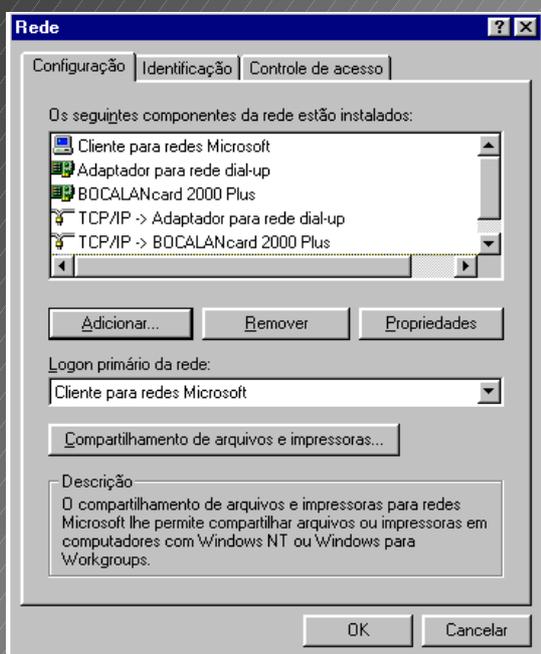
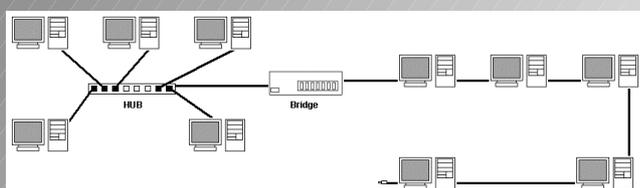


Redes

Guia Completo



Edição especial para a



PC GAMER BRASIL

Carlos E. Morimoto

<http://www.guiadohardware.net>

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 o mais didática possível, abordando todos os detalhes, porém sem cair no tecnicismo, a mesma linguagem que uso em meus outros livros.

Direitos Autorais

Este e-book foi escrito por Carlos E. Morimoto (morimoto@guiadohardware.net) e é vendido através do Guia do Hardware, no endereço <http://www.guiadohardware.net>.

Apesar de estar em formato digital, este livro não é de livre distribuição; é vendido por um preço simbólico de 3 reais por cópia através do próprio autor.

Esta é uma edição especial e exclusiva para a Revista PC Gamer Brasil, um brinde que é parte integrante da sua revista favorita

Para conhecer outros e-books como este, visite o Guia do Hardware:
<http://www.guiadohardware.net>

Conheça o Guia do Hardware

Se você quer se manter atualizado sobre todas as novidades do mundo da informática, conhecer novos processadores e placas antes mesmo de serem lançados e todas as dicas de manutenção de micros, então não pode deixar de nos visitar.

- Curso online de montagem e manutenção de micros
- Informativo diário com dicas e artigos exclusivos via e-mail
- Tutoriais e análises dos últimos lançamentos
- Sessão FAQ com centenas de problemas resolvidos
- Todas as dicas sobre overclock e como envenenar seu micro
- Fóruns, classificados e muito mais

Tudo grátis! É só acessar:

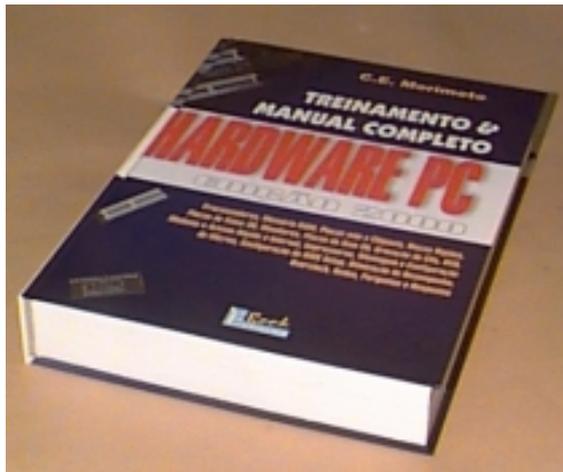
<http://www.guiadohardware.net>

The screenshot shows the homepage of 'Guia do Hardware' in a Microsoft Internet Explorer browser window. The browser's address bar displays 'http://www.guiadohardware.net/'. The website has a blue and white color scheme. At the top, there's a navigation bar with 'Seja Bem-Vindo!' and 'Hoje, 23 de outubro'. Below this, there are several sections: 'Conheça quem faz o Guia do Hardware...', 'Nova E-Book sobre manutenção...', and a 'seções' sidebar listing various content categories like 'Curso de Hard OnLine', 'Fóruns', 'E-Books', 'Dica do Dia', 'Tutoriais', 'Overclock', 'Análises', 'Artigos', 'Palm-Pilot', 'Humor', 'F.A.Q.', 'Download', and 'Tira-Dúvidas'. The main content area features an article titled 'Nova área de Overclock' with a sub-header '27/09 Super atualização: Hoje tivemos mais uma grante atualização no site...'. To the right, there's a 'Destques' sidebar with links to 'E-Books', 'Artigos', 'Análises', 'Tutoriais', and 'Discos Rígidos'. At the bottom, there are sections for 'Entre em contato' and 'Pesquisa'.

Outros Livros

Se você gostou deste livro digital, convido-o a conhecer meus outros trabalhos:

HARDWARE PC Edição 2000



Formato grande : 29 x 24 cm.
640 Páginas, mais de 500 ilustrações
Capa dura
Autor: Carlos E. Morimoto
Ed. Book Express

Preço nas livrarias: R\$ 109

Compre online com desconto no Guia do Hardware:
<http://www.guiadohardware.net>

É indiscutível que atualmente os computadores estão cada vez mais fazendo parte do nosso cotidiano. Acompanhando esta invasão anunciada, existe uma demanda cada vez maior por profissionais especializados na área de manutenção.

Neste livro você encontrará desde os conceitos mais básicos, até tópicos avançados, discutindo por exemplo a arquitetura interna dos processadores Pentium III e AMD Athlon, passando claro por todos os demais componentes do PC, incluindo placas mães, discos rígidos, memórias, chipsets, placas de vídeo 3D, placas de som, monitores, modems, etc., além de todos os procedimentos de montagem e manutenção de micros, solução de problemas, configuração avançada do Bios Setup, overclock e implantação de redes.

Outra grande preocupação que tive enquanto escrevia, foi manter a didática das explicações, deixando o tecnicismo de lado e utilizando uma linguagem mais próxima da realidade. Apesar deste não ser um livro destinado a leigos, mesmo um principiante poderá compreender as explicações facilmente.

Apesar de na área da Informática ser difícil manter um trabalho atualizado por muito tempo, devido à rápida evolução da tecnologia, me esforcei para incluir neste livro todas as tendências e futuras tecnologias o que deve mante-lo atualizado por muito mais tempo. Você encontrará, por exemplo, descrições dos processadores Intel Itanium e AMD Sledgehammer que devem ser lançados apenas em 2002, assim como de outras tecnologias que ainda estão se popularizando, como as tecnologias de acesso rápido à Internet: ADSL, ISDN, VDSL, acesso via cabo e acesso via satélite.

Devido à quantidade de informações reunidas, posso dizer sem falsa modéstia, que atualmente este é o mais completo guia de referência sobre Hardware em língua Portuguesa. Se você trabalha ou pretende trabalhar na área, as informações contidas aqui serão muito úteis para sua vida profissional.

Se você é apenas um usuário com curiosidade acima da média, encontrará aqui todas as referências sobre as antigas e novas tecnologias, que o manterão atualizado durante muito tempo.

Outros e-books

Um e-book, ou eletronic book, é um livro como outro qualquer, a única diferença é que ao invés de ser impresso, é vendido em formato digital; baixado, ou recebido via e-mail.

Para o leitor, a maior vantagem do e-book é o preço, Como um e-book é distribuído em formato digital, não existe custo de impressão, distribuição, nem o risco de encalhe, por isso, ele custa muito menos que custaria caso fosse impresso. Você não paga pelo papel, mas apenas pela informação em sí. O livro pode então ser lido no seu micro ou então impresso. Você escolhe o que acha mais prático.

Os livros a seguir podem ser comprados diretamente através do Guia do Hardware, <http://www.guiadohardware.net>

Guia de Upgrade e Manutenção



Formato Digital (em PDF)

307 Páginas,

Autor: Carlos E. Morimoto

Preço: R\$ 5,00

O upgrade é um recurso usado desde os primeiros micros PC, servindo como uma opção econômica para aumentar o desempenho do micro. Para fazer um bom upgrade é preciso estar por dentro dos componentes disponíveis no mercado, quais apresentam melhor desempenho, melhor

custo-benefício e quais são compatíveis com a placa mãe e os outros componentes que não serão substituídos.

Neste livro você encontrará todas as informações para fazer um bons upgrades, tanto no seu próprio micro, quanto para clientes. Analisaremos com detalhes quais são os processadores, placas de vídeo 3D, placas mãe, memórias, placas de som, modems e HDs disponíveis, e quais são os melhores em cada caso.

Você também encontrará muitas dicas de manutenção, que lhe darão bagagem para resolver os problemas mais cabeludos, montagem de micros passo a passo, além de um guia completo de upgrade em notebooks.

Para comprar visite: <http://www.guiadohardware.net>

HARDWARE – Manual Completo



Formato Digital (em PDF)

317 Páginas,

Autor: Carlos E. Morimoto

Preço: R\$ 5,00

Os computadores estão cada vez mais fazendo parte de nossas vidas. No trabalho ou em casa, é inegável a sua utilidade.

A característica mais marcante dos micros PC é a sua arquitetura aberta, o que permite que os vários fabricantes criem componentes compatíveis entre si. Se, por exemplo, o espaço no seu disco rígido deixou de ser suficiente, bastará ir à qualquer loja de informática e comprar um de maior capacidade, e em poucos minutos ele estará instalado e funcionando.

Devido a esta arquitetura aberta, ao invés de comprar um computador pronto, o próprio usuário tem a liberdade de montar seu próprio micro, escolhendo a configuração que mais atende suas necessidades, podendo futuramente realizar upgrades, atualizando este equipamento conforme novas tecnologias forem surgindo.

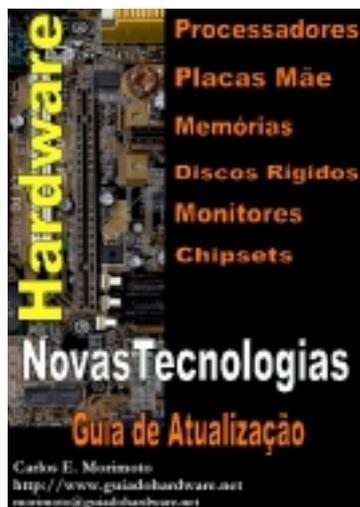
Seja você um técnico especializado, ou simplesmente um usuário com curiosidade acima da média, encontrará neste livro uma fonte rica e atualizada de informações que lhe permitirão, não

somente montar e configurar micros, mas entender todos os seus segredos, muitas vezes ocultados pela linguagem técnica dos manuais, ou pelas complicadas opções do CMOS Setup, tornando-se apto para facilmente deixar qualquer micro PC "em ponto de bala" solucionando qualquer problema de funcionamento e melhorando seu desempenho com configurações otimizadas.

Estudaremos com detalhes neste livro desde cabos e conectores até as opções mais enigmáticas do CMOS Setup, passando pelo funcionamento e especificações técnicas de vários tipos de processadores, discos rígidos, memórias, chipsets, placas mães, placas de vídeo, monitores, e muitos outros periféricos.

Para comprar visite: <http://www.guiadohardware.net>

HARDWARE - Novas Tecnologias



Formato Digital (em PDF)

138 Páginas,

29 ilustrações,

Autor: Carlos E. Morimoto

Preço: R\$ 5,00

O Mundo da Informática está em constante evolução. Neste mundo mutável, não é fácil manter-se atualizado. Praticamente a cada dia surgem novos processadores, novas placas de vídeo, novos chipsets, novos padrões e novos periféricos, muitas vezes incompatíveis com os padrões anteriores. Este livro traz informações sobre a maioria dos novos componentes, incluindo processadores, placas mãe, memórias, discos rígidos, placas de vídeo e monitores.

Você encontrará informações sobre todos os processadores usados em micros PC, do 8088 ao Pentium III, incluindo os novos processadores, como o Athlon Thunderbird e futuros lançamentos, incluindo o AMD Duron, AMD Mustang, AMD Sledgehammer, Intel Tinna, Willamette e Itanium; informações sobre novas tecnologias, como os Slots AGP Pro, AMR e Fireware, memórias Rambus, DDR-SDRAM, novos chipsets, monitores LCD, etc. Seja você um técnico, ou apenas um usuário querendo manter-se por dentro das novas tecnologias, este livro lhe será muito útil.

Para comprar visite: <http://www.guiadohardware.net>

Placas de Vídeo 3D, modelos e recursos



Formato Digital (em PDF)

64 Páginas,

Autor: Carlos E. Morimoto

Preço: R\$ 3,00

As placas de vídeo 3D são cada vez mais indispensáveis para quem não dispensa bons jogos. Jogos como o Quake 3, Unreal Torment e outros, jamais vão rodar satisfatoriamente sem uma placa 3D, independentemente da potência do processador.

Felizmente ou infelizmente, existe uma competição muito grande no ramo de placas 3D, o que aumenta a oferta de modelos, potencializa sua evolução, força a queda dos preços, mas ao mesmo tempo torna cada vez mais difícil a escolha na hora da compra.

Mas afinal, por que uma placa 3D é tão importante? Qual é a melhor placa do mercado? Qual é a melhor em termos de custo benefício? Quais modelos podem ser usados no meu micro? Quanto deve ter de memória? As placas AGP são realmente mais rápidas que as PCI? Leia este livro até o fim e você poderá dar uma verdadeira aula da próxima vez que lhe fizerem estas perguntas :-)

Para comprar visite: <http://www.guiadohardware.net>

Sumário

Prefácio	2
Direitos Autorais	3
Conheça o Guia do Hardware	4
HARDWARE PC Edição 2000	5
Outros e-books	6
Guia de Upgrade e Manutenção	6
HARDWARE – Manual Completo	7
HARDWARE - Novas Tecnologias	8
Placas de Vídeo 3D, modelos e recursos	9
Sumário	10
Porque ligar micros em rede?	13
Compartilhando arquivos	13
Compartilhando periféricos	14
Sistema de mensagens e agenda de grupo	14
Jogos em Rede	14
Como as redes funcionam	14
Placas de Rede	14
Cabos	15
Topologias	15
Arquiteturas	16
Protocolos	16
Recursos	17
N.O.S.	17
Cabeamento	18
Tipos de cabos	18
Cabo coaxial	18
Cabo de par trançado	21
Par trançado x Coaxial	24
Fibra óptica	25
Redes de energia x Redes telefônicas	26
Placas de Rede	26

Hubs	28
Hubs Inteligentes.....	28
Conectando Hubs	29
Repetidores	29
Crescendo junto com a rede	29
10BaseT.....	30
10 ou 100?	30
Bridges, Roteadores e Gateways	31
Bridges (pontes).....	31
Como funcionam os Bridges?.....	31
Roteadores (routers).....	32
Nós de interconexão.....	33
Arquiteturas de rede.....	34
Topologias Lógicas.....	34
Redes Ethernet	35
Pacotes	36
Redes Token Ring	37
Redes Arcnet	39
Ponto a ponto x cliente - servidor.....	39
Cliente - servidor.....	40
Servidores de disco	40
Servidores de arquivos	41
Ponto a ponto	41
Servidores não dedicados.....	41
Impressoras de rede.....	42
Protocolos	42
Camadas da rede	43
NetBEUI.....	43
IPX/SPX.....	44
DLC	44
TCP/IP	45
Segurança na Internet.....	46

Como são feitas as invasões.....	46
Máscara de sub-rede.....	49
Máscaras complexas	50
Usando o DHCP	53
Default Gateway.....	54
Servidor DNS.....	55
Servidor WINS.....	55
Redes Virtuais Privadas	55
Configurando uma estação de trabalho com o Windows 98	56
Instalando a placa de rede	56
Protocolos e serviços de rede.....	56
Configurando uma rede ponto a ponto.....	57
Configurações	58
Logando-se na rede	61
Compartilhando recursos	61
Acessando Discos e pastas compartilhados	63
Acessando impressoras de rede	64
Compartilhamentos ocultos	66
Compartilhando a conexão com a Internet	66
Acessando um Servidor Windows 2000 ou Windows NT	66
Acessando um Servidor Novell NetWare	68
Conectando-se a uma VPN	69

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, assim como 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 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 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, dependendo da marca, entre 15 e 50 dólares; 10 metros de cabos de par trançado, custam de 3 a 5 dólares, enquanto um Hub simples custa entre 50 ou 70 dólares.

Se você mesmo for fazer o trabalho, ligar 10 micros em rede, custaria entre 200 e 400 dólares usando cabos de par trançado e um Hub ou, um pouco menos, caso fosse usado cabo coaxial (já que neste caso não precisaríamos de um hub).

Com a rede funcionando, você poderá compartilhar e transferir arquivos, compartilhar periféricos, melhorar a comunicação entre os usuários da rede através de um sistema de mensagens e 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, estaríamos 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. Além de arquivos individuais, é possível compartilhar pastas ou mesmo, uma unidade de disco inteira, sempre com o recurso de estabelecer senhas.



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 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.

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.

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 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 apenas 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.

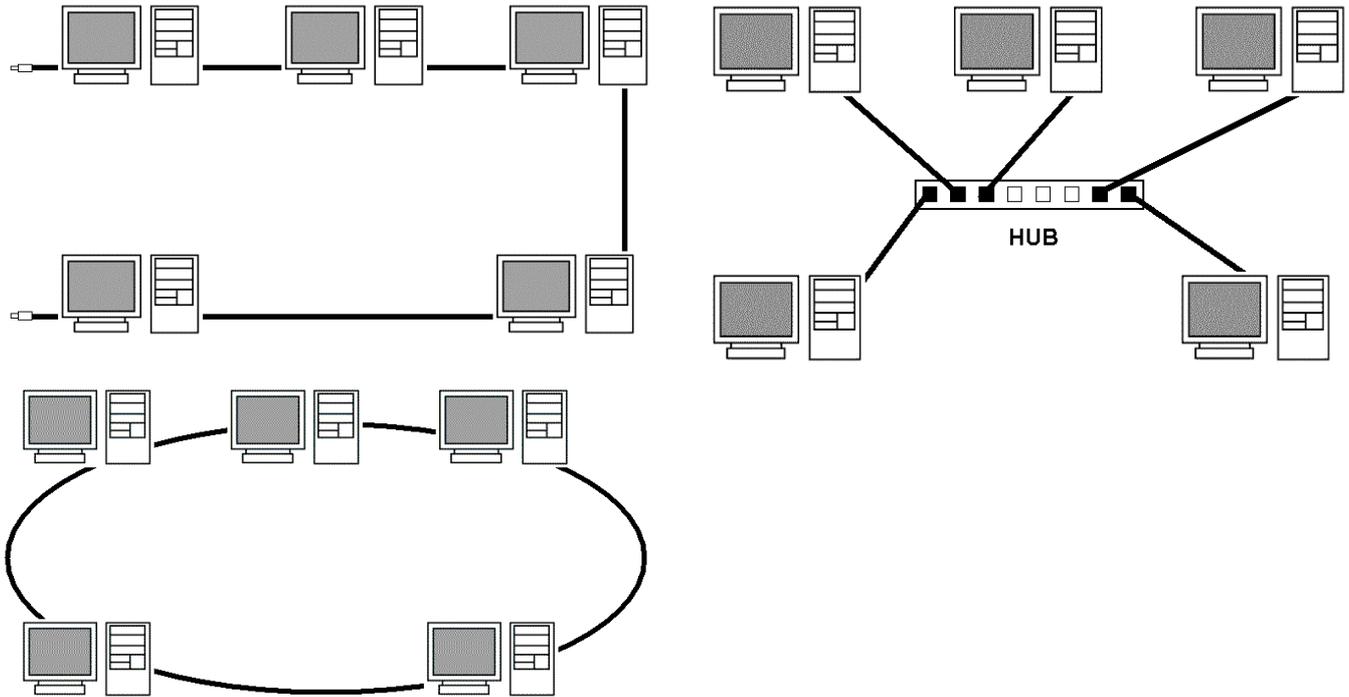
Cabos

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.

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.

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, nela um único cabo coaxial interliga todos os micros. Na topologia de estrela, os micros não são ligados entre si, 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 duas 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.

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 TCP/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 é 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.

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.

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.

Tipos de cabos

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.



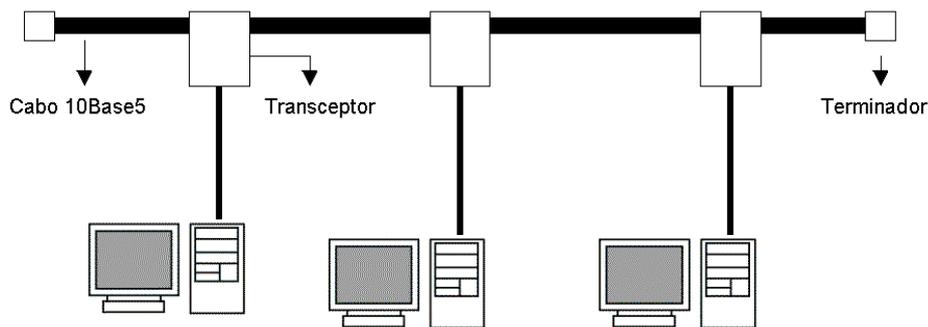
Se você envolver um fio condutor com uma segunda camada de material condutor, a camada externa protegerá a primeira da interferência externa. Devido a esta blindagem, os cabos coaxiais (apesar de ligeiramente mais caros que os de par trançado) podem transmitir dados a distâncias maiores, sem que haja 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.



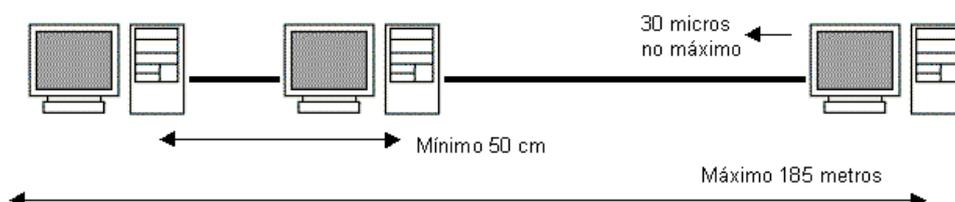
Os cabos 10Base5 foram praticamente os únicos utilizados em redes de mainframes no início da década de 80, mas sua popularidade foi diminuindo com o passar do tempo por motivos óbvios. Atualmente você só se deparará com este tipo de cabo em instalações bem antigas ou, quem sabe, em museus ;-)

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.

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.



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.



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.

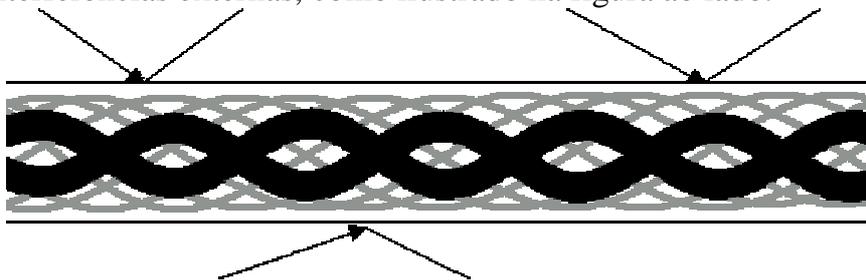


Descascador de cabos coaxiais (à esquerda) e alicate de crimpagem.

Cabo de par trançado

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, como ilustrado na figura ao lado.



Além dos cabos sem blindagem, 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 a 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, porém não é mais utilizado.

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

Categoria 3: É o cabo de par trançado sem blindagem usado em redes, pode se estender por até 100 metros e permite transmissão de dados a até 10 Mbps. A diferença do cabo de categoria 3 (que é praticamente o único tipo de cabo sem blindagem usado atualmente) para os obsoletos cabos de categoria 1 e 2 é o número 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.

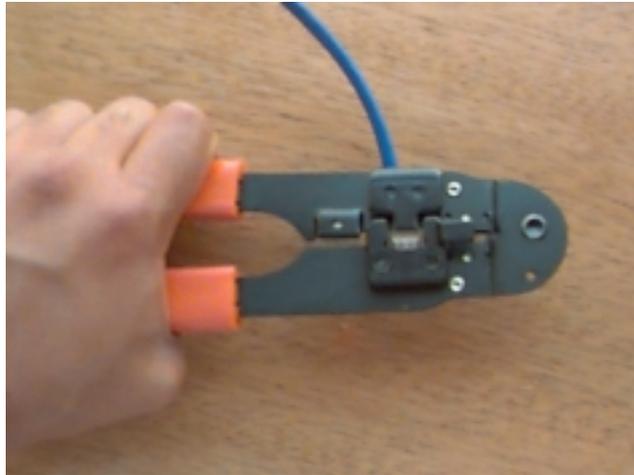
Categoria 5: Este é o cabo blindado de qualidade mais alta, permitindo transferências de dados a até 100 mbps. Apesar de ser um pouco mais caro, este é o cabo mais recomendável, pois além de ser blindado e conseqüentemente mais resistente a interferências externas é o único das 5 categorias que permite seguramente transferências de dados a 100 mbps em conjunto com placas de rede Ethernet de 100 mbps.

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.



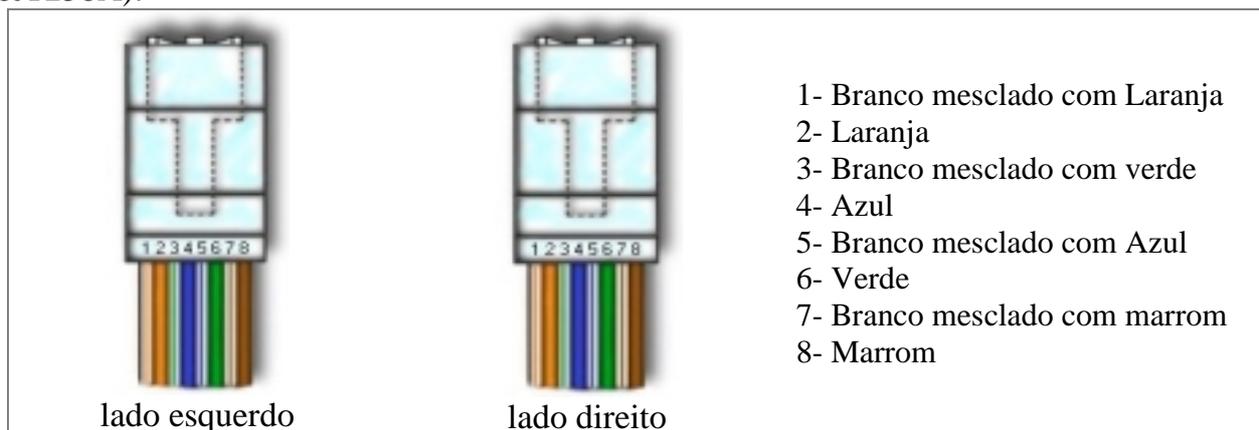
Para prender o cabo ao conector, usamos um alicate de crimpagem. Após retirar a capa protetora externa e inserir os fios dentro do conector, basta pressionar os pinos do conector com o

alicate. 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, deixando o encaixe com os pinos do conector “frouxo”.

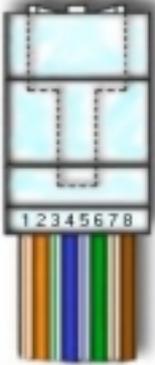


Os alicates para crimpar cabos de par trançado são um pouco mais baratos que os usados para crimpar cabos coaxiais. Os alicates mais simples custam a partir de 40 reais, mas os bons alicates custam bem mais. Existem alguns modelos de alicates feitos de plástico, com apenas as pontas de metal. Estes custam 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.

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 (usando o padrão AT&T258A):



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:

	<p>Conector da esquerda:</p> <ol style="list-style-type: none">1- Branco com Laranja2- Laranja3- Branco com Verde4- Azul5- Branco com Azul6- Verde7- Branco com Marrom8- Marrom		<p>Conector da direita:</p> <ol style="list-style-type: none">1- Branco com Verde2- Verde3- Branco com Laranja4- Azul5- Branco com Azul6- Laranja7- Branco com Marrom8- Marrom
lado esquerdo		lado direito	

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.

Par trançado x Coaxial

Disse anteriormente que cada uma destas categorias de cabos possui algumas vantagens e desvantagens. Na verdade, o coaxial possui mais desvantagens do que vantagens em relação aos cabos de par trançado, mas ainda pode ser atraente para uso em pequenas redes, pois a topologia de barramento traz a vantagem de não exigir um hub. Numa comparação direta entre os dois tipos de cabos teremos:

Distância máxima: o cabo coaxial permite uma distância máxima entre os pontos de até 300 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 maior, pois este tipo de cabo costuma ser mais suscetível a mau contato do que os cabos UTP e STP. Outra desvantagem é que usando o coaxial, quando temos problemas de mau contato no conector de uma das estações, a rede toda cai, ou, na melhor das hipóteses, teremos a rede dividida ao meio. Usando par trançado, por outro lado (devido à existência do hub), apenas o micro problemático ficará isolado da rede.

Custo: Os cabos coaxiais são mais caros que os cabos de par trançado sem blindagem, mas normalmente são mais baratos que os cabos blindados. Por outro lado, usando cabos coaxiais você não precisará de um hub.

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 blindados categoria 5, pois tanto os cabos coaxiais, quanto os cabos de categoria 3, são adequados a transmissões de apenas 10 mbps.

Montar uma rede usando cabos de par trançado é sempre melhor, mas no caso de uma rede pequena, de 3 ou 5 micros, usar cabo coaxial pode mais vantajoso no quesito custo, já que um hub, por mais simples que seja, dificilmente custa menos que 50 ou 70 dólares.

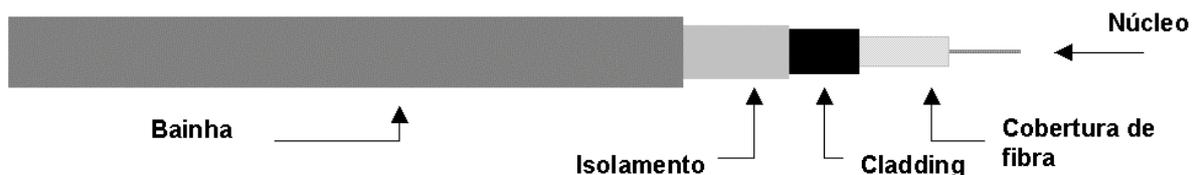
Fibra óptica

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 nas 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.

Redes de energia x Redes telefônicas

Duas novas idéias de ambientes de rede, que vêm ganhando espaço conforme tem amadurecido, é o uso das fiações elétricas e extensões telefônicas, que já estão presentes em praticamente qualquer ambiente, como mídia de comunicação no lugar dos cabos de rede tradicionais. Por um lado, isto tornaria a instalação da rede bem mais prática, pois não seria preciso instalar cabos de rede, apenas ligar os micros nas tomadas elétricas ou extensões telefônicas já existentes usando os periféricos necessários. Por outro lado, há várias dificuldades técnicas. Do lado das redes de energia elétrica temos a taxa de transferência limitada a apenas 350 Kbps e riscos de segurança decorrentes de variações de tensão. Nas redes telefônicas a velocidade é um pouco maior, 1 mbps, mas em compensação as placas de rede são mais caras.

Em ambos os casos, as transmissões de rede são feitas usando transmissões à frequências superiores a 2 MHz, não prejudicando o funcionamento normal da rede elétrica ou atrapalhando as conversas telefônicas e mesmo comunicações via modem, que são feitas utilizando frequências bem inferiores.

Apesar dos produtos comerciais ainda serem raros, estas prometem ser mais duas opções de redes domésticas nos próximos anos, apesar de ambas as tecnologias já nascerem com graves limitações técnicas.

Placas de Rede

A placa de rede é o hardware que permite aos micros conversarem entre si 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, 4 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.



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.

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 si. 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.

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 si através de um barramento especial. 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 si 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.



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.

10BaseT

Você ouvirá muito o termo “rede Ethernet 10BaseT”. O termo 10BaseT é usado para designar uma rede com topologia de estrela, onde temos vários hubs interligados. Esta é apenas uma convenção, não existe necessariamente diferença entre uma “placa de rede Ethernet” e uma “placa de rede Ethernet 10BaseT”. Um “hub 10BaseT” por sua vez, nada mais é do que um hub que pode ser conectado a outros hubs.

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 frequentemente 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?

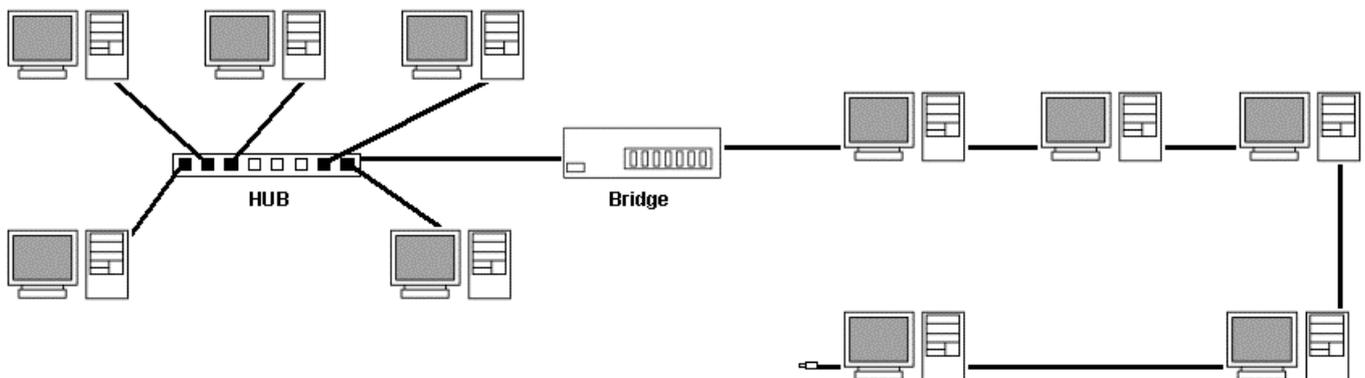
Em redes maiores, além de cabos e hubs, usamos mais alguns dispositivos, um pouco mais caros: bridges (pontes) e Roteadores (routers).

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 si, 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.

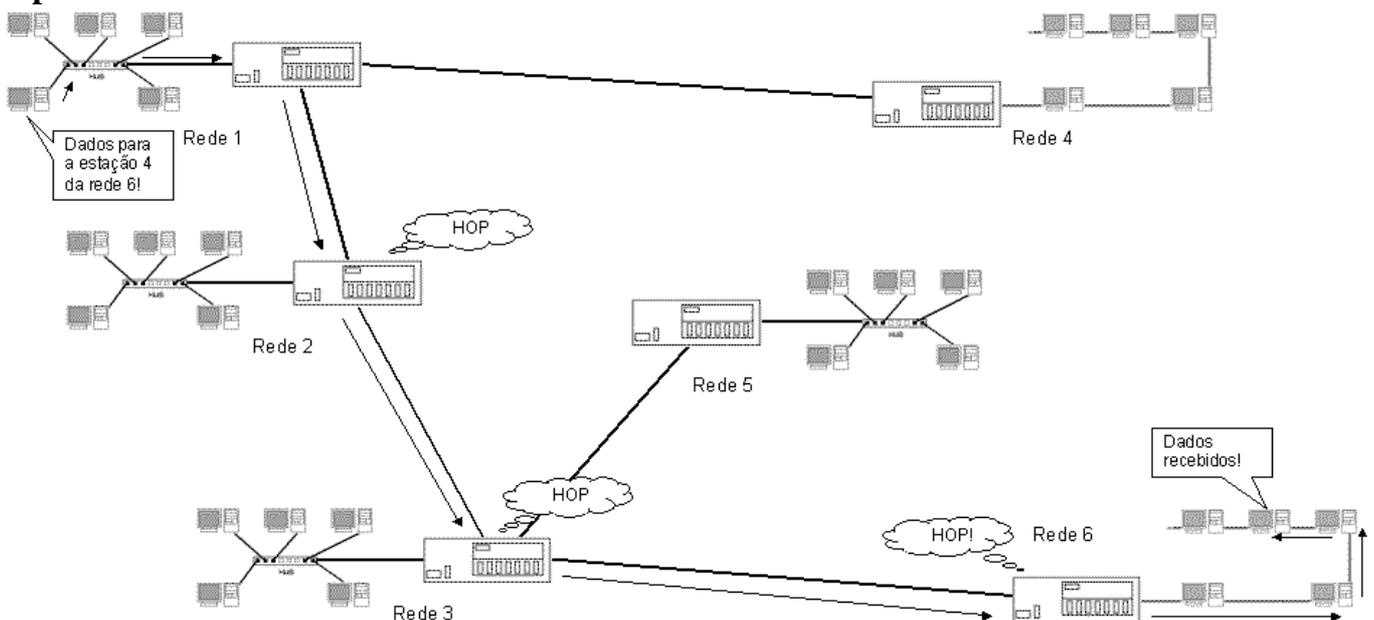
Existem também alguns bridges mais simples (e mais baratos) que não são capazes de distinguir se um pacote se destina ou não ao outro lado da rede. Eles simplesmente encaminham tudo, aumentando desnecessariamente o tráfego na rede. Estes bridges são chamados de bridges de encaminhamento.

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 si.

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, 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

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.

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 TCP/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. 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). 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.

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.

Dependendo do caso, a topologia de barramento pode ser vantajosa para redes de no máximo 8 ou 10 micros, acima disto você deve considerar apenas a topologia de estrela.

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.

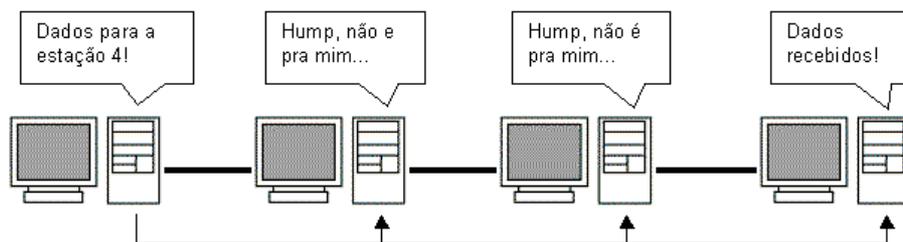
Topologias Lógicas

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.

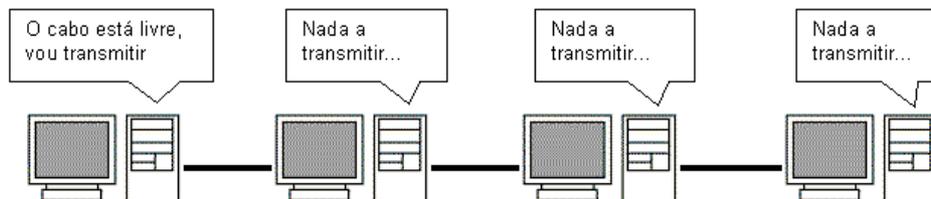
Existem três topologias lógicas de rede: Ethernet, Token Ring e Arcnet. Como a topologia lógica determina diretamente o modo de funcionamento da placa de rede, esta será específica para um tipo de rede. Não é possível usar placas Token Ring em Redes Ethernet, ou placas Ethernet em Redes Arcnet, por exemplo.

Redes Ethernet

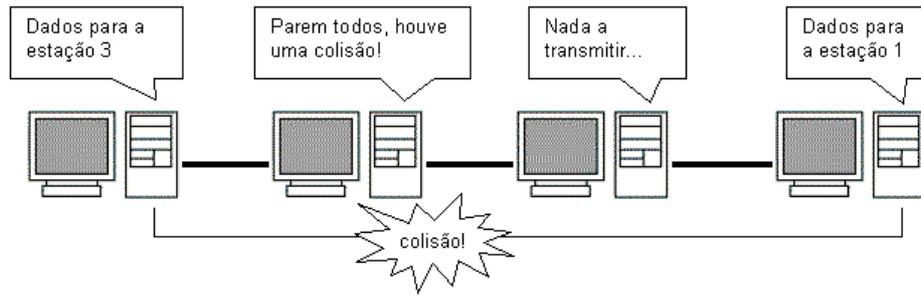
As placas de rede Ethernet são de longe as mais utilizadas atualmente, sobretudo em redes pequenas e médias e provavelmente a única arquitetura de rede com a qual você irá trabalhar. Numa rede Ethernet, temos uma topologia lógica de barramento. Isto significa que quando uma estação precisar transmitir 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.



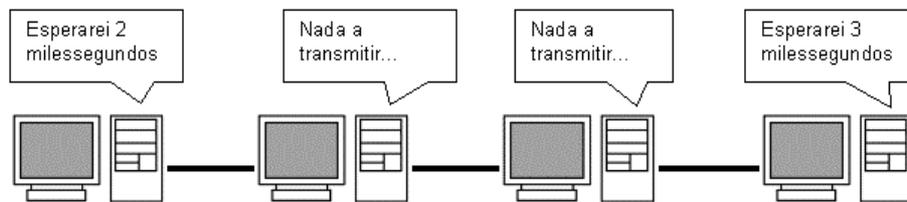
Como apenas uma estação pode falar de cada vez, antes de transmitir dados a estação irá “ouvir” o cabo. Se perceber que nenhuma estação está transmitindo, enviará seu pacote, caso contrário, esperará até que o cabo esteja livre. Este processo é chamado de “Carrier Sense” ou sensor mensageiro.



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 frequência 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 milissegundos antes de tentarem transmitir novamente. Este processo é chamado de TBEB “truncated exponential backof”. Inicialmente as placas escolherão entre 1 ou 2, se houver outra colisão escolherão entre 1 e 4, em seguida entre 1 e 8 milissegundos, 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 3ª 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, será solicitada uma retransmissão do pacote. Quanto pior for a qualidade do cabo e maior forem as interferências, mais pacotes chegarão corrompidos e terão que ser retransmitidos e, conseqüentemente, pior será o desempenho da rede. Os pacotes Ethernet são divididos em 7 partes:

Preâmbulo (7 bytes)	Início (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 sincronizador. O **byte de início** avisa as estações receptoras 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 si, 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.

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 si. 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.

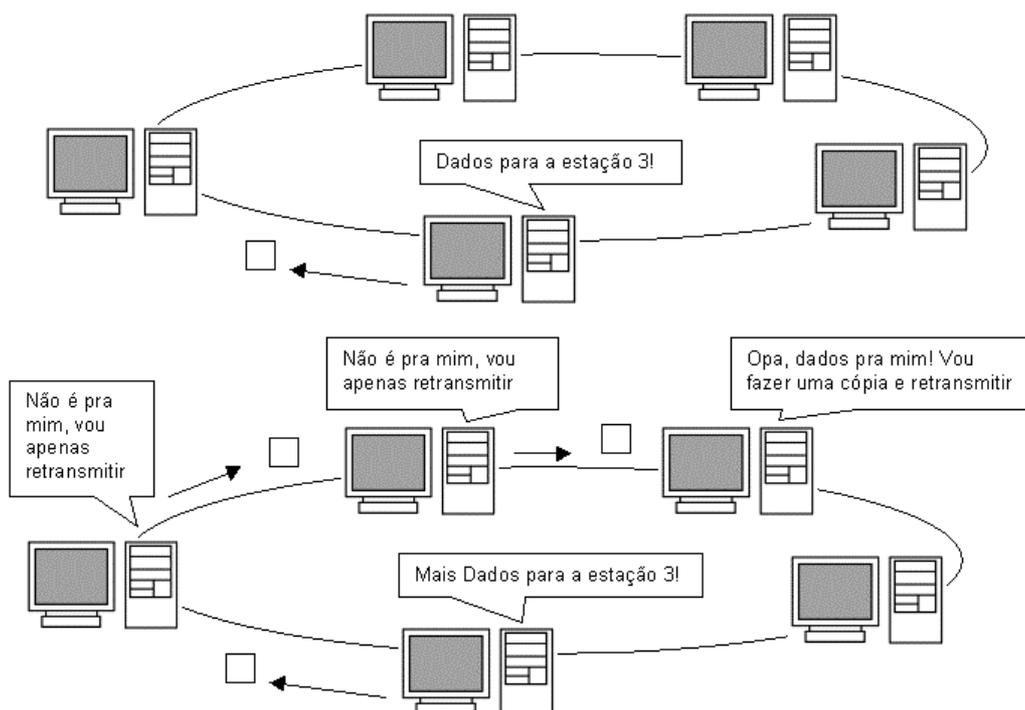
Devido a estas vantagens, as redes Token Ring ainda são razoavelmente utilizadas em redes de médio a grande porte. Contudo, não é recomendável pensar em montar uma rede Token Ring para seu escritório, pois os hubs são muito caros e a velocidade de transmissão em pequenas redes é bem mais baixa que nas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

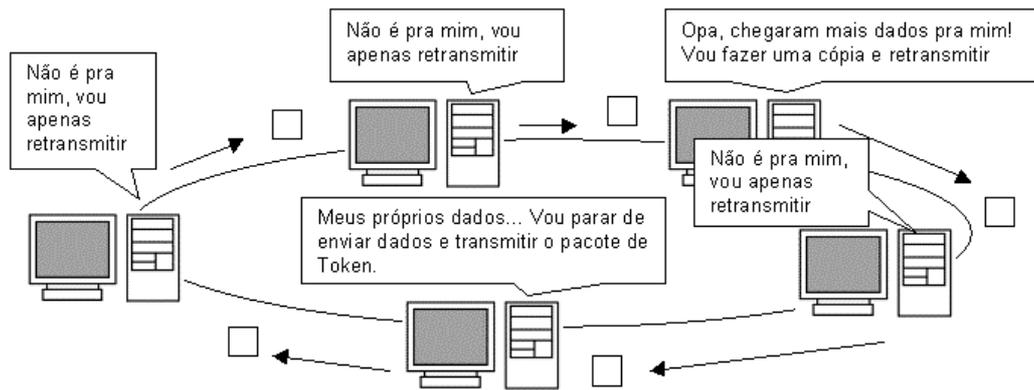
Como disse, as redes Token Ring utilizam uma topologia lógica de anel. Apesar de estarem fisicamente conectadas a um hub, as estações agem como se estivessem num grande anel. Disse anteriormente que as redes Token Ring são praticamente imunes a colisões, curioso em saber como este sistema funciona?

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 si, 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 houve 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.

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 é 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

Simplemente disponibilizar uma impressora a partir de uma estação de trabalho é a forma mais simples e barata de colocá-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 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, conecta-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

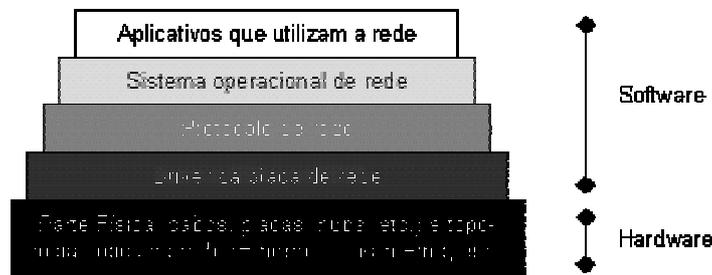
dois computadores possam se comunicar através da rede, é preciso que ambos usem o mesmo protocolo de rede.

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 si 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. O Netware não é um sistema operacional completo, e sim apenas um sistema operacional de rede que roda sobre o sistema operacional, no caso o Windows. As primeiras versões do Netware rodavam sobre o DOS.

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 de JetDirects da HP 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 sendo 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 aficionados que estava criando um aplicativo de correio eletrônico 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 conseqüentemente, 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.

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 si 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 descriptados em cerca de uma semana por alguém competente, porém a descriptação 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 acesso 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 máquina 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 lãbia 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 usando a senha do home banking que havia conseguido com a ajuda do programa.

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 sequência 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.

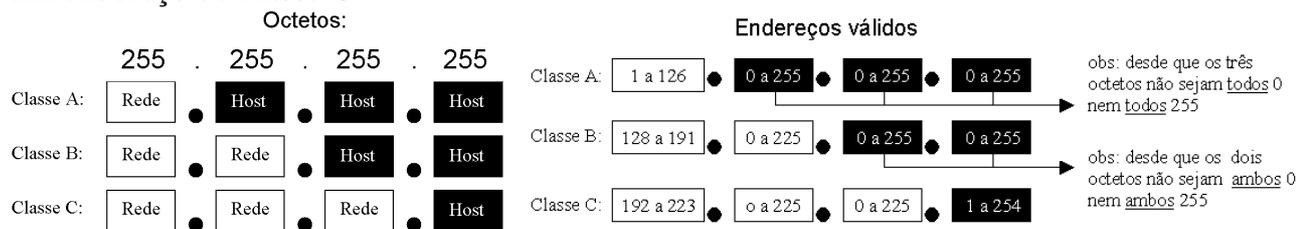
O endereço IP é dividido em duas partes. A primeira identifica a rede à qual o computador está

conectado (pois como já vimos, numa rede TCP/IP podemos ter várias redes interconectadas) 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 si. 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 projetistas 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	89.42.140.2 02	34.76.104.2 05	98.65.108.4 6
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	196.45.32.1 45	218.23.108. 45	212.23.187. 98	220.209.198 .56	198.54.89.3

Como você já 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	Argumento
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
127.xxx.xxx.xxx	Nenhum endereço IP pode começar com o número 127, pois este número é reservado para testes internos
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.

Máscara de sub-rede

Ao configurar o protocolo TCP/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.

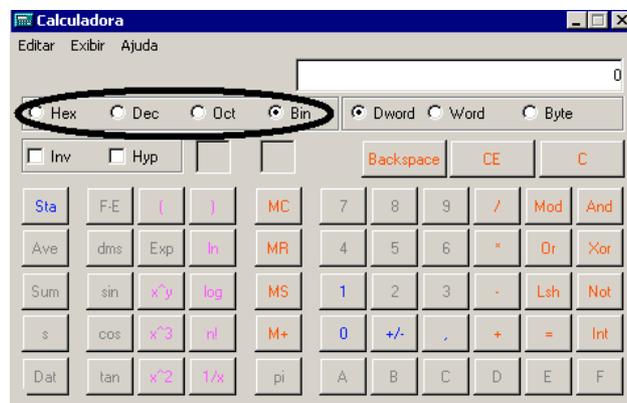
Dentro de uma mesma sub-rede, todos os hosts deverão ser configurados com a mesma máscara de sub-rede, caso contrário poderão não conseguir comunicar-se, pois pensarão estar conectados a redes diferentes. Se por exemplo temos dois micros dentro de uma mesma sub-rede, configurados com os endereços 200.133.103.1 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.

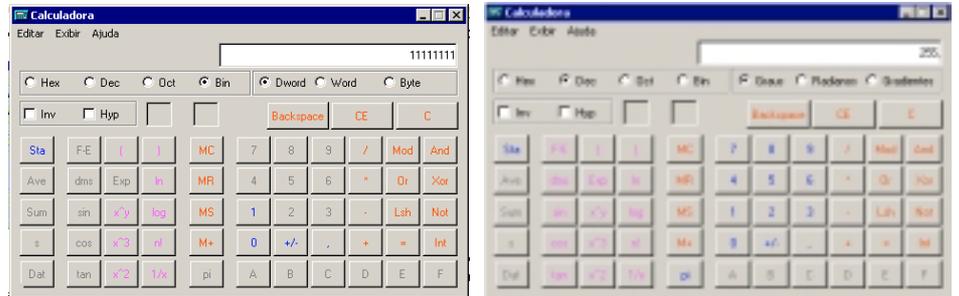
Este conceito é um pouco complicado, mas em compensação, pouca gente sabe usar este recurso, por isso vele à pena fazer um certo esforço para aprender: você vai adorar comentar sobre isso com o administrador da rede de sua empresa e ver a cara de “hein??” que ele vai fazer ;-)

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 (como na ilustração anterior) 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.

Máscara 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 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 11111111.11111111.11111111.11110000). 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 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 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 e 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”

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 default 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) e várias versões do Linux e 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 DHCP 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 DHCP 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 comunicar-se com a 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 dinamicamente 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.

Default Gateway

Um rede TCP/IP pode ser formada por várias redes interligadas entre si por roteadores. Neste caso, quando uma estação precisar transmitir algo a outra que esteja situada em uma rede diferente (ela detecta isto 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 “default gateway”, pois sem esta informação as estações simplesmente não conseguirão acessar o roteador e conseqüentemente 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.

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, ou seja um nome fantasia como “www.carlos_morimoto.com.br” 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.

Configurando uma estação de trabalho com o Windows 98

Depois de montar a parte física da rede, vamos agora para a configuração lógica das estações. O restante deste capítulo é dedicado à configuração de estações de trabalho rodando o Windows 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 mais antigas 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.

Protocolos e serviços de rede

Toda a configuração de rede do Windows 98 é feita através do ícone “rede” do painel de controle. Clicando sobre ele, temos acesso à janela de configuração de rede, que mostrará todos os componentes de rede instalados. Para adicionar novos componentes, basta clicar sobre o botão

“adicionar”. Podemos então escolher entre as categorias “cliente”, “adaptador”, “protocolo” e “serviço”.

Os componentes de rede a serem instalados dependem do tipo de rede da qual fará parte. Além da placa de rede e do protocolo de comunicação, é preciso instalar um software cliente, que permitirá acessar os recursos disponibilizados pelos demais micros da rede, e um serviço de compartilhamento, que permitirá compartilhar recursos com a rede.

Tanto o cliente de rede quanto o serviço de compartilhamento a ser instalado muda de acordo com o tipo de rede (ponto a ponto, NT ou Novell por exemplo) da qual o micro fará parte.

O Windows 98 pode ser configurado tanto como cliente de um servidor, quanto como membro de uma rede ponto a ponto. Também é possível configurá-lo para que ao mesmo tempo faça parte de uma rede ponto a ponto e tenha acesso a um servidor, bastando para isso instalar os protocolos e clientes de rede adequados.

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. Apesar de pessoalmente preferir o TCP/IP, você poderá optar pelo NetBEUI que é mais fácil de configurar e tão rápido quanto o TCP/IP dentro de redes pequenas. Se você precisar acessar um servidor Novell, então você deverá instalar também o IPX/SPX.

É recomendável, sempre que possível, manter apenas um protocolo instalado, pois ao instalar vários protocolos, mais clientes de rede etc., o Windows sempre manterá todos eles carregados. Isto tornará o sistema mais lento, e aumentará desnecessariamente o tráfego na rede. Por isso, instale apenas o que for necessário: use vários protocolos apenas quando precisar manter compatibilidade com algum recurso da rede que não aceite seu protocolo de rede padrão.

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.

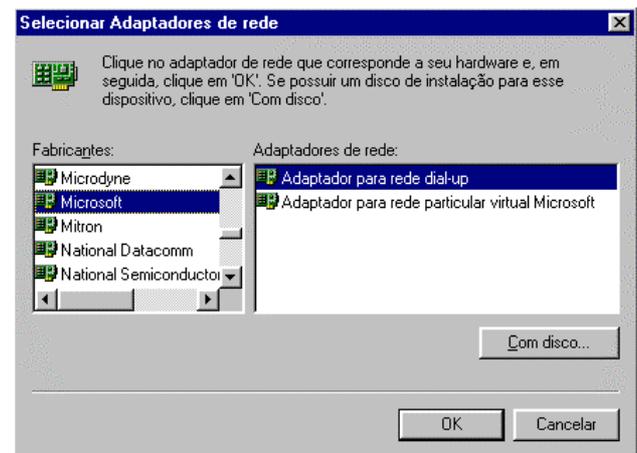
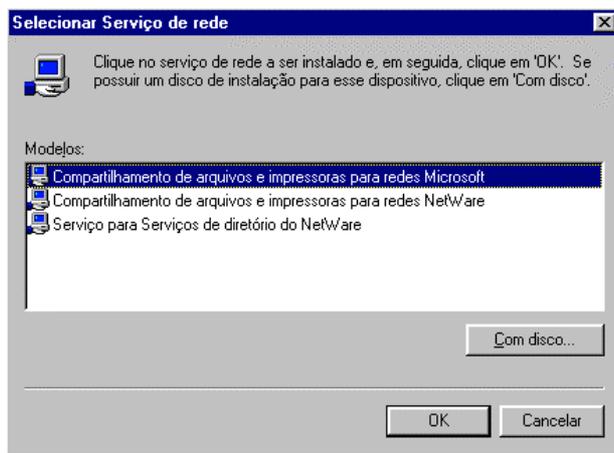
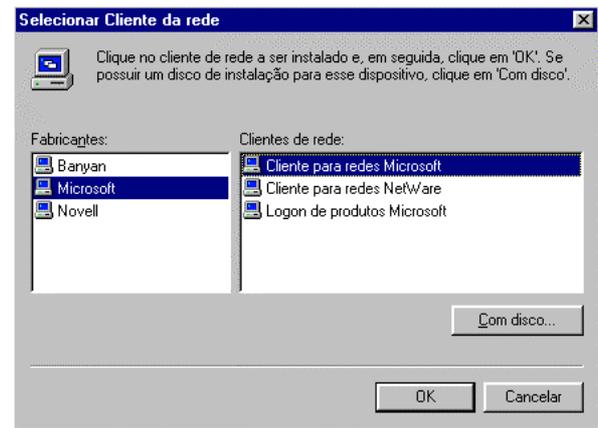


Ambiente de rede

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.

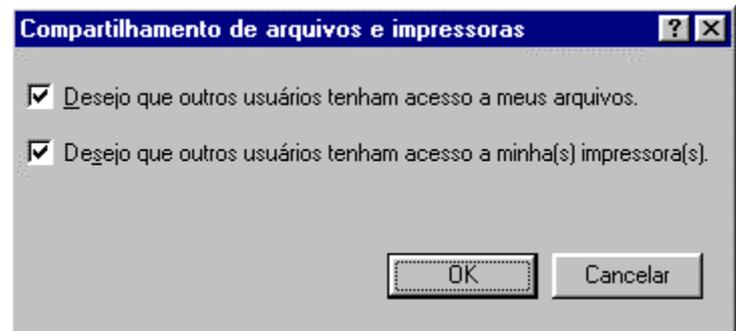
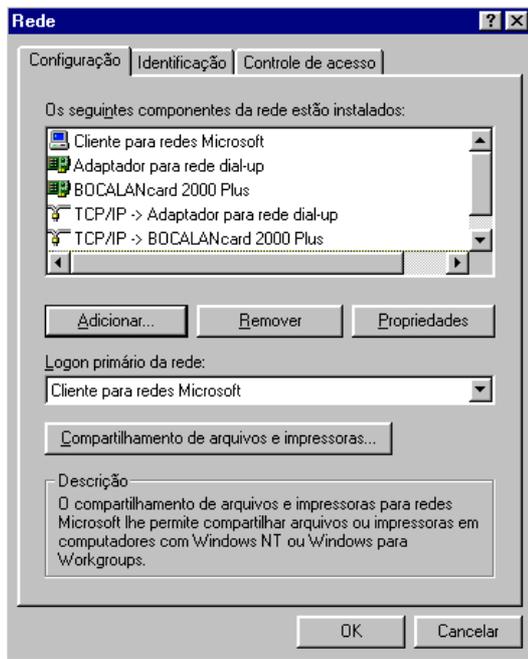
Para finalizar, volte à janela de instalação de componentes, clique em “serviço” e “adicionar”, e instale o “Compartilhamento de arquivos e impressoras para redes Microsoft”, que permitirá a você compartilhar recursos como arquivos e impressoras com outros micros da rede.

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

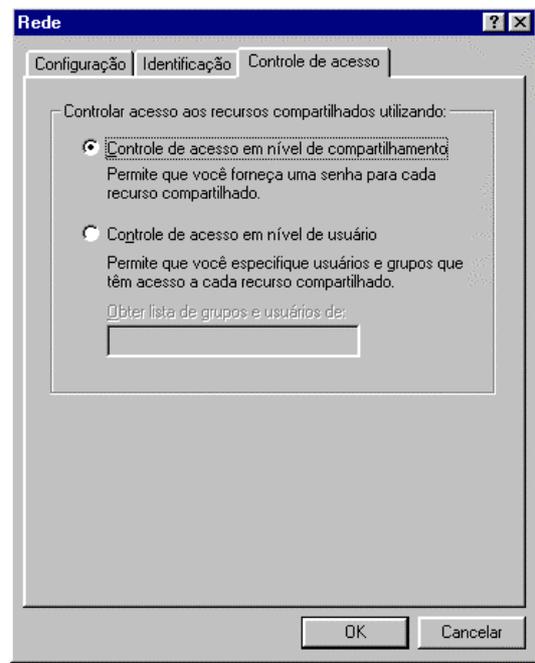
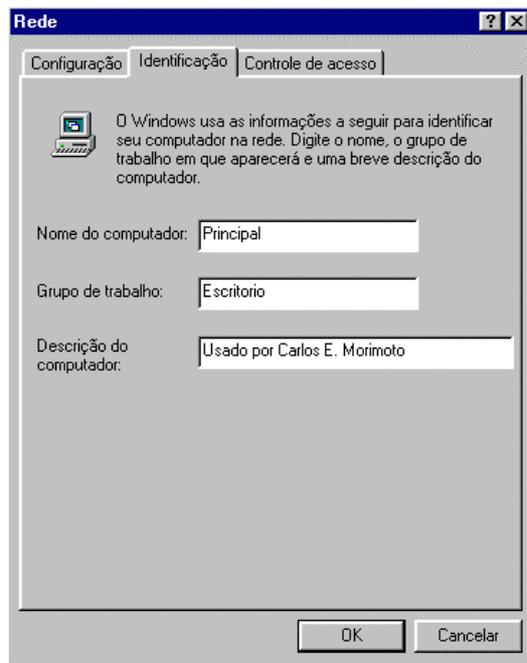
Após instalar os itens anteriores, seu ambiente de rede deverá estar como o exemplo da figura ao lado. Clique no botão “Compartilhamento de arquivos e impressoras” e surgirá um menu com duas seleções: “desejo que outros usuários tenham acesso aos meus arquivos” e “desejo que outros usuários tenham acesso 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”

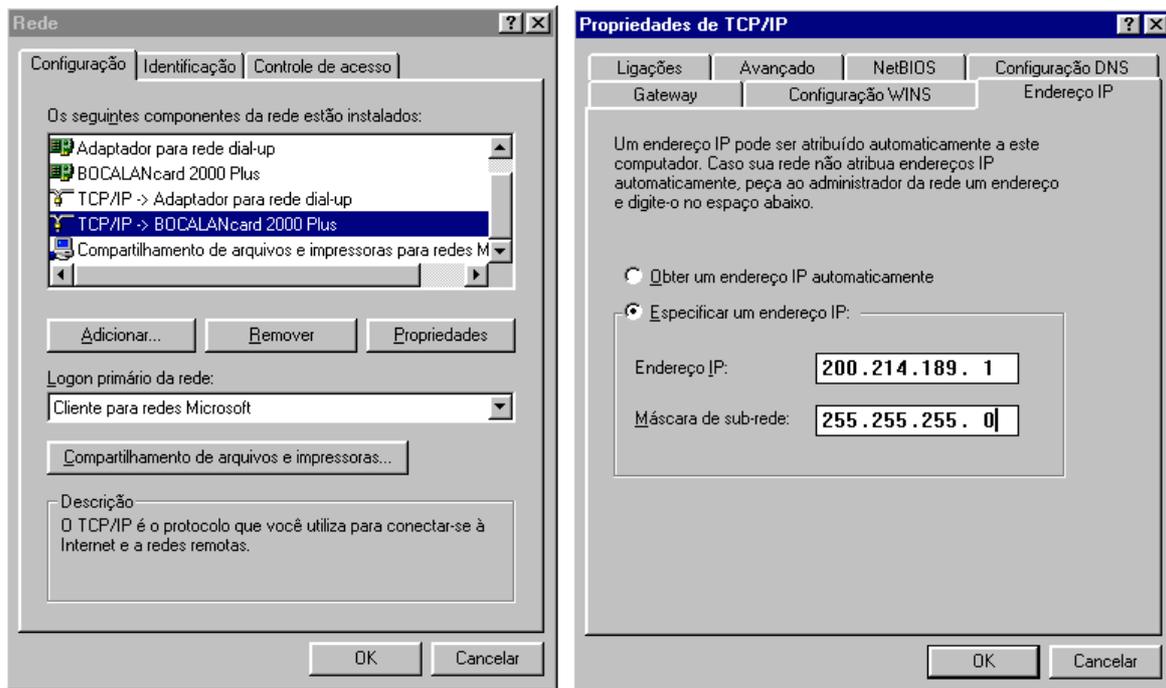
Finalmente, digite algo que descreva o micro no campo “Descrição do computador”, este campo não altera em nada a configuração ou o funcionamento da rede, mas será visto por outros usuários que acessarem recursos compartilhados pelo seu micro. Você pode digitar, por exemplo, o nome do usuário do micro, 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 (caso você o tenha instalado). 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, que aprendemos a configurar no capítulo anterior. O Campo “Obter um endereço automaticamente” deve ser escolhido apenas no caso de você possuir um servidor DHCP corretamente configurado em sua rede.



A guia “Gateway” permite especificar o endereços do ou dos roteadores que a estação usará para acessar outras redes. Este campo deverá ficar em branco caso a sua rede não possua roteadores (o mais provável). Os campos “Configuração Wins” e “Configuração DNS” permitem especificar os endereços de servidores DNS e Wins que façam parte da rede. Ambos devem ficar desativados, a menos que você tenha servidores DNS ou Wins em sua rede (novamente pouco provável ;-)

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.

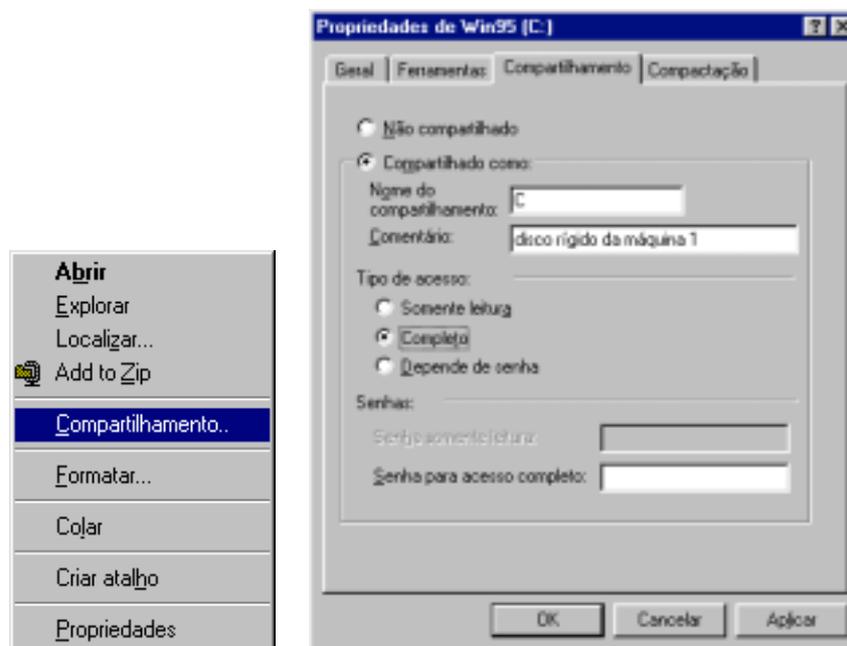
Se a tela de logon não aparecer, significa que o Windows está tendo problemas para acessar a placa de rede, e conseqüentemente a rede está indisponível. Neste caso, verifique se a placa de rede realmente funciona, se não está com nenhum tipo de conflito e se os drivers que você usou são os corretos.

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:

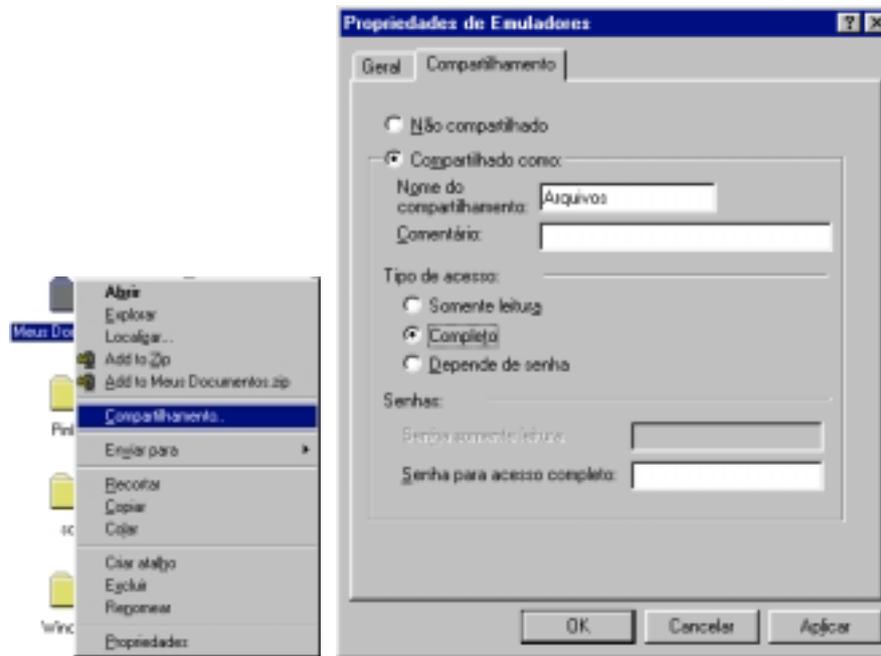
Somente leitura : Os outros usuários poderão apenas ler os arquivos do disco, mas não poderão alterar os arquivos, ou copiar nada para o disco. Você pode usar este tipo de compartilhamento para proteger, por exemplo, arquivos de programas que são acessados por vários usuários, mas que não devem ser alterados.

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

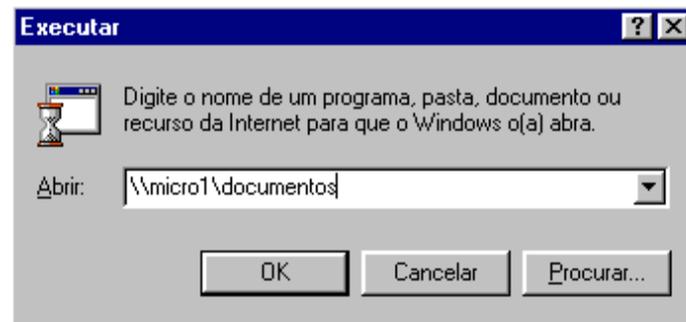
Existem 4 maneiras de acessar um disco rígido, CD-ROM ou pasta compartilhados. A primeira maneira, e a mais simples, é usar o ícone “Ambiente de Rede” que está na área de trabalho. Clicando sobre ele, surgirá uma janela mostrando todos os micros da rede que estão compartilhando algo, bastando clicar sobre cada um para acessar os compartilhamentos.



Ambiente de rede

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.

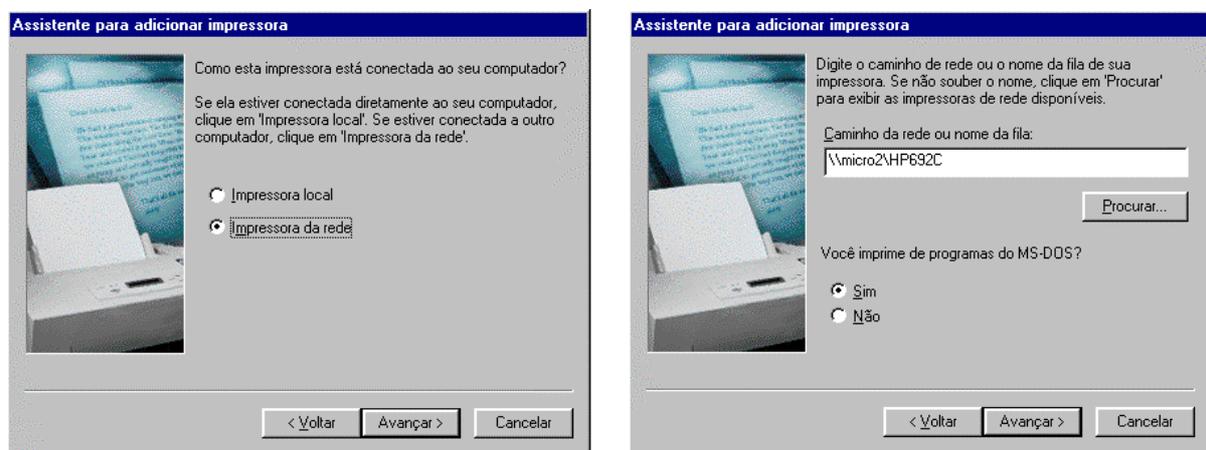
Uma unidade compartilhada também pode ser acessada através dos aplicativos, usando os comandos de abrir arquivo, salvar arquivo, inserir arquivo, etc. Esta é a quarta maneira de acessar os recursos da rede.

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 utilizá-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 é 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.

Compartilhando a conexão com a Internet

O Windows 98 Second Edition incorpora um utilitário bem prático para compartilhar uma conexão à Internet entre dois micros, chamado Internet Connection Sharing. Como a maioria das pessoas ainda acessa a Internet via modem, e como normalmente só se tem uma linha em casa, este recurso acaba sendo uma mão na roda. O primeiro micro irá atuar como um proxy, realizando as conexões solicitadas pelo micro cliente, funcionando como um intermediário entre ele e a Internet. O único problema com este tipo de ligação, é que por compartilharem a mesma conexão, ambos os micros terão o mesmo endereço IP. Isto em algumas situações causará inconvenientes: se os dois entrarem ao mesmo tempo no mesmo servidor de IRC, por exemplo, serão imediatamente desconectados, pois o servidor pensará tratar-se de clonagem, o que geralmente é proibido.

O micro que irá compartilhar a conexão deverá obrigatoriamente ter o Windows 98 Second Edition instalado. Depois de certificar-se de ter configurado a rede corretamente, basta acessar o painel de controle, adicionar/remover programas, instalação do Windows, Ferramentas de Internet e marcar a opção “Enable Internet Connection Sharing”. A máquina cliente por sua vez, pode estar rodando qualquer versão do Windows 95 ou 98. Basta criar na máquina principal, o disquete de configuração para habilitar o compartilhamento da conexão no micro cliente.

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.

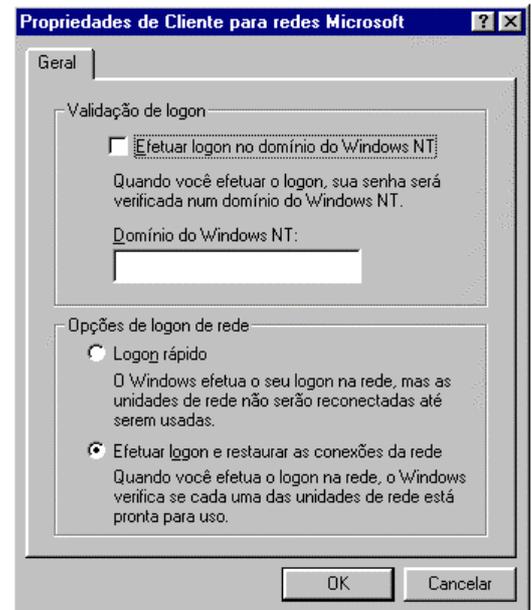
Usando o Windows 98 como cliente de um servidor NT ou Windows 2000 (a configuração da estação é a mesma para os dois), a configuração dos serviços de rede e protocolos são parecidos com os de uma rede ponto a ponto, que vimos até agora, porém, temos à disposição alguns recursos novos, principalmente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

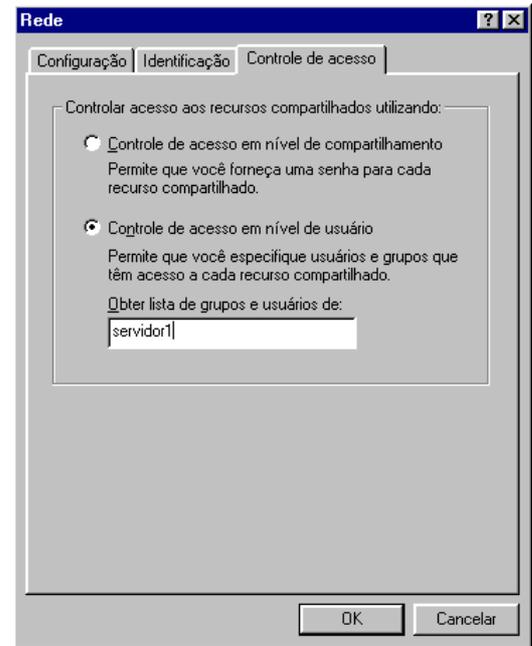
É preciso ativar esta opção para poder utilizar os recursos de perfis do usuário, scripts de logon e diretrizes de sistema permitidos pelo Windows NT e Windows 2000 Server. Ativando a opção de logar-se no servidor NT, a janela de logon que aparece quando o micro é inicializado terá, além dos campos “Nome 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.

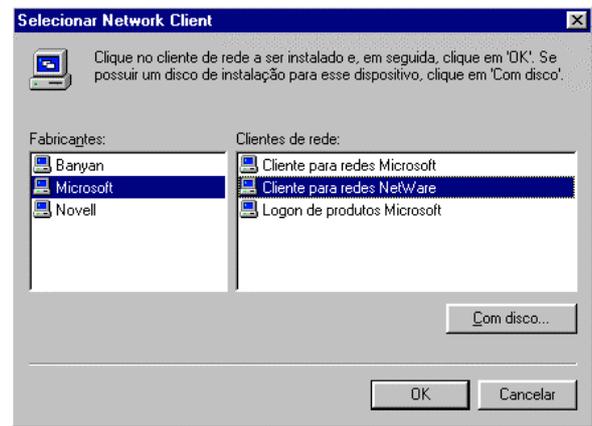
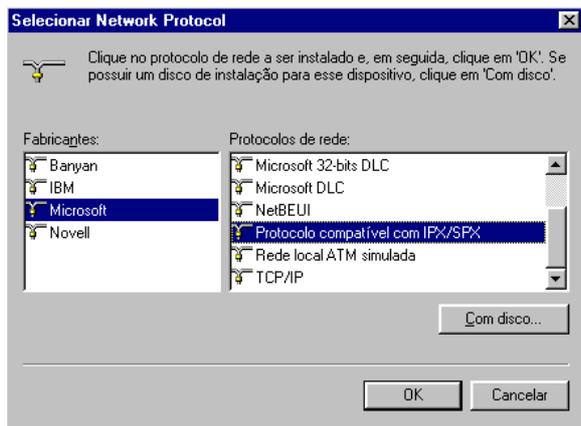
Voltando à janela principal, acesse agora a guia “controle de acesso”. Lembra-se que usando uma rede não hierárquica podíamos apenas usar a primeira opção? Pois bem, logando-se em um servidor podemos agora usar a segunda opção, “Controle de acesso a nível de usuário”, que permite especificar quais usuários 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

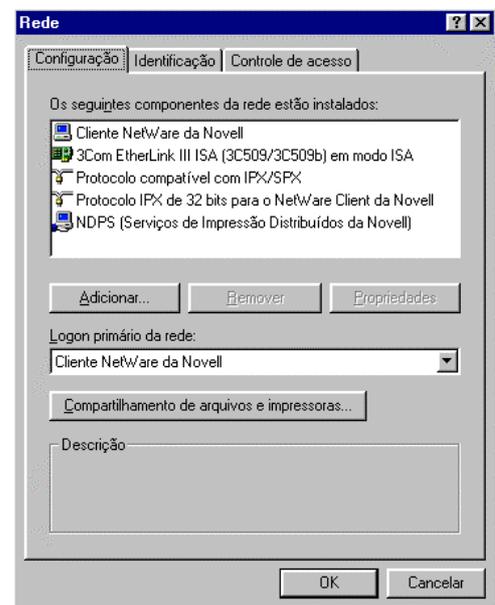
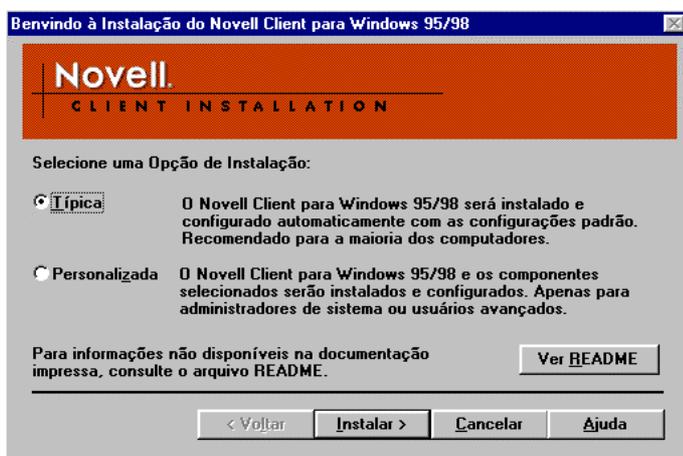
Também é perfeitamente possível usar estações com o Windows 98 para acessar servidores Novell NetWare. Para isto é necessário ter instalado o protocolo IPX/SPX e também um cliente para redes NetWare. O cliente para redes Microsoft, que usamos até agora, permite apenas acessar outras estações Windows 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 “Cliente 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 baixá-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 afirmando no nome de usuário e senha estabelecidos.



Conectando-se a uma VPN

No início deste capítulo, 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.