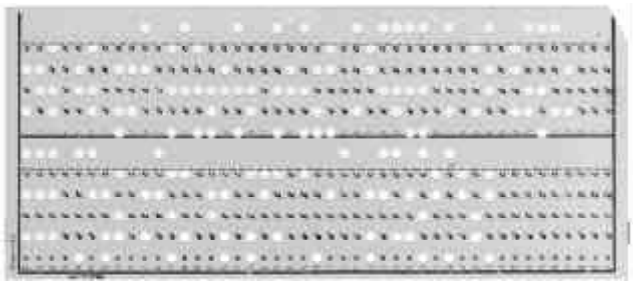
# INTRODUÇÃO

Como quase tudo na informática, as redes passaram por um longo processo de evolução antes de chegarem aos padrões utilizados atualmente. As primeiras redes de computadores foram criadas ainda durante a década de 60, como uma forma de transferir informações de um computador a outro. Na época, o meio mais usado para armazenamento externo de dados e transporte ainda eram os cartões perfurados, que armazenavam poucas dezenas de caracteres cada (o formato usado pela IBM, por exemplo, permitia armazenar 80 caracteres por cartão).

Eles são uma das formas mais lentas, trabalhosas e demoradas de transportar grandes quantidades de informação que se pode imaginar. São, literalmente, cartões de cartolina com furos, que representam os bits um e zero armazenados:



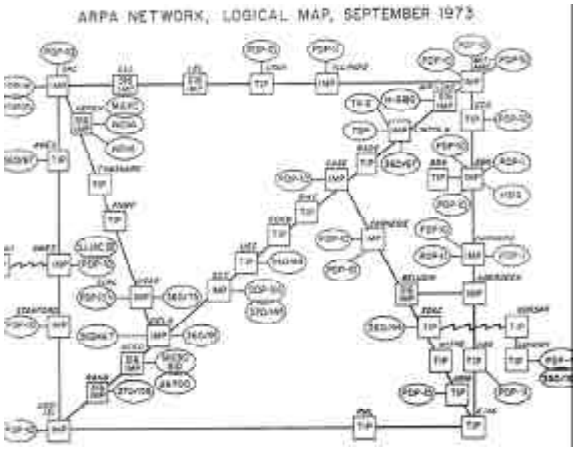
De 1969 a 1972 foi criada a Arpanet, o embrião da Internet que conhecemos hoje. A rede entrou no ar em dezembro de 1969, inicialmente com apenas 4 nós, que respondiam pelos nomes SRI, UCLA, UCSB e UTAH e eram sediados, respectivamente, no Stanford Research Institute, na Universidade da California, na Universidade de Santa Barbara e na Universidade de Utah, nos EUA. Eles eram interligados através de links de 50 kbps, criados usando linhas telefônicas dedicadas, adaptadas para o uso como link de dados.

Pode parecer pouco, mas 50 kbps em conexões de longa distância era uma velocidade impressionante para a época, principalmente se considerarmos que os modems domésticos da década de 1970 transmitiam a apenas 110 bps (bits por segundo), o que corresponde a apenas 825 caracteres de texto por minuto.

Esta rede inicial foi criada com propósitos de teste, com o desafio de interligar 4 computadores de arquiteturas diferentes, mas a rede cresceu rapidamente e em 1973 já interligava 30 instituições, incluindo universidades, instituições militares e empresas. Para garantir a operação da rede, cada nó era interligado a pelo menos dois outros (com exceção dos casos em que isso realmente não era possível), de forma que a rede pudesse continuar funcionando mesmo com a interrupção de várias das conexões.

As mensagens eram roteadas entre os nós e eventuais interrupções nos links eram detectadas rapidamente, de forma que a rede era bastante confiável. Enquanto existisse pelo menos um caminho possível, os pacotes eram roteados até finalmente chegarem ao destino, de forma muito similar ao que temos hoje na Internet.

Esta ilustração, cortesia do computerhistory.org, mostra o diagrama da Arpanet em 1973:

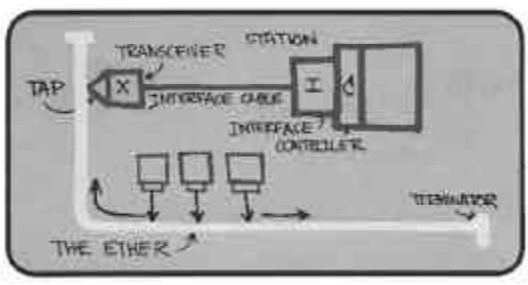



Em 1974 surgiu o TCP/IP, que acabou se tornando o protocolo definitivo para uso na ARPANET e mais tarde na Internet. Uma rede interligando diversas universidades permitiu o livre tráfego de informações, levando ao desenvolvimento de recursos que usamos até hoje, como o e-mail, o telnet e o FTP, que permitiam aos usuários conectados trocar informações, acessar outros computadores remotamente e compartilhar arquivos. Na época, mainframes com um bom poder de processamento eram raros e incrivelmente caros, de forma que eles acabavam sendo compartilhados entre diversos pesquisadores e técnicos, que podiam estar situados em qualquer ponto da rede.

Um dos supercomputadores mais poderosos da época, acessado quase que unicamente via rede, era o Cray-1 (fabricado em 1976). Ele operava a 80 MHz, executando duas instruções por ciclo, e contava com 8 MB de memória, uma configuração que só seria alcançada pelos PCs domésticos quase duas décadas depois. Esta foto do museu da NASA mostra o Cray-1 durante uma manutenção de rotina:

Com o crescimento da rede, manter e distribuir listas de todos os hosts conectados foi se tornando cada vez mais dispendioso, até que em 1980 passaram a ser usados nomes de domínio, dando origem ao "Domain Name System", ou simplesmente DNS, que é essencialmente o mesmo sistema para atribuir nomes de domínio usado até hoje.

A segunda parte da história começa em 1973 dentro do PARC (o laboratório de desenvolvimento da Xerox, em Palo Alto, EUA), quando foi feito o primeiro teste de transmissão de dados usando o padrão Ethernet. Por sinal, foi no PARC onde várias outras tecnologias importantes, incluindo a interface gráfica e o mouse, foram originalmente desenvolvidas. O teste deu origem ao primeiro padrão Ethernet, que transmitia dados a 2.94 megabits através de cabos coaxiais e permitia a conexão de até 256 estações de trabalho. Este célebre desenho, feito por Bob Metcalf, o principal desenvolvedor do padrão, ilustra o conceito:




O termo "ether" era usado para descrever o meio de transmissão dos sinais em um sistema. No Ethernet original, o "ether" era um cabo coaxial, mas em outros padrões pode ser usado um cabo de fibra óptica, ou mesmo o ar, no caso das redes wireless. O termo foi escolhido para enfatizar que o padrão Ethernet não era dependente do meio e podia ser adaptado para trabalhar em conjunto com outras mídias.

Note que tudo isso aconteceu muito antes do lançamento do primeiro micro PC, o que só aconteceu em 1981. Os desenvolvedores do PARC criaram diversos protótipos de estações de trabalho durante a década de 70, incluindo versões com interfaces gráficas elaboradas (para a época) que acabaram não entrando em produção devido ao custo. O padrão Ethernet surgiu, então, da necessidade natural de ligar estas estações de trabalho em rede.

*Xerox Alto (1973), a primeira estação de trabalho e também a primeira a ser ligada em rede.*

A taxa de transmissão de 2.94 megabits do Ethernet original era derivada do clock de 2.94 MHz usado no Xerox Alto, mas ela foi logo ampliada para 10 megabits, dando origem aos primeiros padrões Ethernet de uso geral. Eles foram então sucessivamente aprimorados, dando origem aos padrões utilizados hoje em dia.

A ARPANET e o padrão Ethernet deram origem, respectivamente, à Internet e às redes locais, duas inovações que revolucionaram a computação. Hoje em dia, poderíamos muito bem viver sem processadores dual-core e sem monitores de LCD, mas viver sem a Internet e sem as redes locais seria muito mais complicado.

Inicialmente, a ARPANET e o padrão Ethernet eram tecnologias sem relação direta. Uma servia para interligar servidores em universidades e outras instituições e a outra servia para criar redes locais, compartilhando arquivos e impressoras entre os computadores, facilitando a troca de arquivos e informações em ambientes de trabalho e permitindo o melhor aproveitamento dos recursos disponíveis. Afinal, porque ter uma impressora jato de tinta para cada micro, se você pode ter uma única impressora laser, mais rápida e com uma melhor qualidade de impressão para toda a rede?

Na década de 1990, com a abertura do acesso à Internet, tudo ganhou uma nova dimensão e as redes se popularizaram de forma assustadora, já que não demorou muito para todos perceberem que ter uma rede local era a forma mais barata de conectar todos os micros da rede à Internet.

Há apenas uma década, o acesso via linha discada ainda era a modalidade mais comum e não era incomum ver empresas onde cada micro tinha um modem e uma linha telefônica, o que multiplicava os custos. Nessas situações, locar uma linha de frame relay (uma conexão dedicada de 64 kbits, que é na verdade uma fração de uma linha T1) e compartilhar a conexão entre todos os micros acabava saindo mais barato, além de permitir que todos eles ficassem permanentemente conectados. Com a popularização das conexões de banda larga, a escolha ficou ainda mais evidente.

Hoje em dia, quase todo mundo que possui mais de um PC em casa acaba montando uma pequena rede para compartilhar a conexão entre eles, seja usando um modem ADSL configurado como roteador, seja usando um ponto de acesso wireless, seja usando um cabo cross-over para compartilhar diretamente a conexão entre dois micros. É muito difícil encontrar uma placa-mãe que já não venha com uma placa de rede onboard, ou um notebook que não traga uma placa wireless pré-instalada. O acesso à web se tornou tão ubíquo que é cada vez mais difícil encontrar utilidade para um PC desconectado da rede.

Além disso, as redes continuam cumprindo seu papel como uma forma de compartilhar recursos entre diversos micros, permitindo que você acesse arquivos, use impressoras, CD-ROMs e outros dispositivos e rode aplicativos remotamente.

Você pode usar um notebook como segundo monitor, usando-o como uma extensão da tela do seu desktop (mesmo que os dois rodem sistemas operacionais diferentes), pode usar um micro antigo como servidor de arquivos para a rede ou dar-lhe uma sobrevida como desktop, usando-o como

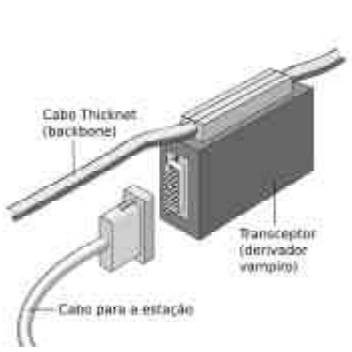
terminal de um micro mais rápido; pode usar um proxy transparente para melhorar a velocidade do acesso à web, só para citar alguns exemplos. Como veremos ao longo do livro, as possibilidades são praticamente infinitas. :)

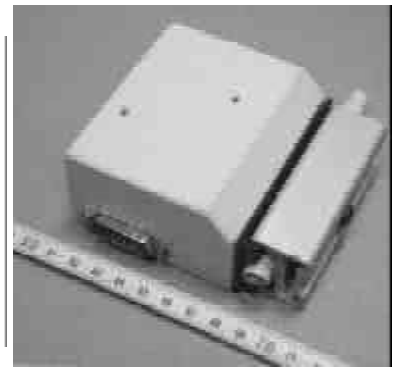
## A evolução do cabeamento

Atualmente, as redes Ethernet de 100 megabits (Fast Ethernet) e 1000 megabits (Gigabit Ethernet) são as mais usadas. Ambos os padrões utilizam cabos de par trançado categoria 5 ou 5e, que são largamente disponíveis, o que facilita a migração de um para o outro. As placas também são intercompatíveis: você pode perfeitamente misturar placas de 100 e 1000 megabits na mesma rede, mas, ao usar placas de velocidades diferentes, a velocidade é sempre nivelada por baixo, ou seja, as placas Gigabit são obrigadas a respeitar a velocidade das placas mais lentas.

Antes deles, tivemos o padrão de 10 megabits, que também foi largamente usado (e ainda pode ser encontrado em algumas instalações) e, no outro extremo, já está disponível o padrão de 10 gigabits (10G), mil vezes mais rápido que o padrão original. Tal evolução demandou também melhorias no cabeamento da rede.

As primeiras redes Ethernet utilizavam cabos thicknet, um tipo de cabo coaxial grosso e pouco flexível, com 1 cm de diâmetro. Um único cabo era usado como backbone para toda a rede e as estações eram conectadas a ele através de transceptores, também chamados de "vampire taps" ou "derivadores vampiros", nome usado porque o contato do transceptor perfurava o cabo thicknet, fazendo contato com o fio central. O transceptor era então ligado a um conector AUI de 15 pinos na placa de rede, através de um cabo menor:



Este era essencialmente o mesmo tipo de cabeamento utilizado no protótipo de rede Ethernet desenvolvido no PARC, mas continuou sendo usado durante a maior parte da década de 80, embora oferecesse diversos problemas práticos, entre eles a dificuldade em se lidar com o cabo central, que era pesado e pouco flexível, sem falar no custo dos transceptores.

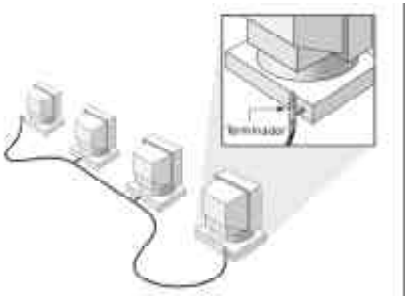
Estas redes eram chamadas de 10BASE-5, sigla que é a junção de 3 informações. O "10" se refere à velocidade de transmissão, 10 megabits, o "BASE" é abreviação de "baseband modulation", o que indica que o sinal é

transmitido diretamente, de forma digital (sem o uso de modems, como no sistema telefônico), enquanto o "5" indica a distância máxima que o sinal é capaz de percorrer, nada menos do que 500 metros.

As redes 10BASE-5 logo deram origem às redes 10BASE-2, ou redes thinnet, que utilizavam cabos RG58/U, bem mais finos. O termo "thinnet" vem justamente da palavra "thin" (fino), enquanto "thicknet" vem de "thick" (espesso).

Nelas, os transceptores foram miniaturizados e movidos para dentro das próprias placas de rede e a ligação entre as estações passou a ser feita usando cabos mais curtos, ligados por um conector em forma de T. Ele permitiu que as estações fossem ligadas diretamente umas às outras, transformando os vários cabos separados em um único cabo contínuo:

Nas duas extremidades eram usados terminadores, que fecham o circuito, evitando que os sinais que chegam ao final do cabo retornem na forma de interferência:



Apesar da importância, os terminadores eram dispositivos passivos, bastante simples e baratos. O grande problema era que, se o cabo fosse desconectado em qualquer ponto (no caso de um cabo rompido, ou com mal contato, por exemplo), toda a rede saía fora do ar, já que era dividida em dois segmentos sem terminação. Como não eram usados leds nem indicadores de conexão, existiam apenas duas opções para descobrir onde estava o problema: usar um testador de cabos (um aparelho que indicava com precisão em que ponto o cabo estava rompido, mas que era caro e justamente por isso incomum aqui no Brasil) ou sair testando ponto por ponto, até descobrir onde estava o problema.

Temos aqui o conector BNC, incluindo a ponteira e a bainha, o conector T e o terminador, que, junto com o cabo coaxial, eram os componentes básicos das redes 10BASE-2:

Os cabos podiam ser crimpados na hora, de acordo com o comprimento necessário, usando um alicate especial. A crimpagem consistia em descascar o cabo coaxial, encaixá-lo dentro do conector, crimpar a ponteira, de forma a prender o fio central e em seguida crimpar a bainha, prendendo o cabo ao conector BNC.

Assim como os alicates para crimpagem de cabos de par trançado que são vendidos atualmente, os alicates de crimpagem de cabos coaxiais não eram muito caros. Em 1997 você podia comprar um alicate simples por menos de 50 reais. Hoje em dia provavelmente custaria mais caro, já que poucas lojas ainda os comercializam:

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

Apesar de ainda ser muito susceptível a problemas, o cabeamento das redes 10BASE-2 era muito mais simples e barato do que o das redes 10BASE-5, o que possibilitou a popularização das redes, sobretudo em empresas e escritórios. Se você tiver acesso a alguns micros 386 ou 486 antigos, é provável que encontre placas de rede que ainda incluem o conector AUI (para redes 10BASE-5), como essa:

Esta placa da foto é uma placa ISA de 10 megabits, que além do conector AUI, inclui o conector BNC para cabos coaxiais thinnet e o conector RJ45 para cabos de par trançado atuais. Estas placas foram muito usadas durante o início da década de 90, o período de transição entre os três tipos de cabeamento. Naturalmente, apesar dos três conectores estarem presentes, você só podia utilizar um de cada vez. A vantagem era que você podia migrar dos cabos coaxiais para os cabos de par trançado trocando apenas o cabeamento, sem precisar trocar as placas de rede.

A única desvantagem das redes thinnet em relação às thicknet é que o uso de um cabo mais fino reduziu o alcance máximo da rede, que passou a ser de apenas 185 metros, o que de qualquer forma era mais do que suficiente para a maioria das rede locais. Por incrível que possa parecer, o obsoleto padrão 10BASE-5 foi o padrão Ethernet para fios de cobre com o maior

alcance até hoje, com seus 500 metros. Apenas os padrões baseados em fibra óptica são capazes de superar esta marca.

Continuando, independentemente do tipo, os cabos coaxiais seguem o mesmo princípio básico, que consiste em utilizar uma camada de blindagem para proteger o cabo central de interferências eletromagnéticas presentes no ambiente. Quanto mais espesso o cabo e mais grossa é a camada de blindagem, mais eficiente é o isolamento, permitindo que o sinal seja transmitido a uma distância muito maior:

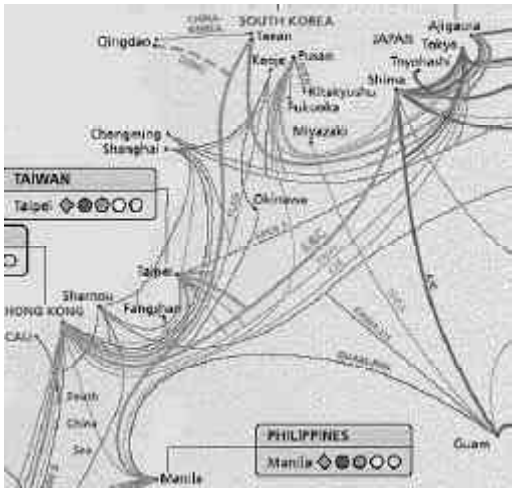
Os cabos coaxiais a muito deram lugar aos cabos de par trançado, que são praticamente os únicos usados em redes locais atualmente. Além de serem mais finos e flexíveis, os cabos de par trançado suportam maiores velocidades (podem ser usados em redes de 10, 100 ou 1000 megabits, enquanto os cabos coaxiais são restritos às antigas redes de 10 megabits) e são ainda por cima mais baratos:

Apesar disso, os cabos coaxiais estão longe de entrar em desuso. Além de serem usados nos sistemas de TV a cabo e em outros sistemas de telecomunicação, eles são usados em todo tipo de antenas, incluindo antenas para redes wireless. Até mesmo os conectores tipo N, tipicamente usados nas antenas para redes wireless de maior ganho são descendentes diretos dos conectores BNC usados nas redes 10BASE-2. Como pode ver, muitas tecnologias que pareciam ser coisa do passado, acabam retornando de formas imprevisíveis. :)

Existem diversas categorias de cabos de par trançado (como veremos em detalhes no próximo capítulo), que se diferenciam pela qualidade e pelas freqüências suportadas. Por exemplo, cabos de categoria 3, que são largamente utilizados em instalações telefônicas podem ser usados em redes de 10 megabits, mas não nas redes de 100 e 1000 megabits atuais. Da mesma forma, os cabos de categoria 5e que usamos atualmente não são adequados para as redes de 10 gigabits, que demandam cabos de categoria 6, ou 6a. Todos eles utilizam o mesmo conector, o RJ-45, mas existem diferenças de qualidade entre os conectores destinados a diferentes padrões de cabos.

Os sucessores naturais dos cabos de par trançado são os cabos de fibra óptica, que suportam velocidades ainda maiores e permitem transmitir a distâncias

praticamente ilimitadas, com o uso de repetidores. Os cabos de fibra óptica são usados para criar os backbones que interligam os principais roteadores da Internet. Sem eles, a grande rede seria muito mais lenta e o acesso muito mais caro.




*Backbones de fibra óptica interligando países da Ásia.*

Apesar disso, os cabos de fibra óptica ainda são pouco usados em redes locais, devido sobretudo à questão do custo, tanto dos cabos propriamente ditos, quanto das placas de rede, roteadores e demais componentes necessários. Apesar de tecnicamente inferiores, os cabos de par trançado são baratos, fáceis de trabalhar e tem resistido ao surgimento de novos padrões de rede.

Durante muito tempo, acreditou-se que os cabos de par trançado ficariam limitados às redes de 100 megabits e, conforme as redes gigabit se popularizassem eles entrariam em desuso, dando lugar aos cabos de fibra óptica. Mas a idéia caiu por terra com o surgimento do padrão de redes gigabit para cabos de par trançado que usamos atualmente.

A história se repetiu com o padrão 10 gigabit (que ainda está em fase inicial de adoção), que inicialmente previa apenas o uso de cabos de fibra óptica. Contrariando todas as expectativas, conseguiram levar a transmissão de dados em fios de cobre ao limite, criando um padrão de 10 gigabits para cabos de par trançado. Como demora pelo menos uma década para um novo padrão de redes se popularizar (assim foi com a migração das redes de 10 megabits para as de 100 e agora das de 100 para as de 1000), os cabos de par trançado têm sua sobrevivência assegurada por pelo menos mais uma década.

Cabos de fibra óptica multimodo.

Continuando, temos as redes wireless, que possuem uma origem ainda mais antiga. Por incrível que possa parecer, a primeira rede wireless funcional, a ALOHAnet, entrou em atividade em 1970, antes mesmo do surgimento da Arpanet.

Ela surgiu da necessidade de criar linhas de comunicação entre diferentes campus da universidade do Havaí, situados em ilhas diferentes. Na época, a estrutura de comunicação era tão precária que a única forma de comunicação era mandar mensagens escritas de barco, já que, devido à distância, não existiam sequer linhas de telefone.

A solução encontrada foi usar transmissores de rádio amador, que permitiam que nós situados nas diferentes ilhas se comunicassem com um transmissor central, que se encarregava de repetir as transmissões, de forma que elas fossem recebidas por todos os demais. A velocidade de transmissão era muito baixa, mas a rede funcionava, o que era o mais importante.

Como todos os transmissores operavam na mesma frequência, sempre que dois nós tentavam transmitir ao mesmo tempo, acontecia uma colisão e ambas as transmissões precisavam ser repetidas, o que era feito automaticamente depois de um curto espaço de tempo. Este mesmo problema ocorre nas redes wireless atuais, que naturalmente incorporam mecanismos para lidar com ele.

Voltando aos dias de hoje, vinte e oito anos depois da ALOHAnet, as redes wireless se tornaram incrivelmente populares, pois permitem criar redes locais rapidamente, sem necessidade de espalhar cabos pelo chão. Além da questão da praticidade, usar uma rede wireless pode em muitos casos sair mais barato, já que o preço de centenas de metros de cabo, combinado com o custo da instalação, pode superar em muito a diferença de preço no ponto de acesso e nas placas.

Existem dois tipos de redes wireless. As redes em modo infra-estrutura são baseadas em um ponto de acesso ou um roteador wireless, que atua como um ponto central, permitindo a conexão dos clientes. As redes ad-hoc por sua vez são um tipo de rede mesh, onde as estações se comunicam diretamente, sem o uso de um ponto de acesso. Embora tenham um alcance reduzido, as redes ad-hoc são uma forma prática de interligar notebooks em rede rapidamente, de forma a compartilhar a conexão ou jogar em rede. Como todos os notebooks hoje em dia possuem placas wireless integradas, criar uma rede ad-hoc pode ser mais rápido do que montar uma rede cabeada.

O alcance típico dos pontos de acesso domésticos são 33 metros em ambientes fechados e 100 metros em campo aberto. Apesar disso, é possível estender o sinal da rede por distâncias muito maiores, utilizando pontos de acesso e placas com transmissores mais potentes ou antenas de maior ganho (ou ambas as coisas combinadas). Desde que exista um caminho livre de obstáculos, não é muito difícil interligar redes situadas em dois prédios diferentes, a 5 km de distância, por exemplo.

Por outro lado, o sinal é facilmente obstruído por objetos metálicos, paredes, lajes e outros obstáculos, além de sofrer interferência de diversas fontes. Devido a isso, você deve procurar sempre instalar o ponto de acesso em um ponto elevado do ambiente, de forma a evitar o maior volume possível de obstáculos.

Se a idéia é permitir que seu vizinho da frente capte o sinal, então o melhor é instalar o ponto de acesso perto da janela, caso contrário o ideal é instalá-lo em uma posição central, de forma que o sinal se propague por todo o ambiente, oferecendo uma boa cobertura em qualquer parte da casa, ou do escritório, ao mesmo tempo em que pouco sinal vaze para fora.

O primeiro padrão a se popularizar foi o 802.11b, que operava a apenas 11 megabits. Ele foi seguido pelo 802.11g, que opera a 54 megabits e pelo 802.11n, que oferece até 300 megabits. Apesar disso, as redes wireless trabalham com um overhead muito maior que as cabeadas, devido à modulação do sinal, colisões e outros fatores, de forma que a velocidade real acaba sendo um pouco menos da metade do prometido. Além disso, a velocidade máxima é obtida apenas enquanto o sinal está bom e existe apenas um micro transmitindo. Conforme o sinal fica mais fraco, ou vários micros passam a transmitir simultaneamente, a velocidade vai decaindo. É por isso que algumas redes wireless acabam sendo tão lentas.

## Padrões

Existem diversos padrões Ethernet, que são utilizados pela maioria das tecnologias de rede local em uso; das placas mais baratas às redes wireless.

Estes padrões definem em detalhes a forma como os dados são organizados e transmitidos, permitindo que produtos de diferentes fabricantes funcionam perfeitamente em conjunto e são desenvolvidos pelo IEEE (Institute of Electrical and Electronics Engineers), que é provavelmente a maior organização profissional sem fins lucrativos que existe atualmente.

O IEEE é o responsável por um grande número de padrões relacionados a comunicações, eletricidade, computação e tecnologia em geral. O grupo responsável pelos padrões de rede é o "IEEE 802 LAN/MAN Standards Committee", que é por sua vez subdividido em grupos de trabalho menores, que recebem números sequenciais. Dentre eles, os quatro mais importantes são:

**802.3**: Este é o grupo responsável pelos diferentes padrões de redes Ethernet cabeadas, que inclui os algoritmos usados para a transmissão dos dados, detecção de colisões e outros detalhes. Existem diversos padrões Ethernet, que se diferenciam pela velocidade e pelo tipo de cabeamento usado. Por exemplo, o 10BASE-2 é o padrão de 10 megabits antigo, que utiliza cabos coaxiais, enquanto o 10BASE-T é o padrão de 10 megabits para cabos de par trançado.

Em seguida temos o 100BASE-T e o 1000BASE-T, que são, respectivamente, os padrões de 100 e 1000 megabits para cabos de par trançado. Embora menos usados, também existem padrões para cabos de fibra óptica, que são popularmente utilizados para criar backbones, interligando duas redes distantes.

Um dos grandes méritos do padrão Ethernet é que todos os padrões são intercompatíveis. Você pode juntar placas de velocidades diferentes na mesma rede e até mesmo misturar segmentos de rede com cabeamento diferente usando bridges. Nesses casos, as transferências entre nós de velocidades diferentes são feitas respeitando a velocidade do mais lento, mas a rede continua funcionando perfeitamente.

Na época da transição das redes com cabos coaxiais para as de par trançado, por exemplo, era comum o uso de hubs que combinavam portas para cabos de par trançado e um conector BNC, para o segmento com cabo coaxial. Estes hubs agiam como bridges, juntando as duas redes. Veremos tudo isso em mais detalhes no capítulo 1, dedicado ao cabeamento da rede e aos diferentes tipos de dispositivos usados.

**802.11**: Este é o grupo de trabalho para redes wireless, responsável pelos padrões 802.11b, 802.11a, 802.11g, 802.11i, 802.11n e outros. Com a popularização das redes wireless, o 802.11 se tornou um dos grupos de trabalho mais importantes.

No 802.11b a rede opera a 11 megabits, utilizando a faixa de freqüência dos 2.4 GHz, no 802.11a opera a 54 megabits, utilizando a faixa dos 5 GHz (menos sujeita à interferência), no 802.11g opera a 54 megabits utilizando a faixa dos 2.4 GHz (o que preserva a compatibilidade com o 802.11b), enquanto o 802.11n opera a até 300 megabits, com opção de utilizar a faixa dos 2.4 GHz ou dos 5 GHz.

Além de desenvolver padrões mais rápidos e mais acessíveis, o grupo se dedica a outra tarefa tão ou mais importante, que é o desenvolvimento de padrões de segurança, um dos problemas fundamentais das redes wireless.

Como o sinal é transmitido através do ar, não existe como impedir que outras pessoas interceptem as transmissões, tudo o que você pode fazer é embaralhar o conteúdo, de forma que ele não seja legível. É aí que entra o 802.11i, um padrão de segurança, que engloba o WPA e o WPA2, os sistemas de encriptação utilizados para proteger a rede. Estudaremos os aspectos técnicos e a configuração das redes wireless em detalhes no capítulo 3.

**802.15.1**: Este é o padrão referente ao Bluetooth, que apesar de ser mais usado em celulares e headsets, também é considerado um padrão de redes sem fio. A característica fundamental do Bluetooth é que os transmissores consomem pouca energia, o que permite que sejam usados em dispositivos muito pequenos.

**802.16**: Assim como o 802.11, o 802.16 também é um grupo de trabalho dedicado ao desenvolvimento de redes wireless. A diferença entre os dois é que o 802.11 desenvolve padrões para redes domésticas, enquanto o 802.16 trabalha no desenvolvimento de redes de longa distância, que podem ser usadas para oferecer acesso à web em grandes cidades, entre outras aplicações. O principal padrão produzido por ele é o WiMAX, que é um forte candidato a substituir as atuais redes 3G oferecidas pelas operadoras de telefonia celular no fornecimento de acesso à web nas grandes cidades.

Embora não sejam exatamente uma leitura didática, você pode obter os textos completos da maior parte dos padrões no http://ieee802.org.

## ARCNET e Token Ring

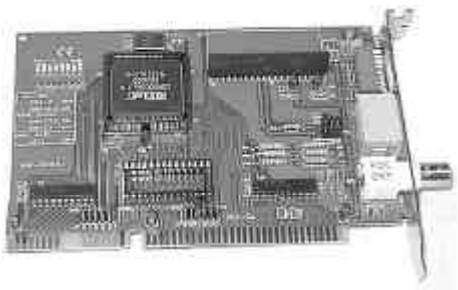
Hoje em dia, "Ethernet" é quase sinônimo de rede. Por ser um padrão aberto, qualquer fabricante pode fabricar placas e outros componentes de rede e desenvolver soluções, o que aumenta a concorrência e o volume produzido,

derrubando os preços. Dentro do cenário atual, desenvolver padrões proprietários de rede não faz muito sentido, pois além de produzir as placas o fabricante precisaria arcar com todos os custos relacionados ao desenvolvimento e à divulgação da tecnologia.

Mas, nem sempre foi assim. Durante a década de 1980 o padrão Ethernet disputava a supremacia com dois padrões então proprietários, o ARCNET e o Token Ring. Apesar de atualmente ambos serem ilustres desconhecidos, citados apenas em textos de referência histórica, eles tiveram sua época de glória. O ARCNET chegou a ser mais popular que o Ethernet e o Token Ring chegou perto de dominar as redes corporativas.

O ARCNET é o mais antigo, ele foi desenvolvido em 1976 e as primeiras placas e hubs chegaram ao mercado em 1977, a custos relativamente baixos para os padrões da época. As redes ARCNET utilizam uma topologia de estrela, que lembra bastante as das redes atuais, com o uso de um hub central e um cabo individual entre ele e cada estação. A principal diferença é que eram utilizados cabos coaxiais RG62/U e não cabos de par trançado.

Esta arquitetura era mais flexível que a dos primeiros padrões Ethernet, que ainda utilizavam uma arquitetura de barramento, com um cabo compartilhado. Temos aqui uma placa ARCNET ISA e um hub de 8 portas para cabos coaxiais:



No ARCNET os cabos podiam ter até 610 metros, mais do que em qualquer padrão Ethernet para fios de cobre e, durante muito tempo, as placas ARCNET foram mais baratas, o que fez com que a arquitetura fosse bastante popular até perto do final da década de 1980.

Os dois grandes problemas do ARCNET eram a baixa taxa de transferência, apenas 2.5 megabits, e o fato do padrão ser proprietário, o que limitou o número de fabricantes produzindo equipamentos e impediu que os preços caíssem na mesma velocidade que os Ethernet.

Eventualmente, o padrão foi aberto, dando origem ao ANSI ARCNET 878.1. Surgiram então mais opções de cabeamento, incluindo o uso de cabos de par trançado categoria 2 e cabos de fibra óptica e, em 1999, foi lançado um padrão atualizado, o ARCNET Plus, que transmitia a 20 megabits. Apesar disso, o ARCNET foi rapidamente substituído pelas redes Ethernet de 10 megabits e o lançamento do padrão de 100 megabits em 1995 acabou com qualquer chance de resistência.

O padrão Token Ring foi desenvolvido pela IBM no início da década de 1980 e também concorreu com os padrões Ethernet 10BASE-5 e 10BASE-2. A IBM

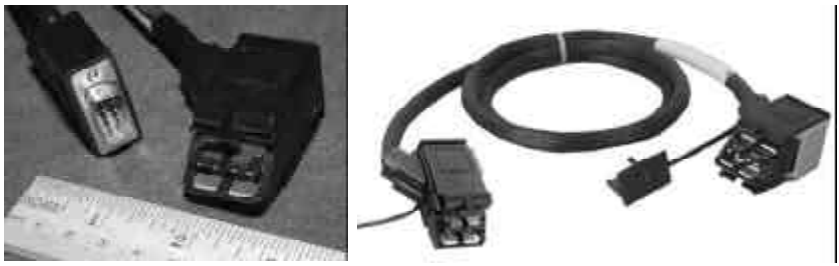
chegou a investir pesado no padrão, o que fez com que ele se tornasse popular no ambiente corporativo, embora ele seja pouco conhecido no Brasil, já que na época o país ainda estava sob a reserva de mercado.

Em 1985 o IEEE desenvolveu um padrão para redes Token Ring, o IEEE 802.5, que era compatível com o padrão da IBM. Apesar disso, a IBM manteve seu padrão proprietário, continuando a desenvolvê-lo de forma separada do padrão do IEEE. Apenas em 1992, quando as redes Token Ring já estavam em declínio, a IBM passou a licenciar a tecnologia para outros fabricantes.

No Token Ring é usada uma topologia física de estrela, com as estações sendo ligadas a hubs centrais (que no Token Ring são chamados de "MAUs", abreviação de "Multistation Access Units") através de cabos de par trançado. Os MAUs tinham tipicamente 10 portas, sendo 8 para as estações e duas para a ligação com outros MAUs:

A primeira porta era ligada ao MAU seguinte, que por sua vez era ligado ao terceiro usando a segunda porta, formando uma cadeia. A segunda porta do último MAU era então ligada ao primeiro, formando um anel.

Apesar do uso de cabos de par trançado, a IBM optou por utilizar cabos blindados e um conector quadrado agigantado, chamado de "IBM data connector". Como o conector era muito grande (media cerca de 3 x 3 cm), os cabos utilizavam o conector IBM do lado do MAU (hub) e utilizavam um conector DB9 (o mesmo utilizado nas portas seriais) do lado da estação. Apenas os cabos destinados a interligarem os MAUs utilizavam o conector IBM dos dois lados do cabo:



Mais tarde, a IBM adicionou a possibilidade de utilizar cabos de par trançado sem blindagem com conectores RJ-45 para ligar as estações ao MAU, mas ao utilizá-los o comprimento máximo dos cabos e o número máximo de estações eram reduzidos.

Embora os MAUs fossem dispositivos burros, que simplesmente encaminhavam as transmissões para todas as estações da rede, as colisões eram evitadas usando um sistema de token, onde um frame especial, de 3 bytes, era continuamente transmitido de uma estação à outra, uma de cada vez. Para transmitir, a estação esperava a chegada do token, enviada um

frame de dados, transmitia o token à estação seguinte, esperava até recebê-lo novamente, transmitia o segundo frame e assim por diante.

Este sistema de transmissão simulava um cabeamento em forma de anel, como se uma estação estivesse diretamente ligada à seguinte. Devido a isso, é comum dizer que as redes Token Ring combinam uma topologia física de estrela e uma topologia lógica de anel.

O uso do token aumentava a latência das transmissões (já que a estação precisa esperar sua vez antes de começar a transmitir), mas eliminava as colisões de pacotes, o que melhorava consideravelmente o desempenho em redes congestionadas. Apesar disso, as redes Token Ring trabalhavam a apenas 4 megabits, de forma que, embora usassem um sistema de transmissão muito menos refinado, as redes Ethernet de 10 megabits ganhavam na base da força bruta.

Em 1989 foi lançado o padrão Token Ring de 16 megabits, o que fez com que as redes Token Ring passassem a ser consideravelmente mais rápidas que as Ethernet. Apesar da vantagem técnica, a introdução do padrão 10BASE-T (com cabos de par trançado) fez com que as redes Ethernet se popularizassem rapidamente, já que eram brutalmente mais baratas.

Como eram mais caras e utilizavam um padrão mais complexo, as redes Token Ring continuaram perdendo terreno, processo que se acelerou com o lançamento do padrão Ethernet de 100 megabits e com a popularização dos switches Ethernet, que praticamente eliminam o problema das colisões, anulando, assim, a principal vantagem do Token Ring.

Em 1994, a própria IBM jogou a toalha e passou a migrar toda a sua linha de produtos para o padrão Ethernet, mantendo apenas uma estrutura mínima de suporte para atender os clientes com redes Token Ring. Hoje em dia é quase impossível encontrar referências ao Token Ring dentro do site ou da documentação técnica da IBM, embora algumas empresas menores ainda produzam placas e MAUs em pequena escala, atendendo às empresas que ainda possuem redes Token Ring instaladas.

## Uma rápida explicação do modelo OSI

Imagine que o objetivo de uma rede é simplesmente transportar os bits uns e zeros usados pelos programas de um ponto a outro. Da mesma forma que as trilhas da placa-mãe transportam informações do processador para a memória RAM, os cabos de par trançado da rede (ou os transmissores de rádio das redes wireless) permitem transportar as mesmas informações de um PC a outro.

Do ponto de vista do aplicativo, faz pouca diferença acessar um arquivo gravado diretamente no HD ou acessá-lo a partir de um compartilhamento dentro da rede, ou na Internet. Em ambos os casos, o próprio sistema operacional (com a ajuda do TCP/IP e das demais camadas que formam a rede) é quem acessa o arquivo e o entrega completo ao programa.

Entra em cena, então, o famoso **modelo OSI**, que tenta explicar o funcionamento da rede, dividindo-a em 7 camadas:

**7- Aplicação** (aqui está o programa, que envia e recebe dados através da rede)
**6- Apresentação**
**5- Sessão**
**4- Transporte** (aqui entra o protocolo TCP e o sistema operacional, que controla a transmissão dos dados, detectando problemas na transmissão e corrigindo erros)
**3- Camada de Rede** (aqui está o protocolo IP)
**2- Link de dados** (aqui estão as placas de rede e os switches)
**1- Camada Física** (aqui estão os cabos e os hubs)

Embora seja apenas um modelo teórico, que não precisa necessariamente ser seguido à risca pelos protocolos de rede, o modelo OSI é interessante, pois serve como deixa para explicar diversos aspectos teóricos do funcionamento da rede. Existem livros e cursos dedicados inteiramente ao assunto, que tentam explicar tudo detalhadamente, classificando cada coisa dentro de uma das camadas, mas na verdade entender o modelo OSI não é tão difícil assim.

Tudo começa com o aplicativo que precisa acessar alguma informação na rede. Digamos que você abriu o navegador e está acessando o http://guiadohardware.net.

Estamos na **camada 7** (aplicação), onde o programa simplesmente solicita os arquivos para o sistema operacional, sem se preocupar com o que precisa ser feito para obtê-lo. É como quando você compra um produto em uma loja online: você não está preocupado com a logística envolvida, sabe apenas que daqui a dois dias o produto vai chegar na sua casa via sedex.

Ao receber a solicitação, o sistema operacional abre uma sessão (**camada 5**). Ela funciona de uma forma semelhante a um ticket de suporte: é aberta ao receber a solicitação e fechada apenas quando o problema é resolvido, ou seja, quando o programa recebe de volta os dados que solicitou.

Como um bom atendente, o sistema operacional ficará de prontidão durante todo o processo, aguardando a resposta do servidor e verificando se todos os arquivos chegaram corretamente ao aplicativo. Caso necessário, ele solicita retransmissões dos pacotes que se perderam e, caso eventualmente não seja possível atender a solicitação (a conexão está fora do ar, por exemplo), ele reporta o erro ao aplicativo, que exibe então alguma mensagem de erro, avisando do problema.

Depois de abrir a sessão, o sistema "vai à luta": verifica qual é o endereço IP do site, qual protocolo será usado e outras informações necessárias, para então enviar a requisição ao servidor que hospeda o site, solicitando o envio dos arquivos que compõem a página. Aqui já estamos na **camada 4** (transporte), onde o sistema operacional faz o trabalho do atendente, que faz o pedido para a central de distribuição, contendo o item que será entregue e o endereço de destino.

Você pode se perguntar o que aconteceu com a **camada 6**. Não a citei no exemplo porque ela nem sempre é usada. Ela funciona como uma camada extra, que é usada quando é necessário fazer algum trabalho adicional. Um exemplo de uso para a camada 6 são os túneis encriptados criados usando o

SSH (que permite acessar máquinas rodando Linux ou outros sistemas Unix remotamente, de forma segura). Eles fazem com que os dados sejam transmitidos de forma encriptada pela rede, aumentando a segurança de forma transparente tanto para o aplicativo quanto para o sistema operacional.

Chegamos então à **camada 3** (rede), onde entra em ação o endereçamento IP. A requisição é transformada em um pacote de dados e endereçada ao endereço IP do servidor do guiadohardware.net. É como se, em vez de usar e-mail ou telefone, o pedido precisasse ser enviado via carta à central de distribuição, que responderia enviando o produto. O sistema operacional atua como o atendente que faz o pedido (camada 4, transporte) e verifica o status do envio (camada 5, sessão). O TCP/IP (camadas 4 e 3) seria representado, no exemplo, pelo trabalho dos correios, incluindo o envelope que contém os endereços do remetente e do destinatário.

Uma observação importante sobre o TCP/IP é que ele é, na verdade, composto por dois protocolos. O "TCP" trabalha no nível 4, auxiliando o sistema operacional na criação, no envio e na checagem dos pacotes, enquanto o "IP" trabalha no nível 3 e é responsável pelo endereçamento. Os dois trabalham em conjunto, como se fossem uma coisa só, muito embora sejam dois protocolos separados.

Voltando à explicação, depois de criado e endereçado corretamente, o pacote é transportado através da rede local, passando pela placa de rede, pelos cabos e pelo hub (ou switch), até chegar ao gateway da rede e, a partir daí, à Internet. É nesta fase que chegamos às **camadas 1** e **2**, onde é feito o trabalho pesado.

Em primeiro lugar, a placa de rede não entende pacotes TCP/IP, é por isso que ela é chamada de "placa Ethernet" e não "placa TCP/IP". Ela não sabe nem mesmo diferenciar um endereço IP do outro. Tudo o que ela conhece são endereços MAC (os endereços físicos das placas de rede, gravados ainda em fábrica).

Para despachar o pacote pela rede local (de forma que ele chegue até o gateway), ela o transforma em um "frame", contendo o endereço MAC da placa destino. É como se ela colocasse o envelope original dentro de outro, que usa um endereçamento mais simples.

Os endereços MAC são endereços de 48 bits, representados através de 12 dígitos hexadecimais (conjunto que engloba os caracteres 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E e F), como em "00:15:00:4B:68:DB". Os endereços MAC são gravados na ROM da própria placa, durante sua fabricação e, a menos que intencionalmente modificado, cada placa de rede possui um endereço MAC diferente. É como no dinheiro: duas cédulas só possuem o mesmo número de série se pelo menos uma delas for falsa.

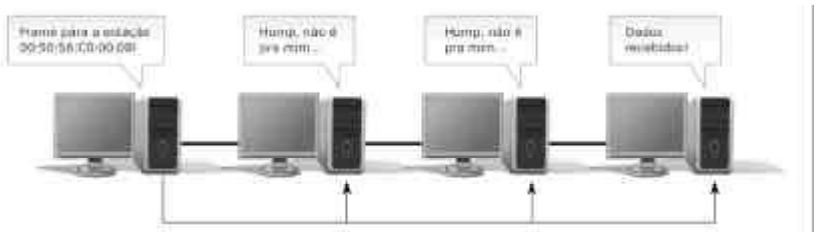
Além do endereço de origem e de destino, o frame inclui 32 bits de CRC, que são usados pela placa de destino para verificar a integridade do frame recebido. Sempre que um frame chega corrompido, a placa solicita sua retransmissão, de forma a garantir que os dados recebidos são sempre os mesmos que foram enviados. O frame é então desmontado e os dados (o pacote TCP) são entregues ao sistema operacional.

Este sistema permite que as redes Ethernet sejam usadas em redes com qualquer protocolo, sem ficarem restritas ao TCP/IP. A rede age como uma camada genérica de transporte, com suas próprias regras, que se limita a transportar informações de um ponto a outro, sem tentar entender o conteúdo dos pacotes.

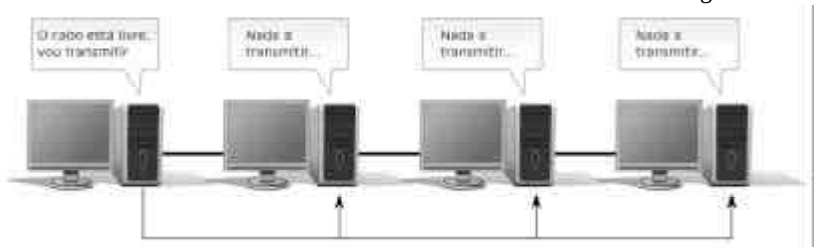
Embora os termos "frame" e "pacote" sejam freqüentemente usados como sinônimos, ao longo do livro procurarei manter o uso da designação correta, usando o termo "pacote" quando estiver me referindo aos pacotes TCP e o termo "frame" quando estiver me referindo às transmissões das placas de rede.

Hoje em dia, o TCP/IP é o protocolo dominante, mas antigamente ele concorria com um grande número de outros protocolos de rede, como o NetBEUI e IPX/SPX. Graças à neutralidade das redes Ethernet, não era necessário alterar o cabeamento da rede ao mudar de protocolo, tudo o que você precisava fazer era mudar a configuração do sistema operacional. Era possível até mesmo manter vários protocolos diferentes instalados.

Outra peculiaridade do sistema Ethernet é a forma como os dados são transmitidos. Hoje em dia, quase todas as redes locais utilizam cabos de par trançado, mas quando o padrão Ethernet foi criado, as redes ainda utilizavam cabos coaxiais, onde todas as estações eram ligadas no mesmo cabo. Porém, graças às origens, as redes Ethernet utilizam até hoje uma topologia lógica de barramento: independentemente da forma como os micros estão fisicamente interligados, eles se comportam como se estivessem todos ligados no mesmo cabo:



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 sua transmissão, caso contrário, esperará até que o cabo esteja livre. Este processo é chamado de "Carrier Sense" ou "Sensor Mensageiro":



Contudo, quando duas estações ouvem o cabo ao mesmo tempo, ambas acabam percebendo que o cabo está livre e enviam seus frames simultaneamente. Temos, então, uma colisão de dados. Para lidar com as colisões e permitir que a rede funcione apesar delas, foi implantado o sistema CSMA-CD ou "Carrier Sense Multiple Access with Collision Detection", que, apesar do nome pomposo, funciona de forma relativamente simples.

Para detectar as colisões, as estações monitoram as transmissões no cabo enquanto transmitem. Ao perceber que outra estação está transmitindo ao mesmo tempo, ela imediatamente pára de transmitir e gera um sinal de interferência, que elimina todos os dados que estiverem trafegando pelo cabo e ao mesmo tempo avisa as demais estações de que uma colisão ocorreu e que todas devem parar de transmitir.

Entra em cena então o algoritmo Binary Exponential Backoff, destinado a evitar que as estações voltem a tentar transmitir simultaneamente, entrando em um loop eterno de colisões e retransmissões.

O sistema é baseado em slots de tempo, cada um com 51.2 microssegundos, valor que corresponde ao tempo máximo que o sinal demora para percorrer o cabo e se propagar para todas as demais estações em uma rede montada dentro dos padrões.

Inicialmente, as estações escolhem entre voltar a transmitir imediatamente ou esperar 1 slot de tempo antes de voltar a retransmitir. Se houver duas estações envolvidas, a possibilidade de haver uma nova colisão é de 50%, de forma que as estações já ficam de sobreaviso. Se uma nova colisão ocorre, o número de possibilidades é dobrado e elas passam a escolher entre esperar 0 e 3 slots de tempo, reduzindo a possibilidade para 25%. Se as colisões continuarem ocorrendo, o volume de combinações vai crescendo exponencialmente, até chegar a 1024 possibilidades (de 0 a 1023 slots de tempo), na décima tentativa, que é o valor máximo permitido pelo algoritmo.

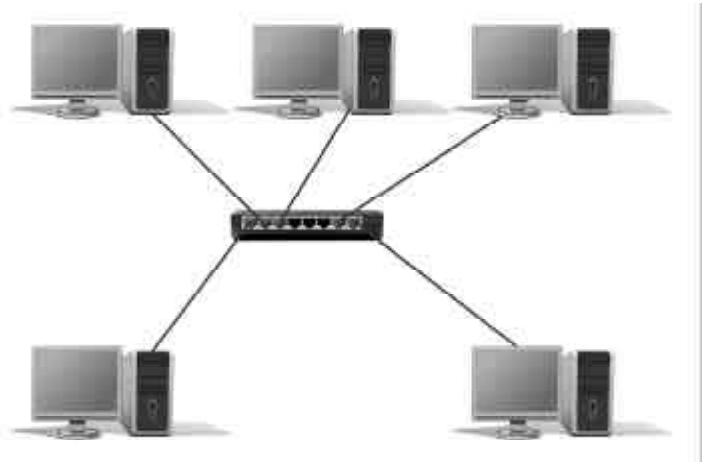
São feitas então mais 6 tentativas usando o valor máximo. Caso as colisões persistam (o que é quase impossível, a menos que exista algum problema de hardware em uma das placas ou no hub), a retransmissão é abortada e o erro é reportado ao sistema operacional. Você recebe então um erro de "conexão encerrada" ou similar.

Em situações normais, as estações conseguem transmitir na segunda ou terceira tentativa, o que causa uma perda de tempo relativamente pequena. As colisões são uma ocorrência absolutamente normal e esperada. O problema é que em redes com muitas estações, as colisões podem reduzir bastante o desempenho da rede. A solução nesses casos é dividir a rede em segmentos menores, interligados por bridges, switches ou roteadores, como veremos em detalhes no capítulo 1.

Pode parecer estranho estar falando sobre os cabos coaxiais que, felizmente, deixamos de usar há mais de uma década, mas esses mesmos princípios continuam válidos nas redes wireless, onde todos os micros estão ligados no mesmo "cabo" (o ar) e as transmissões de todos os micros da rede são recebidas por todos os demais, de forma que as colisões de pacotes são frequentes, assim como nas antigas redes com cabo coaxial.

Nas redes wireless, as colisões não se limitam aos micros da sua própria rede, mas a todos os participantes de redes próximas, que estejam operando na mesma faixa de frequência. Como você pode imaginar, isso pode rapidamente se tornar um problema em regiões densamente povoadas, como em centros financeiros e em grandes conjuntos habitacionais, como veremos em mais detalhes no capítulo 3.

Em uma rede com cabos de par trançado, temos a figura do hub (ou switch), que atua como a figura central que interliga todos os micros, criando uma topologia de estrela:



Se temos cabos separados para cada micro, você pode imaginar que não existe o problema das colisões, pois, afinal, o hub pode encaminhar as transmissões diretamente de um micro a outro. É aqui que entra diferença entre os antigos hubs e os switches, usados atualmente. Explicar a diferença entre os dois é uma boa forma de explicar a diferença entre as camadas 1 e 2 do modelo OSI.

Os hubs são dispositivos burros, que operam na camada 1. Eles não entendem pacotes nem endereços de rede, simplesmente pegam os uns e zeros que recebem em uma porta e os retransmitem para todas as outras. O hub atua simplesmente como um centralizador e repetidor, não é mais inteligente que um pedaço de cabo. Ao usar um hub, as colisões continuam ocorrendo, exatamente como aconteceria se você estivesse usando uma rede antiga, com cabo coaxial.

Os switches, por sua vez, trabalham na camada 2, assim como as próprias placas de rede. Eles entendem frames e endereços MAC e por isso são capazes de "fechar circuitos", transmitindo os frames apenas para o micro ligado na placa correta. Cada porta é ligada a um circuito separado, que são coordenados por um controlador central, que mantém uma tabela com os endereços MAC das estações ligadas a cada porta e pode assim checar o conteúdo de cada frame e encaminhá-lo à porta correta.

Apesar disso, os switches não entendem TCP/IP. Isso é trabalho para os **roteadores**, que trabalham na camada 3 e tomam suas decisões baseadas nos endereços IP dos emissores e destinatários dos pacotes, tentando sempre usar a rota mais curta.

Ao receber um frame Ethernet, o roteador descarta os endereços MAC e as demais estruturas adicionadas pela placa de rede, ficando apenas com o pacote TCP dentro dele. É por isso que não é possível usar regras de firewall baseadas em endereços MAC para hosts da Internet, ao contrário do que temos ao criar regras para os endereços da rede local.

Veremos mais detalhes sobre estas diferenças entre hubs, switches e roteadores logo a seguir, no capítulo 1. Para detalhes sobre os pacotes TCP, frames Ethernet e o uso dos endereços MAC, consulte o capítulo 4.

## Hello World

Nos livros sobre programação, quase sempre o primeiro exercício é um "Hello World" (olá mundo), onde você escreve um pequeno programa destinado a simplesmente mostrar uma mensagem na tela. Geralmente ele contém uma única linha, ou algumas poucas linhas, como este exemplo de um Hello World em C:

```
main () {
printf("Hello World");
}
```

A partir desse exemplo simples, o livro vai então se aprofundando na sintaxe da linguagem, introduzindo exercícios progressivamente mais complexos.

Em se tratando de redes, um "Hello Word" seria montar uma rede simples entre dois micros e testar a conectividade entre os dois usando o ping ou outro utilitário. Vamos então começar com este exemplo simples para "quebrar o gelo" e a partir daí vamos nos aprofundar ao longo do restante do livro.

Como comentei a pouco, praticamente todas as placas-mãe e notebooks trazem placas de rede onboard, o que torna a tarefa de montar a rede bastante simples. Existe a opção de montar a rede usando um switch, ou simplesmente usar um cabo cross-over para ligar diretamente os dois micros. Um cabo cross-over é um cabo de rede crimpado com uma sequência diferente nas duas pontas, que permite a comunicação direta entre os dois micros.

O switch ou o cabo cross-over resolvem o problema da ligação física entre os micros, o que equivale aos níveis 1 e 2 do modelo OSI. Falta agora configurar o TCP (níveis 3 e 4), de forma que eles possam efetivamente se comunicar.

Falando assim pode parecer difícil, mas na prática tudo o que você precisa fazer é usar dois endereços sequenciais (ou simplesmente escolher dois endereços diferentes dentro da mesma faixa de endereços) como "192.168.1.1" e "192.168.1.2" ou "10.0.0.1" e "10.0.0.2" e usar a mesma máscara de sub-rede em ambos:


A máscara diz qual parte do endereço IP é a identificação da rede e qual é a identificação do PC (chamado de host) dentro dela. A máscara

"255.255.255.0", por exemplo, diz que a última parte do endereço é a identificação do host e os três números iniciais são a identificação da rede, de forma que temos o host "1" e o host "2" dentro da rede "192.168.1".

Os endereços começados com "10" e "192.168" (entre outros) não são usados na Internet e por isso são livres para o uso em redes locais. Existem outros endereços reservados, além dos endereços usados para pacotes de broadcast, para a identificação da rede, para a interface de loopback e outros casos especiais e exceções que veremos ao longo do livro.

O gateway e os dois endereços de DNS são necessários para acessar a Internet. O gateway é o "portão de saída da rede", o host que tem a conexão com a Internet e roteia os pacotes dos demais. Quando você compartilha a conexão entre vários micros, o gateway da rede é sempre o PC (ou o modem ADSL) que está compartilhando a conexão. Os servidores DNS por sua vez são necessários para converter os nomes de domínio em endereços IP, o que é uma função essencial. Além dos DNS do provedor, você pode utilizar qualquer servidor público, ou mesmo instalar seu próprio servidor.

Ao usar dois notebooks, ou desktops com placas wireless, existe também a opção de criar uma rede ad-hoc, onde as duas placas wireless se comunicam diretamente, sem necessidade de usar um ponto de acesso.

Diferente do que temos ao usar um cabo cross-over, as redes ad-hoc podem conter vários PCs. Você pode inclusive compartilhar a conexão entre eles obtendo, na prática, algo próximo do que teria ao usar um ponto de acesso. A principal desvantagem é que em uma rede ad-hoc o alcance da rede é bem menor do que ao utilizar um ponto de acesso, já que a potência dos transmissores usados nas placas é menor.

Configurar a rede ad-hoc exige alguns passos adicionais, como veremos em detalhes no final do capítulo 3, mas uma vez estabelecida a conexão, a configuração dos endereços é igual à de uma rede cabeada.

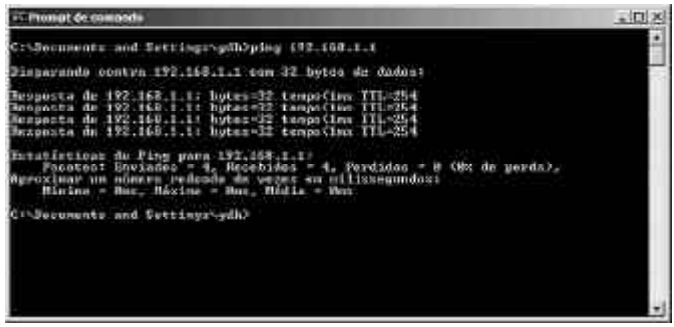
No Windows XP, você configura a rede no Painel de Controle > Conexões de Rede, acessando as propriedades da conexão e em seguida as propriedades do protocolo TCP/IP. No Linux você pode configurar o IP e ativar a rede, independentemente da distribuição usada, usando o comando "ifconfig", como em:

```
# ifconfig eth0 192.168.1.1 up
```

A menos que você tenha mais de uma placa de rede, sua placa cabeada será sempre a eth0. O "192.168.1.1" é o IP que está sendo atribuído e o "up"

conclui o comando, dizendo que a placa deve ser ativada imediatamente. Graças ao uso do TCP/IP, não temos problemas de compatibilidade ao misturar micros com Windows e Linux na rede, já que todos falam a mesma língua.

O ping é o teste mais básico para testar a conectividade entre dois micros. Ele é popular justamente porque é simples e porque está disponível em quase todos os sistemas operacionais, incluindo Linux e Windows. Para usá-lo, basta especificar o endereço, como em "ping 192.168.1.1":




No Windows o ping é executado 4 vezes, enquanto no Linux ele fica sendo executado indefinidamente até que você encerre o comando pressionando "Ctrl+C", ou fechando o terminal. Na versão Linux, você pode também especificar um número de repetições usando o parâmetro "-c" ou especificar um intervalo, usando o parâmetro "-i". Para emitir uma sequência de 15 pings, com intervalo de 30 segundos entre cada um, por exemplo, você usaria o comando "ping -c 15 -i 30 endereço-de-destino".

O ping indica o tempo que o sinal demora para ir de um micro a outro, incluindo o tempo da resposta, o que permite medir a latência da conexão. No screenshot anterior, por exemplo, o tempo de resposta é menor que 1 ms, já que são dois micros dentro da rede local, mas na Internet é muito difícil obter pings inferiores a 100 ms. No caso de servidores distantes, ou no caso de conexões via celular, ou via satélite, não é incomum obter pings de 1000 ms ou mais. Um ping elevado não chega a atrapalhar tanto na hora de navegar ou baixar e-mails, mas é fatal ao rodar games multiplayer, sobretudo nos jogos de tiro em primeira pessoa.

Como o ping pode ser bloqueado no firewall (e muitos o fazem por padrão), o fato de um host da Internet não responder ao ping não significa que ele não esteja lá, apenas que não está respondendo a suas requisições.

Uma forma mais segura (e mais invasiva) de descobrir se o host está online é usar o nmap para localizar portas abertas. Dessa forma, se o host estiver com pelo menos uma porta aberta, ele aparece no teste, mesmo que o firewall tenha sido configurado para bloquear pings. Em uma máquina Linux (com o nmap instalado), você poderia testar cada uma das 65536 portas TCP de um micro da rede rodando (como root) o comando abaixo:

```
# nmap -sS -P0 -p 0-65535 192.168.1.1
```

Ferramentas como o nmap são genericamente chamadas de portscans, ou seja, scanners de portas. A função deles é testar cada uma das portas disponíveis, verificando quais serviços estão ativos na máquina de destino.

Em geral, eles são o ponto de partida para um ataque, já que permitem descobrir quais portas estão abertas e quais serviços estão ativos, o que dá uma boa idéia sobre os pontos vulneráveis da máquina, mas eles podem ser usados também para melhorar a segurança da sua rede e encontrar falhas de segurança, como veremos em mais detalhes no capítulo 5.

Depois de testada a conectividade entre os dois micros, a rede está pronta para ser usada. Você pode aproveitar para compartilhar arquivos, jogar uma partida de algum game em rede, compartilhar a impressora, acessar o outro micro remotamente, compartilhar a conexão ou qualquer outra coisa que tenha em mente. Hoje em dia, praticamente tudo pode ser feito via rede. Se você quiser ir direto à ação, pode dar uma olhada no capítulo 6, onde veremos diversos exemplos práticos.