, apenas o ambiente de redes do Windows.

Para verificar se você é uma das possíveis vítimas, verifique o ícone "rede" do painel de controle. Aqui estão listados todos os protocolos de rede instalados. Presumindo que esteja acessando via modem e o seu micro não esteja ligado em rede, deixe apenas o protocolo TCP/IP e o "adaptador para redes dial-up".

No Windows 2000 abra o painel de controle/conexões dial-up e rede e clique com o botão direito sobre o ícone da conexão e abra as propriedades. O Win 2000 não usa mais o adaptador para redes dial-up, por isso deixe apenas o protocolo TPC/IP.

Se você estiver curioso sobre as portas TCP abertas do seu micro, existe um site, o http://www.hackerwhacker.com que vasculha boa parte das portas TPC do micro, alertando sobre portas abertas.

Roubo de dados e senhas

Esta é outra possibilidade perigosa, mais até do que a possibilidade de ter seu micro invadido. Afinal, se alguém conseguir descobrir a senha do seu Internet Bank vai pode fazer a limpa na sua conta.

Mesmo que o seu micro esteja completamente protegido contra ataques externos, isto não garante que os dados e senhas enviados tenham a mesma segurança.

A arma mais eficiente neste caso é a criptografia, usada para garantir a segurança das transações bancárias online. O uso de criptografia garante que mesmo que alguém consiga interceptar os dados, estes sejam completamente inúteis. Você também pode usar criptografia nos e-mails e mesmo em outras aplicações que considerar importantes, usando os programas adequados.

Outra recomendação importante é trocar regularmente as senhas, se possível uma vez por semana. As senhas não devem ser óbvias, contando palavras do dicionário ou datas. O ideal é criar senhas de pelo menos 7 caracteres que misturem letras, números e (caso o servidor permita), caracteres especiais. Para não esquecer as senhas, você pode inventar as senhas usando frases: "Chico tinha 3 maçãs e comeu duas" por exemplo, pode virar "Ct#3MeC2", uma excelente senha.

Porém, o risco maior neste caso reside no mundo de carne e osso. Na grande maioria dos casos, as senhas são conseguidas não devido à simples adivinhação, mas a algum descuido do usuário. Por isso, tome o cuidado de destruir todos os papeizinhos onde tenha anotado senhas, sempre cubra o teclado ao digitar uma senha, caso tenha alguém por perto, etc.

Um golpe que vem sendo bastante usado é enviar um e-mail fazendo-se passar pelo banco ou provedor de acesso, pedindo dados como parte de alguma confirmação, recadastramento, ou qualquer coisa do gênero. Parece absurdo, mas muita gente acaba acreditando e enviando os dados...

Antivírus

Depois de falar sobre as possíveis brechas de segurança, nada melhor do que começarmos a estudar como nos proteger.

A primeira coisa é manter instalado um bom antivírus. Você pode perguntar o que um antivírus tem a ver com proteção contra invasões, tem tudo a ver! A grande maioria das invasões são feitas usando trojans, como o Back-orifice, Netbus, etc. É relativamente fácil pegar uma destas pragas, pois eles podem ser facilmente mascarados, ou mesmo "temperar" um programa qualquer. Você instala um programa de procedência duvidosa e ganha uma instalação do Back-orifice completamente grátis :-)

Os antivírus estão tornando-se cada vez mais precisos em detectar estes programas, da mesma forma que detectam vírus, já prevenindo 90% das invasões. Para isto vale novamente martelar que o antivírus deve ser atualizado constantemente e a proteção automática deve estar habilitada.

Tenha em mente que os trojans são de longe os mais usados, por serem os mais fáceis de usar. Não é preciso ser Hacker, conhecer portas TCP ou bugs nos programas, usar Linux e nem mesmo ter um QI acima da média para usa-los, basta apenas ter lábia suficiente para levar o usuário a executar o arquivo, e rezar para que o antivírus esteja vencido. Alguns trojans são tão fáceis de usar quanto um programa de FTP.

Completando o antivírus, também vale um pouco de cultura geral: jamais abra qualquer executável antes de passar o antivírus, evite ao máximo abrir qualquer arquivo que lhe tenha sido enviado por e-mail, ou pelo menos passe o antivírus antes, abra arquivos .doc suspeitos no WordPad do Windows ao invés do Word, pois ele não executa macros. Preste atenção na extensão do arquivo, um truque comum é usar nomes como Feiticeira.jpg_____ .pif, onde o usuário desatento vê apenas o "Feiticeira.jpg", pensando se tratar de uma inocente imagem, sem perceber a extensão pif escondida por vários espaços.

Na minha opinião, o melhor antivírus atualmente é o AVP, www.avp.com , mas outras excelentes opções são o Norton Antivírus www.symantec.com , McAfee, www.mcafee.com e o Panda http://www.pandasoftware.com .

Outro excelente antivírus, que se destaca por ser totalmente gratuíto, incluindo as atualizações, é o Free-AV que pode ser baixado em http://www.free-av.com/

Se você for do tipo paranóico, também pode manter mais de um antivírus instalado, afinal, nenhum programa é perfeito. Neste caso o melhor seria deixar o que você confiar mais com a proteção automática habilitada e usar os demais apenas para verificação manual de algum arquivo mais perigoso.

Os fabricantes de antivírus se orgulham de exibir o número de vírus que o programa é capaz de encontrar, mas um programa que é capaz de detectar 70.000 vírus não é necessariamente melhor que um que é capaz de encontrar 50.000 vírus por exemplo. O que adianta detectar um monte de vírus antigos se ele não for capaz de impedi-lo de executar um arquivo infectado por um vírus atual? Assim como a gripe, novas espécies de vírus se alastram muito rapidamente, em questão de dias. É muito maior a possibilidade de você acabar contaminado por um vírus recente do que por um de um ou dois anos atrás.

Por isso, a freqüência das atualizações, e a competência em encontrar novos vírus rapidamente acaba contando muito mais do que simplesmente o total.

Firewalls e portas TCP

Finalmente veremos quais os principais programas de firewall doméstico disponíveis e as principais dicas de configuração. Mas, em primeiro lugar, qual é a função de um firewall e quais meios são usados para nos oferecer proteção?

Presumindo que você já esteja com um bom antivírus instalado, mantenha a proteção automática habilitada e não fique abrindo qualquer coisa que chegue por mail, você já está praticamente protegido dos trojans, que como disse, são os principais responsáveis pelas invasões.

Porém, ainda restam duas maneiras de conseguir invadir seu micro: através de portas TPC abertas e através do seu Browser, quando você visitar alguma página com um script malicioso. Depois que os browsers passaram a ter suporte a java e a Microsoft criou o ActiveX, os browsers se tornaram muito vulneráveis a este tipo de ataque. Por exemplo, o Windows Update transmite dados dos arquivos de configuração do Windows e instala automaticamente programas através do Browser. O http://www.myspace.com , que oferece 300 MB de armazenagem para backups, usa para as transferências de arquivos um applet java que acessa diretamente seu disco rígido. Claro que em ambos os casos os recursos são usados de forma a apenas oferecer mais um serviço ao usuário, sem intenção de causar qualquer dano, mas sistemas semelhantes podem (e já tive notícias de realmente já terem sido usados) para roubar arquivos, instalar trojans e vírus, etc. tudo isso simplesmente por visitar uma página Web!

Um bom firewall se encarrega de barrar este tipo de abuso. O E-Safe por exemplo vai avisar sobre a tentativa de violação tanto ao acessar o Windows Update quanto Myspace já com a configuração de segurança padrão, o que garante a proteção contra sistemas parecidos, mas com fins maliciosos. O E-Safe não vai barrar ação o que seria incômodo, apenas vai exibir um aviso da violação e perguntar se você deseja continuar ou barrar a ação. Configurando a segurança como máxima a ação já vai ser barrada automaticamente, o que vai oferecer uma proteção maior, mas vai se tornar incômodo, por impedir que você acesse serviços úteis.

As portas TCP e UDP por sua vez são portas lógicas, que caso abertas formam o meio conecção que alguém pode usar para obter acesso ao seu micro remotamente. Mesmo alguém que tenha seu endereço IP e domine todas as técnicas de invasão, não vai poder fazer absolutamente nada caso você não tenha nenhuma porta TCP aberta.

O problema é que as portas TCP e UDP são também usadas pelos programas, por isso é muito difícil manter todas as portas fechadas. Sempre vai sobrar alguma entrada para tornar seu PC vulnerável. Novamente entra em cena o firewall, que se encarrega de monitorar todas as portas TPC abertas, barrando qualquer comunicação potencialmente perigosa.

O grande problema dos firewalls, é que acessos perfeitamente legítimos podem ser facilmente confundidas com tentativas de invasão, veja os exemplos do Windows Update de do Myspace por exemplo. Um bom firewall deve ser esperto o suficiente para distinguir o joio do trigo e não focar incomodando o usuário com avisos falsos. Afinal, o que ia adiantar um firewall que ficasse emitindo alertas cada vez que você tentasse abrir uma página qualquer, abrir o ICQ ou simplesmente baixar os e-mails?

Zone-alarm

O Zone Alarm oferece uma boa proteção, não exige muita configuração e tem a vantagem de possuir uma versão gratuíta, que pode ser baixada em: http://www.zonelabs.com/

O Zone Alarm tem três opção de segurança: Normal, High (alta) e Low (baixa), que podem ser alteradas a qualquer momento na janela principal. Na minha opinião, a melhor opção é a Normal, pois na High o programa emite muitos avisos falsos e bloqueia vários programas, enquanto na Low ele oferece pouca proteção.

Em comparação com outros firewalls, o Zone Alarm emite poucos alarmes falsos (na configuração defaut) e tem um sistema de Log, que permite que o programa “aprenda”, passando a emitir cada vez menos avisos desnecessários. Ele também pedirá autorização para cada aplicativo que

deseje abrir uma porta TCP, permitindo que você autorize os programas que use (IE, Netscape, ICQ, etc.), mas possa barrar o Back Orifice por exemplo :-) Em termos de eficiência ele é um dos melhores.

Black ICE

É outro programa excelente. O ponto forte é o fato de emitir avisos detalhados, dando detalhes sobre o tipo de ataque e dando o IP do autor. A configuração do Black ICE tem quatro opções: Paranoid (paranóico), Nervous, Cautions e Trunsting (confiante).

A opção Paranoid bloqueia quase tudo, não é utilizável a menos que você acesse as configurações avançadas do programa e especifique manualmente o que o programa deve permitir. A opção Trunsting por outro lado não emite avisos, mas oferece pouca proteção.

A Cautions, oferece segurança média e poucos avisos desnecessários, detecta apenas ataques mais sérios, mas é bastante falha. Se você já estiver contaminado pelo Back Orifice por exemplo, esta opção não vai bloquear as invasões caso o BO seja configurado para usar outra porta TPC que não seja a Defaut.

A opção Nervous já detecta todas as tentativas de invasão, mas por outro lado impede o funcionamento de alguns programas. O ICQ por exemplo só vai funcionar depois de você mexer nas configurações avançadas do programa.

Em termos de recursos e eficiência, o BlackICE rivaliza com o Zone Alarm, a grande desvantagem é o fato de custar 40 dólares, enquanto o Zone Alarm é gratuíto. Você pode obter detalhes sobre o preço e condições de compra no: http://www.networkice.com/html/small_home_office.html

E-Safe

O E-Safe oferece como ponto forte o antivírus embutido e as Sandboxes. Estes dois recursos permitem que o E-Safe trabalhe de uma forma bem diferente dos outros firewalls. Ao invés de monitorar os aplicativos e o que entra e sai pelas portas TCP e UDP, o E-Safe monitora os dados que entram e saem, além de monitorar a ação de vírus.

Isto permite que o E-Safe emita poucos alarmes falsos, dando avisos apenas quando realmente ocorre alguma violação mais séria. Em contrapartida ele não oferece alguns recursos úteis encontrados nos outros dois: não bloqueia automaticamente portas TCP, não esconde portas TCP e não protege contra nukes e ataques DoS (que fazem a conexão cair). No caso dos nukes, não chega a ser uma deficiência grave, pois o Windows apartir do 95 OSR/2 já não é vulnerável a este tipo de ataque.

Como disse, o E-Safe não bloqueia as portas TCP automaticamente. Para isso você deve abrir a janela de configuração ("Configurar" na janela principal) e clicar em "Configuração Avançada". Acesse em seguida a Guia "Firewall", clique em "Mapa de firewall" e no espaço escrito "Blank" escolha "Trojans/Hackers Ports" e adicione as portas que deseja bloquear. Visite o http://networkscan.com:4000/startdemo.dyn para ver quais portas TCP estão abertas no seu micro.

Na mesma janela de configurações avançadas , você pode configurar o antivírus e os filtros de

conteúdo, outro recurso interessante do E-Safe, que permite usa-lo também para bloquear o acesso a páginas indesejáveis, ou até mesmo para sumir com os e-mails com propagandas. Clicando no botão "assistente" surge um Wizzard que ajuda a configurar algumas opções mais básicas, como se por exemplo você deseja limpar o Histórico do Internet Explorer sempre que desligar o micro.

Por precisar de muita configuração manual, o E-Safe é recomendado para usuários intermediários ou avançados. O programa é gratuíto para uso pessoal e pode ser baixado em: http://www.aladdin.com.br

Usando tanto o Zone Alarm quanto o BlackICE, é indispensável que você mantenha também um bom antivírus instalado. Usando o E-Safe o antivírus já passa a ser opcional, pois sozinho o programa oferece proteção contra vírus. Entretanto, se você deseja o máximo de proteção, pode manter o E-Safe junto com o seu antivírus favorito sem problema algum.

Se você está preocupado com o desempenho do micro, o E-Safe sozinho gasta bem menos recursos do sistema do que o Zone Alarm (ou BlackICE) mais um Antivírus, apesar de sozinho também oferecer uma proteção um pouco mais falha.

Xô Bobus

Este é um programa Brasileiro que vem sendo bastante elogiado. "Xô BoBus" é abreviação de "Xô Back Orifice e Net Bus". Na verdade este não é um firewall completo, mas sim um detector de trojans. Ele monitora 55 portas TCP e é capaz de detectar 170 trojans e worms. A principal vantagem do Xô BoBus é o fato do programa ser extremamente leve e fácil de usar e de ser todo em português, contanto inclusive com suporte técnico da equipe. Ele não oferece uma proteção tão completa quanto o Zone Alarm ou BlackICE e como ele não dispensa a ajuda de bom antivírus, mas já é capaz de impedir a maioria das tentativas de invasão. O Xô BoBus é gratuíto e pode ser baixado em: http://www.xobobus.com.br

McAfee Personal Firewall

Além do antivírus, a McAfee também tem o seu firewall doméstico. Também tem uma boa eficiência e os mesmos três níveis de proteção do Zone Alarm, mas gera bem mais mensagens desnecessárias que ele. Também gera um arquivo de log, com todas as tentativas de invasão detectadas, mas ele não é tão completo nem tão simples de entender quanto o log do BlackICE. Outra desvantagem é o fato e custar 30 dólares.

Para baixar um trial de 10 dias, ou para informações, consulte:
http://www.mcafee.com/login_page.asp?a=ok

Norton Personal Firewall

O Norton é o programa de Firewall mais caro que encontrei. Custa 50 dólares e mais 7 dólares por ano pelas atualizações, apartir do segundo ano. O ponto forte do Norton é a grande quantidade de opções. É possível, por exemplo, bloquear aquelas janelas pop-up que são abertas quando você acessa alguns sites. De qualquer forma, a configuração pode confundir quem não tem muita base

sobre o assunto, ou quem não entende inglês.

Informações em: http://www.symantec.com/sabu/nis/npf/

Sybergen Secure Desktop

O Secure desktop é outro Firewall gratuíto. O ponto forte é a Interface bastante simples e um log detalhado e fácil de acessar. Mas, em termos de eficiência fica devendo um pouco. Ele não coloca as portas TCP em modo de reserva, não oferece proteção contra ataques DoS e Nukes, detecta o Back Orifice apenas no modo de segurança máxima e não desativa o compartilhamento de arquivos e impressoras (caso o usuário tenha esquecido de desativar). Na minha opinião é o programa mais fraco dos que indiquei aqui.

O Secure Desktop pode ser baixado em: http://www.sybergen.com/products/shield_ov.htm

Dicas para tornar seu Windows 2000 um sistema seguro

Um bom programa de Firewall garante um nível extra se segurança para qualquer sistema. Muitas vezes, mesmo um sistema vulnerável pode tornar-se seguro com a ajuda de um bom firewall. Afinal, mesmo que um servidor qualquer esteja habilitado, se ninguém conseguir enxergar sua máquina na Web, ou todas as tentativas de conexão forem barradas pelo firewall, ninguém poderá fazer nada.

Mas, eu penso que um sistema deve ser seguro mesmo sem a proteção de um firewall. Você se sentiria seguro contratando um segurança, mas deixando todas as portas da sua casa abertas?

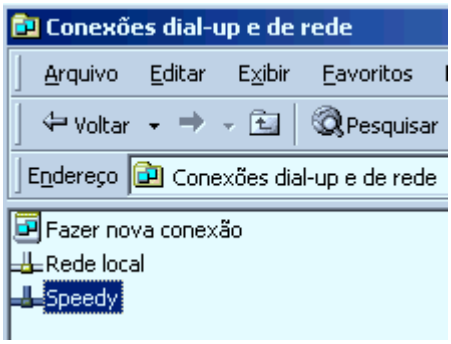
A idéia deste texto é dar dicas de como tornar o seu Windows 2000, tanto Professional quanto Server um sistema mais seguro. Com estes cuidados, mesmo alguém experiente terá grandes dificuldades em fazer qualquer coisa, mesmo sem um firewall ativo. Claro, que estes cuidados não dispensam a dupla antivírus e firewall, mas aumentarão bastante a segurança do seu sistema. Hoje em dia, existem vários bons programas gratuítos, você pode usar por exemplo o Free-AV e o Zone Alarm que estão disponíveis na sessão de download, ambos são excelentes programas, além de gratuítos.

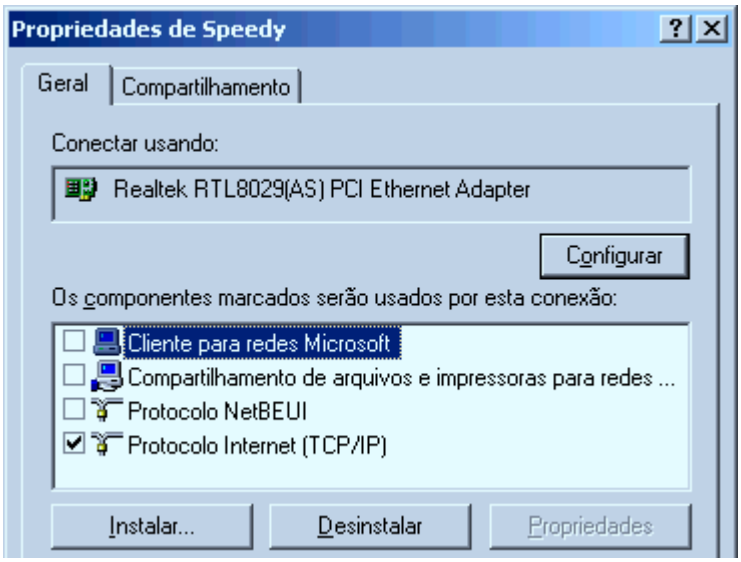
O básico

Parece incrível, mas mesmo hoje em dia, muita gente ainda esquece o compartilhamento de arquivos e impressoras habilitado. Isto é uma falha de segurança incrível, mesmo que todos os compartilhamentos estejam protegidos por senha. Já existem cracks que permitem quebrar as senhas de compartilhamento rapidamente.

Mesmo que você tenha uma rede doméstica e precise manter estes recursos ativos na rede interna, não existe desculpa para mante-los ativos também na conexão com a Internet.

No Windows 2000, as conexões aparecem como ícones separados na pasta "Conexões dial-up e de rede", dentro do painel de controle. Você pode configurar as conexões de forma independente, deixando o compartilhamento de arquivos, cliente para redes Microsoft, etc. habilitados para a rede doméstica e desabilitar tudo, com exceção do TCP/IP na conexão com a Internet





Outra coisa básica é o problema dos vírus e trojans, que chegam ataxados sobretudo nos e-mails. A proteção neste caso é um pouco de cultura, dicas manjadas como não abrir arquivos ataxados com extensões suspeitas, .vbs, .exe, etc. e manter um antivírus atualizado. Note que mesmo um antivírus atualizado todo mês ou toda semana não é uma proteção 100% eficaz, pois os vírus mais perigosos costumam ser os mais recentes, que se espalham em questão de horas, antes de qualquer desenvolvedor de anti-virus conseguir desenvolver uma vacina. Outros vilões são os arquivos .doc. Eu simplesmente não abro arquivos .doc que recebo por e-mail no Word. Ou simplesmente deleto, ou caso seja algo importante, os abro no Wordpad, que não executa vírus de macro. Quando for enviar um texto para alguém, salve-o em html ou então em .rtf, que são formatos de arquivos que qualquer um poderá abrir sem susto.

As dicas

Não fique chateado, este primeiro trecho do texto trouxe as dicas se sempre apenas para constar, nunca é demais martelar na mesma tecla. Se alguns vírus conseguem contaminar 10 milhões de computadores em 10 ou 12 horas, significa que muita gente ainda não está seguindo estas dicas simples.

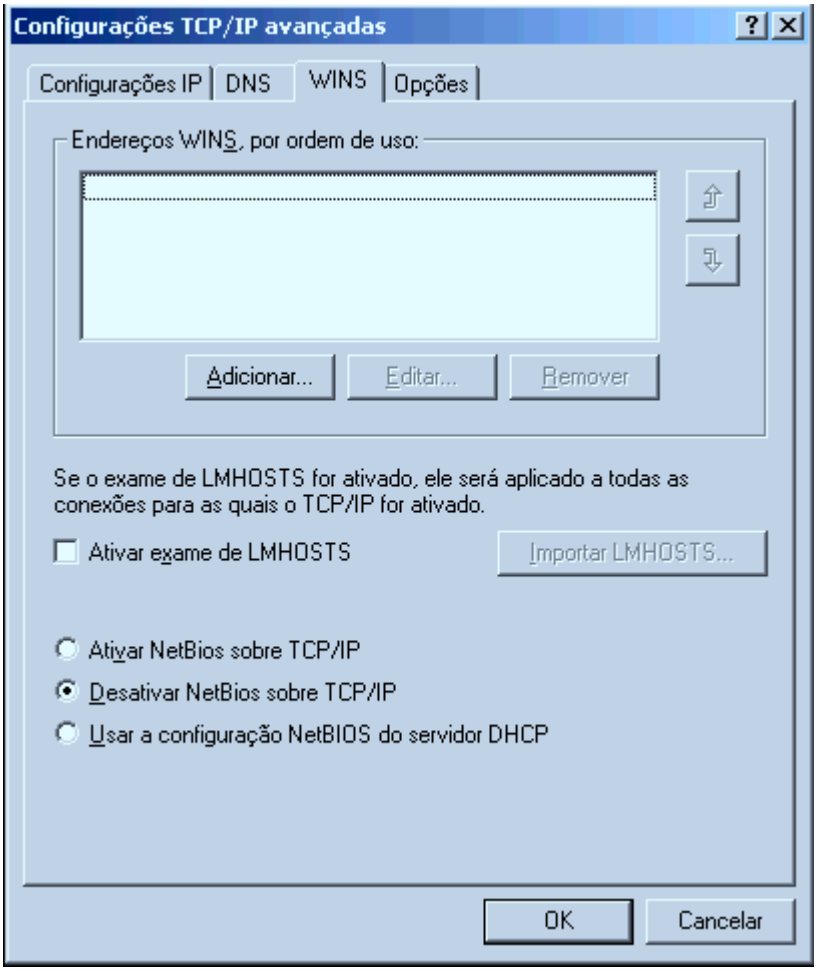
Abaixo estão finalmente as dicas que gostaria de dar neste artigo. Se você já tem conhecimentos básicos de segurança, esqueça a primeira parte e imagine que o tutorial está começando agora.

TCP/ IP

Na janela de propriedades da sua conexão com a Internet, a mesma da figura anterior, selecione o protocolo TCP/IP e clique em propriedades e em seguida no botão "avançado"

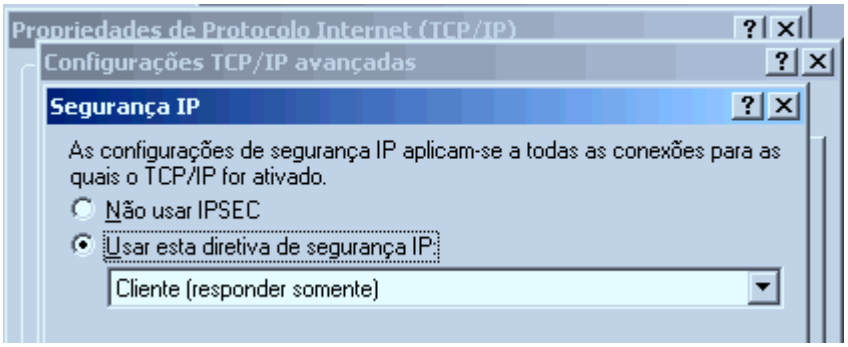
Aqui estão algumas configurações importantes do TCP/IP, que muitos não conhecem.

Comece abrindo a aba "Wins". Desative as opções "Ativar exame de LMHosts" (a menos que você vá precisar deste recurso, claro) e, o mais importante, marque a opção "desativar netBios sobre TCP/IP" que vem ativada por defaut.



O recurso de NetBios sobre TCP/IP permite localizar compartilhamentos de arquivos e impressoras disponíveis na máquina. Isto significa que o seu Windows responderá se existem compartilhamentos ativos na sua máquina para qualquer um que perguntar. Caso você não tenha esquecido nenhum compartilhamento habilitado, não existe um grande risco, pois o Windows responderá apenas que "não existe nenhum compartilhamento habilitado", mas, caso você tenha esquecido algum compartilhamento ativo, pode ter certeza que com o NetBios habilitado, qualquer um com um mínimo de disposição poderá acessa-lo, mesmo que esteja protegido por senha. Bastará dar um Netstat, ou usar um port scanner qualquer e em seguida usar uma das já manjadas ferramentas para quebrar a senha do compartilhamento. É melhor não facilitar.

Na aba de "opções" existe uma outra configuração interessante. Clique em "segurança de IP" e em "propriedades". Marque a opção "ativar esta diretiva se segurança IP" e escolha a opção "Cliente (responder somente)". Esta opção serve apenas para máquinas usadas para acessar a Net, não para servidores, naturalmente.



Contas

Terminada a configuração dentro do protocolo TCP/IP, vamos para outra medida de segurança igualmente importante. Abra o painel de controle > Usuários e senhas.

O Windows, por defaut, cria compartilhamentos administrativos de todas as suas unidades de disco. Estes compartilhamentos podem ser acessados remotamente apenas pelo administrador. O problema é que a conta "administrador" é padrão em todas as máquinas com o Win 2K, isto significa que se alguém souber seu IP e sua senha de administrador, que você configurou durante a instalação do Windows (e que provavelmente usa como login :-) poderá, com a ferramenta adequada, ter acesso a todos os seus arquivos.

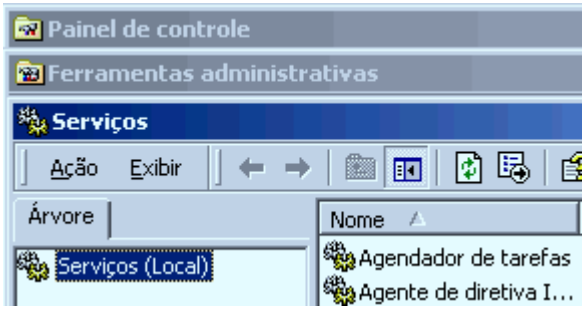
Para eliminar esta possibilidade, em primeiro lugar crie uma senha de administrador decente, com pelo menos 8 caracteres. Feito isso, crie um outra conta, com privilégios de administrador e passe a logar-se através dela. Renomeie a conta padrão de administrador. Dê outro nome qualquer, que não seja muito óbvio.

Finalizando, aproveite para renomear também a conta "convidado" (guest nas versões em Inglês) que é outra conta padrão que pode ser usada para ter acesso (embora restrito) à sua máquina. Nas propriedades da conta você também pode desativa-la, se preferir.

Pronto, agora, alguém que tente se logar na sua máquina, através da conta padrão de administrador, usando um programa de força bruta, não achará a conta e mesmo que descubra qual foi o novo nome que deu para ela, não conseguirá nada, pois uma senha de 8 caracteres é impossível de ser quebrada por um ataque de força bruta. Uma possibilidade a menos.

Serviços

Volte ao painel de controles e abra agora o ícone "Ferramentas administrativas" e em seguida "Serviços".



Aqui podem ser configurados todos os serviços que rodarão na sua máquina. Alguns são vitais para o funcionamento do sistema, mas outros são um risco desnecessário em termos de segurança. No tutorial sobre como otimizar o Windows 2000 que havia publicado a pouco mais de um mês, citei alguns serviços que podem ser desabilitados para melhorar o desempenho do sistema, vou citar agora quais podem ser desabilitados para melhorar a segurança:

*** Telnet** : Que tal um serviço que permita qualquer um, que conheça a senha de qualquer uma das contas de usuário que criou no painel de controle > usuários e senhas possa conectar-se à sua máquina apartir de qualquer máquina conectada à Web? É exatamente isto que este serviço faz. ele vem habilitado por defaut no Windows 2000 Server e é um grande risco de segurança, principalmente por que recentemente foi descoberto um bug neste serviço que permite conectar-se mesmo sem saber a senha. A menos que pretenda usar este recurso, desative este serviço.

*** Compartilhamento remoto da área de trabalho** : Permite compartilhar sua área de trabalho através do netmeeting. Se você não usa o netmeeting, ou o usa, mas não pretende dar este tipo de liberdade a nenhum dos seus amigos, desabilite este serviço também.

*** True Vector Internet Monitor** : Você pode manter este serviço habilitado caso deseje um log de todas as tentativas de conexão não autorizadas ao se sistema.

*** Área de armazenamento** : Este serviço permite que o que for armazenado no clipboard da sua maquina (ctrl + v) possa ser visualizado remotamente. Não chega a ser um grande risco, mas pelo sim e pelo não, é melhor desabilitar este recurso caso não pretenda usa-lo.

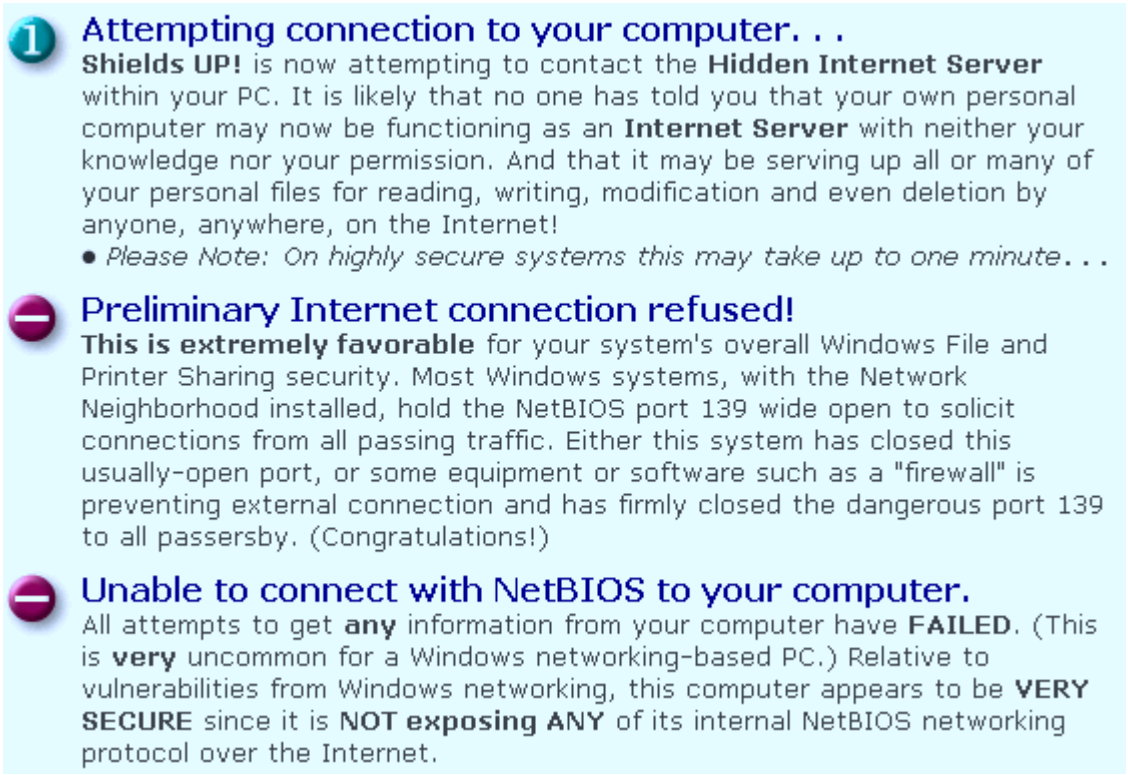
* **Serviço Auxiliar NetBios sobre TCP/IP** : Você vai precisar deste serviço para compartilhar arquivos e impressoras com outros micros da sua rede doméstica. Mas, por precaução, mantenha o "tipo de inicialização" deste serviço em Manual, assim ele só será habilitado quando for necessário

Teste sua segurança

Depois de terminada esta primeira rodada de configuração, você pode fazer um teste rápido, para verificar como ficou a segurança do seu sistema, acesse o **http:// grc.com/ default.htm** e clique no "Shields UP!". Estão disponíveis dois testes, "Test my shields" e "Probe my ports". No primeiro a ferramenta tentará se conectar ao seu sistema e na segunda o vasculhará em busca de portas abertas.

Se você estiver usando algum programa de firewall, desabilite-o momentaneamente, juntamente com qualquer programa servidor (FTP server, servidor de e-mail, proxy, etc), ou de compartilhamento de arquivos (Audiogalaxy, Gnutella...) que esteja habilitado. Se quiser, pode refazer o teste depois com tudo habilitado, mas no momento queremos testar como ficou a segurança do seu Windows, sem nenhuma camada extra.

Depois das alterações, você deverá receber duas telas como estas ao fazer o teste, indicando que o sistema não foi capaz de encontrar nenhuma vulnerabilidade no seu PC:



23	Telnet	Closed	Your computer has responded that this port exists but is currently closed to connections.
25	SMTP	Stealth!	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
79	Finger	Closed	Your computer has responded that this port exists but is currently closed to connections.
110	POP3	Closed	Your computer has responded that this port exists but is currently closed to connections.
113	IDENT	Closed	Your computer has responded that this port exists but is currently closed to connections.
139	Net BIOS	Closed	Your computer has responded that this port exists but is currently closed to connections.
143	IMAP	Closed	Your computer has responded that this port exists but is currently closed to connections.
443	HTTPS	Closed	Your computer has responded that this port exists but is currently closed to connections.

Obs: As portas reconhecidas como “Stealth”, são portas que estão sendo bloqueadas pelo firewall do seu provedor. Ou seja, são 100% seguras, já que numa requisição chegará à sua máquina através delas. Se você estiver usando o Speedy por exemplo, terá várias portas “Stealth”.

Este teste serve apenas para detectar alguma brecha mais gritante no seu sistema. Só para constar, este teste rápido acusa três portas abertas numa instalação defaut do Windows 2000. Pelo menos estas já conseguimos fechar.

Não se iluda por que seu PC passou nos testes, como disse, este teste só detecta algumas brechas óbvias de segurança, não garante que o seu sistema está realmente seguro. Afinal, só o fato de trancar a porta garante que o seu carro não seja roubado?

Se, por outro lado, o teste apontou alguma porta aberta no seu PC, significa que, ou você esqueceu algum dos programas de compartilhamento de arquivos ou algum servidor de FTP por exemplo habilitado, neste caso é normal que ele indique que a porta usada pelo programa está aberta, ou então que, realmente, você tem algum trojam instalado no seu micro. Lembra-se das dicas de não abrir arquivos ataxados nos mails e manter um antivírus instalado? Esta na hora de começar a coloca-las em prática.

Outro teste que pode ser feito é o do http://www.hackerwhacker.com

Patches

Mesmo que o seu sistema não tenha nenhuma porta vulnerável, isso não elimina a possibilidade de alguma falha de segurança em algum dos programas que você está rodando. Descobrem brechas no IIS quase todos os dias...

Para garantir proteção contra esta última possibilidade, é recomendável instalar os patches de segurança lançados pelos desenvolvedores, sempre que algo importante for disponibilizado. No caso do Windows ainda fica mais fácil, pois as atualização podem ser baixadas no Windows Update. Claro que você só deve se preocupar em baixar as atualizações relacionadas com brechas de segurança e apenas para os programas que está rodando. Pra que baixar uma correção para o IIS Server se você não o usa?

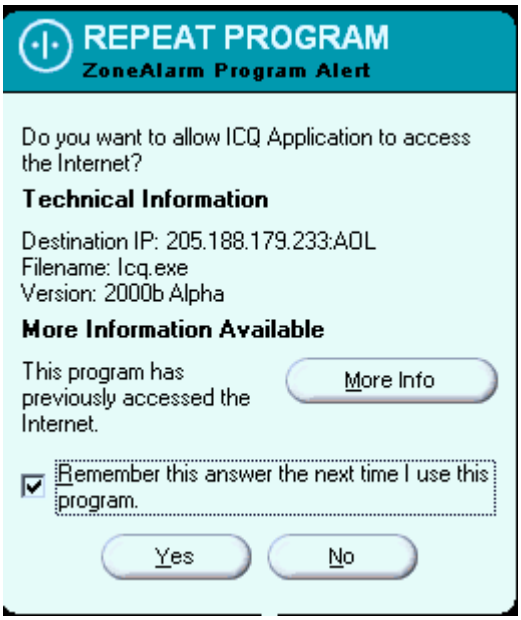
Mais uma dica é que qualquer programa servidor, seja um servidor de FTP, um servidor Web, ou mesmo um simples servidor Proxy ou de e-mail que mantenha ativado, representa um risco em termos de segurança. Antes de usar um programa qualquer, seria recomendável das uma passeada pelos sites com cracks para ver se o programa possui alguma falha grave de segurança que possa ser explorar. Um bom lugar para começar a pesquisa é o www.astalavista.box.sk . O Serv-U por exemplo, um servidor de FTP bastante popular, tem várias vulnerabilidades, que permitem desde simplesmente travar o programa, até acessar arquivos de outras pastas além das disponibilizadas no FTP. O Audiogaxy Satelite tem um problema minha com senhas, enquanto até mesmo o ICQ traz seus riscos...

O bom e velho firewall

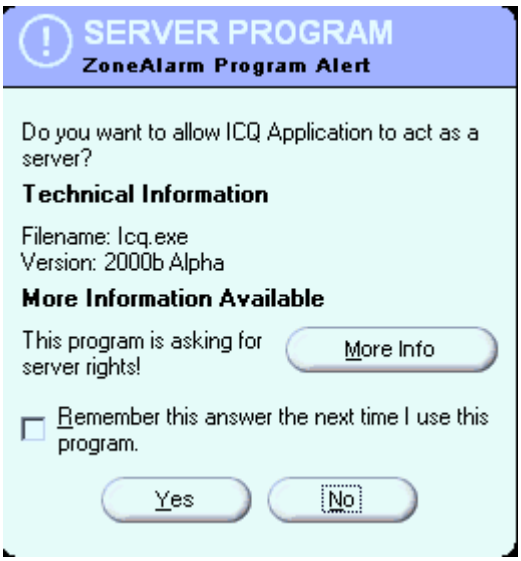
Para completar o time, nada melhor que um bom programa de firewall. Ele garantirá um nível de segurança adicional monitorando as portas do seu sistema, bloqueando tentativas de acesso não autorizadas, dizendo quais programas estão acessando a internet, etc.

Se você ainda não tem um firewall de confiança, eu recomendo começar pelo Zone Alarm, que é fácil de configurar e gratuíto. você pode baixa-lo em http://www.zonelabs.com/ ou aqui mesmo na área de downloads do Guia do Hardware.

O Zone perguntará cada vez que um programa tentar acessar a internet. Marque a opção “Remember this answer the next time I use this program” para os programas mais comuns, para que ele não fique incomodando ao repetir a mesma pergunta toda hora.



Existem duas telas de alerta do zone alarm, a primeira, significa que o programa está tentando apenas fazer uma acesso normal à Internet, como cliente, apenas tentando acessar uma página, receber uma mensagem, etc. Isto não chega a ser muito preocupante. Mas, que tal um segundo aviso, como o que está abaixo:



Um programa tentando atuar como servidor é um pouco mais preocupante. pois significa que ele está enviando algum tipo de informação. Se for o servidor de FTP que você está usando para compartilhar arquivos com alguns amigos, nada demais, mas o que dizer de um programinha como o ICQ exigindo direitos de servidor? Hum... o que será que ele pretende fazer? Enviar informações sobre os seus hábitos de navegação para o servidor da AOL? Bem, neste caso a escolha é sua. O ICQ por exemplo funciona perfeitamente se você negar os direitos de servidor, mas dar permissão para acessar a Internet.

Mas que tal um programinha que você nunca ouviu falar, nem sabia que estava instalado no seu micro, exigindo direitos de servidor? Aham...

Spywares

Os Spywares são programas usados como ferramenta de marketing. Eles enviam dados sobre os hábitos de navegação do usuário entre outros dados do gênero. Algumas pessoas não se importam com isso, outras consideram isso uma brecha de segurança. Em geral os spywares são instalados junto com outros programas, sem pedir sua opinião sobre o fato.

Alguns exemplos são o "Cydoor Ad-System", usado por vários Ad-wares (os programas que exibem banners), como por exemplo o Flash-Get, e o WebHancer, que é instalado junto com o Audiogalaxy Satellite, etc. etc.

Estes programas precisam de conexão com a Internet para funcionar. Usando o Zone-Alarm ou outro bom firewall, você pode bloquear as conexões, impedindo que enviem qualquer informação.

Como configurar um servidor Linux

Embora o Linux ainda esteja engatinhando nos desktops, como servidor de rede ele é quase imbatível. A combinação de estabilidade, baixo custo de implantação e baixo custo total de propriedade e, mais recentemente, ferramentas amigáveis de configuração são responsáveis por quase 20% dos servidores do mundo rodarem Linux. Combinado com os números do Solaris e das várias versões do Unix, temos uma base instalada maior do que a dos servidores Windows.

Esta é provavelmente a área em que o Linux está melhor servido de aplicativos. O Apache é um servidor web poderoso, com suporte a Perl, PHP, vários bancos de dados, etc. não é à toa que ele é utilizado na maior parte dos servidores Web do mundo. Existem servidores de FTP, de e-mail, News, etc. Montar um grupo de discussão por exemplo, algo que no Windows tomaria várias horas, entre o tempo de pesquisar, conseguir um programa e aprender a configura-lo, no Linux é apenas questão de habilitar o serviço e configurá-lo rapidamente.

Além de poder servir arquivos e impressoras para outras máquinas Linux, é possível criar redes mistas, com máquinas Windows e Linux através do Samba, compartilhar a conexão com a Web, montar um Proxy com vários recursos de segurança usando o Squid, entre muitos outros recursos.

Nas páginas a seguir veremos como configurar um servidor Linux baseado no Linux Mandrake 8.1. Com excessão das instruções de instalação as instruções também se aplicam a outras distribuições, incluindo o Conectiva e o Red Hat, que também trazem a maior parte das ferramentas que iremos abordar.

A distribuição

O Mandrake 8.1 Standard é composto por um total de três CDs. O primeiro é o CD de instalação, com a base do sistema e os aplicativos mais importantes. O segundo CD complementa o primeiro com uma grande coleção de softwares open source, enquanto o terceiro CD contém programas mais específicos (os servidores de banco de dados por exemplo) e alguns aplicativos comerciais.

Existem ainda dois manuais, o User Manual e o Reference Manual. Infelizmente, nenhum dos dois está disponível em Português (justamente por isso estou escrevendo este guia ;-) mas além da versão em inglês, existe a opção da versão em Espanhol. Os links para os Manuais estão abaixo.

Inglês:
http://www.linux-mandrake.com/en/doc/81/en
Espanhol:
http://www.linux-mandrake.com/en/doc/81/es

Existe ainda o MandrakeCampus, que oferece cursos online gratuitos (infelizmente nada em Português):
http://www.mandrakecampus.com/

Instalando

Para abrir o programa de instalação, a melhor opção (como em outras distros) é dar boot diretamente através do CD-ROM, para isso basta configurar a opção “boot sequence” no Setup.

Se por qualquer motivo isto não for possível, você pode instalá-lo também através de um disquete de boot. Neste caso, as opções são instalar através do CD-ROM, instalar apartir do HD ou mesmo instalar via rede. Veremos isto com mais detalhes mais adiante.

Um detalhe importante, que você deve verificar antes de iniciar a instalação, é se os componentes do seu PC, principalmente a placa de vídeo e o modem são suportados. Você pode conferir a lista de hardware suportado do Mandrake no:
http://www.mandrakelinux.com/en/hardware.php3

Você pode descobrir a marca e modelo dos dispositivos através do gerenciador de dispositivos do Windows. Lembre-se que como outras, a lista de hardware suportados não contém referências para todos os dispositivos. A menos que o dispositivo apareça explicitamente como não suportado, existe uma grande possibilidade dele funcionar. Experimente fazer uma busca no http://www.google.com.br (pode ser outro, mas o google é o melhor :-) por **Mandrake Linux Modelo_da_placa**. Esta dica serve não apenas para encontrar informações sobre periféricos, mas sobre qualquer problema ou dúvida que tenha. Existe muita documentação sobre Linux, mas disponível de forma esparsa, um problema que os mecanismos de busca ajudam a resolver.

O Mandrake não inclui drivers para nenhum modelo de Winmodem, mas a maioria dos Winmodems já são suportados pelo Linux, incluindo os com chipset PC-Tel ou Lucent, que são provavelmente os mais comuns por aqui. Para verificar se o seu modem é suportado e baixar os drivers e instruções necessárias, acesse o http://www.linmodems.org/ . Este tópico postado no fórum também contém bastante informação:
http://www.forumgdh.net/forum/link.asp?TOPIC_ID=14677

Outra opção, caso você não consiga instalar o seu Winmodem é utilizar o Techlinux, uma distribuição Brasileira, baseada no Mandrake que oferece um utilitário que detecta automaticamente modems com chipsets PC-Tel e Motorola e inclui drivers para os Lucent. O Techlinux traz a maioria dos utilitários de configuração que estudaremos neste tutorial, incluindo o Mandrake Control Center, por isso a maior parte das informações também se aplicam a ele. De qualquer forma, se optar por utiliza-lo, não deixe de ler o manual para conhecer suas particularidades da distribuição: http://www.techlinux.com.br/

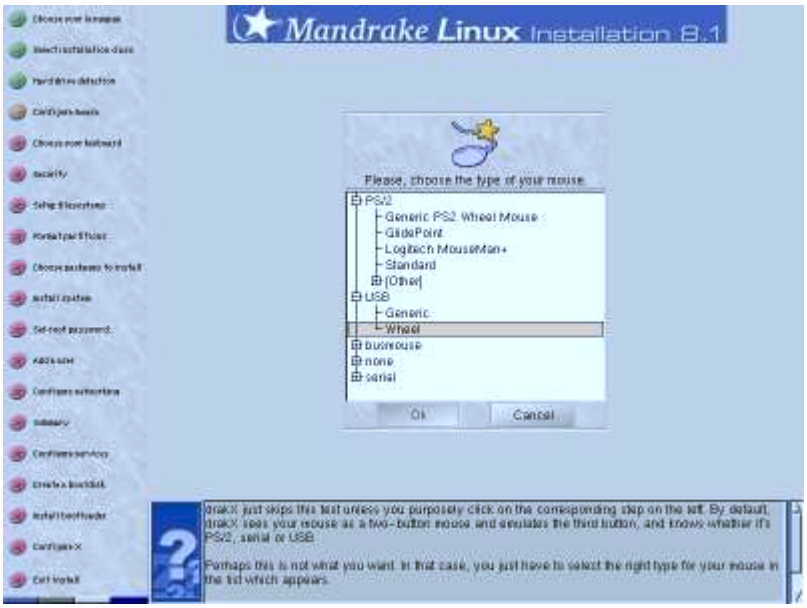
Depois destas etapas preliminares, chegamos à instalação do sistema propriamente dita. A instalação do Mandrake é bastante intuitiva, fazendo apenas perguntas básicas sobre a linguagem de instalação, layout do teclado, programas a serem instalados etc. Mesmo o particionamento do disco, que é um ponto crítico em outras distribuições é bastante simples no Mandrake, como veremos com detalhes mais adiante.

Ao abrir o programa de instalação, você terá a opção de abrir o programa "default" de instalação, em modo gráfico (Enter) ou escolher entre os modos de baixa resolução (caso o seu monitor não suporte 800 x 600) ou instalar em modo texto, caso tenha problemas com o primeiro. Mas, se o instalador gráfico não abrir, provavelmente a sua placa de vídeo não é suportada, então mesmo instalando em modo texto, você não conseguirá utilizar o Linux em modo gráfico. Verifique a lista de compatibilidade.

A primeira pergunta feita pelo instalador é a linguagem que será usada. O Português do Brasil está entre as opções, mas a tradução está incompleta. É comum menus aparecerem em Português, mas as opções internas ou os arquivos de ajuda aparecerem em inglês, sem falar em vários erros de tradução e termos em Português de Portugal. É usável, mas está muito longe de ser uma tradução perfeita.

A segunda pergunta é sobre o modo de instalação. O modo "**Recommended**" é voltado para usuários leigos, que querem instalar o sistema sem muitas perguntas. O layout do teclado por exemplo é "subentendido" apartir da linguagem escolhida na sessão anterior. Eu recomendo o modo "**Expert**", que também é muito simples, mas permite ter um melhor controle da instalação. Durante toda a instalação você terá um assistente tira-dúvidas para ajudar com qualquer opção que não conheça.

Depois de perguntar se você tem alguma placa SCSI instalada (essa é fácil né ;-) o instalador pergunta sobre o tipo de mouse instalado. Geralmente ele detectará o mouse corretamente na primeira, mas ele pode cometer enganos como não detectar a roda do mouse ou algo parecido. Neste caso basta indicar o modelo correto. Logo depois você terá a chance de testar o mouse e retornar caso tenha escolhido errado:



A próxima seleção (apenas no modo expert) é o layout do teclado: ABNT-2 caso o seu teclado tenha o "ç" e US Keyboard Internacional caso não tenha.

Logo depois você terá a chance de configurar o nível de segurança do sistema. O modo Medium é o mais recomendado, pois no low a segurança é fraca e o High pode bloquear alguns programas. Você poderá alterar essa configuração, posteriormente, através do Mandrake Control Center.

Depois destas configurações básicas, chegamos à parte mais crítica da instalação, o "terrível" particionamento do disco. Felizmente o Mandrake traz uma ferramenta bastante amigável para facilitar esta tarefa, o DiskDrake.

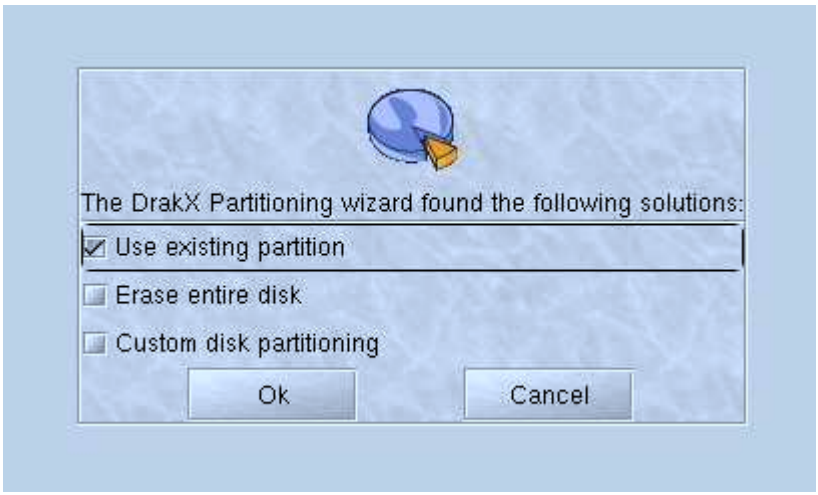
Particionando o HD

Você pode deixar que o utilitário redimensione uma partição Windows (FAT 16 ou FAT 32) já existente, usando o espaço livre para instalar o Linux ("**Use the free space on the Windows partition**"), pode utilizar uma partição Linux previamente criada ("**Use existing partition**"), usar o espaço não particionado do disco, caso tenha ("**Use free space**") ou pode simplesmente apagar tudo que estiver gravado e partir para uma instalação limpa (**Erase entire disk**).

Se você pretende reparticionar a partição Windows, existem dois cuidados necessários para que tudo saia bem. Em primeiro lugar, o óbvio, certificar-se que existe espaço em disco suficiente. Com 1 GB já é possível fazer uma instalação básica do sistema, mas para instalar vários programas, armazenar seus arquivos pessoais etc. seria recomendável reservar um espaço maior, pelo menos 2 ou 3 GB. Quanto mais espaço melhor.

Outro detalhe importante é desfragmentar o disco. O DiskDrake é capaz de redimensionar a partição mesmo que esteja fragmentada, porém além do processo demorar bem mais que o normal, a possibilidade de ocorrer algum problema é muito maior.

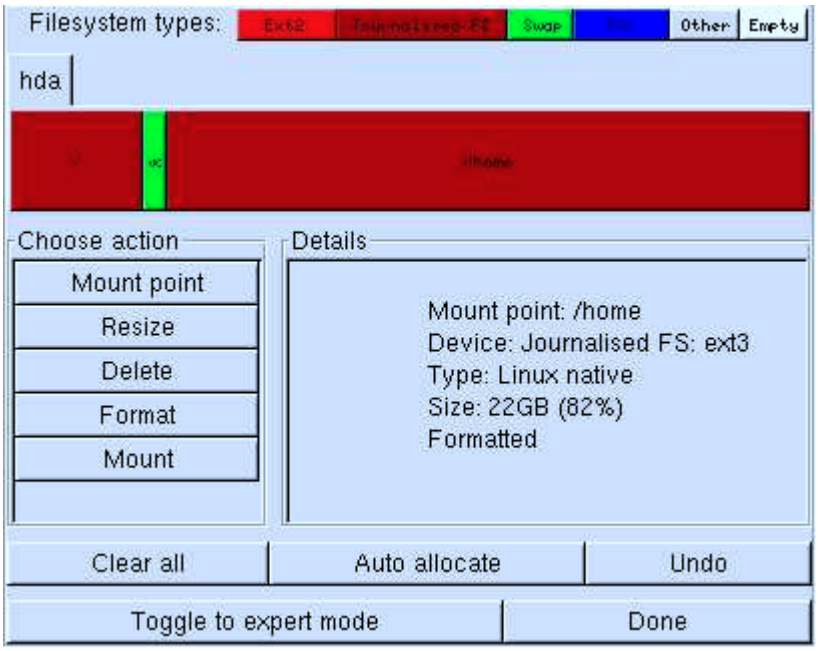
Escolhendo a opção Erase entire disk o programa vai simplesmente limpar a tabela de partição do HD e dividí-lo em duas partições: uma menor, usada para os arquivos do sistema e outra maior, montada no diretório **/ home**, onde ficam guardados os arquivos dos usuários.



As duas opção automáticas servem bem para os usuários leigos, que mal sabem o que é uma partição de disco, mas ou escolher a opção Custom disk partitioning você terá muito mais opções.

Nota: Os screenshots a seguir são do diskdrake, não do programa de instalação, que possui uma interface levemente diferente. Editei algumas imagens para mostrar as opções que estão disponíveis no programa de instalação.

A interface do programa é bastante intuitiva, lembra bastante a do Partition Magic 6, mas é mais fácil, por conter apenas os sistemas de arquivos suportados pelo Linux:



No topo da tela temos a lista dos sistemas de arquivos suportados: **EXT2**, **Journalised FS**, **Swap**, **FAT** (inclui FAT 16 e FAT 32) além de **Other** (outro sistema de arquivos não reconhecido) e **Empty** (espaço não particionado).

Na aba logo abaixo, você tem uma lista dos HDs instalados. No screenshot existe apenas um, que aparece como **hda**.

A barra colorida mostra um mapa do disco, com todas as partições que ele contém. No exemplo o disco já está particionado, pronto para a instalação do sistema, dividido em duas partições, montadas no diretório raiz (**/**) e no diretório **/ home** (que aparecem em vermelho), além de uma partição swap, em verde.

Para alterar uma partição, basta clicar sobre ela e usar a opção "**Resize**", que redimensiona, sem perda de dados. A opção "**Delete**" permite apagar partições a fim de criar outras depois usando o espaço livre, enquanto a opção "**Format**" formata uma partição já criada. Não é preciso formatar as partições que forem criadas, pois ao terminar o particionamento (clicando em "**done**") o assistente se oferecerá para formatar as partições criadas.

Para criar uma nova partição você precisará clicar sobre uma área de espaço livre (aparece em branco no mapa) e em seguida clicar no botão do sistema de arquivos que será usado (na parte superior). Para liberar espaço você deve usar as opções anteriores, de redimensionar ou deletar uma outra partição.

Na hora de escolher o sistema de arquivos a ser utilizado as opções são basicamente duas: usar o velho sistema EXT2, que acompanha o Linux a vários anos, ou utilizar um dos novos sistemas com journaling. Clicando em "**Journalised FS**" você poderá escolher entre o **EXT3**, **RiserFS** e **JFS**.

O journaling permite que o sistema de arquivos mantenha um log, onde são armazenadas todas as mudanças feitas em arquivos do disco. Quando qualquer erro inesperado surge ou o sistema é desligado incorretamente é possível localizar todas as operações que não haviam sido concluídas, restaurando a consistência do sistema de arquivos em poucos segundos, sem a necessidade de vascular arquivo por arquivo. Isso é bem diferente do que acontece no EXT2, onde o fsck precisa vasculhar todo o disco em busca de erros depois de cada desligamento incorreto, um processo que pode demorar mais de 10 minutos, dependendo do tamanho da partição.

Além disso, a frequência com que são perdidos arquivos ou mesmo pastas inteiras (ou até mesmo a tabela de partição do disco se você for realmente azarado :-) no EXT2 por causa dos desligamentos incorretos é espantosamente alta, um perigo que não existe nos sistemas com suporte a journaling.

Dentre os três, o **EXT3** foi o que pude testar melhor e por isso é a minha recomendação pessoal. Evite usar o EXT2, principalmente se o seu PC não tiver no-break. Não existem desvantagens aparentes em usar o EXT3; pelo contrário, o desempenho do sistema chega a ser um pouco melhor.

Junto com estas opções, estão vários outros sistemas de arquivos, incluindo FAT 16, FAT 32 e até mesmo outros sistemas de que provavelmente você nunca ouviu falar. O único sistema importante que não consta na lista é o NTFS, que ainda não é completamente suportado pelo Linux. Essa fartura de sistemas de arquivos suportados permite até mesmo que este utilitário seja usado no lugar do Partition Magic na hora de formatar HDs e redimensionar partições, mesmo que o objetivo não seja instalar o Linux.

Você precisará ainda criar uma **partição swap**, que armazenará a memória virtual do sistema. O Linux não permite aumentar dinâmicamente o tamanho do arquivo de troca, como no Windows,

ao acabar o espaço da partição você receberá uma mensagem de falta de memória e terá que fechar alguns aplicativos para continuar trabalhando. Para evitar isso, crie um arquivo razoavelmente grande, de 200 ou até 300 MB, dependendo de quanto espaço livre em disco tiver disponível. Se você tiver bastante memória (256 MB ou mais) e não desejar usar memória virtual, você pode criar um arquivo pequeno, de 8 ou 16 MB, apenas para evitar que um ou outro aplicativo gere mensagens de erro pela falta da memória swap.

As partições no Linux

Você deve ter notado que no exemplo dividi o HD em duas partições, ao invés de criar apenas uma. A idéia é a mesma de dividir o HD em C: e D: no Windows: simplesmente manter seus arquivos pessoais numa partição diferente da dos arquivos do sistema, para melhorar a segurança e permitir que você possa tranqüilamente reformatar a partição do sistema quando precisar reinstalá-lo, sem correr o risco de perder junto seus arquivos.

Mais um detalhe interessante é que se depois da reinstalação você recriar os usuários antigos, automaticamente o sistema se encarregará de utilizar as configurações de cada um, evitando que você precisa configurar tudo manualmente.

A primeira partição deve ser montada no diretório raiz, ou "**/**", enquanto a segunda deve ser montada no diretório **/home**, onde ficam as pastas dos usuários (/home/maria, /home/fernando, etc.). O ponto de montagem é solicitado logo depois de criar a partição, mas pode ser alterado mais tarde através do **DiskDrake** ou do comando **mount**.

Você pode criar mais partições se desejar. Se você for montar um servidor FTP ou um servidor Web, pode criar uma partição separada para os arquivos do servidor por exemplo.

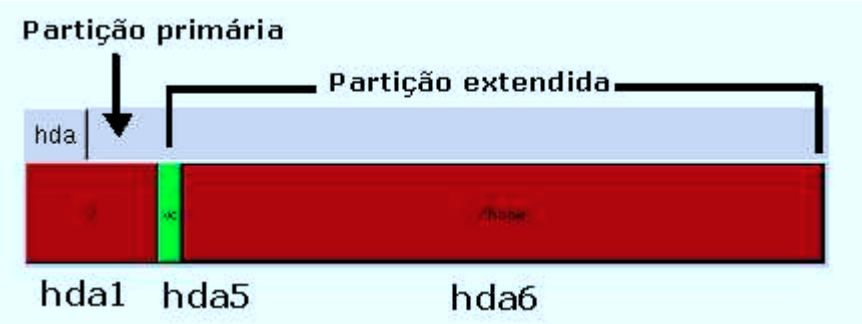
Cabe aqui uma pequena explicação sobre o modo como o Linux enxerga os HDs instalados e as partições de disco.

Temos num PC duas interfaces IDE, onde cada uma permite a conexão de dois HDs, configurados como master ou slave. O primeiro HD, conectado à interface IDE primária e configurado como master é reconhecido pelo Linux como **hda**, o segundo HD, slave da IDE primária é reconhecido como **hdb**, enquanto os dois HDs conectados à IDE secundária são reconhecidos como **hdc** e **hdd**.

Ao mesmo tempo, cada HD pode ser dividido em várias partições. Podemos ter um total de 4 partições primárias ou três partições primárias e mais uma partição extendida, que pode englobar até 255 partições lógicas.

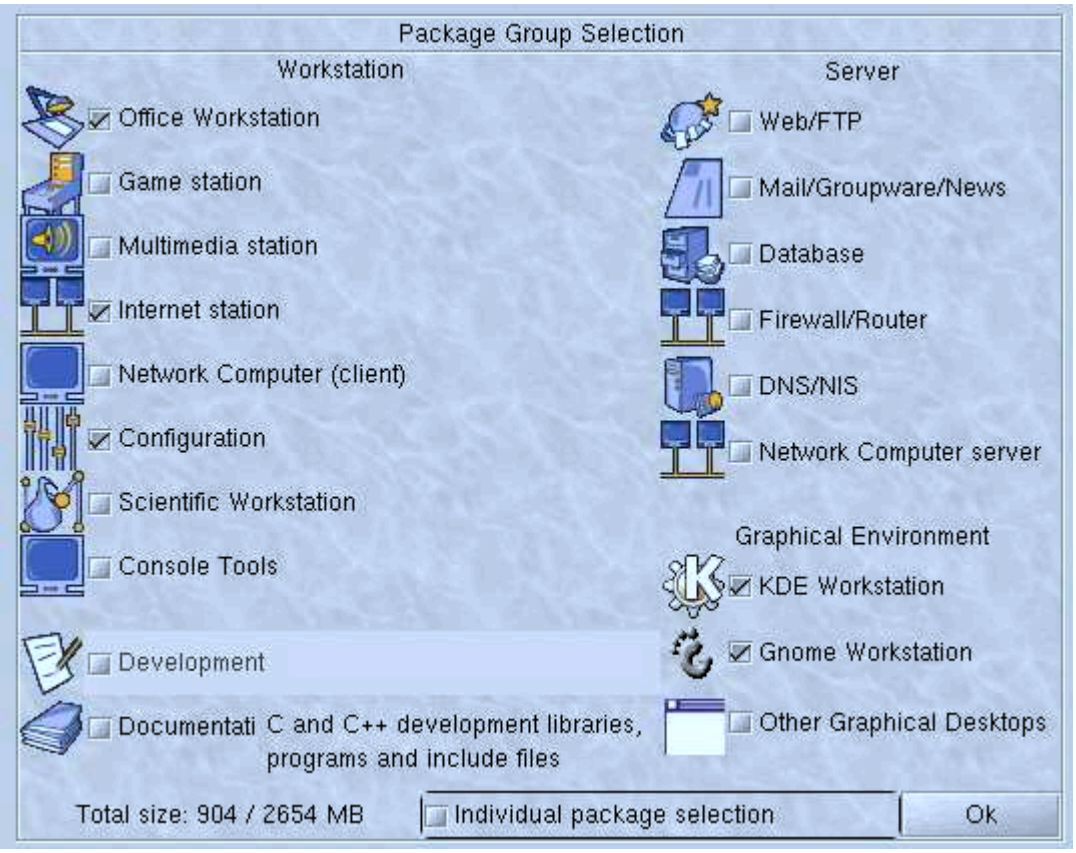
A primeira partição primária, do primeiro HD (hda) é chamada de **hda1**. Caso o HD seja dividido em várias partições, as demais partições primárias são camadas de **hda2**, **hda3** e **hda4**. Porém, o mais comum ao dividir o HD em várias partições é criar apenas uma partição primária e criar as demais partições dentro de uma partição extendida. É isso que o particionador faz por default.

As partições extendidas recebem números de 5 em diante (**hda5**, **hda6**, **hda7**, etc.) mesmo que as partições hda2 e hda3 não existam:



Pacotes de Aplicativos

Depois de particionar o disco você deverá escolher quais aplicativos serão instalados no sistema. Os nomes já são bem explicativos, mas algumas categorias que você não deve deixar de instalar são **Internet Station** (conectividade de rede e um conjunto de browsers, leitores de e-mail, ICQ, etc.) e **Configuration** (que instala o Mandrake Control Center e os outros utilitários de configuração que veremos adiante).



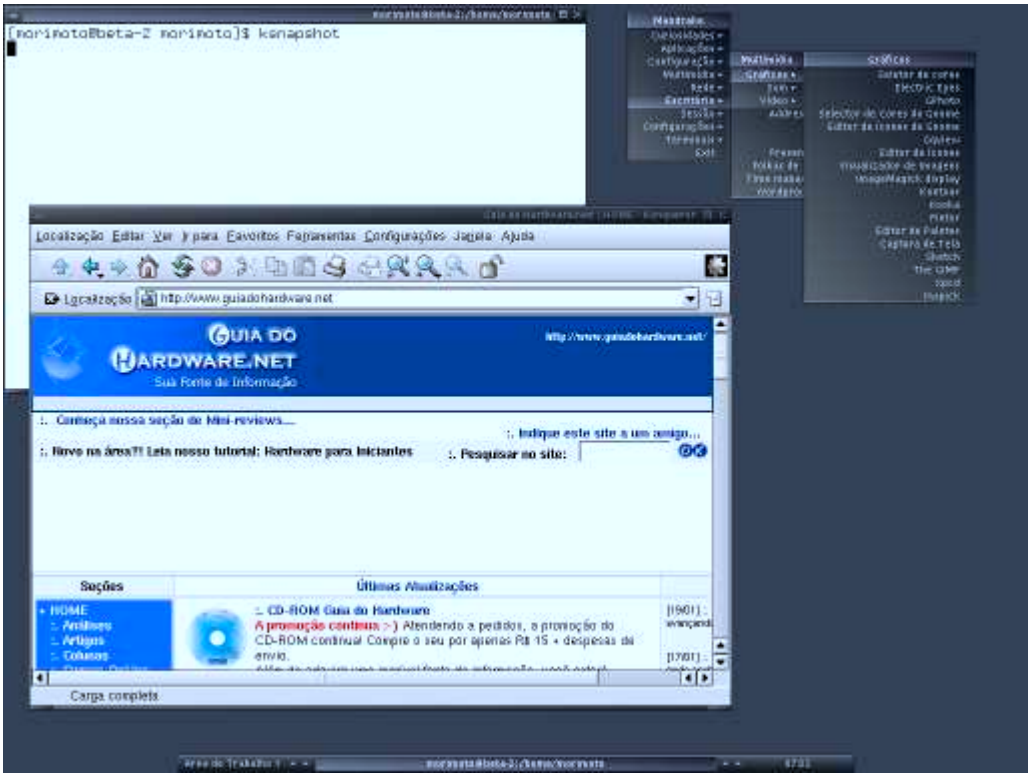
As opções "**Network Computer Server**" e "**Web/ FTP**" instalam o Apache, Samba, servidor de FTP e outros utilitários para transformar a máquina num servidor de rede. O Samba é essencial se

você pretende compartilhar arquivos e impressoras com máquinas Windows.

Entre as interfaces gráficas você pode escolher entre KDE e Gnome além de algumas interfaces mais leves, como o BlackBox e o WindowMaker. Seja qual for a interface de sua escolha, é recomendável manter tanto o Gnome quanto o KDE instalados, pois cada uma das interfaces possui um conjunto próprio de aplicativos, que utilizam módulos da interface e por isso necessitam que ela esteja instalada para rodar.

Por exemplo, o Gnome traz o Nautilus, um gerenciador de arquivos muito mais sofisticado graficamente que o Konkeror do KDE. O KDE por sua vez traz um KOffice, uma suíte de escritório bastante elaborada e por aí vai. Mantendo ambos instalados, você terá à disposição um número muito maior de aplicativos e poderá juntar o melhor dos dois mundos.

Um porém é que se você utilizar o KDE e abrir um aplicativo do Gnome (ou vice-versa) o sistema precisará carregar junto uma boa parte das bibliotecas do outro. Além de tornar a inicialização do aplicativo um pouco mais lenta (apenas para o primeiro aplicativo) isso consome bastante memória RAM. Para misturar aplicativos das duas interfaces, sem perder em desempenho, o recomendável é ter pelo menos 196 MB. Caso você esteja usando um micro antigo, com 32 MB ou menos, você pode ter um bom desempenho utilizando o BlackBox, uma interface extremamente leve, que consome apenas 800 KB de memória RAM, que vem sendo bastante utilizada hoje em dia por possuir um visual limpo e moderno.



Blackbox

Mas, nesse caso, evite abrir programas do KDE ou do Gnome, caso contrário o esforço não melhorará muita coisa.

Além do BlackBox, existem várias outras boas opções leves, como o WindowMaker ou até mesmo

o AfterStep, que são muito bonitos graficamente, sem abrir mão da leveza. Este é um ponto forte do Linux, a liberdade de escolha, não apenas das interfaces gráficas, mas também dos vários programas incluídos nas distribuições.

Você pode instalar várias interfaces e testá-las com calma até escolher sua favorita. É possível escolher qual usar cada vez que fizer logon no sistema, ou até mesmo abrir vários terminais gráficos e utilizar várias delas ao mesmo tempo, como veremos com detalhes mais adiante.

Todas estas interfaces suportam o uso de temas, você pode baixar alguns no:
http://www.themes.org

Finalizando

Depois de copiar todos os arquivos para o HD, o que pode demorar quase uma hora se você escolheu instalar tudo, chegamos à parte final da instalação, onde configuraremos as contas de usuário, os endereços de rede e o acesso à Web.

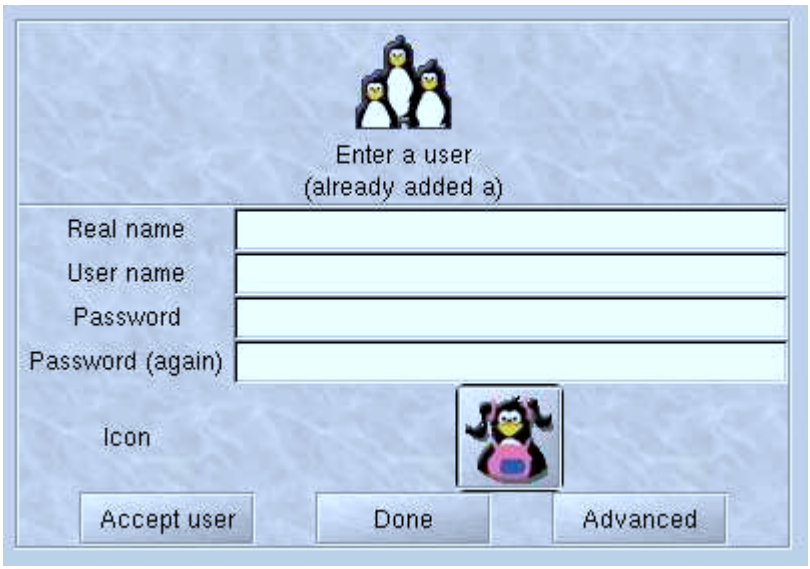
É recomendável que além do root você crie pelo menos mais um usuário e passe a utilizá-lo. Para prevenir acidentes, além da velha recomendação de não utilizar a conta root para uso normal do sistema, já que com ela você tem permissão para fazer tudo e pode destruir o sistema simplesmente digitando um comando errado no prompt, o Mandrake dificulta bastante o uso da conta root.

Em primeiro lugar, o root não aparece na tela de login. Sempre que você quiser usá-lo você precisará escrever "root" ao invés de clicar no ícone da conta desejada. Para dificultar ainda mais as coisas, depois de logar você verá uma mensagem de alerta, e cairá num desktop sem atalhos e com um fundo vermelho, um ambiente nada confortável ;-)

Enfim, ao invés de cultivar o mau hábito de usar a conta root para tudo, crie sua conta de usuário e utilize o sistema com mais segurança. Como usuário normal você também terá acesso a todas as ferramentas de configuração, basta fornecer a senha de root para abrir o Mandrake Control Center ou o que mais desejar.

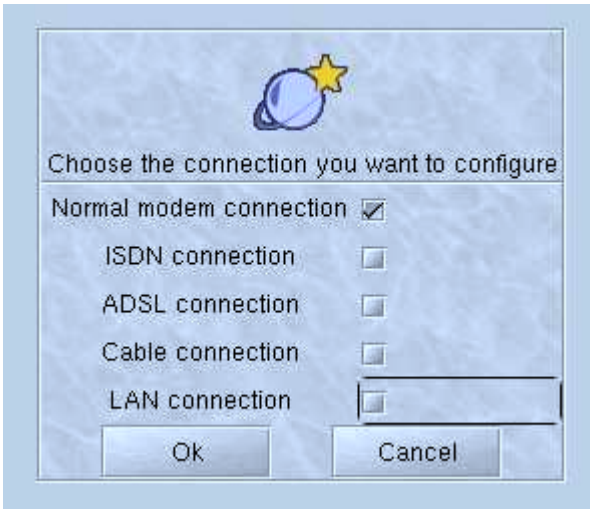
Além das ferramentas de configuração, qualquer aplicativo pode ser aberto com privilégios de root, usando os comandos "**su**" e "**kdesu**" que veremos a seguir.

Mesmo que esta seja a primeira vez que esteja instalando o Linux, vale à pena começar a cultivar desde já este hábito saudável.



Acesso à Web e rede

Outra etapa importante da instalação é a configuração do acesso à Web e da rede (caso tenha). Assim como as configurações anteriores, tudo é feito através de um Wizzard, que torna as coisas bastante simples. Escolha as conexões de rede disponíveis no menu, entre conexão via modem, ISDN, ADSL ou via rede e o Wizzard apresentará as opções referentes à escolhida. Você pode marcar mais de uma opção caso tenha um modem e uma placa de rede no micro por exemplo, neste caso o Wizzard apresentará as duas configurações e no final perguntará qual das duas deve ser usada para acessar a Internet.



Para a configuração do acesso via modem o Wizzard pede apenas os dados básicos, como o número do provedor, login, senha, etc. porém o instalador é bastante limitado neste ponto, pois só é capaz de instalar hardmodems. Se você tiver um Winmodem será necessário instalá-lo

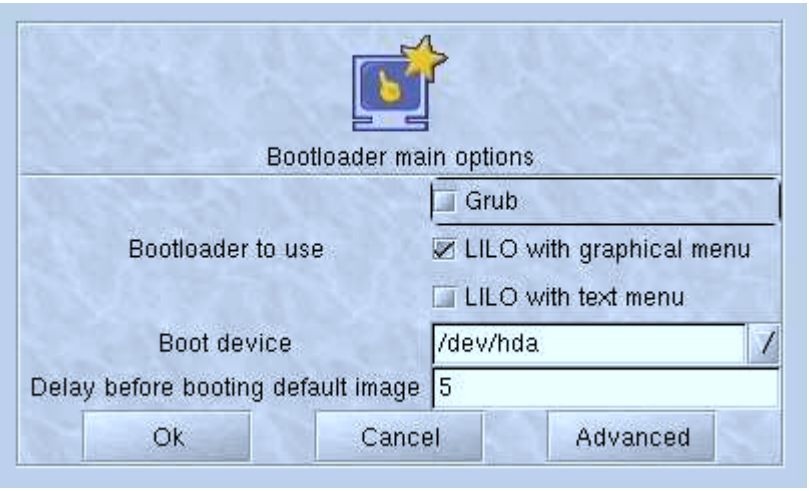
manualmente depois, como expliquei no início do texto.

Na configuração de rede (Lan Connection) você deverá fornecer o endereço IP da máquina e a máscara de sub-rede, além dos endereços do gateway e do servidor DNS. Caso a máquina Linux vá acessar através de uma conexão compartilhada através do ICS do Windows, você deverá preencher os dois últimos campos com o endereço da máquina que está compartilhando a conexão (192.168.0.1 que é o default do ICS). Está disponível também a opção de obter o endereço IP automaticamente, que também funciona.

A opção de acesso via ADSL serve não apenas para os serviços de ADSL, como o Speedy, mas também para o acesso via cabo e outros serviços de banda larga que utilizem uma placa de rede como meio de conexão. Na primeira geração do Speedy, onde eram utilizados IPs fixos, a configuração era muito simples, bastava configurar o endereço IP, gateway e DNS com os endereços fornecidos pelo provedor. Atualmente ficou um pouco mais complicado, pois é necessário utilizar um software de autenticação, que é fornecido apenas em versão Windows. Mas, isso não impede de utilizar banda larga no Linux. O artigo abaixo, do linux.trix.net contém várias dicas, não apenas sobre o Speedy, mas também sobre cabo e outros serviços:
http://www.linux.matrix.com.br/bandalarga_intro.htm

Gerenciador de boot

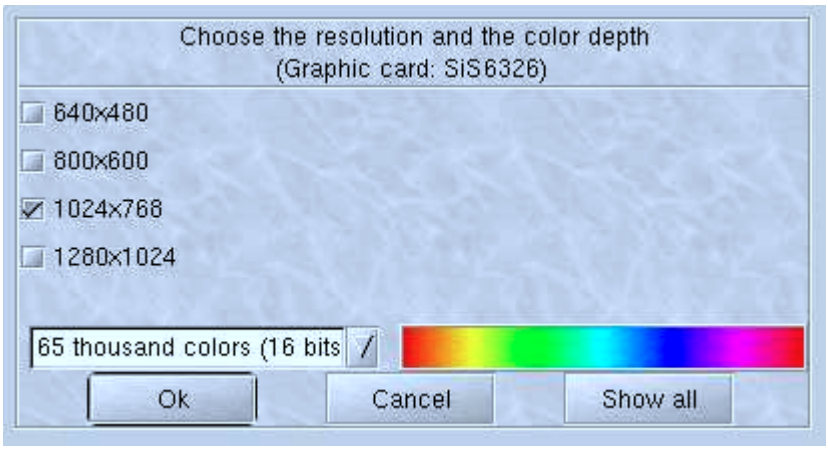
A configuração do gerenciador de Boot é feita automaticamente pelo instalador, que configura inclusive o dual-boot com o Windows se for o caso. Mas, de qualquer forma, você terá a opção de revisar ou mesmo alterar a configuração se desejar. Também é possível escolher o gerenciador de boot, entre o Lilo e o Grub. Durante um certo tempo o Grub levou vantagem na briga, pois oferecia um menu gráfico para a escolha do sistema, enquanto no Lilo o menu era em modo texto. Mas, não demorou muito para que o Lilo também oferecesse o menu gráfico e equilibrasse a briga. Apesar da semelhança entre os dois, o Lilo é melhor documentado que o Grub, por isso é o default.



Configuração do vídeo

Para finalizar a instalação, falta apenas configurar o X. A placa de vídeo será detectada automaticamente pelo assistente, mas em muitos casos você precisará escolher o monitor. Para isso você precisará apenas saber qual a frequência e taxas de atualização máximas do monitor e escolher a opção adequada entre os monitores genéricos. A maioria dos monitores de 15 polegadas suportam 1024 x 768 com 75 Hz e a maioria dos de 17" suportam 1280 x 1024 com 76 Hz. Usando estas configurações, a taxa de atualização do monitor subirá para 85 Hz, caso você opte por utilizar respectivamente 800x600 e 1024x768.

A seguir você deverá escolher a resolução e profundidade de cor entre as opções suportadas pelo monitor. Você poderá alterar essas configurações mais tarde através do Mandrake Control Center.



Não se preocupe pois depois de escolher o monitor e a resolução, o instalador irá testar a configuração. Se não funcionar, basta voltar e configurar novamente.

Você terá ainda a chance de escolher entre qual versão do XFree gostaria de usar. A versão 4.1.0 é naturalmente a mais recomendável por trazer várias melhorias em relação à 3.3.6, incluindo suporte a mais placas. O problema é que algumas placas de vídeo suportadas na versão 3 deixaram de ser suportadas na versão 4. Na lista de hardware suportado no site do Mandrake, você verá uma observação de qual versão suporta a sua placa. Mas, na dúvida escolha o 4.1.0.

Existem ainda as opções de instalar uma das versões do XFree com suporte a aceleração 3D. Este suporte é necessário para rodar alguns jogos, como por exemplo o TuxRacer, que acompanha o Mandrake, sem falar o Quake III e outros que já estão disponíveis para Linux. O problema é que estes drivers ainda estão em estágio experimental e não são totalmente estáveis. A menos que você realmente pretenda rodar alguns dos jogos, o melhor é utilizar a versão normal, até que os drivers 3D estejam maduros.

Terminando, o instalador fará a célebre pergunta "você deseja que inicialize o X automaticamente durante o boot" (responda que sim para não ter que digitar "startx" toda vez que der boot :-) e mostrará uma tela de congratulações dizendo que a instalação foi concluída com êxito.

Depois de reiniciar (não esqueça de tirar o CD do drive para não abrir a instalação de novo :-) Você verá a tela de login, com os usuários que configurou durante a instalação. Como havia dito, o root não aparece na lista, para usar esta conta você precisará digitar manualmente.

Da primeira vez que se logar você verá o First Time Wizzard, que permite configurar qual interface gráfica será usada por default, qual servidor de e-mail será usado etc. Você também verá um formulário para registrar o Mandrake Linux. Esse registro dá acesso ao Mandrake Campus (que contém cursos via Web gratuítos) e outros serviços, mas é opcional.

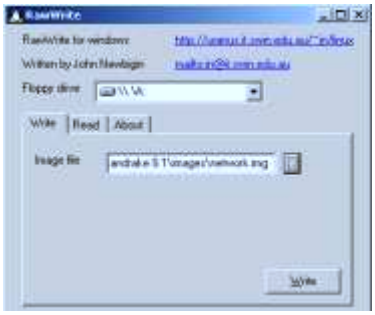
Como instalar via rede ou apartir do HD

Apesar do modo de instalação mais rápido ser dar boot pelo CD-ROM, o Linux também pode ser instalado de várias outras maneiras. Para isso você precisará ter em mãos o disco de boot adequado. Este é um tema que interessa a mais gente, por isso vou aproveitar para detalhar estas formas alternativas de instalação.

Você encontrará as imagens de vários discos de boot no diretório **Images** da sua distribuição Linux. Em alguns CDs de revista este diretório é excluído para economizar espaço, mas geralmente você ainda poderá conseguir os arquivos no site da distribuição.

Abrindo o diretório você encontrará vários arquivos .**IMG** que precisam ser gravados nos disquetes usando um programa chamado **Rawwrite**. Este é um programa para DOS que fica no diretório **Dosutils** do CD. Você pode baixar uma versão Windows do programa, que é mais prática de usar através do link abaixo:
http://www.downloads-guiadohardware.net/download/rawwritewin.exe

Basta apontar o arquivo da imagem a ser gravada e clicar em Write.



Para instalar o Linux apartir do CD, num PC que não suporte boot via CD-ROM você deve usar o arquivo **CDROM.IMG**, que é o disquete de boot que costuma ser incluído nas caixas completas das distribuições.

Se o micro não tiver CD-ROM, você pode instalar o Linux apartir do HD. Basta copiar todo o conteúdo do CD para um diretório do HD (pode ser inclusive para uma partição Windows FAT 16 ou 32) e usar o disco de boot **HD.IMG**. O disquete inicializará o micro e perguntará o diretório onde estão os arquivos, basta dar as informações necessárias. Lembre-se que a primeira partição do primeiro HD (o C: no Windows) é hda1 no Linux, como vimos a pouco e que ao invés de barras invertidas, usamos barras comuns para indicar os diretórios.

Você também pode instalar via rede, através de um servidor HTTP, FTP ou através de um servidor NFS.

Neste caso você deverá usar os disquetes **NETWORK.IMG**, **PCMCIA.IMG** ou **USBNET.IMG**. O primeiro serve para micros de mesa, com placas de rede PCI (o disquete terá dificuldades com placas ISA, apesar de também ser possível instalar através de uma), o segundo deve ser usado em notebooks com placas de rede PCMCIA (que por incrível que possa parecer, são quase sempre reconhecidas sem problemas) enquanto o terceiro serve para quem utiliza uma placa de rede USB.

Existe ainda o disquete **OTHERS.IMG**, que permite instalar o Linux através de outras mídias suportadas, como por exemplo através de discos Zip.

As opções de instalar apartir de uma partição Windows, via FTP e HTTP geralmente só funcionarão num micro com 64 MB de RAM ou mais, pois como nesta fase da instalação você ainda não particionou o disco e ainda não é possível utilizar memória virtual, o disquete cria um Ramdisk com os arquivos necessários e carrega vários módulos na memória. Os disquetes do TechLinux por exemplo exigem 56 MB de RAM para instalar via HTTP. Se for o caso de instalar num PC antigo, que não tenha tudo isso de RAM, o melhor seria instalar provisoriamente mais RAM ou então instalar um segundo HD ou CD-ROM com os arquivos de instalação.

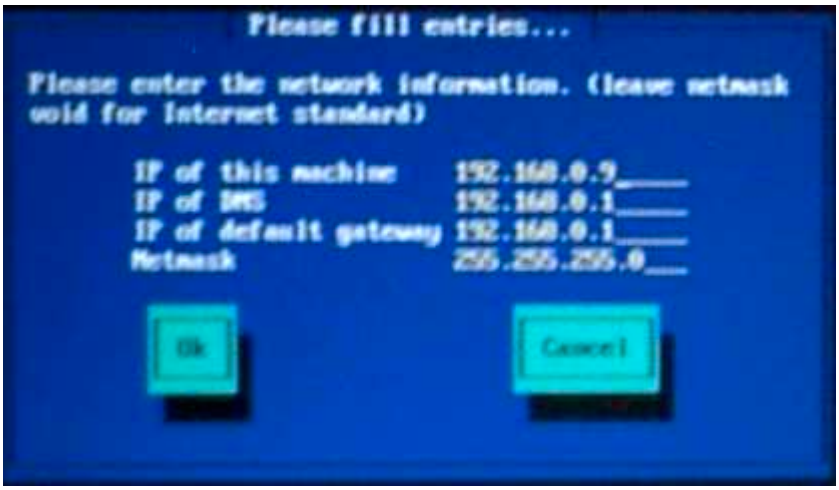
Se no início da instalação você optar pelo instalador em modo texto, a quantidade de memória cairá bastante e na maioria dos casos você conseguirá instalar num PC com 32 MB. Um detalhe importante é que o Mandrake não pode ser instalado em micros 486, pois os pacotes são compilados com otimizações para a plataforma Pentium, que melhoram um pouco o desempenho do sistema. Se for o seu caso, você pode tentar outra distribuição, como o Conectiva, Red Hat, Debian, etc. O Conectiva 4 é muito bom para PCs antigos, pois instala via rede com apenas 16 MB de RAM, ocupa pouco espaço no HD e instala um set de aplicativos bastante leves.

Resolvido o problema da memória e com o disquete escolhido, vamos à instalação.

Ao inicializar usando qualquer um dos três disquetes de instalação via rede a primeira pergunta será sobre o endereço IP da estação. Estes disquetes só funcionam em redes TCP/IP, mais um motivo para preferir o uso do TCP/IP sobre o NetBEUI, mesmo em redes pequenas.

As opções aqui são **Static**, **DHCP** e **ADSL**. A opção DHCP pode ser usado se na rede houver um micro compartilhando a conexão através do ICS do Windows ou outro programa que inclua um servidor DHCP. Apesar disso, eu recomendo que você utilize a opção de usar um endereço IP estático, que vai funcionar sempre. A opção ADSL não está disponível nos disquetes de todas as distribuições e tem uma funcionalidade um tanto quanto limitada, pois você poderá utilizá-la apenas nos serviços ADSL onde não é necessário autenticar utilizando nenhum programa de terceiros. Funciona por exemplo no Speedy ATM (as instalações antigas, onde basta configurar o endereço IP e o endereço do Gateway para ativar o acesso), mas não funciona nas instalações mais recentes do Speedy, onde é preciso instalar um programa que faz a autenticação.

Escolhendo a opção de usar endereços IP estáticos, chegamos à tradicional configuração do TCP/IP, onde é necessário especificar o IP da máquina na rede, o IP do DNS (caso exista algum na rede), o default Gateway e a máscara de sub-rede. Caso você tenha dúvidas sobre a configuração da rede, pode consultar o tutorial sobre configuração de redes que publiquei a algum tempo: http://www.guiadohardware.net/tutoriais/sharing/index.asp



Em seguida você precisa especificar um nome para o computador e o domínio, caso a rede faça parte de algum. O nome da máquina é importante caso você tenha configurado o servidor de onde serão baixados os arquivos para dar acesso apenas a algumas máquinas.

Finalmente, você precisará especificar o endereço do servidor HTTP, FTP ou NFS e o diretório do servidor onde estão os arquivos de instalação. Apartir daí as opções da instalação são as mesmas que seriam ao instalar apartir do CD. Na verdade, para o sistema não existe muita diferença, pois os arquivos no servidor serão justamente uma cópia do conteúdo do CD.

Apesar de já ser algo fora de moda, ainda existem alguns servidores FTP públicos que disponibilizam arquivos de instalação de várias distribuições. Caso você conheça algum você poderia colocar o micro numa rede com acesso compartilhado à Internet, configurar corretamente os endereços IP e acessar o servidor. Claro que esta opção seria viável apenas caso o FTP fosse rápido e a sua conexão fosse no mínimo de 256k. Baixar os arquivos de instalação de uma distro atual via modem demoraria dias :-)

Mas, o mais prático seria instalar apartir de algum micro da rede. Com uma rede de 100 megabits por exemplo a instalação não demorará mais do que demoraria via CD-ROM.

Se as demais estações da rede rodarem Windows você pode usar um servidor HTTP ou de preferência FTP qualquer para disponibilizar os arquivos. Você pode encontrar vários servidores gratuítos no Tucows ou outro site de downloads. Outra opção seria usar o IIS da Microsoft que é fácil de configurar, mas não deixe de desinstalá-lo depois de terminada a instalação, já que é muito perigoso mantê-lo ativo sem necessidade devido às varias brechas de segurança.

No Linux você também poderá utilizar estes recursos, através do Apache ou do servidor FTP que acompanha a sua distribuição preferida. O Mandrake inclui o FTPD, que é bastante simples de configurar. Não existe mistério, basta fornecer o endereço IP do micro que está disponibilizando os arquivos, além de login e senha de acesso.

Para instalar apartir de um servidor NFS (que é o modo mais prático aqui) os passos são os seguintes:

Presumindo que você tenha marcado a opção de instalar o NFS durante a instalação do Linux (no servidor) e que o serviço esteja ativo, você precisará apenas editar o arquivo **/etc/exports**,

adicionando os diretórios que serão compartilhados com a rede. Para verificar se o NFS está ativo, basta dar um:

/ etc/ rc.d/ init.d/ nfs status

Caso não esteja, você precisará ativa-lo através do Mandrake Control Center, LinuxConf, ou outro utilitário de configuração disponível na sua distribuição.

Por padrão o arquivo estará em branco. Adicione um diretório a ser exportado por linha, gerando um arquivo como o abaixo:

 # Isto é só um comentário
/ home/ morimoto/ install
/ mnt/ cdrom

Neste caso estamos disponibilizando tanto o diretório /home/morimoto/install quanto o CD-ROM, que naturalmente deverá estar montado no momento em que o cliente for acessá-lo. Para instalar apartir de uma pasta do HD você precisa apenas copiar todos os arquivos dos CDs para ela.

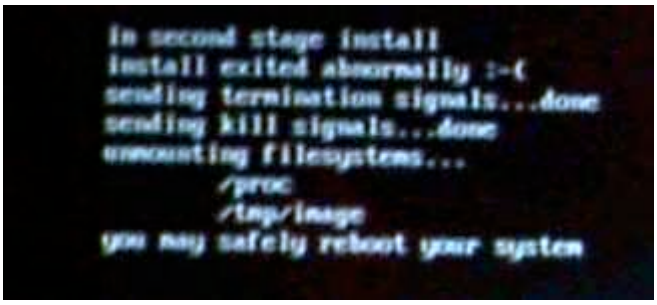
É possível definir vários parâmetros, especificando quais usuários terão acesso a cada diretório, dar permissões de apenas leitura, etc. opções que veremos com mais detalhes adiante, no tópico sobre servidores Linux. Compartilhando os diretórios sem parâmetros, como no exemplo, qualquer usuário da rede poderá acessá-los.

Para alterar o arquivo você precisará estar logado como root. Após terminar, basta reiniciar o serviço usando os comandos abaixo para que alterações surtam efeito:

/ etc/ rc.d/ init.d/ nfs stop
/ etc/ rc.d/ init.d/ nfs start

Na foto abaixo por exemplo havia habilitado o NFS no micro 192.168.0.2 e estava fazendo a instalação apartir do CD-ROM (/mnt/cdrom) que havia compartilhado.

Se depois de tudo resolvido a instalação for abortada com uma mensagem como:



"Install exited abnormally :-(
You may safely reboot your system"

Provavelmente o PC não tem memória RAM suficiente para carregar o instalador. Como disse, o mais recomendável é utilizar a instalação via rede em PCs com 64 MB ou mais. Você pode verificar as mensagens do Kernel para ver exatamente o que houve pressionando Alt + F3.

Colocando a mão na massa

Simplesmente instalar o Linux é a parte mais fácil. A menos que a sua placa de vídeo não seja compatível com o sistema, que o HD não tenha espaço livre suficiente, ou algo do gênero, você não terá maiores problemas para instalar praticamente nenhuma distribuição atual (com excessão talvez do Debian e Slackware, que ainda precisam de alguma configuração manual).

O problema começa justamente depois de instalar o sistema. O maior erro de muitos que instalam o Linux pela primeira vez é achar que o sistema é uma espécie de clone do Windows. Apesar das interfaces serem parecidas, o Linux conserva muitas particularidades e exige uma curva de aprendizado maior. Você não vai conseguir simplesmente sair fazendo de imediato as mesmas coisas que fazia no Windows.

Os programas disponíveis são diferentes, as configurações do sistema estão em locais diferentes e nem sempre são centralizadas, o Linux traz vários recursos, principalmente de linha de comando que não existem no Windows e muitas configurações que você nem imaginava que existiam estão disponíveis, o que pode causar confusão no início.

O sistema foi projetado com uma grande ênfase na segurança (por isso toda a recomendação em não usar o root) o que também dificulta as coisas no início. Por exemplo, antes de executar um arquivo recém baixado você precisará acessar as suas propriedades e marcar a opção de execução, para abrir os programas de configuração você precisará fornecer a senha de root, etc.

Enfim, é um mundo novo a ser explorado, que deve ser encarado como tal. Reserve algum tempo para explorar os recursos do sistema, como um final de semana, quando você puder fazer tudo com paciência.

Comandos do prompt

Apesar da interface gráfica ser muito mais fácil de usar, é bom você ter pelo menos uma boa noção de como as coisas funcionam pelo prompt de comando, isso vai lhe dar um domínio muito maior sobre o sistema. Aqui estão alguns comandos básicos:

cd : Serve para acessar os diretórios, como no DOS. "**cd /** " volta ao diretório Raiz, e "**cd ..**" sobe um diretório. Para abrir o diretório "/proc" por exemplo, digite "cd /proc".
Se você estiver dentro da pasta /home/fernando/mail por exemplo e quiser ir para a pasta /usr/local, não é preciso usar o "cd .." para voltar ao diretório raiz, para só depois abrir a pasta, basta dar o comando "cd /usr/local" dentro de qualquer pasta, que o sistema se encarregará de acessar a pasta correta. Se por outro lado, você quiser apenas abrir a pasta "old" dentro da pasta /home/fernando/mail, basta apenas digitar "cd old".

startx : Serve para abrir a interface gráfica apartir do prompt, caso você tenha escolhido inicializar em modo texto.

ls : corresponde ao DIR do DOS. O "**ls l more**" quebra a lista em páginas, serve para pausar a listagem, para que você consiga ler tudo. "**ls -a**" mostra também arquivos ocultos (que no Linux têm o nome iniciado com um ponto) e "**ls -alh**" mostra mais detalhes sobre os arquivos, incluindo as permissões de acesso e o tamanho.

man : esse comando quebra um galhão, serve para acessar os manuais do comandos. Se você tiver dúvida sobre a sintaxe ou as opções de um comando qualquer basta digitar "man comando" como por exemplo "**man ls**". ele vai abrir um arquivo de texto com todos os detalhes sobre o comando. Para sair, pressione "**q**"

info : Traz informações mais detalhadas sobre o comando, nem todos os comando tem uma página info, mas o número vem crescendo. Para usa-lo, basta digitar "info comando", como em "**info lsmod**"

Se você preferir transformar as páginas de manual num arquivo, para ler num editor de textos ou imprimir, use o comando "**man comando | col -b > arquivo.txt**", que copia toda a saída do comando man para o arquivo.txt mantendo a formatação. Naturalmente, você pode salvar em qualquer arquivo, nem mesmo a extensão .txt é obrigatória no Linux. Para imprimir direto, sem gerar o arquivo, use o "**man comando | col -b | lpr**", onde o lpr é a porta da impressora.

cp : para copiar arquivos, corresponde ao COPY do DOS. Se você copiar todos os arquivos, use apenas um "*****" ao invés de "*.*" como usaria no DOS. Por exemplo, "**cp * /home/fernando**" copia todo o conteúdo da pasta atual para a pasta "/home/fernando".

mv : Move. Serve tanto para mover arquivos, como em "**mv foto.pgn /home/morimoto**", que move o arquivo do diretório atual para o /home/morimoto, quanto para renomear arquivos, como em "**mv foto.png foto-old.png**"

rm : para deletar arquivos, corresponde ao del do DOS. Para deletar um diretório, use o "rm -r", como em "rm -r teste". Se preferir que o comando seja executado imediatamente, sem avisar sobre erros ou confirmar a cada arquivo, acrescente um **f** de "force", como em "**rm -rf teste**"

mkdir : para criar um diretório, "mkdir fernando"

rmdir : para deletar um diretorio, como em "**rmdir fernando**". O rmdir só funciona com

diretórios vazios. No caso de diretórios com arquivos, use o "**rm -r**" ou "**rm -rf**"

cat : serve para ver o conteúdo de um arquivo. Por exemplo, "cat carta" mostra o conteúdo do arquivo "carta". Este comando serve bem para ver o conteúdo de arquivos de texto pequenos, sem precisar abrir um editor mais sofisticado.

pwd : Mostra o diretório atual, use sempre que estiver em dúvida:

```
[morimoto@beta-2 morimoto]$ pwd
/home/morimoto
[morimoto@beta-2 morimoto]$
```

clear : limpa a tela

& : Este é um parâmetro que permite rodar aplicativos mantendo o terminal livre. No Linux, todos os aplicativos, mesmo os gráficos podem ser chamados a partir de uma janela de terminal. O comando "**konqueror**" por exemplo abre o Browser com o mesmo nome. O problema é que ao chamar algum aplicativo, o terminal ficará bloqueado até que o aplicativo seja finalizado, lhe obrigando a abrir um para cada programa.
Acrescentar o **&** no final do comando, como em "**konqueror &**" resolve este problema, mantendo o terminal livre. Note que alguns aplicativos exibem mensagens depois de serem abertos, basta pressionar **Enter** para voltar ao prompt.

ln : Permite criar links. Existem dois tipos de links suportados pelo Linux, os hard links e os links simbólicos. Os links simbólicos têm uma função parecida com os atalhos do Windows, eles apontam para um arquivo, mas se o arquivo é movido para outro diretório o link fica quebrado. Os hard links são semelhantes aos atalhos do OS/2 da IBM, eles são mais intimamente ligados ao arquivo e são alterados junto com ele. Se o arquivo muda de lugar, o link é automaticamente atualizado.
O comando **ln** dado sem argumentos cria um hard link, como em "**ln arquivo.txt /home/morimoto/arquivo.txt**". Para criar um link simbólico, basta acrescentar o argumento "-s", como em "**ln -s arquivo.txt /home/morimoto/arquivo.txt**".
Você verá muitos links espalhados pela estrutura de diretórios do Linux, um recurso muito usado quando os arquivos de sistemas mudam de lugar numa nova versão. Mantendo um link na localização antiga, todos os programas antigos continuam funcionando sem problemas.

Histórico : O Linux mantém um histórico dos últimos 500 comandos digitados. Para repetir um comando recente, simplesmente pressione as setas para cima ou para baixo até encontrá-lo. Para fazer uma busca use o comando "**history | grep comando**" , como em "**history | grep vi**" para mostrar todas as entradas começadas com "vi".

Você também pode executar uma fila de comandos de uma vez. Basta separá-los por ponto e vírgula, como em "**ls; pwd**" ou "**cd /home/morimoto; ls**"

Lembre-se que o Linux distingue letras maiúsculas e minúsculas. "ls" é diferente de "LS". Quando criar novos arquivos e pastas, prefira usar nomes em minúsculas, assim você evita confusão.

Usando o terminal : Existem duas formas de utilizar o prompt. A primeira é simplesmente abrir uma janela de terminal dentro da Interface gráfica, mas você também pode usar os terminais virtuais através do atalho **Ctrl+Alt+F2**. Você pode usar as teclas F de 1 a 6, onde cada uma representa um terminal independente. Para voltar para a interface gráfica, pressione Crtl+Alt+F7.

Assim como por default tem vários terminais de texto, também é possível ter vários terminais gráficos independentes, usando as teclas F de 7 a 12, onde cada um pode não apenas rodar aplicativos diferente, mas também rodar interfaces gráficas diferentes. Mas, só vou contar como mais pra frente, se você conseguir ler tudo até lá :-)

Uma alternativa mais corriqueira é usar os desktops virtuais. Cada desktop funciona como uma área independente e você pode alternar entre eles usando os atalhos presentes na interface gráfica que estiver utilizando:

Para enviar um programa aberto para outro desktop virtual, basta clicar sobre a barra com o botão direito do mouse e em seguida em "Para o ambiente...".

Mais um aviso importante é que quando tiver um problema, não tente simplesmente reiniciar o micro como no Windows. Reiniciar o Linux não resolve os problemas, assim que o micro reiniciar, ele estará igual ao que estava antes. Os erros de sistema são raros no Linux, embora muitos programas travem e causem outros tipos de problemas. Sempre que isso acontecer, reinicie o programa, tentar reiniciar o sistema inteiro será quase sempre perda de tempo.

Fechando programas travados

Apesar do Kernel do Linux ser extremamente estável, quase impossível de travar, os programas nem sempre são. Para complicar, o rápido desenvolvimento do sistema e a necessidade por novos aplicativos acabam fazendo que com muitas vezes as distribuições tragam programas ainda em estágio Beta, ou mesmo Alpha, que ainda não estão completamente estáveis. Isto acaba resultando em travamentos. A vantagem do Linux neste ponto é que você nunca precisará reiniciar todo o sistema, bastará matar o aplicativo problemático, ou no pior dos casos reiniciar a interface gráfica.

A forma mais prática de finalizar aplicativos é usar o **xkill**. Ao clicar sobre o ícone do programa, ou chama-lo pelo terminal (digitando **xkill**) o cursor do mouse virará um ícone de caveira. Basta clicar sobre o programa para finaliza-lo

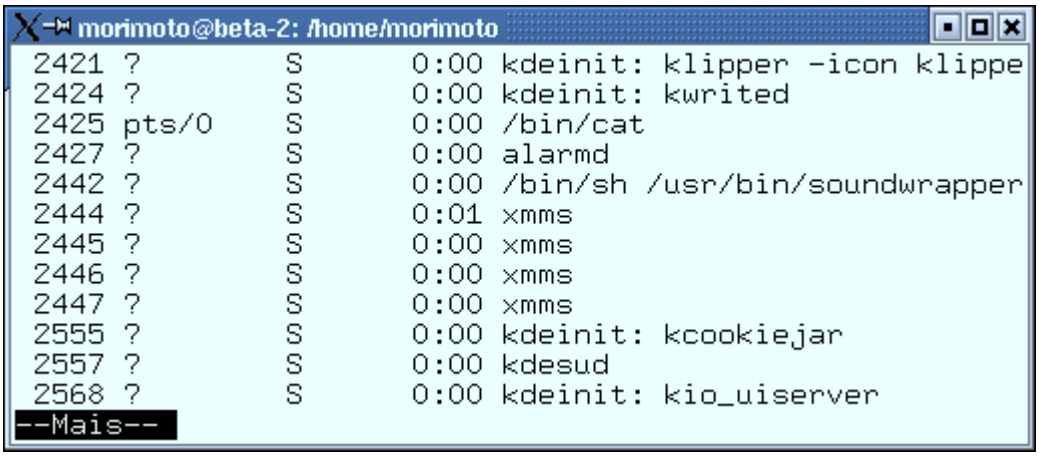
Você também pode finalizar os programas através do terminal, usando os comandos **kill** e **killall**. O killall pode ser usado sempre que você souber o comando que inicializa o programa a ser fechado. Por exemplo, para fechar o **xmms**, o mesmo do screenshot acima, bastaria escrever

"**killall xmms**", para finalizar o konqueror o comando seria "**killall konqueror**" e assim por diante.

O problema com o killall é que em muitos casos o comando para fechar o programa não é o mesmo que seu nome. Para fechar o mozilla por exemplo, você teria que digitar "**killall mozilla-bin**" e não apenas "killall mozilla", que seria o mais lógico.

Para os casos onde você não souber o nome do programa, existe o comando "**ps**" que mostra todos os processos em execução.

Existem várias opções para este comando. A que costumo usar mais freqüentemente é "ps -x | more" que mostra todos os processos iniciados por você no terminal atual, sempre dando uma pausa quando esta encher a tela:



Na coluna direita da lista você verá os nomes dos aplicativos. Veja que em muitos casos o mesmo programa aparece várias vezes, como o xmms, mas o **killall** se encarrega de acabar com todos os vestígios.

Na coluna da esquerda está o PID de cada processo, que pode ser usado em conjunto com o comando **kill**, como em "**kill 2444**"

Além do ps -x, você pode tentar o "**ps -aux**", que inclui os processos iniciados por outros usuários e em outros terminais. Ele resulta numa lista bem mais detalhada e também maior.

Se ao invés de um programa quem travar for o gerenciador de janelas, use o atalho **Ctrl+ Alt+ Backspace** para finalizá-lo. Você voltará para a janela de login e poderá inicializar novamente o gerenciador, ou tentar outro.

Montando e desmontando

Para tornar acessível o seu CD-ROM, disquete, ou mesmo uma partição que use um formato de arquivos suportado pelo Linux, como por exemplo uma partição Fat32, é preciso usar o comando "mount".

Para acessar o CD-ROM digite: "**mount /mnt/cdrom**"

Se você quiser trocar o CD que está na bandeja, você deverá primeiro "desmontar" o CD-ROM, com o comando "**umount /mnt/cdrom**". Depois de trocar o CD é só dar novamente o comando de montagem.

Para montar e desmontar disquetes os comandos são "**mount/mnt/floppy**" e "**umount /mnt/floppy**".

No KDE você pode montar e desmontar o CD-ROM simplesmente clicando com o botão direito sobre o ícone correspondente na área de trabalho. A interface gráfica está aqui para simplificar as coisas :-)

O Kernel 2.2, a última versão estável antes da atual, que é a 2.4, suportava o recurso de automount, que automatizava esta tarefa pelo menos para o CD-ROM. Por algum motivo este recurso deixou de ser suportado na versão atual, mas deve voltar nas próximas versões.

Acessando a partição do Windows apartir do Linux

Se você instalou o Windows 9x e o Linux em dual boot na mesma máquina, e quer acessar os arquivos que estão na partição Windows apartir do Linux, é só seguir as dicas abaixo:

Primeiro verifique qual é a partição onde o Windows está instalado. Lembre-se de como o Linux identifica suas partições de disco. Se o Windows estiver instalado na partição primária do primeiro HD (o mais provável), então a partição é **/dev/hda1**.

No prompt, digite "cd /mnt" e crie um diretório "windows" (pode ser outro nome qualquer) com o comando "**mkdir windows**". Agora é só dar o comando:

mount /dev/hda1 /mnt/windows -t vfat

Pronto, agora é só dar um "cd windows" para acessar todos os arquivos que estão na partição Windows. Você pode acessar os arquivos apartir da interface gráfica.

O comando mount é usado para montar vários sistemas de arquivos, incluindo unidades de rede. Veremos este recurso com mais detalhes adiante.

O terceiro botão

O botão central do mouse, que não tem muita serventia no Windows, permite copiar e colar entre aplicativos ou até mesmo entre aplicativos gráficos e terminais abertos dentro da interface gráfica. Isso substitui o crtl+c, crtl+v com a vantagem do comando ser dado com um único clique do mouse. Basta selecionar o trecho de texto, a imagem, ou o que quiser copiar numa janela e clicar com o botão central na janela onde quiser colar a seleção. Se você não tiver um mouse de três botões, pressione simultâneamente os dois botões. A maioria dos aplicativos também permite usar

o copiar/colar, como no Windows.

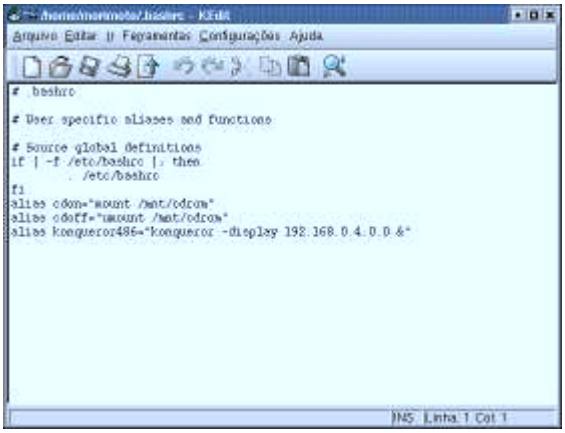
Editando arquivos de texto

Apesar de todos os programas de configuração que existem, a maior parte das configurações do Linux pode ser feita através de arquivos texto. Na verdade, a maioria dos programas de configuração nada mais são do que assistentes que facilitam a configuração destes arquivos.

Mas, muitas ferramentas de configuração podem mudar de uma distribuição para a outra, enquanto os arquivos de configuração são universais. Por isso, a maioria dos autores, prefere explicar a configuração dos arquivos ao uso das ferramentas, para que as instruções possam ser seguidas por todos os leitores.

Ou seja, gostando ou não, muitas vezes você precisará editar algum arquivo de configuração, ou talvez prefira fazer isso algumas vezes para ganhar tempo.

Para editar os arquivos você precisará apenas de um editor de textos. Existem vários exemplos: você pode por exemplo usar o **kedit**, em modo gráfico, ou o **vi** se estiver em modo texto. Para abrir o kedit, já no arquivo a ser editado, abra um terminal e digite "kedit nome_do_arquivo", como em "**kedit / home/ morimoto/ .bashrc**".



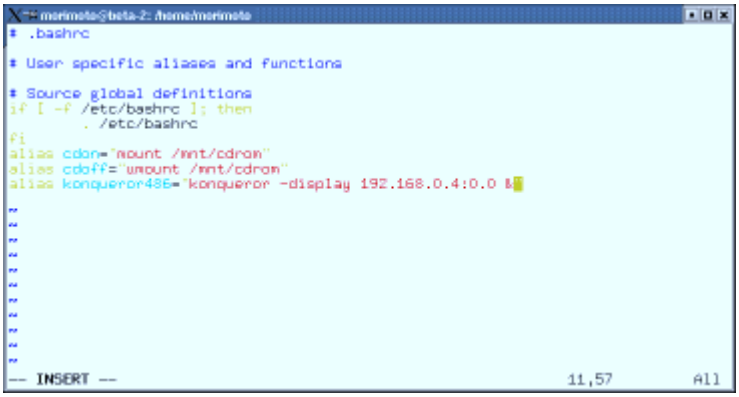
Kedit

O kedit é muito parecido com o notepad do Windows. Basta escrever o texto e salvar. No vi os comandos são um pouco mais complicados, pois ele tem muitos recursos e todos são ativados através do teclado. Mas, para editar um texto simples você não terá muito trabalho.

Digite: **vi nome_do_arquivo** Para abrir o arquivo a ser editado. Se o arquivo não existir o programa se encarregará de criá-lo. Se quiser abrir um arquivo que não está dentro da pasta onde está, basta dar o caminho completo. Se por exemplo, se você está na pasta home/morimoto e quer abrir o arquivo /etc/fstab, basta digitar **vi / etc/ fstab**

Ao abrir o vi você perceberá que o programa possui uma interface muito simples. Na verdade não há interface alguma :-) Mesmo assim, usá-lo é bem simples. O vi tem três modos de operação: comando, edição e o modo ex. Ao abrir o programa, você estará em modo de comando, para começar a editar o texto basta pressionar a tecla "**i**". Apartir daí ele funciona como um editor de

textos normal, onde o Enter insere uma nova linha, as setas movem o cursor, etc. Quando terminar de aditar o arquivo, pressione **Esc** para voltar ao modo de comando e em seguida "**ZZ**" (dois Z maiúsculos) para salvar o arquivo e sair. Para sair sem salvar pressione **Esc** e digite "**:q!**"



vi

Você voltará imediatamente para o terminal. Verifique se está tudo ok com o arquivo digitando **cat nome_do_arquivo**.

Desligando

Assim como no Windows, você precisa desligar o sistema corretamente para evitar perda de arquivos. Além da opção disponível na Interface gráfica, você pode desligar o sistema através de um terminal, usando um dos comandos abaixo:

reboot - Reinicia o micro.

halt – Desliga o micro.

shutdown -h now – Também serve para desligar o sistema. Você pode substituir o now (agora) por um tempo em minutos que o sistema esperará antes de desligar, usando o argumento "+" como em **shutdown -h +60**. Você pode ainda especificar o tempo no formato hh:mm como em **shutdown -h +06:00** (para desligar às 6:00 da manhã). É útil se você tem o hábito de deixar o micro ligado durante a madrugada baixando arquivos.

Ctrl+ Alt+ Del - Este é uma atalho de teclado, que dependendo da distribuição desliga ou apenas reinicia o sistema.

Configurando o Servidor

Com o sistema instalado, chegamos finalmente à configuração dos servidores. Abordarei aqui três ferramentas, o Samba, NFS e o Apache.

O Samba é o que ganhou mais atenção, pois permite interligar máquinas Linux a uma rede

Windows já existente, com a possibilidade de substituir ou trabalhar em conjunto com servidores Windows NT ou 2000, ou ainda trabalhar como uma estação Windows 98, apenas compartilhando arquivos e impressoras.

O NFS é um modo fácil e eficiente de compartilhar arquivos entre máquinas Linux e o Apache é simplesmente o servidor Web mais usado no mundo.

Para instalar estas ferramentas é necessário marcar as opções "**Web/ FTP**", "**Mail/ Groupware/ News**", "**Network Computer Server**" e também "**Database Server**" se você deseja oferecer acesso a banco de dados através do Apache. Os pacotes também podem ser instalados através do Mandrake Control Center, no utilitário "**Software Manager**".

Caso você tenha optado por marcar os pacotes durante a instalação do Mandrake, você receberá um aviso logo no final da instalação, chamando sua atenção para o fato de que alguns servidores estão ativos na máquina, o que pode representar um risco de segurança, etc. e dando a opção de desativa-los.

Caso você tenha desativado os serviços na instalação, você poderá ativá-los depois através do Mandrake Control Center, na seção: Sistema > Serviços.

Nos próximos tópicos estudaremos como é possível transformar sua máquina Linux num poderoso servidor de arquivos, impressoras, NFS, Web e FTP, capaz de se integrar a uma rede de máquinas Windows, a outras máquinas rodando Windows, ou mesmo como combinar máquinas Windows e Linux na mesma rede, aproveitando todo o potencial de ambos os sistemas.

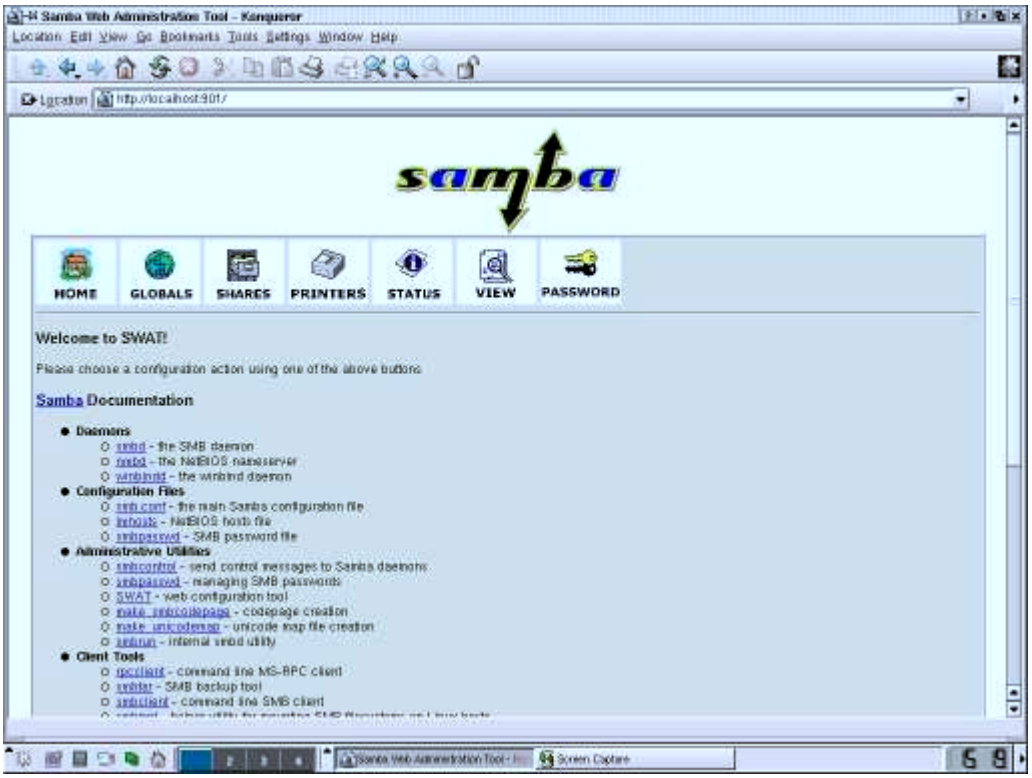
Samba

O Samba pode ser configurado através do Swat, um utilitário de configuração via Web, semelhante ao encontrado em alguns roteadores. Para acessa-lo basta abrir o Konqueror ou outro Browser disponível e acessar o endereço **http://localhost:901** basta fornecer a senha de root para acessar.

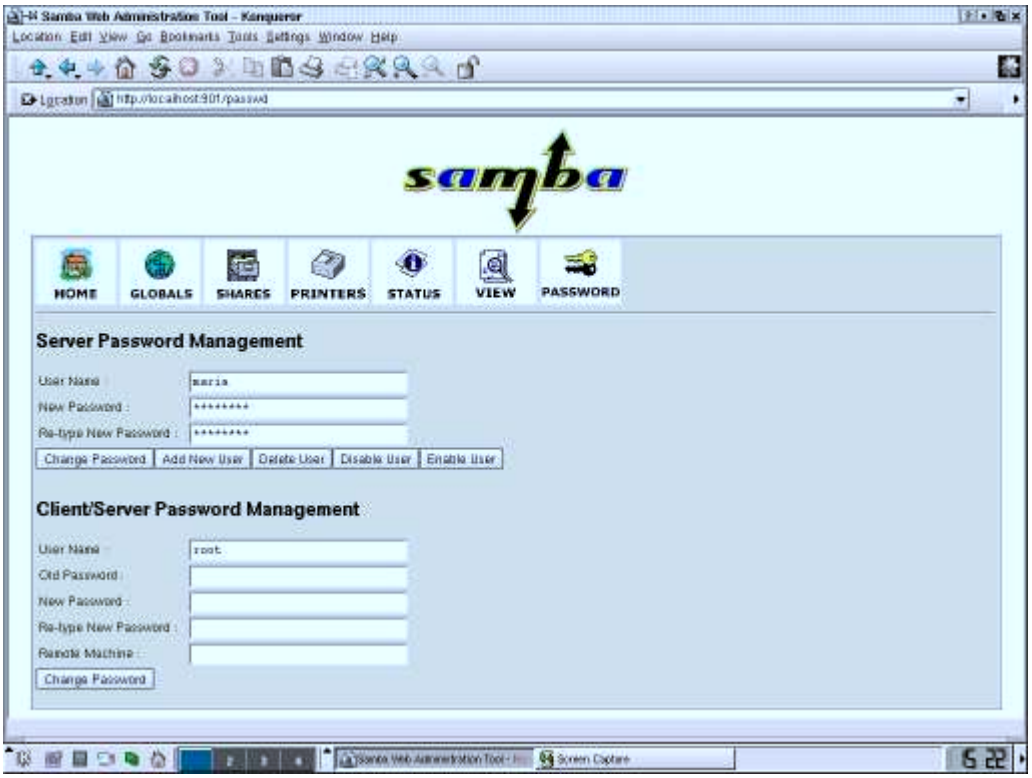
Antes de mais nada você deverá criar logins para todos os usuários que forem acessar o servidor. Você pode fazer isso através do Iniciar > Configuration > Other > UserDrake. Os logins e senhas devem ser os mesmos que os usuários irão utilizar para se logar no Windows. Um detalhe importante é que na configuração de rede das máquinas Windows (Painel de controle > Redes) você deve marcar a opção de login como "Login do Windows" e não como "Cliente para redes Microsoft" que é o default.

Falta agora apenas configurar o Samba para se integrar à rede e compartilhar as pastas desejadas.

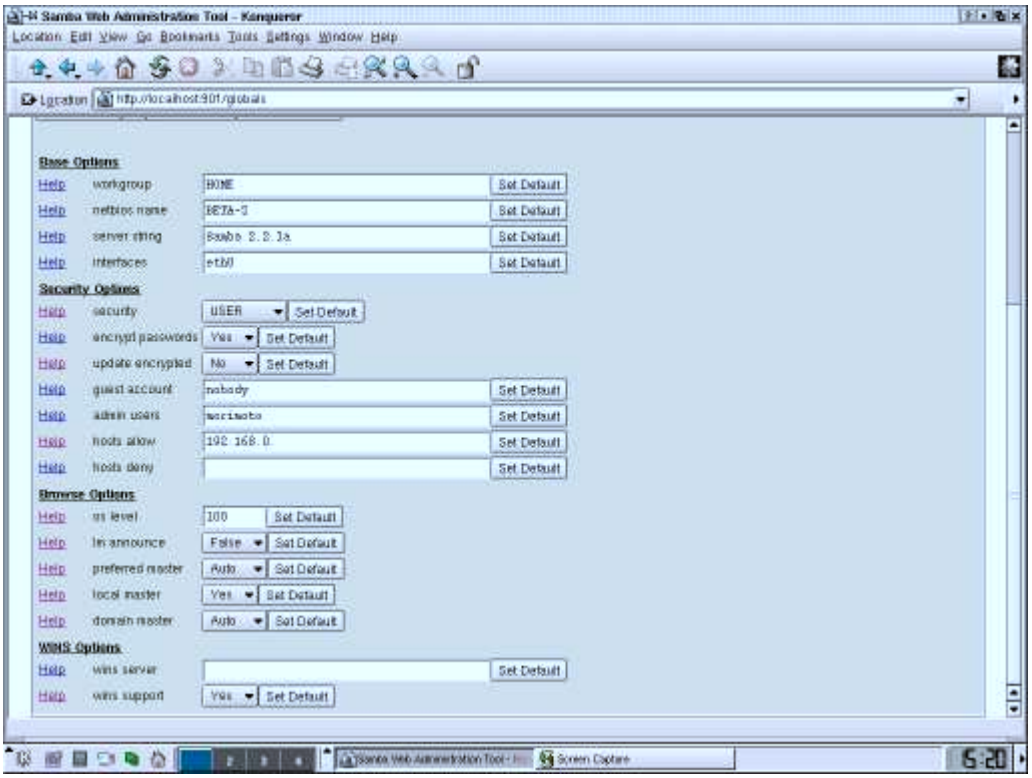
Ao abrir o Swat você verá um menu como o do screenshot abaixo, com vários links para a documentação disponível sobre o Samba, que você pode consultar para se aprofundar no sistema. Na parte de cima estão os links para as sessões da configuração, que é o que nos interessa:



Acesse primeiro a seção **Password**, onde você deverá cadastrar todos os usuários que terão acesso às pastas compartilhadas através do Samba, os mesmos que anteriormente cadastrou no UserDrake. Não apenas o Samba, mas vários outros programas servidores exigem que os usuários também estejam cadastrados no sistema, uma questão de segurança. Basta escrever o nome e senha do usuário e clicar no botão add new user.



Em seguida, acesse a seção “Globals”, que engloba todas as configurações de rede e de acesso:



Nas opções **Workgroup** e **NetBios** name você deve colocar o nome do computador e o grupo de trabalho a que ele pertence, como faria numa máquina Windows.

Na seção security coloque a opção **Security** como "**User**", o que permitirá definir quais usuários terão acesso ao sistema. A opção **Encrypt Password** também é importantíssima e deve ser configurada de acordo com a versão do Windows que rodar nas máquinas clientes. O Windows 95 original não suporta encriptação de senhas, por isso só poderá se conectar ao servidor caso a opção seja configurada com o valor "**No**". Porém, o Windows 95 OSR/2, Windows 98/SE/ME, Windows NT, Windows 2000 e Windows XP utilizam senhas encriptadas, por isso ao utilizar máquinas com qualquer um destes sistemas, que é o mais provável, a opção deve ser configurada como "**Yes**".

A opção **Hosts Allow** deve incluir os endereços IP todos os computadores que terão permissão para acessar o servidor. Se quiser que todos os PCs da rede tenham acesso, basta escrever apenas a primeira parte do endereço IP, como em 192.168.0., onde todos os endereços dentro do escopo serão permitidos.

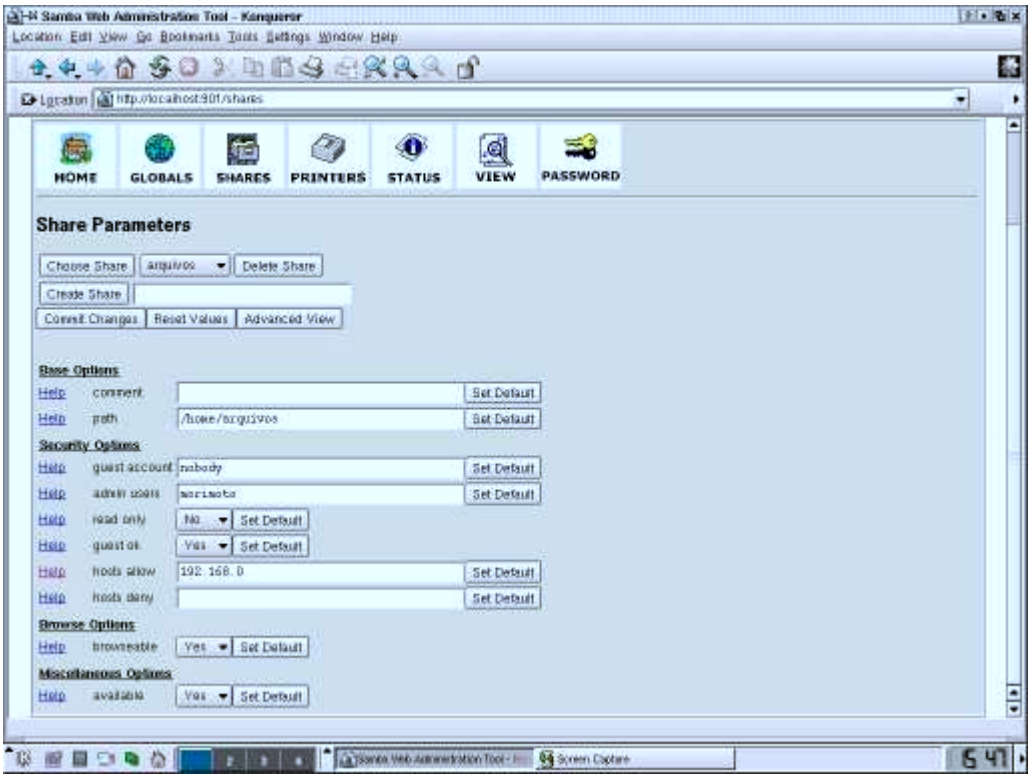
A opção **Hosts Deny** por sua vez permite especificar máquinas dentro do escopo configurados na opção Hosts Allow que não terão permissão para acessar o servidor, as exceções à regra. Por exemplo, se você configurou a opção acima como 192.168.0., mas deseja bloquear o acesso do PC 192.168.0.7, basta incluí-lo aqui. Se quiser incluir várias máquinas basta separar os endereços por espaços.

Na seção Browse Options, a opção **OS Level** permite especificar qual chance o servidor Linux terá de ser o master browser do domínio. No nosso caso é desejável que ele seja o master browser pois ele está concentrando todos os recursos acessados pelas estações. Sendo assim configure esta opção com um valor alto, 100 por exemplo, para que ele sempre ganhe as eleições. O default dessa opção é 20, que faz com que ele perca para qualquer máquina Windows NT, Windows 2000 ou Windows XP. Para completar, deixe a opção **Local Master** como "**Yes**" e as opções **Preferred Master** e **Domain Master** como "Auto".

Abaixo, deixe a opção **Wins Support** ativada (**Yes**). A opção **Wins Server** deve ser deixada em branco, a menos que exista na rede algum servidor Wins. Como no seu caso o único servidor é a máquina Linux, você pode configurar as máquinas Windows para utilizá-la como servidor Wins, para isto basta colocar o seu endereço IP no campo "Servidor Wins" na configuração de rede das estações.

Terminando, pressione o botão **Commit Changes** no topo da tela para que as alterações entrem em vigor.

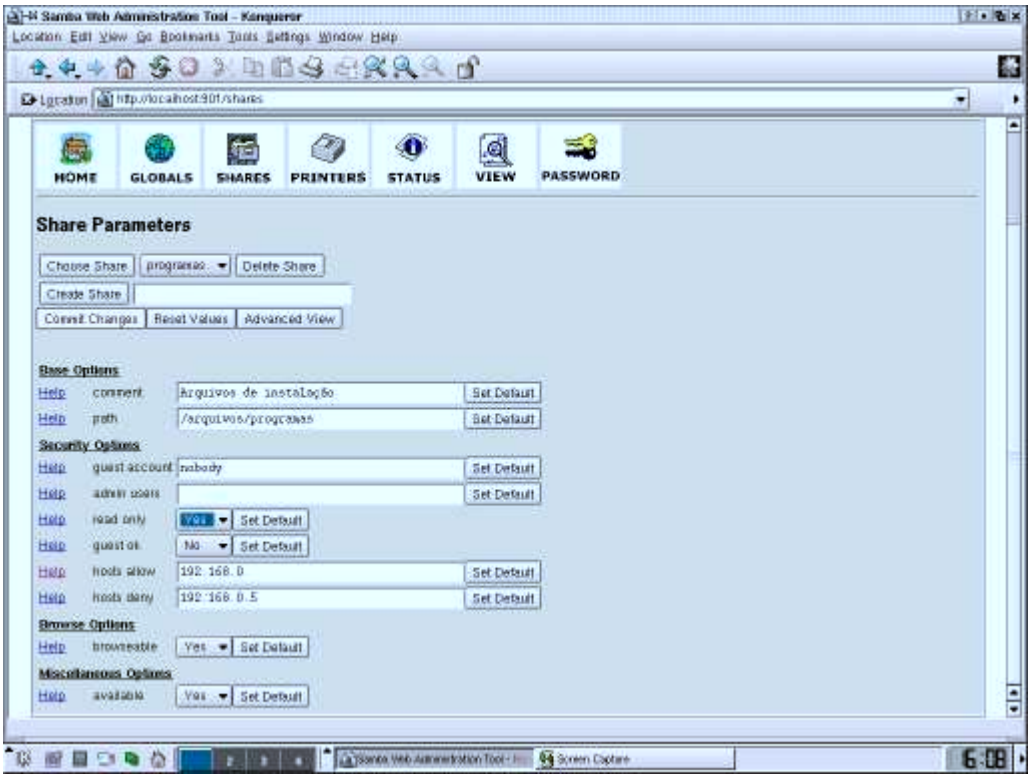
Finalmente, você deve configurar as pastas a serem compartilhadas com as estações, através da seção Shares:



Cada usuário que cadastrou no sistema já possui um diretório home criado. Estas pastas ficam dentro do diretório /home e podem ser usadas para guardar arquivos pessoais, já que a menos que seja estabelecido o contrário, um usuário não terá acesso à pasta pessoal do outro. Além dos diretórios home você pode compartilhar mais pastas de uso geral.

Para criar um compartilhamento basta escrever seu nome no campo no topo da tela e clicar no botão **Create Share**:

Depois de criado um compartilhamento, escolha-o na lista e clique no botão **Choose Share** para configura-la. Você verá uma lista de opções como a abaixo:



O campo **Path** é o mais importante, pois diz justamente qual pasta será compartilhada. O nome do compartilhamento diz apenas com que novo ele aparecerá no ambiente de redes. No caso do compartilhamento do screenshot a pasta compartilhada é /arquivos/programas.

A opção **Read Only** determina se a pasta ficará disponível apenas para leitura (opção **Yes**) ou se os usuários poderão também gravar arquivos (opção **No**). Você também pode determinar quais máquinas terão acesso ao compartilhamento através das opções **Hosts Allow** e **Hosts Deny**. As configurações feitas aqui subscrevem as feitas na seção global. Se por exemplo a máquina 192.168.0.5 possui permissão para acessar o sistema, mas foi incluída na campo Hosts Deny do compartilhamento **programas**, ela poderá acessar outros compartilhamentos do sistema, mas não o compartilhamento programas.

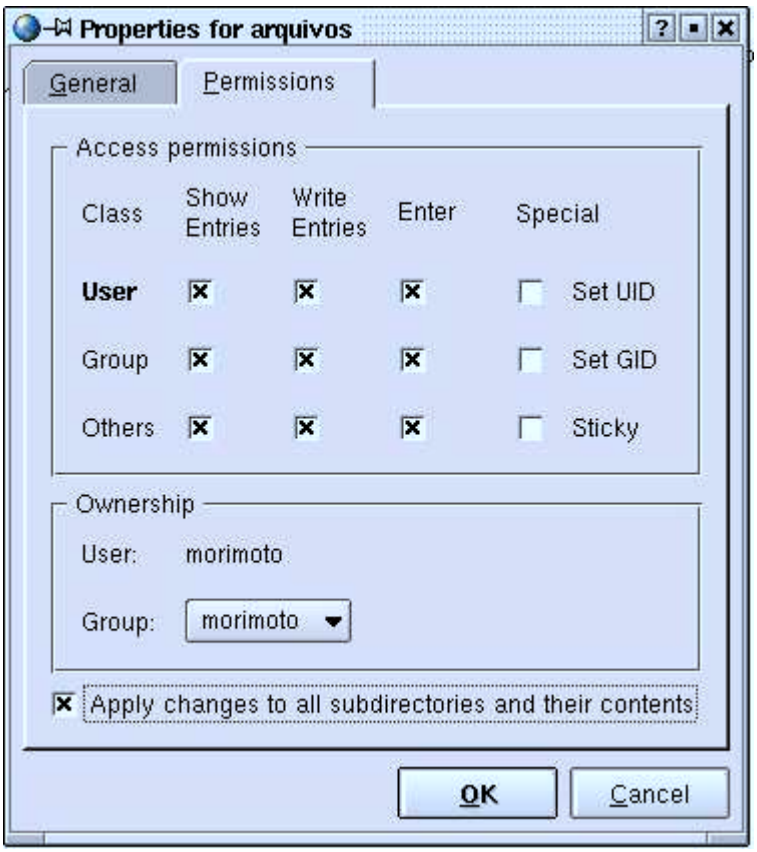
A opção **Browseable** permite configurar se o compartilhamento aparecerá entre os outros compartilhamentos do servidor no ambiente de redes, ou se será um compartilhamento oculto, que poderá ser acessado apenas por quem souber que ele existe. Isso tem uma função semelhante a colocar um "$" numa pasta compartilhada no Windows 98. Ela fica compartilhada, mas não aparece no ambiente de redes.

Finalmente, a opção **Available** especifica se o compartilhamento está ativado ou não. Você desativar temporariamente um compartilhamento configurando esta opção como "**No**". Fazendo isso ele continuará no sistema e você poderá torna-lo disponível quando quiser, alterando a opção para "**Yes**".

Um detalhe importante é que os usuários só terão permissão para acessar pastas que o login permite acessar. Por exemplo, no Linux o único usuário que pode acessar a pasta /root é o próprio root, ou outro autorizado por ele. Mesmo que você compartilhe a pasta root através do Samba, os

demais usuários não poderão acessá-la.

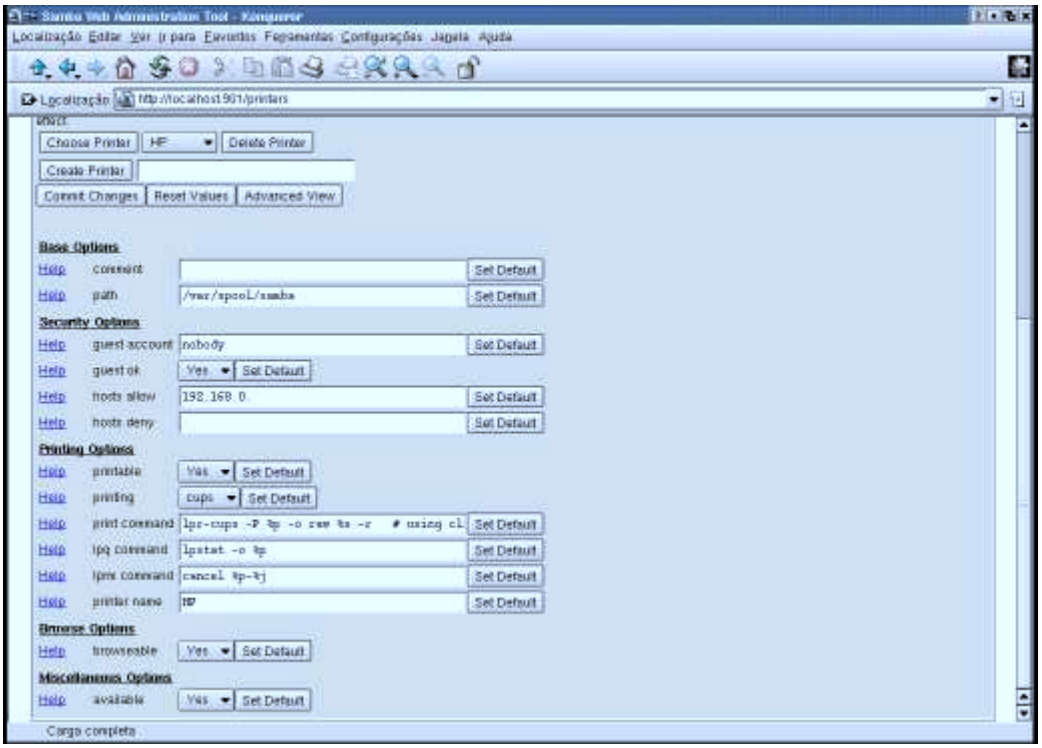
Para editar as permissões de uma pasta, basta abrir o gerenciador de arquivos e nas propriedades da pasta acessar a guia **Permissions**. As permissões podem ser dadas apenas ao usuário, para todos os usuários pertencentes ao grupo do usuário dono da pasta, ou para todos os usuários. A opção Apply changes to all subdirectories e their contents deve ficar marcada para que as permissões sejam aplicadas também às subpastas:



Terminadas as configurações, o servidor já irá aparecer no ambiente de redes, como se fosse um servidor Windows. Os compartilhamentos podem ser acessados de acordo com as permissões que tiverem sido configuradas e podem ser mapeados como unidades de rede entre outros recursos.

Você pode compartilhar inclusive o CD-ROM do servidor se desejar, basta para isso compartilhar a pasta **/mnt/cdrom**, mas isso não é muito prático, pois além de trocar o CD-ROM, é necessário montar e desmontar a unidade apartir do servidor.

Para compartilhar uma impressora já instalada na máquina Linux o procedimento é o mesmo. Acesse a seção **printers**, escolha a impressora a ser compartilhada (a lista mostrará todas as instaladas no sistema), configure a opção **available** como "**yes**" e configure as permissões de acesso como vimos anteriormente. No Mandrake você pode instalar impressoras através do Mandrake Control Center. Caso você esteja usando outra distribuição e o utilitário não esteja disponível, tente o linuxconf.



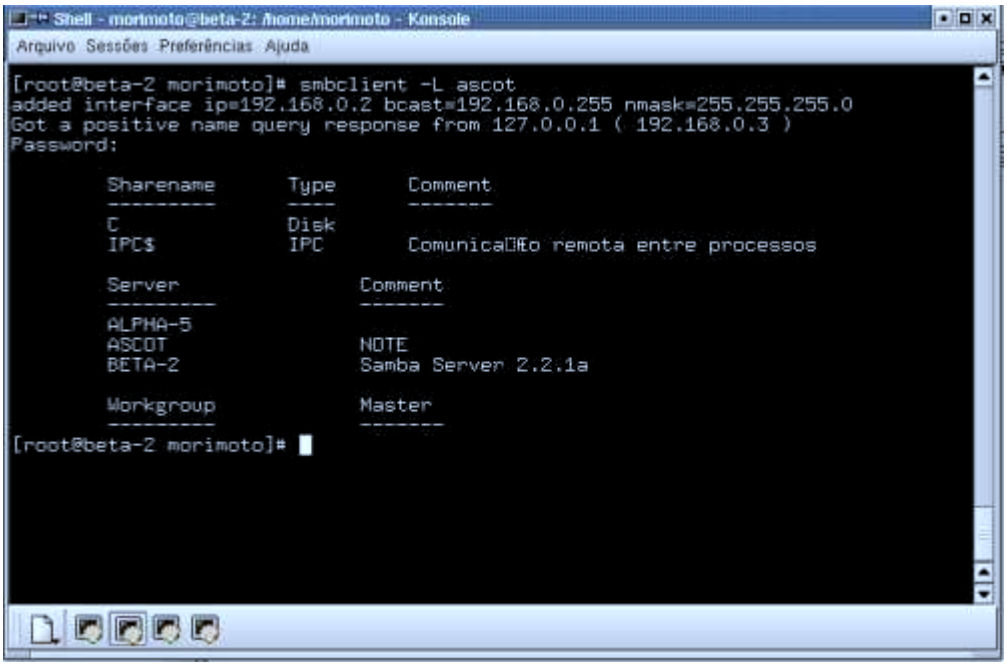
Acessando compartilhamentos de máquinas Windows

O Samba também inclui um módulo cliente, o **smbclient** que pode ser usado para fazer inverso, ou seja, acessar compartilhamentos de máquinas Windows apartir do Linux.

O uso deste comando é bastante simples. Abra um terminal e digite:

smbclient -L nome_da_maquina

Como por exemplo "smbclient -L ascot". Ele pedirá a sua senha de usuário e em seguida mostrará uma lista dos compartilhamentos disponíveis na máquina que solicitou:



Lembre-se as máquinas Windows 95/98/ME aceitam conexões de rede por parte de qualquer usuário. A única opção de segurança é colocar senhas nos compartilhamentos. Mas, as máquinas rodando Windows NT ou Windows 2000 precisam ser configuradas para dar acesso ao login que você está utilizando na máquina Linux. Para isso basta acessar o painel de controle > usuários e senhas (no Windows 2000) e adicionar o login e senha.

Voltando à configuração do smbclient, depois de decidir qual compartilhamento quer acessar, você deverá montá-lo para ganhar acesso. Você pode montar o compartilhamento em qualquer pasta vazia do sistema. Como exemplo eu montei o compartilhamento "C" disponível na máquina "ascot" no diretório "/mnt/windows" da máquina Linux. Para isso o comando é o seguinte:

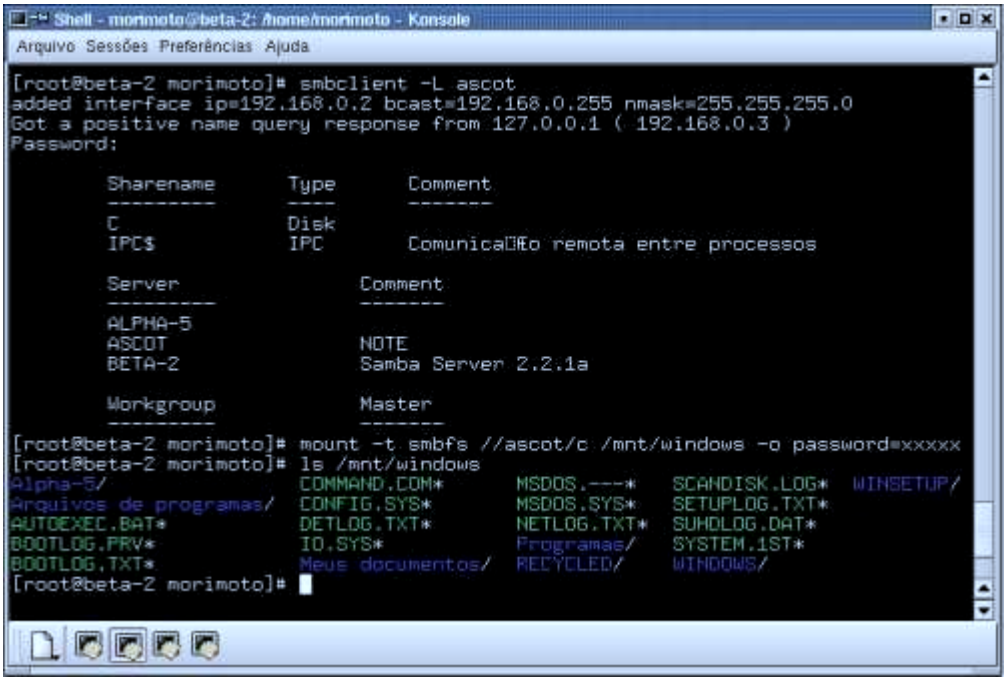
mount -t smbfs //ascot/c /mnt/windows -o password=xxxxx
(substituindo o xxxxx pela senha, naturalmente)

O comando mount é um dos comandos mais tradicionais do Linux, que permite "mapear" um diretório qualquer dentro de outro diretório do sistema para que este possa ser acessado. A opção "**-t**" serve para especificar o sistema de arquivos, já que não estamos utilizando um sistema de arquivos nativo do Linux. O "**smbfs**" indica o sistema de arquivos que será utilizado, este sistema que permite mapear unidades de rede compartilhadas pelo Windows.

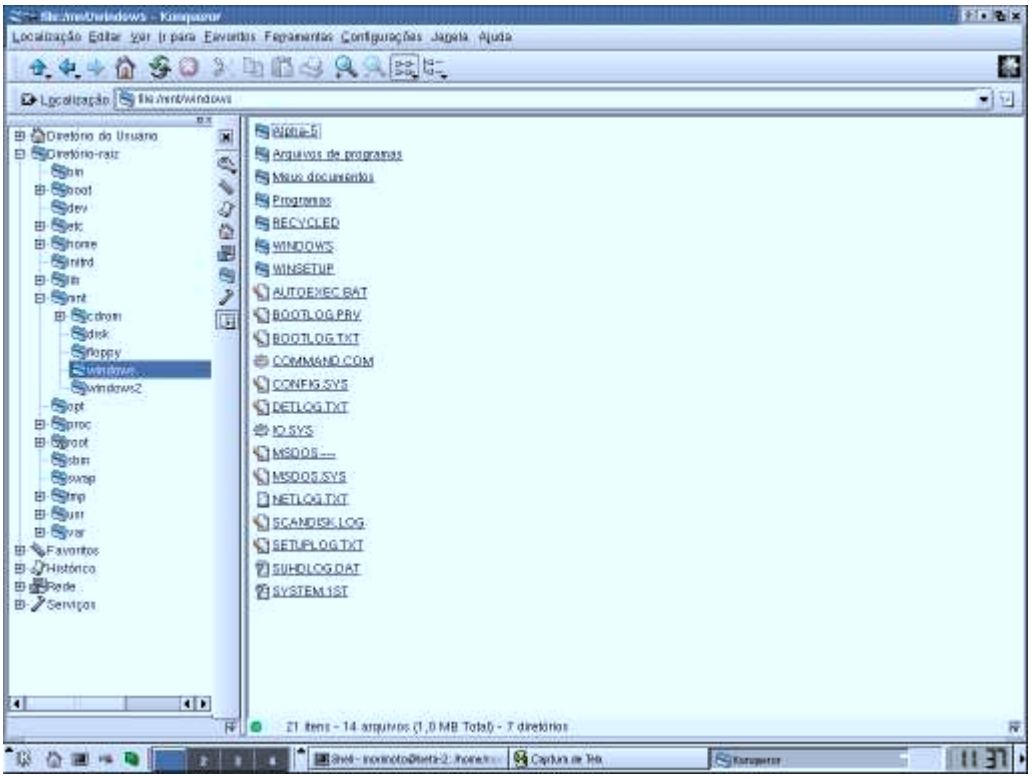
Em seguida, especificamos o compartilhamento e o diretório onde ele será montado seguido pelo "**-o**". Este é só um exemplo. Se você for montar o compartilhamento "arquivos" dentro da máquina "ricardo" no diretório "/home/maria/ricardo" da máquina Linux, o comando seria:
mount -t smbfs //ricardo/arquivos /home/maria/ricardo -o password=xxxxx
E assim por diante.

No "**password=xxxxx**" você deve informar a senha do compartilhamento que está sendo acessado. Se ele não tiver senha, basta deixar este último campo em branco.

Depois do comando você pode dar um “ls” no diretório onde o compartilhamento foi montado só para checar se os arquivos realmente estão lá:

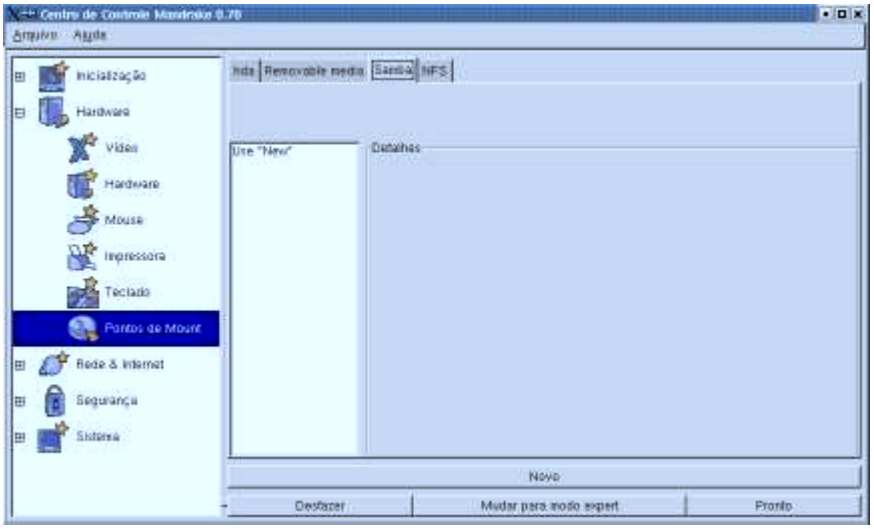


Depois de montado, o compartilhamento pode ser acessado pelo gerenciador de arquivos da sua interface (Konkeror no KDE, nautilus no Gnome, etc.):



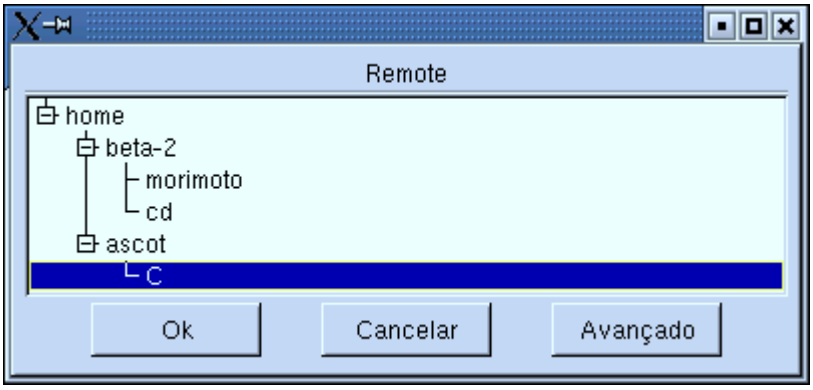
No Mandrake 8.1 e outras distribuições que trazem a ferramenta DiskDrake, como por exemplo o TechLinux, você pode montar as partições Windows de um jeito mais prático.

O DiskDrake pode ser encontrado dentro do Mandrake Control Center na seção Hardware > Pontos de Montagem. A parte que nos interessa está na aba "Samba":

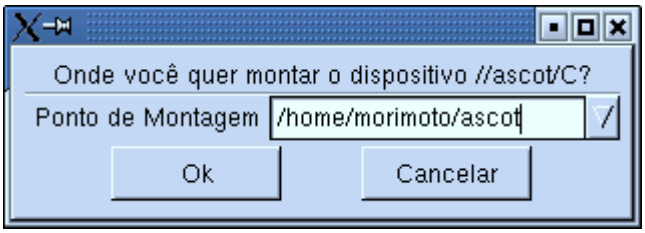


O funcionamento é muito simples. Clique em "novo" e aponte o compartilhamento a ser montado na janela que será aberta. Serão mostrados todos os compartilhamentos disponíveis na rede,

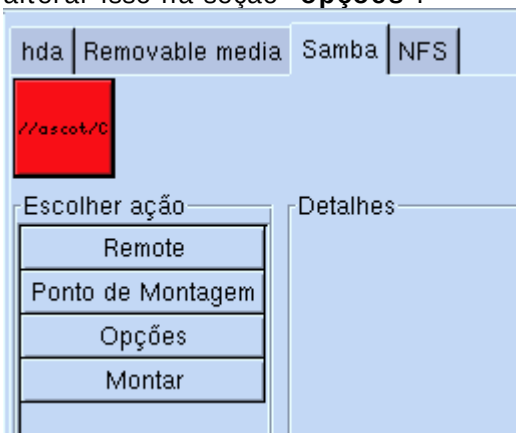
inclusive os de outras máquinas Linux rodando o Samba.



Em seguida, basta fornecer o ponto de montagem desejado. Note que dentro do diskdrake você tem privilégios de root e pode montar os compartilhamentos onde quiser. Mas, tenha o cuidado de não montar numa pasta onde seu login de usuário (ou de quem for usar a máquina) não tenha permissão de acesso.



Para finalizar, basta montar o sistema de arquivos para ter acesso. Por default, ele passará a ser montado a cada inicialização do sistema, até que você volte aqui e desmonte-o. Mas, você pode alterar isso na seção "**opções**".



Configurando manualmente

Se por qualquer motivo o Swat não estiver instalado no seu sistema, ou você preferir configurar

tudo manualmente, basta abrir o arquivo **smb.conf**, que concentra as configurações do Samba, num formato semelhante ao das opções do Swat, mantendo as mesmas seções: global, homes, printers, etc. Ao instalar o Samba é criado um smb.conf com configurações default, você precisará apenas alterar as mesmas opções que alteraria no Swat.

O smb.conf pode ser encontrado em **/ etc/ samba** (no caso do Mandrake) ou em **/ etc** (no caso de algumas distros). Para abri-lo, com privilégios de root, você pode digitar simplesmente "**kdesu kedit / etc/ samba/ smb.conf**" num terminal.

```
# Global parameters
[global]
        workgroup = HOME
        netbios name = BETA-2
        server string = Samba Server %v
        interfaces = eth0
        encrypt passwords = Yes
        log file = /var/log/samba/log.%m
        max log size = 50
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        printcap name = lpstat
        os level = 100
        dns proxy = No
        hosts allow = 192.168.0.
        printing = cups

[homes]
        comment = Home Directories
        read only = No
        browseable = No

[printers]
        comment = All Printers
        path = /var/spool/samba
        create mask = 0700
        guest ok = Yes
        printable = Yes
        print command = lpr-cups -P %p -o raw %s -r   # using client side printer drivers.
        lpq command = lpstat -o %p
        lprm command = cancel %p-%j
        browseable = No

[morimoto]
        path = /home/morimoto
        read only = No

[cd]
        path = /mnt/cdrom

[HP]
        path = /var/spool/samba
        read only = No
        create mask = 0700
        guest ok = Yes
        printable = Yes
        print command = lpr-cups -P %p -o raw %s -r   # using client side printer drivers.
        lpq command = lpstat -o %p
        lprm command = cancel %p-%j
        printer name = HP
        oplocks = No
        share modes = No
```

O Swat serve apenas como uma interface para a edição deste arquivo. Seja qual for o modo de configuração escolhido, basta fazer backups regulares deste arquivo para restaurar as configurações do servidor em caso de problemas.

Sempre que alterar manualmente **smb.conf**, ou mesmo alterar algumas opções pelo Swat e quiser verificar se as configurações estão corretas, rode o **testparm** (basta chama-lo num terminal). Ele funciona como uma espécie de debug, indicando erros grosseiros no arquivo.

Se por acaso você estiver utilizando uma distro que não venha com o Samba, basta baixar o RPM adequando à sua distribuição aqui:
http://us1.samba.org/samba/ftp/Binary_Packages

Para instalar, basta clicar sobre o arquivo ou usar o comando "**rpm -ivh nome_do_arquivo**" no terminal.

Depois de instalar o arquivo e configurar o **smb.conf**, use os comandos abaixo para inicializar, parar e verificar o status do serviço sempre que precisar:

/ etc/ rc.d/ init.d/ smb start
/ etc/ rc.d/ init.d/ smb stop
/ etc/ rc.d/ init.d/ smb status

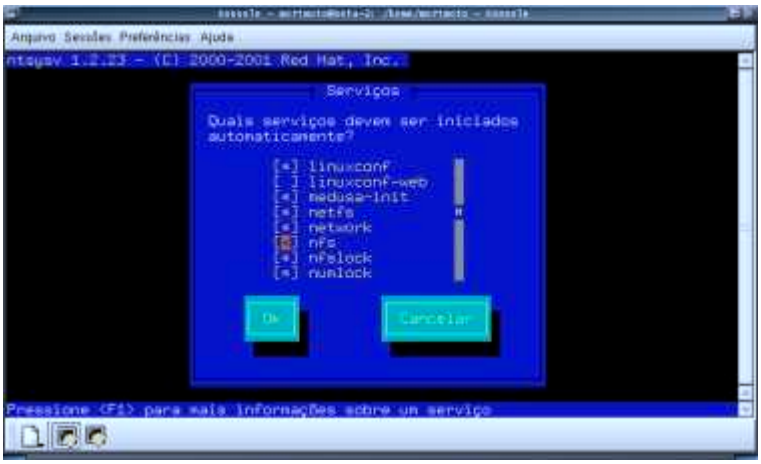
O comando **smbstatus** também é muito útil, pois permite verificar quais estações estão conectadas ao servidor e quais recursos estão sendo acessados no momento.

Usando o NFS

Enquanto o Samba permite solucionar sem muita dor de cabeça o desafio de interligar máquinas Linux e Windows na mesma rede, o NFS permite compartilhar sistemas de arquivos entre máquinas Linux.

Na verdade, você pode perfeitamente usar o Samba para compartilhar arquivos entre máquinas Linux, como vimos acima e é o que você terá mais facilidade em fazer numa rede mista.

Mas, o NFS não deixa de ser um recurso importante, que você não deve deixar de estudar, principalmente por que este é um recurso muito prático de usar. O suporte a NFS faz parte do Kernel do Linux e vem habilitado por default, mas, nem todas as distribuições trazem o serviço habilitado por default. Você pode checar se o serviço está habilitado usando o comando "**/ etc/ rc.d/ init.d/ nfs status**". Caso não esteja, habilite o serviço no Mandrake Control Center, em Sistema > Serviços, ou no LinuxConf caso o Mcc não esteja disponível na sua distribuição. Outra opção prática para habilitar o serviço é o **ntsysv**, que é incluído na maioria das distribuições. Basta das o comando num terminal:



Para compartilhar diretórios através da rede você deve editar o arquivo "**/etc/exports**". Você precisará apenas incluir os diretórios a serem exportados, um por linha, incluindo as restrições para acesso a cada diretório.

Por exemplo, se você desejar exportar o diretório /home/fernando/tralhas, sem estabelecer restrições, ou seja, permitir que qualquer máquina tenha permissão de leitura e escrita, basta incluir o diretório no arquivo, que ficará assim:

 # isto é só um comentário
/home/fernando/tralhas

Para estabelecer restrições, basta adicionar os argumentos entre parênteses depois do diretório. Se você deseja que apenas o host "**andre**" tenha acesso à pasta, e mesmo assim somente para leitura, a linha ficaria assim:

/home/fernando/tralhas andre(ro)

Para adicionar mais hosts, basta incluir os argumentos na linha, separados por espaços:

/home/fernando/tralhas andre(ro) morimoto(ro) gdh(ro) pia_da_cozinha(ro)

Veja que os compartilhamentos são feitos com base nos nomes dos hosts, e não com base no nome dos usuários.

Para dar acesso de leitura e escrita, use o argumento **rw**. Você pode usar ainda o **noacess**, que permite que você compartilhe apenas os arquivos dentro do diretório, mas não seus subdiretórios, que ficarão invisíveis.

Depois de incluir todos os diretórios que deseja compartilhar, basta salvar o arquivo e reiniciar o serviço **nfs** para que as alterações surtam efeito. Para isso, use os comandos:

/etc/rc.d/init.d/nfs stop
/etc/rc.d/init.d/nfs start

Você pode usar estes comandos sempre que desejar parar o serviço.

Ao compartilhar os diretórios, resolvemos apenas metade do problema. Ainda falta acessá-las apartir dos clientes.

Para isso, você precisará apenas montar as pastas num diretório qualquer, usando o comando **mount**, fornecendo o endereço IP ou o nome da máquina que está compartilhando os diretórios, o diretório que irá ser montado e o diretório na sua máquina onde ele será montado, como por exemplo:

mount 192:168.0.4:/ home/ fernando/ tralhas / home/ morimoto/ docs

Este comando monta o diretório /home/fernando/tralhas, que está na máquina 192.168.0.2 no diretório /home/morimoto/docs. Você também pode usar o nome da máquina ao invés do endereço IP:

mount fernando:/ home/ fernando/ tralhas / home/ morimoto/ docs

Note que ao montar uma pasta qualquer num diretório que não esteja vazio, o conteúdo do diretório ficará inacessível até que você desmonte o sistema de arquivos, usando o **umount**.

Se preferir que o diretório seja montado automaticamente na inicialização do micro, basta incluir as pastas a serem montadas no arquivo **/ etc/ fstab** incluindo "**nfs defaults 0 0**" no final da linha, que indica o sistema de arquivos. Ao incluir a linha acima, seu fstab ficará parecido com o abaixo:

/ dev/ hda1 / ext3 defaults 1 1
/ dev/ hda6 / home ext3 defaults 1 2
/ dev/ hda5 swap swap defaults 0 0
/ / ascot/ c / mnt/ windows smbfs username=% 0 0
mount fernando:/ home/ fernando/ tralhas / home/ morimoto/ docs nfs defaults 0 0

Veja que no meu caso incluí também a linha**:**
/ / ascot/ c / mnt/ windows smbfs username=% 0 0
Que serve para mapear o drive C da máquina Ascot usando o Samba, como descrevi acima. Veja que a sintaxe do comando mudou um pouco, pois agora o sistema de arquivos é escrito no final da linha, não no início.

Você pode usar o fstab para incluir qualquer sistema de arquivos que gostaria que fosse montado automaticamente durante a inicialização. Se por exemplo você quiser montar a partição C: do Windows, inclua **/ dev/ hda1 / mnt/ windows vfat defaults 00** para monta-la no diretório /mnt/windows.

Naturalmente, o "/dev/hda1" muda caso a partição Windows não seja a partição primária do primeiro HD. Caso a partição Windows esteja formatada em NTFS (Windows 2000 ou XP) você deve usar **ntfs** ao invés de **vfat**. Funciona, apesar do suporte a NTFS ainda ser experimental e ainda assim somente-leitura.

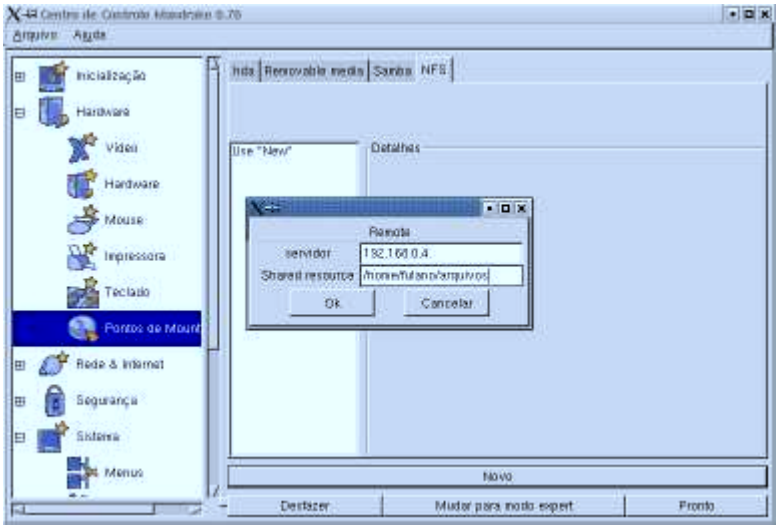
Se preferir dar todos os comandos manualmente, você pode simplificar as coisas usando o recurso de alias. Ao invés de digitar "mount /dev/hda1 /mnt/win -t vfat" e "umount /dev/hda1 /mnt/win -t vfat", você pode digitar apenas "winon" e "winoff" por exemplo.

Para isso basta editar o arquivo .**bashrc** que está no seu diretório de usuário e incluir linhas

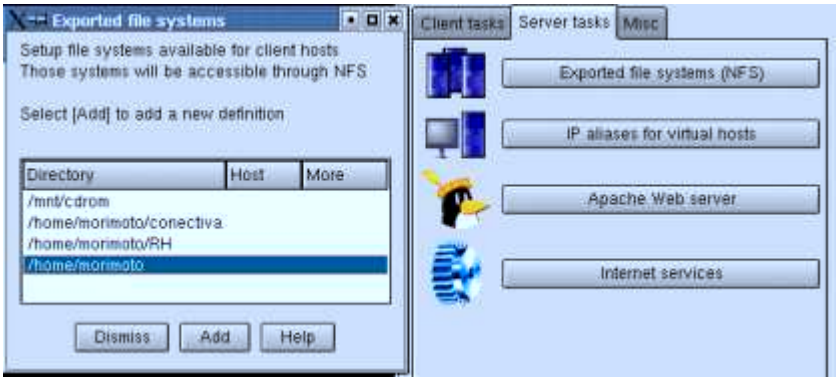
como: "**alias winon="mount / dev/ hda1 / mnt/ win -t vfat**"

Para criar os atalhos para os comandos que desejar. Depois de salvar o arquivo, basta digitar os novos comandos no terminal.

Além de fazer tudo via fstab ou manualmente, você também pode montar os sistemas de arquivos através do Mandrake Control Center, na sessão Pontos de Montagem, assim como fizemos com o Samba:



Para compartilhar os diretórios, você pode usar o "**netconf**" presente no Mandrake, Red Hat, Conectiva e na maioria das outras distribuições. Basta chama-lo no terminal.



Apache

O Apache é o servidor Web mais usado no mundo, graças ao seu bom desempenho e confiabilidade. Durante a instalação você teve a oportunidade de instalar o Apache. Se ele já estiver instalado, basta habilitar o serviço "**httpd**" no Mandrake Control Center, ou usar o

comando "**/ etc/ rc.d/ init.d/ httpd start**"

Para parar o serviço, você pode novamente recorrer ao mcc, ou usar o comando "**/ etc/ rc.d/ init.d/ httpd stop**". Os dois comandos também valem para outras distribuições.

Em seguida, abra um browser e acesse o endereço http://localhost. Se tudo estiver funcionando, você verá a página padrão do Apache. Em seguida, veja se o servidor pode ser acessado através da rede ou através da Internet, através do endereço http://seu_ip

Se o servidor estiver acessível apenas localmente provavelmente você se esqueceu de abrir a porta do apache no Firewall. Se você estiver usando o TinyFirewall que vem no Mandrake, basta rodar novamente o assistente através do Mandrake Control Center e abrir a porta do Servidor http quando perguntado.

Se o Apache ainda não está instalado, basta abrir o gerenciador de software no Mandrake Control Center e instalar os pacotes do Apache, na seção Server > Web/FTP > Outros. Se preferir, baixe a versão mais recente no http://www.apache.org/

Basicamente, é apenas isso que você precisa fazer para ter seu servidor Apache funcionando. Basta agora colocar os arquivos das páginas a serem disponibilizadas no diretório **/ var/ www/ html**

A maior parte da configuração do Apache pode ser feita através de um único arquivo, o **httpd.conf** , que no Mandrake pode ser encontrado no diretório **/ etc/ httpd/ conf/** . Em outras distribuições o diretório pode ser o **/ etc/ apache**

Depois de verificar a localização correta, use o comando **su** para ganhar privilégios de root e abra o arquivo: "vi /etc/httpd/conf/httdp.conf" substituindo o vi pelo seu editor favorito.

A primeira configuração importante é a (ou as) portas TCP que serão usadas pelo servidor. Por default, a porta é a 80, mas alguns serviços de banda larga, como por exemplo o Speedy da Telefonica bloqueiam esta porta, obrigando os usuários a manter seus servidores em portas alternativas. Você também pode alterar a porta para manter o seu servidor um pouco mais secreto, principalmente se for utilizada uma porta acima de 1024, já que além do endereço IP ou domínio, os visitantes precisariam saber também a porta do servidor.

A configuração da porta está perto do final do arquivos, mas linhas:

```
# BindAddress *
<IfDefine !APACHEPROXIED>
    Port 80
    Listen 80
</IfDefine>
```

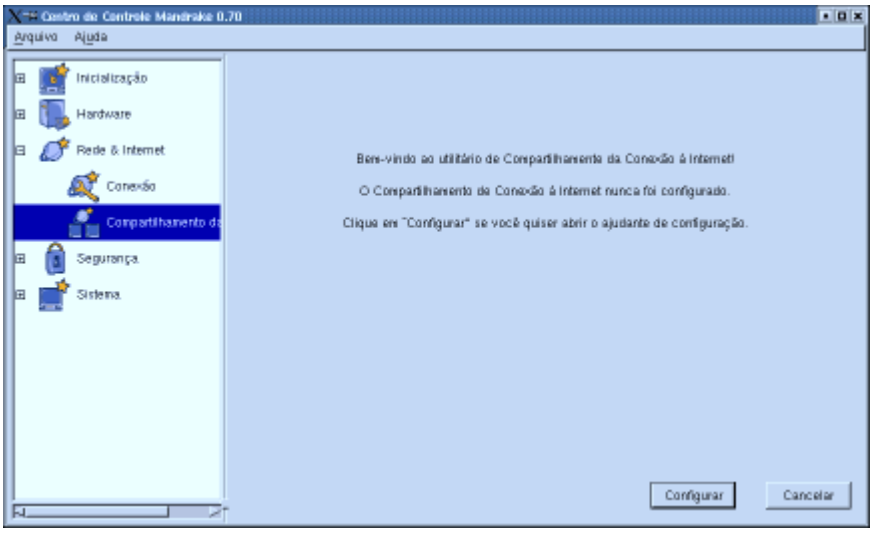
Veja que por default o Apache escuta a porta a 80. Basta alterar o 80 pela porta desejada e salvar o arquivo.

O Apache também possui uma versão for Windows, que pode ser usada em substituição ao IIS da Microsoft. Porém, devido à maneira como o Windows gerencia a geração de novos processos, e threads, o desempenho da versão Windows do Apache não é o mesmo da versão for Windows. As primeiras versões chegavam até mesmo a perder para o IIS em desempenho, mas os desenvolvedores vêm fazendo um grande esforço para melhorar seu desempenho. As versões atuais já são muito mais rápidas (embora ainda sejam mais lentas que no Linux) e possuem uma segurança muito boa. Mesmo no Windows, o Apache é uma solução muito interessante para quem quer fugir dos problemas de segurança do IIS e ao mesmo tempo procura um servidor Web rápido. Você pode baixar o Apache for Windows no http://www.apache.org/

Compartilhar a conexão

Quase todas as distribuições Linux atuais trazem utilitários para compartilhar a conexão com a Web. No Mandrake bastante acessar o Mandrake Control Center (basta digitar **mcc** num terminal) e abra a categoria Rede & Internet > Compartilhamento da Conexão.

Você verá ainda um assistente para compartilhamento da conexão. As regras são muito parecidas com as que temos no Windows. Para compartilhar uma conexão via modem, você precisará ter o modem funcionando e uma placa de rede ligada aos demais PCs. Se você tiver banda larga, precisará de duas placas de rede.



Este assistente é bastante simples de usar. Tendo um modem e uma placa de rede, ele automaticamente irá configurar a placa com o endereço 192.168.0.1, o mesmo utilizado pelo ICS do Windows, que permite até mesmo substituir uma máquina Windows por outra rodando o Mandrake sem precisar alterar as configurações das estações.

Se você desejar desativar o compartilhamento da conexão, basta rodar novamente o assistente e marcar a opção “desativar”

Se você tiver duas placas de rede, ele perguntará qual placa será usada para conectar na Internet e qual será usada para a rede local. Um detalhe importante é que se o nível de segurança do sistema (veremos a seguir) estiver configurado com a opção “Bem vindos Crackers” que deixa o sistema completamente vulnerável, a qualquer acesso externo, o Wizzard desativará a conexão. Para ativa-la, você precisará configurar o nível de segurança com no mínimo a opção “Pobre”.

O Linux é considerado um sistema bastante seguro, mas desde que você saiba configurá-lo corretamente e baixe as atualizações de segurança. Caso contrário, por ter muitos servidores disponíveis (Web, FTP, Telnet, etc.) disponíveis, que podem ser facilmente ativados, o sistema pode tornar-se muito vulnerável. Mesmo que você não pretenda tornar-se um expert em segurança. Pelo menos uma configuração cuidadosa do firewall é essencial.

Servidores em Cluster e balanceamento de carga

Hoje em dia, os servidores mais comuns são os servidores de banco de dados. Este tipo de servidor não abrange só os servidores com extensas listas de clientes ou de produtos, que servem à equipe de vendas ou de marketing de alguma empresa. Veja por exemplo os fóruns do Guiadohardware, as mensagens, assim como dados complementares, com quem postou, quando, quantas vezes foi visualizada, etc. são armazenadas num de banco de dados e o software se encarrega se organizar as mensagens por tópico, dividi-las em páginas, mostrar o número de visualizações, as respostas e assim por diante.

Cada vez mais sites organizam seu conteúdo dessa maneira, como se fosse uma espécie de fórum,

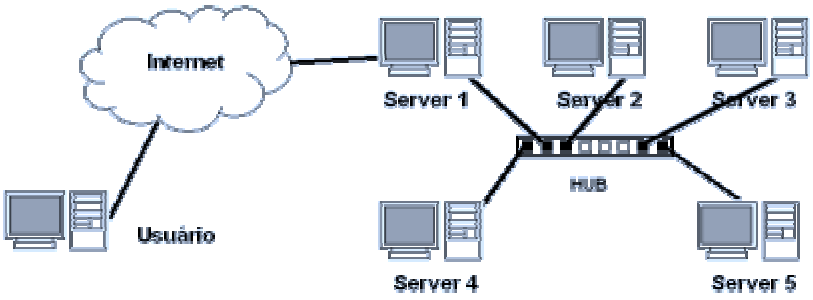
os textos, imagens, etc fazem parte de um grande banco de dados e o servidor gera as páginas conforme solicitado pelos usuários. Isso permite uma série de recursos e facilita as atualizações, mas em compensação aumenta muito o trabalho do servidor. Enquanto num site construído com páginas estáticas, em html o servidor simplesmente lê os arquivos no disco rígido e o despacha pela rede, num site baseado num banco de dados ele precisa ler vários arquivos diferentes, cruzar dados, montar a página, etc. cada vez que um visitante clica em um link.

Enquanto o site tiver pouco tráfego, digamos umas 20 ou 30 mil pageviews por dia, provavelmente um único servidor, de configuração média dará conta do recado sozinho. Mas, imagine que derrepente a audiência deste site aumentou muito, foi para 5 milhões de pageviews por dia, que é o que um grande portal costuma ter.

Provavelmente, um único servidor, mesmo que tenha 2 ou 4 processadores, não vai dar conta de todo este tráfego.

Um cluster nada mais é do que um grupo de servidores, ligados em rede, que graças a um software qualquer, dividem entre sí as tarefas necessárias para desempenhar uma tarefa qualquer, ou seja, vários servidores que trabalham como se fossem um só.

Já que o nosso primeiro servidor não está dando conta da tarefa de servir as 5 milhões de páginas diariamente, podemos montar um cluster, com por exemplo, mais 4 servidores. Agora temos 5 no total, ligados através de uma rede Ethernet de 100 megabits (ou uma rede gigabit Ethernet, dependendo do tráfego). O link com a Internet está no servidor 1, enquanto os outros estão ligados a ele através de uma rede local, como na ilustração abaixo:



Veja de qualquer modo, todos os dados continuarão passando pelo server 1, pois é ele quem possui o link com a Web, mas o grande problema aqui não é a simples transmissão dos dados, pois mesmo que fosse um link de 40 megabits, qualquer HD razoavelmente rápido poderia dar conta do recado. O grande problema é processar os pedidos e montar as páginas. É para isso que os servidores 2, 3, 4 e 5 estão aqui.

Entraria em cena então a idéia de balanceamento de carga, onde os servidores dividiriam entre sí os pedidos. Cada um cuidaria de parte das requisições e enviaria as páginas prontas para o server 1, que por sua vez as enviaria para o usuário.

A idéia já está pronta, faltaria agora coloca-la em prática. Além dos servidores, precisaríamos de um programa que possa gerenciar tudo isso. Existem várias opções. A versão Enterprise do Cold Fusion por exemplo vem com um software de balanceamento de carga, o ClusterCATS. Se a idéia é usar um software GNU, então uma boa opção seria o Linux Virtual server, que pode ser baixado

em: http://www.linuxvirtualserver.org/

Como o software de balanceamento rodaria no servidor 1, os demais servidores poderiam rodar qualquer outro sistema, Win 2k Server, Linux, Solaris, o que preferisse.

Todos os servidores manteriam uma cópia integral de todos os dados do site, já que de qualquer forma cada servidor precisará de todos os dados para atender as requisições que chegarem até ele. Isto já é um tipo de espelhamento. Caso algum dos servidores precise ser desligado, seja por alguma falha, ou então para algum tipo de manutenção, os outros três continuariam trabalhando normalmente. O Virtual Linux Server por exemplo tem a capacidade de detectar a desconexão automaticamente e passar a enviar tarefas apenas para os outros três. Ou seja, o site continuaria no ar mesmo que três dos servidores entrassem em pane, embora com a performance comprometida.

Depois de terminada a manutenção, o Virtual Linux Server se encarregaria de atualizar os dados para que os servidores parados pudessem voltar a trabalhar.

Existem claro, vários outros programas que podem ser usados para criar mirror de um servidor, que passam a ser automaticamente atualizados. Você poderia usar um software assim para criar um mirror do server 1, para substituí-lo quando fosse necessário fazer algum tipo de manutenção, por exemplo. Um software relativamente popular para isso é o Sure-Sync (Windows), que pode ser encontrado em: http://www.softwarepursuits.com/suresync/mirror.htm

Economizando com o uso de terminais leves

Hoje em dia é possível comprar placas de rede 10/100 por menos de 30 reais e, com o barateamento dos novos padrões, estes preços não voltarão a subir. Com as redes tão baratas, aplicações que estavam fora de moda, como os terminais diskless, terminais gráficos, etc. voltaram a ser atrativas.

Os PCs continuam relativamente caros, mas a banda de rede está muito barata. Com isto, começa a fazer sentido aproveitar PCs antigos, transformando-os em terminais de PCs mais rápidos. Com uma rede bem planejada, um único Pentium III ou Duron pode servir 5, 10 ou até mesmo 20 terminais 486 e com um desempenho muito bom, já que os aplicativos rodam no servidor, não nos terminais.

A grande vantagem é a economia de custos. Para montar um laboratório com 10 PCs novos, ligados em rede, você gastaria pelo menos 16.000 reais, fora a mão de obra. Usando um servidor e 10 terminais 486 você gastaria menos de 4500 reais (fora mão de obra), presumindo que comprasse cada 486 por R$ 200. O desempenho nos terminais porém não será o de um 486, mas sim o de um Pentium III ou Duron. Esta solução é muito útil também em "ambientes hostis", como terminais de acesso público, já que um 486 custa muito menos para ser substituído do que um PC novo. Você também pode incluir mais terminais caso necessário a um preço muito baixo.

Todas as soluções que apresentarei a seguir são baseadas no Linux. A Microsoft oferece uma solução para terminais, chamada Windows Terminal Server. A eficiência também é boa, mas é inviável por causa do custo do software, já que além da licença do servidor, é preciso pagar por mais uma licença para cada terminal. No final, os custos do sistema da Microsoft são parecidos

com os de simplesmente trocar todos os micros. Não é à toa que esta solução é tão pouco usada...

Existem quatro formas de rodar aplicativos remotamente:

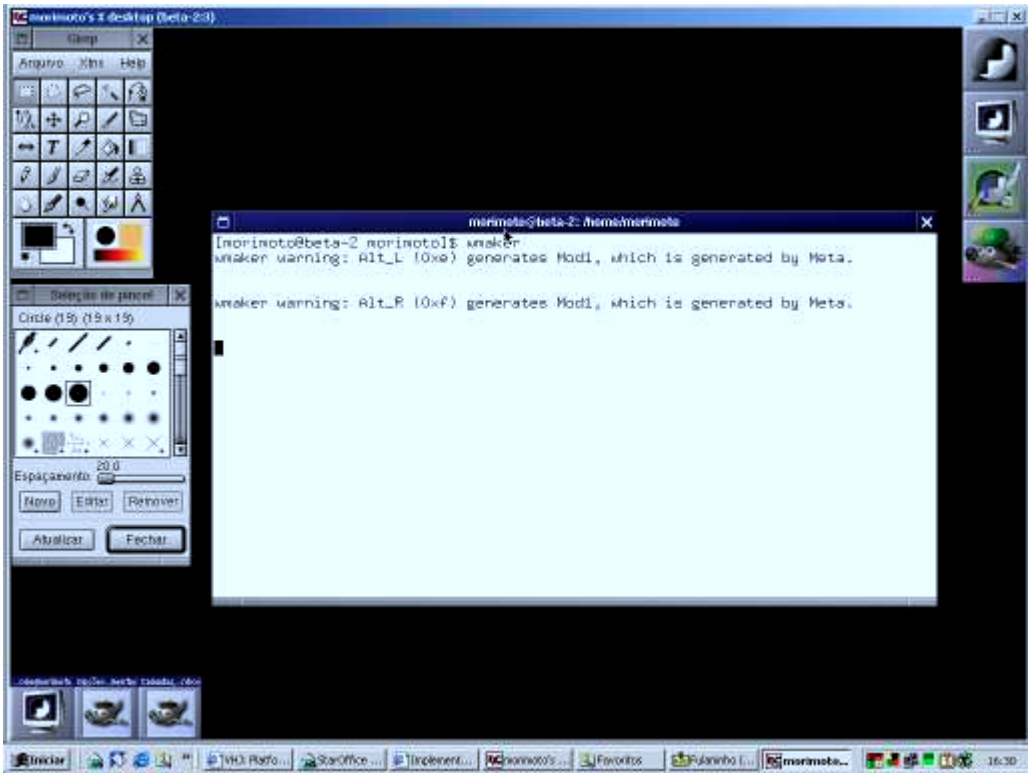
1- Via VNC, numa estação com o Windows ou Linux instalado

2- Rodando aplicativos via SSH ou Telnet, numa estação com Linux ou Windows

3- Rodando toda a interface gráfica apartir do servidor, numa estação com Linux

4- Usando o Etherboot para criar estações diskless, que baixam todo o software apartir do servidor.

O VNC é interessante para máquinas que rodam Windows, pois permite misturar programas das duas plataformas. Mas, em compensação, ele também é mais pesado, tanto para o cliente quanto para o servidor, e consome mais banda da rede. Com uma rede de 10 megabits e um 233 MMX você já poderá usa-lo confortavelmente, mas para ter realmente a mesma velocidade de atualização de tela que teria sentado na frente do servidor, você precisaria de uma rede de 100 megabits.



VNC em ação

Outra solução é usar o SSH ou Telnet para rodar aplicativos remotamente. Se o cliente rodar Windows é possível apenas rodar aplicativos de modo texto, mas se o cliente também rodar Linux é possível rodar também qualquer aplicativo gráfico instalado no servidor. A vantagem neste caso é que você pode misturar aplicativos locais e remotos. Esta é a solução ideal caso você tenha estações Linux com uma configuração razoavelmente atual.

Via SSH também é possível carregar toda a interface gráfica apartir do servidor e rodar todos os programas a partir dele. Este seria o próximo nível, que poderia ser usado se você tiver um monte de terminais 486 com 12 ou 16 MB de RAM, mas com pelo menos 200 ou 300 MB de espaço em disco para uma instalação mínima do Linux. Neste caso é possível configurar as estações para abrir diretamente na tela de Login do servidor, dispensando o uso do SSH, como veremos mais adiante.

Finalmente, se as estações não tiverem sequer HD, você pode configurá-las para dar boot através da rede, usando um disquete ou a ROM da placa de rede. Neste caso elas baixarão todo o software apartir do servidor. Esta é a solução mais trabalhosa e a menos flexível, mas a que exige menos hardware nas estações.

Falando assim, até parece que o assunto é complicado, mas tenha em mente que não é. Se você tentar colocar estas idéias na prática, vai ver como é algo bastante simples. Vou começar com o VNC que tem a configuração mais simples (e que já expliquei numa matéria anterior) para manter um nível gradual de dificuldade.

Vamos então aos detalhes:

Montando a rede

Numa rede "normal" teríamos apenas uma placa de rede em cada micro, uma no servidor e um hub interligando todos. Mas, isto não serviria muito bem no nosso caso, pois ao utilizar um hub apenas uma estação pode transmitir de cada vez. Isto funcionaria bem caso você tivesse apenas dois, três, ou talvez quatro terminais, acima disto você começará a notar perda de desempenho pelo congestionamento da rede. Esta medida pode variar de acordo com a intensidade do uso naturalmente, a ponto de com 6 ou 8 micros você conseguir um desempenho satisfatório, mas não é a melhor solução.

Trocar um Hub por um switch aumentaria nossos custos em 300 ou 400 reais e não resolveria o problema. Um switch permite que várias estações transmitam dados ao mesmo tempo, mas desde que não para o mesmo destinatário. Como no nosso caso quase tudo parte do servidor, o switch apenas evitaria as colisões de pacotes, mas não resolveria o problema da banda. O custo é relativamente grande, para um ganho de desempenho pequeno.

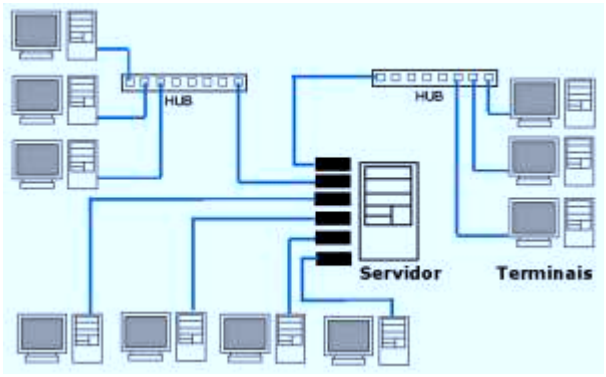
A melhor solução, e bem mais barata que usar um switch, seria combinar várias placas de rede no servidor e, caso necessário, alguns hubs.

A vantagem é óbvia. Com apenas uma placa de rede, os 10 ou 100 megabits são divididos entre todas as estações. Adicionando mais placas, temos 10 ou 100 megabits para cada placa, que será compartilhada por um número menor de estações. O único limite para o número de placas de rede que você pode ter no servidor é o número de slots PCI livres.

Isto também é vantajoso do ponto de vista do custo. Uma placa de rede popular custa hoje entre 25 e 30 reais por unidade. Um hub de 10 megabits, de 8 portas custa de 50 a 70 reais, enquanto um de 100 megabits custa apartir de 100 reais. Um switch por sua vez não sai por menos de 300 ou 400 reais.

Ou seja, com o dinheiro de um switch podemos comprar um batalhão de placas de rede e hubs, que combinados oferecerão um desempenho muito melhor.

Pois bem, se você tiver até 6 terminais, o melhor negócio será simplesmente dispensar o hub e usar uma placa de rede para cada terminal (presumindo que existam slots PCI suficientes). Se o número de terminais for maior que o número de slots disponíveis, então o ideal será usar o máximo de placas de rede possível e usar um ou mais hubs para conectar todos os terminais, sempre procurando manter o menor número possível de terminais por hub. Se você tiver 10 terminais, puder colocar 6 placas de rede no servidor e tiver dinheiro para comprar mais 2 hubs, o ideal seria ligar 4 terminais diretamente ao servidor e pendurar mais 3 terminais em cada hub. Veja um esquema de ficaria a rede neste exemplo:



Lembre-se que apenas as placas de rede PCI são 10/100, todas as placas de rede ISA são de 10 megabits. Ao misturar placas de 10 e 100 no mesmo hub, todas passarão a trabalhar a apenas 10 megabits, para manter compatibilidade com as mais lentas.

Se você for misturar estações com placas Ide 10 e 100 megabits, prefira ligar as estações com placas de 10 diretamente ao servidor e distribuir as com placas 10/100 entre os Hubs (que também devem ser de 100 megabits). É mais fácil dividir 100 megabits entre 4 ou 5 estações do que dividir 10 megabits.

Configuração do servidor

Além da penca de placas de rede, o servidor precisa ter uma configuração razoável, já que vai rodar vários aplicativos diferentes e ao mesmo tempo.

O mínimo recomendável para um bom desempenho seria um Pentium III, Celeron ou Duron de 600 MHz, 128 MB de RAM e mais 32 MB para cada cliente, além de um HD razoavelmente rápido e uma placa mãe com 6 slots PCI, de preferencia com uma placa de vídeo AGP (ou onboard) para não ocupar nenhum dos slots PCI. Claro que um processador mais rápido seria muito bem vindo. Não deixe também de monitorar o uso de memória RAM no servidor e fazer um upgrade sempre que necessário.

A placa de vídeo pode ser qualquer uma suportada pelo Linux, embora segundo o Wooky, usar uma GeForce 2 com os drivers oficiais da Nvidia permite que você execute aplicativos 3D

(inclusive jogos) nas estações com aceleração 3D, feita pelo servidor. Os jogos 3D não seriam muito interessantes, já que a velocidade de atualização da tela não é suficiente para mais do que dois ou três FPS em tela cheia, mas é uma mão na roda se você pretender rodar algum aplicativo gráfico com suporte a OpenGL.

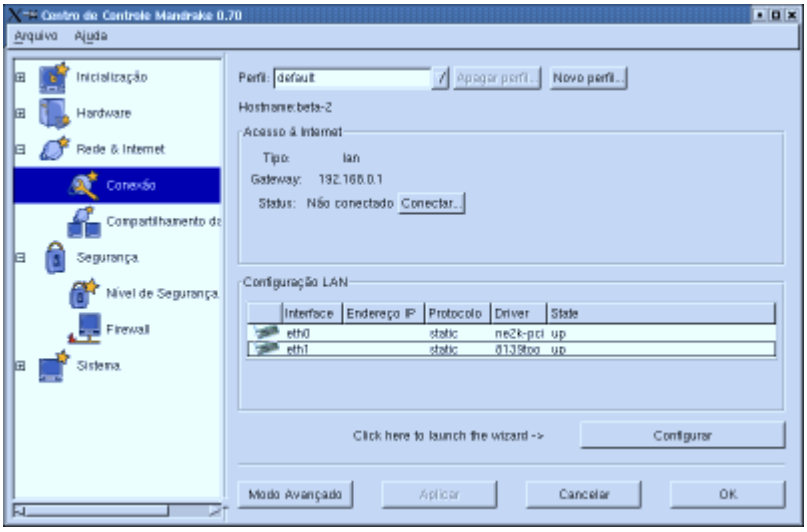
O HD também deve ter espaço suficiente para guardar todos os arquivos pessoais dos usuários. O servidor também não vai precisar de um monitor, pois depois de configurado você poderá acessar as configurações a partir de qualquer terminal. Nada impede entretanto que você use o próprio servidor como mais um terminal, já que com o usuário logado no sistema como um usuário normal (jamais deixe que utilizem a conta root neste caso) terá pouca chance de fazer barbeiragens no sistema.

Depois de planejar a rede e montar o servidor, falta montar a rede e instalar o Linux no servidor. Você pode tirar as suas dúvidas sobre cabeamento aqui:
http://www.guiadohardware.net/tutoriais/sharing/

Você pode utilizar qualquer distribuição Linux mas, se você é iniciante, eu recomendo o Mandrake 8.1, que é atualmente o mais simples de configurar. Você vai encontrar instruções detalhadas de como instalar e configurar o sistema no:
http://www.guiadohardware.net/tutoriais/entendendo_e_utilizando_o_linux/

Com o sistema instalado, você ainda precisará configurar as placas de rede. A forma menos problemática de fazer isso é instalar o sistema com apenas uma placa e adicionar mais uma placa a cada reinicializarão. O Kudzu detectará as novas placas a cada boot, terminado você ainda precisará configurar os endereços IP de cada uma.

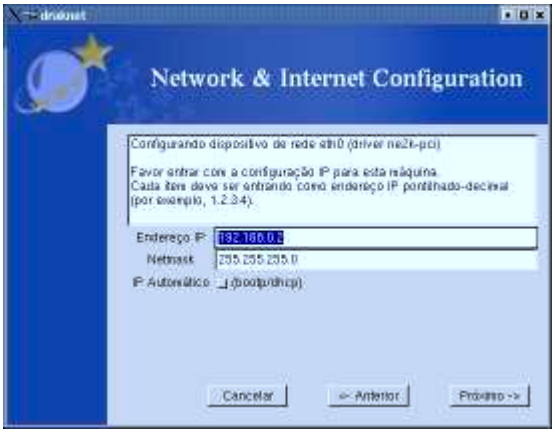
No Mandrake você pode fazer isso através do Mandrake Control Center > Rede & Internet > Conexão. Você verá uma lista com todas as placas de rede instaladas no sistema. Clique em "Configurar" para abrir o Wizzard que permitirá que especifique o endereço IP a ser usado por cada uma.



Naturalmente, cada placa de rede deverá ter um endereço diferente. Você pode utilizar tanto a faixa de endereços 192.168.0.x (que permite o uso de até 254 hosts) com máscara de sub-rede

255.255.255.0 quanto a faixa 10.x.x.x. com máscara de sub-rede 255.0.0.0, que permite um número quase ilimitado de endereços.

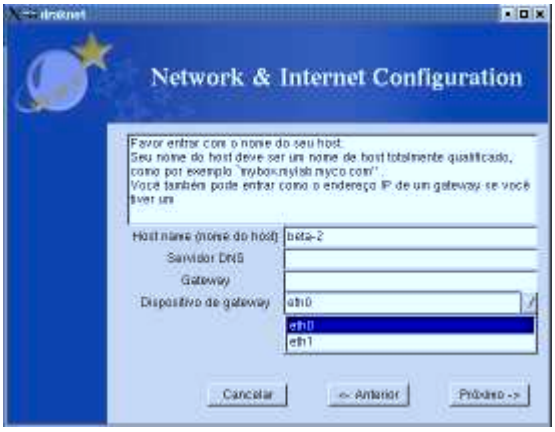
Os endereços podem ser por exemplo 10.0.0.1, 10.0.0.2, 10.0.0.3, etc. Lembre-se que se uma placas placas de rede estiver sendo usada para conectar à Internet (ADSL, cabo...) ela deverá ser configurada com o endereço fornecido pelo provedor, ou com a opção "bootop/DHCP", não com o endereço de rede local.



A configuração poderia ficar assim:

Placa 1 (**eth0**): Conexão com a Internet via Speedy, IP: 200.223.201.56, máscara de sub-rede 255.255.255.0.
Placa 2 (**eth1**): Rede local, IP: 10.0.0.1
Placa 3 (**eth2**): Rede local, IP: 10.0.0.2
Placa 4 (**eth3**): Rede local, IP: 10.0.0.3
Placa 5 (**eth4**): Rede local, IP: 10.0.0.4
Placa 6 (**eth5**): Rede local, IP: 10.0.0.5

Na etapa final você deverá especificar o nome do host, o servidor DNS e o Gateway para acesso à Web e qual das placas de rede está conectada ao Gateway. No nosso exemplo seria a eth0.

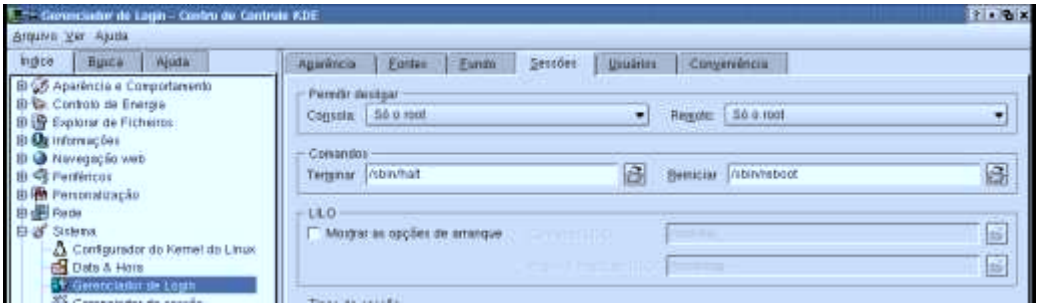


Se você tiver uma conexão via ADSL ou cabo, os dois campos deverão ser preenchidos com os dados fornecidos pelo provedor e o dispositivo de gateway será a placa de rede conectada ao ADSL/Cable Modem. Se o servidor está acessando através de uma conexão compartilhada por outra máquina, os dois campos devem ser preenchidos com o endereço IP do servidor de conexão (192.168.0.1 se for uma máquina Windows compartilhando a conexão através do ICS).

Logo abaixo você verá o utilitário para compartilhar a conexão com a Internet, mas no nosso caso ele não é necessário, pois o único que acessará a Web será o servidor. Os terminais apenas mostram a janela do Browser, montada por ele.

Estas instruções se aplicam ao Mandrake e ao Techlinux. Se você estiver usando o Conectiva ou o Red Hat você deverá fazer a configuração através do Linuxconf.

Como o servidor será acessado por vários usuários, outro detalhe importante é estabelecer que apenas o root poderá reiniciar o sistema. Para isso, abra o Kcontrol com permissões de root (**kdesu kcontrol** num terminal) e acesse a seção Sistema > Gerenciador de login > Sessões



Esta é a configuração básica do servidor. Daqui pra frente, as configurações necessárias variam de acordo com o meio de acesso escolhido.

Terminais via VNC

O VNC é na verdade um programa de administração remota, mas que, rodando num servidor Linux, também desempenho bem a função de servidor de terminal. A vantagem é que ele roda em praticamente qualquer sistema operacional, incluindo naturalmente Windows e Linux. Ele é a melhor opção para usar programas Linux junto com o Windows.

O problema com o VNC é que ele transmite os dados da tela na forma de imagens, incluindo o texto das janelas. Isto é bem menos eficiente que o protocolo do Xfree, utilizado pelas opções a seguir, onde são transferidas instruções para criar as janelas, junto com seu conteúdo. Além do tráfego de dados via VNC ser maior, a utilização de processador, tanto no servidor quanto nas estações é bem maior. O VNC é recomendável apenas para estações com processadores Pentium 133 ou mais rápidos.

Se você chegou a utilizar o VNC no Windows, provavelmente ficou decepcionado com a velocidade de atualização da tela e com a possibilidade de abrir um único terminal, que mostra a mesma área de trabalho que quem estiver na frente do micro verá. Não é à toa que a versão Windows do VNC é geralmente apresentada como uma simples ferramenta de administração remota. Realmente

não serve para muita coisa além disso. Para detalhes de como utilizar o VNC no Windows leia: http://www.guiadohardware.net/artigos/156-administracao_remota.asp

No Linux as coisas são um pouco diferentes. Graças à forma como o X gerencia os dados a serem mostrados no vídeo, o VNC torna-se muito mais rápido e eficiente e ganha o suporte a múltiplos terminais. Basta lembrar que o X foi originalmente desenvolvido justamente para esta função, possibilitar o uso de um terminal gráfico Unix em computadores com pouco poder de processamento, isso ainda na década de 70.

Usando uma rede de 10 megabits é possível usar uma máquina Linux remotamente com quase a mesma qualidade que teria sentado na frente dela e com uma rede de 100 megabits é quase impossível notar diferença, com o detalhe de que o cliente VNC roda numa janela do Windows (também é possível usa-lo em tela cheia), o que permite que você use a máquina Linux ao mesmo tempo que roda outros programas. Melhor ainda, como o cliente apenas mostra a imagem da tela, você pode abrir vários aplicativos na máquina Linux, sem que a máquina Windows fique lenta. Obviamente, para isso você precisará ter uma máquina Linux configurada ligada em rede com a máquina Windows.

Isto tem duas utilidades. A primeira é claro a possibilidade de ter uma workstation Linux dentro do Windows e rodar ao mesmo tempo seus aplicativos preferidos das duas plataformas. Rodar o servidor VNC não impede que alguém utilize a máquina Linux normalmente.

Instalar o VNCserver no servidor Linux é razoavelmente simples. Comece baixando o programa aqui:
http://www.downloads-guiadohardware.net/download/vnc-3.3.3r2_x86_linux_2.0.zip

Descompacte o arquivo e copie os arquivos:

vncpasswd
vncserver
Vncviewer
vncviewer
Xvnc

... de dentro da pasta que será criada para o diretório "**/usr/local/bin**" (você precisa de permissões de root para isso, use o comando "kdesu konqueror" para abrir o gerenciador de arquivos com privilégios de root)

Se quiser habilitar o recurso de acesso via browser, crie o diretório "**vnc**" dentro da pasta "**/usr/local**" e copie a pasta **classes** para dentro da pasta (o caminho ficará "/usr/local/vnc/classes").

Feito isso, abra o arquivo "**vncserver**" que foi copiado e altere as linhas:

```
$geometry = "1024x768";
$depth = 8;
```

.. para a resolução e quantidade de cores que deseja usar. A resolução pode ser qualquer uma, não necessariamente uma das resoluções padrão. Se for maior que a resolução de vídeo do cliente, a janela ocupará apenas parte da tela e se for maior aparecerão barras de rolagem.

Se você quiser usar a janela do VNC junto com a barra de tarefas do Windows, como no screenshot que coloquei no início do tutorial, você deve usar uma resolução um pouco menor que a padrão. No meu caso por exemplo o cliente usa 1024x768 então usei:

```
$geometry = "1014x710";
$depth = 16;
```

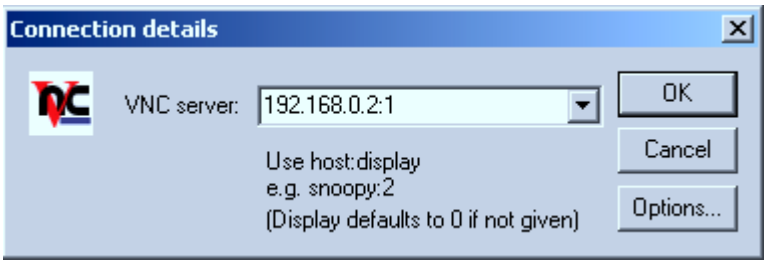
Como pode notar, aproveitei para aumentar também a resolução de cores, de 8 para 16 bits. Naturalmente, ao usar 16 bits de cor a velocidade de atualização da tela cairá um pouco, mas a diferença não chega a ser muito grande, graças ao bom trabalho de compactação que o VNC faz.

É importante iniciar o VNC com a mesma profundidade de cores usada no servidor, caso contrário as cores ficarão alteradas. Não é necessário que a estação use a mesma profundidade de cores que o servidor, pois o VNC se encarrega de fazer a conversão, neste caso sem alterar as cores.

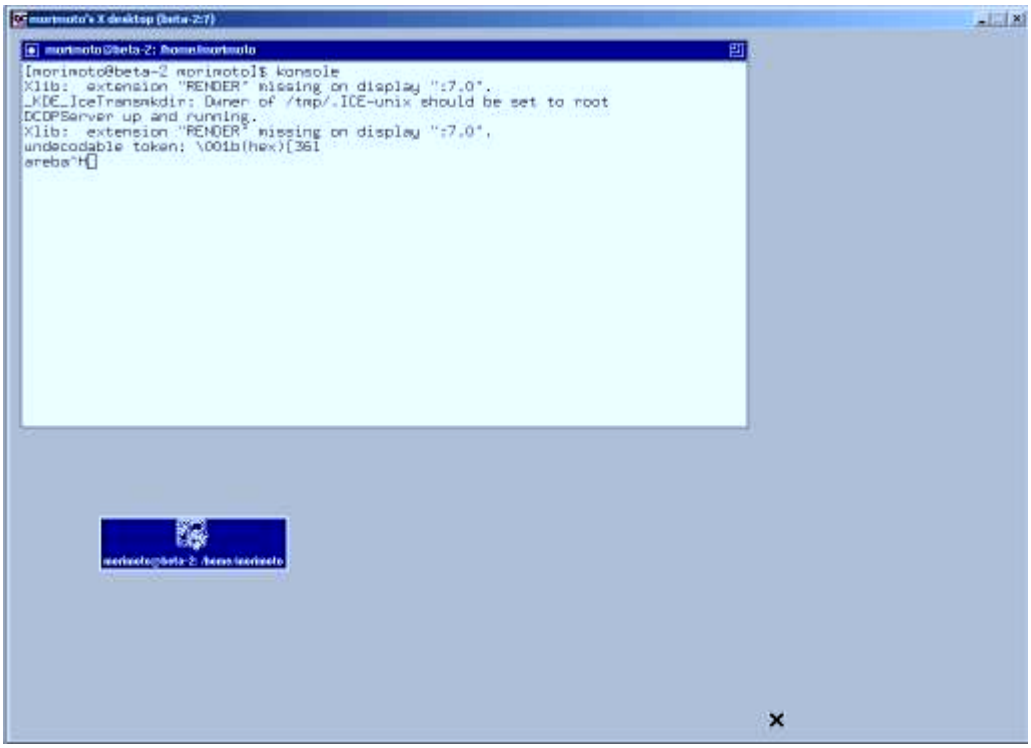
Depois de salvar o arquivo, abra um terminal e use o comando "**vncserver**" para iniciar o VNC. Da primeira vez que for executado, o programa pedirá que você defina uma senha de acesso. Pode ser qualquer coisa com 6 caracteres ou mais. A senha naturalmente serve para impedir que qualquer um possa se conectar à sua máquina, sem autorização.

Para acessar o servidor, baixe o VNC for Windows no Link abaixo:
http://www.downloads-guiadohardware.net/download/vnc-3.3.3r9_x86_win32.zip
Você pode baixar versões para outros sistemas operacionais (inclusive Windows CE e Palm) em:
http://www.uk.research.att.com/vnc/

Basta descompactar o arquivo e executar o **vncviewer.exe**. Forneça o endereço IP do servidor, seguido por um "**:**" e o número do terminal (ou display). Cada vez que você executa o vncserver no servidor será criado um terminal virtual diferente. O primeiro terminal recebe o número 1, o segundo 2, e assim por diante. É possível criar um número teoricamente ilimitado de terminais na mesma máquina Linux e cada um permite a conexão de um cliente diferente, respeitando naturalmente as limitações de velocidade do servidor e principalmente da rede. Para chamar o cliente VNC no Linux basta usar o comando "**vncviewer**" num terminal.



Da primeira vez que se conectar ao servidor você terá uma surpresa desagradável. O gerenciador de janelas default do VNC é o TWM, um gerenciador antigo e com poucos recursos:



Para mudar isso, abra o diretório **.vnc**, que será criado dentro do seu diretório de usuário (/home/nome_do_usuario/.vnc) da primeira vez que rodar o vncserver e edite o arquivo "**xtartup**". Lembre-se que todos os diretórios cujo nome começa com "." são ocultos, não se esqueça de marcar a opção "mostrar todos os arquivos" no gerenciador de arquivos.

Basta substituir o "**twm**" na última linha pelo nome da interface gráfica que gostaria de utilizar. A minha preferida nesse caso é o "**blackbox**", que por ser leve e não utilizar imagens nem ícones nos menus é a que oferece um melhor desempenho via rede, ao mesmo tempo em que permite abrir muitos terminais, sem acabar com a memória RAM do servidor. Na falta do blackbox você pode usar qualquer outra interface que tenha instalada.

O arquivo ficará assim:

 # !/ bin/ sh

xrdb $HOME/ .Xresources
xsetroot -solid grey
xterm -geometry 80+24+10+10 -ls -title "$VNCDESKTOP Desktop" &
blackbox &

Como disse, você pode utilizar qualquer interface gráfica que tenha instalada na máquina, bastando substituir o "blackbox" pelo comando adequado. Alguns exemplos são:

startkde : para abrir o KDE (em algumas distribuições o comando é apenas kde)
gnome-session : usar o Gnome
afterstep : usar o afterstep
wmaker : Window Maker

E assim por diante.

Para que a alteração surta efeito, feche o terminal virtual que havia sido criado com o comando **vncserver -kill :1** e chame novamente o **vncserver**. O mesmo comando pode ser usado sempre que você desejar fechar os terminais virtuais criados.

Você pode inclusive criar vários terminais com diferentes resoluções e diferentes interfaces gráficas. Para isso, basta alterar a resolução de tela no **/usr/local/bin/vncserver**, alterar a interface gráfica no **xstartup** e digitar novamente o comando vncserver depois de cada alteração.

Uma opção mais prática para abrir vários terminais com resoluções e profundidade de cores diferentes é usar o comando vncserver com os parâmetros "**-depth**" e "**-geometry**" como em:

vncserver -depth 16 -geometry 1014x710

É um pouco longo, mas muito mais prático que editar os dois arquivos de configuração a cada mudança. Assim você poderá ter o terminal 1 com 1024x768 e KDE, o terminal 2 com 800x600 e BlackBox e assim por diante.

Rodar aplicativos a partir do servidor

Se os terminais rodarem Linux, não faz sentido usar o VNC, já que o próprio Xfree possui recursos mais eficientes para rodar aplicativos remotamente. Com poucos comandos você pode abrir qualquer aplicativo instalado no servidor, ou mesmo abrir toda a interface gráfica. Para isto, basta contatar o servidor usando o SSH ou Telnet.

Antes de mais nada, você precisa configurar o cliente para aceitar as conexões, o que é feito através do comando "xhost endereço_IP_do_servidor". Se por exemplo o servidor usa o endereço 10.0.01 e a estação usa o 10.0.0.12, o comando ficaria assim:

xhost 10.0.0.1

Se não estiver preocupado com a segurança, você pode usar o comando "**xhost +**" para aceitar conexões de qualquer PC.

Depois, acesse o servidor via Telnet, com o comando "**telnet 192.168.0.1**" (logo a seguir veremos as vantagens de fazer o mesmo via SSH, mas uma coisa de cada vez).

Depois de fazer o login, use o comando:

aplicativo -display 192.168.0.2:0.0 &

Como por exemplo:
konqueror -display 192.168.0.2:0.0 &

Além de ser usado nos terminais, este recurso também pode ser utilizado sempre que você precisar de um aplicativo que não está instalado na sua máquina de trabalho, mas existe em

alguma outra máquina da rede.

Para não precisar escrever toda vez o "aplicativo -display 192.168.0.74:0.0" você pode criar aliases, editando o arquivo **.bashrc** encontrado dentro do diretório do usuário usado (ex: /home/morimoto/.bashrc).

Adicione linhas como:
alias konqueror486="konqueror -display 192.168.0.72:0.0 &"

Veja as propriedades dos atalhos do KDE para ver os comandos para inicializar cada aplicativo via linha de comando.

Rodando aplicativos via SSH

O SSH é uma espécie de versão evoluída do Telnet, que também permite executar arquivos remotamente, mas com várias vantagens.

Assim como no Telnet, uma máquina com o serviço habilitado pode ser acessada via linha de comando por usuários que tenham o login e senha de uma das contas do sistema. O SSH permite ter acesso completo ao sistema via terminal, seja via rede ou via Internet, limitado aos privilégios do login usado.

O **sshd** é o módulo servidor (que deve ser ativado na seção "Serviços" do Mandrake Control Center, ou no **ntsysv**, que pode ser aberto pelo terminal, com permissões de root), enquanto o **ssh** é o módulo cliente, incluído em praticamente todas as distribuições Linux, mesmo as relativamente antigas.

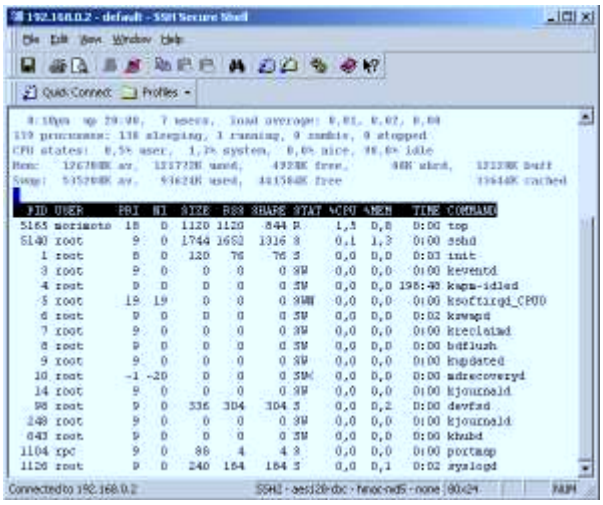
Para usar, basta usar o comando "ssh -l login nome_ou_IP_da_maquina", como em "**ssh -l morimoto 10.0.0.1**" ou "**ssh -l morimoto beta-2**" para abrir o terminal do usuário morimoto no host beta-2.

O SSH inclui muitas opções de segurança, não deixe de ler a documentação disponível no:
http://www.openssh.com

A segurança é justamente a principal vantagem sobre o antigo Telnet, onde os dados, incluindo senhas trafegam na forma de texto pela rede ou pela Internet, uma carta aberta para quem desejar ler. O SSH por sua vez pode ser praticamente indecifrável se bem configurado.

Existem diversas versões do SSH e o Mandrake (assim como outras distribuições Linux) inclui o OpenSSH, que não possui um cliente for Windows. A solução nesse caso é usar a versão da SSH Security, que tem vários recursos mas é gratuita apenas para universidades e usuários domésticos. O link é: http://www.ssh.com

O SSH da SSH Security e o OpenSSH são totalmente intercompatíveis, permitindo que você acesse um servidor Linux através de uma máquina Windows, como no caso do Telnet.



Cliente SSH for Windows

Além de oferecer acesso via linha de comando, o SSH permite rodar aplicativos gráficos remotamente, da mesma forma que expliquei no tópico anterior, mas com bem mais praticidade.

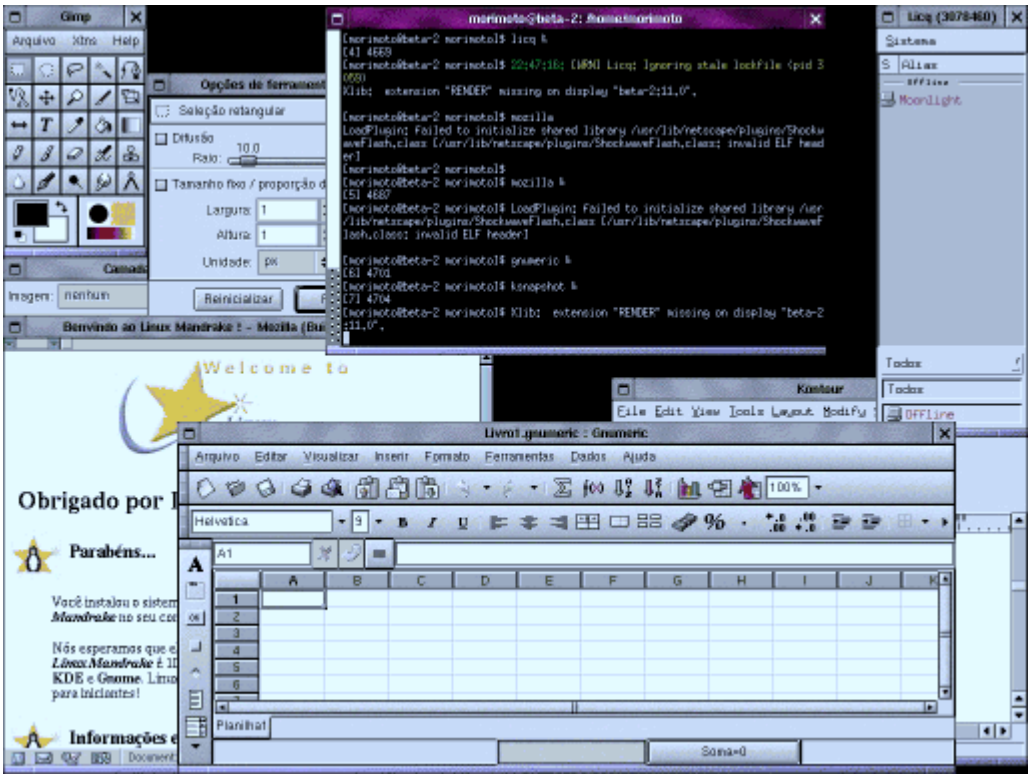
Abra uma janela de terminal e acesse a máquina Linux que está com o servidor SSH habilitado com o "**ssh -l login endereço_do_servidor**" e forneça a senha de acesso. Uma logado, o seu terminal mostra na verdade o terminal do servidor. Mas, se você inicializar qualquer aplicativo gráfico. Dando um "konqueror" por exemplo, o aplicativo não será inicializado no servidor, mas sim na sua máquina. É o mesmo efeito do comando que citei no tópico anterior, mas você não precisou usar o comando longo.

Outra vantagem é que inicializando os aplicativos desta forma todos rodarão, ao contrário do comando longo, que não funciona com todos os aplicativos.

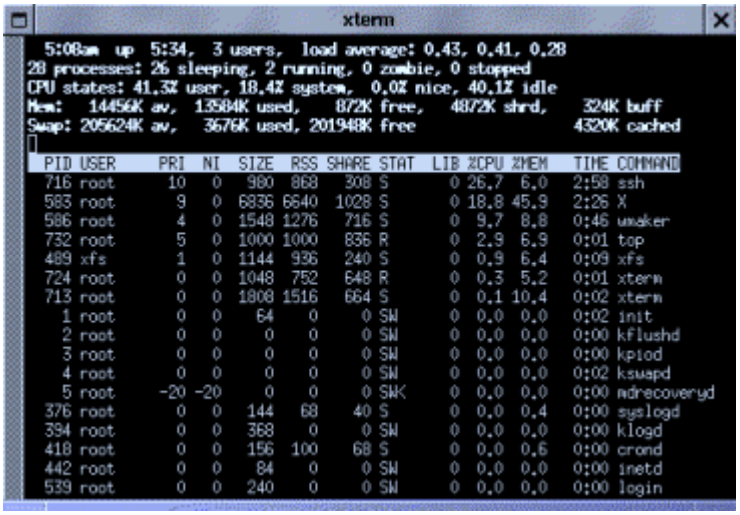
Note que este recurso só funciona nos clientes Linux, o cliente Windows está limitado ao modo texto. Talvez algum dia alguém consiga desenvolver um servidor X para que o Windows também possa rodar os aplicativos gráficos, mas até lá esta é mais uma exclusividade do Linux.

Você pode usar o SSH até mesmo via Internet. Uma conexão via modem vai ser suficiente para trabalhar no modo texto, mas a coisa complica se você quiser rodar aplicativos gráficos. Com uma conexão via cabo ou ADSL eles já ficam usáveis, mas o ideal é uma rede local, onde os aplicativos rodam com o mesmo, desempenho com que rodam no servidor e com uma velocidade de atualização de tela também muito semelhante.

Veja o caso do screenshot abaixo por exemplo. Através do terminal SSH abri vários aplicativos, como o Gnumeric, Gim, Licq, Mozzila, Kontour, etc. todos rodando com um desempenho muito bom, apesar da amontoeira na tela:



O detalhe é que este screenshot foi tirado naquele 486 com 16 MB de memória. Como todos os programas rodam apartir do servidor, eles consomem memória e recursos do servidor. Segundo o top, o 486 estava usando apenas 17 MB de memória, incluindo memória física e swap:



Você pode até mesmo rodar o gerenciador de janelas a partir do servidor. Para isto, inicie a interface gráfica usando o "**xinit**" ao invés do "**startx**". Isto abrirá o servidor X "puro", sem gerenciador de janelas algum. Use o terminal para abrir a conexão via SSH e em seguida chame o gerenciador de janelas desejado com os comandos "**startkde**", "**wmaker**", "**gnome-session**", "**blackbox**" etc. Isto também funciona pelo comando longo como "blackbox -display

192.168.0.4", que também pode ser usado via Telnet.

Apesar de ser um pouco mais lento do que rodar apenas os aplicativos (já que o tráfego de dados na rede será maior) este recurso torna possível rodar o KDE ou o Gnome nos terminais 486, que provavelmente serão muito mais familiares aos usuários vindos do Windows do que o Window Maker ou o Blackbox.

Você pode configurar várias opções relacionadas ao servidor SSH, incluindo a porta TCP a ser usada editando o arquivo **/ etc/ ssh/ sshd_config**.

Rodar a interface gráfica e todos os programas a partir do servidor

Se você tiver um monte de terminais 486 em mãos e não pretender rodar aplicativos locais, a melhor opção é configurar as estações para automaticamente carregar a janela de login do servidor durante o boot. Logo ao ligar a máquina você verá a tela de login, como veria no servidor, onde poderá escolher qual conta de usuário e qual interface gráfica utilizar. Apesar disso, ainda é possível rodar aplicativos de modo texto locais pressionando Crtl + Alt + F2 (F3, F4, F5, F6).

Para isto, você precisará ter pelo menos 200 MB de espaço livre em disco em cada estação e pelo menos 12 MB de memória. É possível instalar com 8 ou até mesmo 4 MB, mas o desempenho ficará comprometido. Não seja mão de vaca, um pente de 8 MB de memória FPM não custa mais de 20 reais...

Como vamos rodar tanto a interface gráfica quanto todos os aplicativos a partir do servidor, você só precisará instalar os pacotes básicos da distribuição escolhida e o Xfree. Nos meus 486 eu costumo utilizar o Conectiva 4, que apesar de estar bem desatualizado é bem flexível para este tipo de instalação mínima. Você claro, pode utilizar sua distribuição favorita. Eu cheguei até a instalar o Red Hat 7.2 num destes 486 (http://www.guiadohardware.net/artigos/190-rh72.asp) mas em termos de desempenho esta é uma péssima idéia, é muito complicado fazer uma instalação reduzida com ele. O Mandrake sequer instala em micros 486, enquanto o SuSE 7 é um pouco mais flexível, mas ainda longe do ideal. Boas opções neste caso seriam o Debian ou o Slack, desde que você tenha uma boa familiaridade com o escolhido.

No meu caso, instalo da seguinte forma:

1- Copio os arquivos do CD 1 do Conectiva 4 para uma pasta do servidor (/home/morimoto/conectiva por exemplo)

2- Compartilho a pasta via NFS. Para isso, basta editar o arquivo /etc/exports, adicionando uma linha com o diretório a ser compartilhado, como em:
#
/ home/ morimoto/ conectiva

3- Para ativar a alteração, uso o comando:
/ etc/ rc.d/ init.d/ nfs restart

4- Agora posso instalar nos terminais via rede, sem precisar instalar um CD-ROM em cada um.

Basta gravar um disquete com o arquivo **bootnet.img** que está na pasta **Images** do CD. Você pode fazer isso através do Windows mesmo, usando o Rawwritewin, que pode ser baixado em: http://www.downloads-guiadohardware.net/download/rawwritewin.exe

5- Basta configurar o terminal para dar boot através do disquete e manter o servidor ligado para iniciar a instalação. A primeira pergunta é sobre o chipset da placa de rede. A lista inclui a maior parte das placas, incluindo as placas com chipsets Realtek 8129 ou 8139 que são as mais vendidas ultimamente. Nas distros atuais o disquete é capaz de detectar a placa automaticamente.

6- Escolha a opção de instalação via NFS e forneça o endereço IP a ser usado pela estação, o endereço IP do servidor (o endereço da placa a ser utilizada pelo terminal) e o diretório que havíamos compartilhado no passo 2.

7- Iniciada a instalação, escolha a opção "Instalação mínima" que ocupa apenas 170 MB de espaço em disco e tem tudo de que iremos precisar. Se tiver espaço sobrando, você pode instalar mais pacotes que pretenda usar. A partição Swap, criada durante a etapa de particionamento deve ser de pelo menos 16 MB, mas procure reservar um pouco mais de espaço se puder.

8- Não se esqueça de configurar adequadamente a placa de vídeo, pois apesar da interface gráfica rodar no servidor, o servidor X roda no terminal. No final da configuração, marque a opção de inicializar a interface gráfica durante o boot.

Para configurar o servidor, basta fazer duas pequenas alterações em dois arquivos de configuração:

1- Abra o arquivo "**/etc/X11/xdm/xdm-config**" e comente a linha
"**DisplayManager.requestPort: 0**" adicionando uma "**!**" ou uma "**#**" no início. Se a linha já estiver comentada, deixe como está. Lembre-se que as linhas comentadas aparecem em azul no vi.

2- Abra o arquivo "**/etc/X11/xdm/Xaccess**" e descomente a linha
"*** #any host can get a login window"**, retirando a tralha. Preste atenção para não retirar nenhum dos espaços, apenas a tralha.

Feito isso, os terminais já poderão abrir a tela de login do servidor através do comando "**X -query IP_do_servidor**", como em "**X -query 10.0.0.1**". O comando deve ser dado com o terminal em modo texto

Para automatizar o processo, fazendo com que o terminal abra automaticamente a tela de login do servidor, sem passar pelo login local e sem a necessidade de digitar este comando a cada boot, edite o arquivo "**/etc/inittab**" (como root) e altere a linha
"**x:5:respawn:/etc/X11/prefdm -nodaemon**", que estará no final do arquivo para:
"x:5:respawn:/etc/X11/X -query IP_do_servidor", como em:

"**x:5:respawn:/etc/X11/X -query 10.0.0.1**"

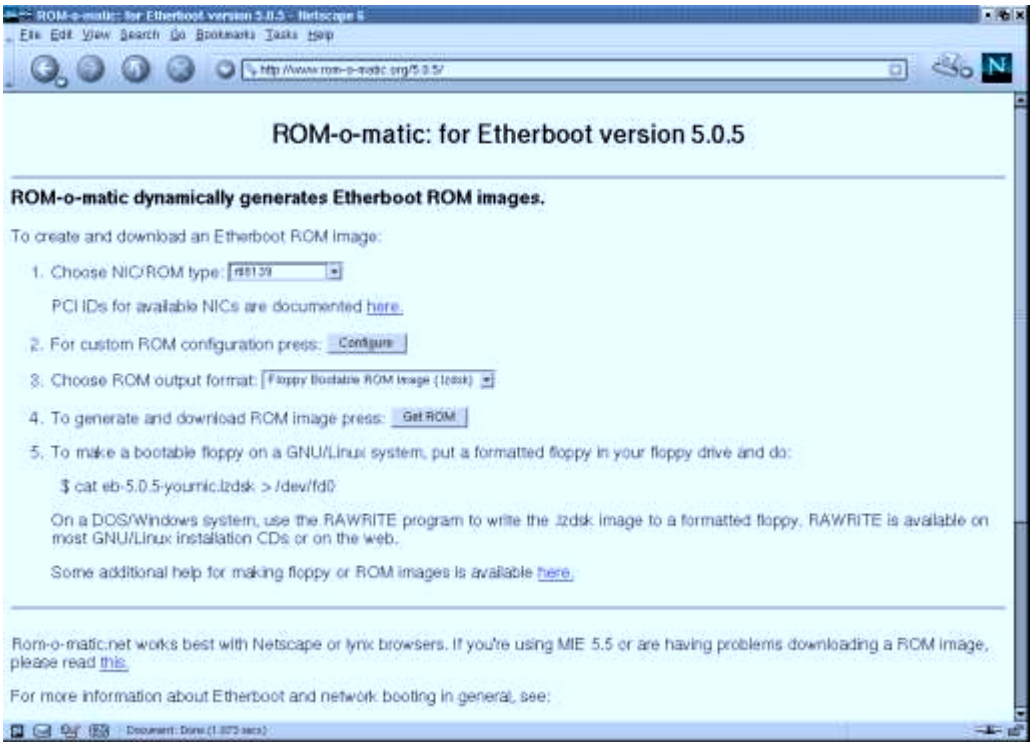
Lembre-se que caso o servidor tenha várias placas de rede, cada estação deve ser configurada com o IP da placa de rede a que estiver conectada. Veja o resultado:

Como disse, não é preciso fazer mas nenhuma configuração nas estações, apenas instalar os programas necessários no servidor. Isso se aplica também à Impressora, que uma vez instalada no servidor funciona em todos os terminais.

Estações diskless com o Etherboot

O Etherboot é o software que permite que as estações dêem boot através da rede, obtendo todo o software a partir do servidor. Como o software é muito pequeno, apenas 35 ou 40 KB, dependendo do driver usado pela placa de rede. O boot pode ser dado tanto através de um disquete, quanto a partir da ROM da placa de rede. A maior parte das placas de rede, mesmo as Realtek de 25 reais trazem um soquete vago para o encaixe de uma ROM. As ROMs são relativamente baratas, de 10 a 20 reais em média, mas você ainda precisará grava-las com o Etherboot. A menos que você pretenda gravar um número muito grande de ROMs, o mais econômico é procurar alguém que tenha um gravador de EPROMs. Como a maior parte dos gravadores de BIOS também grava ROMs de placas de rede, isto não é um grande problema hoje em dia.

Você pode conseguir os arquivos no http://rom-o-matic.net/ . Basta escolher o modelo do chipset da placa de rede e o formato da ROM (escolha Floppy Bootable ROM Image para dar boot através de um disquete) e clicar em Get ROM. Basta agora gravar o arquivo num disquete usando o Rawwritewin (veja o link acima). No Linux basta usar o comando "**cat nome_do_arquivo > /dev/fd0**"



Para descobrir o chipset da sua placa de rede, basta usar o comando "**lspci**" num terminal do Linux ou dar uma olhada no gerenciador de dispositivos do Windows. O Etherboot é compatível com um número relativamente limitado de placas, mas as Realtek 8129 e 8139, que representam uns 80% das placas vendidas atualmente no Brasil são suportadas perfeitamente. Estas placas estão entre as mais baratas, e são comercializadas sob várias marcas (Encore, Genius, etc.). O desempenho não é dos melhores e a utilização do processador não é das mais baixas, mas pelo menos as placas são baratas e compatíveis com os principais sistemas. Servem bem no nosso caso.

A configuração dos terminais se resume a gerar os disquetes ou ROMs. O problema maior é na configuração do servidor, bem mais complicada do que no sistema do tópico anterior.

O primeiro passo é ir no http://www.ltsp.org e baixar o LTSP, o software que iremos utilizar no servidor. Existem vários pacotes, com alguns aplicativos e vários drivers de vídeo, mas os pacotes básicos são:

ltsp_core-3.0.0-1.i386.rpm
ltsp_kernel-3.0.1-1.i386.rpm
ltsp_x_core-3.0.1-1.i386.rpm
ltsp_x_fonts-3.0.0-0.i386.rpm

Depois de baixar e instalar os quatro pacotes (através do comando **rpm -ivh nome_do_pacote**, ou simplesmente clicando sobre o arquivo através do gerenciador de arquivos) você ainda precisará configurar os parâmetros referentes aos terminais editando os arquivos:

/ etc/ dhcpd.conf
/ etc/ hosts

/ opt/ ltsp/ i386/ etc/ lts.conf

O primeiro, /etc/dhcpd.conf, é o principal pois contém os endereços IP do servidor e de cada estação, o /etc/hosts contém os nomes das estações e o endereço IP correspondente a cada uma, para permitir que você possa acessa-las usando os nomes ao invés dos endereços IP. Finalmente, o /opt/ltsp/i386/etc/lts.conf permite que especifique opções relacionadas a cada terminal, como o servidor X a ser usado, o driver do mouse, etc.

Você pode encontrar detalhes sobre a configuração de cada arquivo no:
http://www.ltsp.org/documentation/ltsp-3.0.0/ltsp-3.0.html

Existem algumas limitações no uso do LTSP. O servidor deve ser o único servidor DHCP disponível na rede. Você não pode por exemplo manter uma estação Windows com o ICS ativado na mesma rede. Apesar da configuração ser centralizada no servidor, você precisará configurar cada estação de forma independente no /opt/ltsp/i386/etc/lts.conf, sem direito a qualquer mecanismo de detecção automática. E, o mais limitante, o servidor deverá ter uma única placa de rede, o que impede o uso de todo o projeto de rede para otimizar o desempenho das estações que havia mostrado anteriormente. O melhor projeto de rede neste caso seria usar uma placa Gigabit Ethernet no servidor e um switch para permitir que as placas das estações trabalhem a 10 ou 100, sem limitar o desempenho da placa do servidor. Mas, este projeto é mais caro e menos eficiente.

Eu pessoalmente prefiro usar o modo anterior, usando um HD em cada estação, mas você pode estudar ambos os sistemas e decidir qual é mais vantajoso para você, já que ambos possuem prós e contras.

O Linux Conectiva possui um sistema de boot remoto semelhante ao do LTSP.org, mas que já acompanha o sistema, conta com um módulo de configuração gráfica através do LinuxConf e possui documentação em Português que você encontra no:
http://www.conectiva.com/doc/livros/online/7.0/servidor/implementa-bootremoto.html

Usando os terminais

Tenha em mente que como todos os aplicativos rodam no servidor, todos os arquivos também são salvos no servidor. Por isso, o ideal é criar uma conta de usuário para cada usuário do sistema, de modo que ele possa salvar seus arquivos, seus e-mails, etc. Isso é muito mais eficiente e mais barato do que a idéia da prefeitura de São Paulo de financiar a compra de um cartão de memória flash para cada usuário. Como um usuário não tem permissão para acessar os arquivos das pastas dos outros, isso oferece uma segurança e privacidade muito boa.

O backup também é bastante simples, já que estará centralizado. Você pode ter por exemplo um segundo HD e uma gaveta para fazer o backup sempre que necessário e guardá-lo num local seguro. Uma dica importante é usar o sistema de arquivos EXT3 no servidor, que é muito mais seguro que o antigo EXT2, que é muito susceptível à perda de dados depois de desligamentos incorretos.

A manutenção do servidor pode ser feita a partir de qualquer terminal, ou até mesmo via internet (se você configurar o Firewall para liberar o acesso via SSH) e se precisar instalar novos programas, basta instalá-los no servidor, para que todos os usuários possam usar.

Os problemas com vírus e cavalos de Tróia são muito menores no Linux. Um programa executado pelo usuário não tem mais permissões do que ele mesmo. Ou seja, se um usuário não tem permissão para alterar arquivos fora da sua pasta, qualquer programa executado por ele também não terá. Na pior das hipóteses ele pode acabar com seus próprios arquivos pessoais, mas não afetar os arquivos dos demais usuários ou o sistema.

Nas estações a única preocupação é com problemas de hardware, que provavelmente serão relativamente freqüentes, já que estamos falando de máquinas com 6, 8 ou até 10 anos de uso. Mas, pelo menos você não precisará se preocupar com perda de dados, já que estará tudo no servidor. Basta resolver o problema ou até mesmo reinstalar o sistema se necessário, refazer a configuração e pronto, o terminal estará de volta à rede.

Existem naturalmente algumas limitações no uso dos terminais, os jogos por exemplo. Jogos de cartas, ou de tabuleiro, ou até mesmo títulos como o Freeciv (um clone do Civilization 2) onde existe pouca movimentação rodam sem problemas, mas jogos de movimentação rápida em tela cheia não vão rodar satisfatoriamente.

Para usar a placa de som do servidor a partir de uma das estações, o mesmo usuário deverá estar logado localmente no servidor. Se por exemplo estou utilizando o login "morimoto" e quero ouvir um MP3 usando a placa de som do servidor, precisarei primeiro ligar o monitor do servidor e logar o morimoto, para que o servidor de som seja iniciado. O som só funcionará nos terminais usando o login morimoto, embora nada impeça que você use o mesmo login em mais de um terminal ao mesmo tempo.

O CD-ROM e o drive de disquetes do servidor poderão ser usados normalmente pelos usuários, inclusive com vários usuários acessando o CD que está na bandeja por exemplo.

Fora estes detalhes, você conseguirá rodar todo tipo de programas nos terminais, usar qualquer efeito pesado do gimp, etc. A princípio, pode parecer que rodar aplicativos de 10 clientes no servidor ao mesmo tempo irá deixá-lo bastante lento, mas na prática isso funciona da mesma forma que as linhas dos provedores de acesso. Nenhum provedor tem o mesmo número de linhas e de assinantes, geralmente utilizam uma proporção de 8 ou 10 pra um, presumindo que jamais todos os assinantes vão resolver conectar ao mesmo tempo. Mesmo com 10 clientes, raramente todos vão resolver rodar ao mesmo tempo algo que consuma todos os recursos do servidor por muito tempo. Normalmente temos apenas tarefas rápidas, como abrir um programa, carregar uma página Web, etc. feitas de forma intercalada.

Outro ponto interessante diz respeito às suas estratégias de upgrade. Ao invés de gastar dinheiro com upgrades de memória e processador para os clientes, você deve investir os recursos disponíveis em melhorar o servidor e a rede, além de trocar monitores, teclados e mouses nas estações. Um monitor de 15" e um teclado novo numas das estações vão fazer muito mais efeito que um upgrade na torre.