

ciona, oficialmente, seu status de nível 1. Como se costuma dizer, se você tiver de perguntar se é um membro de um grupo, provavelmente não é.

Um ISP de nível 2 normalmente tem alcance regional ou nacional e (o que é importante) conecta-se apenas a uns poucos ISPs de nível 1 (veja Figura 1.15).

Assim, para alcançar uma grande parcela da Internet global, um ISP de nível 2 tem de direcionar o tráfego por um dos ISPs de nível 1 com o qual está conectado. Um ISP de nível 2 é denominado um cliente do ISP de nível 1 com o qual está conectado, que, por sua vez, é denominado provedor de seu cliente. Muitas empresas de grande porte e instituições conectam suas redes corporativas diretamente a um provedor de nível 1 ou 2, tornando-se, desse modo, cliente daquele ISP. O provedor ISP cobra uma tarifa de seu cliente, que normalmente depende da taxa de transmissão do enlace que interliga ambos. Uma rede de nível 2 também pode preferir conectar-se diretamente a outras redes de mesmo nível, caso em que o tráfego pode fluir entre as duas sem ter de passar por uma rede de nível 1. Abaixo dos ISPs de nível 2 estão os de níveis mais baixos que se conectam à Internet por meio de um ou mais ISPs de nível 2 e, na parte mais baixa da hierarquia, estão os ISPs de acesso. Para complicar ainda mais as coisas, alguns provedores de nível 1 também são provedores de nível 2 (isto é, integrados verticalmente) e vendem acesso para Internet diretamente a usuários finais e provedores de conteúdo, bem como os ISPs de níveis mais baixos. Quando dois ISPs estão ligados diretamente um ao outro são denominados pares (peers) um do outro. Um estudo interessante [Subramanian, 2002] procura definir mais exatamente a estrutura em níveis da Internet estudando sua topologia em termos de relacionamentos cliente-provedor e entre parceiros (peer-peer). Para uma discussão mais clara sobre esses relacionamentos, veja Van der Berg, 2008.

Dentro da rede de um ISP, os pontos em que ele se conecta a outros ISPs (seja abaixo, acima ou no mesmo nível na hierarquia) são conhecidos como pontos de presença (*points of presence* — POPs). Um POP é simplesmente um grupo de um ou mais roteadores na rede do ISP com os quais roteadores em outros ISPs, ou em redes pertencentes a clientes do ISP, podem se conectar. Um provedor de nível 1 normalmente tem muitos POPs espalhados por diferentes localidades geográficas em sua rede e várias redes clientes e outros ISPs ligados a cada POP. Para se conectar ao POP de um provedor, uma rede cliente normalmente aluga um enlace de alta velocidade de um provedor de telecomunicações de terceiros e conecta um de seus roteadores diretamente a um roteador no POP do provedor. Dois ISPs de nível 1 também podem formar um par conectando um par de POPs, cada um proveniente de um dos dois ISPs. Além disso, dois ISPs podem ter vários pontos de emparelhamento conectando-se um ao outro em dois ou mais de pares de POPs.

Resumindo, a topologia da Internet é complexa, consistindo em dezenas de ISPs de níveis 1 e 2 e milhares de ISPs de níveis mais baixos. A cobertura dos ISPs é bastante diversificada; alguns abrangem vários continentes e oceanos e outros se limitam a pequenas regiões do mundo. Os ISPs de níveis mais baixos conectam-se a ISPs de níveis mais altos e estes (normalmente) se interconectam uns com os outros. Usuários e provedores de conteúdo são clientes de ISPs de níveis mais baixos e estes são clientes de ISPs de níveis mais altos.

1.4 Atraso, perda e vazão em redes de comutação de pacotes

Na Seção 1.1 dissemos que a Internet pode ser vista como uma infraestrutura que fornece serviços a aplicações distribuídas que são executadas nos sistemas finais. De modo ideal, gostaríamos que os serviços da Internet transferissem tantos dados quanto desejamos entre dois sistemas finais, instantaneamente, sem nenhuma perda. Infelizmente, esse é um objetivo elusivo, algo inalcançável. Ao contrário disso, as redes de computador, necessariamente, restringem a vazão (a quantidade de dados por segundo que podem ser transferidos) entre sistemas finais, apresentam atrasos entre sistemas finais e podem perder pacotes. Por um lado, infelizmente as leis físicas da realidade introduzem atraso e perda, bem como restringem a vazão. Por outro lado, como as redes de computadores possuem esses problemas, existem muitas questões fascinantes sobre como lidar com eles — mais do que questões suficientes para frequentar um curso de rede de computadores e motivar centenas de teses de doutorado! Nesta seção, começaremos a examinar e quantificar atraso, perda e vazão em redes de computadores.

1.4.1 Uma visão geral de atraso em redes de comutação de pacotes

Lembre-se de que um pacote começa em um sistema final (a origem), passa por uma série de roteadores e termina sua jornada em um outro sistema final (o destino). Quando um pacote viaja de um nó (sistema final ou roteador) ao nó subsequente (sistema final ou roteador), sofre, ao longo desse caminho, diversos tipos de atraso em *cada* nó existente no caminho. Os mais importantes deles são o atraso de processamento nodal, o atraso de fila, o atraso de transmissão e o atraso de propagação; juntos, eles se acumulam para formar o atraso nodal total. Para entender a fundo a comutação de pacotes e redes de computadores, é preciso entender a natureza e a importância desses atrasos.

Tipos de atraso

Vamos examinar esses atrasos no contexto da Figura 1.16. Como parte de sua rota fim a fim entre origem e destino, um pacote é enviado do nó anterior por meio do roteador A até o roteador B. Nossa meta é caracterizar o atraso nodal no roteador A. Note que este tem um enlace de saída que leva ao roteador B. Esse enlace é precedido de uma fila (também conhecida como buffer). Quando o pacote chega ao roteador A, vindo do nó anterior, o roteador examina o cabeçalho do pacote para determinar o enlace de saída apropriado e então o direciona ao enlace. Nesse exemplo, o enlace de saída para o pacote é o que leva ao roteador B. Um pacote pode ser transmitido por um enlace somente se não houver nenhum outro pacote sendo transmitido por ele e se não houver outros pacotes à sua frente na fila. Se o enlace estiver ocupado, ou com pacotes à espera, o pacote recém-chegado entrará na fila.

Atraso de processamento

O tempo requerido para examinar o cabeçalho do pacote e determinar para onde direcioná-lo é parte do atraso de processamento, que pode também incluir outros fatores, como o tempo necessário para verificar os erros em bits existentes no pacote que ocorreram durante a transmissão dos bits desde o nó anterior ao roteador A. Atrasos de processamento em roteadores de alta velocidade normalmente são da ordem de microssegundos, ou menos. Depois desse processamento nodal, o roteador direciona o pacote à fila que precede o enlace com o roteador B. (No Capítulo 4, estudaremos os detalhes da operação de um roteador.)

Atraso de fila

O pacote sofre um atraso de fila enquanto espera para ser transmitido no enlace. O tamanho desse atraso para um pacote específico dependerá da quantidade de outros pacotes que chegarem antes e que já estiverem na fila esperando pela transmissão. Se a fila estiver vazia, e nenhum outro pacote estiver sendo transmitido naquele momento, então o tempo de fila de nosso pacote será zero. Por outro lado, se o tráfego estiver pesado e houver muitos pacotes também esperando para ser transmitidos, o atraso de fila será longo. Em breve, veremos que o número de pacotes que um determinado pacote provavelmente encontrará ao chegar é uma função da intensi-

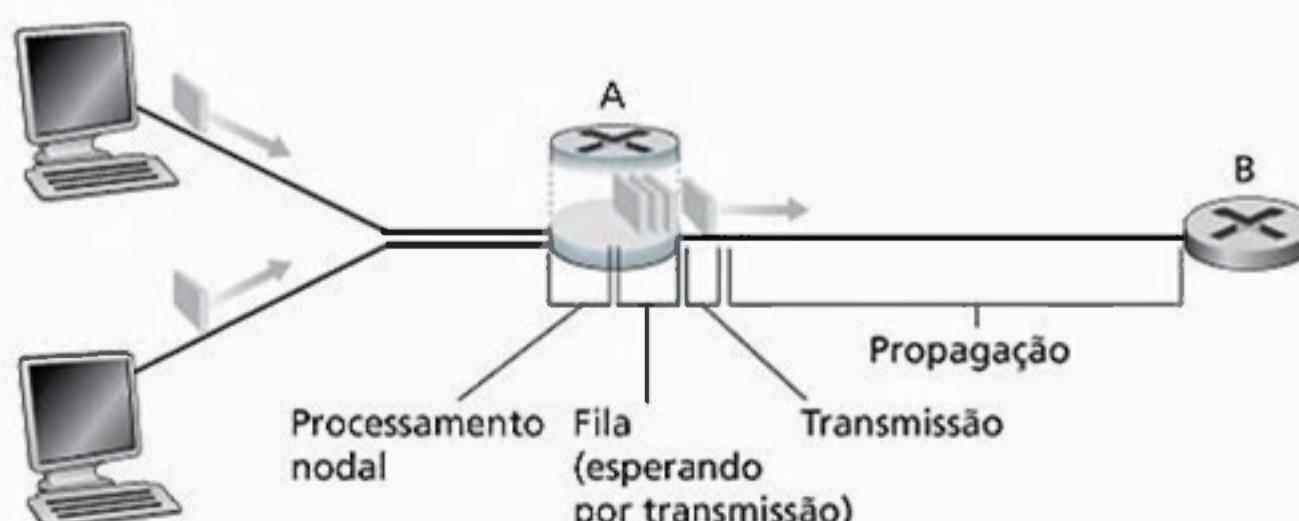


Figura 1.16 O atraso nodal no roteador A

dade e da natureza do tráfego que está chegando à fila. Na prática, atrasos de fila podem ser da ordem de micro a milissegundos.

Atraso de transmissão

Admitindo-se que pacotes são transmitidos segundo a estratégia de “o primeiro a chegar será o primeiro a ser processado”, como é comum em redes de comutação de pacotes, nosso pacote somente poderá ser transmitido depois que todos aqueles que chegaram antes tenham sido enviados. Denominemos o tamanho do pacote como L bits e a velocidade de transmissão do enlace do roteador A ao roteador B como R bits/s. A velocidade R é determinada pela velocidade de transmissão do enlace ao roteador B. Por exemplo, para um enlace Ethernet de 10 Mbps, a velocidade é $R \cdot 10$ Mbps; para um enlace Ethernet de 100 Mbps, a velocidade é $R \cdot 100$ Mbps. O atraso de transmissão (também denominado atraso de armazenamento e reenvio, como discutimos na Seção 1.3) é L/R . Esta é a quantidade de tempo requerida para empurrar (isto é, transmitir) todos os bits do pacote para o enlace. Na prática, atrasos de transmissão são comumente da ordem de micro a milissegundos.

Atraso de propagação

Assim que é lançado no enlace, um bit precisa se propagar até o roteador B. O tempo necessário para propagar o bit desde o início do enlace até o roteador B é o atraso de propagação. O bit se propaga à velocidade de propagação do enlace, a qual depende do meio físico do enlace (isto é, fibra ótica, par de fios de cobre trançado e assim por diante) e está na faixa de

$$2 \cdot 10^8 \text{ m/s} \text{ a } 3 \cdot 10^8 \text{ m/s}$$

que é igual à velocidade da luz, ou um pouco menor. O atraso de propagação é a distância entre dois roteadores dividida pela velocidade de propagação. Isto é, o atraso de propagação é d/s , onde d é a distância entre o roteador A e o roteador B, e s é a velocidade de propagação do enlace. Assim que o último bit do pacote se propagar até o nó B, ele e todos os outros bits precedentes do pacote serão armazenados no roteador B. Então, o processo inteiro continua, agora com o roteador B executando a retransmissão. Em redes WAN, os atrasos de propagação são da ordem de milissegundos.

Comparação entre atrasos de transmissão e de propagação

Os principiantes na área de redes de computadores às vezes tem dificuldade para entender a diferença entre atraso de transmissão e atraso de propagação. A diferença é sutil, mas importante. O atraso de transmissão é a quantidade de tempo requerida para o roteador empurrar o pacote para fora; é uma função do comprimento do pacote e da taxa de transmissão do enlace, mas nada tem a ver com a distância entre os dois roteadores. O atraso de propagação, por outro lado, é o tempo que leva para um bit se propagar de um roteador até o seguinte; é uma função da distância entre os dois roteadores, mas nada tem a ver com o comprimento do pacote ou com a taxa de transmissão do enlace.

Podemos esclarecer melhor as noções de atrasos de transmissão e de propagação com uma analogia. Considere uma rodovia que tenha um posto de pedágio a cada 100 quilômetros, como mostrado na Figura 1.17. Imagine que os trechos da rodovia entre os postos de pedágio sejam enlaces e que os postos de pedágio sejam roteadores. Suponha que os carros trasguem (isto é, se propaguem) pela rodovia a uma velocidade de 100 km/h (isto é, quando o carro sai de um posto de pedágio, acelera instantaneamente até 100 km/h e mantém essa velocidade entre os dois postos de pedágio). Agora, suponha que dez carros viajem em comboio, um atrás do outro, em ordem fixa. Imagine que cada carro seja um bit e que o comboio seja um pacote. Suponha ainda que cada posto de pedágio libere (isto é, transmita) um carro a cada 12 segundos, que seja tarde da noite e que os carros do comboio sejam os únicos na estrada. Por fim, suponha que, ao chegar a um posto de pedágio, o primeiro carro do comboio aguarde na entrada até que os outros nove cheguem e formem uma fila atrás dele. (Assim, o comboio inteiro deve ser ‘armazenado’ no posto de pedágio antes de começar a ser ‘reenviado’.) O tempo necessário para que todo o comboio passe pelo posto de pedágio e volte à estrada é de $(10 \text{ carros})/(5 \text{ carros/minuto}) = 2 \text{ minutos}$. Esse tempo é análogo ao atraso de transmissão em um roteador. O tempo necessário para um carro trasregar da

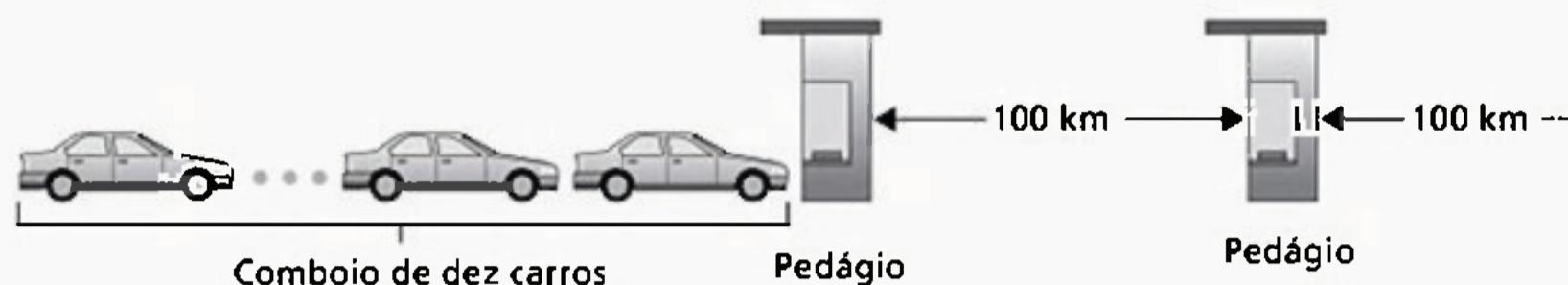


Figura 1.17 Analogia do comboio

saída de um posto de pedágio até o próximo posto de pedágio é de $(100 \text{ km})/(100 \text{ km/h}) = 1 \text{ hora}$. Esse tempo é análogo ao atraso de propagação. Portanto, o tempo decorrido entre o instante em que o comboio é ‘armazenado’ em frente a um posto de pedágio até o instante em que é ‘armazenado’ em frente ao seguinte é a soma do atraso de transmissão e do atraso de propagação — nesse exemplo, 62 minutos.

Vamos explorar um pouco mais essa analogia. O que aconteceria se o tempo de liberação do comboio no posto de pedágio fosse maior do que o tempo que um carro leva para trasegar entre dois postos? Por exemplo, suponha que os carros traseguem a uma velocidade de 1.000 km/h e que o pedágio libere um carro por minuto. Então, o atraso de trânsito entre dois postos de pedágio é de 6 minutos e o tempo de liberação do comboio no posto de pedágio é de 10 minutos. Nesse caso, os primeiros carros do comboio chegarão ao segundo posto de pedágio antes que os últimos carros saiam do primeiro posto. Essa situação também acontece em redes de comutação de pacotes — os primeiros bits de um pacote podem chegar a um roteador enquanto muitos dos remanescentes ainda estão esperando para ser transmitidos pelo roteador precedente.

Se uma imagem vale mil palavras, então uma animação vale um milhão. O Companion Website apresenta um aplicativo interativo Java que ilustra e contrasta o atraso de transmissão e o atraso de propagação. Recomenda-se que o leitor visite esse aplicativo.

Se d_{proc} , d_{fila} , d_{trans} e d_{prop} forem, respectivamente, os atrasos de processamento, de fila, de transmissão e de propagação, então o atraso nodal total é dado por:

$$d_{\text{total}} = d_{\text{proc}} + d_{\text{fila}} + d_{\text{trans}} + d_{\text{prop}}$$

A contribuição desses componentes do atraso pode variar significativamente. Por exemplo, d_{prop} pode ser desprezível (por exemplo, dois microssegundos) para um enlace que conecta dois roteadores no mesmo campus universitário; contudo, é de centenas de milissegundos para dois roteadores interconectados por um enlace de satélite geoestacionário e pode ser o termo dominante no d_{total} . De maneira semelhante, d_{trans} pode variar de desprezível a significativo. Sua contribuição normalmente é desprezível para velocidades de transmissão de 10 Mbps e mais altas (por exemplo, em LANs); contudo, pode ser de centenas de milissegundos para grandes pacotes de Internet enviados por enlaces de modems discados de baixa velocidade. O atraso de processamento, d_{proc} , é quase sempre desprezível; no entanto, tem forte influência sobre a produtividade máxima de um roteador, que é a velocidade máxima com que ele pode encaminhar pacotes.

1.4.2 Atraso de fila e perda de pacote

O mais complicado e interessante componente do atraso nodal é o atraso de fila, d_{fila} . Realmente, o atraso de fila é tão importante e interessante em redes de computadores que milhares de artigos e numerosos livros já foram escritos sobre ele [Bertsekas, 1991; Daigle, 1991; Kleinrock, 1975, 1976; Ross, 1995]. Neste livro, faremos apenas uma discussão intuitiva, de alto nível, sobre o atraso de fila; o leitor mais curioso pode consultar alguns dos livros citados (ou até mesmo escrever uma tese sobre o assunto!). Diferentemente dos três outros atrasos (a saber, d_{proc} , d_{trans} e d_{prop}), o atraso de fila pode variar de pacote a pacote. Por exemplo, se dez pacotes chegarem a uma fila vazia ao mesmo tempo, o primeiro pacote transmitido não sofrerá nenhum atraso, ao passo que o último pacote sofrerá um atraso relativamente grande (enquanto espera que os outros nove pacotes sejam transmitidos). Por conseguinte, para se caracterizar um atraso de fila, normalmente são utilizadas medições estatísticas, tais como atraso de fila médio, variância do atraso de fila e a probabilidade de ele exceder um valor especificado.

Quando o atraso de fila é grande e quando é insignificante? A resposta a essa pergunta depende da velocidade de transmissão do enlace, da taxa com que o tráfego chega à fila e de sua natureza, isto é, se chega intermitentemente, em rajadas. Para entendermos melhor, vamos adotar a para representar a taxa média com que os pacotes chegam à fila (a é medida em pacotes/segundo). Lembre-se de que R é a taxa de transmissão, isto é, a taxa (em bits/segundo) com que os bits são retirados da fila. Suponha também, para simplificar, que todos os pacotes tenham L bits. Então, a taxa média com que os bits chegam à fila é La bits/s. Por sim, imagine que a fila seja muito longa, de modo que, essencialmente, possa conter um número infinito de bits. A razão La/R , denominada intensidade de tráfego, frequentemente desempenha um papel importante na estimativa do tamanho do atraso de fila. Se $La/R > 1$, então a velocidade média com que os bits chegam à fila excederá a velocidade com que eles podem ser transmitidos para fora da fila. Nessa situação desastrosa, a fila tenderá a aumentar sem limite e o atraso de fila tenderá ao infinito! Por conseguinte, uma das regras de ouro da engenharia de tráfego é: projete seu sistema de modo que a intensidade de tráfego não seja maior do que 1.

Agora, considere o caso em que $La/R \leq 1$. Aqui, a natureza do tráfego influencia o atraso de fila. Por exemplo, se pacotes chegarem periodicamente — isto é, se chegar um pacote a cada L/R segundos — então todos os pacotes chegarão a uma fila vazia e não haverá atraso. Por outro lado, se pacotes chegarem em rajadas, mas periodicamente, poderá haver um significativo atraso de fila médio. Por exemplo, suponha que N pacotes cheguem ao mesmo tempo a cada $(L/R)N$ segundos. Então, o primeiro pacote transmitido não sofrerá atraso de fila; o segundo pacote transmitido terá um atraso de fila de L/R segundos e, de modo mais geral, o enésimo pacote transmitido terá um atraso de fila de $(n - 1)L/R$ segundos. Deixamos como exercício para o leitor o cálculo do atraso de fila médio para esse exemplo.

Os dois exemplos de chegadas periódicas que acabamos de descrever são um tanto acadêmicos. Na realidade, o processo de chegada a uma fila é aleatório — isto é, não segue um padrão e os intervalos de tempo entre os pacotes são ao acaso. Nessa hipótese mais realista, a quantidade La/R normalmente não é suficiente para caracterizar por completo a estatística do atraso. Não obstante, é útil para entender intuitivamente a extensão do atraso de fila. Em especial, se a intensidade de tráfego for próxima de zero, então as chegadas de pacotes serão poucas e bem espaçadas e é improvável que um pacote que esteja chegando encontre outro na fila. Consequentemente, o atraso de fila médio será próximo de zero. Por outro lado, quando a intensidade de tráfego for próxima de 1, haverá intervalos de tempo em que a velocidade de chegada excederá a capacidade de transmissão (devido às variações na taxa de chegada do pacote) e uma fila será formada durante esses períodos de tempo; quando a taxa de chegada for menor do que a capacidade de transmissão, a extensão da fila diminuirá. Todavia, à medida que a intensidade de tráfego se aproxima de 1, o comprimento médio da fila fica cada vez maior. A dependência qualitativa entre o atraso de fila médio e a intensidade de tráfego é mostrada na Figura 1.18.

Um aspecto importante a observar na Figura 1.18 é que, quando a intensidade de tráfego se aproxima de 1, o atraso de fila médio aumenta rapidamente. Uma pequena porcentagem de aumento na intensidade resulta em

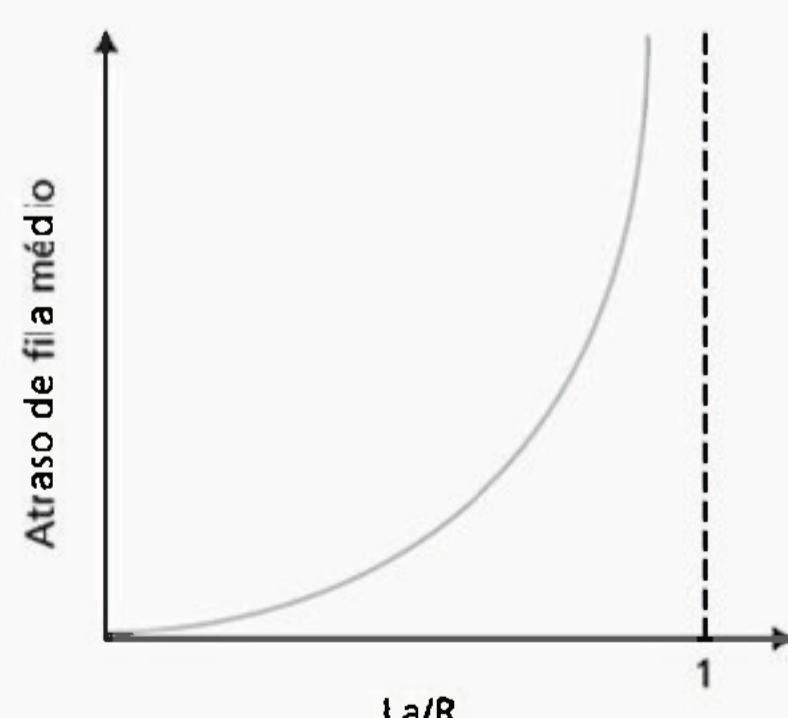


Figura 1.18 Dependência entre atraso de fila médio e intensidade de tráfego

um aumento muito maior no atraso, em termos de porcentagem. Talvez você já tenha percebido esse fenômeno na estrada. Se você dirige regularmente por uma estrada que normalmente está congestionada, o fato de ela estar sempre assim significa que a intensidade de tráfego é próxima de 1. Se algum evento causar um tráfego ligeiramente maior do que o usual, as demoras que você sofrerá poderão ser enormes.

Para compreender um pouco mais os atrasos de fila, visite o Companion Website, que apresenta um aplicativo Java interativo. Se você aumentar a taxa de chegada do pacote o suficiente de forma que a intensidade do tráfego exceda 1, você verá a fila aumentar ao longo do tempo.

Perda de pacote

Na discussão anterior, admitimos que a fila é capaz de conter um número infinito de pacotes. Na realidade, a capacidade da fila que precede um enlace é finita, embora a sua formação dependa bastante do projeto e do custo do comutador. Como a capacidade da fila é finita, na verdade os atrasos de pacote não se aproximam do infinito quando a intensidade de tráfego se aproxima de 1. O que realmente acontece é que um pacote pode chegar e encontrar uma fila cheia. Sem espaço disponível para armazená-lo, o roteador descartará esse pacote; isto é, ele será perdido. Esse excesso em uma fila pode ser observado novamente no aplicativo Java quando a intensidade do tráfego é maior do que 1. Do ponto de vista de um sistema final, uma perda de pacote é vista como um pacote que foi transmitido para o núcleo da rede, mas sem nunca ter emergido dele no destino. A fração de pacotes perdidos aumenta com o aumento da intensidade de tráfego. Por conseguinte, o desempenho em um nó é frequentemente medido não apenas em termos de atraso, mas também em termos da probabilidade de perda de pacotes. Como discutiremos nos capítulos subsequentes, um pacote perdido pode ser retransmitido sim a sim para garantir que todos os dados sejam finalmente transferidos da origem ao local de destino.

1.4.3 Atraso fim a fim

Até o momento, nossa discussão focalizou o atraso nodal, isto é, o atraso em um único roteador. Concluiremos essa discussão considerando brevemente o atraso da origem ao destino. Para entender esse conceito, suponha que haja $N - 1$ roteadores entre a máquina de origem e a máquina de destino. Imagine também que a rede não esteja congestionada (e, portanto, os atrasos de fila sejam desprezíveis), que o atraso de processamento em cada roteador e na máquina de origem seja d_{proc} , que a taxa de transmissão de saída de cada roteador e da máquina de origem seja R bits/s e que o atraso de propagação em cada enlace seja d_{prop} . Os atrasos nodais se acumulam e resultam em um atraso fim a fim

$$d_{fim\ a\ fim} = N (d_{proc} + d_{trans} + d_{prop})$$

onde, mais uma vez, $d_{trans} = L/R$ e L é o tamanho do pacote. Convidamos você a generalizar essa fórmula para o caso de atrasos heterogêneos nos nós e para o caso de um atraso de fila médio em cada nó.

Traceroute

Para perceber o que é realmente o atraso em uma rede de computadores, podemos utilizar o Traceroute, programa de diagnóstico que pode ser executado em qualquer máquina da Internet. Quando o usuário especifica um nome de hospedeiro de destino, o programa no hospedeiro de origem envia vários pacotes especiais em direção àquele destino. Ao seguir seu caminho até o destino, esses pacotes passam por uma série de roteadores. Um deles recebe um desses pacotes especiais e envia uma curta mensagem à origem. Essa mensagem contém o nome e o endereço do roteador.

Mais especificamente, suponha que haja $N - 1$ roteadores entre a origem e o destino. Então, a fonte enviará N pacotes especiais à rede e cada um deles estará endereçado ao destino final. Esses N pacotes especiais serão marcados de 1 a N , sendo a marca do primeiro pacote 1 e a do último, N . Assim que o enésimo roteador recebe o enésimo pacote com a marca n , não envia o pacote a seu destino, mas uma mensagem à origem. Quando o hospedeiro de destino recebe o pacote N , também envia uma mensagem à origem, que registra o tempo transcorrido entre o envio de um pacote e o recebimento da mensagem de retorno correspondente. A origem registra também o

nome e o endereço do roteador (ou do hospedeiro de destino) que retorna a mensagem. Dessa maneira, a origem pode reconstruir a rota tomada pelos pacotes que vão da origem ao destino e pode determinar os atrasos de ida e volta para todos os roteadores intervenientes. Na prática, o programa Traceroute repete o processo que acabamos de descrever três vezes, de modo que a fonte envia, na verdade, $3 \cdot N$ pacotes ao destino. O RFC 1393 descreve detalhadamente o Traceroute.

Eis um exemplo de resultado do programa Traceroute, no qual a rota traçada ia do hospedeiro de origem `gaia.cs.umass.edu` (na Universidade de Massachusetts) até `cis.poly.edu` (na Polytechnic University no Brooklyn). O resultado tem seis colunas: a primeira coluna é o valor n descrito acima, isto é, o número do roteador ao longo da rota; a segunda coluna é o nome do roteador; a terceira coluna é o endereço do roteador (na forma `xxx.xxx.xxx.xxx`); as últimas três colunas são os atrasos de ida e volta para três tentativas. Se a fonte receber menos do que três mensagens de qualquer roteador determinado (devido à perda de pacotes na rede), o Traceroute coloca um asterisco logo após o número do roteador e registra menos do que três tempos de duração de viagens de ida e volta para aquele roteador.

```
1 cs-gw (128.119.240.254) 1.009 ms 0.899 ms 0.993 ms
2 128.119.3.154 (128.119.3.154) 0.931 ms 0.441 ms 0.651 ms
3 border4-rt-gi-1-3.gw.umass.edu (128.119.2.194) 1.032 ms 0.484 ms 0.451 ms
4 acrl-ge-2-1-0.Boston.cw.net (208.172.51.129) 10.006 ms 8.150 ms 8.460 ms
5 agr4-loopback.NewYork.cw.net (206.24.194.104) 12.272 ms 14.344 ms 13.267 ms
6 acr2-loopback.NewYork.cw.net (206.24.194.62) 13.225 ms 12.292 ms 12.148 ms
7 pos10-2.core2.NewYork1.Level3.net (209.244.160.133) 12.218 ms 11.823 ms 11.793 ms
8 gige9-1-52.hsipaccess1.NewYork1.Level3.net (64.159.17.39) 13.081 ms 11.556 ms 13.297 ms
9 p0-0.polyu.bbnplanet.net (4.25.109.122) 12.716 ms 13.052 ms 12.786 ms
10 cis.poly.edu (128.238.32.126) 14.080 ms 13.035 ms 12.802 ms
```

No exemplo anterior há nove roteadores entre a origem e o destino. Quase todos eles têm um nome e todos têm endereço. Por exemplo, o nome do Roteador 3 é `border4-rt-gi-1-3.gw.umass.edu` e seu endereço é `128.119.2.194`. Examinando os dados apresentados para esse roteador, verificamos que na primeira das três tentativas, o atraso de ida e volta entre a origem e o roteador foi de 1,03 milissegundos. Os atrasos para as duas tentativas subsequentes foram 0,48 e 0,45 milissegundos e incluem todos os atrasos que acabamos de discutir, ou seja, atrasos de transmissão, de propagação, de processamento do roteador e de fila. Como o atraso de fila varia com o tempo, o atraso de ida e volta do pacote n enviado a um roteador n pode, às vezes, ser maior do que o do pacote $n+1$ enviado ao roteador $n+1$. Realmente, observamos esse fenômeno no exemplo acima: os atrasos do roteador 6 são maiores que os atrasos do roteador 7!

Você quer experimentar o Traceroute por conta própria? Recomendamos muito que visite o site <http://www.traceroute.org>, que provê uma interface Web para uma extensa lista de fontes para traçar rotas. Escolha uma fonte, forneça o nome de hospedeiro para qualquer destino e o programa Traceroute fará todo o trabalho. Existem muitos programas de software gratuitos que apresentam uma interface gráfica para o Traceroute; um dos nossos favoritos é o PingPlotter [PingPlotter, 2009].

Sistema final, aplicativo e outros atrasos

Além dos atrasos de processamento, transmissão e de propagação, os sistemas finais podem adicionar outros atrasos significativos. Os modems discados apresentam um atraso de modulação/codificação, que pode ser da ordem de dezenas de microssegundos. (Os atrasos de modulação/codificação para outras tecnologias de acesso — incluindo a Ethernet, o modem a cabo e a DSL — são menos significativos e normalmente desprezíveis.) Um sistema final que quer transmitir um pacote para uma mídia compartilhada (por exemplo, como em um cenário WiFi ou Ethernet) pode, intencionalmente, atrasar sua transmissão como parte de seu protocolo por compartilhar a mídia com outros sistemas finais; vamos analisar tais protocolos no Capítulo 5. Um outro importante atraso é o atraso de empacotamento de mídia, o qual está presente nos aplicativos VoIP (voz sobre IP). No VoIP, o

remetente deve primeiro carregar um pacote com voz digitalizada e codificada antes de transmitir o pacote para a Internet. A etapa de carregar um pacote — chamada de atraso de empacotamento — pode ser significativa e ter impacto sobre a qualidade visível pelo usuário de uma chamada VoIP. Esse assunto será explorado mais adiante nos exercícios de fixação no final deste capítulo.

1.4.4 Vazão nas redes de computadores

Além do atraso e da perda de pacotes, outra medida de desempenho importante em redes de computadores é a vazão fim a fim. Para definir vazão, considere a transferência de um arquivo grande do Hospedeiro A para o Hospedeiro B através de uma rede de computadores. Essa transferência pode ser, por exemplo, um clipe extenso de um parceiro para outro por meio do sistema de compartilhamento P2P. A vazão instantânea a qualquer momento é a taxa (em bits/s) em que o Hospedeiro B está recebendo o arquivo. (Muitos aplicativos, incluindo muitos sistemas de compartilhamento P2P, exibem a vazão instantânea durante os downloads na interface do usuário — talvez você já tenha observado isso!) Se o arquivo consistir em F bits e a transferência levar T segundos para o Hospedeiro B receber todos os F bits, então a vazão média da transferência do arquivo é F/T bits/s. Para algumas aplicações, como a telefonia via Internet, é desejável ter um atraso baixo e uma vazão instantânea acima de algum limiar (por exemplo, superior a 24 kbps para telefonia via Internet, e superior a 256 kbps para alguns aplicativos de vídeo em tempo real). Para outras aplicações, incluindo as de transferência de arquivo, o atraso não é importante, mas é recomendado ter a vazão mais alta possível.

Para obter uma visão mais detalhada, vamos analisar alguns exemplos. A Figura 1.19 (a) mostra dois sistemas finais, um servidor e um cliente, conectados por dois enlaces de comunicação e um roteador. Considere a vazão para uma transferência de arquivo do servidor para o cliente. Suponha que R_s seja a taxa do enlace entre o roteador e o cliente; e R_c seja a taxa do enlace entre o roteador e o cliente. Imagine que os únicos bits enviados na rede inteira sejam os do servidor para o cliente. Agora vem a pergunta, neste cenário ideal, qual é a vazão servidor-para-cliente? Para responder a ela, pense nos bits como um *líquido* e nos enlaces de comunicação como *canos*. Evidentemente, o servidor não pode enviar os bits através de seu enlace a uma taxa mais rápida do que R_s bps e o roteador não pode encaminhar os bits a uma taxa mais rápida do que R_c bps. Se $R_s < R_c$, então os bits enviados pelo servidor irão “correr” diretamente pelo roteador e chegar no cliente a uma taxa de R_c bps. Se, por outro lado, $R_s > R_c$, então o roteador não poderá encaminhar os bits tão rapidamente quanto ele os recebe. Neste caso, os bits somente deixarão o roteador a uma taxa R_c , dando uma vazão fim a fim de R_c . (Observe também que se os bits continuarem a chegar no roteador a uma taxa R_s , e continuarem a deixar o roteador a uma taxa R_c , o acúmulo de bits no roteador esperando para transmissão ao cliente só aumentará — uma situação, na maioria das vezes, indesejável!) Assim, para essa rede simples de dois enlaces, a vazão é $\min\{R_s, R_c\}$, ou seja, é a taxa de transmissão do enlace de gargalo. Após determinar a vazão, agora podemos

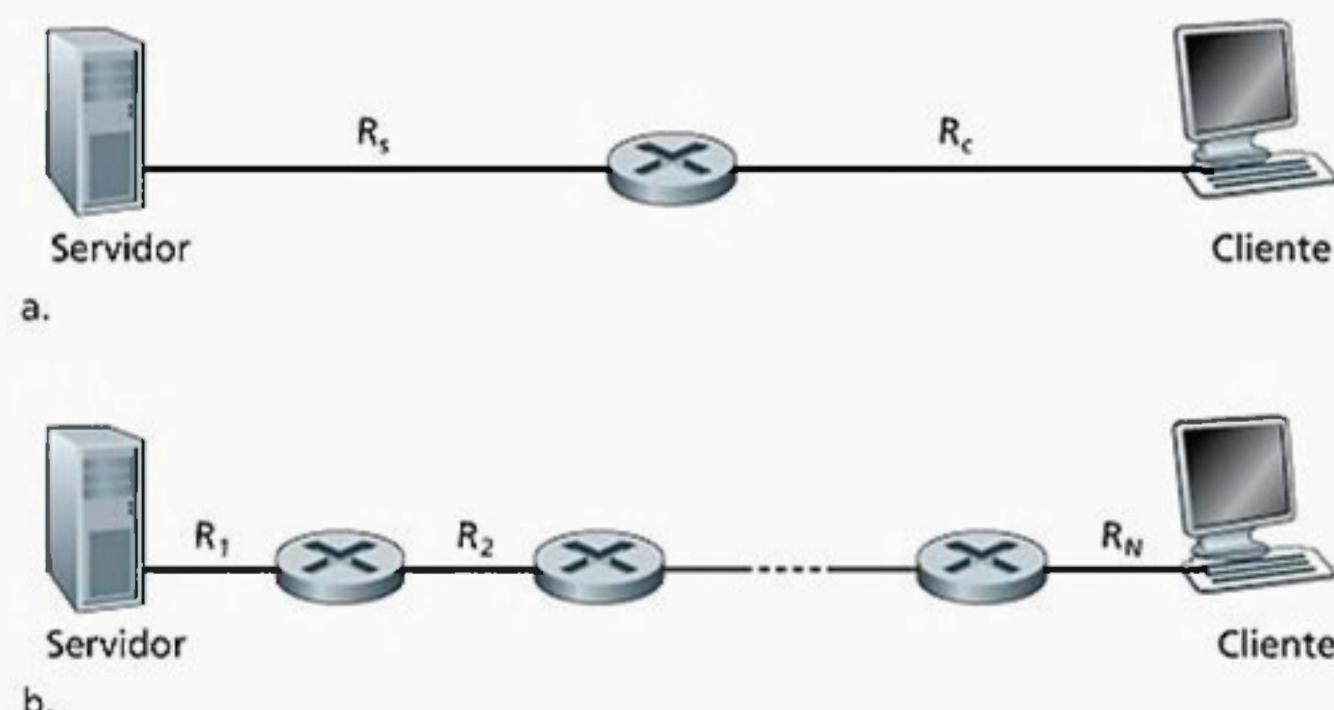


Figura 1.19 Vazão para uma transferência de arquivo do servidor ao cliente

aproximar o tempo que leva para transferir um arquivo grande de F bits do servidor ao cliente como $F/\min\{R_s, R_c\}$. Para um exemplo específico, suponha que você está fazendo o download de um arquivo MP3 de $F = 32$ milhões de bits, o servidor tem uma taxa de transmissão de $R_s = 2$ Mbps, e você tem um enlace de acesso de $R_c = 1$ Mbps. O tempo necessário para transferir o arquivo é, então, 32 segundos. Naturalmente essas expressões para tempo de vazão e de transferência são apenas aproximações, já que elas não contabilizam assuntos relacionados a protocolos e pacotes.

A Figura 1.19 (b) agora mostra uma rede com N enlaces entre o servidor e o cliente, com as taxas de transmissão de N enlaces sendo R_1, R_2, \dots, R_N . Aplicando a mesma análise da rede de dois enlaces, descobrimos que a vazão para uma transferência de arquivo do servidor ao cliente é $\min\{R_1, R_2, \dots, R_N\}$, a qual é novamente a taxa de transmissão do enlace de gargalo ao longo do caminho entre o servidor e o cliente.

Agora considere outro exemplo motivado pela Internet de hoje. A Figura 1.20 (a) mostra dois sistemas finais, um servidor e um cliente, conectados a uma rede de computadores. Considere a vazão para uma transferência de arquivo do servidor ao cliente. O servidor está conectado à rede com um enlace de acesso de taxa R_s e o cliente está conectado à rede com um enlace de acesso de R_c . Agora suponha que todos os enlaces no núcleo da rede de comunicação tenham taxas altas de transmissão, muito maiores do que R_s e R_c . Realmente, hoje, o núcleo da Internet está superabastecido com enlaces de alta velocidade que sofrem pouco congestionamento [Akella, 2003]. Suponha, também, que os únicos bits que estão sendo enviados em toda a rede sejam os do servidor para o cliente. Como o núcleo da rede de computadores é como um cano largo neste exemplo, a taxa a qual os bits correm da origem ao lugar de destino é novamente o mínimo de R_s e R_c , ou seja, vazão = $\min\{R_s, R_c\}$. Portanto, o fator coercitivo para vazão na Internet de hoje é, normalmente, o acesso à rede.

Para um exemplo final, considere a Figura 1.20 (b) na qual existem 10 servidores e 10 clientes conectados ao núcleo da rede de computadores. Neste exemplo, 10 downloads simultâneos estão sendo realizados, envolvendo 10 pares de clientes-servidores. Suponha que esses 10 downloads sejam o único tráfego na rede no momento presente. Como mostrado na figura, há um enlace no núcleo que é atravessado por todos os 10 downloads. Considere R a taxa de transmissão desse enlace. Suponha que todos os enlaces de acesso do servidor possuem a mesma taxa

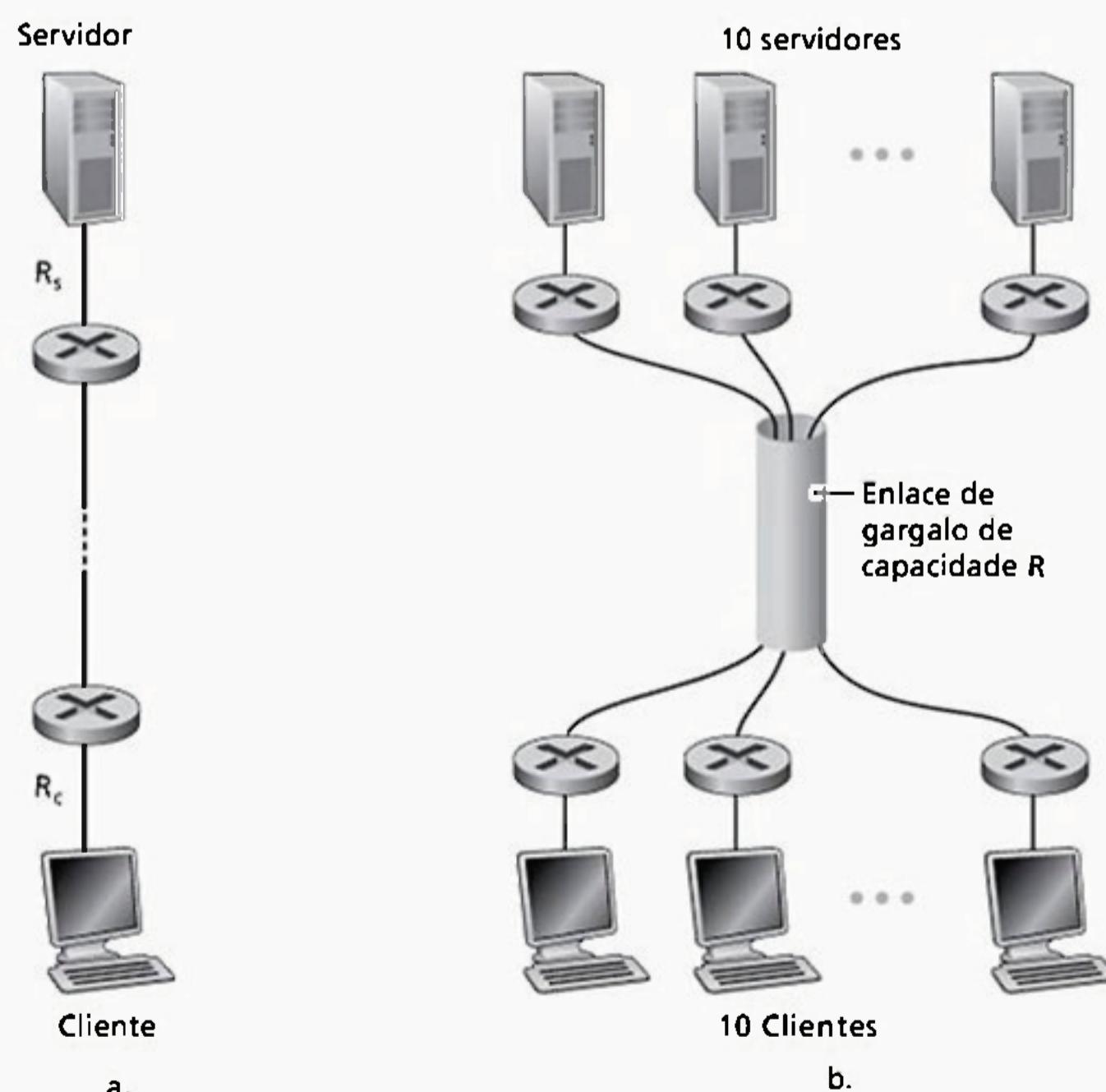


Figura 1.20 Vazão fim a fim: (a) O cliente baixa um arquivo do servidor; (b) 10 clientes fazem o download com 10 servidores

R_s , todos os enlaces de acesso do cliente possuem a mesma taxa R_s e a taxa de transmissão de todos os enlaces no núcleo — com exceção de um enlace comum de taxa R — sejam muito maiores do que R_s , R_c e R . Agora perguntemos, quais são as vazões dos downloads? Evidentemente, se a taxa do enlace comum, R , é grande — digamos que cem vezes maior do que R_s , R_c — então a vazão para cada download será novamente mín { R_s , R_c }. Mas e se a taxa do enlace comum for da mesma ordem que R_s e R_c ? Qual será a vazão neste caso? Vamos observar um exemplo específico. Suponha que $R_s = 2$ Mbps, $R_c = 1$ Mbps, $R = 5$ Mbps, e o enlace comum divide sua taxa de transmissão igualmente entre 10 downloads. Então, o gargalo para cada download não se encontra mais na rede de acesso, mas e o enlace compartilhado no núcleo, que somente fornece para cada download 500 kbps de vazão. Deste modo, a vazão sim a sim para cada download é agora reduzida a 500 kbps.

Os exemplos na Figura 1.19 e Figura 1.20 (a) mostram que a vazão depende das taxas de transmissão dos enlaces sobre as quais os dados correm. Vimos que quando não há tráfego interveniente, a vazão pode simplesmente ser aproximada como a taxa de transmissão mínima ao longo do caminho entre a origem e o local de destino. O exemplo na Figura 1.20 (b) mostra que, de maneira geral, a vazão depende não somente das taxas de transmissão dos enlaces ao longo do caminho, mas também do tráfego interveniente. Em especial, um enlace com uma alta taxa de transmissão pode, todavia, ser o enlace de gargalo para uma transferência de arquivo, caso muitos outros fluxos de dados estejam também passando por aquele enlace. Analisaremos mais detalhadamente vazão em redes de computadores nos exercícios de fixação e nos capítulos subsequentes.

1.5 Camadas de protocolo e seus modelos de serviço

Até aqui, nossa discussão demonstrou que a Internet é um sistema *extremamente complicado* e que possui muitos componentes: inúmeras aplicações e protocolos, vários tipos de sistemas finais e conexões entre eles, roteadores, além de vários tipos de meios físicos de enlace. Dada essa enorme complexidade, há alguma esperança de organizar a arquitetura de rede ou, ao menos, nossa discussão sobre ela? Felizmente, a resposta a ambas as perguntas é sim.

1.5.1 Arquitetura de camadas

Antes de tentarmos organizar nosso raciocínio sobre a arquitetura da Internet, vamos procurar uma analogia humana. Na verdade, lidamos com sistemas complexos o tempo todo em nosso dia a dia. Imagine se alguém pedisse que você descrevesse, por exemplo, o sistema de uma companhia aérea. Como você encontraria a estrutura para descrever esse sistema complexo que tem agências de emissão de passagens, pessoal para embarcar a bagagem para ficar no portão de embarque, pilotos, aviões, controle de tráfego aéreo e um sistema mundial de roteamento de aeronaves? Um modo de descrever esse sistema poderia ser apresentar a relação de uma série de ações que você realiza (ou que outros realizam para você) quando voa por uma empresa aérea. Você compra a passagem, despacha suas malas, dirige-se ao portão de embarque e, finalmente, entra no avião, que decola e segue uma rota até seu destino. Após a aterrissagem, você desembarca no portão designado e recupera suas malas. Se a viagem foi ruim, você reclama na agência que lhe vendeu a passagem (esforço em vão). Esse cenário é ilustrado na Figura 1.21.

Já podemos notar aqui algumas analogias com redes de computadores: você está sendo despachado da origem ao destino pela companhia aérea; um pacote é despachado da máquina de origem à máquina de destino na Internet. Mas essa não é exatamente a analogia que buscamos. Estamos tentando encontrar alguma estrutura na Figura 1.21. Observando essa figura, notamos que há uma função referente à passagem em cada ponta; há também uma função de bagagem para passageiros que já apresentaram a passagem e uma função de portão de embarque para passageiros que já apresentaram a passagem e despacharam a bagagem. Para passageiros que já passaram pelo portão de embarque (isto é, aqueles que já apresentaram a passagem, despacharam a bagagem e passaram pelo portão), há uma função de decolagem e de aterrissagem e, durante o voo, uma função de roteamento do avião. Isso sugere que podemos examinar a funcionalidade na Figura 1.21 na horizontal, como mostra a Figura 1.22.



Figura 1.21 Uma viagem de avião: ações

A Figura 1.22 dividiu a funcionalidade da linha aérea em camadas, provendo uma estrutura com a qual podemos discutir a viagem aérea. Note que cada camada, combinada com as camadas abaixo dela, implementa alguma funcionalidade, algum serviço. Na camada da passagem aérea e abaixo dela, é realizada a transferência ‘balcão-de-linha-aérea-balcão-de-linha-aérea’ de um passageiro. Na camada de bagagem e abaixo dela, é realizada a transferência ‘despacho-de-bagagem–recuperação-de-bagagem’ de um passageiro e de suas malas. Note que a camada da bagagem provê esse serviço apenas para a pessoa que já apresentou a passagem. Na camada do portão, é realizada a transferência ‘portão-de-embarque-portão-de-desembarque’ de um passageiro e de sua bagagem. Na camada de decolagem/aterriagem, é realizada a transferência ‘pista-a-pista’ de passageiros e de suas bagagens. Cada camada provê seu serviço (1) realizando certas ações dentro da camada (por exemplo, na camada do portão, embarcar e desembarcar pessoas de um avião) e (2) utilizando os serviços da camada imediatamente inferior (por exemplo, na camada do portão, aproveitando o serviço de transferência ‘pista-a-pista’ de passageiros da camada de decolagem/aterriagem).

Uma arquitetura de camadas nos permite discutir uma parcela específica e bem definida de um sistema grande e complexo. Essa simplificação tem considerável valor intrínseco, pois provê modularidade fazendo com que fique muito mais fácil modificar a implementação do serviço prestado pela camada. Contanto que a camada forneça o mesmo serviço para a que está acima dela e use os mesmos serviços da camada abaixo dela, o restante do sistema permanece inalterado quando a sua implementação é modificada. (Note que modificar a implementação de um serviço é muito diferente de mudar o serviço em si!) Por exemplo, se as funções de portão fossem modificadas (digamos que passassem a embarcar e desembarcar passageiros por ordem de altura), o restante do sistema da linha aérea permaneceria inalterado, já que a camada do portão continuaria a prover a mesma função.

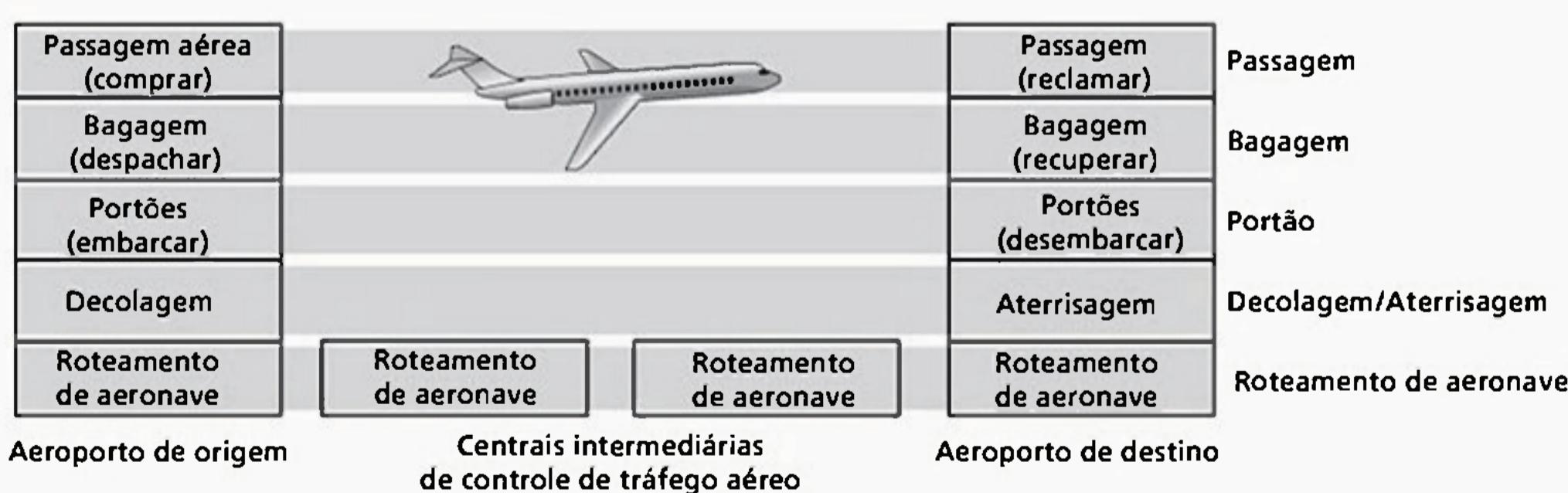


Figura 1.22 Camadas horizontais da funcionalidade de linha aérea

(embarcar e desembarcar passageiros); ela simplesmente implementaria aquela função de maneira diferente após a modificação. Para sistemas grandes e complexos que são atualizados constantemente, a capacidade de modificar a implementação de um serviço sem afetar outros componentes do sistema é outra vantagem importante da divisão em camadas.

Camadas de protocolo

Mas chega de linhas aéreas! Vamos agora voltar nossa atenção a protocolos de rede. Para prover uma estrutura para o projeto de protocolos de rede, projetistas de rede organizam protocolos — e o hardware e o software de rede que implementam os protocolos — em camadas. Cada protocolo pertence a uma das camadas, exatamente como cada função na arquitetura de linha aérea da Figura 1.22 pertencia a uma camada. Novamente estamos interessados nos serviços que uma camada oferece à camada acima dela — denominado modelo de serviço de uma camada. Exatamente como no nosso exemplo da linha aérea, cada camada prove seu serviço (1) executando certas ações dentro da camada e (2) utilizando os serviços da camada diretamente abaixo dela. Por exemplo, os serviços providos pela camada n podem incluir entrega confiável de mensagens de uma extremidade da rede à outra, que pode ser implementada utilizando um serviço não confiável de entrega de mensagem sim a sim da camada $n - 1$ e adicionando funcionalidade da camada n para detectar e retransmitir mensagens perdidas.

Uma camada de protocolo pode ser implementada em software, em hardware, ou em uma combinação dos dois. Protocolos de camada de aplicação como HTTP e SMTP — quase sempre são implementados em software em sistemas finais; o mesmo acontece com protocolos de camada de transporte. Como a camada física e as camadas de enlace de dados são responsáveis pelo manuseio da comunicação por um enlace específico, normalmente são implementadas em uma placa de interface de rede (por exemplo, placas de interface Ethernet ou Wi-Fi) associadas a um determinado enlace. A camada de rede quase sempre é uma implementação mista de hardware e software. Note também que, exatamente como as funções na arquitetura em camadas da linha aérea eram distribuídas entre os vários aeroportos e centrais de controle de tráfego aéreo que compunham o sistema, também um protocolo de camada n é distribuído entre os sistemas finais, comutadores de pacote e outros componentes que formam a rede. Isto é, há sempre uma parcela de um protocolo de camada n em cada um desses componentes de rede.

O sistema de camadas de protocolos tem vantagens conceituais e estruturais. Como vimos, a divisão em camadas proporciona um modo estruturado de discutir componentes de sistemas. A modularidade facilita a atualização de componentes de sistema. Devemos mencionar, no entanto, que alguns pesquisadores e engenheiros de rede se opõem veementemente ao sistema de camadas [Wakeman, 1992]. Uma desvantagem potencial desse sistema é que uma camada pode duplicar a funcionalidade de uma camada inferior. Por exemplo, muitas pilhas de protocolos oferecem serviço de recuperação de erros na camada de enlace e também sim a sim. Uma segunda desvantagem potencial é que a funcionalidade em uma camada pode necessitar de informações (por exemplo, um valor de carimbo de tempo) que estão presentes somente em uma outra camada, o que infringe o objetivo de separação de camadas.

Quando tomados em conjunto, os protocolos das várias camadas são denominados pilha de protocolos, que é formada por cinco camadas: física, de enlace, de rede, de transporte e de aplicação, como mostra a Figura 1.23 (a). Se você verificar o sumário, verá que organizamos este livro utilizando as camadas da pilha de protocolos da Internet. Fazemos uma abordagem descendente, primeiro abordando as camadas de aplicação e, então, os processos.

Camada de aplicação

A camada de aplicação é onde residem aplicações de rede e seus protocolos. Ela inclui muitos protocolos, tais como o protocolo HTTP (que provê requisição e transferência de documentos pela Web), o SMTP (que provê transferência de mensagens de correio eletrônico) e o FTP (que prove a transferência de arquivos entre dois sistemas finais). Veremos que certas funções de rede, como a tradução de nomes fáceis de entender dados a sistemas finais da Internet (por exemplo, gaia.cs.umass.edu) para um endereço de rede de 32 bits, também são executadas com a ajuda de um protocolo de camada de aplicação, no caso, o sistema de nomes de domínio (*domain name system* — DNS). Veremos no Capítulo 2 que é muito fácil criar nossos próprios novos protocolos de camada de aplicação.

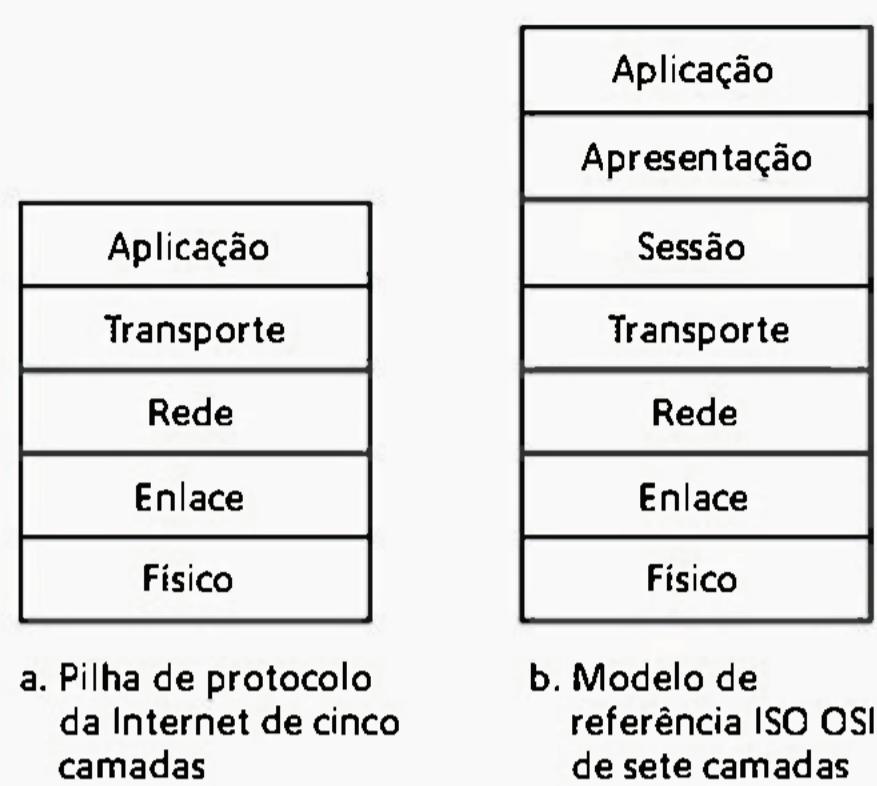


Figura 1.23 A pilha de protocolo da Internet (a) e o modelo de referência OSI (b)

Um protocolo de camada de aplicação é distribuído por diversos sistemas finais, sendo que a aplicação em um sistema final utiliza o protocolo para trocar pacotes de informação com a aplicação em outro sistema final. Denominaremos esse pacote de informação na camada de aplicação de mensagem.

Camada de transporte

A camada de transporte da Internet transporta mensagens da camada de aplicação entre os lados do cliente e servidor de uma aplicação. Há dois protocolos de transporte na Internet: TCP e UDP, e qualquer um deles pode levar mensagens de camada de aplicação. O TCP provê serviços orientados para conexão para suas aplicações. Alguns desses serviços são a entrega garantida de mensagens da camada de aplicação ao destino e controle de fluxo (isto é, compatibilização das velocidades do remetente e do receptor). O TCP também fragmenta mensagens longas em segmentos mais curtos e provê mecanismo de controle de congestionamento, de modo que uma origem regula sua velocidade de transmissão quando a rede está congestionada. O protocolo UDP provê serviço não orientado para conexão a suas aplicações. Este é um serviço econômico que fornece segurança, sem controle de fluxo e de congestionamento. Neste livro, um pacote de camada de transporte será denominado segmento.

Camada de rede

A camada de rede da Internet é responsável pela movimentação, de uma máquina para outra, de pacotes de camada de rede conhecidos como *datagramas*. O protocolo de camada de transporte da Internet (TCP ou UDP) em uma máquina de origem passa um segmento de camada de transporte e um endereço de destino à camada de rede, exatamente como você passaria ao serviço de correios uma carta com um endereço de destinatário. A camada de rede então provê o serviço de entrega do segmento à camada de transporte na máquina destinatária.

A camada de rede da Internet tem dois componentes principais. Um deles é um protocolo que define os campos no datagrama, bem como o modo como os sistemas finais e os roteadores agem nesses campos. Este é o famoso protocolo IP. Existe somente um único protocolo IP, e todos os componentes da Internet que têm uma camada de rede devem executar esse protocolo. O outro componente importante é o protocolo de roteamento que determina as rotas que os datagramas seguem entre origens e destinos. A Internet tem muitos protocolos de roteamento. Como vimos na Seção 1.3, a Internet é uma rede de redes e, dentro de uma delas, o administrador pode executar qualquer protocolo de roteamento que queira. Embora a camada de rede contenha o protocolo IP e também numerosos protocolos de roteamento, ela quase sempre é denominada simplesmente camada IP, refletindo o fato de que ele é o elemento fundamental que mantém a integridade da Internet.

Camada de enlace

A camada de rede da Internet roteia um datagrama por meio de uma série de roteadores entre a origem e o destino. Para levar um pacote de um nó (sistema final ou comutador de pacotes) ao nó seguinte na rota, a camada de rede depende dos serviços da camada de enlace. Em especial, em cada nó, a camada de rede passa o datagrama para a camada de enlace, que o entrega, ao longo da rota, ao nó seguinte, no qual o datagrama é passado da camada de enlace para a de rede.

Os serviços prestados pela camada de enlace dependem do protocolo específico empregado no enlace. Alguns protocolos de camada de enlace proveem entrega garantida entre enlaces, isto é, desde o nó transmissor, passando por um único enlace, até o nó receptor. Note que esse serviço confiável de entrega é diferente do serviço de entrega garantida do TCP, que provê serviço de entrega garantida de um sistema final a outro. Exemplos de protocolos de camadas de enlace são Ethernet, WiFi e PPP (*point-to-point protocol* — protocolo ponto-a-ponto). Como datagramas normalmente precisam transitar por diversos enlaces para irem da origem ao destino, serão manuseados por diferentes protocolos de camada de enlace em diferentes enlaces ao longo de sua rota, podendo ser manuseados por Ethernet em um enlace e por PPP no seguinte. A camada de rede receberá um serviço diferente de cada um dos variados protocolos de camada de enlace. Neste livro, pacotes de camada de enlace serão denominados quadros.

Camada física

Enquanto a tarefa da camada de enlace é movimentar quadros inteiros de um elemento da rede até um elemento adjacente, a da camada física é movimentar os bits individuais que estão dentro do quadro de um nó para o seguinte. Os protocolos nessa camada novamente dependem do enlace e, além disso, dependem do próprio meio de transmissão do enlace (por exemplo, fios de cobre trançado ou fibra ótica monomodal). Por exemplo, a Ethernet tem muitos protocolos de camada física: um para par de fios de cobre trançado, outro para cabo coaxial, um outro para fibra e assim por diante. Em cada caso, o bit é movimentado pelo enlace de um modo diferente.

O modelo OSI

Após discutir detalhadamente a pilha de protocolo da Internet, devemos mencionar que essa não é a única pilha de protocolo existente. Particularmente, no final dos anos 1970, a Organização Internacional para Padronização (ISO) propôs que as redes de computadores fossem organizadas em, aproximadamente, sete camadas, denominadas modelo de Interconexão de Sistemas Abertos (OSI) [ISO, 2009]. O modelo OSI tomou forma quando os protocolos que iriam se tornar protocolos da Internet estavam em amadurecimento; e eram um dos muitos conjuntos de protocolos em desenvolvimento; na verdade, os inventores do modelo OSI original provavelmente não tinham a Internet em mente ao criá-lo. No entanto, no final dos anos 1970, muitos cursos universitários e de treinamento obtiveram conhecimentos sobre a exigência do ISO e organizaram cursos voltados para o modelo de sete camadas. Em razão de seu impacto precoce na educação de redes, o modelo de sete camadas continua presente em alguns livros sobre redes e em cursos de treinamento.

As sete camadas do modelo de referência OSI, mostradas na Figura 1.23 (b), são: camada de aplicação, camada de apresentação, camada de sessão, camada de transporte, camada de rede, camada de enlace e camada física. A função de cinco dessas camadas é a mesma que seus componentes da Internet. Desse modo, vamos considerar as duas camadas adicionais presentes no modelo de referência OSI — a camada de apresentação e a camada de sessão. O papel da camada de apresentação é prover serviços que permitam que as aplicações de comunicação interpretem o significado dos dados trocados. Entre esses serviços estão a compressão de dados e a codificação de dados (o que não precisa de explicação), assim como a descrição de dados (que, como veremos no Capítulo 9, livram as aplicações da preocupação com o formato interno onde os dados estão sendo descritos/armazenados — formato esse que podem se diferenciar de um computador para o outro). A camada de sessão provê a delimitação e sincronização da troca de dados, incluindo os meios de construir um esquema de pontos de verificação e de recuperação.

O fato de a Internet ser desprovida de duas camadas encontradas no modelo de referência OSI faz surgir duas questões: os serviços fornecidos por essas camadas são irrelevantes? E se uma aplicação precisar de um desses

serviços? A resposta da Internet para essas perguntas é a mesma — depende do criador da aplicação. Cabe ao criador da aplicação decidir se um serviço é importante, e se o serviço *for* importante, cabe ao criador da aplicação desenvolver essa função para ela.

1.5.2 Mensagens, segmentos, datagramas e quadros

A Figura 1.24 apresenta o caminho físico que os dados percorrem: para baixo na pilha de protocolos de um sistema final emissor, para cima e para baixo nas pilhas de protocolos de um comutador de camada de enlace interveniente e de um roteador e então para cima na pilha de protocolos do sistema final receptor. Como discutiremos mais adiante neste livro, ambos, comutadores de camada de enlace e roteadores, são comutadores de pacotes. De modo semelhante a sistemas finais, roteadores e comutadores de camada de enlace organizam seu hardware e software de rede em camadas. Mas roteadores e comutadores de camada de enlace não implementam *todas* as camadas da pilha de protocolos; normalmente implementam apenas as camadas de baixo. Como mostra a Figura 1.24, comutadores de camada de enlace implementam as camadas 1 e 2; roteadores implementam as camadas 1, 2 e 3. Isso significa, por exemplo, que roteadores da Internet são capazes de implementar o protocolo IP (da camada 3), mas comutadores de camada de enlace não. Veremos mais adiante que, embora não reconheçam endereços IP, comutadores de camada de enlace são capazes de reconhecer endereços de camada 2, tais como endereços da Ethernet. Note que sistemas finais implementam todas as cinco camadas, o que é consistente com a noção de que a arquitetura da Internet concentra sua complexidade na periferia da rede.

A Figura 1.24 também ilustra o importante conceito de encapsulamento. Uma mensagem de camada de aplicação na máquina emissora (M na Figura 1.24) é passada para a camada de transporte. No caso mais simples, esta pega a mensagem e anexa informações adicionais (denominadas informações de cabeçalho de camada de transporte, H_t na Figura 1.24) que serão usadas pela camada de transporte do lado receptor. A mensagem de camada de aplicação e as informações de cabeçalho da camada de transporte, juntas, constituem o segmento da camada de transporte, que encapsula a mensagem da camada de aplicação. As informações adicionadas podem

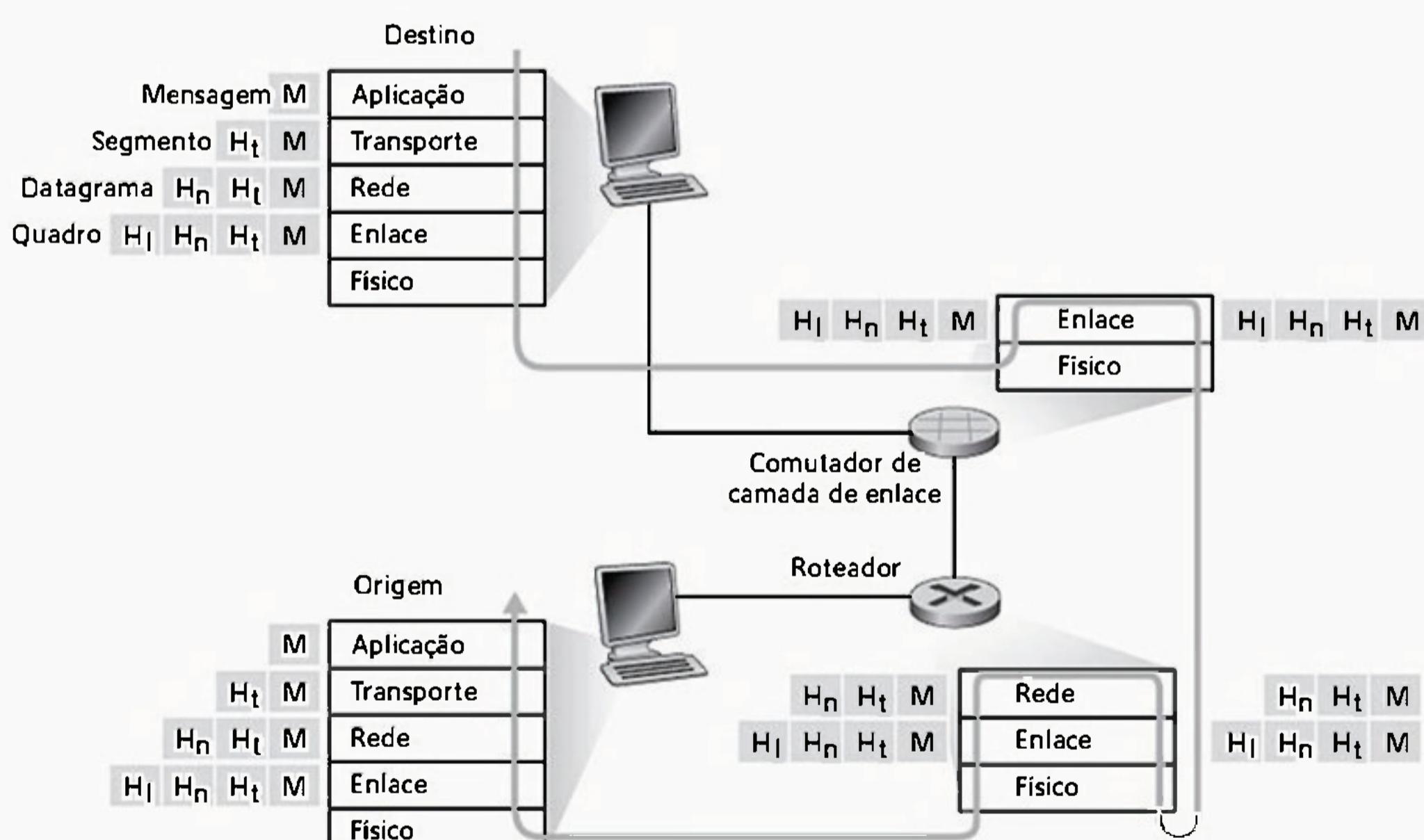


Figura 1.24 Hospedeiros, roteadores e comutadores de camada de enlace; cada um contém um conjunto diferente de camadas, refletindo suas diferenças em funcionalidade

incluir dados que habilitem a camada de transporte do lado do receptor a entregar a mensagem à aplicação apropriada, além de bits de detecção de erro que permitem que o receptor determine se os bits da mensagem foram modificados em trânsito. A camada de transporte então passa o segmento à camada de rede, que adiciona informações de cabeçalho de camada de rede (H_n , na Figura 1.24), como endereços de sistemas finais de origem e de destino, criando um datagrama de camada de rede. Este é então passado para a camada de enlace, que (é claro!), adicionará suas próprias informações de cabeçalho e criará um quadro de camada de enlace. Assim, vemos que, em cada camada, um pacote possui dois tipos de campos: campos de cabeçalho e um campo de carga útil. A carga útil é normalmente um pacote da camada acima.

Uma analogia útil que podemos usar aqui é o envio de um memorando entre escritórios de uma empresa pelo correio de uma filial corporativa a outra. Suponha que Alice, que está em uma filial, queira enviar um memorando a Bob, que está na outra filial. O memorando *representa* uma mensagem da camada de aplicação. Alice coloca o memorando em um envelope de correspondência interna em cuja face são escritos o nome e o departamento de Bob. O envelope de correspondência interna representa o segmento da camada de aplicação — contém as informações de cabeçalho (o nome de Bob e seu departamento) e encapsula a mensagem de camada de aplicação (o memorando). Quando a central de correspondência do escritório emissor recebe o envelope, ele é colocado dentro de outro envelope adequado para envio pelo correio. A central de correspondência emissora também escreve o endereço postal do remetente e do destinatário no envelope postal. Neste ponto, o envelope postal é análogo ao datagrama — encapsula o segmento de camada de transporte (o envelope de correspondência interna), que por sua vez encapsula a mensagem original (o memorando). O correio entrega o envelope postal à central de correspondência do escritório destinatário. Nesse local, o processo de reencapsulamento se inicia. A central de correspondência retira o memorando e o encaminha a Bob. Este, finalmente, abre o envelope e retira o memorando. O processo de encapsulamento pode ser mais complexo do que o descrito acima. Por exemplo, uma mensagem grande pode ser dividida em vários segmentos de camada de transporte (que também podem ser divididos em vários datagramas de camada de rede). Na extremidade receptora, cada segmento deve ser reconstruído a partir dos datagramas que o compõem.

1.6 Redes sob ameaça

A Internet se tornou essencial para muitas instituições hoje, incluindo empresas grandes e pequenas, universidades e órgãos do governo. Muitas pessoas também contam com a Internet para suas atividades profissionais, sociais e pessoais. Mas atrás de toda essa utilidade e entusiasmo, existe o lado negro, um lado no qual “vilões” tentam causar problemas em nosso cotidiano danificando nossos computadores conectados à Internet, violando nossa privacidade e tornando inoperantes os serviços da Internet dos quais dependemos [Skoudis, 2006].

A área de segurança de rede abrange como esses vilões podem ameaçar as redes de computadores e como nós, futuros especialistas no assunto, podemos defender a rede contra essas ameaças ou, melhor ainda, criar novas arquiteturas imunes a tais ameaças em primeiro lugar. Dadas a frequência e a variedade das ameaças existentes, bem como o perigo de novos e mais destrutivos futuros ataques, a segurança de rede se tornou, recentemente, um assunto principal na área de redes de computadores. Um dos objetivos deste livro é trazer as questões de segurança de rede para primeiro plano. Iniciaremos nossa discussão sobre redes de computadores nesta seção, com uma breve descrição de alguns dos ataques mais predominantes e prejudiciais na Internet de hoje. Então, à medida que retratarmos em detalhes as diversas tecnologias de redes de computadores e protocolos nos capítulos seguintes, analisaremos as diversas questões relacionadas à segurança associadas a essas tecnologias e protocolos. Finalmente, no Capítulo 8, munidos com nosso know-how em redes de computadores e protocolos da Internet recém-adquirido, estudaremos a fundo como as redes de computadores podem ser defendidas contra ameaças, ou projetadas e operadas para impossibilitá-las.

Visto que ainda não temos o know-how em rede de computadores e em protocolos da Internet, começaremos com uma análise de alguns dos atuais problemas mais predominantes relacionados à segurança. Isto irá aguçar nosso apetite para mais discussões importantes nos capítulos futuros. Começamos com a pergunta, o que pode dar errado? Como as redes de computadores são frágeis? Quais são alguns dos tipos de ameaças mais predominantes hoje?

Os vilões podem colocar "malware" em seu hospedeiro através da Internet

Conectamos aparelhos à Internet porque queremos receber/enviar dados de/para a Internet. Isso inclui todos os tipos de recursos vantajosos, como páginas da Web, mensagens de e-mail, MP3, chamadas telefônicas, vídeo em tempo real, resultados de mecanismo de busca etc. Porém, infelizmente, junto com esses recursos vantajosos aparecem os maliciosos — conhecidos conjuntamente como malware — que também podem entrar e infectar nossos aparelhos. Uma vez que o malware infecta nosso aparelho, ele é capaz de fazer coisas tortuosas, como apagar nossos arquivos; instalar spyware que coleta nossas informações particulares, como nosso número de cartão de crédito, senhas e combinação de teclas, e as envia (através da Internet, é claro!) de volta aos vilões. Nosso hospedeiro comprometido pode estar, também, envolvido em uma rede de milhares de aparelhos comprometidos, conhecidos como "botnet", o qual é controlado e influenciado pelos vilões para distribuição de spams ou ataques de recusa de serviço distribuídos (que serão brevemente discutidos) contra hospedeiros direcionados.

Muitos malwares existentes hoje são autorreprodutivos: uma vez que infecta um hospedeiro, a partir deste, ele faz a busca por entradas em outros hospedeiros através da Internet, e a partir de hospedeiros recém-infectados, ele faz a busca por entrada em mais hospedeiros. Desta maneira, o malware autorreprodutivo pode se disseminar rapidamente. Por exemplo, o número de aparelhos infectados pelo worm 2003 Saphire/Slammer dobrou a cada 8,5 segundos nos primeiros minutos após seu ataque, infectando mais de 90 por cento dos hospedeiros frágeis em 10 minutos [Moore, 2003]. O malware pode se espalhar na forma de vírus, worms ou cavalo de Troia [Skoudis, 2004]. Os vírus são malwares que necessitam de uma interação do usuário para infectar seu aparelho. O exemplo clássico é um anexo de e-mail contendo um código executável malicioso. Se o usuário receber e abrir tal anexo, o malware será executado em seu aparelho. Geralmente, tais vírus de e-mail se autorreproduzem: uma vez executado, o vírus pode enviar uma mensagem idêntica, com um anexo malicioso idêntico, para, por exemplo, todos os contatos da lista de endereços do usuário. Worms (como o Slammer) são malwares capazes de entrar em um aparelho sem qualquer interação do usuário. Por exemplo, um usuário pode estar executando uma aplicação de rede frágil para a qual um atacante pode enviar um malware. Em alguns casos, sem a intervenção do usuário, a aplicação pode aceitar o malware da Internet e executá-lo, criando um worm. Este, no aparelho recém-infectado, então, varre a Internet em busca de outros hospedeiros que estejam executando a mesma aplicação de rede frágil. Ao encontrar outros hospedeiros frágeis, ele envia uma cópia de si mesmo para eles. Por fim, um cavalo de Troia é uma parte oculta de um software funcional. Hoje, o malware é persuasivo e é caro para se criar uma proteção. À medida que trabalhar com este livro, sugerimos que pense na seguinte questão: O que os projetistas de computadores podem fazer para proteger os aparelhos que utilizam a Internet de ameaças de malware?

Os vilões podem atacar servidores e infraestrutura de redes

Um amplo grupo de ameaças à segurança pode ser classificado como ataques de recusa de serviços (DoS). Como o nome sugere, um ataque DoS torna uma rede, hospedeiro ou outra parte da infraestrutura inutilizável por usuários verdadeiros. Servidores da Web, de e-mails e DNS (discutidos no Capítulo 2), e redes institucionais podem estar sujeitos aos ataques DoS. Na Internet, esses ataques são extremamente comuns, com milhares deles ocorrendo todo ano [Moore, 2001; Mirkovic, 2005]. A maioria dos ataques DoS na Internet podem ser divididos em três categorias:

Ataque de vulnerabilidade. Envolve o envio de mensagens perfeitas a uma aplicação vulnerável ou a um sistema operacional sendo executado em um hospedeiro direcionado. Se a sequência correta de pacotes é enviada a uma aplicação vulnerável ou a um sistema operacional, o serviço pode parar ou, pior, o hospedeiro pode pisar.

Inundação na largura de banda. O atacante envia um grande número de pacotes ao hospedeiro direcionado — tantos pacotes que o enlace de acesso do alvo se entope, impedindo os pacotes legítimos de alcançarem o servidor.

Inundação na conexão. O atacante estabelece um grande número de conexões TCP semiabertas ou abertas (as conexões TCP são discutidas no Capítulo 3) no hospedeiro-alvo. O hospedeiro pode ficar tão atolado com essas conexões falsas que para de aceitar conexões legítimas.

Vamos agora explorar mais detalhadamente o ataque de inundação na largura de banda. Lembrando de nossa análise sobre atraso e perda na seção 1.4.2, é evidente que se o servidor possui uma taxa de acesso R bps, então o atacante precisará enviar tráfego a uma taxa de, aproximadamente, R bps para causar dano. Se R for muito grande, uma fonte de ataque única pode não ser capaz de gerar tráfego suficiente para prejudicar o servidor. Além disso, se todo o tráfego provier de uma fonte única, um roteador upstream pode conseguir detectar o ataque e bloquear todo o tráfego da fonte antes que ele se aproxime do servidor. Em um ataque DoS distribuído (DDoS), ilustrado na Figura 1.25, o atacante controla múltiplas fontes que sobrecarregam o alvo. Com tal abordagem, a taxa de tráfego agregada por todas as fontes controladas precisa ser, aproximadamente, R para incapacitar o serviço. Os ataques DDoS que potencializam botnets com centenas de hospedeiros comprometidos são uma ocorrência comum hoje em dia [Mirkovic, 2005]. Os ataques DDoS são muito mais difíceis de detectar e de prevenir do que um ataque DoS de um único hospedeiro.

Os vilões podem analisar pacotes

Muitos usuários hoje acessam à Internet por meio de aparelhos sem fio, como laptops conectados à tecnologia Wi-Fi ou aparelhos portáteis com conexões à Internet via telefone celular (abordado no Capítulo 6). Enquanto o acesso onipresente à Internet é extremamente conveniente e disponibiliza novas aplicações sensacionais aos usuários móveis, ele também cria uma grande vulnerabilidade de segurança — posicionando um receptor passivo nas proximidades do transmissor sem fio, o receptor pode obter uma cópia de cada pacote transmitido! Esses pacotes podem conter todo tipo de informações confidenciais, incluindo senhas, número de inscrição da previdência social, segredos comerciais e mensagens pessoais. Um receptor passivo que grava uma cópia de cada pacote que passa é denominado analisador de pacote.

Os analisadores também podem estar distribuídos em ambientes de conexão com fio. Nesses ambientes, como em muitas Ethernet LANs, um analisador de pacote pode obter cópias de todos os pacotes enviados pela LAN. Como descrito na Seção 1.2, as tecnologias de acesso a cabo também transmitem pacotes e são, dessa forma, vulneráveis à análise. Além disso, um vilão que quer ganhar acesso ao roteador de acesso de uma instituição ou enlace de acesso para a Internet pode instalar um analisador que faça uma cópia de cada pacote que vai para/de a empresa. Os pacotes farejados podem, então, ser analisados off-line em busca de informações confidenciais.

O software para analisar pacotes está disponível gratuitamente em diversos sites da Internet e em produtos comerciais. Professores que ministram um curso de redes passam exercícios que envolvem a composição de um programa de reconstrução de dados da camada de aplicação e um programa analisador de pacotes.

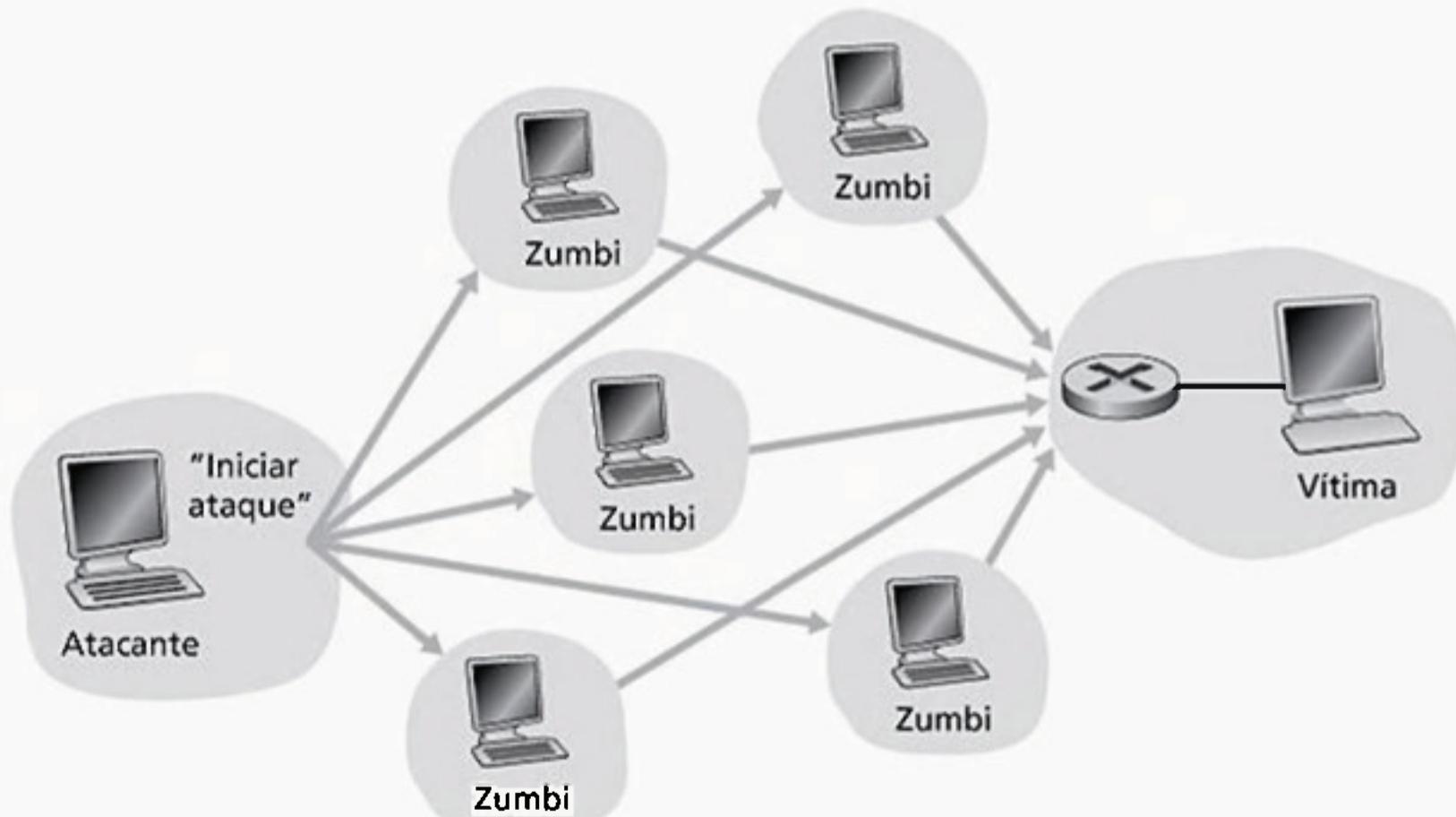


Figura 1.25 Um ataque de recusa de serviço distribuído (DDoS)

Como os analisadores de pacote são passivos — ou seja, eles não introduzem pacotes no canal — eles são difíceis de detectar. Portanto, quando enviamos pacotes para um canal sem fio, devemos aceitar a possibilidade de que alguém possa estar copiando nossos pacotes. Como você deve ter imaginado, uma das melhores defesas contra a análise de pacote envolve a criptografia, que será analisada no Capítulo 8, já que se aplica à segurança de rede.

Os vilões podem se passar por alguém de sua confiança

Por incrível que pareça, é extremamente fácil (você saberá como conforme ler este livro!) criar um pacote com um endereço de fonte arbitrário, conteúdo de pacote e um endereço de destino e, então, transmitir esse pacote feito à mão para a Internet, que, obedientemente, o encaminhará para seu destino. Imagine que um receptor inocente (digamos um roteador da Internet) que recebe tal pacote, acredita que a fonte (falsa) seja confiável e então executa um comando integrado aos conteúdos do pacote (digamos que modifica sua base de encaminhamento). A habilidade de introduzir pacotes na Internet com uma fonte falsa de endereço é conhecida como IP spoofing, e é uma das muitas maneiras pelas quais o usuário pode se passar por outro.

Para resolver esse problema, precisaremos de uma comprovação da fonte, ou seja, um mecanismo que nos permitirá determinar com certeza se uma mensagem se origina de onde pensamos. Mais uma vez, sugerimos que pense em como isso pode ser feito em aplicações de rede e protocolos à medida que avança sua leitura pelos capítulos deste livro. Exploraremos mais mecanismos para comprovação da fonte no Capítulo 8.

Os vilões podem alterar ou excluir mensagens

Encerramos esta breve análise de ataques na rede descrevendo os ataques *man-in-the-middle* (homem no meio). Nessa categoria de ataques, o vilão está infiltrado no percurso da comunicação entre duas entidades comunicantes. Vamos chamar essas entidades de Alice e Bob, que podem ser seres humanos reais ou entidades de rede como dois roteadores ou dois servidores de e-mail. O vilão pode ser, por exemplo, um roteador comprometido no percurso da comunicação, ou um módulo de software residente em um dos hospedeiros finais em uma camada inferior da pilha de protocolo. No ataque *man-in-the-middle*, o vilão não somente possui a possibilidade de analisar todos os pacotes que passam entre Bob e Alice, como também pode introduzir, alterar ou excluir pacotes. No jargão da segurança de rede, um ataque *man-in-the-middle* pode comprometer a integridade dos dados enviados entre Alice e Bob. Assim como veremos no Capítulo 8, os mecanismos que oferecem sigilo (proteção contra análise) e autenticação da origem (permitindo que o receptor verifique com certeza o gerador da mensagem) não necessariamente oferecem integridade dos dados.

Ao encerrar esta seção, deve-se considerar como a Internet se tornou um local inseguro, em primeiro lugar. A resposta resumidamente é que a Internet foi, a princípio, criada para ser assim, baseada no modelo de “um grupo de usuários de confiança mútua ligados a uma rede transparente” [Blumenthal, 2001] — um modelo no qual (por definição) não há necessidade de segurança. Muitos aspectos da arquitetura inicial da Internet refletem profundamente essa noção de confiança mútua. Por exemplo, a capacidade de um usuário enviar um pacote a qualquer outro é mais uma falha do que um recurso solicitado/concedido, e acredita-se piamente na identidade do usuário em vez de ela ser confirmada automaticamente.

Mas a Internet de hoje certamente não envolve “usuários de confiança mútua”. Contudo, os usuários atuais ainda precisam se comunicar mesmo quando não confiam um no outro, podem se comunicar anonimamente, podem se comunicar indiretamente através de terceiros (por exemplo, Web caches, que serão estudados no Capítulo 2, ou agentes móveis para assistência, que serão estudados no Capítulo 6), e podem desconfiar do hardware, software e até mesmo do ar pelo qual eles se comunicam. Temos agora muitos desafios relacionados à segurança perante nós à medida que prosseguimos com o livro: devemos procurar por proteção contra a análise, disfarce da origem, ataques *man-in-the-middle*, ataques DDoS, malware e mais. Devemos manter em mente que a comunicação entre usuários de confiança mútua é mais uma exceção do que uma regra.

Seja bem-vindo ao mundo da moderna rede de computadores!

1.7 História das redes de computadores e da Internet

Da seção 1.1 à 1.6, apresentamos um panorama da tecnologia de redes de computadores e da Internet. Agora, você já deve saber o suficiente para impressionar sua família e amigos. Contudo, se realmente quiser ser o maior sucesso do próximo coquetel, você deve rechear seu discurso com pérolas da fascinante história da Internet [Segaller, 1998].

1.7.1 Desenvolvimento da comutação de pacotes: 1961-1972

Os primeiros passos da disciplina de redes de computadores e da Internet podem ser traçados desde o início da década de 1960, quando a rede telefônica era a rede de comunicação dominante no mundo inteiro. Lembre-se de que na Seção 1.3 dissemos que a rede de telefonia usa comutação de circuitos para transmitir informações entre uma origem e um destino — uma escolha acertada, já que a voz é transmitida a uma taxa constante entre a origem e o destino. Dada a importância cada vez maior (e o alto custo) dos computadores no início da década de 1960 e o advento de computadores com multiprogramação (*time-sharing*), nada seria mais natural (agora que temos uma visão perfeita do passado) do que considerar a questão de como interligar computadores para que pudessem ser compartilhados entre usuários distribuídos em localizações geográficas diferentes. O tráfego gerado por esses usuários provavelmente era intermitente, por *rajadas* — períodos de atividade, como o envio de um comando a um computador remoto, seguidos de períodos de inatividade, como a espera por uma resposta ou o exame de uma resposta recebida.

Três grupos de pesquisa ao redor do mundo, sem que nenhum tivesse conhecimento do trabalho do outro [Leiner, 1998], começaram a inventar a comutação de pacotes como uma alternativa poderosa e eficiente à de circuitos. O primeiro trabalho publicado sobre técnicas de comutação de pacotes foi o de Leonard Kleinrock [Kleinrock, 1961, 1964], que, naquela época, era um doutorando do MIT. Usando a teoria de filas, o trabalho de Kleinrock demonstrou, com elegância, a eficácia da abordagem da comutação de pacotes para fontes de tráfego intermitentes (*em rajadas*). Em 1964, Paul Baran [Baran, 1964], do Rand Institute, começou a investigar a utilização de comutação de pacotes na transmissão segura de voz pelas redes militares, ao mesmo tempo que Donald Davies e Roger Scantlebury desenvolviam suas ideias sobre esse assunto no National Physical Laboratory, na Inglaterra.

Os trabalhos desenvolvidos no MIT, no Rand Institute e no National Physical Laboratory foram os alicerces do que hoje é a Internet. Mas a Internet também tem uma longa história de atitudes do tipo “construir e demonstrar”, que também data do início da década de 1960. J. C. R. Licklider [DEC, 1990] e Lawrence Roberts, ambos colegas de Kleinrock no MIT, foram adiante e lideraram o programa de ciência de computadores na ARPA (Advanced Research Projects Agency — Agência de Projetos de Pesquisa Avançada), nos Estados Unidos. Roberts publicou um plano geral para a ARPAnet [Roberts, 1967], a primeira rede de computadores por comutação de pacotes e uma ancestral direta da Internet pública de hoje. Os primeiros comutadores de pacotes eram conhecidos como processadores de mensagens de interface (*interface message processors* — IMPs), e o contrato para a fabricação desses comutadores foi entregue à empresa BBN. Em 1969, no Dia do Trabalho nos Estados Unidos, foi instalado o primeiro IMP na UCLA (Universidade da Califórnia em Los Angeles) sob a supervisão de Kleinrock. Logo em seguida foram instalados três IMPs adicionais no Stanford Research Institute (SRI), na Universidade da Califórnia em Santa Bárbara e na Universidade de Utah (Figura 1.26).

O incipiente precursor da Internet tinha quatro nós no final de 1969. Kleinrock recorda que a primeiríssima utilização da rede foi fazer um login remoto entre a UCLA e o SRI, derrubando o sistema [Kleinrock, 2004].

Em 1972, a ARPAnet tinha aproximadamente 15 nós e foi apresentada publicamente pela primeira vez por Robert Kahn na Conferência Internacional sobre Comunicação por Computadores (International Conference on Computer Communications) daquele ano. O primeiro protocolo fim a fim entre sistemas finais da ARPAnet, conhecido como protocolo de controle de rede (*network-control protocol* — NCP), estava concluído [RFC 001] e a partir desse momento a escrita de aplicações tornou-se possível. Em 1972, Ray Tomlinson, da BBN, escreveu o primeiro programa de e-mail.

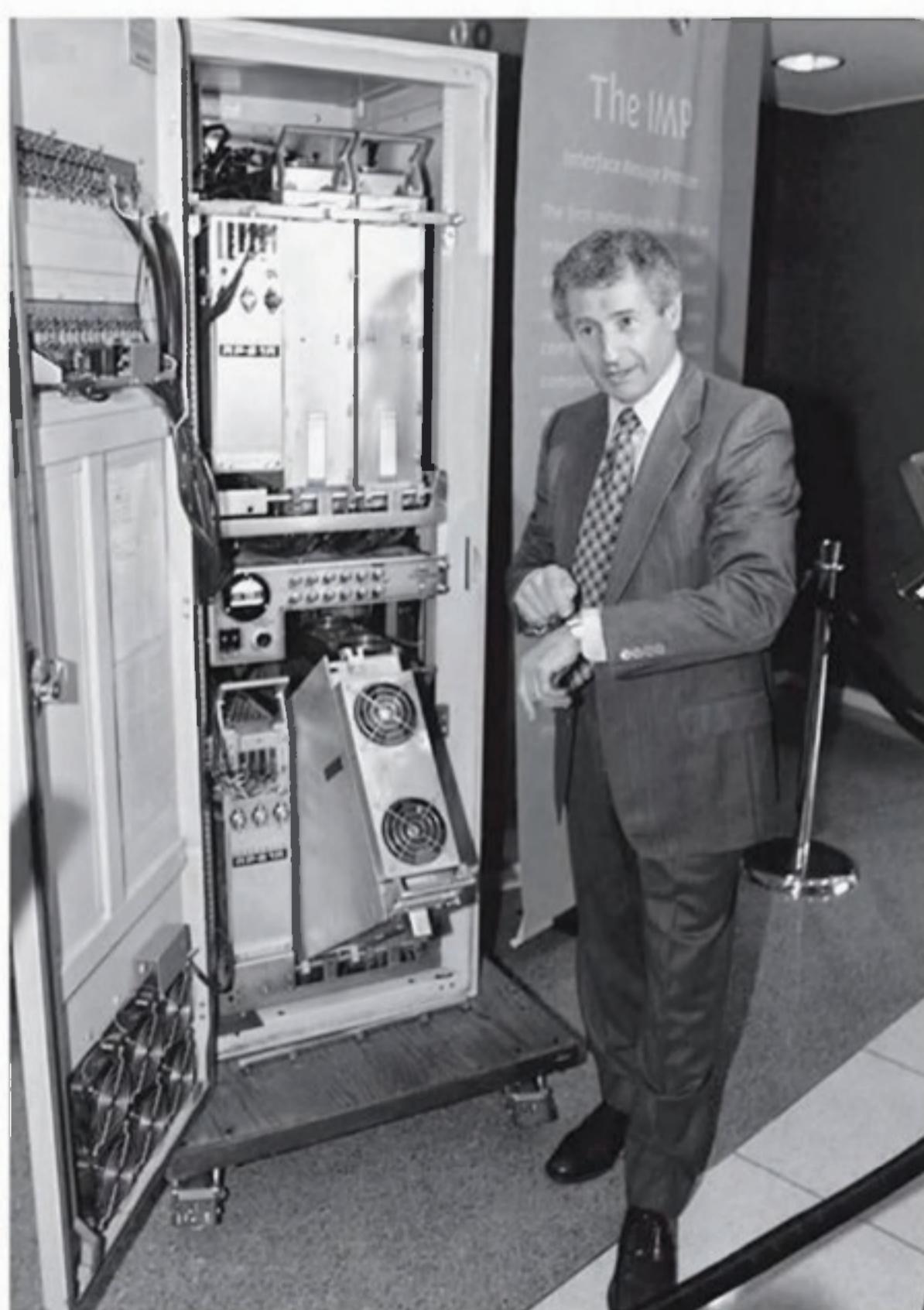


Figura 1.26 Um dos primeiros processadores de mensagens de interface (IMP) e L. Kleinrock (Mark J. Terrill, AP/Wide World Photos)

1.7.2 Redes proprietárias e trabalho em rede: 1972-1980

A ARPAnet inicial era um rede isolada, fechada. Para se comunicar com uma máquina da ARPAnet, era preciso estar ligado a um outro IMP dessa rede. Do inicio a meados de 1970, surgiram novas redes independentes de comutação de pacotes:

- ALOHAnet, uma rede de micro-ondas ligando universidades das ilhas do Havaí [Abramson, 1970], bem como as redes de pacotes por satélite [RFC 829] e por rádio [Kahn, 1978] da DARPA [Kahn, 1978];
- Telenet, uma rede comercial de comutação de pacotes da BBN fundamentada na tecnologia ARPAnet;
- Cyclades, uma rede de comutação de pacotes pioneira na França, montada por Louis Pouzin [Think, 2002];
- redes de tempo compartilhado como a Tymnet e a rede GE Information Services, entre outras que surgiram no final da década de 1960 e início da década de 1970 [Schwartz, 1977];
- rede SNA da IBM (1969-1974), cujo trabalho comparava-se ao da ARPAnet [Schwartz, 1977].

O número de redes estava crescendo. Hoje, com perfeita visão do passado, podemos perceber que aquela era a hora certa para desenvolver uma arquitetura abrangente para conectar redes. O trabalho pioneiro de interconexão de redes, sob o patrocínio da DARPA (Defense Advanced Research Projects Agency — Agencia de Projetos de Pesquisa Avançada de Defesa), criou em essência *uma rede de redes* e foi realizado por Vinton Cerf e Robert Kahn [Cerf, 1974]; o termo *internettting* foi cunhado para descrever esse trabalho.

Esses princípios de arquitetura foram incorporados ao TCP. As primeiras versões desse protocolo, contudo, eram muito diferentes do TCP de hoje. Aquelas versões combinavam uma entrega sequencial confiável de dados via retransmissão por sistema final (que ainda faz parte do TCP de hoje) com funções de envio (que hoje são desempenhadas pelo IP). As primeiras experiências com o TCP, combinadas com o reconhecimento da importância de um serviço de transporte sim a sim não confiável, sem controle de fluxo, para aplicações como voz em pacotes, levaram à separação entre IP e TCP e ao desenvolvimento do protocolo UDP. Os três protocolos fundamentais da Internet que temos hoje — TCP, UDP e IP — estavam conceitualmente disponíveis no final da década de 1970.

Além das pesquisas sobre a Internet realizadas pela DARPA, muitas outras atividades importantes relacionadas ao trabalho em rede estavam em curso. No Havaí, Norman Abramson estava desenvolvendo a ALOHAnet, uma rede de pacotes por rádio que permitia que vários lugares remotos das ilhas havaianas se comunicassem entre si. O ALOHA [Abramson, 1970] foi o primeiro protocolo de acesso múltiplo que permitiu que usuários distribuídos em diferentes localizações geográficas compartilhassem um único meio de comunicação broadcast (uma frequência de rádio). O trabalho de Abramson sobre protocolo de múltiplo acesso foi aprimorado por Metcalfe e Boggs com o desenvolvimento do protocolo Ethernet [Metcalfe, 1976] para redes compartilhadas de transmissão broadcast por fio; veja a Figura 1.27.

O interessante é que o protocolo Ethernet de Metcalfe e Boggs foi motivado pela necessidade de conectar vários PCs, impressoras e discos compartilhados [Perkins, 1994]. Há 25 anos, bem antes da revolução do PC e da explosão das redes, Metcalfe e Boggs estavam lançando as bases para as LANs de PCs de hoje. A tecnologia Ethernet representou uma etapa importante para o trabalho em redes interconectadas. Cada rede Ethernet local era, em si, uma rede, e, à medida que o número de LANs aumentava, a necessidade de interconectar essas redes foi se tornando cada vez mais importante. Discutiremos detalhadamente a tecnologia Ethernet, ALOHA e outras tecnologias de LAN no Capítulo 5.

1.7.3 Proliferação de redes: 1980-1990

Ao final da década de 1970, aproximadamente 200 máquinas estavam conectadas à ARPAnet. Ao final da década de 1980, o número de máquinas ligadas à Internet pública, uma confederação de redes muito parecida com a Internet de hoje, alcançaria cem mil. A década de 1980 seria uma época de formidável crescimento.

Grande parte daquele crescimento foi consequência de vários esforços distintos para criar redes de computadores para interligar universidades. A BITNET processava e-mails e fazia transferência de arquivos entre diversas universidades do nordeste dos Estados Unidos. A CSNET (computer science network — rede da ciência de com-

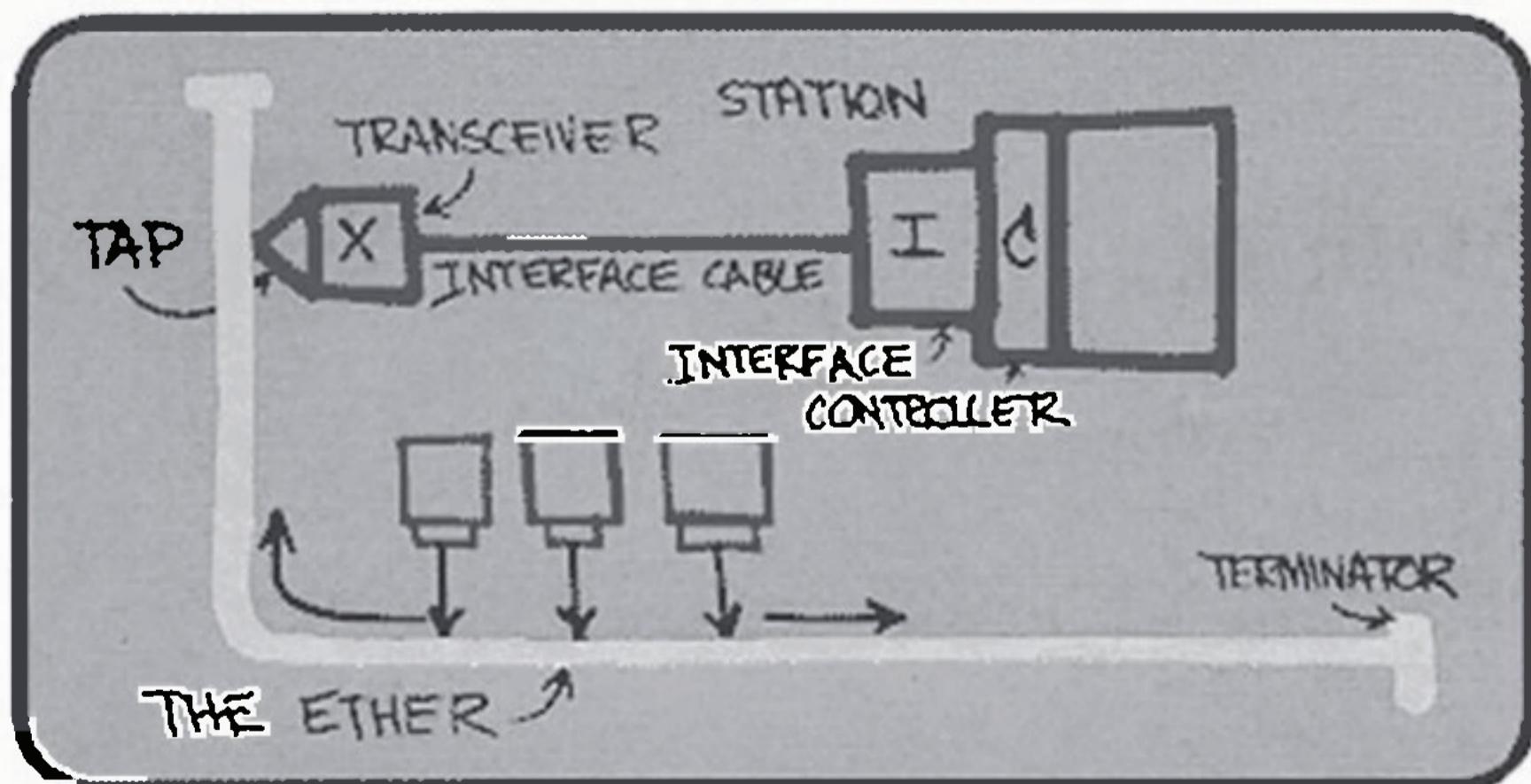


Figura 1.27 A concepção original de Metcalfe para a Ethernet

putadores) foi formada para interligar pesquisadores de universidades que não tinham acesso à ARPAnet. Em 1986, foi criada a NSFNET para prover acesso a centros de supercomputação patrocinados pela NSF. Partindo de uma velocidade inicial de 56 kbps, ao final da década o backbone da NSFNET estaria funcionando a 1,5 Mbps e servindo como backbone primário para a interligação de redes regionais.

Na comunidade da ARPAnet, já estavam sendo encaixados muitos dos componentes finais da arquitetura da Internet de hoje. No dia 1º de janeiro de 1983, o TCP/IP foi adotado oficialmente como o novo padrão de protocolo de máquinas para a ARPAnet (em substituição ao protocolo NCP). Devido à importância do evento, o dia da transição do NCP para o TCP/IP [RFC 801] foi marcado com antecedência — a partir daquele dia todas as máquinas tiveram de adotar o TCP/IP. No final da década de 1980, foram agregadas importantes extensões ao TCP para implementação do controle de congestionamento baseado em hospedeiros [Jacobson, 1988]. Também foi desenvolvido o sistema de nomes de domínios (DNS) utilizado para mapear nomes da Internet fáceis de entender (por exemplo, *gaia.cs.umass.edu*) para seus endereços IP de 32 bits [RFC 1034]. Paralelamente ao desenvolvimento da ARPAnet (que em sua maior parte deve-se aos Estados Unidos), no início da década de 1980 os franceses lançaram o projeto Minitel, um plano ambicioso para levar as redes de dados para todos os lares. Patrocinado pelo governo francês, o sistema Minitel consistia em uma rede pública de comutação de pacotes (baseada no conjunto de protocolos X.25, que usava circuitos virtuais), servidores Minitel e terminais baratos com modems de baixa velocidade embutidos. O Minitel transformou-se em um enorme sucesso em 1984, quando o governo francês forneceu, gratuitamente, um terminal para toda residência francesa que quisesse. O sistema Minitel incluía sites de livre acesso — como o da lista telefônica — e também sites particulares, que cobravam uma taxa de cada usuário baseada no tempo de utilização. No seu auge, em meados de 1990, o Minitel oferecia mais de 20 mil serviços, que iam desde home banking até bancos de dados especializados para pesquisa. Era usado por mais de 20 por cento da população da França, gerava receita de mais de um bilhão de dólares por ano e criou dez mil empregos. Estava presente em grande parte dos lares franceses dez anos antes de a maioria dos norte-americanos ouvir falar de Internet.

1.7.4 A explosão da Internet: a década de 1990

A década de 1990 estreou com vários eventos que simbolizaram a evolução contínua e a comercialização iminente da Internet. A ARPAnet, a progenitora da Internet, deixou de existir. Durante a década de 1980, a MILNET e a Defense Data Network (Rede de Dados de Defesa) cresceram e passaram a carregar a maior parte do tráfego do Departamento de Defesa dos Estados Unidos e a NSFNET começou a servir como uma rede de backbone conectando redes regionais nos Estados Unidos com nacionais no exterior. Em 1991, a NSFNET extinguiu as restrições que impunha à sua utilização com finalidades comerciais, mas, em 1995, perderia seu mandato quando o tráfego de backbone da Internet passou a ser carregado por provedores de serviços de Internet.

O principal evento da década de 1990, no entanto, foi o surgimento da World Wide Web, que levou a Internet para os lares e as empresas de milhões de pessoas no mundo inteiro. A Web serviu também como plataforma para a habilitação e a disponibilização de centenas de novas aplicações, inclusive negociação de ações e serviços bancários on-line, serviços multimídia em tempo real e serviços de recuperação de informações. Para um breve histórico dos primórdios da Web, consulte [W3C, 1995].

A Web foi inventada no CERN (European Center for Nuclear Physics — Centro Europeu para Física Nuclear) por Tim Berners-Lee entre 1989 e 1991 [Berners-Lee, 1989], com base em ideias originadas de trabalhos anteriores sobre hipertexto realizados por Bush [Bush, 1945], na década de 1940, e por Ted Nelson [Ziff-Davis, 1998], na década de 1960. Berners-Lee e seus companheiros desenvolveram versões iniciais de HTML, HTTP, um servidor para a Web e um browser — os quatro componentes fundamentais da Web. Os browsers originais do CERN ofereciam apenas uma interface de linha de comando. Perto do final de 1992 havia aproximadamente 200 servidores Web em operação, e esse conjunto de servidores era apenas uma amostra do que estava por vir. Nessa época, vários pesquisadores estavam desenvolvendo browsers da Web com interfaces GUI (*graphical user interface* — interface gráfica de usuário), entre eles Marc Andreessen, que liderou o desenvolvimento do popular browser Mosaic. Em 1994, Marc Andreessen e Jim Clark formaram a Mosaic Communications, que mais

tarde se transformou na Netscape Communications Corporation [Cusumano, 1998; Quittner, 1998]. Em 1995, estudantes universitários estavam usando browsers Mosaic e Netscape para navegar na Web diariamente. Nessa época, empresas — grandes e pequenas — começaram a operar servidores Web e a realizar transações comerciais pela Web. Em 1996, a Microsoft começou a fabricar browsers, dando início à guerra dos browsers entre Netscape e Microsoft, vencida pela última alguns anos mais tarde.

A segunda metade da década de 1990 foi um período de tremendo crescimento e inovação para a Internet, com grandes corporações e milhares de novas empresas criando produtos e serviços para a Internet. O correio eletrônico pela Internet (e-mail) continuou a evoluir com leitores ricos em recursos provendo agendas de endereços, anexos, hot links e transporte de multimídia. No final do milênio a Internet dava suporte a centenas de aplicações populares, entre elas quatro de enorme sucesso:

- e-mail, incluindo anexos e correio eletrônico com acesso pela Web;
- a Web, incluindo navegação pela Web e comércio pela Internet;
- serviço de mensagem instantânea, com listas de contato, cujo pioneiro foi o ICQ;
- compartilhamento peer-to-peer de arquivos MP3, cujo pioneiro foi o Napster.

O interessante é que as duas primeiras dessas aplicações de sucesso arrasador vieram da comunidade de pesquisas, ao passo que as duas últimas foram criadas por alguns jovens empreendedores.

No período de 1995 a 2001, a Internet realizou uma viagem vertiginosa nos mercados financeiros. Antes mesmo de se mostrarem lucrativas, centenas de novas empresas da Internet faziam suas ofertas públicas iniciais de ações e começavam a ser negociadas em bolsas de valores. Muitas empresas eram avaliadas em bilhões de dólares sem ter nenhum fluxo significativo de receita. As ações da Internet sofreram uma queda também vertiginosa em 2000-2001, e muitas novas empresas fecharam. Não obstante, várias empresas surgiram como grandes vencedoras no mundo da Internet (mesmo que os preços de suas ações tivessem sofrido com aquela queda), entre elas Microsoft, Cisco, Yahoo, e-Bay, Google e Amazon.

1.7.5 Desenvolvimentos recentes

A inovação na área de redes de computadores continua a passos largos. Há progressos em todas as frentes, incluindo desenvolvimento de novas aplicações, distribuição de conteúdo, telefonia por Internet, velocidades de transmissão mais altas em LANs e roteadores mais rápidos. Mas três desenvolvimentos merecem atenção especial: a proliferação de redes de acesso de alta velocidade (incluindo acesso sem fio), a segurança e as redes P2P.

Como discutimos na Seção 1.2, a penetração cada vez maior do acesso residencial de banda larga à Internet via modem a cabo e DSL montou o cenário para uma profusão de novas aplicações multimídia, entre elas voz e vídeo sobre IP [Skype, 2009], compartilhamento de vídeo [Youtube, 2009] e televisão sobre IP [PPLive, 2009]. A crescente onipresença de redes Wi-Fi públicas de alta velocidade (11 Mbps e maiores) e de acesso de média velocidade (centenas de kbps) à Internet por redes de telefonia celular não está apenas possibilitando conexão constante, mas também habilitando um novo conjunto muito interessante de serviços específicos para localizações determinadas. Abordaremos redes sem fio e mobilidade no Capítulo 6.

Em seguida a uma série de ataques de recusa de serviço em importantes servidores Web no final da década de 1990 e à proliferação de ataques de worms (por exemplo, o Blaster) que infectam sistemas finais e emperram a rede com tráfego excessivo, a segurança da rede tornou-se uma questão extremamente importante. Esses ataques resultaram no desenvolvimento de sistemas de detecção de intrusão capazes de prevenir ataques com antecedência, na utilização de firewalls para filtrar tráfego indesejado antes que entre na rede. Abordaremos vários tópicos importantes relacionados à segurança no Capítulo 8.

A última inovação que queremos destacar são as redes P2P. Uma aplicação de rede P2P explora os recursos de computadores de usuários — armazenagem, conteúdo, ciclos de CPU e presença humana — e tem significativa autonomia em relação a servidores centrais. A conectividade dos computadores de usuários (isto é, dos pares, ou peers) normalmente é intermitente. Há alguns anos, houve diversas histórias de sucesso com o P2P, incluindo o compartilha-

mento de arquivo P2P (Napster, Kazaa, Gnutella, eDonkey, Lime Wire etc.), distribuição de arquivos (BitTorrent), Voz sobre IP (Skype) e IPTV (PPLive, ppStream). Muitas dessas aplicações P2P serão discutidas no Capítulo 2.

1.8 Resumo

Neste capítulo, abordamos uma quantidade imensa de assuntos. Examinamos as várias peças de hardware e software que compõem a Internet, em especial, e redes de computadores, em geral. Começamos pela periferia da rede, examinando sistemas finais e aplicações, além do serviço de transporte fornecido às aplicações que executam nos sistemas finais. Também vimos as tecnologias de camada de enlace e meio físico normalmente encontrados na rede de acesso. Em seguida, mergulhamos no interior da rede e chegamos ao seu núcleo, identificando comutação de pacotes e comutação de circuitos como as duas abordagens básicas do transporte de dados por uma rede de telecomunicações, expondo os pontos fortes e fracos de cada uma delas. Examinamos, então, as partes inferiores (do ponto de vista da arquitetura) da rede — as tecnologias de camada de enlace e os meios físicos comumente encontrados na rede de acesso. Examinamos também a estrutura da Internet global e aprendemos que ela é uma rede de redes. Vimos que a estrutura hierárquica da Internet, composta de ISPs de níveis mais altos e mais baixos, permitiu que ela se expandisse e incluísse milhares de redes.

Na segunda parte deste capítulo introdutório, abordamos diversos tópicos fundamentais da área de redes de computadores. Primeiramente examinamos as causas de atrasos e perdas de pacotes em uma rede de comutação de pacotes. Desenvolvemos modelos quantitativos simples de atrasos de transmissão, de propagação e de fila; esses modelos de atrasos serão muito usados nos problemas propostos em todo o livro. Em seguida examinamos camadas de protocolo e modelos de serviço, princípios fundamentais de arquitetura de redes aos quais voltaremos a nos referir neste livro. Analisamos também alguns dos ataques mais comuns na Internet atualmente. Terminamos nossa introdução sobre redes com uma breve história das redes de computadores. O primeiro capítulo constitui um minicurso sobre redes de computadores.

Portanto, percorremos realmente um extraordinário caminho neste primeiro capítulo! Se você estiver um pouco assustado, não se preocupe. Abordaremos todas essas ideias em detalhes nos capítulos seguintes (é uma promessa, e não uma ameaça!). Por enquanto, esperamos que, ao encerrar este capítulo, você tenha adquirido uma noção, ainda que incipiente, das peças que formam uma rede, um domínio ainda em desenvolvimento do vocabulário (não se acanhe de voltar aqui para consulta) e um desejo cada vez maior de aprender mais sobre redes. Esta é a tarefa que nos espera no restante deste livro.

O guia deste livro

Antes de iniciarmos qualquer viagem, sempre é bom consultar um guia para nos familiarizar com as estradas principais e desvios que encontraremos pela frente. O destino final da viagem que estamos prestes a empreender é um entendimento profundo do como, do quê e do porque das redes de computadores. Nossa guia é a sequência de capítulos deste livro:

1. Redes de computadores e a Internet
2. Camada de aplicação
3. Camada de transporte
4. Camada de rede
5. Camada de enlace e redes locais (LANs)
6. Sem fio e redes móveis
7. Redes multimídia
8. Segurança em redes de computadores
9. Gerenciamento de rede

Os capítulos 2 a 5 são os quatro capítulos centrais deste livro. Note que esses capítulos estão organizados segundo as quatro camadas superiores da pilha de cinco camadas de protocolos da Internet, com um capítulo para

cada camada. Note também que nossa jornada começará no topo da pilha de protocolos da Internet, a saber, a camada de aplicação, e prosseguirá daí para baixo. O princípio racional que orienta essa jornada de cima para baixo é que, entendidas as aplicações, podemos compreender os serviços de rede necessários para dar suporte a elas. Então, poderemos examinar, um por um, os vários modos como esses serviços poderiam ser implementados por uma arquitetura de rede. Assim, o estudo das aplicações logo no início dá motivação para o restante do livro.

A segunda metade deste livro — capítulos 6 a 9 — aborda quatro tópicos extremamente importantes (e de certa maneira independentes) de redes modernas. No Capítulo 6, examinamos tecnologia sem fio e mobilidade, incluindo LANs sem fio (Wi-Fi, WiMAX e Bluetooth), redes de telefonia celular (GSM) e mobilidade (nas redes IP e GSM). No Capítulo 7 (Redes multimídia), examinamos aplicações de áudio e vídeo, como telefone por Internet, videoconferência e recepção de mídia armazenada. Examinamos também como uma rede de comutação de pacotes pode ser projetada para prover serviço de qualidade consistente para aplicações de áudio e vídeo. No Capítulo 8 (Segurança em redes de computadores), analisamos, primeiramente, os fundamentos da criptografia e da segurança de redes e, em seguida, de que modo a teoria básica está sendo aplicada a um amplo leque de contextos da Internet. No último capítulo (Gerenciamento de redes), examinamos as questões fundamentais do gerenciamento de redes, bem como os protocolos primários da Internet utilizados para esse fim.



Exercícios de fixação

Capítulo 1 Questões de revisão

Seção 1.1

1. Qual é a diferença entre um hospedeiro e um sistema final? Cite os tipos de sistemas finais. Um servidor Web é um sistema final?
2. A palavra protocolo é muito usada para descrever relações diplomáticas. Dê um exemplo de um protocolo diplomático.

Seção 1.2

3. O que é um programa cliente? O que é um programa servidor? Um programa servidor requisita e recebe serviços de um programa cliente?
4. Cite seis tecnologias de acesso. Classifique cada uma delas nas categorias acesso residencial, acesso corporativo ou acesso móvel.
5. A taxa de transmissão HFC é dedicada ou é compartilhada entre usuários? É possível haver colisões na direção provedor-usuário de um canal HFC? Por quê?
6. Cite seis tecnologias de acesso residencial disponíveis em sua cidade. Para cada tipo de acesso, apresente a taxa downstream, a taxa upstream e o preço mensal anunciados.
7. Qual é a taxa de transmissão de LANs Ethernet? Para uma dada taxa de transmissão, cada usuário da LAN pode transmitir continuamente a essa taxa?

8. Cite alguns meios físicos utilizados para instalar a Ethernet.
9. Modems discados, HFC e ADSL são usados para acesso residencial. Para cada uma dessas tecnologias de acesso, cite uma faixa de taxas de transmissão e comente se a largura de banda é compartilhada ou dedicada.
10. Descreva as tecnologias de acesso sem fio mais populares atualmente. Faça uma comparação entre elas.

Seção 1.3

11. Qual é a vantagem de uma rede de comutação de circuitos em relação a uma de comutação de pacotes? Quais são as vantagens da TDM sobre a FDM em uma rede de comutação de circuitos?
12. Por que se afirma que a comutação de pacotes emprega multiplexação estatística? Compare a multiplexação estatística com a multiplexação que ocorre em TDM.
13. Suponha que exista exatamente um comutador de pacotes entre um computador de origem e um de destino. As taxas de transmissão entre a máquina de origem e o comutador e entre este e a máquina de destino são R_1 e R_2 , respectivamente. Admitindo que um roteador use comutação de pacotes do tipo armazena e reenvia, qual é o atraso total fim a fim para enviar um pacote de comprimento L ? (Desconsidere

- formação de fila, atraso de propagação e atraso de processamento).
14. Qual é principal diferença que distingue ISPs de nível 1 e de nível 2?
- Suponha que usuários compartilhem um enlace de 2 Mbps e que cada usuário transmita continuamente a 1 Mbps, mas cada um deles transmite apenas 20 por cento do tempo. (Veja a discussão sobre multiplexação estatística na Seção 1.3).
- Quando a comutação de circuitos é utilizada, quantos usuários podem usar o enlace?
 - Para o restante deste problema, suponha que seja utilizada a comutação de pacotes. Por que não haverá atraso de fila antes de um enlace se dois ou menos usuários transmitirem ao mesmo tempo? Por que haverá atraso de fila se três usuários transmitirem ao mesmo tempo?
 - Determine a probabilidade de um dado usuário estar transmitindo.
 - Suponha agora que haja três usuários. Determine a probabilidade de, a qualquer momento, os três usuários transmitirem simultaneamente. Determine a fração de tempo durante o qual a fila cresce.
- Seção 1.4**
16. Considere o envio de um pacote de uma máquina de origem a uma de destino por uma rota fixa. Relacione os componentes do atraso que formam o atraso fim a fim. Quais deles são constantes e quais são variáveis?
17. Visite o applet "Transmission versus Propagation Delay" no Companion Website. Entre as taxas, o atraso de propagação e os tamanhos de pacote disponíveis, determine uma combinação para a qual o emissor termine de transmitir antes que o primeiro bit do pacote chegue ao receptor.
18. Quanto tempo um pacote de 1.000 bytes leva para se propagar através de um enlace de 2.500 km de distância, com uma velocidade de propagação de $2.5 \cdot 10^8$ m/s e uma taxa de transmissão de 2 Mbps? Geralmente, quanto tempo um pacote de comprimento L leva para se propagar através de um enlace de distância d , velocidade de propagação s , e taxa de transmissão de R bps? Esse atraso depende do comprimento do pacote? Esse atraso depende da taxa de transmissão?
19. Suponha que o Hospedeiro A queira enviar um arquivo grande para o Hospedeiro B. O percurso do Hospedeiro A para o Hospedeiro B possui três enlaces, de taxas $R_1 = 500$ kbps, $R_2 = 2$ Mbps, e $R_3 = 1$ Mbps.
- Considerando que não haja nenhum outro tráfego na rede, qual é a vazão para a transferência de arquivo?
 - Suponha que o arquivo tenha 4 milhões de bytes. Dividindo o tamanho do arquivo pela vazão, quanto tempo levará a transferência para o Hospedeiro B?
 - Repita os itens "a" e "b", mas agora com R_1 reduzido a 100 kbps.
20. Suponha que o sistema final A queira enviar um arquivo grande para o sistema B. Em um nível muito alto, descreva como o sistema A cria pacotes a partir do arquivo. Quando um desses arquivos chegar ao comutador de pacote, quais informações no pacote o comutador utiliza para determinar o enlace através do qual o pacote é encaminhado? Por que a comutação de pacote na Internet é análoga a dirigir de uma cidade para outra pedindo informações ao longo do caminho?
21. Visite o applet "Queuing and Loss" no Companion Website. Qual é a taxa de emissão máxima e a taxa de emissão mínima? Com essas taxas, qual é a intensidade do tráfego? Execute o applet com essas taxas e determine o tempo que leva a ocorrência de uma perda de pacote. Repita o procedimento uma segunda vez e determine novamente o tempo de ocorrência para a perda de pacote. Os resultados são diferentes? Por quê? Por que não?
- Seção 1.5**
22. Cite cinco tarefas que uma camada pode executar. É possível que uma (ou mais) dessas tarefas seja(m) realizada(s) por duas (ou mais) camadas?
23. Quais são as cinco camadas da pilha de protocolo da Internet? Quais as principais responsabilidades de cada uma dessas camadas?
24. O que é uma mensagem de camada de aplicação? Um segmento de camada de transporte? Um datagrama de camada de rede? Um quadro de camada de enlace?
25. Que camadas da pilha do protocolo da Internet um roteador implementa? Que camadas um comutador de camada de enlace implementa? Que camadas um sistema final implementa?
- Seção 1.6**
26. Qual é a diferença entre um vírus, um worm e um cavalo de Troia?
27. Descreva como pode ser criado uma botnet e como ela pode ser utilizada no ataque DDoS.

28. Suponha que Alice e Bob estejam enviando pacotes um para o outro através de uma rede de computadores e que Trudy se posicione na rede para que ela consiga capturar todos os pacotes enviados por Alice

e enviar o que quiser para Bob; ela também consegue capturar todos os pacotes enviados por Bob e enviar o que quiser para Alice. Cite algumas atitudes maliciosas que Trudy pode fazer a partir de sua posição.



Problemas

1. Projete e descreva um protocolo de nível de aplicação para ser usado entre um caixa automático e o computador central de um banco. Esse protocolo deve permitir verificação do cartão e da senha de um usuário, consulta do saldo de sua conta (que é mantido no computador central) e saque de dinheiro da conta corrente (isto é, entrega de dinheiro ao usuário). As entidades do protocolo devem estar preparadas a resolver o caso comum em que não há dinheiro suficiente na conta do usuário para cobrir o saque. Faça uma especificação de seu protocolo relacionando as mensagens trocadas e as ações realizadas pelo caixa automático ou pelo computador central do banco na transmissão e recepção de mensagens. Esquematize a operação de seu protocolo para o caso de um saque simples sem erros, usando um diagrama semelhante ao da Figura 1.2. Descreva explicitamente o que seu protocolo espera do serviço de transporte fim a fim.
2. Considere uma aplicação que transmita dados a uma taxa constante (por exemplo, a origem gera uma unidade de dados de N bits a cada k unidades de tempo, onde k é pequeno e fixo). Considere também que, quando essa aplicação começa, continuará em funcionamento por um período de tempo relativamente longo. Responda às seguintes perguntas, dando uma breve justificativa para suas respostas:
 - a. O que seria mais apropriado para essa aplicação: uma rede de comutação de circuitos ou uma rede de comutação de pacotes? Por quê?
 - b. Suponha que seja usada uma rede de comutação de pacotes e que o único tráfego dessa rede venha de aplicações como a descrita anteriormente. Além disso, admita que a soma das velocidades de dados da aplicação seja menor do que a capacidade de cada um dos enlaces. Será necessário algum tipo de controle de congestionamento? Por quê?
3. Considere a rede de comutação de circuitos da Figura 1.12. Lembre-se de que há n circuitos em cada enlace.
 - a. Qual é o número máximo de conexões simultâneas que podem estar em curso a qualquer instante nessa rede?
4. Suponha que todas as conexões sejam entre o comutador do canto superior esquerdo e o comutador do canto inferior direito. Qual é o número máximo de conexões simultâneas que podem estar em curso?
 - a. Considere novamente a analogia do comboio de carros da Seção 1.4. Admita uma velocidade de propagação de 100 km/h.
 - a. Suponha que o comboio viaje 150 km, começando em frente ao primeiro dos postos de pedágio, passando por um segundo e terminando após um terceiro. Qual é o atraso fim a fim?
 - b. Repita o item 'a' admitindo agora que haja sete carros no comboio em vez de dez.
 - b. Este problema elementar começa a explorar atrasos de propagação e de transmissão, dois conceitos centrais em redes de computadores. Considere dois computadores, A e B, conectados por um único enlace de taxa R bps. Suponha que esses computadores estejam separados por m metros e que a velocidade de propagação ao longo do enlace seja de s metros/segundo. O computador A tem de enviar um pacote de L bits ao computador B.
 - a. Expresse o atraso de propagação, d_{prop} , em termos de m e s .
 - b. Determine o tempo de transmissão do pacote, d_{trans} , em termos de L e R .
 - c. Ignorando os atrasos de processamento e de fila, obtenha uma expressão para o atraso fim a fim.
 - d. Suponha que o computador A comece a transmitir o pacote no instante $t = 0$. No instante $t = d_{trans}$, onde estará o último bit do pacote?
 - e. Suponha que d_{prop} seja maior do que d_{trans} . Onde estará o primeiro bit do pacote no instante $t = d_{trans}$?
 - f. Suponha que d_{prop} seja menor do que d_{trans} . Onde estará o primeiro bit do pacote no instante $t = d_{trans}$?
 - g. Suponha $s = 2,5 \cdot 10^8$, $L = 100$ bits e $R = 56$ kbps. Encontre a distância m de forma que d_{prop} seja igual a d_{trans} .
 - c. Neste problema, consideramos o envio de voz em tempo real do computador A para o computador

- B por meio de uma rede de comutação de pacotes (VoIP). O computador A converte voz analógica para uma cadeia digital de bits de 64 kbps e, em seguida, agrupa os bits em pacotes de 56 bytes. Há apenas um enlace entre os computadores A e B; sua taxa de transmissão é de 2 Mbps e seu atraso de propagação, de 10 milissegundos. Assim que o computador A recolhe um pacote, ele o envia ao computador B. Quando recebe um pacote completo, o computador B converte os bits do pacote em um sinal analógico. Quanto tempo decorre entre o momento em que um bit é criado (a partir do sinal analógico no computador A) e o momento em que ele é decodificado (como parte do sinal analógico no computador B)?
7. Suponha que usuários compartilhem um enlace de 3 Mbps e que cada usuário precise de 150 kbps para transmitir, mas que transmita apenas durante 10 por cento do tempo. (Veja a discussão sobre multiplexação estatística na Seção 1.3.)
 - a. Quando é utilizada comutação de circuitos, quantos usuários podem ter suporte?
 - b. Suponha que haja 120 usuários. Determine a probabilidade que, a um tempo dado, exatamente n usuários estejam transmitindo simultaneamente. (Dica: Use a distribuição binomial.)
 - c. Determine a probabilidade de haver 21 ou mais usuários transmitindo simultaneamente.
 8. Considere a discussão na Seção 1.3 sobre multiplexação estatística, na qual é dado um exemplo com um enlace de 1 Mbps. Quando em atividade, os usuários estão gerando dados a uma taxa de 100 kbps; mas a probabilidade de estarem em atividade, gerando dados, é de $p = 0,1$. Suponha que o enlace de 1 Mbps seja substituído por um enlace de 1 Gbps.
 - a. Qual é o número máximo de usuários, N , que pode ser suportado simultaneamente por comutação de pacotes?
 - b. Agora considere comutação de circuitos e um número M de usuários. Elabore uma fórmula (em termos de p , M , N) para a probabilidade de que mais de N usuários estejam enviando dados.
 9. Considere um pacote de comprimento L que se inicia no sistema final A e percorre três enlaces até um sistema final de destino. Esses três enlaces estão conectados por dois comutadores de pacotes. Suponha que d_i , s_i e R_i representem o comprimento, a velocidade de propagação e a taxa de transmissão do enlace i , sendo $i = 1, 2, 3$. O comutador de pacote atrasa cada pacote por d_{proc} . Considerando que não haja nenhum atraso de fila, em relação a d_i , s_i e R_i ($i = 1, 2, 3$) e L , qual é o atraso fim a fim total para o pacote? Suponha agora que o pacote tenha 1.500 bytes, a velocidade de propagação de ambos enlaces seja $2,5 \cdot 10^8$ m/s, as taxas de transmissão dos três enlaces sejam 2 Mbps, o atraso de processamento do comutador de pacote seja de 3 milissegundos, o comprimento do primeiro enlace seja 5.000 km, o comprimento do segundo seja 4.000 km e do último seja 1.000 km. Dados esses valores, qual é o atraso fim a fim?
 10. No problema anterior, suponha que $R_1 = R_2 = R_3 = R$ e $d_{\text{proc}} = 0$. Suponha que o comutador de pacote não armazena e envia pacotes, mas transmite imediatamente cada bit recebido antes de esperar o pacote chegar. Qual é o atraso fim a fim?
 11. Um comutador de pacote recebe um pacote e determina o enlace de saída pelo qual o pacote deve ser enviado. Quando o pacote chega, um outro já está sendo transmitido nesse enlace de saída e outros quatro já estão esperando para serem transmitidos. Os pacotes são transmitidos em ordem de chegada. Suponha que todos os pacotes tenham 1.500 bytes e que a taxa do enlace seja 2 Mbps. Qual é o atraso de fila para o pacote? Em um amplo sentido, qual é o atraso de fila quando todos os pacotes possuem comprimento L , o enlace possui uma taxa de transmissão $R \times$ bits do pacote sendo enviado já foram transmitidos e N pacotes já estão na fila?
 12. Suponha que N pacotes cheguem simultaneamente ao enlace no qual não há pacotes sendo transmitidos e nem pacotes enfileirados. Cada pacote tem L de comprimento e é transmitido à taxa R . Qual é o atraso médio para os N pacotes?
 13. Considere o atraso de fila em um buffer de roteador (antes de um enlace de saída). Suponha que todos os pacotes tenham L bits, que a taxa de transmissão seja de R bps e que N pacotes cheguem simultaneamente ao buffer a cada LN/R segundos. Determine o atraso de fila médio para um pacote. (Dica: o atraso de fila para o primeiro pacote é zero; para o segundo pacote, L/R ; para o terceiro pacote, $2L/R$. O pacote de ordem N já terá sido transmitido quando o segundo lote de pacotes chegar.)
 14. Considere o atraso de fila em um buffer de roteador, sendo I a intensidade de tráfego; isto é, $I = La/R$. Suponha que o atraso de fila tome a forma de IL/R ($1 - I$) para $I < 1$.
 - a. Deduza uma fórmula para o atraso total, isto é, para o atraso de fila mais o atraso de transmissão.
 - b. Faça um gráfico do atraso total como uma função de L/R .
 15. Sendo α a taxa de pacotes que chegam a um enlace em pacotes/s, e μ a taxa de transmissão de enlaces em pacotes/s, baseado na fórmula do atraso total (isto é, o atraso de fila mais o atraso de transmissão) do problema anterior, deduza uma fórmula para o atraso total em relação a α e μ .

16. Considere um buffer de roteador antes de um enlace de saída. Neste problema, você usará a fórmula de Little, uma famosa fórmula da teoria das filas. Sendo N o número médio de pacotes no buffer mais o pacote sendo transmitido, a a taxa de pacotes que chegam no enlace, e d o atraso total médio (isto é, o atraso de fila mais o atraso de transmissão) sofrido pelo pacote. Dada a fórmula de Little $N = a \cdot d$, suponha que, na média, o buffer contenha 10 pacotes, o atraso de fila de pacote médio seja 10 milissegundos e a taxa de transmissão do enlace seja 100 pacotes/s. Utilizando tal fórmula, qual é a taxa média de chegada de pacote, considerando que não há perda de pacote?
17. a. Generalize a fórmula para o atraso fim a fim na Seção 1.4.3 para taxas de processamento, atrasos de propagação e taxa de transmissão heterogêneos.
b. Repita o item "a", mas suponha também que haja um atraso de fila médio d_{fil} em cada nó.
18. Execute o programa Traceroute para verificar a rota entre uma origem e um destino, no mesmo continente, para três horários diferentes do dia.
a. Determine a média e o desvio padrão dos atrasos de ida e volta para cada um dos três horários.
b. Determine o número de roteadores no caminho para cada um dos três. Os caminhos mudaram em algum dos horários?
c. Tente identificar o número de redes ISPs pelas quais o pacote do Traceroute passa entre origem e destino. Roteadores com nomes semelhantes e/ou endereços IP semelhantes devem ser considerados como parte do mesmo ISP. Em suas respostas, os maiores atrasos ocorrem nas interfaces de formação de pares entre ISPs adjacentes?
d. Faça o mesmo para uma origem e um destino em continentes diferentes. Compare os resultados dentro do mesmo continente com os resultados entre continentes diferentes.
19. Considere o exemplo de vazão correspondente à Figura 1.20 (b). Agora imagine que haja M pares de cliente-servidor em vez de 10. R_s , R_c e R representam as taxas do enlace do servidor, enlaces do cliente e enlace da rede. Suponha que os outros enlaces possuam capacidade abundante e que não haja outro tráfego na rede além daquele gerado pelos M pares de cliente-servidor. Deduza uma expressão geral para a vazão em relação a R_s , R_c , R e M .
20. Considere a Figura 1.19 (b). Agora suponha que haja M percursos entre o servidor e o cliente. Nenhum dos dois percursos compartilham qualquer enlace. O percurso k ($k = 1, \dots, M$) consiste em N_k enlaces com taxas de transmissão $R_1^k, R_2^k, \dots, R_{N_k}^k$. Se o servidor pode usar somente um percurso para enviar dados ao cliente, qual é a vazão máxima que ele pode atingir? Se o servidor pode usar todos os M percursos para enviar dados, qual é a vazão máxima que ele pode atingir?
21. Considere a Figura 1.19 (b). Suponha que cada enlace entre o servidor e o cliente possua uma probabilidade de perda de pacote p , e que as probabilidades de perda de pacote para esses enlaces sejam independentes. Qual é a probabilidade de um pacote (enviado pelo servidor) ser recebido com sucesso pelo receptor? Se o pacote se perder no percurso do servidor para o cliente, então o servidor retransmitirá o pacote. Na média, quantas vezes o servidor retransmitirá o pacote para que o cliente o receba com sucesso?
22. Considere a Figura 1.19 (a). Suponha que o enlace de gargalo ao longo do percurso do servidor para o cliente seja o primeiro com a taxa R_g bps. Imagine que enviamos um par de pacotes um após o outro do servidor para o cliente, e que não haja nenhum outro tráfego nesse percurso. Imagine também que cada pacote de tamanho L bits e os dois enlaces tenham o mesmo atraso de propagação d_{prop}
a. Qual é o tempo entre chegadas ao destino? Isto é, quanto tempo transcorre de quando o último bit do primeiro pacote chega até o último bit do segundo pacote chegar?
b. Agora suponha que o segundo enlace seja o de gargalo (isto é, $R_g < R_s$). É possível que o segundo pacote entre na fila de entrada do segundo enlace? Explique. Agora imagine que o servidor envie o segundo pacote T segundos após enviar o primeiro. Quão grande deve ser T para garantir que não haja nenhuma fila antes do segundo enlace? Explique.
23. Suponha que você queira enviar, urgentemente, 40 terabytes de dados de Boston para Los Angeles. Você tem disponível um enlace dedicado de 100 Mbps para transferência de dados. Você escolheria transmitir os dados por meio desse enlace ou usar o serviço de entrega 24 horas FedEx? Explique.
24. Suponha que dois computadores, A e B, estejam separados por uma distância de 20 mil quilômetros e conectados por um enlace direto de $R = 2$ Mbps. Suponha que a velocidade de propagação pelo enlace seja de $2,5 \cdot 10^8$ metros por segundo.
a. Calcule o produto largura de banda-atraso $R \cdot d_{\text{prop}}$.
b. Considere o envio de um arquivo de 800 mil bits do computador A para o computador B. Suponha que o arquivo seja enviado continuamente, como se fosse uma única grande mensagem. Qual é o número máximo de bits que estará no enlace a qualquer dado instante?

- c. Interprete o produto largura de banda-atraso.
- d. Qual é o comprimento (em metros) de um bit no enlace? É maior do que a de um campo de futebol?
- c. Derive uma expressão geral para o comprimento de um bit em termos da velocidade de propagação s , da velocidade de transmissão R e do comprimento do enlace m .
25. Com referência ao problema 24, suponha que possamos modificar R . Para qual valor de R o comprimento de um bit será o mesmo que o comprimento do enlace?
26. Considere o problema 24, mas agora com um enlace de $R = 1$ Gbps.
- Calcule o produto largura de banda-atraso, $R \cdot d_{\text{prop}}$.
 - Considere o envio de um arquivo de 800 mil bits do computador A para o computador B. Suponha que o arquivo seja enviado continuamente, como se fosse uma única grande mensagem. Qual será o número máximo de bits que estará no enlace a qualquer dado instante?
 - Qual é o comprimento (em metros) de um bit no enlace?
27. Novamente com referência ao problema 24.
- Quanto tempo demora para enviar o arquivo, admitindo que ele seja enviado continuamente?
 - Suponha agora que o arquivo seja fragmentado em 20 pacotes e que cada pacote contenha 40 mil bits. Suponha que cada pacote seja verificado pelo receptor e que o tempo de transmissão de uma verificação de pacote seja desprezível. Finalmente, admita que o emissor não possa enviar um pacote até que o anterior tenha sido reconhecido. Quanto tempo demorará para enviar o arquivo?
 - Compare os resultados de 'a' e 'b'.
- Suponha que haja um enlace de microondas de 10 Mbps entre um satélite geoestacionário e sua estação-base na Terra. A cada minuto o satélite tira uma foto digital e a envia à estação-base. Admita uma velocidade de propagação de $2,4 \cdot 10^8$ metros por segundo.
- Qual é o atraso de propagação do enlace?
 - Qual é o produto largura de banda-atraso, $R \cdot d_{\text{prop}}$?
 - Seja x o tamanho da foto. Qual é o valor mínimo de x para que o enlace de micro-ondas transmita continuamente?
28. Considere a analogia da viagem aérea que utilizamos em nossa discussão sobre camadas na Seção 1.7, e a adição de cabeçalhos a unidades de dados de protocolo enquanto passam por sua pilha. Existe uma noção equivalente de adição de informações de cabeçalho à movimentação de passageiros e suas malas pela pilha de protocolos da linha aérea?
29. Em redes modernas de comutação de pacotes, a máquina de origem segmenta mensagens longas de camada de aplicação (por exemplo, uma imagem ou um arquivo de música) em pacotes menores e os envia pela rede. A máquina destinatária, então, monta novamente os pacotes restaurando a mensagem original. Denominamos esse processo *segmentação de mensagem*. A Figura 1.28 ilustra o transporte sim a sim de uma mensagem com e sem segmentação. Considere que uma mensagem de $8 \cdot 10^6$ bits de comprimento tenha de ser enviada da origem ao destino na Figura 1.28. Suponha que a velocidade de cada enlace da figura seja 2 Mbps. Ignore atrasos de propagação, de fila e de processamento.
- Considere o envio da mensagem da origem ao destino *sem segmentação*. Quanto tempo essa mensagem levará para ir da máquina de origem até o primeiro comutador de pacotes? Tendo em mente que cada comutador usa comutação de pacotes do tipo armazena-e-reenvia, qual é o tempo total para levar a mensagem da máquina de origem à máquina de destino?
 - Agora suponha que a mensagem seja segmentada em 4 mil pacotes, cada um com 2.000 bits de comprimento. Quanto tempo demorará para o primeiro pacote ir da máquina de origem até o primeiro comutador? Quando o primeiro pacote está sendo enviado do primeiro ao segundo comutador, o segundo pacote está sendo enviado da máquina de origem ao primeiro comutador. Em que instante o segundo pacote terá sido completamente recebido no primeiro comutador?
 - Quanto tempo demorará para movimentar o arquivo da máquina de origem até a máquina de destino quando é usada segmentação de mensagem? Compare este resultado com sua resposta na parte 'a' e comente.
 - Discuta as desvantagens da segmentação de mensagem.
30. Experimente o applet "Message Segmentation apresentado" no site Web deste livro. Os atrasos no applet correspondem aos atrasos obtidos no problema anterior? Como os atrasos de propagação no enlace afetam o atraso total sim a sim na comutação de pacotes (com segmentação de mensagem) e na comutação de mensagens?

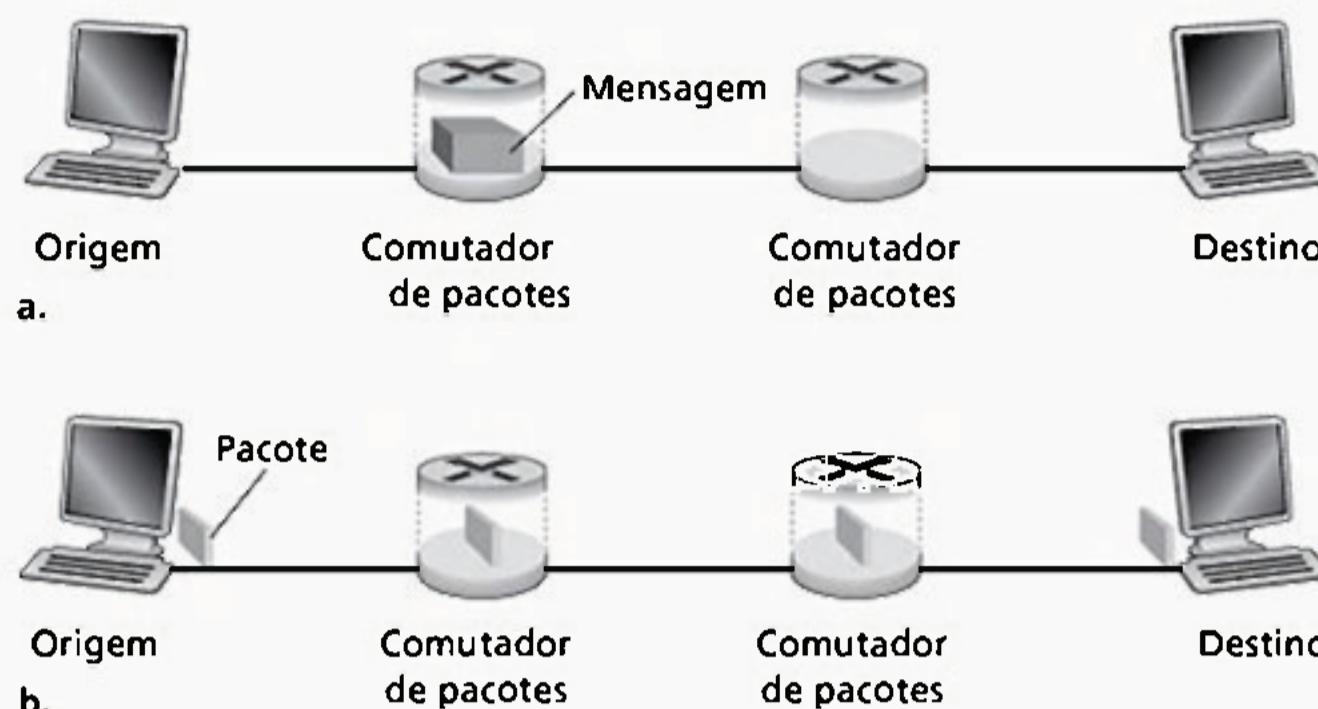


Figura 1.28 Transporte fim a fim de mensagem: a) sem segmentação de mensagem; (b) com segmentação de mensagem

31. Considere o envio de um arquivo grande de F bits do computador A para o computador B. Há dois enlaces (e um comutador) entre eles e os enlaces não estão congestionados (isto é, não há atrasos de fila). O computador A fragmenta o arquivo em segmentos de S bits cada e adiciona 80 bits de cabeçalho a cada segmento, formando pacotes de $L = 40 + S$ bits. Cada enlace tem uma taxa de transmissão de R bps. Qual é o valor de S que minimiza o atraso para levar o arquivo de A para B? Desconsidere o atraso de propagação.



Questões dissertativas

- Que tipos de serviços de telefone celular sem fio estão disponíveis em sua área?
- Usando tecnologia de LAN sem fio 802.11, elabore o projeto de uma rede doméstica para sua casa ou para a casa de seus pais. Relacione os modelos de produtos específicos para essa rede doméstica juntamente com seus custos.
- Descreva os serviços Skype PC para PC. Experimente o serviço de vídeo do Skype PC para PC e relate a experiência.
- O Skype oferece um serviço que permite realizar chamadas telefônicas de um computador para um computador comum. Isso significa que a chamada deve passar pela Internet e pela rede telefônica. Discuta como esse processo deve ser feito.
- O que é Short Message Service? Em quais países/continentes esse serviço é comum? É possível enviar uma mensagem SMS de um site Web para um telefone portátil?
- O que é recepção de vídeo armazenado? Quais são os sites Web mais populares que oferecem esse serviço hoje?
- O que é recepção de vídeo em tempo real por P2P? Quais são os sites Web mais populares que oferecem esse serviço hoje?
- Descubra cinco empresas que oferecem serviços de compartilhamento de arquivos P2P. Cite os tipos de arquivos (isto é, conteúdo) que cada empresa processa.
- Quem inventou o ICQ, o primeiro serviço de mensagem instantânea? Quando foi inventado e que idade tinham seus inventores? Quem inventou o Napster? Quando foi inventado e que idade tinham seus inventores?
- Quais são as semelhanças e diferenças entre as tecnologias Wi-Fi e 3G de acesso sem fio à Internet? Quais são as taxas de bits dos dois serviços? Quais são os custos? Discuta roaming e acesso de qualquer lugar.
- Por que o serviço original de compartilhamento de arquivo P2P Napster deixou de existir? O que é a RIAA e que providências está tomando para limitar o compartilhamento de arquivos P2P de conteúdo protegido por direitos autorais? Qual é a diferença entre violação de direitos autorais direta e indireta?
- O que é BitTorrent? No que ele difere de um serviço de compartilhamento de arquivo P2P, como eDonkey, LimeWire ou Kazaa?
- Você acha que daqui a dez anos redes de computadores ainda compartilharão amplamente arquivos protegidos por direitos autorais? Por que sim ou por que não? Justifique.

Wireshark Lab

*“Conte-me e eu esquecerei. Mostre-me e eu lembrarei.
Envolva-me e eu entenderei.”*

Provérbio chinês

A compreensão de protocolos de rede pode ser muito mais profunda se os virmos em ação e interagirmos com eles — observando a sequência de mensagens trocadas entre duas entidades de protocolo, pesquisando detalhes de sua operação, fazendo com que elas executem determinadas ações e observando essas ações e suas consequências. Isso pode ser feito em cenários simulados ou em um ambiente real de rede, tal como a Internet. Os applets Java apresentados (em inglês) no site deste livro adotam a primeira abordagem. Nos Wireshark labs adotaremos a última. Você executará aplicações de rede em vários cenários utilizando seu computador no escritório, em casa ou em um laboratório e observará também os protocolos de rede interagindo e trocando mensagens com entidades de protocolo que estão executando em outros lugares da Internet. Assim, você e seu computador serão partes integrantes desses laboratórios ao vivo e você observará — e aprenderá — fazendo.

A ferramenta básica para observar as mensagens trocadas entre entidades de protocolos em execução é denominada analisador de pacotes. Como o nome sugere, um analisador de pacotes recebe passivamente mensagens enviadas e recebidas por seu computador; também exibe o conteúdo dos vários campos de protocolo das mensagens que captura. Uma tela do analisador de pacotes Wireshark é mostrada na Figura 1.29. O Wireshark é um analisador de pacotes gratuito que funciona em computadores com sistemas operacionais Windows, Linux/Unix e Mac. Por todo o livro, você encontrará Wireshark labs que o habilitarão a explorar vários dos protocolos estudados em cada capítulo. Neste primeiro Wireshark lab, você obterá e instalará uma cópia do programa, acessará um site Web e examinará as mensagens de protocolo trocadas entre seu browser e o servidor Web.

Você encontrará detalhes completos, em inglês, sobre este primeiro Wireshark Lab (incluindo instruções sobre como obter e instalar o programa) no site www.aw.com/kurose.

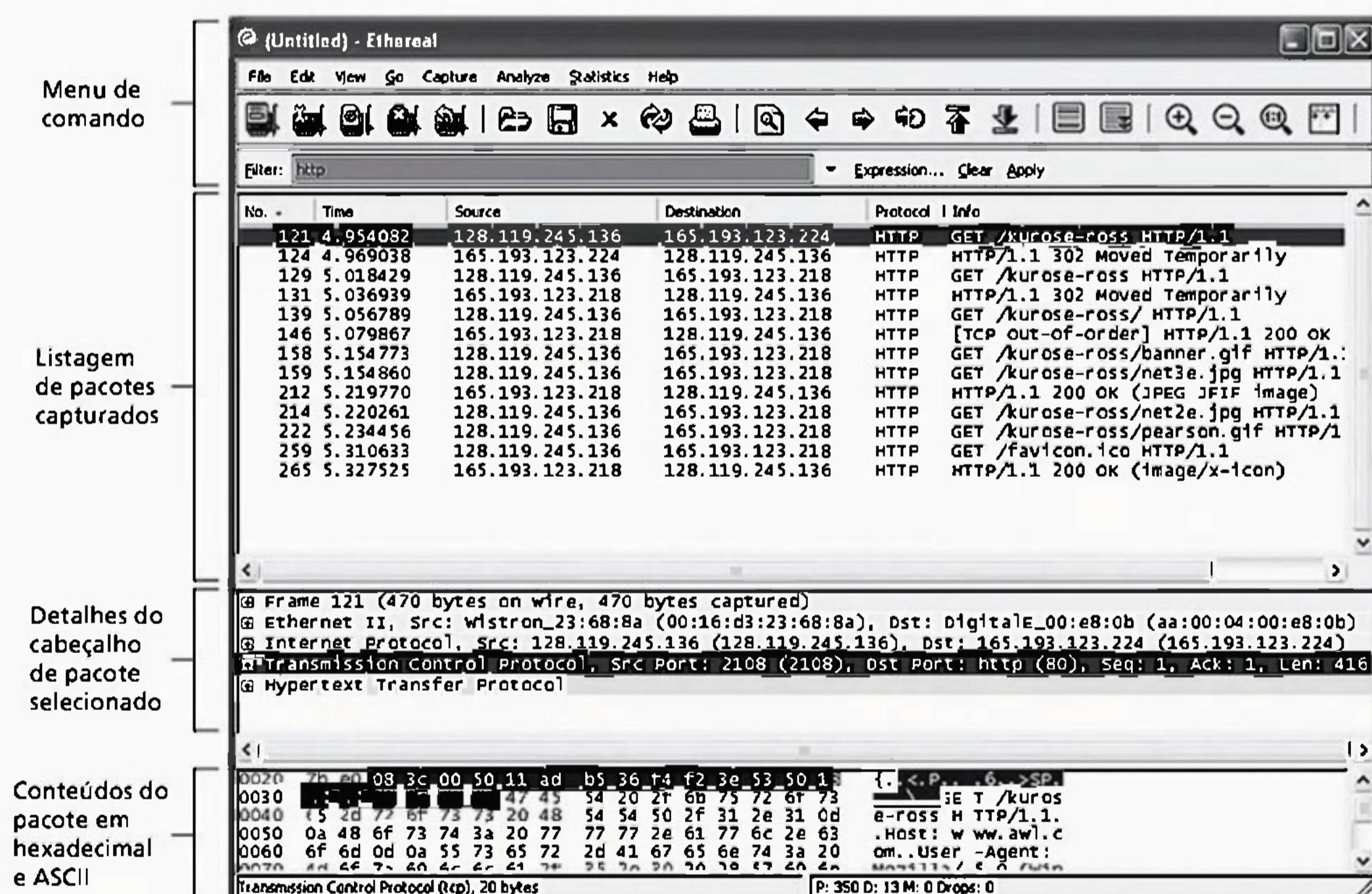


Figura 1.29 Uma amostra de tela do programa Wireshark

Entrevista

Leonard Kleinrock

Leonard Kleinrock é professor de ciência da computação da Universidade da Califórnia em Los Angeles. Em 1969, seu computador na UCLA se tornou o primeiro nó da Internet. Ele criou os princípios da comutação de pacotes em 1961, que se tornou a tecnologia básica da Internet. Leonard também é presidente e fundador da Nomadix, Inc., uma companhia cuja tecnologia oferece maior acessibilidade a serviços de Internet banda larga. Ele é bacharel em engenharia elétrica pela City College of New York (CCNY) e mestre e doutor em engenharia elétrica pelo Instituto de Tecnologia de Massachusetts (MIT).



O que o fez se decidir pela especialização em tecnologia de redes/Internet?

Como doutorando do MIT em 1959, percebi que a maioria dos meus colegas de turma estava fazendo pesquisas nas áreas de teoria da informação e de teoria da codificação. Havia no MIT o grande pesquisador Claude Shannon, que já tinha proposto estudos nessas áreas e resolvido a maior parte dos problemas importantes. Os problemas que restaram para pesquisar eram difíceis e de menor importância. Portanto, decidi propor uma nova área na qual até então ninguém tinha pensado. Lembre-se de que no MIT, eu estava cercado de computadores, e era evidente para mim que brevemente aquelas máquinas teriam de se comunicar umas com as outras. Na época, não havia nenhum meio eficaz de fazer isso; portanto, decidi desenvolver a tecnologia que permitiria a criação de redes de dados eficientes.

Qual foi seu primeiro emprego no setor de computação? O que implicava?

Frequentei o curso noturno de graduação em engenharia elétrica da CCNY de 1951 a 1957. Durante o dia, trabalhei inicialmente como técnico e depois como engenheiro em uma pequena empresa de eletrônica industrial chamada Photobell. Enquanto trabalhava lá, introduzi tecnologia digital na linha de produtos da empresa. Essencialmente, estávamos usando equipamentos fotoelétricos para detectar a presença de certos itens (caixas, pessoas etc.) e a utilização de um circuito conhecido na época como *multivibrador biestável* era exatamente o tipo de tecnologia de que precisávamos para levar o processamento digital a esse campo da detecção. Acontece que esses circuitos são os blocos de construção básicos dos computadores e vieram a ser conhecidos como *flip-flops* ou *comutadores* na linguagem coloquial de hoje.

O que passou por sua cabeça quando enviou a primeira mensagem computador a computador (da UCLA para o Stanford Research Institute)?

Francamente, eu não fazia a menor ideia da importância daquele acontecimento. Não havíamos preparado uma mensagem de significância histórica, como muitos criadores do passado o fizeram (Samuel Morse com “Que obra fez Deus.”, ou Alexandre Graham Bell, com “Watson, venha cá! Preciso de você.”, ou Neal Armstrong com “Este é um pequeno passo para o homem, mas um grande salto para a humanidade.”) Esses caras eram inteligentes! Eles entendiam de meios de comunicação e relações públicas. Nossa objetivo foi nos conectar ao computador do SRI. Então digitamos a letra “L”, que foi aceita corretamente, digitamos a letra “o”, que foi aceita, e depois digitamos a letra “g”, que fez o computador hospedeiro pisar! Então, nossa mensagem acabou sendo curta e, talvez, a mais profética de todas, ou seja, “Lo！”, como em “*Lo and behold*” (“*Pasmem!*”).

Anteriormente, naquele mesmo ano, fui citado em um comunicado de imprensa da UCLA por ter dito que, logo que a rede estivesse pronta e em funcionamento, seria possível ter acesso a utilidades de outros computadores a partir de nossa casa e escritório tão facilmente quanto tínhamos acesso à eletricidade e ao telefone. Portanto,

a visão que eu tinha da Internet naquela época era que ela seria onipresente, estaria sempre em funcionamento e sempre disponível, que qualquer pessoa que possuísse qualquer equipamento poderia se conectar com ela de qualquer lugar e que ela seria invisível. Mas jamais imaginei que minha mãe, aos 99 anos de idade, usaria a Internet — como ela realmente usou!

Em sua opinião, qual é o futuro das redes?

O fácil é predizer a infraestrutura por si mesma. Eu antecipo que vemos uma implantação considerável de computação nômade, aparelhos móveis e espaços inteligentes. Realmente, a disponibilidade de computação portátil, de alto desempenho, acessível e leve e de aparelho de comunicação (mais a onipresença da Internet) nos permitiu tornar nômades.

A computação nômade refere-se à tecnologia que permite aos usuários finais, que viajam de um lugar para o outro, ganhar acesso aos serviços da Internet de maneira transparente, não importando para onde vão e qual aparelho possuem ou ganham acesso. O difícil é predizer as aplicações e serviços, que nos surpreenderam consistentemente de formas dramáticas (e-mail, tecnologias de busca, a rede de alcance mundial, blogs, redes sociais, geração de usuários e compartilhamento de música, fotos, vídeos etc.). Estamos na margem de uma nova categoria de aplicações móveis, inovadoras e surpreendentes presentes em nossos aparelhos portáteis.

O passo seguinte vai nos capacitar a sair do mundo misterioso do ciberespaço para o mundo físico dos espaços inteligentes. A tecnologia dará vida a nossos ambientes (mesas, paredes, veículos, relógios e cintos, entre outros) por meio de atuadores, sensores, lógica, processamento, armazenagem, câmeras, microfones, alto-falantes, painéis e comunicação. Essa tecnologia embutida permitirá que nosso ambiente forneça os serviços IP que quisermos. Quando eu entrar em uma sala, ela saberá que entrei. Poderei me comunicar com meu ambiente naturalmente, como se estivesse falando o meu idioma nativo; minhas solicitações gerarão respostas apresentadas como páginas Web em painéis de parede, por meus óculos, por voz, por hologramas e assim por diante.

Analizando um panorama mais longínquo, vejo um futuro para as redes que inclui componentes fundamentais que ainda virão. Vejo agentes inteligentes de software distribuídos por toda a rede cuja função é fazer mineração de dados, agir sobre esses dados, observar tendências e adaptar e realizar tarefas dinamicamente. Vejo tráfego de rede consideravelmente maior gerado não tanto por seres humanos, mas por esses equipamentos embutidos e agentes inteligentes de software. Vejo grandes conjuntos de sistemas auto-organizáveis controlando essa rede imensa e veloz. Vejo quantidades enormes de informações zunindo por essa rede instantaneamente e passando por extraordinários processamentos e filtragens. A Internet será, essencialmente, um sistema nervoso de presença global. Vejo tudo isso e mais enquanto entramos de cabeça no século XXI.

Que pessoas o inspiraram profissionalmente?

Quem mais me inspirou foi Claude Shannon, do MIT, um brilhante pesquisador que tinha a capacidade de relacionar suas ideias matemáticas com o mundo físico de modo muitíssimo intuitivo. Ele fazia parte da banca examinadora de minha tese de doutorado.

Você pode dar algum conselho aos estudantes que estão ingressando na área de redes/Internet?

A Internet, e tudo o que ela habilita, é uma vasta fronteira nova, cheia de desafios surpreendentes. Há espaço para grandes inovações. Não fiquem limitados à tecnologia existente hoje. Soltem sua imaginação e pensem no que poderia acontecer e transformem isso em realidade.

