6 edição

**KuRose | Ross Redes de computadores e a internet** uma abordagem top-down

6a edição

**Redes de computadores e a internet**

Kurose | ross **Redes de computadores e a internet** uma abordagem top-down

6a edição

©2014 by Jim F. Kurose e Keith W. Ross

Todos os direitos reservados. Nenhuma parte desta publicação poderá ser reproduzida ou transmitida de qualquer modo ou por qualquer outro meio, eletrônico ou mecânico, incluindo fotocópia, gravação ou qualquer outro tipo de sistema de armazenamento e transmissão de informação, sem prévia autorização, por escrito, da Pearson Education do Brasil.

Diretor editorial e de conteúdo Roger Trimer Gerente editorial Kelly Tavares Supervisora de produção editorial Silvana Afonso Coordenadora de produção gráfica Tatiane Romano

Editor de aquisições Vinícius Souza

Editora de texto Daniela Braz

Preparação Christiane Colas

Revisão Carmen Simões Costa Editor assistente Luiz Salla

Capa Solange Rennó

(Sob projeto original) Projeto gráfico e Diagramação Casa de Ideias

Dados Internacionais de Catalogação na Publicação (CIP) (Câmara Brasileira do Livro, sP, Brasil)

Kurose, James F.

Redes de computadores e a Internet: uma abordagem top-down/ James F. Kurose, Keith W. Ross ; tradução Daniel Vieira; revisão técnica Wagner Luiz Zucchi. – 6. ed. – São Paulo: Pearson Education do Brasil, 2013.

Título original: Computer networking: a top-down approach Bibliografia. ISBN 978-85-430-1443-2

1. Internet 2. Redes de computadores I. Ross, Keith W.. II. Zucchi, Wagner Luiz. III. Título.

13-04218 CDD-004.67

1. Internet : redes de computadores: Processamento de dados 004.67

2013 Direitos exclusivos para a língua portuguesa cedidos à Pearson Education do Brasil Ltda., uma empresa do grupo Pearson Education Rua Nelson Francisco, 26 CEP 02712-100 – São Paulo – SP – Brasil Fone: 11 2178-8686 – Fax: 11 2178-8688 vendas@pearson.com

Sobre oS autoreS

Jim Kurose

Jim Kurose é um destacado professor universitário de Ciência da Computação na Universidade de Massachu- setts, Amherst.

Dr. Kurose recebeu diversos reconhecimentos por suas atividades educacionais, incluindo o Outstanding Teacher Awards da National Technological University (oito vezes), na Universidade de Massachusetts e na Northeast Asso- ciation of Graduate Schools. Recebeu a IEEE Taylor Booth Education Medal e foi reconhecido por sua liderança da Commonwealth Information Technology Initiative de Massachusetts. Também recebeu um GE Fellowship, um IBM Faculty Development Award e um Lilly Teaching Fellowship.

Foi editor-chefe da *IEEE Transactions of Communications* e da IEEE/ACM Transactions on Networking. Trabalhou ativamente nos comitês de programa para *IEEE Infocom*, *ACM SIGCOMM*, *ACM Internet Measurement Conference* e *ACM SIGMETRICS* por vários anos, e atendeu como copresidente de programa técnico nessas conferências. Ele é *fellow* do IEEE e da ACM. Seus interesses de pesquisa incluem protocolos e arquitetura de rede, medição de redes, redes de sensores, comunicação multimídia e modelagem e avaliação de desempenho. Tem doutorado em Ciência da Computação pela Universidade de Columbia.

Keith Ross

Keith Ross é professor na cátedra de Leonard J. Shustek e diretor do Departamento de Ciência da Computação no Instituto Politécnico da Universidade de Nova York. Antes de ingressar nesse Instituto em 2003, foi professor na Universidade da Pensilvânia (13 anos) e no Eurécom Institute (5 anos). Obteve bacharelado pela Universidade Tufts, mestrado pela Universidade de Columbia e doutorado em Computador e Engenharia de Controle pela Universidade de Michigan. Keith Ross também é fundador e CEO original da Wimba, que desenvolve aplicações de multimídia *on-line* para *e-learning* e foi adquirida pela Blackboard em 2010.

Os interesses de pesquisa do professor Ross estão em segurança e privacidade, redes sociais, redes P2P, medição na Internet, fluxo contínuo de vídeo, redes de distribuição de conteúdo e modelagem estocástica. É *fellow* do IEEE, recebeu o Infocom 2009 Best Paper Award e também os Best Paper Awards de 2011 e 2008 por Comunicações em Multimídia (concedido pela IEEE Communications Society). Trabalhou em diversos comitês editoriais de jornal e comitês de programa de conferência, incluindo IEEE/ACM Transactions on Networking, ACM SIGCOMM, ACM CoNext e ACM Internet Measurement Conference. Ele também trabalhou como consultor de compartilhamento de arquivos P2P para a Federal Trade Commission.

Para Julie e nossas três preciosidades: Chris, Charlie e Nina JFK

Um grande MUITO OBRIGADO aos meus professores, colegas e alunos do mundo inteiro. KWR

Prefácio

Bem-vindo à sexta edição de *Redes de computadores e a Internet: uma abordagem top-down*. Desde a publicação da primeira edição, há doze anos, nosso livro foi adotado em centenas de universidades e instituições de ensino supe- rior, traduzido para mais de 14 idiomas e utilizado por mais de cem mil estudantes e profissionais no mundo inteiro. Muitos desses leitores entraram em contato conosco e ficamos extremamente satisfeitos com sua reação positiva.

QUAIS SÃO AS NOVIDADES DA SEXTA EDIÇÃO?

Acreditamos que uma importante razão para esse sucesso é que o livro continua a oferecer uma abordagem moderna do ensino de redes de computadores. Fizemos mudanças nesta sexta edição, mas também mantive- mos inalterado o que acreditamos (e os instrutores e estudantes que usaram nosso livro confirmaram) serem os aspectos mais importantes do livro: sua abordagem *top-down*, seu foco na Internet e um tratamento moderno das redes de computadores, sua atenção aos princípios e à prática, e seu estilo e método acessíveis em relação ao aprendizado de redes de computadores. Apesar disso, a esta edição foi revisada e atualizada de modo substancial:

• O site de apoio do livro foi significativamente expandido e enriquecido para incluir exercícios interativos, conforme discutido mais adiante neste Prefácio.

• No Capítulo 1, o tratamento das redes de acesso foi modernizado e a descrição do ecossistema de ISP da Internet foi substancialmente revisada, considerando o surgimento recente das redes de provedor de con- teúdo, como a do Google. A apresentação da comutação de pacotes e da comutação de circuitos também foi reorganizada, oferecendo uma orientação mais tópica, em vez de histórica.

• No Capítulo 2, Python substituiu Java para a apresentação da programação de *sockets*. Embora ainda expondo explicitamente as ideias por trás da API *sockets*, o código Python é mais fácil de entender para o programador iniciante. Além do mais, diferentemente do Java, ele fornece acesso a *sockets* brutos, permi- tindo que os alunos construam maior variedade de aplicações de rede. Laboratórios de programação de *sockets* baseados em Java foram substituídos por laboratórios Python correspondentes, e foi acrescentado um novo laboratório ICMP Ping baseado em Python. Como sempre, quando um material é retirado — como aquele sobre programação de *sockets* baseada em Java — ele permanece disponível no site de apoio do livro (ver texto mais adiante).

• No Capítulo 3, a apresentação de um dos protocolos de transferência de dados confiável foi simplificada e uma nova nota em destaque sobre divisão do TCP, normalmente usada para otimizar o desempenho de serviços de nuvem, foi acrescentada.

• REDES DE COMPUTADORES E A INTERNET X• No Capítulo 4, a seção sobre arquiteturas de roteador foi significativamente atualizada, refletindo de- senvolvimentos e práticas recentes nessa área. Incluímos diversas novas notas em destaque, envolvendo DNS, BGP e OSPF.

• O Capítulo 5 foi reorganizado e simplificado, considerando a onipresença da Ethernet comutada em redes locais e o consequente aumento do uso da Ethernet em cenários ponto a ponto. Além disso, acres- centamos uma seção sobre redes de centro de dados.

• O Capítulo 6 foi atualizado para refletir os avanços recentes nas redes sem fio, em particular redes de dados por celular e serviços e arquiteturas 4G.

• O Capítulo 7, que enfoca as redes multimídia, passou por uma grande revisão. Ele agora contém uma discussão profunda do vídeo de fluxo contínuo (*streaming*), incluindo fluxo contínuo adaptativo, e uma discussão nova e modernizada de CDNs. Uma seção recém-incluída descreve os sistemas de ví- deo de fluxo contínuo Netflix, YouTube e Kankan. O material que foi removido para dar espaço para esses novos tópicos ainda está disponível no site de apoio.

• O Capítulo 8 agora contém uma discussão expandida sobre autenticação do ponto final.

• Acrescentamos um novo material significativo, envolvendo problemas de fim de capítulo. Assim como em todas as edições anteriores, trabalhos de casa foram revisados, acrescentados e removidos.

PÚBLICOdALVO

Este livro destina-se a um estudo inicial de redes de computadores. Pode ser usado em cursos de ciência da computação e de engenharia elétrica. Em termos de linguagens de programação, ele requer que os estudantes te- nham alguma experiência com as linguagens C, C++, Java ou Python (mesmo assim, apenas em alguns lugares). Embora seja mais minucioso e analítico do que muitos outros de introdução às redes de computadores, rara- mente utiliza conceitos matemáticos que não sejam ensinados no ensino médio. Fizemos um esforço deliberado para evitar o uso de quaisquer conceitos avançados de cálculo, probabilidade ou processos estocásticos (embora tenhamos incluído alguns problemas para alunos com tal conhecimento avançado). Por conseguinte, o livro é apropriado para cursos de graduação e para o primeiro ano dos cursos de pós-graduação. É também muito útil para os profissionais do setor de telecomunicações.

O QUE HÁ DE SINGULAR NESTE LIVRO?

O assunto rede de computadores é bastante vasto e complexo, envolvendo muitos conceitos, protocolos e tecnologias que se entrelaçam inextricavelmente. Para dar conta desse escopo e complexidade, muitos livros so- bre redes são, em geral, organizados de acordo com as “camadas” de uma arquitetura de rede. Com a organização em camadas, os estudantes podem vislumbrar a complexidade das redes de computadores — eles aprendem os conceitos e os protocolos distintos de uma parte da arquitetura e, ao mesmo tempo, visualizam o grande quadro da interconexão entre as camadas. Do ponto de vista pedagógico, nossa experiência confirma que essa aborda- gem em camadas é, de fato, muito boa. Entretanto, achamos que a abordagem tradicional, a *bottom-up* — da camada física para a camada de aplicação —, não é a melhor para um curso moderno de redes de computadores.

UMA ABORDAGEM TOPdDOWN

Na primeira edição, propusemos uma inovação adotando uma visão *top-down* — isto é, começando na ca- mada de aplicação e descendo até a camada física. O retorno que recebemos de professores e alunos confirmou que essa abordagem tem muitas vantagens e realmente funciona bem do ponto de vista pedagógico. Primeiro, o livro dá ênfase à camada de aplicação, que tem sido a área de “grande crescimento” das redes de computadores. De fato, muitas das recentes revoluções nesse ramo — incluindo a Web, o compartilhamento de arquivos P2P e o fluxo contínuo de mídia — tiveram lugar nessa camada. A abordagem de ênfase inicial à camada de aplicação é diferente das seguidas por muitos outros livros, que têm apenas pouco material sobre aplicações de redes, seus requisitos, paradigmas da camada de aplicação (por exemplo, cliente-servidor e P2P) e interfaces de programação

prefácio • Xi

de aplicação. Segundo, nossa experiência como professores (e a de muitos outros que utilizaram este livro) confirma que ensinar aplicações de rede logo no início do curso é uma poderosa ferramenta motivadora. Os estudantes ficam mais entusiasmados ao aprender como funcionam as aplicações de rede — aplicações como o e-mail e a Web, que a maioria deles usa diariamente. Entendendo as aplicações, o estudante pode entender os serviços de rede necessários ao suporte de tais aplicações. Pode também, por sua vez, examinar as várias manei- ras como esses serviços são fornecidos e executados nas camadas mais baixas. Assim, a discussão das aplicações logo no início fornece a motivação necessária para os demais assuntos do livro.

Terceiro, a abordagem *top-down* habilita o professor a apresentar o desenvolvimento das aplicações de rede no estágio inicial. Os estudantes não só veem como funcionam aplicações e protocolos populares, como também aprendem que é fácil criar suas próprias aplicações e protocolos de aplicação de rede. Com a abordagem *top- -down*, eles entram imediatamente em contato com as noções de programação de *sockets*, modelos de serviços e protocolos — conceitos importantes que reaparecem em todas as camadas subsequentes. Ao apresentar exemplos de programação de *sockets* em Python, destacamos as ideias centrais sem confundir os estudantes com códigos complexos. Estudantes de engenharia elétrica e ciência da computação talvez não tenham dificuldades para en- tender o código Python.

UM FOCO NA INTERNET

Continuamos a colocar a Internet em foco nesta edição do livro. Na verdade, como ela está presente em toda parte, achamos que qualquer livro sobre redes deveria ter um foco significativo na Internet. Continuamos a utilizar a arquitetura e os protocolos da Internet como veículo primordial para estudar conceitos fundamentais de redes de computadores. É claro que também incluímos conceitos e protocolos de outras arquiteturas de rede. Mas os holofotes estão claramente dirigidos à Internet, fato refletido na organização do livro, que gira em torno da arquitetura de cinco camadas: aplicação, transporte, rede, enlace e física.

Outro benefício de colocá-la sob os holofotes é que a maioria dos estudantes de ciência da computação e de engenharia elétrica está ávida por conhecer a Internet e seus protocolos. Eles sabem que a Internet é uma tecnologia revolucionária e inovadora e podem constatar que ela está provocando uma profunda transformação em nosso mundo. Dada sua enorme relevância, os estudantes estão naturalmente curiosos em saber o que há por trás dela. Assim, fica fácil para um professor manter seus alunos interessados nos princípios básicos, usando a Internet como guia.

ENSINANDO PRINCÍPIOS DE REDE

Duas das características exclusivas deste livro — sua abordagem *top-down* e seu foco na Internet — apa- recem no título e subtítulo. Se pudéssemos, teríamos acrescentado uma *terceira* palavra — *princípios*. O campo das redes agora está maduro o suficiente para que uma quantidade de assuntos de importância fundamental possa ser identificada. Por exemplo, na camada de transporte, entre os temas importantes estão a comunicação confiável por uma camada de rede não confiável, o estabelecimento/encerramento de conexões e mútua apre- sentação (*handshaking*), o controle de congestionamento e de fluxo e a multiplexação. Na camada de rede, dois assuntos muito importantes são: como determinar “bons” caminhos entre dois roteadores e como interconectar um grande número de redes heterogêneas. Na camada de enlace, um problema fundamental é como comparti- lhar um canal de acesso múltiplo. Na segurança de rede, técnicas para prover sigilo, autenticação e integridade de mensagens são baseadas em fundamentos da criptografia. Este livro identifica as questões fundamentais de redes e apresenta abordagens para enfrentar tais questões. Aprendendo esses princípios, o estudante adquire conheci- mento de “longa validade” — muito tempo após os padrões e protocolos de rede de hoje tornarem-se obsoletos, os princípios que ele incorpora continuarão importantes e relevantes. Acreditamos que o uso da Internet para apresentar o assunto aos estudantes e a ênfase dada à abordagem das questões e das soluções permitirão que os alunos entendam rapidamente qualquer tecnologia de rede.

• REDES DE COMPUTADORES E A INTERNET Xii

CARACTERÍSTICAS PEDAGÓGICAS

Há quase 20 anos damos aulas de redes de computadores. Adicionamos a este livro uma experiência agre- gada de mais de 50 anos de ensino para milhares de estudantes. Nesse período, também participamos ativamente na área de pesquisas sobre redes de computadores. (De fato, Jim e Keith se conheceram quando faziam mestrado, frequentando um curso sobre redes de computadores ministrado por Mischa Schwartz, em 1979, na Universida- de de Colúmbia.) Achamos que isso nos dá uma boa perspectiva do que foi a rede e de qual será, provavelmente, seu futuro. Não obstante, resistimos às tentações de dar ao material deste livro um viés que favorecesse nossos projetos de pesquisa prediletos. Se você estiver interessado em nossas pesquisas, consulte nosso site pessoal. Este livro é sobre redes de computadores modernas — é sobre protocolos e tecnologias contemporâneas, bem como sobre os princípios subjacentes a esses protocolos e tecnologias. Também achamos que aprender (e ensinar!) re- des pode ser divertido. Esperamos que algum senso de humor e a utilização de analogias e exemplos do mundo real que aparecem aqui tornem o material ainda mais divertido.

DEPENDêNCIAS DE CAPÍTULO

O primeiro capítulo apresenta um apanhado geral sobre redes de computadores. Com a introdução de muitos conceitos e terminologias fundamentais, ele monta o cenário para o restante do livro. Todos os outros capítulos dependem diretamente desse primeiro. Recomendamos que os professores, após o terem comple- tado, percorram em sequência os Capítulos 2 ao 5, seguindo nossa filosofia *top-down*. Cada um dos cinco primeiros capítulos utiliza material dos anteriores. Após tê-los completado, o professor terá bastante flexibi- lidade. Não há interdependência entre os quatro últimos capítulos, de modo que eles podem ser ensinados em qualquer ordem. Porém, cada um dos quatro últimos capítulos depende do material nos cinco primeiros. Muitos professores a princípio ensinam os cinco primeiros capítulos e depois ensinam um dos quatro últimos para “arrematar”.

AGRADECIMENTOS

Desde o início deste projeto, em 1996, muitas pessoas nos deram inestimável auxílio e influenciaram nossas ideias sobre como melhor organizar e ministrar um curso sobre redes. Nosso MUITO OBRIGADO a todos os que nas ajudaram desde os primeiros rascunhos deste livro, até a quinta edição. Também somos *muito* gratos sobretudo às muitas centenas de leitores de todo o mundo - estudantes, acadêmicos e profissionais - que nos enviaram sugestões e comentários sobre edições anteriores e sugestões para edições futuras. Nossos agradeci- mentos especiais para:

Al Aho (Universidade de Columbia) Hisham Al-Mubaid (Universidade de Houston-Clear Lake) Pratima Akkunoor (Universidade do Estado do Arizona) Paul Amer (Universidade de Delaware) Shamiul Azom (Universidade do Estado do Arizona) Lichun Bao (Universidade da Califórnia, Irvine) Paul Barford (Universidade do Wisconsin) Bobby Bhattacharjee (Universidade de Maryland) Steven Bellovin (Universidade de Columbia) Pravin Bhagwat (Wibhu) Supratik Bhattacharyya (anteriormente na Sprint) Ernst Biersack (Eurécom Institute) Shahid Bokhari (Universidade de Engenharia & Tecnologia, Lahore) Jean Bolot (Technicolor Research)

prefácio • Xiii

Daniel Brushteyn (ex-aluno da Universidade da Pensilvânia) Ken Calvert (Universidade do Kentucky) Evandro Cantu (Universidade Federal de Santa Catarina) Jeff Case (SNMP Research International) Jeff Chaltas (Sprint) Vinton Cerf (Google) Byung Kyu Choi (Universidade Tecnológica de Michigan) Bram Cohen (BitTorrent, Inc.) Constantine Coutras (Universidade Pace) John Daigle (Universidade do Mississippi) Edmundo A. de Souza e Silva (Universidade Federal do Rio de Janeiro) Philippe Decuetos (Eurécom Institute) Christophe Diot (Technicolor Research) Prithula Dhunghel (Akamai) Deborah Estrin (Universidade da Califórnia, Los Angeles) Michalis Faloutsos (Universidade da Califórnia, Riverside) Wu-chi Feng (Oregon Graduate Institute) Sally Floyd (ICIR, Universidade da Califórnia, Berkeley) Paul Francis (Max Planck Institute) Lixin Gao (Universidade de Massachusetts) JJ Garcia-Luna-Aceves (Universidade da Califórnia, Santa Cruz) Mario Gerla (Universidade da Califórnia, Los Angeles) David Goodman (NYU-Poly) Yang Guo (Alcatel/Lucent Bell Labs) Tim Griffin (Universidade de Cambridge) Max Hailperin (Gustavus Adolphus College) Bruce Harvey (Universidade da Flórida A&M) Carl Hauser (Universidade do Estado de Washington) Rachelle Heller (Universidade George Washington) Phillipp Hoschka (INRIA/W3C) Wen Hsin (Universidade Park) Albert Huang (ex-aluno da Universidade da Pensilvânia) Cheng Huang (Microsoft Research) Esther A. Hughes (Universidade Virginia Commonwealth) Van Jacobson (Xerox PARC) Pinak Jain (ex-aluno da NYU-Poly) Jobin James (Universidade da Califórnia, Riverside) Sugih Jamin (Universidade de Michigan) Shivkumar Kalyanaraman (IBM Research, Índia) Jussi Kangasharju (Universidade de Helsinki) Sneha Kasera (Universidade de Utah) Parviz Kermani (anteriormente da IBM Research) Hyojin Kim (ex-aluno da Universidade da Pensilvânia)

• REDES DE COMPUTADORES E A INTERNET XiV

Leonard Kleinrock (Universidade da Califórnia, Los Angeles) David Kotz (Dartmouth College) Beshan Kulapala (Universidade do Estado do Arizona) Rakesh Kumar (Bloomberg) Miguel A. Labrador (Universidade South Florida) Simon Lam (Universidade do Texas) Steve Lai (Universidade do Estado de Ohio) Tom LaPorta (Universidade do Estado de Pensilvânia) Tim-Berners Lee (World Wide Web Consortium) Arnaud Legout (INRIA) Lee Leitner (Universidade Drexel) Brian Levine (Universidade de Massachusetts) Chunchun Li (ex-aluno da NYU-Poly) Yong Liu (NYU-Poly) William Liang (ex-aluno da Universidade da Pensilvânia) Willis Marti (Universidade Texas A&M) Nick McKeown (Universidade Stanford) Josh McKinzie (Universidade Park) Deep Medhi (Universidade do Missouri, Kansas City) Bob Metcalfe (International Data Group) Sue Moon (KAIST) Jenni Moyer (Comcast) Erich Nahum (IBM Research) Christos Papadopoulos (Universidade do Estado do Colorado) Craig Partridge (BBN Technologies) Radia Perlman (Intel) Jitendra Padhye (Microsoft Research) Vern Paxson (Universidade da Califórnia, Berkeley) Kevin Phillips (Sprint) George Polyzos (Universidade de Economia e Negócios de Atenas) Sriram Rajagopalan (Universidade do Estado do Arizona) Ramachandran Ramjee (Microsoft Research) Ken Reek (Rochester Institute of Technology) Martin Reisslein (Universidade do Estado do Arizona) Jennifer Rexford (Universidade de Princeton) Leon Reznik (Rochester Institute of Technology) Pablo Rodrigez (Telefonica) Sumit Roy (Universidade de Washington) Avi Rubin (Universidade Johns Hopkins) Dan Rubenstein (Universidade de Columbia) Douglas Salane (John Jay College) Despina Saparilla (Cisco Systems) John Schanz (Comcast)

prefácio • XV

Henning Schulzrinne (Universidade de Columbia) Mischa Schwartz (Universidade de Columbia) Ardash Sethi (Universidade de Delaware) Harish Sethu (Universidade Drexel) K. Sam Shanmugan (Universidade do Kansas) Prashant Shenoy (Universidade de Massachusetts) Clay Shields (Universidade Georgetown) Subin Shrestra (Universidade da Pensilvânia) Bojie Shu (ex-aluno da NYU-Poly) Mihail L. Sichitiu (Universidade do Estado de NC) Peter Steenkiste (Universidade Carnegie Mellon) Tatsuya Suda (Universidade da Califórnia, Irvine) Kin Sun Tam (Universidade do Estado de Nova York, Albany) Don Towsley (Universidade de Massachusetts) David Turner (Universidade do Estado da Califórnia, San Bernardino) Nitin Vaidya (Universidade de Illinois) Michele Weigle (Universidade Clemson) David Wetherall (Universidade de Washington) Ira Winston (Universidade da Pensilvânia) Di Wu (Universidade Sun Yat-sen) Shirley Wynn (NYU-Poly) Raj Yavatkar (Intel) Yechiam Yemini (Universidade de Columbia) Ming Yu (Universidade do Estado de Nova York, Binghamton) Ellen Zegura (Instituto de Tecnologia da Geórgia) Honggang Zhang (Universidade Suffolk) Hui Zhang (Universidade Carnegie Mellon) Lixia Zhang (Universidade da Califórnia, Los Angeles) Meng Zhang (ex-aluno da NYU-Poly) Shuchun Zhang (ex-aluno da Universidade da Pensilvânia) Xiaodong Zhang (Universidade do Estado de Ohio) ZhiLi Zhang (Universidade de Minnesota) Phil Zimmermann (consultor independente) Cliff C. Zou (Universidade Central Florida)

Queremos agradecer, também, a toda a equipe da Addison-Wesley — em particular, a Michael Hirsch, Marilyn Lloyd e Emma Snider — que fez um trabalho realmente notável nesta sexta edição (e que teve de suportar dois autores muito complicados e quase sempre atrasados). Agradecemos aos artistas gráficos Janet Theurer e Patrice Rossi Calkin, pelo trabalho que executaram nas belas figuras deste livro, e a Andrea Stefa- nowicz e sua equipe na PreMediaGlobal, pelo maravilhoso trabalho de produção desta edição. Por fim, um agradecimento muito especial a Michael Hirsch, nosso editor na Addison-Wesley, e a Susan Hartman, nossa antiga editora. Este livro não seria o que é (e talvez nem tivesse existido) sem a administração cordial de am- bos, constante incentivo, paciência quase infinita, bom humor e perseverança.

• REDES DE COMPUTADORES E A INTERNET XVi

Agradecimentos — Edição brasileira

Agradecemos a todos os profissionais envolvidos na produção desta edição no Brasil, em especial ao Prof. Dr. Wagner Luiz Zucchi (Escola Politécnica da USP, Instituto de Pesquisas Tecnológicas — IPT — e Universidade Nove de Julho), por sua dedicação e empenho na revisão técnica do conteúdo.

Materiais adicionais

A Sala Virtual (<sv.pearson.com.br>) oferece recursos adicionais que auxiliarão professores e alunos na exposição das aulas e no processo de aprendizagem.

Para o professor:

• Apresentações em PowerPoint

• Manual de soluções (em inglês)

Para o aluno:

• Exercícios autocorrigíveis (10 por capítulo)

• Exercícios interativos

• Material de aprendizagem interativo (applets e códigos-fonte)

• Tarefas extras de programação – Python e Java (em inglês)

• Wireshark labs (em inglês)

• Exemplos para implementação de laboratórios (em inglês)

Sumário

Capítulo 1 Redes de computadores e a Internet 1

1.1 O que é a Internet? 2 1.1.1 Uma descrição dos componentes da rede 3 1.1.2 Uma descrição do serviço 4 1.1.3 O que é um protocolo? 5 1.2 A periferia da Internet 7 1.2.1 Redes de acesso 8 1.2.2 Meios físicos 14 1.3 O núcleo da rede 16 1.3.1 Comutação de pacotes 16 1.3.2 Comutação de circuitos 20 1.3.3 Uma rede de redes 23 1.4 Atraso, perda e vazão em redes de comutação de pacotes 26 1.4.1 Uma visão geral de atraso em redes de comutação de pacotes 26 1.4.2 Atraso de fila e perda de pacote 29 1.4.3 Atraso fim a fim 31 1.4.4 Vazão nas redes de computadores 32 1.5 Camadas de protocolo e seus modelos de serviço 35 1.5.1 Arquitetura de camadas 35 1.5.2 Encapsulamento 39 1.6 Redes sob ameaça 41 1.7 História das redes de computadores e da Internet 44 1.7.1 Desenvolvimento da comutação de pacotes: 1961-1972 44 1.7.2 Redes proprietárias e trabalho em rede: 1972-1980 46 1.7.3 Proliferação de redes: 1980-1990 46 1.7.4 A explosão da Internet: a década de 1990 47 1.7.5 O novo milênio 48 1.8 Resumo 48 Exercícios de fixação e perguntas 50 Problemas 52 Wireshark Lab 57 Entrevista: Leonard Kleinrock 58

• REDES DE COMPUTADORES E A INTERNET XViii

Capítulo 2 Camada de aplicação 61

2.1 Princípios de aplicações de rede 62 2.1.1 Arquiteturas de aplicação de rede 62 2.1.2 Comunicação entre processos 65 2.1.3 Serviços de transporte disponíveis para aplicações 66 2.1.4 Serviços de transporte providos pela Internet 68 2.1.5 Protocolos de camada de aplicação 71 2.1.6 Aplicações de rede abordadas neste livro 71 2.2 A Web e o HTTP 72 2.2.1 Descrição geral do HTTP 72 2.2.2 Conexões persistentes e não persistentes 73 2.2.3 Formato da mensagem HTTP 76 2.2.4 Interação usuário-servidor: *cookies* 79 2.2.5 *Caches* Web 81 2.2.6 GET condicional 83 2.3 Transferência de arquivo: FTP 85 2.3.1 Comandos e respostas FTP 86 2.4 Correio eletrônico na Internet 87 2.4.1 SMTP 88 2.4.2 Comparação com o HTTP 91 2.4.3 Formatos de mensagem de correio 91 2.4.4 Protocolos de acesso ao correio 92 2.5 DNS: o serviço de diretório da Internet 95 2.5.1 Serviços fornecidos pelo DNS 96 2.5.2 Visão geral do modo de funcionamento do DNS 97 2.5.3 Registros e mensagens DNS 102 2.6 Aplicações P2P 106 2.6.1 Distribuição de arquivos P2P 106 2.6.2 Distributed Hash Tables (DHTs) 111 2.7 Programação de *sockets*: criando aplicações de rede 115 2.7.1 Programação de *sockets* com UDP 116 2.7.2 Programação de *sockets* com TCP 119 2.8 Resumo 123 Exercícios de fixação e perguntas 124 Problemas 125 Tarefas de programação de *sockets* 131 Wireshark Lab: HTTP 132 Wireshark Lab: DNS 132 Entrevista: Marc Andreessen 133 Capítulo 3 Camada de transporte 135

3.1 Introdução e serviços de camada de transporte 135 3.1.1 Relação entre as camadas de transporte e de rede 137 3.1.2 Visão geral da camada de transporte na Internet 138 3.2 Multiplexação e demultiplexação 139 3.3 Transporte não orientado para conexão: UDP 145 3.3.1 Estrutura do segmento UDP 147 3.3.2 Soma de verificação UDP 148 3.4 Princípios da transferência confiável de dados 149 3.4.1 Construindo um protocolo de transferência confiável de dados 151 3.4.2 Protocolos de transferência confiável de dados com paralelismo 159 3.4.3 Go-Back-N (GBN) 161

XiX Sumário •

3.4.4 Repetição seletiva (SR) 164 3.5 Transporte orientado para conexão: TCP 168 3.5.1 A conexão TCP 169 3.5.2 Estrutura do segmento TCP 171 3.5.3 Estimativa do tempo de viagem de ida e volta e de esgotamento

de temporização 175 3.5.4 Transferência confiável de dados 177 3.5.5 Controle de fluxo 184 3.5.6 Gerenciamento da conexão TCP 185 3.6 Princípios de controle de congestionamento 190 3.6.1 As causas e os custos do congestionamento 190 3.6.2 Mecanismos de controle de congestionamento 195 3.6.3 Exemplo de controle de congestionamento assistido pela rede:

controle de congestionamento ATM ABR 196 3.7 Controle de congestionamento no TCP 198 3.7.1 Equidade 205 3.8 Resumo 208 Exercícios de fixação e perguntas 210 Problemas 212 Tarefa de programação 221 Wireshark Lab: explorando TCP 221 Wireshark Lab: explorando UDP 221 Entrevista: Van Jacobson 222 Capítulo 4 A camada de rede 224

4.1 Introdução 225 4.1.1 Repasse e roteamento 225 4.1.2 Modelos de serviço de rede 228 4.2 Redes de circuitos virtuais e de datagramas 230 4.2.1 Redes de circuitos virtuais 231 4.2.2 Redes de datagramas 233 4.2.3 Origens das redes de circuitos virtuais e de datagramas 235 4.3 O que há dentro de um roteador? 235 4.3.1 Processamento de entrada 237 4.3.2 Elemento de comutação 239 4.3.3 Processamento de saída 241 4.3.4 Onde ocorre formação de fila? 241 4.3.5 O plano de controle de roteamento 243 4.4 O Protocolo da Internet (IP): repasse e endereçamento na Internet 244 4.4.1 Formato do datagrama 245 4.4.2 Endereçamento IPv4 249 4.4.3 Protocolo de Mensagens de Controle da Internet (ICMP) 260 4.4.4 IPv6 263 4.4.5 Uma breve investida em segurança IP 267 4.5 Algoritmos de roteamento 268 4.5.1 O algoritmo de roteamento de estado de enlace (LS) 271 4.5.2 O algoritmo de roteamento de vetor de distâncias (DV) 274 4.5.3 Roteamento hierárquico 280 4.6 Roteamento na Internet 283 4.6.1 Roteamento intra-AS na Internet: RIP 283 4.6.2 Roteamento intra-AS na Internet: OSPF 286 4.6.3 Roteamento inter-AS: BGP 288 4.7 Roteamento por difusão e para um grupo 295

• REDES DE COMPUTADORES E A INTERNET XX

4.7.1 Algoritmos de roteamento por difusão *(broadcast)* 295 4.7.2 Serviço para um grupo *(multicast)* 299 4.8 Resumo 305 Exercícios de fixação e perguntas 306 Problemas 308 Tarefas de programação de *sockets* 317 Tarefas de programação 318 Wireshark Lab 318 Entrevista: Vinton G. Cerf 319 Capítulo 5 Camada de enlace: enlaces, redes de acesso e redes locais 321

5.1 Introdução à camada de enlace 322 5.1.1 Os serviços fornecidos pela camada de enlace 323 5.1.2 Onde a camada de enlace é implementada? 324 5.2 Técnicas de detecção e correção de erros 325 5.2.1 Verificações de paridade 326 5.2.2 Métodos de soma de verificação 328 5.2.3 Verificação de redundância cíclica (CRC) 328 5.3 Enlaces e protocolos de acesso múltiplo 330 5.3.1 Protocolos de divisão de canal 332 5.3.2 Protocolos de acesso aleatório 333 5.3.3 Protocolos de revezamento 340 5.3.4 DOCSIS: O protocolo da camada de enlace para acesso

à Internet a cabo 341 5.4 Redes locais comutadas 342 5.4.1 Endereçamento na camada de enlace e ARP 343 5.4.2 Ethernet 348 5.4.3 Comutadores da camada de enlace 352 5.4.4 Redes locais virtuais (VLANs) 357 5.5 Virtualização de enlace: uma rede como camada de enlace 359 5.5.1 Multiprotocol Label Switching (MPLS) 360 5.6 Redes do datacenter 362 5.7 Um dia na vida de uma solicitação de página Web 366 5.7.1 Começando: DHCP, UDP, IP e Ethernet 367 5.7.2 Ainda começando: DNS, ARP 368 5.7.3 Ainda começando: roteamento intradomínio ao servidor DNS 369 5.7.4 Interação cliente-servidor Web: TCP e HTTP 369 5.8 Resumo 370 Exercícios de fixação e perguntas 372 Problemas 373 Wireshark Lab 378 Entrevista: Simon S. Lam 378 Capítulo 6 Redes sem fio e redes móveis 380

6.1 Introdução 381 6.2 Características de enlaces e redes sem fio 384 6.2.1 CDMA 387 6.3 Wi-Fi: LANs sem fio 802.11 389 6.3.1 A arquitetura 802.11 390 6.3.2 O protocolo MAC 802.11 393 6.3.3 O quadro IEEE 802.11 397 6.3.4 Mobilidade na mesma sub-rede IP 400 6.3.5 Recursos avançados em 802.11 401

XXi Sumário •

6.3.6 Redes pessoais: Bluetooth e Zigbee 402 6.4 Acesso celular à Internet 404 6.4.1 Visão geral da arquitetura de rede celular 405 6.4.2 Redes de dados celulares 3G: estendendo a Internet a

assinantes de celular 406 6.4.3 No caminho para o 4G: LTE 409 6.5 Gerenciamento da mobilidade: princípios 410 6.5.1 Endereçamento 412 6.5.2 Roteamento para um nó móvel 413 6.6 IP móvel 418 6.7 Gerenciamento de mobilidade em redes celulares 421 6.7.1 Roteando chamadas para um usuário móvel 421 6.7.2 Transferências (*handoffs*) em GSM 423 6.8 Redes sem fio e mobilidade: impacto sobre protocolos de camadas superiores 425 6.9 Resumo 427 Exercícios de fixação e perguntas 427 Problemas 429 Wireshark Lab 431 Entrevista: Deborah Estrin 431 Capítulo 7 Redes multimídia 433

7.1 Aplicações de rede multimídia 434 7.1.1 Propriedades de vídeo 434 7.1.2 Propriedades de áudio 435 7.1.3 Tipos de aplicações de redes multimídia 436 7.2 Vídeo de fluxo contínuo armazenado 437 7.2.1 UDP de fluxo contínuo 439 7.2.2 HTTP de fluxo contínuo 439 7.2.3 Fluxo contínuo adaptativo e DASH 443 7.2.4 Redes de distribuição de conteúdo 444 7.2.5 Estudos de caso: Netflix, YouTube e KanKan 449 7.3 Voice-over-IP 452 7.3.1 As limitações de um serviço IP de melhor esforço 452 7.3.2 Eliminação da variação de atraso no receptor para áudio 453 7.3.3 Recuperação de perda de pacotes 456 7.3.4 Estudo de caso: VoIP com Skype 458 7.4 Protocolos para aplicações interativas em tempo real 460 7.4.1 Protocolo de Tempo Real (RTP) 460 7.4.2 SIP 463 7.5 Suporte de rede para multimídia 467 7.5.1 Dimensionando redes de melhor esforço 468 7.5.2 Fornecendo múltiplas classes de serviço 469 7.5.3 Diffserv 478 7.5.4 Garantias de QoS por conexão: reserva de recurso e

admissão de chamada 481 7.6 Resumo 484 Exercícios de fixação e perguntas 484 Problemas 486 Tarefa de programação 492 Entrevista: Henning Schulzrinne 492 Capítulo 8 Segurança em redes de computadores 495

8.1 O que é segurança de rede? 496 8.2 Princípios de criptografia 497

• REDES DE COMPUTADORES E A INTERNET XXii

8.2.1 Criptografia de chaves simétricas 498 8.2.2 Criptografia de chave pública 503 8.3 Integridade de mensagem e assinaturas digitais 507 8.3.1 Funções de *hash* criptográficas 508 8.3.2 Código de autenticação da mensagem 509 8.3.3 Assinaturas digitais 510 8.4 Autenticação do ponto final 515 8.4.1 Protocolo de autenticação *ap1.0* 516 8.4.2 Protocolo de autenticação *ap2.0* 516 8.4.3 Protocolo de autenticação *ap3.0* 517 8.4.4 Protocolo de autenticação *ap3.1* 518 8.4.5 Protocolo de autenticação *ap4.0* 518 8.5 Protegendo o e-mail 519 8.5.1 E-mail seguro 520 8.5.2 PGP 522 8.6 Protegendo conexões TCP: SSL 523 8.6.1 Uma visão abrangente 525 8.6.2 Uma visão mais completa 527 8.7 Segurança na camada de rede: IPsec e redes virtuais privadas 528 8.7.1 IPsec e redes virtuais privadas (VPNs) 529 8.7.2 Os protocolos AH e ESP 530 8.7.3 Associações de segurança 530 8.7.4 O datagrama IPsec 531 8.7.5 IKE: Gerenciamento de chave no IPsec 533 8.8 Segurança de LANs sem fio 534 8.8.1 Privacidade Equivalente Cabeada (WEP) 534 8.8.2 IEEE 802.11i 536 8.9 Segurança operacional: *firewalls* e sistemas de detecção de invasão 538 8.9.1 *Firewalls* 538 8.9.2 Sistemas de detecção de invasão 544 8.10 Resumo 546 Exercícios de fixação e perguntas 547 Problemas 549 Wireshark Lab 553 IPsec Lab 553 Entrevista: Steven M. Bellovin 553 Capítulo 9 Gerenciamento de rede 555

9.1 O que é gerenciamento de rede? 555 9.2 A infraestrutura do gerenciamento de rede 558 9.3 A estrutura de gerenciamento padrão da Internet 562 9.3.1 SMI (Estrutura de Informações de Gerenciamento) 563 9.3.2 Base de informações de gerenciamento: MIB 566 9.3.3 Operações do protocolo SNMP e mapeamentos de transporte 568 9.3.4 Segurança e administração 570 9.4 ASN.1 572 9.5 Conclusão 576 Exercícios de fixação e perguntas 576 Problemas 577 Entrevista: Jennifer Rexford 578

Referências 580 Índice 607

C 21 A P 3456 Í T U L O 897

redeS e COMPUTADORES a internet

de

A Internet de hoje é provavelmente o maior sistema de engenharia já criado pela humanidade, com cente- nas de milhões de computadores conectados, enlaces de comunicação e comutadores; bilhões de usuários que se conectam por meio de laptops, tablets e smartphones; e com uma série de dispositivos como sensores, webcams, console para jogos, quadros de imagens, e até mesmo máquinas de lavar sendo conectadas. Dado que a Internet é tão ampla e possui inúmeros componentes e utilidades, há a possibilidade de compreender como ela funciona? Existem princípios de orientação e estrutura que forneçam um fundamento para a compreensão de um sistema surpreendentemente complexo e abrangente? Se a resposta for sim, é possível que, nos dias de hoje, seja interes- sante *e* divertido aprender sobre rede de computadores? Felizmente, as respostas para todas essas perguntas é um retumbante SIM! Na verdade, nosso objetivo neste livro é fornecer uma introdução moderna ao campo dinâmico das redes de computadores, apresentando os princípios e o entendimento prático necessários para utilizar não apenas as redes de hoje, como também as de amanhã.

O primeiro capítulo apresenta um panorama de redes de computadores e da Internet. Nosso objetivo é pin- tar um quadro amplo e estabelecer um contexto para o resto deste livro, para ver a floresta por entre as árvores. Cobriremos um terreno bastante extenso neste capítulo de introdução e discutiremos várias peças de uma rede de computadores, sem perder de vista o quadro geral.

O panorama geral de redes de computadores que apresentaremos neste capítulo será estruturado como segue. Após apresentarmos brevemente a terminologia e os conceitos fundamentais, examinaremos primeiro os compo- nentes básicos de hardware e software que compõem uma rede. Partiremos da periferia da rede e examinaremos os sistemas finais e aplicações de rede executados nela. Consideraremos os serviços de transporte fornecidos a essas aplicações. Em seguida exploraremos o núcleo de uma rede de computadores examinando os enlaces e comutadores que transportam dados, bem como as redes de acesso e meios físicos que conectam sistemas finais ao núcleo da rede. Aprenderemos que a Internet é uma rede de redes e observaremos como essas redes se conectam umas com as outras. Após concluirmos essa revisão sobre a periferia e o núcleo de uma rede de computadores, adotaremos uma visão mais ampla e mais abstrata na segunda metade deste capítulo. Examinaremos atraso, perda e vazão de dados em uma rede de computadores e forneceremos modelos quantitativos simples para a vazão e o atraso fim a fim: modelos que levam em conta atrasos de transmissão, propagação e enfileiramento. Depois apresentaremos alguns princípios fundamentais de arquitetura em redes de computadores, a saber: protocolos em camadas e modelos de serviço. Aprenderemos, também, que as redes de computadores são vulneráveis a diferentes tipos de ameaças; analisaremos algumas dessas ameaças e como a rede pode se tornar mais segura. Por fim, encerraremos este capítulo com um breve histórico da computação em rede.

• 2REDES DE COMPUTADORES E A INTERNET 1.1 O QUE É A INTERNET?

Neste livro, usamos a Internet pública, uma rede de computadores específica, como o veículo principal para discutir as redes de computadores e seus protocolos. Mas o que *é* a Internet? Há diversas maneiras de responder a essa questão. Primeiro, podemos descrever detalhadamente os aspectos principais da Internet, ou seja, os com- ponentes de software e hardware básicos que a formam. Segundo, podemos descrever a Internet em termos de uma infraestrutura de redes que fornece serviços para aplicações distribuídas. Iniciaremos com a descrição dos componentes, utilizando a Figura 1.1 como ilustração para a nossa discussão.

FIGURA 1.1 ALGUNS COMPONENTES DA INTERNET

Legenda:

*Host* (ou sistema final)

ISP nacional ou global Rede móvel

ISP local ou regional

Rede doméstica

Rede corporativa

Servidor Móvel Roteador Comutador

Modem Estação- da camada

-base de enlace (switch)Smartphone Torre de telefonia celular

REDES DE COMPUTADORES E A INTERNET • 3

1.1.1 Uma descrição dos componentes da rede

A Internet é uma rede de computadores que interconecta centenas de milhões de dispositivos de compu- tação ao redor do mundo. Há pouco tempo, esses dispositivos eram basicamente PCs de mesa, estações de tra- balho Linux, e os assim chamados servidores que armazenam e transmitem informações, como páginas da Web e mensagens de e-mail. No entanto, cada vez mais sistemas finais modernos da Internet, como TVs, laptops, consoles para jogos, telefones celulares, *webcams*, automóveis, dispositivos de sensoriamento ambiental, quadros de imagens, e sistemas internos elétricos e de segurança, estão sendo conectados à rede. Na verdade, o termo *rede de computadores* está começando a soar um tanto desatualizado, dados os muitos equipamentos não tradicionais que estão sendo ligados à Internet. No jargão da rede, todos esses equipamentos são denominados **hospedeiros** ou **sistemas finais**. Em julho de 2011, havia cerca de 850 milhões de sistemas finais ligados à Internet [ISC, 2012], sem contar os smartphones, laptops e outros dispositivos que são conectados à rede de maneira intermitente. No todo, estima-se que haja 2 bilhões de usuários na Internet [ITU, 2011].

Sistemas finais são conectados entre si por **enlaces (*links*) de comunicação** e **comutadores (*switches*) de pacotes**. Na Seção 1.2, veremos que há muitos tipos de enlaces de comunicação, que são constituídos de diferen- tes tipos de meios físicos, entre eles cabos coaxiais, fios de cobre, fibras óticas e ondas de rádio. Enlaces diferentes podem transmitir dados em taxas diferentes, sendo a **taxa de transmissão** de um enlace medida em bits por segundo. Quando um sistema final possui dados para enviar a outro sistema final, o sistema emissor segmenta esses dados e adiciona bytes de cabeçalho a cada segmento. Os pacotes de informações resultantes, conhecidos como **pacotes** no jargão de rede de computadores, são enviados através da rede ao sistema final de destino, onde são remontados para os dados originais.

Um comutador de pacotes encaminha o pacote que está chegando em um de seus enlaces de comunicação de entrada para um de seus enlaces de comunicação de saída. Há comutadores de pacotes de todos os tipos e formas, mas os dois mais proeminentes na Internet de hoje são **roteadores** e **comutadores de camada de enla- ce**. Esses dois tipos de comutadores encaminham pacotes a seus destinos finais. Os comutadores de camada de enlace geralmente são utilizados em redes de acesso, enquanto os roteadores são utilizados principalmente no núcleo da rede. A sequência de enlaces de comunicação e comutadores de pacotes que um pacote percorre desde o sistema final remetente até o sistema final receptor é conhecida como **rota** ou **caminho** através da rede. É difícil de estimar a exata quantidade de tráfego na Internet, mas a Cisco [Cisco VNI, 2011] estima que o tráfego global da Internet esteve perto do 40 exabytes por mês em 2012.

As redes comutadas por pacotes (que transportam pacotes) são, de muitas maneiras, semelhantes às redes de transporte de rodovias, estradas e cruzamentos (que transportam veículos). Considere, por exemplo, uma fábrica que precise transportar uma quantidade de carga muito grande a algum depósito localizado a milhares de quilômetros. Na fábrica, a carga é dividida e carregada em uma frota de caminhões. Cada caminhão viaja, de modo independente, pela rede de rodovias, estradas e cruzamentos ao depósito de destino. No depósito, a carga é descarregada e agrupada com o resto da carga pertencente à mesma remessa. Deste modo, os pacotes se asse- melham aos caminhões, os enlaces de comunicação representam rodovias e estradas, os comutadores de pacote seriam os cruzamentos e cada sistema final se assemelha aos depósitos. Assim como o caminhão faz o percurso pela rede de transporte, o pacote utiliza uma rede de computadores.

Sistemas finais acessam a Internet por meio de **Provedores de Serviços de Internet** (*Internet Service Providers* — ISPs), entre eles ISPs residenciais como empresas de TV a cabo ou empresas de telefonia; corporativos, de univer- sidades e ISPs que fornecem acesso sem fio em aeroportos, hotéis, cafés e outros locais públicos. Cada ISP é uma rede de comutadores de pacotes e enlaces de comunicação. ISPs oferecem aos sistemas finais uma variedade de tipos de acesso à rede, incluindo acesso residencial de banda larga como modem a cabo ou DSL (linha digital de assinan- te), acesso por LAN de alta velocidade, acesso sem fio e acesso por modem discado de 56 kbits/s. ISPs também for- necem acesso a provedores de conteúdo, conectando sites diretamente à Internet. Esta se interessa pela conexão entre os sistemas finais, portanto os ISPs que fornecem acesso a esses sistemas também devem se interconectar. Esses ISPs de nível mais baixo são interconectados por meio de ISPs de nível mais alto, nacionais e internacionais, como Level 3 Communications, AT&T, Sprint e NTT. Um ISP de nível mais alto consiste em roteadores de alta velocidade

• REDES DE COMPUTADORES E A INTERNET 4interconectados com enlaces de fibra ótica de alta velocidade. Cada rede ISP, seja de nível mais alto ou mais baixo, é gerenciada de forma independente, executa o protocolo IP (ver adiante) e obedece a certas convenções de nomeação e endereço. Examinaremos ISPs e sua interconexão mais em detalhes na Seção 1.3.

Os sistemas finais, os comutadores de pacotes e outras peças da Internet executam **protocolos** que controlam o envio e o recebimento de informações. O **TCP** (**Transmission Control Protocol** — Protocolo de Controle de Trans- missão) e o **IP** (**Internet Protocol** — Protocolo da Internet) são dois dos mais importantes da Internet. O protocolo IP especifica o formato dos pacotes que são enviados e recebidos entre roteadores e sistemas finais. Os principais protocolos da Internet são conhecidos como **TCP/IP**. Começaremos a examinar protocolos neste capítulo de intro- dução. Mas isso é só um começo — grande parte deste livro trata de protocolos de redes de computadores!

Dada a importância de protocolos para a Internet, é adequado que todos concordem sobre o que cada um deles faz, de modo que as pessoas possam criar sistemas e produtos que operem entre si. É aqui que os padrões entram em ação. **Padrões da Internet** são desenvolvidos pela IETF (Internet Engineering Task Force — Força de Trabalho de Engenharia da Internet) [IETF, 2012]. Os documentos padronizados da IETF são denominados **RFCs** (**Request For Comments** — pedido de comentários). Os RFCs começaram como solicitações gerais de co- mentários (daí o nome) para resolver problemas de arquitetura que a precursora da Internet enfrentava [Allman, 2011]. Os RFCs costumam ser bastante técnicos e detalhados. Definem protocolos como TCP, IP, HTTP (para a Web) e SMTP (para e-mail). Hoje, existem mais de 6.000 RFCs. Outros órgãos também especificam padrões para componentes de rede, principalmente para enlaces. O IEEE 802 LAN/MAN Standards Committee [IEEE 802, 2009], por exemplo, especifica os padrões Ethernet e Wi-Fi sem fio.

1.1.2 Uma descrição do serviço

A discussão anterior identificou muitos dos componentes que compõem a Internet. Mas também po- demos descrevê-la partindo de um ângulo completamente diferente — ou seja, como *uma infraestrutura que provê serviços a aplicações.* Tais aplicações incluem correio eletrônico, navegação na Web, redes sociais, men- sagem instantânea, Voz sobre IP (VoIP), vídeo em tempo real, jogos distribuídos, compartilhamento de arquivos *peer-to -peer* (P2P), televisão pela Internet, login remoto e muito mais. Essas aplicações são conhecidas como **aplicações distribuídas**, uma vez que envolvem diversos sistemas finais que trocam informações mutuamente. De forma significativa, as aplicações da Internet são executadas em sistemas finais — e não em comutadores de pacote no núcleo da rede. Embora os comutadores de pacotes facilitem a troca de dados entre os sistemas finais, eles não estão relacionados com a aplicação, que é a origem ou o destino dos dados.

Vamos explorar um pouco mais o significado de uma infraestrutura que fornece serviços a aplicações. Nesse sentido, suponha que você tenha uma grande ideia para uma aplicação distribuída para a Internet, uma que possa beneficiar bastante a humanidade ou que simplesmente o enriqueça e o torne famoso. Como transformar essa ideia em uma aplicação real da Internet? Como as aplicações são executadas em sistemas finais, você precisará criar programas que sejam executados em sistemas finais. Você poderia, por exemplo, criar seus programas em Java, C ou Python. Agora, já que você está desenvolvendo uma aplicação distribuída para a Internet, os progra- mas executados em diferentes sistemas finais precisarão enviar dados uns aos outros. E, aqui, chegamos ao as- sunto principal — o que leva ao modo alternativo de descrever a Internet como uma plataforma para aplicações. De que modo um programa, executado em um sistema final, orienta a Internet a enviar dados a outro programa executado em outro sistema final?

Os sistemas finais ligados à Internet oferecem uma **Interface de Programação de Aplicação** (API) que es- pecifica como o programa que é executado no sistema final solicita à infraestrutura da Internet que envie dados a um programa de destino específico, executado em outro sistema final. Essa API da Internet é um conjunto de regras que o software emissor deve cumprir para que a Internet seja capaz de enviar os dados ao programa de destino. Discutiremos a API da Internet mais detalhadamente no Capítulo 2. Agora, vamos traçar uma simples comparação, que será utilizada com frequência neste livro. Suponha que Alice queria enviar uma carta para Bob utilizando o serviço postal. Alice, é claro, não pode apenas escrever a carta (os dados) e atirá-la pela janela.

REDES DE COMPUTADORES E A INTERNET • 5

Em vez disso, o serviço postal necessita que ela coloque a carta em um envelope; escreva o nome completo de Bob, endereço e CEP no centro do envelope; feche; coloque um selo no canto superior direito; e, por fim, leve o envelope a uma agência de correio oficial. Dessa maneira, o serviço postal possui sua própria “API de serviço postal”, ou conjunto de regras, que Alice deve cumprir para que sua carta seja entregue a Bob. De um modo se- melhante, a Internet possui uma API que o software emissor de dados deve seguir para que a Internet envie os dados para o software receptor.

O serviço postal, claro, fornece mais de um serviço a seus clientes: entrega expressa, aviso de recebimento, carta simples e muito mais. De modo semelhante, a Internet provê diversos serviços a suas aplicações. Ao de- senvolver uma aplicação para a Internet, você também deve escolher um dos serviços que a rede oferece. Uma descrição dos serviços será apresentada no Capítulo 2.

Acabamos de apresentar duas descrições da Internet: uma delas diz respeito a seus componentes de hardware e software, e a outra, aos serviços que ela oferece a aplicações distribuídas. Mas talvez você ainda esteja confuso sobre o que é a Internet. O que é comutação de pacotes e TCP/IP? O que são roteadores? Que tipos de enlaces de comunicação estão presentes na Internet? O que é uma aplicação distribuída? Como uma torradeira ou um sensor de variações meteorológicas podem ser ligados à Internet? Se você está um pouco assustado com tudo isso agora, não se preocupe — a finalidade deste livro é lhe apresentar os mecanismos da Internet e também os princípios que determinam como e por que ela funciona. Explicaremos esses termos e questões importantes nas seções e nos capítulos subsequentes.

1.1.3 O que é um protocolo?

Agora que já entendemos um pouco o que é a Internet, vamos considerar outra palavra fundamental usada em redes de computadores: *protocolo*. O que é um protocolo? O que um protocolo faz?

**Uma analogia humana**

Talvez seja mais fácil entender a ideia de um protocolo de rede de computadores considerando primeiro algumas analogias humanas, já que executamos protocolos o tempo todo. Considere o que você faz quando quer perguntar as horas a alguém. Um diálogo comum é ilustrado na Figura 1.2. O protocolo humano (ou as boas maneiras, ao menos) dita que, ao iniciarmos uma comunicação com outra pessoa, primeiro a cumprimentemos (o primeiro “oi” da Figura 1.2). A resposta comum para um “oi” é um outro “oi”. Implicitamente, tomamos a res- posta cordial “oi” como uma indicação de que podemos prosseguir e perguntar as horas. Uma reação diferente ao “oi” inicial (tal como “Não me perturbe!”, “*I don’t speak Portuguese*!” ou alguma resposta atravessada) poderia indicar falta de vontade ou incapacidade de comunicação. Nesse caso, o protocolo humano seria não perguntar que horas são. Às vezes, não recebemos nenhuma resposta para uma pergunta, caso em que em geral desistimos de perguntar as horas à pessoa. Note que, no nosso protocolo humano, *há mensagens específicas que enviamos e ações específicas que realizamos em reação às respostas recebidas ou a outros eventos* (como nenhuma resposta após certo tempo). É claro que mensagens transmitidas e recebidas e ações realizadas quando essas mensagens são enviadas ou recebidas ou quando ocorrem outros eventos desempenham um papel central em um protocolo humano. Se as pessoas executarem protocolos diferentes (por exemplo, se uma pessoa tem boas maneiras, mas a outra não; se uma delas entende o conceito de horas, mas a outra não), os protocolos não interagem e nenhum trabalho útil pode ser realizado. O mesmo é válido para redes — é preciso que duas (ou mais) entidades comuni- cantes executem o mesmo protocolo para que uma tarefa seja realizada.

Vamos considerar uma segunda analogia humana. Suponha que você esteja assistindo a uma aula (sobre redes de computadores, por exemplo). O professor está falando monotonamente sobre protocolos e você está confuso. Ele para e pergunta: “Alguma dúvida?” (uma mensagem que é transmitida a todos os alunos e recebida por todos os que não estão dormindo). Você levanta a mão (transmitindo uma mensagem implícita ao profes- sor). O professor percebe e, com um sorriso, diz “Sim...” (uma mensagem transmitida, incentivando-o a fazer sua

• 6REDES DE COMPUTADORES E A INTERNET FIGURA 1.2 UM PROTOCOLO HUMANO E UM PROTOCOLO DE REDE DE COMPUTADORES

Oi

Solicitação de conexão TCP

Que horas são, por favor? Oi

Resposta de conexão TCP

GET http://www.awl.com/kurose-ross

2h00

<arquivo>

Tempo Tempo

Tempo Tempo

pergunta — professores *adoram* perguntas) e você então faz a sua (isto é, transmite sua mensagem ao professor). Ele ouve (recebe sua mensagem) e responde (transmite uma resposta a você). Mais uma vez, percebemos que a transmissão e a recepção de mensagens e um conjunto de ações convencionais, realizadas quando as mensagens são enviadas e recebidas, estão no centro desse protocolo de pergunta e resposta.

**Protocolos de rede**

Um protocolo de rede é semelhante a um protocolo humano; a única diferença é que as entidades que tro- cam mensagens e realizam ações são componentes de hardware ou software de algum dispositivo (por exemplo, computador, smartphone, tablet, roteador ou outro equipamento habilitado para rede). Todas as atividades na Internet que envolvem duas ou mais entidades remotas comunicantes são governadas por um protocolo. Por exemplo, protocolos executados no hardware de dois computadores conectados fisicamente controlam o fluxo de bits no “cabo” entre as duas placas de interface de rede; protocolos de controle de congestionamento em sistemas finais controlam a taxa com que os pacotes são transmitidos entre a origem e o destino; protocolos em roteadores determinam o caminho de um pacote da origem ao destino. Eles estão em execução por toda a Internet e, em consequência, grande parte deste livro trata de protocolos de rede de computadores.

Como exemplo de um protocolo de rede de computadores com o qual você provavelmente está familiarizado, considere o que acontece quando fazemos uma requisição a um servidor Web, isto é, quando digitamos o URL de uma página Web no *browser*. Isso é mostrado no lado direito da Figura 1.2. Primeiro, o computador enviará uma mensagem de requisição de conexão ao servidor Web e aguardará uma resposta. O servidor receberá essa mensa- gem de requisição de conexão e retornará uma mensagem de resposta de conexão. Sabendo que agora está tudo cer- to para requisitar o documento da Web, o computador envia então o nome da página Web que quer buscar naquele servidor com uma mensagem GET. Por fim, o servidor retorna a página (arquivo) para o computador.

Dados o exemplo humano e o exemplo de rede anteriores, as trocas de mensagens e as ações realizadas quando essas mensagens são enviadas e recebidas são os elementos fundamentais para a definição de um protocolo:

REDES DE COMPUTADORES E A INTERNET • 7

*Um* ***protocolo*** *define o formato e a ordem das mensagens trocadas entre duas ou mais entidades comuni- cantes, bem como as ações realizadas na transmissão e/ou no recebimento de uma mensagem ou outro evento.*

A Internet e as redes de computadores em geral fazem uso intenso de protocolos. Diferentes tipos são usados para realizar diferentes tarefas de comunicação. À medida que for avançando na leitura deste livro, você perceberá que alguns protocolos são simples e diretos, enquanto outros são complexos e intelectualmente profundos. Dominar a área de redes de computadores equivale a entender o que são, por que existem e como funcionam os protocolos de rede.

1.2 A PERIFERIA DA INTERNET

Nas seções anteriores, apresentamos uma descrição de alto nível da Internet e dos protocolos de rede. Agora passaremos a tratar com um pouco mais de profundidade os componentes de uma rede de computadores (e da Internet, em particular). Nesta seção, começamos pela periferia de uma rede e examinamos os componentes com os quais estamos mais familiarizados — a saber, computadores, smartphones e outros equipamentos que usamos diariamente. Na seção seguinte, passaremos da periferia para o núcleo da rede e estudaremos comutação e rotea- mento em redes de computadores.

Como descrito na seção anterior, no jargão de rede de computadores, os computadores e outros dispositivos conectados à Internet são frequentemente chamados de sistemas finais, pois se encontram na periferia da Inter- net, como mostrado na Figura 1.3. Os sistemas finais da Internet incluem computadores de mesa (por exemplo, PCs de mesa, MACs e caixas Linux), servidores (por exemplo, servidores Web e de e-mails), e computadores móveis (por exemplo, notebooks, smartphones e tablets). Além disso, diversos aparelhos alternativos estão sendo utilizados com a Internet como sistemas finais (veja nota em destaque).

Sistemas finais também são denominados *hospedeiros* (ou *hosts*) porque hospedam (isto é, executam) progra- mas de aplicação, tais como um navegador (*browser*) da Web, um programa servidor da Web, um programa leitor de e-mail ou um servidor de e-mail. Neste livro, utilizaremos os termos hospedeiros e sistemas finais como sinônimos.

***HISTÓRICO DO CASO***

Um conjunto impressionante de sistemas finais da Internet

Não faz muito tempo, os sistemas finais conec- tados à Internet eram quase sempre computadores tradicionais, como máquinas de mesa e servidores de grande capacidade. Desde o final da década de 1990 até hoje, um amplo leque de equipamentos e dispo- sitivos interessantes, cada vez mais diversos, vem sendo conectado à Internet, aproveitando sua capa- cidade de enviar e receber dados digitais. Tendo em vista a onipresença da Internet, seus protocolos bem definidos (padronizados) e a disponibilidade comercial de hardware capacitado para ela, é natural usar sua tecnologia para interconectar esses dispositivos entre si e a servidores conectados à Internet.

Muitos deles parecem ter sido criados exclusiva- mente para diversão — consoles de videogame (por exemplo, Xbox da Microsoft), televisores habilitados para Internet, quadros de fotos digitais que baixam e

exibem imagens digitais, máquinas de lavar, refrige- radores e até mesmo uma torradeira da Internet que baixa informações meteorológicas de um servidor e grava uma imagem da previsão do tempo do dia em questão (por exemplo, nublado, com sol) na sua torrada matinal [BBC, 2001]. Telefones celulares que utilizam IP com recursos de GPS permitem o uso fácil de serviços dependentes do local (mapas, informa- ções sobre serviços ou pessoas nas proximidades). Redes de sensores incorporadas ao ambiente físico permitem a monitoração de prédios, pontes, ativi- dade sísmica, habitats da fauna selvagem, estuários de rios e clima. Aparelhos biomédicos podem ser in- corporados e conectados em rede, numa espécie de rede corporal. Com tantos dispositivos diversificados sendo conectados em rede, a Internet está realmente se tornando uma “Internet de coisas” [ITU, 2005b].

• 8REDES DE COMPUTADORES E A INTERNET FIGURA 1.3 INTERAÇÃO ENTRE SISTEMAS FINAIS

Rede móvel

Às vezes, sistemas finais são ainda subdivididos em duas categorias: **clientes** e **servidores**. Informalmente, clien- tes costumam ser PCs de mesa ou portáteis, smartphones e assim por diante, ao passo que servidores tendem a ser máquinas mais poderosas, que armazenam e distribuem páginas Web, vídeo em tempo real, retransmissão de e-mails e assim por diante. Hoje, a maioria dos servidores dos quais recebemos resultados de busca, e-mail, páginas e vídeos reside em grandes **datacenters**. Por exemplo, o Google tem 30 a 50 datacenters, com muitos deles tendo mais de cem mil servidores.

1.2.1 Redes de acesso

Tendo considerado as aplicações e sistemas finais na “periferia da Internet”, vamos agora considerar a rede de acesso — a rede física que conecta um sistema final ao primeiro roteador (também conhecido como “roteador

ISP nacional ou global

ISP local ou regional

Rede doméstica

Rede corporativa

REDES DE COMPUTADORES E A INTERNET • 9

de borda”) de um caminho partindo de um sistema final até outro qualquer. A Figura 1.4 apresenta diversos tipos de redes de acesso com linhas espessas, linhas cinzas e os ambientes (doméstico, corporativo e móvel sem fio) em que são usadas.

**Acesso doméstico: DSL, cabo, FTTH, discado e satélite**

Hoje, nos países desenvolvidos, mais de 65% dos lares possuem acesso à Internet, e, dentre eles, Coreia, Ho- landa, Finlândia e Suécia lideram com mais de 80%, quase todos por meio de uma conexão de banda larga em alta velocidade [ITU, 2011]. A Finlândia e a Espanha há pouco declararam que o acesso à Internet de alta velocidade é um “direito legal”. Dado a esse interesse intenso no acesso doméstico, vamos começar nossa introdução às redes de acesso considerando como os lares se conectam à Internet.

Os dois tipos de acesso residencial banda largas predominantes são a **linha digital de assinante (DSL)** ou a cabo. Normalmente uma residência obtém acesso DSL à Internet da mesma empresa que fornece acesso telefôni- co local com fio (por exemplo, a operadora local). Assim, quando a DSL é utilizada, uma operadora do cliente é também seu provedor de serviços de Internet (ISP). Como ilustrado na Figura 1.5, o modem DSL de cada cliente utiliza a linha telefônica existente (par de fios de cobre trançado, que discutiremos na Seção 1.2.2) para trocar

FIGURA 1.4 REDES DE ACESSO

ISP nacional ou global Rede móvel

ISP local ou regional

Rede doméstica

Rede corporativa

• 10REDES DE COMPUTADORES E A INTERNET dados com um multiplexador digital de acesso à linha do assinante (DSLAM), em geral localizado na CT da ope- radora. O modem DSL da casa apanha dados digitais e os traduz para sons de alta frequência, para transmissão pelos fios de telefone até a CT; os sinais analógicos de muitas dessas residências são traduzidos de volta para o formato digital no DSLAM.

A linha telefônica conduz, simultaneamente, dados e sinais telefônicos tradicionais, que são codificados em frequências diferentes:

• um canal *downstream* de alta velocidade, com uma banda de 50 kHz a 1 MHZ;

• um canal *upstream* de velocidade média, com uma banda de 4 kHz a 50 kHz;

• um canal de telefone bidirecional comum, com uma banda de 0 a 4 kHz.

Essa abordagem faz que a conexão DSL pareça três conexões distintas, de modo que um telefonema e a conexão com a Internet podem compartilhar a DSL ao mesmo tempo. (Descreveremos essa técnica de multiple- xação por divisão de frequência na Seção 1.3.2.) Do lado do consumidor, para os sinais que chegam até sua casa, um distribuidor separa os dados e os sinais telefônicos e conduz o sinal com os dados para o modem DSL. Na operadora, na CT, o DSLAM separa os dados e os sinais telefônicos e envia aqueles para a Internet. Centenas ou mesmo milhares de residências se conectam a um único DSLAM [Dischinger, 2007].

Os padrões DSL definem taxas de transmissão de 12 Mbits/s *downstream* e 1,8 Mbits/s *upstream* [ITU, 1999] e 24 Mbits/s *downstream* e 2,5 Mbits/s *upstream* [ITU, 2003]. Em razão de as taxas de transmissão e recebimento serem diferentes, o acesso é conhecido como assimétrico. As taxas reais alcançadas podem ser menores do que as indicadas anteriormente, pois o provedor de DSL pode, de modo proposital, limitar uma taxa residencial quando é oferecido o serviço em camadas (diferentes taxas, disponíveis a diferentes preços), ou por- que a taxa máxima pode ser limitada pela distância entre a residência e a CT, pela bitola da linha de par trançado e pelo grau de interferência elétrica. Os engenheiros projetaram o DSL expressamente para distâncias curtas entre a residência e a CT; quase sempre, se a residência não estiver localizada dentro de 8 a 16 quilômetros da CT, ela precisa recorrer a uma forma de acesso alternativa à Internet.

Embora o DSL utilize a infraestrutura de telefone local da operadora, o **acesso à Internet a cabo** utiliza a infraestrutura de TV a cabo da operadora de televisão. Uma residência obtém acesso à Internet a cabo da mesma empresa que fornece a televisão a cabo. Como ilustrado na Figura 1.6, as fibras óticas conectam o terminal de distribuição às junções da região, sendo o cabo coaxial tradicional utilizado para chegar às casas e apartamentos de maneira individual. Cada junção costuma suportar de 500 a 5.000 casas. Em razão de a fibra e o cabo coaxial fazerem parte desse sistema, a rede é denominada híbrida fibra-coaxial (HFC).

O acesso à Internet a cabo necessita de modems especiais, denominados modems a cabo. Como o DSL, o modem a cabo é, em geral, um aparelho externo que se conecta ao computador residencial pela porta Ethernet. (Discutiremos Ethernet em detalhes no Capítulo 5.) No terminal de distribuição, o sistema de término do mo- dem a cabo (CMTS) tem uma função semelhante à do DSLAM da rede DSL — transformar o sinal analógico

FIGURA 1.5 ACESSO À INTERNET POR DSL

Telefone residencialModem DSL

Computador residencial

Linha telefônica existente: telefone com 0-4 KHz; dados *upstream* com 4-50 KHz; dados *downstream* com 50 KHZ – 1 MHz

DSLAM

Central telefônicaInternet Splitter

Rede telefônica

REDES DE COMPUTADORES E A INTERNET • 11

FIGURA 1.6 UMA REDE DE ACESSO HÍBRIDA FIBRAdCOAXIAL

Cabo coaxial

Centenas de residências

Nó de fibra

Cabo de fibra ótica

Internet

ótica

CMTS

Centenas de

Nó de residências

fibra

Terminal de distribuição ótica

enviado dos modems a cabo de muitas residências *downstream* para o formato digital. Os modems a cabo di- videm a rede HFC em dois canais, um de transmissão (*downstream*) e um de recebimento (*upstream*). Como a tecnologia DSL, o acesso costuma ser assimétrico, com o canal *downstream* recebendo uma taxa de transmissão maior do que a do canal *upstream*. O padrão DOCSIS 2.0 define taxas *downstream* de até 42,8 Mbits/s e taxas *upstream* de até 30,7 Mbits/s. Como no caso das redes DSL, a taxa máxima possível de ser alcançada pode não ser observada por causa de taxas de dados contratadas inferiores ou problemas na mídia.

Uma característica importante do acesso a cabo é o fato de ser um meio de transmissão compartilhado. Em especial, cada pacote enviado pelo terminal viaja pelos enlaces *downstream* até cada residência e cada pacote enviado por uma residência percorre o canal *upstream* até o terminal de transmissão. Por essa razão, se diversos usuários estiverem fazendo o *download* de um arquivo em vídeo ao mesmo tempo no canal *downstream*, cada um receberá o arquivo a uma taxa bem menor do que a taxa de transmissão a cabo agregada. Por outro lado, se há somente alguns usuários ativos navegando, então cada um poderá receber páginas da Web a uma taxa de *downstream* máxima, pois esses usuários raramente solicitarão uma página ao mesmo tempo. Como o canal *upstream* também é compartilhado, é necessário um protocolo de acesso múltiplo distribuído para coordenar as transmissões e evitar colisões. (Discutiremos a questão de colisão no Capítulo 5.)

Embora as redes DSL e a cabo representem mais de 90% do acesso de banda larga residencial nos Estados Unidos, uma tecnologia que promete velocidades ainda mais altas é a implantação da ***fiber to the home* (FTTH)** [FTTH Council, 2011a]. Como o nome indica, o conceito da FTTH é simples — oferece um caminho de fibra ótica da CT diretamente até a residência. Nos Estados Unidos, a Verizon saiu na frente com a tecnologia FTTH, lançando o serviço FIOS [Verizon FIOS, 2012].

Existem várias tecnologias concorrentes para a distribuição ótica das CTs às residências. A rede mais sim- ples é chamada fibra direta, para a qual existe uma fibra saindo da CT para cada casa. Em geral, uma fibra que sai da central telefônica é compartilhada por várias residências; ela é dividida em fibras individuais do cliente apenas após se aproximar relativamente das casas. Duas arquiteturas concorrentes de rede de distribuição ótica apre- sentam essa divisão: redes óticas ativas (AONs) e redes óticas passivas (PONs). A AON é na essência a Ethernet comutada, assunto discutido no Capítulo 5.

Aqui, falaremos de modo breve sobre a PON, que é utilizada no serviço FIOS da Verizon. A Figura 1.7 mos- tra a FTTH utilizando a arquitetura de distribuição de PON. Cada residência possui um terminal de rede ótica (ONT), que é conectado por uma fibra ótica dedicada a um distribuidor da região. O distribuidor combina certo número de residências (em geral menos de 100) a uma única fibra ótica compartilhada, que se liga a um terminal de linha ótica (OLT) na CT da operadora. O OLT, que fornece conversão entre sinais ópticos e elétricos, se co-

• 12REDES DE COMPUTADORES E A INTERNET FIGURA 1.7 ACESSO A INTERNET POR FTTH

Internet Central telefônica

ONT

Distribuidor óptico ONT

ONT

necta à Internet por meio de um roteador da operadora. Na residência, o usuário conecta ao ONT um roteador residencial (quase sempre sem fio) pelo qual acessa a Internet. Na arquitetura de PON, todos os pacotes enviados do OLT ao distribuidor são nele replicados (semelhante ao terminal de distribuição a cabo).

A FTTH consegue potencialmente oferecer taxas de acesso à Internet na faixa de gigabits por segundo. Porém, a maioria dos provedores de FTTH oferece diferentes taxas, das quais as mais altas custam muito mais. A velocidade de *downstream* média dos clientes FTTH nos Estados Unidos era de mais ou menos 20 Mbits/s em 2011 (em com- paração com 13 Mbits/s para as redes de acesso a cabo e menos de 5 Mbits/s para DSL) [FTTH Council, 2011b].

Duas outras tecnologias também são usadas para oferecer acesso da residência à Internet. Em locais onde DSL, cabo e FTTH não estão disponíveis (por exemplo, em algumas propriedades rurais), um enlace de satélite pode ser empregado para conexão em velocidades não maiores do que 1 Mbit/s; StarBand e HughesNet são dois desses provedores de acesso por satélite. O acesso discado por linhas telefônicas tradicionais é baseado no mesmo modelo do DSL — um modem doméstico se conecta por uma linha telefônica a um modem no ISP. Em com- paração com DSL e outras redes de acesso de banda larga, o acesso discado é terrivelmente lento em 56 kbits/s.

**Acesso na empresa (e na residência): Ethernet e Wi-Fi**

Nos *campi* universitários e corporativos, e cada vez mais em residências, uma rede local (LAN) costuma ser usada para conectar sistemas finais ao roteador da periferia. Embora existam muitos tipos de tecnologia LAN, a Ethernet é, de longe, a de acesso predominante nas redes universitárias, corporativas e domésticas. Como mos- trado na Figura 1.8, os usuários utilizam um par de fios de cobre trançado para se conectarem a um comutador Ethernet, uma tecnologia tratada com mais detalhes no Capítulo 5. O comutador Ethernet, ou uma rede desses comutadores interconectados, é por sua vez conectado à Internet maior. Com o acesso por uma rede Ethernet, os usuários normalmente têm acesso de 100 Mbits/s com o comutador Ethernet, enquanto os servidores possuem um acesso de 1 Gbit/s ou até mesmo 10 Gbits/s.

Está cada vez mais comum as pessoas acessarem a Internet sem fio, seja por notebooks, smartphones, tablets ou por outros dispositivos (veja o texto “Um conjunto impressionante de sistemas finais da Internet”, na seção “His- tórico do caso”, p. 9). Em uma LAN sem fio, os usuários transmitem/recebem pacotes para/de um ponto de acesso que está conectado à rede da empresa (quase sempre incluindo Ethernet com fio) que, por sua vez, é conectada à Internet com fio. Um usuário de LAN sem fio deve estar no espaço de alguns metros do ponto de acesso. O acesso à LAN sem fio baseado na tecnologia IEEE 802.11, ou seja, Wi-Fi, está presente em todo lugar — universidades, empresas, cafés, aeroportos, residências e, até mesmo, em aviões. Em muitas cidades, é possível ficar na esquina de uma rua e estar dentro da faixa de dez ou vinte estações-base (para um mapa global de estações-base 802.11 que foram descobertas e acessadas por pessoas que apreciam coisas do tipo, veja wigle.net [2012]). Como discutido com detalhes no Capítulo 6, hoje o 802.11 fornece uma taxa de transmissão compartilhada de até 54 Mbits/s.

OLT Fibras ópticas

REDES DE COMPUTADORES E A INTERNET • 13

FIGURA 1.8 ACESSO A INTERNET POR ETHERNET

100 Mbits/s

Comutador

Roteador

100 Mbits/s

Ethernet

institucional

institucional

Para ISP da instituição 100 Mbits/s

Servidor

Embora as redes de acesso por Ethernet e Wi-Fi fossem implantadas no início em ambientes corporativos (empresas, universidades), elas há pouco se tornaram componentes bastante comuns das redes residenciais. Mui- tas casas unem o acesso residencial banda larga (ou seja, modems a cabo ou DSL) com a tecnologia LAN sem fio a um custo acessível para criar redes residenciais potentes [Edwards, 2011]. A Figura 1.9 mostra um esquema de uma rede doméstica típica. Ela consiste em um notebook móvel e um computador com fio; uma estação-base (o ponto de acesso sem fio), que se comunica com o computador sem fio; um modem a cabo, fornecendo acesso banda larga à Internet; e um roteador, que interconecta a estação-base e o computador fixo com o modem a cabo. Essa rede permite que os moradores tenham acesso banda larga à Internet com um usuário se movimentando da cozinha ao quintal e até os quartos.

**Acesso sem fio em longa distância: 3G e LTE**

Cada vez mais, dispositivos como iPhones, BlackBerrys e dispositivos Android estão sendo usados para enviar e-mail, navegar na Web, tuitar e baixar música enquanto se movimentam. Esses dispositivos empregam a mesma infraestrutura sem fios usada para a telefonia celular para enviar/receber pacotes por uma estação-base que é controlada pela operadora da rede celular. Diferente do Wi-Fi, um usuário só precisa estar dentro de algu- mas dezenas de quilômetros (ao contrário de algumas dezenas de metros) da estação-base.

As empresas de telecomunicação têm investido enormemente na assim chamada terceira geração (3G) sem fio, que oferece acesso remoto à Internet por pacotes comutados a velocidades que ultrapassam 1 Mbit/s. Porém, até mesmo tecnologias de acesso remotas de maior velocidade — uma quarta geração (4G) — já estão sendo im-

FIGURA 1.9 ESQUEMA DE UMA REDE DOMÉSTICA TÍPICA

Terminal de distribuição a cabo Residência

Internet

• REDES DE COMPUTADORES E A INTERNET 14plantadas. LTE (de “Long -Term Evolution”, um candidato ao prêmio de Pior Acrônimo do Ano, PAA) tem suas raízes na tecnologia 3G, e tem potencial para alcançar velocidades superiores a 10 Mbits/s. Taxas *downstream* LTE de muitas dezenas de Mbits/s foram relatadas em implementações comerciais. Veremos os princípios básicos das redes sem fio e mobilidade, além de tecnologias Wi -Fi, 3G e LTE (e mais!) no Capítulo 6.

1.2.2 Meios físicos

Na subseção anterior, apresentamos uma visão geral de algumas das mais importantes tecnologias de acesso à Internet. Ao descrevê-las, indicamos também os meios físicos utilizados por elas. Por exemplo, dissemos que o HFC usa uma combinação de cabo de fibra ótica. Dissemos que DSL e Ethernet utilizam fios de cobre. Dissemos também que redes de acesso móveis usam o espectro de rádio. Nesta subseção damos uma visão geral desses e de outros meios de transmissão empregados na Internet.

Para definir o que significa meio físico, vamos pensar na curta vida de um bit. Considere um bit saindo de um sistema final, transitando por uma série de enlaces e roteadores e chegando a outro sistema final. Esse pobre e pequeno bit é transmitido muitas e muitas vezes. Primeiro, o sistema final originador transmite o bit e, logo em seguida, o primeiro roteador da série recebe -o; então, o primeiro roteador envia-o para o segundo roteador e assim por diante. Assim, nosso bit, ao viajar da origem ao destino, passa por uma série de pares transmissor- -receptor, que o recebem por meio de ondas eletromagnéticas ou pulsos ópticos que se propagam por um **meio físico**. Com muitos aspectos e formas possíveis, o meio físico não precisa ser obrigatoriamente do mesmo tipo para cada par transmissor–receptor ao longo do caminho. Alguns exemplos de meios físicos são: par de fios de cobre trançado, cabo coaxial, cabo de fibra ótica multimodo, espectro de rádio terrestre e espectro de rádio por satélite. Os meios físicos se enquadram em duas categorias: **meios guiados** e **meios não guiados**. Nos meios guia- dos, as ondas são dirigidas ao longo de um meio sólido, tal como um cabo de fibra ótica, um par de fios de cobre trançado ou um cabo coaxial. Nos meios não guiados, as ondas se propagam na atmosfera e no espaço, como é o caso de uma LAN sem fio ou de um canal digital de satélite.

Contudo, antes de examinar as características dos vários tipos de meios, vamos discutir um pouco seus custos. O custo real de um enlace físico (fio de cobre, cabo de fibra ótica e assim por diante) costuma ser insignificante em comparação a outros. Em especial, o custo da mão de obra de instalação do enlace físico pode ser várias vezes maior do que o do material. Por essa razão, muitos construtores instalam pares de fios trançados, fibra ótica e cabo coaxial em todas as salas de um edifício. Mesmo que apenas um dos meios seja usado inicialmente, há uma boa probabilidade de outro ser usado no futuro próximo — portanto, poupa-se dinheiro por não ser preciso instalar fiação adicional depois.

**Par de fios de cobre trançado**

O meio de transmissão guiado mais barato e mais usado é o par de fios de cobre trançado, que vem sendo empregado há mais de cem anos nas redes de telefonia. De fato, mais de 99% da fiação que conecta aparelhos telefônicos a centrais locais utilizam esse meio. Quase todos nós já vimos um em casa ou no local de trabalho: esse par constituído de dois fios de cobre isolados, cada um com cerca de um milímetro de espessura, enrolados em espiral. Os fios são trançados para reduzir a interferência elétrica de pares semelhantes que estejam próximos. Normalmente, uma série de pares é conjugada dentro de um cabo, isolando-se os pares com blindagem de pro- teção. Um par de fios constitui um único enlace de comunicação. O **par trançado sem blindagem** (*unshielded twisted pair* — UTP) costuma ser usado em redes de computadores de edifícios, isto é, em LANs. Hoje, as taxas de transmissão de dados para as LANs de pares trançados estão na faixa de 10 Mbits/s a 10 Gbits/s. As taxas de trans- missão de dados que podem ser alcançadas dependem da bitola do fio e da distância entre transmissor e receptor. Quando a tecnologia da fibra ótica surgiu na década de 1980, muitos depreciaram o par trançado por suas taxas de transmissão de bits relativamente baixas. Alguns até acharam que a tecnologia da fibra ótica o substitui- ria por completo. Mas ele não desistiu assim tão facilmente. A moderna tecnologia de par trançado, tal como o

REDES DE COMPUTADORES E A INTERNET • 15

cabo de categoria 6a, pode alcançar taxas de transmissão de dados de 10 Gbits/s para distâncias de até algumas centenas de metros. No final, o par trançado firmou-se como a solução dominante para LANs de alta velocidade. Como vimos anteriormente, o par trançado também é usado para acesso residencial à Internet. Vimos que a tecnologia do modem discado possibilita taxas de acesso de até 56 kbits/s com pares trançados. Vimos também que a tecnologia DSL (linha digital de assinante) permitiu que usuários residenciais acessem a Internet em deze- nas de Mbits/s com pares de fios trançados (quando as residências estão próximas ao modem do ISP).

**Cabo coaxial**

Como o par trançado, o cabo coaxial é constituído de dois condutores de cobre, porém concêntricos e não pa- ralelos. Com essa configuração, isolamento e blindagem especiais, pode alcançar taxas altas de transmissão de dados. Cabos coaxiais são muito comuns em sistemas de televisão a cabo. Como já comentamos, recentemente sistemas de televisão a cabo foram acoplados com modems a cabo para oferecer aos usuários residenciais acesso à Internet a ve- locidades de dezenas de Mbits/s. Em televisão a cabo e acesso a cabo à Internet, o transmissor passa o sinal digital para uma banda de frequência específica e o sinal analógico resultante é enviado do transmissor para um ou mais receptores. O cabo coaxial pode ser utilizado como um **meio compartilhado** guiado. Vários sistemas finais podem ser conectados diretamente ao cabo, e todos eles recebem qualquer sinal que seja enviado pelos outros sistemas finais.

**Fibras ópticas**

A fibra ótica é um meio delgado e flexível que conduz pulsos de luz, cada um deles representando um bit. Uma única fibra ótica pode suportar taxas de transmissão elevadíssimas, de até dezenas ou mesmo centenas de gigabits por segundo. Fibras óticas são imunes à interferência eletromagnética, têm baixíssima atenuação de sinal até cem quilômetros e são muito difíceis de derivar. Essas características fizeram da fibra ótica o meio preferido para a transmissão guiada de grande alcance, em especial para cabos submarinos. Hoje, muitas redes telefôni- cas de longa distância dos Estados Unidos e de outros países usam exclusivamente fibras óticas, que também predominam no *backbone* da Internet. Contudo, o alto custo de equipamentos ópticos — como transmissores, receptores e comutadores — vem impedindo sua utilização para transporte a curta distância, como em LANs ou em redes de acesso residenciais. As velocidades de conexão do padrão Optical Carrier (OC) variam de 51,8 Mbits/s a 39,8 Gbits/s; essas especificações são frequentemente denominadas OC-*n*, em que a velocidade de conexão se iguala a n × 51,8 Mbits/s. Os padrões usados hoje incluem OC-1, OC-3, OC-12, OC-24, OC-48, OC-96, OC-192 e OC-768. Mukherjee [2006] e Ramaswamy [2010] apresentam uma abordagem de vários aspectos da rede óptica.

**Canais de rádio terrestres**

Canais de rádio carregam sinais dentro do espectro eletromagnético. São um meio atraente porque sua insta- lação não requer cabos físicos, podem atravessar paredes, dão conectividade ao usuário móvel e, potencialmente, conseguem transmitir um sinal a longas distâncias. As características de um canal de rádio dependem muito do am- biente de propagação e da distância pela qual o sinal deve ser transmitido. Condições ambientais determinam perda de sinal no caminho e atenuação por efeito de sombra (que reduz a intensidade do sinal quando ele transita por distâncias longas e ao redor/através de objetos interferentes), atenuação por caminhos múltiplos (devido à reflexão do sinal quando atinge objetos interferentes) e interferência (por outras transmissões ou sinais eletromagnéticos).

Canais de rádio terrestres podem ser classificados, de modo geral, em três grupos: os que operam sobre distâncias muito curtas (por exemplo, com um ou dois metros); os de pequeno alcance, que funcionam em locais próximos, normalmente abrangendo de dez a algumas centenas de metros, e os de longo alcance, que abrangem dezenas de quilômetros. Dispositivos pessoais como fones sem fio, teclados e dispositivos médicos operam por curtas distâncias; as tecnologias LAN sem fio, descritas na Seção 1.2.1, utilizam canais de rádio local; as tecnolo-

• REDES DE COMPUTADORES E A INTERNET 16gias de acesso em telefone celular utilizam canal de rádio de longo alcance. Abordaremos canais de rádio deta-

lhadamente no Capítulo 6.

**Canais de rádio por satélite**

Um satélite de comunicação liga dois ou mais transmissores-receptores de micro-ondas baseados na Terra, denominados estações terrestres. Ele recebe transmissões em uma faixa de frequência, gera novamente o sinal usando um repetidor (sobre o qual falaremos a seguir) e o transmite em outra frequência. Dois tipos de satélites são usados para comunicações: **satélites geoestacionários** e **satélites de órbita baixa (LEO)**.

Os satélites geoestacionários ficam de modo permanente sobre o mesmo lugar da Terra. Essa presença estacio- nária é conseguida colocando-se o satélite em órbita a 36 mil quilômetros acima da superfície terrestre. Essa enorme distância da estação terrestre ao satélite e de seu caminho de volta à estação terrestre traz um substancial atraso de propagação de sinal de 280 milissegundos. Mesmo assim, enlaces por satélite, que podem funcionar a velocidades de centenas de Mbits/s, são frequentemente usados em áreas sem acesso à Internet baseado em DSL ou cabo.

Os satélites de órbita baixa são posicionados muito mais próximos da Terra e não ficam sempre sobre um único lugar. Eles giram ao redor da Terra (exatamente como a Lua) e podem se comunicar uns com os outros e com estações terrestres. Para prover cobertura contínua em determinada área, é preciso colocar muitos satélites em órbita. Hoje, existem muitos sistemas de comunicação de baixa altitude em desenvolvimento. A página da Web referente à constelação de satélites da Lloyd [Wood, 2012] fornece e coleta informações sobre esses sistemas para comunicações. A tecnologia de satélites de órbita baixa poderá ser utilizada para acesso à Internet no futuro.

1.3 O NÚCLEO DA REDE

Após termos examinado a periferia da Internet, vamos agora nos aprofundar mais no núcleo da rede — a rede de comutadores de pacote e enlaces que interconectam os sistemas finais da Internet. Os núcleos da rede aparecem destacados em cinza na Figura 1.10.

1.3.1 Comutação de pacotes

Em uma aplicação de rede, sistemas finais trocam **mensagens** entre si. Mensagens podem conter qualquer coisa que o projetista do protocolo queira. Podem desempenhar uma função de controle (por exemplo, as men- sagens “oi” no nosso exemplo de comunicação na Figura 1.2) ou conter dados, tal como um e-mail, uma imagem JPEG ou um arquivo de áudio MP3. Para enviar uma mensagem de um sistema final de origem para um destino, o originador fragmenta mensagens longas em porções de dados menores, denominadas **pacotes**. Entre origem e destino, cada um deles percorre enlaces de comunicação e **comutadores de pacotes** (há dois tipos principais de comutadores de pacotes: **roteadores** e **comutadores de camada de enlace**). Pacotes são transmitidos por cada enlace de comunicação a uma taxa igual à de transmissão *total*. Assim, se um sistema final de origem ou um comutador de pacotes estiver enviando um pacote de *L* bits por um enlace com taxa de transmissão de *R* bits/s, então o tempo para transmitir o pacote é *L*/*R* segundos.

**Transmissão armazena-e-reenvia**

A maioria dos comutadores de pacotes utiliza a **transmissão armazena-e-reenvia (*store-and-forward*)** nas entradas dos enlaces. A transmissão armazena-e-reenvia significa que o comutador de pacotes deve receber o pacote inteiro antes de poder começar a transmitir o primeiro bit para o enlace de saída. Para explorar a transmissão arma- zena-e-reenvia com mais detalhes, considere uma rede simples, consistindo em dois sistemas finais conectados por um único roteador, conforme mostra a Figura 1.11. Um roteador em geral terá muitos enlaces incidentes, pois sua

REDES DE COMPUTADORES E A INTERNET • 17

FIGURA 1.10 O NÚCLEO DA REDE

ISP nacional ou global Rede móvel

ISP local ou regional

Rede doméstica

Rede corporativa

função é comutar um pacote que chega para um enlace de saída; neste exemplo simples, o roteador tem a tarefa de transferir um pacote de um enlace (entrada) para o único outro enlace conectado. Aqui, a origem tem três pacotes, cada um consistindo em *L* bits, para enviar ao destino. No instante de tempo mostrado na Figura 1.11, a origem transmitiu parte do pacote 1, e a frente do pacote 1 já chegou no roteador. Como emprega a transmissão armazena -e-reenvia, nesse momento, o roteador não pode transmitir os bits que recebeu; em vez disso, ele precisa primeiro manter em buffer (isto é, “armazenar”) os bits do pacote. Somente depois que o roteador tiver recebido *todos* os bits, poderá começar a transmitir (isto é, “reenviar”) o pacote para o enlace de saída. Para ter uma ideia da transmissão armazena-e-reenvia, vamos agora calcular a quantidade de tempo decorrido desde quando a origem começa a en- viar até que o destino tenha recebido o pacote inteiro. (Aqui, ignoraremos o atraso de propagação — o tempo gasto para os bits atravessarem o fio em uma velocidade próxima à da luz —, o que será discutido na Seção 1.4.) A origem começa a transmitir no tempo 0; no tempo *L*/*R* segundos, a origem terá transmitido o pacote inteiro, que terá sido recebido e armazenado no roteador (pois não há atraso de propagação). No tempo *L*/*R* segundos, como o roteador

• 18REDES DE COMPUTADORES E A INTERNET FIGURA 1.11 COMUTAÇÃO DE PACOTES ARMAZENAdEdREENVIA

3

12

*R* bits/s Origem Frente do pacote 1

Destino armazenado no roteador, esperando bits restantes antes de repassar

já terá recebido o pacote inteiro, ele pode começar a transmiti-lo para o enlace de saída, em direção ao destino; no tempo 2*L*/*R*, o roteador terá transmitido o pacote inteiro, e este terá sido recebido pelo destino. Assim, o atraso total é 2*L*/*R*. Se o comutador, em vez disso, reenviasse os bits assim que chegassem (sem primeiro receber o pacote intei- ro), então o atraso total seria *L*/*R*, pois os bits não são mantidos no roteador. Mas, conforme discutiremos na Seção 1.4, os roteadores precisam receber, armazenar e *processar* o pacote inteiro antes de encaminhar.

Agora vamos calcular a quantidade de tempo decorrido desde quando a origem começa a enviar o primeiro pacote até que o destino tenha recebido todos os três. Como antes, no instante *L*/*R*, o roteador começa a reenviar o primeiro pacote. Mas, também no tempo *L*/*R*, a origem começará a enviar o segundo, pois ela terá acabado de mandar o primeiro pacote inteiro. Assim, no tempo 2*L*/*R*, o destino terá recebido o primeiro pacote e o roteador terá recebido o segundo. De modo semelhante, no instante 3*L*/*R*, o destino terá recebido os dois primeiros pa- cotes e o roteador terá recebido o terceiro. Por fim, no tempo 4*L*/*R*, o destino terá recebido todos os três pacotes! Vamos considerar o caso geral do envio de um pacote da origem ao destino por um caminho que consiste em *N* enlaces, cada um com taxa *R* (assim, há *N* – 1 roteadores entre origem e destino). Aplicando a mesma lógica usada anteriormente, vemos que o atraso fim a fim é:

*d*fim a fim = *N R L*(1.1) Você poderá tentar determinar qual seria o atraso para *P* pacotes enviados por uma série de *N* enlaces.

**Atrasos de fila e perda de pacote**

A cada comutador de pacotes estão ligados vários enlaces. Para cada um destes, o comutador de pacotes tem um **buffer de saída** (também denominado **fila de saída**), que armazena pacotes prestes a serem enviados pelo roteador para aquele enlace. Os buffers de saída desempenham um papel fundamental na comutação de pacotes. Se um pacote que está chegando precisa ser transmitido por um enlace, mas o encontra ocupado com a transmissão de outro pacote, deve aguardar no buffer de saída. Desse modo, além dos atrasos de armazenagem e reenvio, os pacotes sofrem **atrasos de fila** no buffer de saída. Esses atrasos são variáveis e dependem do grau de congestionamento da rede. Como o espaço do buffer é finito, um pacote que está chegando pode encontrá-lo lotado de outros que estão esperando transmissão. Nesse caso, ocorrerá uma **perda de pacote** — um pacote que está chegando ou um dos que já estão na fila é descartado.

A Figura 1.12 ilustra uma rede simples de comutação de pacotes. Como na Figura 1.11, os pacotes são repre- sentados por placas tridimensionais. A largura de uma placa representa o número de bits no pacote. Nessa figura, todos os pacotes têm a mesma largura, portanto, o mesmo tamanho. Suponha que os hospedeiros A e B estejam enviando pacotes ao hospedeiro E. Os hospedeiros A e B primeiro enviarão seus pacotes por enlaces Ethernet de 10 Mbits/s até o primeiro comutador, que vai direcioná-los para o enlace de 1,5 Mbits/s. Se, durante um peque- no intervalo de tempo, a taxa de chegada de pacotes ao roteador (quando convertida para bits por segundo) for maior do que 1,5 Mbits/s, ocorrerá congestionamento no roteador, pois os pacotes formarão uma fila no buffer de saída do enlace antes de ser transmitidos para o enlace. Por exemplo, se cada um dos hospedeiros A e B enviar uma rajada de cinco pacotes de ponta a ponta ao mesmo tempo, então a maior parte deles gastará algum tempo

REDES DE COMPUTADORES E A INTERNET • 19

FIGURA 1.12 COMUTAÇÃO DE PACOTES

Ethernet de 10 Mbits/s

AC

1,5 Mbits/s

Fila de pacotes esperando por um enlace de saída

B

Legenda:

D E

Pacotes

esperando na fila. De fato, a situação é semelhante a muitas no dia a dia — por exemplo, quando aguardamos na fila de um caixa de banco ou quando esperamos em uma cabine de pedágio. Vamos analisar esse atraso de fila mais detalhadamente na Seção 1.4.

**Tabelas de repasse e protocolos de roteamento**

Dissemos anteriormente que um roteador conduz um pacote que chega a um de seus enlaces de comunica- ção para outro de seus enlaces de comunicação conectados. Mas como o roteador determina o enlace que deve conduzir o pacote? Na verdade, isso é feito de diversas maneiras por diferentes tipos de rede de computadores. Aqui, descreveremos de modo resumido como isso é feito pela Internet.

Na Internet, cada sistema final tem um endereço denominado endereço IP. Quando um sistema final de origem quer enviar um pacote a um destino, a origem inclui o endereço IP do destino no cabeçalho do pacote. Como os endereços postais, este possui uma estrutura hierárquica. Quando um pacote chega a um roteador na rede, este examina uma parte do endereço de destino e o conduz a um roteador adjacente. Mais especificamente, cada roteador possui uma **tabela de encaminhamento** que mapeia os endereços de destino (ou partes deles) para enlaces de saída desse roteador. Quando um pacote chega a um roteador, este examina o endereço e pesquisa sua tabela de encaminhamento, utilizando esse endereço de destino para encontrar o enlace de saída apropriado. O roteador, então, direciona o pacote a esse enlace de saída.

O processo de roteamento fim a fim é semelhante a um motorista que não quer consultar o mapa, prefe- rindo pedir informações. Por exemplo, suponha que Joe vai dirigir da Filadélfia para 156 Lakeside Drive, em Orlando, Flórida. Primeiro, Joe vai ao posto de gasolina de seu bairro e pergunta como chegar a 156 Lakeside Drive, em Orlando, Flórida. O frentista do posto extrai a palavra Flórida do endereço e diz que Joe precisa pegar a interestadual I-95 South, cuja entrada fica ao lado do posto. Ele também diz a Joe para pedir outras informações assim que chegar à Flórida. Então, Joe pega a I-95 South até chegar a Jacksonville, na Flórida, onde pede mais informações a outro frentista. Este extrai a palavra Orlando do endereço a diz a Joe para continuar na I-95 até Daytona Beach, e lá se informar de novo. Em Daytona Beach, outro frentista também extrai a palavra Orlando do endereço e pede para que ele pegue a I-4 diretamente para Orlando. Joe segue suas orientações e chega a uma saída para Orlando. Ele vai até outro posto de gasolina, e dessa vez o frentista extrai a palavra Lakeside Drive do endereço e diz a ele qual estrada seguir para Lakeside Drive. Assim que Joe chega a Lakeside Drive, pergunta a uma criança andando de bicicleta como chegar a seu destino. A criança extrai o número 156 do endereço e aponta para a casa. Joe finalmente chega enfim a seu destino. Nessa analogia, os frentistas de posto de gasolina e as crianças andando de bicicleta são semelhantes aos roteadores.

• REDES DE COMPUTADORES E A INTERNET 20

Vimos que um roteador usa um endereço de destino do pacote para indexar uma tabela de encaminha- mento e determinar o enlace de saída apropriado. Mas essa afirmação traz ainda outra questão: como as tabelas de encaminhamento são montadas? Elas são configuradas manualmente em cada roteador ou a Internet utiliza um procedimento mais automatizado? Essa questão será estudada com mais profundidade no Capítulo 4. Mas, para aguçar seu apetite, observe que a Internet possui uma série de **protocolos de roteamento** especiais, que são utilizados para configurar automaticamente as tabelas de encaminhamento. Um protocolo de roteamento pode, por exemplo, determinar o caminho mais curto de cada roteador a cada destino e utilizar os resultados para con- figurar as tabelas de encaminhamento nos roteadores.

Você gostaria de ver a rota fim a fim que os pacotes realizam na Internet? Nós o convidamos a colocar a mão na massa e interagir com o programa Traceroute, visitando o site <www.traceroute.org>, escolhendo uma origem em um país qualquer e traçando a rota dessa origem até o seu computador. (Para obter detalhes sobre o Traceroute, veja a Seção 1.4.)

1.3.2 Comutação de circuitos

Há duas abordagens fundamentais para locomoção de dados através de uma rede de enlaces e comutadores: **comutação de circuitos** e **comutação de pacotes**. Tendo visto estas últimas na subseção anterior, agora vamos voltar nossa atenção às redes de comutação de circuitos.

Nessas redes, os recursos necessários ao longo de um caminho (buffers, taxa de transmissão de enlaces) para oferecer comunicação entre os sistemas finais são *reservados* pelo período da sessão de comunicação entre os sistemas finais. Em redes de comutação de pacotes, tais recursos *não* são reservados; as mensagens de uma sessão usam os recursos por demanda e, como consequência, poderão ter de esperar (isto é, entrar na fila) para conse- guir acesso a um enlace de comunicação. Como simples analogia, considere dois restaurantes — um que exige e outro que não exige nem aceita reserva. Se quisermos ir ao restaurante que exige reserva, teremos de passar pelo aborrecimento de telefonar antes de sair de casa. Mas, quando chegarmos lá, poderemos, em princípio, ser logo atendidos e servidos. No segundo restaurante, não precisaremos nos dar ao trabalho de reservar mesa, porém, quando lá chegarmos, talvez tenhamos de esperar para sentar.

As redes de telefonia tradicionais são exemplos de redes de comutação de circuitos. Considere o que acon- tece quando uma pessoa quer enviar a outra uma informação (por voz ou por fax) por meio de uma rede tele- fônica. Antes que o remetente possa enviar a informação, a rede precisa estabelecer uma conexão entre ele e o destinatário. Essa é uma conexão forte, na qual os comutadores no caminho entre o remetente e o destinatário mantêm o estado. No jargão da telefonia, essa conexão é denominada **circuito**. Quando a rede estabelece o circui- to, também reserva uma taxa de transmissão constante nos enlaces da rede durante o período da conexão. Visto que foi reservada largura de banda para essa conexão remetente-destinatário, o remetente pode transferir dados ao destinatário a uma taxa constante *garantida*.

A Figura 1.13 ilustra uma rede de comutação de circuitos. Nela, os quatro comutadores de circuitos estão inter- conectados por quatro enlaces. Cada enlace tem quatro circuitos, de modo que cada um pode suportar quatro cone- xões simultâneas. Cada um dos hospedeiros (por exemplo, PCs e estações de trabalho) está conectado diretamente a um dos circuitos. Quando dois sistemas finais querem se comunicar, a rede estabelece uma **conexão fim a fim** dedi- cada entre os dois hospedeiros. Assim, para que o sistema final A envie mensagens ao sistema final B, a rede deve pri- meiro reservar um circuito em cada um dos dois enlaces. Neste exemplo, a conexão fim a fim dedicada usa o segundo circuito no primeiro enlace e o quarto circuito no segundo enlace. Como cada enlace tem quatro circuitos, para cada enlace usado pela conexão fim a fim, esta fica com um quarto da capacidade de transmissão total durante o período da conexão. Assim, por exemplo, se cada enlace entre comutadores adjacentes tiver uma taxa de transmissão de 1 Mbit/s, então cada conexão de comutação de circuitos fim a fim obtém 250 kbits/s de taxa de transmissão dedicada. Ao contrário, considere o que ocorre quando um sistema final quer enviar um pacote a outro hospedeiro por uma rede de comutação de pacotes, como a Internet. Como acontece na comutação de circuitos, o pacote é transmitido por uma série de enlaces de comunicação. Mas, na comutação de pacotes, ele é enviado à rede sem reservar qualquer

REDES DE COMPUTADORES E A INTERNET • 21

FIGURA 1.13 UMA REDE SIMPLES DE COMUTAÇÃO DE CIRCUITOS COMPOSTA DE QUATRO COMUTADORES E

QUATRO ENLACES

recurso do enlace. Se um dos enlaces estiver congestionado porque outros pacotes precisam ser transmitidos ao mes- mo tempo, então nosso pacote terá de esperar em um buffer na extremidade de origem do enlace de transmissão e sofrerá um atraso. A Internet faz o melhor esforço para entregar os dados de pronto, mas não dá garantia alguma.

**Multiplexação em redes de comutação de circuitos**

Um circuito é implementado em um enlace por **multiplexação por divisão de frequência** (*frequency-di- vision multiplexing* — FDM) ou por **multiplexação por divisão de tempo** (*time-division multiplexing* — TDM). Com FDM, o espectro de frequência de um enlace é compartilhado entre as conexões estabelecidas através desse enlace. Ou seja, o enlace reserva uma banda de frequência para cada conexão durante o período da ligação. Em redes telefônicas, a largura dessa banda de frequência em geral é 4 kHz (isto é, 4 mil Hertz ou 4 mil ciclos por segundo). A largura da banda é denominada, claro, **largura de banda**. Estações de rádio FM também usam FDM para compartilhar o espectro de frequência entre 88 MHz e 108 MHz, sendo atribuída para cada estação uma banda de frequência específica.

Em um enlace TDM, o tempo é dividido em quadros de duração fixa, e cada quadro é dividido em um número fixo de compartimentos (*slots*). Quando estabelece uma conexão por meio de um enlace, a rede dedica à conexão um compartimento de tempo em cada quadro. Esses compartimentos são reservados para o uso exclusivo dessa conexão, e um dos compartimentos de tempo (em cada quadro) fica disponível para transmitir os dados dela.

A Figura 1.14 ilustra as técnicas FDM e TDM para um enlace de rede que suporta até quatro circuitos. Para FDM, o domínio de frequência é segmentado em quatro faixas, com largura de banda de 4 kHz cada. Para TDM, o domínio de tempo é segmentado em quadros, cada um com quatro compartimentos de tempo; a cada circuito é designado o mesmo compartimento dedicado nos quadros sucessivos TDM. Para TDM, a taxa de transmissão de um circuito é igual à taxa do quadro multiplicada pelo número de bits em um compartimento. Por exemplo, se o enlace transmite 8 mil quadros por segundo e cada compartimento consiste em 8 bits, então a taxa de trans- missão de um circuito é 64 kbits/s.

Os defensores da comutação de pacotes sempre argumentaram que comutação de circuitos é desperdí- cio, porque os circuitos dedicados ficam ociosos durante **períodos de silêncio**. Por exemplo, quando um dos participantes de uma conversa telefônica para de falar, os recursos ociosos da rede (bandas de frequências ou compartimentos nos enlaces ao longo da rota da conexão) não podem ser usados por outras conexões em curso. Para outro exemplo de como esses recursos podem ser subutilizados, considere um radiologista que usa uma rede de comutação de circuitos para acessar remotamente uma série de exames. Ele estabelece uma conexão, requisita uma imagem, examina-a e, em seguida, solicita uma nova. Recursos de rede são atribuídos à conexão, mas não utilizados (isto é, são desperdiçados) no período em que o radiologista examina a imagem. Defensores

• 22REDES DE COMPUTADORES E A INTERNET FIGURA 1.14 COM FDM, CADA CIRCUITO DISPõE CONTINUAMENTE DE UMA FRAÇÃO DA LARGURA DE

BANDA. COM TDM, CADA CIRCUITO DISPõE DE TODA A LARGURA DE BANDA PERIODICAMENTE, DURANTE BREVES INTERVALOS DE TEMPO (ISTO É, DURANTE COMPARTIMENTOS DE TEMPO)

FDM

4KHz

Enlace Frequência

4KHz

TDM

12 3 4 1 2 3 4 1 2 3 4 1 2 3 4

Compartimento

Quadro

Tempo Legenda:

Todos os compartimentos 2

de número “2” são dedicados a um par transmissor/receptor específico.

da comutação de pacotes também gostam de destacar que estabelecer circuitos e reservar larguras de banda fim a fim é complicado e exige softwares complexos de sinalização para coordenar a operação dos comutadores ao longo do caminho.

Antes de encerrarmos esta discussão sobre comutação de circuitos, examinaremos um exemplo numérico que deverá esclarecer melhor o assunto. Vamos considerar o tempo que levamos para enviar um arquivo de 640 kbits/s do hospedeiro A ao hospedeiro B por uma rede de comutação de circuitos. Suponha que todos os enlaces da rede usem TDM de 24 compartimentos e tenham uma taxa de 1,536 Mbits/s. Suponha também que um circuito fim a fim leva 500 milissegundos para ser ativado antes que A possa começar a transmitir o arquivo. Em quanto tempo o arquivo será enviado? Cada circuito tem uma taxa de transmissão de (1,536 Mbits/s)/24 = 64 kbits/s; portanto, demorará (640 kbits/s)/(64 kbits/s) = 10 segundos para transmitir o arquivo. A esses 10 segundos adicionamos o tempo de ativação do circuito, resultando 10,5 segundos para o envio. Observe que o tempo de transmissão é in- dependente do número de enlaces: o tempo de transmissão seria 10 segundos se o circuito fim a fim passasse por um ou por uma centena de enlaces. (O atraso real fim a fim também inclui um atraso de propagação; ver Seção 1.4.)

**Comutação de pacotes *versus* comutação de circuitos**

Agora que já descrevemos comutação de pacotes e comutação de circuitos, vamos comparar as duas. Opo- sitores da comutação de pacotes costumam argumentar que ela não é adequada para serviços de tempo real (por exemplo, ligações telefônicas e videoconferência) por causa de seus atrasos fim a fim variáveis e imprevisíveis (que se devem principalmente a variáveis e imprevisíveis atrasos de fila). Defensores da comutação de pacotes argumentam que (1) ela oferece melhor compartilhamento de banda do que comutação de circuitos e (2) sua implementação é mais simples, mais eficiente e mais barata do que a de comutação de circuitos. Uma discussão interessante sobre comutação de pacotes e comutação de circuitos pode ser encontrada em Molinero-Fernandez [2002]. De modo geral, quem não gosta de perder tempo fazendo reserva de mesa em restaurantes prefere comu- tação de pacotes à comutação de circuitos.

Por que a comutação de pacotes é mais eficiente? Vamos examinar um exemplo simples. Suponha que usuá- rios compartilhem um enlace de 1 Mbit/s. Considere também que cada usuário alterne períodos de atividade, quando gera dados a uma taxa constante de 100 kbits/s, e de inatividade, quando não gera dados. Imagine ainda

REDES DE COMPUTADORES E A INTERNET • 23

que o usuário esteja ativo apenas 10% do tempo (e fique ocioso, tomando cafezinho, durante os restantes 90%). Com comutação de circuitos, devem ser *reservados* 100 kbits/s para *cada usuário* durante todo o tempo. Por exemplo, com TDM, se um quadro de um segundo for dividido em 10 compartimentos de tempo de 100 milisse- gundos cada, então seria alocado um compartimento de tempo por quadro a cada usuário.

Desse modo, o enlace de comutação de circuitos pode suportar somente 10 (= 1 Mbit/s/100 kbits/s) usuá- rios simultaneamente. Com a comutação de pacotes, a probabilidade de haver um usuário específico ativo é 0,1 (isto é, 10%). Se houver 35 usuários, a probabilidade de haver 11 ou mais usuários ativos ao mesmo tempo é de mais ou menos 0,0004. (O Problema P8 dos Exercícios de Fixação demonstra como essa probabilidade é calcu- lada.) Quando houver dez ou menos usuários ativos simultâneos (a probabilidade de isso acontecer é 0,9996), a taxa agregada de chegada de dados é menor ou igual a 1 Mbit/s, que é a taxa de saída do enlace. Assim, quando houver dez ou menos usuários ativos, pacotes de usuários fluirão pelo enlace essencialmente sem atraso, como é o caso na comutação de circuitos. Quando houver mais de dez usuários ativos ao mesmo tempo, a taxa agregada de chegada de pacotes excederá a capacidade de saída do enlace, e a fila de saída começará a crescer. (E continua- rá a crescer até que a velocidade agregada de entrada caia novamente para menos de 1 Mbit/s, ponto em que o comprimento da fila começará a diminuir.) Como a probabilidade de haver mais de dez usuários ativos é ínfima nesse exemplo, a comutação de pacotes apresenta, em essência, o mesmo desempenho da comutação de circuitos, *mas o faz para mais de três vezes o número de usuários.*

Vamos considerar agora um segundo exemplo simples. Suponha que haja dez usuários e que um deles de repente gere mil pacotes de mil bits, enquanto os outros nove permanecem inativos e não geram pacotes. Com comutação de circuitos TDM de dez compartimentos de tempo por quadro, e cada quadro consistindo em mil bits, o usuário ativo poderá usar somente seu único compartimento por quadro para transmitir dados, enquanto os nove compartimentos restantes em cada quadro continuarão ociosos. Dez segundos se passarão antes que todo o milhão de bits de dados do usuário ativo seja transmitido. No caso da comutação de pacotes, o usuário ativo poderá enviá-los continuamente à taxa total de 1 Mbit/s, visto que não haverá outros gerando pacotes que precisem ser multiplexados com os dele. Nesse caso, todos os dados do usuário ativo serão transmitidos dentro de 1 segundo.

Os exemplos citados ilustram duas maneiras pelas quais o desempenho da comutação de pacotes pode ser superior à da comutação de circuitos. Também destacam a diferença crucial entre as duas formas de comparti- lhar a taxa de transmissão de um enlace entre vários fluxos de bits. A comutação de circuitos aloca previamente a utilização do enlace de transmissão independentemente da demanda, com desperdício de tempo de enlace desnecessário alocado e não utilizado. A comutação de pacotes, por outro lado, aloca utilização de enlace *por demanda*. A capacidade de transmissão do enlace será compartilhada pacote por pacote somente entre usuários que tenham pacotes que precisam ser transmitidos pelo enlace.

Embora tanto a comutação de pacotes quanto a de circuitos predominem nas redes de telecomunicação de hoje, a tendência é, sem dúvida, a comutação de pacotes. Até mesmo muitas das atuais redes de telefonia de comutação de circuitos estão migrando aos poucos para a comutação de pacotes. Em especial, redes telefônicas usam comutação de pacotes na parte cara de uma chamada telefônica para o exterior.

1.3.3 Uma rede de redes

Vimos anteriormente que sistemas finais (PCs, smartphones, servidores Web, servidores de correio eletrô- nico e assim por diante) conectam-se à Internet por meio de um provedor local (ISP). Este pode fornecer uma conectividade tanto com ou sem fio, utilizando diversas tecnologias de acesso, que incluem DSL, cabo, FTTH, Wi-Fi e telefone celular. Observe que o provedor local não precisa ser uma operadora de telefonia ou uma empre- sa de TV a cabo: pode ser, por exemplo, uma universidade (que oferece acesso à Internet para os alunos, os fun- cionários e o corpo docente) ou uma empresa (que oferece acesso para seus funcionários). Mas conectar usuários finais e provedores de conteúdo a um provedor de acesso (ISP) é apenas uma pequena peça do quebra-cabeça

• REDES DE COMPUTADORES E A INTERNET 24que é interligar os bilhões de sistemas finais que compõem a Internet. Isso é feito criando uma *rede de redes* —

entender essa frase é a chave para entender a Internet.

Com o passar dos anos, a rede de redes que forma a Internet evoluiu para uma estrutura bastante complexa. Grande parte dessa evolução é controlada pela política econômica e nacional, e não por considerações de desem- penho. Para entender a estrutura de rede da Internet de hoje, vamos criar, de modo incremental, uma série de estruturas de rede, com cada nova estrutura sendo uma aproximação melhor da Internet complexa que temos. Lembre-se de que o objetivo dominante é interconectar os provedores de acesso de modo que todos os sistemas finais possam enviar pacotes entre si. Um método ingênuo seria fazer que cada ISP se conectasse *diretamente* a cada outro ISP. Esse projeto em malha, é evidente, seria muito caro para os ISPs, pois exigiria que cada ISP tivesse um enlace de comunicação separado para as centenas de milhares de outros ISPs do mundo inteiro.

Nossa primeira estrutura de rede, a *Estrutura de Rede 1*, interconecta todos os ISPs de acesso a um único *ISP de trânsito global*. Nosso (imaginário) ISP de trânsito global é uma rede de roteadores e enlaces de comunicação que não apenas se espalha pelo planeta, mas também tem pelo menos um roteador próximo de cada uma das centenas de milhares de ISPs de acesso. Claro, seria muito dispendioso para o ISP global montar essa rede tão extensa. Para que seja lucrativo, ele naturalmente cobraria de cada um dos ISPs de acesso pela conectividade, com o preço refletindo (mas nem sempre diretamente proporcional à) a quantidade de tráfego que um ISP de acesso troca com o ISP global. Como o ISP de acesso paga ao ISP de trânsito global, ele é considerado um **cliente**, e o ISP de trânsito global é considerado um **provedor**.

Agora, se alguma empresa montar e operar um ISP de trânsito global que seja lucrativo, então será natural para outras empresas montarem seus próprios ISPs de trânsito global e competirem com o original. Isso leva à *Estrutura de Rede 2*, que consiste em centenas de milhares de ISPs de acesso e *múltiplos* ISPs de trânsito global. Os ISPs de acesso decerto preferem a Estrutura de Rede 2 à Estrutura de Rede 1, pois agora podem escolher entre os provedores de trânsito global concorrentes comparando seus preços e serviços. Note, porém, que os próprios ISPs de trânsito global precisam se interconectar: caso contrário, os ISPs de acesso conectados a um dos provedores de trânsito glo- bal não poderiam se comunicar com os ISPs de acesso conectados aos outros provedores de trânsito global.

A Estrutura de Rede 2, que acabamos de descrever, é uma hierarquia de duas camadas com provedores de trânsito global residindo no nível superior e os ISPs de acesso no nível inferior. Isso considera que os ISPs de trânsito global não são capazes de chegar perto de todo e qualquer ISP de acesso, mas também consideram economicamente desejável fazer isso. Na realidade, embora alguns ISPs tenham uma cobertura global impressio- nante e se conectem diretamente com muitos ISPs de acesso, nenhum tem presença em toda e qualquer cidade do mundo. Em vez disso, em determinada região, pode haver um **ISP regional** ao qual os ISPs de acesso na região se conectam. Cada ISP regional, então, se conecta a **ISPs de nível 1**. Estes são semelhantes ao nosso (imaginário) ISP de trânsito global; mas os ISPs de nível 1, que realmente existem, não têm uma presença em cada cidade do mundo. Existe mais ou menos uma dúzia de ISPs de nível 1, incluindo Level 3 Communications, AT&T, Sprint e NTT. É interessante que nenhum grupo sanciona oficialmente o *status* de nível 1; como diz o ditado — se você tiver que perguntar se é membro de um grupo, provavelmente não é.

Retornando a essa rede de redes, não apenas existem vários ISPs de nível 1 concorrentes, mas pode haver múltiplos ISPs regionais concorrentes em uma região. Em tal hierarquia, cada ISP de acesso paga ao regional ao qual se conecta, e cada ISP regional paga ao ISP de nível 1 ao qual se interliga. (Um ISP de acesso também pode se conectar diretamente a um ISP de nível 1, quando pagará ao ISP de nível 1.) Assim, existe uma relação cliente -provedor em cada nível da hierarquia. Observe que os ISPs de nível 1 não pagam a ninguém, pois estão no topo. Para complicar as coisas ainda mais, em algumas regiões pode haver um ISP regional maior (talvez se espalhando por um país inteiro) ao qual os ISPs regionais menores nessa região se conectam; o ISP regional maior, então, se conecta a um ISP de nível 1. Por exemplo, na China existem ISPs de acesso em cada cidade, que se conectam a ISPs provinciais, que por sua vez se ligam a ISPs nacionais, que por fim se interligam a ISPs de nível 1 [Tian, 2012]. Chamamos a essa hierarquia multinível, que ainda é apenas uma aproximação bruta da Internet de hoje, *Estrutura de Rede 3*.

REDES DE COMPUTADORES E A INTERNET • 25

Para montar uma rede que se assemelhe mais à Internet de hoje, temos que acrescentar pontos de presença (PoPs — Points of Presence), *multi-homing*, emparelhamento e pontos de troca da Internet (IXPs — Internet eXchange Points) à Estrutura de Rede 3. Existem PoPs em todos os níveis da hierarquia, exceto para o nível de baixo (ISP de acesso). Um **PoP** é simplesmente um grupo de um ou mais roteadores (no mesmo local) na rede do provedor, onde os ISPs clientes podem se conectar no ISP provedor. Para que uma rede do cliente se conecte ao PoP de um provedor, ele pode alugar um enlace de alta velocidade de um provedor de telecomunicações de ter- ceiros para conectar diretamente um de seus roteadores a um roteador no PoP. Qualquer ISP (exceto os de nível 1) pode decidir efetuar o ***multi-home***, ou seja, conectar-se a dois ou mais ISPs provedores. Assim, por exemplo, um ISP de acesso pode efetuar *multi-home* com dois ISPs regionais, ou então com dois ISPs regionais e também com um ISP de nível 1. De modo semelhante, um ISP regional pode efetuar *multi-home* com vários ISPs de nível 1. Quando um ISP efetua *multi-home*, ele pode continuar a enviar e receber pacotes na Internet, mesmo que um de seus provedores apresente uma falha.

Como vimos, os ISPs clientes pagam aos seus ISPs provedores para obter interconectividade global com a Internet. O valor que um ISP cliente paga a um ISP provedor reflete a quantidade de tráfego que ele troca com o provedor. Para reduzir esses custos, um par de ISPs próximos no mesmo nível da hierarquia pode **emparelhar**, ou seja, conectar diretamente suas redes, de modo que todo o tráfego entre elas passe pela conexão direta, em vez de passar por intermediários mais à frente. Quando dois ISPs são emparelhados, isso em geral é feito em acordo, ou seja, nenhum ISP paga ao outro. Como já dissemos, os ISPs de nível 1 também são emparelhados uns com os ou- tros, sem taxas. Para ver uma discussão legível sobre emparelhamento e relações cliente-provedor, consulte Van der Berg [2008]. Nesses mesmos termos, uma empresa de terceiros pode criar um **ponto de troca da Internet (IXP** — **Internet Exchange Point)** — quase sempre em um prédio isolado com seus próprios comutadores —, que é um ponto de encontro onde vários ISPs podem se emparelhar. Existem cerca de 300 IXPs na Internet hoje [Augustin, 2009]. Referimo-nos a esse ecossistema — consistindo em ISPs de acesso, ISPs regionais, ISPs de nível 1, PoPs, *multi-homing*, emparelhamento e IXPs — como *Estrutura de Rede 4*.

Agora, chegamos finalmente na *Estrutura de Rede 5*, que descreve a Internet de 2012. Essa estrutura, ilustrada na Figura 1.15, se baseia no topo da Estrutura de Rede 4 acrescentando **redes de provedor de conteúdo**. A Google é um dos principais exemplos dessa rede de provedor de conteúdo. No momento, estima-se que tenha de 30 a 50 cen- tros de dados distribuídos na América do Norte, Europa, Ásia, América do Sul e Austrália. Alguns desses centros de dados acomodam mais de cem mil servidores, enquanto outros são menores, acomodando apenas centenas de servi- dores. Os centros de dados da Google são todos interconectados por meio de uma rede TCP/IP privativa, que se es- palha pelo mundo inteiro, mas apesar disso é separada da Internet pública. O importante é que essa rede privada só transporta tráfego de/para servidores da Google. Como vemos na Figura 1.15, a rede privativa da Google tenta “con- tornar” as camadas mais altas da Internet emparelhando (sem custo) com outros ISPs de nível mais baixo, seja conec- tando diretamente ou interligando com eles em IXPs [Labovitz, 2010]. Entretanto, como muitos ISPs de acesso ainda

FIGURA 1.15 INTERCONEXÃO DE ISPs

ISP de

ISP de

Provedor de conteúdo nível 1

nível 1

(p.ex., Google)

IXP

IXP IXP

ISP

ISP regional

regional

ISP de acesso

ISP de acesso

ISP de acesso

ISP de acesso

ISP de acesso

ISP de acesso

ISP de acesso

ISP de acesso

• REDES DE COMPUTADORES E A INTERNET 26só podem ser alcançados transitando por redes de nível 1, a rede da Google também se conecta a ISPs de nível 1 e paga a esses ISPs pelo tráfego que troca com eles. Criando sua própria rede, um provedor de conteúdo não apenas reduz seus pagamentos aos ISPs da camada mais alta, mas também tem maior controle de como seus serviços por fim são entregues aos usuários finais. A infraestrutura de rede da Google é descrita com mais detalhes na Seção 7.2.4.

Resumindo, a topologia da Internet é complexa, consistindo em uma dúzia ou mais de ISPs de nível 1 e cen- tenas de 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 geográficas. Os ISPs de níveis mais baixos conectam-se a ISPs de níveis mais altos e estes 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. Nos últimos anos, os principais provedores de conteúdo também têm criado suas próprias redes e se conectam diretamente a ISPs de níveis mais baixos, quando possível.

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 aplica- ções 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, de modo instantâneo, sem nenhuma perda. É uma pena, mas esse é um objetivo muito elevado, algo inalcançável. Em vez disso, as redes de compu- tadores, 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, como as redes de computadores têm esses problemas, existem muitas questões fascinantes sobre como lidar com eles — ques- tões mais do que suficientes para preencher um curso de redes de computadores e motivar milhares 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 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. Os mais importantes deles são o **atraso de processamento nodal**, o **atraso de fila**, o **atraso de trans- missão** e o **atraso de propagação**; juntos, eles se acumulam para formar o **atraso nodal total**. O desempenho de muitas aplicações da Internet — como busca, navegação Web, e-mail, mapas, mensagens instantâneas e voz sobre IP — é bastante afetado por atrasos na rede. Para entender a fundo a comutação de pacotes e redes de computa- dores, 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 prece- dido 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 transmiti- do por um enlace apenas se não houver nenhum outro sendo transmitido por ele e se não houver outros à sua frente na fila. Se o enlace estiver ocupado, ou com pacotes à espera, o recém-chegado entrará na fila.

REDES DE COMPUTADORES E A INTERNET • 27

FIGURA 1.16 O ATRASO NODAL NO ROTEADOR A

A

B

Processamento nodal

Propagação

**Atraso de processamento**

O tempo exigido 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 rotea dores de alta velocidade em geral são da ordem de microssegundos, ou menos. Depois desse processamento nodal, o roteador direciona o pacote à fila que precede o enlace com o rotea- dor 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 dependerá da quantidade de outros pacotes que chegarem antes e que já estiverem na fila esperando pela trans- missão no enlace. Se a fila estiver vazia, e nenhum outro pacote estiver sendo transmitido naquele momento, en- tão o tempo de fila de nosso pacote será zero. Por outro lado, se o tráfego estiver intenso 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 intensidade 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 pri- meiro a ser processado”, como é comum em redes de comutação de pacotes, o nosso somente poderá ser transmitido depois de todos os que chegaram antes terem 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. Por exemplo, para um enlace Ethernet de 10 Mbits/s, a velocidade é *R* = 10 Mbits/s; para um enlace Ethernet de 100 Mbits/s, a velocidade é *R* = 100 Mbits/s. O **atraso de transmissão** é *L*/*R*. Esta é a quantidade de tempo exigida para empurrar (isto é, transmitir) todos os bits do pacote para o enlace. Na prática, atrasos de trans- missão costumam ser 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 pro- pagar 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 (isto é, fibra ótica, par de fios de cobre trançado e assim por diante) e está na faixa de

2 ∙ 108 m/s a 3 ∙ 108 m/s

Fila

Transmissão (esperando por transmissão)

• 28REDES DE COMPUTADORES E A INTERNET que é igual à velocidade da luz. O atraso de propagação é a distância entre dois roteadores dividida pela velocidade de propagação. Isto é, o atraso de propagação é *d*/*s*, sendo *d* a distância entre o roteador A e o roteador B, e *s* 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 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 têm dificuldade para entender a diferença entre atrasos de transmissão e de propagação. Ela é sutil, mas importante. O atraso de transmissão é a quantidade de tempo necessária 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 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 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. Con- sidere 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 trafeguem (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 velo- cidade entre os dois postos de pedágio). Agora, considere 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, imagine 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 carros)/(5 carros/minuto) = 2 minutos, semelhante ao atraso de transmissão em um roteador. O tempo necessário para um carro trafegar da saída de um posto de pedágio até o próximo é de (100 km)/(100 km/h) = 1 hora, semelhante 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 momento 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 trafegar entre dois postos? Por exemplo, su- ponha que os carros trafeguem a uma velocidade de 1.000 km/h e que o pedágio libere um carro por minuto. En- tão, 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.

FIGURA 1.17 ANALOGIA DO COMBOIO

Comboio de dez carros

100 km 100 km

Pedágio Pedágio

REDES DE COMPUTADORES E A INTERNET • 29

Se uma imagem vale mil palavras, então uma animação vale um milhão. O site de apoio deste livro apresen- ta um aplicativo interativo Java que ilustra e compara o atraso de transmissão com o de propagação. Recomenda- -se que o leitor visite esse aplicativo. Smith [2009] também oferece uma discussão bastante legível sobre atrasos de propagação, fila e transmissão.

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*nodal = *d*proc + *d*fila + *d*trans + *d*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*nodal. De maneira semelhante, *d*trans pode variar de des- prezível a significativo. Sua contribuição costuma ser desprezível para velocidades de transmissão de 10 Mbits/s 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 velo- cidade 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. Na verdade, 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!). Diferente 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 de fila, ao passo que o último sofrerá um relativamente grande (enquanto espera que os outros nove sejam transmitidos). Por conseguinte, para se caracterizar um atraso de fila, são utilizadas em geral medições estatísticas, tais como atraso de fila médio, variância do atraso de fila e a probabilidade de que ele exceda um valor especificado.

Quando o atraso de fila é grande e quando é insignificante? A resposta a essa pergunta depende da velo- cidade de transmissão do enlace, da taxa com que o tráfego chega à fila e de sua natureza, isto é, se de modo intermitente, 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 fim, imagine que a fila seja muito longa, de modo que possa conter um número infinito de bits. A razão *La*/*R*, denominada **intensidade de tráfe- go**, costuma desempenhar 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 aquela 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* ≤ 1. Aqui, a natureza do tráfego influencia o atraso de fila. Por exem- plo, 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 chegarem em rajadas, mas periodicamen- te, 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 terá

• 30REDES DE COMPUTADORES E A INTERNET um atraso 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. Em geral, o processo de chegada a uma fila é *aleatório* — isto é, não segue um padrão e os intervalos de tempo entre os paco- tes são ao acaso. Nessa hipótese mais realista, a quantidade *La*/*R* quase sempre 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 in- tervalos de tempo em que a velocidade de chegada excederá a capacidade de transmissão (por causa das variações na taxa de chegada do pacote) e uma fila será formada durante esses períodos; 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 depressa. Uma pequena porcentagem de aumento na intensidade resulta em 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 costuma ser congestionada, o fato de ela estar sempre assim significa que a intensidade de tráfego é próxima de 1. Se algum evento causar um tráfego um pouco maior do que o normal, as demoras que você sofrerá poderão ser enormes.

Para compreender um pouco mais os atrasos de fila, visite o site de apoio do livro, que apresenta um apli- cativo Java interativo para uma fila. Se você aumentar a taxa de chegada do pacote o suficiente de forma que a intensidade do tráfego exceda 1, verá a fila aumentar ao longo do tempo.

**Perda de pacotes**

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 quan- do a intensidade de tráfego se aproxima de 1. O que acontece de fato é que um pacote pode chegar e encontrar uma fila cheia. Sem espaço disponível para armazená-lo, o roteador o **descartará**; 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

FIGURA 1.18 DEPENDêNCIA ENTRE ATRASO DE FILA MÉDIO E INTENSIDADE DE TRÁFEGO

*La*/*R* 1

REDES DE COMPUTADORES E A INTERNET • 31

o aumento da intensidade de tráfego. Por conseguinte, o desempenho em um nó costuma ser medido não ape- nas em termos de atraso, mas também da probabilidade de perda de pacotes. Como discutiremos nos capítulos subsequentes, um pacote perdido pode ser retransmitido fim a fim para garantir que todos os dados sejam trans- feridos da origem ao local de destino.

1.4.3 Atraso fim a fim

Até o momento, nossa discussão focalizou o atraso nodal, isto é, 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 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 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) (1.2)

em que, mais uma vez, *d*trans = *L*/*R* e *L* é o tamanho do pacote. Note que a Equação 1.2 é uma generalização da Equação 1.1, na qual não levamos em conta os atrasos de processamento e propagação. Convidamos você a generalizar a Equação 1.2 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 de fato o atraso em uma rede de computadores, podemos utilizar o Traceroute, pro- grama de diagnóstico que pode ser executado em qualquer hospedeiro da Internet. Quando o usuário especifica um nome de hospedeiro de destino, o programa no hospedeiro de origem envia vários pacotes especiais em dire- ção 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 à origem uma curta mensagem, contendo 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 hos- pedeiro 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 ori- gem 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 realidade, o programa Traceroute repete o processo que acabamos de descrever três vezes, de modo que a fonte envia, na verdade, *3 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 é o valor *n* descrito, isto é, o número do roteador ao longo da rota; a se- gunda é o nome do roteador; a terceira é o endereço do roteador (na forma xxx.xxx.xxx.xxx); as últimas três são os atrasos de ida e volta para três tentativas. Se a fonte receber menos do que três mensagens de qualquer roteador determinado (por causa da 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 ida e volta para aquele roteador.

• REDES DE COMPUTADORES E A INTERNET 321 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 acr1-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 to- dos têm endereços. 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 ele, verificamos que, na primeira das três tentativas, o atraso de ida e volta entre a origem e o roteador foi de 1,03 ms. Os atrasos de ida e volta para as duas tentativas subsequentes foram 0,48 e 0,45 ms, e incluem todos os atrasos que acabamos de discutir, ou seja, 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 anterior: os atrasos do roteador 6 são maiores que os do roteador 7!

Você quer experimentar o Traceroute por conta própria? Recomendamos *muito* que visite o site <http:// www. traceroute.org>, que oferece 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, 2012].

**Sistema final, aplicativo e outros atrasos**

Além dos atrasos de processamento, transmissão e de propagação, os sistemas finais podem adicionar outros atrasos significativos. Por exemplo, um sistema final que quer transmitir um pacote para uma mídia compartilha- da (por exemplo, como em um cenário Wi-Fi ou modem a cabo) pode, *intencionalmente*, atrasar sua transmissão como parte de seu protocolo por compartilhar a mídia com outros sistemas finais; vamos analisar tais protocolos em detalhes no Capítulo 5. 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. Esse tempo para carregar um pacote — chamado de atraso de empacotamento — pode ser significativo 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 por uma rede de computadores. Essa transferência pode ser, por exemplo, um videoclipe extenso de um parceiro para outro por meio do sistema de compartilhamento de arquivos P2P. A **vazão instantânea** a qual- quer momento é a taxa (em bits/s) em que o hospedeiro B está recebendo o arquivo. (Muitos aplicativos, incluin- do 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* segun- dos para o hospedeiro B receber todos os *F* bits, então a **vazão média** da transferência do arquivo é *F/T* bits/s.

REDES DE COMPUTADORES E A INTERNET • 33

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 kbits/s para aplicações de telefonia via Internet, e superior a 256 kbits/s para algumas aplicações 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 do importante conceito de vazão, 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. seja a taxa do enlace entre o servidor e o que os únicos bits enviados na rede inteira roteador; sejam os e do *Rc* servidor seja a taxa para do o enlace cliente. entre Agora o roteador vem e o Suponha que cliente. Imagine *Rs* a pergunta: nesse cená- rio ideal, qual é a vazão servidor-para-cliente? Para responder, pense nos bits como um *líquido* e nos enlaces de comunicação como *tubo.* Claro, o servidor não pode enviar os bits através de seu enlace a uma taxa mais rápida do então que os *Rs* bits bits/s; enviados e o roteador pelo não pode encaminhar os bits a uma taxa mais rápida servidor “fluirão” diretamente pelo roteador e chegarão do ao que cliente *Rc* bits/s. a uma bits/s, gerando uma vazão tão rápido quanto ele os recebe. de *Rs* bits/s. Neste Se, caso, por os outro bits somente lado, *Rc* < deixarão *Rs*, então o o roteador roteador a não poderá uma taxa fim a fim de uma das vezes, taxa *R*indesejável!) *c*, transmissão *R*o *c*. acúmulo (Observe do **enlace** também que se os bits continuarem a chegar no roteador a uma de bits esperando para transmissão ao cliente só aumentará — uma Assim, para essa **de gargalo**. Após rede simples de dois enlaces, a determinar a vazão, agora podemos vazão é aproximar mín{*Rc*, encaminhar Se taxa *R*os *s* de < bits *RRc*, s taxa *Rc*, situação, dando *Rs*, uma vazão e a deixá-lo a na maioria *R*o *s*}, tempo ou seja, é a que leva taxa de para transferir um arquivo grande de *F* bits do suponha que você está fazendo o *download* servidor ao de um arquivo cliente como *F*/mín{*R*MP3 de *F* = 32 milhões *s*, *Rc*,}. Para um exemplo específico, de bits, o servidor tem uma taxa de transmissão transferir o arquivo é, de então, *Rs* = 2 32 Mbits/s, segundos. e você Claro tem que um essas enlace expressões de acesso para de *R*tempo *c* = 1 Mbit/s. de vazão O tempo e de transferência necessário para são apenas aproximações, já que elas não consideram os atrasos para armazenar-e-reenviar e de processamento, bem como assuntos relacionados a protocolos.

A Figura 1.19(b) agora mostra uma rede com *N* enlaces entre o servidor e o cliente, com as taxas de trans- missão transferência *R*1, *R*2, de ..., arquivo *RN*. Aplicando a mesma análise da rede de dois enlaces, descobrimos que a vazão para do servidor ao cliente enlace de gargalo ao longo do caminho entre o uma é servidor mín{*R*1, e *R*o 2, cliente.

..., *RN*}, a qual é novamente a taxa de transmissão do

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 transfe- rência de arquivo do servidor ao cliente. O servidor está conectado o cliente está conectado à rede com um enlace de acesso de da rede de comunicação tenham taxas de transmissão muito *R*altas, *c*. à rede com um enlace Agora suponha que todos de os acesso enlaces de no taxa núcleo *Rs* e

muito maiores do que *Rs* e *Rc*. De fato, hoje, o

FIGURA 1.19 VAZÃO PARA UMA TRANSFERêNCIA DE ARQUIVO DO SERVIDOR AO CLIENTE

Servidor

*Rs*

*Rc*

Cliente a.*R*1 *R*2 *RN*

Servidor b.

Cliente

• 34REDES DE COMPUTADORES E A INTERNET FIGURA 1.20 VAZÃO FIM A FIM: (A) O CLIENTE BAIXA UM ARQUIVO DO SERVIDOR; (B) 10 CLIENTES FAZEM O

*DOWNLOAD* COM 10 SERVIDORES

núcleo da Internet está superabastecido com enlaces de alta velocidade que sofrem pouco congestionamento. Su- ponha, 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 tubo largo neste exemplo, a taxa a qual os bits correm da origem ao destino é novamente o mínimo vazão na Internet de hoje é, em geral, a rede de de *Rs* acesso.

e *Rc*, ou seja, vazão = mín{*Rs*, *Rc*}. Portanto, o fator restritivo para

Para um exemplo final, considere a Figura 1.20(b), na qual existem dez servidores e dez clientes conectados ao núcleo da rede de computadores. Nesse exemplo, dez *downloads* simultâneos estão sendo realizados, envolven- do dez pares cliente-servidor. Suponha que esses *downloads* sejam o único tráfego na rede no momento. Como mostrado na figura, há um enlace no núcleo que é atravessado por todos os dez *downloads*. Considere *R* a taxa de transmissão desse enlace. Imagine os enlaces de acesso do cliente possuem — com exceção de um enlace comum quais são as vazões de *download*? É que todos os enlaces de acesso do servidor de a taxa mesma *R* — taxa sejam *Rc* muito e a taxa de transmissão maiores do que claro que se a taxa do enlace comum, *R*, possuem de a mesma todos os enlaces taxa no *Rs*núcleo , todos

é *R*grande *s*, *Rc* e *R*. Agora perguntamos: — digamos, cem vezes maior mesma que tre 10 *Rs downloads*. do = ordem 2 que Mbits/s, *Rs* que e *R*Então, *Rc R*—, *c s* = e então a vazão 1 *R*Mbit/s, *c*? Qual será *R* = o gargalo para para cada *download* será novamente mín{*R*a vazão nesse caso? Vamos observar um 5 Mbits/s, e o enlace comum divide sua taxa cada *download* não se encontra mais na Servidor *RsRc*

a. b.

exemplo *s*, *Rc*}. Mas específico. e se essa taxa Suponha for da

de transmissão por igual en- rede de acesso, mas é o enlace compartilhado no núcleo, que somente fornece para cada *download* 500 kbits/s de vazão. Desse modo, a vazão fim a fim é agora reduzida a 500 kbits/s por *download*.

Os exemplos nas Figuras 1.19 e 1.20(a) mostram que a vazão depende das taxas de transmissão dos enlaces sobre as quais os dados fluem. Vimos que quando não há tráfego interveniente, a vazão pode apenas ser aproxi- mada 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 modo geral, a vazão depende não somente das taxas de transmissão dos enla- ces ao longo do caminho, mas também do tráfego interveniente. Em especial, um enlace com uma alta taxa de transmissão pode, apesar disso, ser o enlace de gargalo para uma transferência de arquivo, caso muitos outros

10 servidoresEnlace de gargalo de capacidade *R*

Cliente 10 clientes

REDES DE COMPUTADORES E A INTERNET • 35

fluxos de dados estejam também passando por aquele enlace. Analisaremos em mais detalhes a 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, comutadores de pacotes, além de vários tipos de mídia em nível 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 analo- gia 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 estru- tura 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 poderia ser apresentar a relação de uma série de ações que você realiza (ou que outros executam para você) quando voa por uma empresa aérea. Você compra a passagem, despacha suas malas, dirige-se ao portão de embarque e, por fim, 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 ori- gem 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-a, notamos que há uma função referente à passagem em cada ponta; há também uma função de bagagem para passageiros que já apresentaram o bilhete e uma de portão de embarque para os que já apresentaram o tíquete e despacharam as malas. 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

Passagem (comprar)

Bagagem (despachar)

Portões (embarcar)

Decolagem

Roteamento da aeronave

Passagem (reclamar)

Bagagem (recuperar)

Portões (desembarcar)

Aterrissagem

Roteamento da aeronave

Roteamento da aeronave

• 36

REDES DE COMPUTADORES E A INTERNET FIGURA 1.22 CAMADAS HORIZONTAIS DA FUNCIONALIDADE DE LINHA AÉREA

Passagem aérea (comprar) Bagagem (despachar) Portões (embarcar)

Decolagem

Roteamento de aeronave A Figura 1.22 dividiu a funcionalidade da linha aérea em camadas, provendo uma estrutura com a qual pode- mos discutir a viagem aérea. Note que cada camada, combinada com as que estão 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 trans- ferência “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 o bilhete. Na camada do portão, é realizada a transferência “portão-de-embarque-portão-de -desembarque” do viajante e de suas malas. Na camada de decola- gem/aterrissagem, é realizada a transferência “pista-a-pista” de passageiros e de suas bagagens. Cada camada provê seu serviço (1) realizando certas ações dentro dela (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 do portão, aproveitando o serviço de transferência “pista-a-pista” de passageiros da camada de decolagem/aterrissagem).

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, tornando muito mais fácil modificar a execução do serviço prestado pela camada. Contanto que a camada forneça o mesmo serviço para a que está acima e use os mesmos serviços da que vem abaixo dela, o restante do sistema permanece inalterado quando a sua realização 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 per- maneceria inalterado, já que a camada do portão continuaria a prover a mesma função (embarcar e desembarcar passageiros); ela apenas executaria aquela função de maneira diferente após a alteração. Para sistemas grandes e complexos que são atualizados constantemente, a capacidade de modificar a realização 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 es- trutura para o projeto, projetistas de rede organizam protocolos — e o hardware e o software de rede que os executam — em **camadas**. Cada protocolo pertence a uma das camadas, assim como cada função na arquitetura de linha aérea da Figura 1.22 pertencia a uma camada. Mais uma vez estamos interessados nos **serviços** que uma camada oferece à camada acima dela — denominado **modelo de serviço**. Assim como em nosso exemplo da linha aérea, cada camada provê seu serviço (1) executando certas ações dentro dela 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 fim a fim da camada *n* – 1 e adicionando funcionalidade da camada *n* para detectar e retransmitir mensagens perdidas.

Roteamento de aeronave Roteamento de aeronave Passagem (reclamar) Bagagem (recuperar) Portões (desembarcar)

Aterrissagem

Roteamento de aeronave

Passagem

Bagagem

Portão

Decolagem/Aterrissagem

Roteamento de aeronave

Aeroporto de origem Centrais intermediárias

Aeroporto de destino de controle de tráfego aéreo

REDES DE COMPUTADORES E A INTERNET • 37

Uma camada de protocolo pode ser executada em software, em hardware, ou em uma combinação dos dois. Protocolos de camada de aplicação — como HTTP e SMTP — quase sempre são realizados em software nos sistemas finais; o mesmo acontece com protocolos de camada de transporte. Como a camada física e as de enlace de dados são responsáveis pelo manuseio da comunicação por um enlace específico, em geral são executadas em uma placa de interface de rede (por exemplo, placas de interface Ethernet ou Wi-Fi) associadas a determinado enlace. A camada de rede quase sempre é uma execução mista de hardware e software. Note também que, tal 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, um protocolo de camada *n* é *distribuído* entre sistemas finais, comutadores de pacote e outros componentes que formam a rede. Isto é, há sempre uma parte de um pro- tocolo de camada *n* em cada componente de rede.

O sistema de camadas de protocolos tem vantagens conceituais e estruturais [RFC 3439]. 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 é que uma camada pode duplicar a funcionalidade de uma inferior. Por exemplo, muitas pilhas de protocolos oferecem serviço de recuperação de erros para cada enlace e também de fim a fim. Uma segunda desvantagem é que a funcionalidade em uma camada pode necessitar de informações (por exemplo, um valor de carimbo de tempo) que estão presentes somente em outra, o que infringe o objetivo de separação de camadas.

Quando tomados em conjunto, os protocolos das várias camadas são denominados **pilha de protocolos**. A pilha de protocolos da Internet é formada por cinco camadas: física, de enlace, de rede, de transporte e de apli- cação, 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 *top-down*** (de cima para baixo), primeiro abordando a camada de aplicação e prosseguindo para baixo.

**Camada de aplicação**

A camada de aplicação é onde residem aplicações de rede e seus protocolos. A camada de aplicação da Inter- net inclui muitos protocolos, tais como o HTTP (que provê requisição e transferência de documentos pela Web), o SMTP (que provê transferência de mensagens de correio eletrônico) e o FTP (que provê a transferência de arquivos entre dois sistemas finais). Veremos que certas funções de rede, como a tradução de nomes fáceis de entender, que são dados a sistemas finais da Internet (por exemplo, de <www.ietf.org> para um endereço de rede de 32 bits), tam- bém são executadas com a ajuda de um protocolo de camada de aplicação, no caso, o sistema de nomes de domínio

FIGURA 1.23 A PILHA DE PROTOCOLOS DA INTERNET (A) E O MODELO DE REFERêNCIA OSI (B)

Transporte

Aplicação

Apresentação

Aplicação

Rede

Rede

Enlace

Enlace

Físico

Físico

a. Pilha de protocolos

b. Modelo de referência da Internet de

ISO de sete camadas cinco camadas

Sessão

Transporte

• REDES DE COMPUTADORES E A INTERNET 38(*domain name system* — DNS). Veremos no Capítulo 2 que é muito fácil criar nossos próprios novos protocolos

de camada de aplicação.

Um protocolo de camada de aplicação é distribuído por diversos sistemas finais, e a aplicação em um siste- ma final utiliza o protocolo para trocar pacotes de informação com a aplicação em outro sistema final. Chamare- mos de **mensagem** a esse pacote de informação na camada de aplicação.

**Camada de transporte**

A camada de transporte da Internet carrega 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 pode levar mensagens da camada de aplicação. O TCP provê serviços orientados a 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 reduz sua velocidade de transmissão quando a rede está congestionada. O protocolo UDP provê serviço não orientado a conexão para suas aplicações. É um serviço econômico que fornece segurança, sem controle de fluxo e de con- gestionamento. Neste livro, chamaremos de **segmento** a um pacote da camada de transporte.

**Camada de rede**

A camada de rede da Internet é responsável pela movimentação, de um hospedeiro para outro, de pa- cotes da camada de rede, conhecidos como **datagramas**. O protocolo de camada de transporte da Internet (TCP ou UDP) em um hospedeiro de origem passa um segmento da 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 no hospedeiro de destino.

Essa camada inclui o famoso protocolo IP, que define os campos no datagrama e o modo como os sistemas finais e os roteadores agem nesses campos. Existe apenas um único protocolo IP, e todos os componentes da In- ternet que têm uma camada de rede devem executá-lo. A camada de rede da Internet também contém protocolos de roteamento que determinam as rotas que os datagramas seguem entre origens e destinos. A Internet tem mui- tos 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. Embora a camada de rede contenha o protocolo IP e também numerosos outros de roteamento, ela quase sempre é denominada apenas 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 roteia um datagrama por meio de uma série de roteadores entre a origem e o destino. Para levar um pacote de um nó (hospedeiro ou roteador) 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 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. Por exemplo, alguns desses protocolos proveem entrega garantida entre enlaces, isto é, desde o nó transmissor, pas- sando por um único enlace, até o nó receptor. Note que esse serviço confiável de entrega é diferente do 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, Wi-Fi e o protocolo DOCSIS da rede de acesso por cabo. Como datagramas normalmente precisam transitar por diversos enlaces para irem da origem ao destino, serão manuseados por diferentes protocolos de camada de enlace em diversos enlaces ao longo de sua rota, podendo ser manuseados

REDES DE COMPUTADORES E A INTERNET • 39

por Ethernet em um 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 de novo dependem do enlace e, além disso, 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, mais um para fibra e assim por diante. Em cada caso, o bit atravessa o enlace de um modo diferente.

**O modelo OSI**

Após discutir em detalhes a pilha de protocolos da Internet, devemos mencionar que ela não é a única exis- tente. No final dos anos 1970, a Organização Internacional para Padronização (ISO — International Organization for Standardization) propôs que as redes de computadores fossem organizadas em, mais ou menos, sete camadas, denominadas modelo de Interconexão de Sistemas Abertos (OSI — *Open Systems Interconnection*) [ISO, 2012]. O modelo OSI tomou forma quando os protocolos que iriam se tornar protocolos da Internet estavam em sua infância e eram um dos muitos conjuntos 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 uni- versitários 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, esse modelo 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: de aplicação, de apresen- tação, de sessão, de transporte, de rede, de enlace e camada física. A funcionalidade de cinco dessas camadas é a mesma que seus correspondentes da Internet. Desse modo, vamos considerar as duas camadas adicionais presentes no modelo de referência OSI — a de apresentação e a 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 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 no qual os dados estão sendo representados/armazenados — formatos que podem ser diferentes 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 des- ses serviços? A resposta da Internet para essas perguntas é a mesma — depende do desenvolvedor da aplicação. Cabe a ele decidir se um serviço é importante; e se o serviço *for* importante, cabe ao desenvolvedor da aplicação construir essa funcionalidade para ela.

1.5.2 Encapsulamento

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 e roteador de camada de enlace interveniente, e depois para cima na pilha de protocolos do sistema final receptor. Como discutiremos mais adiante neste livro, ambos, roteadores e comutadores de camada de enlace, são comutadores de pacotes. De modo semelhante a sistemas finais, ambos organizam seu hardware e software de rede em camadas. Mas não implementam *todas* as camadas da pilha de protocolos; em geral executam apenas as camadas de baixo. Como

• 40REDES DE COMPUTADORES E A INTERNET FIGURA 1.24 HOSPEDEIROS, ROTEADORES E COMUTADORES DE CAMADA DE ENLACE; CADA UM

CONTÉM UM CONJUNTO DIFERENTE DE CAMADAS, REFLETINDO SUAS DIFERENÇAS EM FUNCIONALIDADE

MMMM

ilustra a Figura 1.24, comutadores de camada de enlace realizam as camadas 1 e 2; roteadores executam as ca- madas 1, 2 e 3. Isso significa, por exemplo, que roteadores da Internet são capazes de executar 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, os da Ether- net. Note que os hospedeiros 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 da camada de aplicação** na máquina emissora (M na Figura 1.24) é passada para a camada de transporte. No caso mais sim- ples, esta pega a mensagem e anexa informações adicionais (denominadas informações de cabeçalho de camada de transporte, camada de aplicação H*t* na Figura 1.24) que serão usadas pela camada de transporte do lado receptor. A mensagem da 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 incluir dados que habilitem a camada de transporte do lado do receptor a entregar a mensagem à aplicação apro- priada, 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 infor- mações destino, Origem Mensagem

Aplicação

Segmento

HtTransporte Datagrama

HnHtRede Quadro

Hl

Hn Ht

Enlace

Físico

Hl

Hn Ht M Enlace

Hl Hn Ht M Físico

Comutador da camada de enlace

Destino

Roteador

MAplicação

HtMTransporte

Hn Ht M Rede

Hn Ht M HtMRede

Hl Hn Ht M Enlace

Hl Hn Ht M Ht

M

Enlace

Físico Físico de criando cabeçalho um **datagrama** de camada **de** de **camada** rede (H*n* **de** na **rede**. Figura Este 1.24), é então como passado endereços para a de camada sistemas de HnHl Hn finais de origem e 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 em geral 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 a outra. Suponha que Alice, que está em uma filial, queira enviar um memorando a Bob, que está na outra filial. O *memorando* representa a *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 *enve- lope de correspondência interna* representa o *segmento da camada de aplicação* — contém as informações de ca-

REDES DE COMPUTADORES E A INTERNET • 41

beçalho (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, adequado para envio pelo correio. A central de correspondência emissora também escreve o endereço postal do remetente e do destinatário no envelope postal. Nesse ponto, o *envelope postal* é análogo ao *datagrama* — encap- sula 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 escri- tório destinatário. Nesse local, o processo de desencapsulamento se inicia. A central de correspondência retira o memorando e o encaminha a Bob. Este, por fim, abre o envelope e retira o memorando.

O processo de encapsulamento pode ser mais complexo do que o descrito. 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, incluindo empresas grandes e pequenas, universi- dades 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 escuro, 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 rede dos quais dependemos.

A área de segurança trata de 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 riscos primeiro. Dadas a frequência e a variedade das ameaças existentes, bem como o perigo de novos e mais destrutivos futuros ataques, a segurança se tornou um assunto principal na área de redes de computadores. Um dos objetivos deste livro é trazer as questões de segurança de rede para o primeiro plano.

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

**Os vilões podem colocar “*malware*” em seu hospedeiro por meio da Internet**

Conectamos aparelhos à Internet porque queremos receber/enviar dados de/para a rede. 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 de modo coletivo como ***malware*** — que também podem entrar e infectar nossos aparelhos. Uma vez que o *malware* infecta nosso aparelho, ele é capaz de fazer coisas perversas, como apagar nossos arquivos; instalar *spyware* que coleta informações particulares, como nosso número de cartão de crédito, senhas e combinação de teclas, e as envia (pela Internet, é claro!) de volta aos vilões. Nosso hospedeiro comprometido pode estar, também, envolvido em uma rede de milhares de aparelhos comprometidos, conheci- dos como ***botnet***, a qual é controlada e utilizada pelos vilões para distribuição de *spams* ou ataques de recusa de serviço distribuídos (que serão discutidos em breve) contra hospedeiros direcionados.

Muitos *malwares* existentes hoje são **autorreprodutivos**: uma vez que infectam um hospedeiro, a par- tir deste, ele faz a busca por entradas em outros hospedeiros pela Internet, e a dos hospedeiros recém-in- fectados, procura por entrada em mais hospedeiros. Dessa maneira, o *malware* autorreprodutivo pode se disseminar rapidamente. O *malware* pode se espalhar na forma de um vírus ou um *worm*. Os **vírus** são

• REDES DE COMPUTADORES E A INTERNET 42*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*** 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 aplica- ção 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 vulnerável. Ao encontrá-los, envia uma cópia de si mesmo para eles. 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 ques- tão: o que os projetistas de computadores podem fazer para proteger os aparelhos que utilizam a Internet contra as 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** — Denial-of-Service**)**. Como o nome sugere, um ataque DoS torna uma rede, hospedeiro ou outra parte da infraes- trutura inutilizável por usuários verdadeiros. Servidores da Web, de e-mail 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 pode ser dividida em três categorias:

*• Ataque de vulnerabilidade.* Envolve o envio de algumas mensagens bem elaboradas a uma aplicação vul- nerável ou a um sistema operacional sendo executado em um hospedeiro direcionado. Se a sequência correta de pacotes é enviada a uma aplicação ou sistema operacional vulnerável, o serviço pode parar ou, pior, o hospedeiro pode pifar.

*• Inundação na largura de banda.* O atacante envia um grande número de pacotes ao hospedeiro dire- cionado — 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 aber- tas (as conexões TCP são discutidas no Capítulo 3) no hospedeiro-alvo. O hospedeiro pode ficar tão atolado com essas conexões falsas que deixa 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 de *R* bits/s, o atacante precisará enviar tráfego a uma taxa de, mais ou menos, *R* bits/s para causar dano. Se *R* for muito grande, uma fonte de ataque única pode não ser capaz de gerar tráfego suficiente para prejudicar o servi- dor. Além disso, se todo o tráfego emanar de uma fonte única, um roteador mais adiante 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** — **Distributed DoS)**, ilustrado na Figura 1.25, o atacante controla múltiplas fontes que sobrecarregam o alvo. Com essa tática, 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 compro- metidos 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.

Encorajamos o leitor a considerar a seguinte questão à medida que trabalhar com este livro: o que os proje- tistas de redes de computadores podem fazer para se protegerem contra ataques DoS? Veremos que são necessá- rias diferentes defesas para os três tipos de ataques DoS.

REDES DE COMPUTADORES E A INTERNET • 43

FIGURA 1.25 UM ATAQUE DE RECUSA DE SERVIÇO DISTRIBUÍDO (DDOS)

Zumbi

Zumbi“Iniciar ataque”

Zumbi

AtacanteZumbi

**Os vilões podem analisar pacotes**

Muitos usuários hoje acessam a Internet por meio de aparelhos sem fio, como laptops conectados à tecno- logia Wi-Fi ou aparelhos portáteis com conexões à Internet via telefone celular (abordado no Capítulo 6). Em- bora o acesso onipresente à Internet seja de extrema conveniência e disponibilize 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 identificação, segredos comerciais e mensagens pessoais. Um receptor passivo que grava uma cópia de cada pacote que passa é denominado **analisador de pacote** (*packet sniffer*).

Os analisadores também podem estar distribuídos em ambientes de conexão com fio. Nesses ambientes, como em muitas LANs Ethernet, 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 for- ma, 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 escrita de um pro- grama de reconstrução de dados da camada de aplicação e um programa analisador de pacotes. De fato, os Wire- shark labs [Wireshark, 2012] associados a este texto (veja o Wireshark lab introdutório ao final deste capítulo) utilizam exatamente tal analisador de pacotes.

Como os analisadores de pacote são passivos — ou seja, 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 explicada 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 facílimo (*você* saberá como fazer isso à medida que ler este livro!) criar um pacote com qualquer endereço de origem, conteúdo de pacote e endereço de destino e, depois, transmiti-lo para a Inter- net, que, obedientemente, o encaminhará ao destino. Imagine que um receptor inocente (digamos, um roteador da Internet) que recebe tal pacote acredita que o endereço de origem (falso) seja confiável e então executa um

Vítima

Zumbi

• REDES DE COMPUTADORES E A INTERNET 44comando integrado ao conteúdo do pacote (digamos, que modifica sua base de encaminhamento). A capacidade de introduzir pacotes na Internet com um endereço de origem falso 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 *autenticação do ponto final*, ou seja, um mecanismo que nos permita 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.

Ao encerrar esta seção, deve-se considerar como a Internet se tornou um local inseguro, antes de tudo. A resposta breve é que a Internet foi, a princípio, criada dessa maneira, baseada no modelo de “um grupo de usuá- rios de confiança mútua ligados a uma rede transparente” [Blumenthal, 2001] — um modelo no qual (por defini- ção) 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 autenticada como padrão.

Mas a Internet de hoje decerto não envolve “usuários de confiança mútua”. Contudo, os usuários atuais ainda precisam se comunicar mesmo quando não confiam um no outro, podem querer se comunicar de modo anônimo, podem se comunicar indiretamente por 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 buscar proteção contra a análise, disfarce da origem, ataques *man-in-the-middle*, ataques DDoS, *malware* e outros. Precisamos 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 quiser ser mesmo o maior sucesso na próxima festa, você deve rechear seu discurso com pérolas da fascinante história da Internet [Segaller, 1998].

1.7.1 DesenvOlvimentO da cOmutaçãO de pacOtes: 1961d1972

Os primeiros passos da disciplina de redes de computadores e da Internet atual 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 in- formações de uma origem a um destino — uma escolha acertada, já que a voz é transmitida a uma taxa constante entre os pontos. Dada a importância cada vez maior dos computadores no início da década de 1960 e o advento de computadores com tempo compartilhado, nada seria mais natural do que considerar a questão de como inter- ligar computadores para que pudessem ser compartilhados entre usuários geograficamente dispersos. O tráfego gerado por esses usuários provavelmente era feito 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 co- mutação 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 aluno de graduação no MIT. Usando a teoria de

REDES DE COMPUTADORES E A INTERNET • 45

filas, seu trabalho 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 NPL foram os alicerces do que hoje é a Internet. Mas a Internet 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 ARPA- net [Roberts, 1967], a primeira rede de computadores por comutação de pacotes e uma ancestral direta da Inter- net pública de hoje. Em 1969, no Dia do Trabalho nos Estados Unidos, foi instalado o primeiro comutador de pacotes na UCLA (Universidade da Califórnia em Los Angeles) sob a supervisão de Kleinrock. Pouco tempo depois, foram instalados três comutadores de pacotes adicionais no Stanford Research Institute (SRI), na Univer- sidade da Califórnia em Santa Bárbara e na Universidade de Utah (Figura 1.26). O incipiente precursor da Inter- net 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 cerca de 15 nós e foi apresentada publicamente pela primeira vez por Robert Kahn. 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]. Com um protocolo fim a fim à disposição, 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 COMUTADORES DE PACOTES

• REDES DE COMPUTADORES E A INTERNET 461.7.2 Redes prOprietárias e trabalhO em rede: 1972d1980

A ARPAnet inicial era uma rede isolada, fechada. Para se comunicar com uma máquina da ARPAnet, era pre- ciso estar ligado a um outro IMP dessa rede. Do início 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; Telenet, uma rede comercial de comutação de pacotes da BBN baseada 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 intercone- xão de redes, sob o patrocínio da DARPA (Defense Advanced Research Projects Agency — Agência de Projetos de Pesquisa Avançada de Defesa), criou basicamente *uma rede de redes* e foi realizado por Vinton Cerf e Robert Kahn [Cerf, 1974]; o termo *internetting* foi cunhado para descrever esse trabalho.

Esses princípios de arquitetura foram incorporados ao TCP. As primeiras versões desse protocolo, con- tudo, eram muito diferentes do TCP de hoje. Elas 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 desem- penhadas pelo IP). As primeiras experiências com o TCP, combinadas com o reconhecimento da importância de um serviço de transporte fim a fim 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 rela- cionadas ao trabalho em rede estavam em andamento. No Havaí, Norman Abramson estava desenvolvendo a ALOHAnet, uma rede de pacotes por rádio que permitia que vários lugares remotos das ilhas havaianas se co- municassem entre si. O ALOHA [Abramson, 1970] foi o primeiro protocolo de acesso múltiplo que permitiu que usuários geograficamente dispersos compartilhassem um único meio de comunicação *broadcast* (uma frequên- cia de rádio). Metcalfe e Boggs se basearam no trabalho de Abramson sobre protocolo de múltiplo acesso quando desenvolveram o protocolo Ethernet [Metcalfe, 1976] para redes compartilhadas de transmissão broadcast por fio. 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.

1.7.3 PrOliferaçãO de redes: 1980d1990

Ao final da década de 1970, cerca de 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 Inter- net 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 compu- tadores para interligar universidades. A BITNET processava e-mails e fazia transferência de arquivos entre diver- sas universidades do nordeste dos Estados Unidos. A CSNET (Computer Science NETwork — rede da ciência de computadores) 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. Par- tindo de uma velocidade inicial de 56 kbits/s, ao final da década o *backbone* da NSFNET estaria funcionando a 1,5 Mbits/s 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

REDES DE COMPUTADORES E A INTERNET • 47

protocolo de máquinas para a ARPAnet (em substituição ao protocolo NCP). Pela 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 en- tender (por exemplo, gaia.cs.umass.edu) para seus endereços IP de 32 bits [RFC 1034].

Em paralelo ao desenvolvimento da ARPAnet (que em sua maior parte deve-se aos Estados Unidos), no iní- cio 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 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 incluía sites de livre acesso — como o da lista telefônica — e também 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. Estava presente em grande parte dos lares franceses dez anos antes sequer 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. 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.

O principal evento da década de 1990, no entanto, foi o surgimento da World Wide Web, que levou a Inter- net 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 busca (por exemplo, Google e Bing), comércio pela Internet (por exemplo, Amazon e eBay) e redes sociais (por exemplo, Facebook).

A Web foi inventada no CERN (European Center for Nuclear Physics — Centro Europeu para Física Nu- clear) por Tim Berners-Lee entre 1989 e 1991 [Berners-Lee, 1989], com base em ideias originadas de trabalhos anteriores sobre hipertexto realizados por Vannevar Bush [Bush, 1945], na década de 1940, e por Ted Nelson [Xanadu, 2012], na década de 1960. Berners-Lee e seus companheiros desenvolveram versões iniciais de HTML, HTTP, um servidor Web e um navegador (*browser*) — os quatro componentes fundamentais da Web. Por volta de 1993, havia cerca de 200 servidores Web em operação, e esse conjunto era apenas um prenúncio do que es- tava por vir. Nessa época, vários pesquisadores estavam desenvolvendo navegadores Web com interfaces GUI (Graphical User Interface — interface gráfica de usuário), entre eles Marc Andreessen, que liderou o desenvolvi- mento do popular navegador Mosaic, junto com Kim Clark, que formaram a Mosaic Communications, que mais tarde se transformou na Netscape Communications Corporation [Cusumano, 1998; Quittner, 1998]. Em 1995, estudantes universitários estavam usando navegadores Mosaic e Netscape para navegar na Web diariamente. Na época, empresas — grandes e pequenas — começaram a operar servidores e a realizar transações comerciais pela Web. Em 1996, a Microsoft começou a desenvolver navegadores, dando início à guerra entre Netscape e Microsoft, vencida pela última alguns anos mais tarde [Cusumano, 1998].

A segunda metade da década de 1990 foi um período de tremendo crescimento e inovação, com grandes corporações e milhares de novas empresas criando produtos e serviços para a Internet. 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;

• compartilhamento *peer-to-peer* de arquivos MP3, cujo pioneiro foi o Napster.

• REDES DE COMPUTADORES E A INTERNET 48

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 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 outras surgiram como grandes vencedoras no mundo da Internet, entre elas Microsoft, Cisco, Yahoo, eBay, Google e Amazon.

1.7.5 O nOvO milêniO

A inovação na área de redes de computadores continua a passos largos. Há progressos em todas as frentes, incluindo distribuição de roteadores mais velozes e velocidades de transmissão mais altas nas redes de acesso e nos *backbones* da rede. Mas os seguintes desenvolvimentos merecem atenção especial:

• Desde o início do milênio, vimos a implementação agressiva do acesso à Internet por banda larga nos lares — não apenas modems a cabo e DSL, mas também “*fiber to the home*”, conforme discutimos na Seção 1.2. Esse acesso à Internet de alta velocidade preparou a cena para uma série de aplicações de ví- deo, incluindo a distribuição de vídeo gerado pelo usuário (por exemplo, YouTube), fluxo contínuo por demanda de filmes e shows de televisão (por exemplo, Netflix) e videoconferência entre várias pessoas (por exemplo, Skype).

• A onipresença cada vez maior das redes Wi-Fi públicas de alta velocidade (54 Mbits/s e mais altas) e o acesso à Internet com velocidade média (até alguns Mbits/s) por redes de telefonia celular 3G e 4G não apenas está possibilitando permanecer constantemente conectado enquanto se desloca, mas também permite novas aplicações específicas à localização. O número de dispositivos sem fio conectados ultra- passou o número de dispositivos com fio em 2011. Esse acesso sem fio em alta velocidade preparou a cena para o rápido surgimento de computadores portáteis (iPhones, Androids, iPads etc.), que possuem acesso constante e livre à Internet.

• Redes sociais on-line, como Facebook e Twitter, criaram redes de pessoas maciças em cima da Internet. Muitos usuários hoje “vivem” principalmente dentro do Facebook. Através de suas APIs, as redes sociais on-line criam plataformas para novas aplicações em rede e jogos distribuídos.

• Conforme discutimos na Seção 1.3.3, os provedores de serviços on-line, como Google e Microsoft, im- plementaram suas próprias amplas redes privativas, que não apenas conectam seus centros de dados distribuídos em todo o planeta, mas são usadas para evitar a Internet ao máximo possível, emparelhando diretamente com ISPs de nível mais baixo. Como resultado, Google oferece resultados de busca e acesso a e-mail quase instantaneamente, como se seus centros de dados estivessem rodando dentro do compu- tador de cada usuário.

• Muitas empresas de comércio na Internet agora estão rodando suas aplicações na “nuvem” — como na EC2 da Amazon, na Application Engine da Google ou na Azure da Microsoft. Diversas empresas e universidades também migraram suas aplicações da Internet (por exemplo, e-mail e hospedagem de páginas Web) para a nuvem. Empresas de nuvem não apenas oferecem ambientes de computação e armazenamento escaláveis às aplicações, mas também lhes oferecem acesso implícito às suas redes privativas de alto desempenho.

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

REDES DE COMPUTADORES E A INTERNET • 49

da rede, examinando sistemas finais e aplicações, além do serviço de transporte fornecido às aplicações que exe- cutam nos sistemas finais. Também vimos as tecnologias de camada de enlace e meio físico 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. Estudamos 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. Primeiro 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, bem como modelos de vazão; 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. Terminamos nossa introdução sobre redes com uma breve história das redes de computadores. O pri- meiro capítulo constitui um minicurso sobre redes de computadores.

Portanto, percorremos de fato 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 partes que formam uma rede, um domínio ainda em desenvolvimento do vocabulário de redes (não se acanhe de voltar aqui para consulta) e um desejo cada vez maior de aprender mais sobre elas. Essa 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 estra- das principais e desvios que encontraremos pela frente. O destino final da viagem que estamos prestes a empreen- der é um entendimento profundo do como, do quê e do porquê das redes de computadores. Nosso guia é a sequência de capítulos:

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. Redes sem fio e 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 eles estão organizados segundo as quatro camadas superiores da pilha de cinco camadas de protocolos da Internet, com um capítulo para cada uma. Note também que nossa jornada começará no topo da pilha, 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-lhes suporte. Então, poderemos examinar, um por um, os vários modos como esses serviços poderiam ser executados por uma arquitetura de rede. Assim, o estudo das aplicações logo no início dá motivação para o restante do livro.

• REDES DE COMPUTADORES E A INTERNET 50

A segunda metade — Capítulos 6 a 9 — aborda quatro tópicos de extrema importância (e de certa maneira independentes) de redes modernas. No Capítulo 6, examinamos as redes sem fio e móvel, incluindo LANs sem fio (incluindo Wi-Fi 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 fluxo contínuo de mídia armazenada. Examinamos também como uma rede de comutação de pacotes pode ser projetada para prover qualidade de serviço consistente para aplicações de áudio e vídeo. No Capítulo 8 (Segu- rança em redes de computadores), analisamos, primeiro, 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 principais protocolos da Internet utilizados para esse fim.

EXERCÍCIOS DE FIXAÇÃO E PERGUNTAS

Questões de revisãO dO CapítulO 1

SEÇÃO 1.1

R1. Qual é a diferença entre um hospedeiro e um sistema final? Cite os tipos de sistemas finais. Um servidor Web

é um sistema final? R2. A palavra *protocolo* é muito usada para descrever relações diplomáticas. Como a Wikipedia descreve um

protocolo diplomático? R3. Por que os padrões são importantes para os protocolos?

SEÇÃO 1.2

R4. Cite seis tecnologias de acesso. Classifique cada uma delas nas categorias acesso residencial, acesso corporativo

ou acesso móvel. R5. 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? R6. Cite as 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. R7. Qual é a taxa de transmissão de LANs Ethernet? R8. Cite alguns meios físicos utilizados para instalar a Ethernet. R9. Modems discados, HFC, DSL e FTTH são usados para acesso residencial. Para cada uma dessas tecnologias de acesso, cite uma faixa de taxas de transmissão e comente se a taxa de transmissão é compartilhada ou dedicada. R10. Descreva as tecnologias de acesso sem fio mais populares atualmente. Faça uma comparação entre elas.

SEÇÃO 1.3

R11. 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.)

REDES DE COMPUTADORES E A INTERNET • 51

R12. 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? R13. Suponha que usuários compartilhem um enlace de 2 Mbits/s e que cada usuário transmita continuamente a 1 Mbit/s, mas cada um deles transmite apenas 20% do tempo. (Veja a discussão sobre multiplexação estatística na Seção 1.3.) a. Quando a comutação de circuitos é utilizada, quantos usuários podem ser admitidos? b. 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? c. Determine a probabilidade de um dado usuário estar transmitindo. d. 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. R14. Por que dois ISPs no mesmo nível de hierarquia farão emparelhamento? Como um IXP consegue ter lucro? R15. Alguns provedores de conteúdo criaram suas próprias redes. Descreva a rede da Google. O que motiva os

provedores de conteúdo a criar essas redes?

SEÇÃO 1.4

R16. 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? R17. Visite o applet “Transmission *versus* Propagation Delay” no site de apoio do livro. 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. Ache outra combinação para a qual o primeiro bit do pacote alcança o receptor antes que o emissor termine de transmitir. R18. 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 ∙ 108 m/s e uma taxa de transmissão de 2 Mbits/s? Em geral, 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* bits/s? Esse atraso depende do comprimento do pacote? Depende da taxa de transmissão? R19. Suponha que o hospedeiro A queira enviar um arquivo grande para o hospedeiro B. O percurso de A para

B possui três enlaces, de taxas *R*1 = 500 kbits/s, *R*2 = 2 Mbits/s, e *R*3 = 1 Mbit/s. a. Considerando que não haja nenhum outro tráfego na rede, qual é a vazão para a transferência de arquivo? b. 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? c. Repita os itens “a” e “b”, mas agora com *R*2 reduzido a 100 kbits/s. R20. 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 chega 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 pacotes na Internet é semelhante a dirigir de uma cidade para outra pedindo informações ao longo do caminho? R21. Visite o applet “Queuing and Loss” no site de apoio do livro. Qual é a taxa de emissão máxima e a taxa de transmissão 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 mais uma vez e determine de novo o tempo de ocorrência para a perda de pacote. Os resultados são diferentes? Por quê? Por que não?

• REDES DE COMPUTADORES E A INTERNET 52SEÇÃO 1.5

R22. 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? R23. Quais são as cinco camadas da pilha de protocolo da Internet? Quais as principais responsabilidades de

cada uma dessas camadas? R24. 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? R25. Que camadas da pilha do protocolo da Internet um roteador processa? Que camadas um comutador de

camada de enlace processa? Que camadas um sistema final processa?

SEÇÃO 1.6

R26. Qual é a diferença entre um vírus e um *worm*? R27. Descreva como pode ser criado uma *botnet* e como ela pode ser utilizada no ataque DDoS. R28. Suponha que Alice e Bob estejam enviando pacotes um para o outro por uma rede de computadores e que Trudy se posicione na rede para poder 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

P1. Projete e descreva um protocolo de nível de aplicação para ser usado entre um caixa eletrônico 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 (isto é, entrega de dinheiro ao usuário). As entidades do protocolo devem estar preparadas para resolver o caso comum em que não há dinheiro suficiente na conta para cobrir o saque. Especifique 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. P2. A Equação 1.1 contém uma fórmula para o atraso fim a fim do envio de um pacote de comprimento *L* por *N* enlaces com taxa de transmissão *R*. Generalize essa fórmula para enviar *P* desses pacotes de ponta a ponta pelos *N* enlaces. P3. 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 venha de aplicações como a descrita anteriormente. Além disso, imagine que a soma das velocidades de dados da aplicação seja menor do que a capacidade de cada enlace. Será necessário algum tipo de controle de congestionamento? Por quê? P4. Considere a rede de comutação de circuitos da Figura 1.13. Lembre-se de que há 4 circuitos em cada enlace.

Rotule os quatro comutadores A, B, C e D, seguindo no sentido horário. a. Qual é o número máximo de conexões simultâneas que podem estar em curso a qualquer instante nessa

rede?

REDES DE COMPUTADORES E A INTERNET • 53

b. Suponha que todas as conexões sejam entre os comutadores A e C. Qual é o número máximo de conexões

simultâneas que podem estar em curso? c. Suponha que queiramos fazer quatro conexões entre os comutadores A e C, e outras quatro conexões entre os *switches* B e D. Podemos rotear essas chamadas pelos quatro enlaces para acomodar todas as oito conexões? P5. 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 oito carros no comboio em vez de dez. P6. Este problema elementar começa a explorar atrasos de propagação e de transmissão, dois conceitos centrais em redes de computadores. Considere dois hospedeiros, A e B, conectados por um único enlace de taxa *R* bits/s. Suponha que eles estejam separados por *m* metros e que a velocidade de propagação ao longo do enlace seja de *s* metros/segundo. O hospedeiro A tem de enviar um pacote de *L* bits ao hospedeiro 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 hospedeiro A comece a transmitir o pacote no instante *t* = 0. No instante *t* = *d*trans, onde

estará o último bit do pacote? e. Imagine que *d*prop seja maior do que *d*trans. Onde estará o primeiro bit do pacote no instante *t* = *d*trans? f. Considere que *d*prop seja menor do que *d*trans. Onde estará o primeiro bit do pacote no instante *t* = *d*trans? g. Suponha que *s* = 2,5 ∙ 108, *L* = 120 bits e *R* = 56 kbits/s. Encontre a distância *m* de modo que *d*prop seja igual

a *d*trans. P7. Neste problema, consideramos o envio de voz em tempo real do hospedeiro A para o hospedeiro B por meio de uma rede de comutação de pacotes (VoIP). O hospedeiro A converte voz analógica para uma cadeia digital de bits de 64 kbits/s e, em seguida, agrupa os bits em pacotes de 56 bytes. Há apenas um enlace entre os hospedeiros A e B; sua taxa de transmissão é de 2 Mbits/s e seu atraso de propagação, de 10 ms. Assim que o hospedeiro A recolhe um pacote, ele o envia ao hospedeiro B. Quando recebe um pacote completo, o hospedeiro 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 hospedeiro A) e o momento em que ele é decodificado (como parte do sinal analógico no hospedeiro B)? P8. Suponha que usuários compartilhem um enlace de 3 Mbits/s e que cada usuário precise de 150 kbits/s para transmitir, mas que transmita apenas durante 10% do tempo. (Veja a discussão sobre comutação de pacotes *versus* comutação de circuitos na Seção 1.3.) a. Quando é utilizada comutação de circuitos, quantos usuários podem ser aceitos? b. Para o restante deste problema, suponha que seja usada a comutação de pacotes. Determine a probabilidade

de que determinado usuário esteja transmitindo. c. Suponha que haja 120 usuários. Determine a probabilidade que, a um tempo dado, exatamente *n* usuários

estejam transmitindo simultaneamente. (*Dica*: Use a distribuição binomial.) d. Determine a probabilidade de haver 21 ou mais usuários transmitindo simultaneamente. P9. Considere a discussão na Seção 1.3 sobre comutação de pacotes *versus* comutação de circuitos, na qual é dado um exemplo com um enlace de 1 Mbit/s. Quando em atividade, os usuários estão gerando dados a uma taxa de 100 kbits/s; mas a probabilidade de estarem em atividade, gerando dados, é de *p* = 0,1. Suponha que o enlace de 1 Mbit/s seja substituído por um de 1 Gbit/s. a. Qual é o número máximo de usuários, *N*, que pode ser suportado simultaneamente por comutação de

pacotes?

• REDES DE COMPUTADORES E A INTERNET 54

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. P10. Considere um pacote de comprimento *L* que se inicia no sistema final A e percorre três enlaces até um sistema final de destino. Eles estão conectados por dois comutadores de pacotes. Suponha que *di, si* e *Ri* 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 *di*, *si* e *Ri*, (*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 os enlaces seja 2,5 ∙ 108 m/s, as taxas de transmissão dos três enlaces sejam 2 Mbits/s, o atraso de processamento do comutador de pacotes seja de 3 ms, o comprimento do primeiro enlace seja 5.000 km, o do segundo seja 4.000 km e do último 1.000 km. Dados esses valores, qual é o atraso fim a fim? P11. No problema anterior, suponha que *R*1 = *R*2 = *R*3 = *R* e *d*proc = 0. Suponha que o comutador de pacote não armazene e reenvie pacotes, mas transmita imediatamente cada bit recebido antes de esperar o pacote chegar. Qual é o atraso fim a fim? P12. Um comutador de pacotes recebe um pacote e determina o enlace de saída pelo qual deve ser enviado. Quando o pacote chega, 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 Mbits/s. Qual é o atraso de fila para o pacote? De modo geral, qual é o atraso de fila quando todos os pacotes possuem comprimento *L*, a taxa de transmissão é *R*, *x* bits do pacote sendo transmitido já foram transmitidos e *N* pacotes já estão na fila? P13. (a) 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? (b) Agora considere que *N* desses pacotes cheguem ao enlace a cada *LN/R* segundos. Qual é o atraso de fila

médio de um pacote? P14. 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*. P15. Sendo *a* 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 *a* e *μ*. P16. Considere um buffer de roteador anterior a um enlace de saída. Neste problema, você usará a fórmula de Little, uma famosa fórmula da teoria das filas. Considere *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* ∙ *d*, suponha que, na média, o buffer contenha 10 pacotes, o atraso de fila de pacote médio seja 10 ms e a taxa de transmissão do enlace seja 100 pacotes/s. Utilizando tal fórmula, qual é a taxa média de chegada, considerando que não há perda de pacote? P17. (a) Generalize a Equação 1.2 na Seção 1.4.3 para taxas de processamento heterogêneas, taxas de transmissão

e atrasos de propagação. (b) Repita o item (a), mas suponha também que haja um atraso definição fila médio *d*fila em cada nó. P18. 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?

REDES DE COMPUTADORES E A INTERNET • 55

c. Tente identificar o número de redes de ISP pelas quais o pacote do Traceroute passa entre origem e destino. Roteadores com nomes semelhantes e/ou endereços IP semelhantes devem ser considerados 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. P19. (a) Visite o site <www.traceroute.org> e realize traceroutes de duas cidades diferentes na França para o mesmo hospedeiro de destino nos Estados Unidos. Quantos enlaces são iguais nos dois traceroutes? O enlace transatlântico é o mesmo? (b) Repita (a), mas desta vez escolha uma cidade na França e outra cidade na Alemanha. (c) Escolha uma cidade nos Estados Unidos e realize traceroutes para dois hosts, cada um em uma cidade diferente na China. Quantos enlaces são comuns nos dois traceroutes? Os dois traceroutes divergem antes de chegar à China? P20. 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, *Rc* 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 cliente-servidor. Deduza uma expressão geral para a vazão em relação a *R*s, *Rc*, *R* e *M*. P21. Considere a Figura 1.19(b). Agora suponha que haja *M* percursos entre o servidor e o cliente. Dois percursos nunca compartilham qualquer enlace. O percurso *k* (*k* = 1, ..., *M*) consiste em *N* enlaces com taxas de transmissão *Rk*1, *Rk*2...; *RKN*. 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? P22. 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? P23. 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 *Rs* bits/s. Imagine que enviemos um par de pacotes um após o outro do servidor para o cliente, e que não haja outro tráfego nesse percurso. Suponha 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 do pacote ao destino? Isto é, quanto tempo transcorre desde quando o

último bit do primeiro pacote chega até quando o último bit do segundo pacote chega? b. Agora suponha que o segundo enlace seja o de gargalo (isto é, *Rc < Rs*). 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. Qual deverá ser o tamanho de *T* para garantir que não haja uma fila antes do segundo enlace? Explique. P24. Imagine que você queira enviar, com urgência, 40 terabytes de dados de Boston para Los Angeles. Você tem disponível um enlace dedicado de 100 Mbits/s para transferência de dados. Escolheria transmitir os dados por meio desse enlace ou usar um serviço de entrega em 24 horas? Explique. P25. Suponha que dois hospedeiros, A e B, estejam separados por uma distância de 20 mil quilômetros e conectados por um enlace direto de *R* = 2 Mbits/s. Suponha que a velocidade de propagação pelo enlace seja de 2,5 ∙ 108 m/s. a. Calcule o produto largura de banda-atraso *R ∙ d*prop.

• REDES DE COMPUTADORES E A INTERNET 56

b. Considere o envio de um arquivo de 800 mil bits do hospedeiro A para o hospedeiro 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 o de um campo de futebol? e. 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*. P26. Com referência ao Problema P25, suponha que possamos modificar *R.* Para qual valor de *R* o comprimento

de um bit será o mesmo que o comprimento do enlace? P27. Considere o Problema P25, mas agora com um enlace de *R* = 1 Gbit/s.

a. Calcule o produto largura de banda × atraso, *R* × *d*prop. b. Considere o envio de um arquivo de 800 mil bits do hospedeiro 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? c. Qual é o comprimento (em metros) de um bit no enlace? P28. Novamente com referência ao Problema P25.

a. Quanto tempo demora para mandar o arquivo, admitindo que ele seja enviado continuamente? b. Suponha agora que o arquivo seja fragmentado em 20 pacotes e que cada um contenha 40 mil bits. Imagine que cada pacote seja verificado pelo receptor e que o tempo de transmissão de uma verificação de pacote seja desprezível. Por fim, admita que o emissor não possa enviar um pacote até que o anterior tenha sido reconhecido. Quanto tempo demorará para enviar o arquivo? c. Compare os resultados de ‘a’ e ‘b’. P29. Suponha que haja um enlace de micro-ondas de 10 Mbits/s 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. Considere uma velocidade de propagação de 2,4 ∙ 108 m/s. a. Qual é o atraso de propagação do enlace? b. Qual é o produto largura de banda-atraso, *R* ∙ *d*prop? c. Seja *x* o tamanho da foto. Qual é o valor mínimo de *x* para que o enlace de micro -ondas transmita

continuamente? P30. Considere a analogia da viagem aérea que utilizamos em nossa discussão sobre camadas na Seção 1.5, e o acréscimo de cabeçalhos a unidades de dados de protocolo enquanto passam pela pilha. Existe uma noção equivalente de acréscimo de informações de cabeçalho à movimentação de passageiros e suas malas pela pilha de protocolos da linha aérea? P31. Em redes modernas de comutação de pacotes, inclusive a Internet, o hospedeiro 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. O destinatário, então, monta novamente os pacotes restaurando a mensagem original. Denominamos esse processo *segmentação de mensagem*. A Figura 1.27 ilustra o transporte fim a fim de uma mensagem com e sem segmentação. Considere que uma mensagem de 8 × 106 bits de comprimento tenha de ser enviada da origem ao destino na Figura 1.27. Suponha que a velocidade de cada enlace da figura seja 2 Mbits/s. Ignore atrasos de propagação, de fila e de processamento. a. Considere o envio da mensagem da origem ao destino *sem* segmentação. Quanto tempo essa mensagem levará para ir do hospedeiro 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 do hospedeiro de origem ao hospedeiro de destino? b. Agora suponha que a mensagem seja segmentada em 800 pacotes, cada um com 10.000 bits de comprimento. Quanto tempo demorará para o primeiro pacote ir do hospedeiro de origem até o primeiro comutador?

REDES DE COMPUTADORES E A INTERNET • 57

FIGURA 1.27 TRANSPORTE FIM A FIM DE MENSAGEM: (A) SEM SEGMENTAÇÃO DE MENSAGEM; (B) COM

SEGMENTAÇÃO DE MENSAGEM

Mensagem

a. Origem Comutador

Comutador de pacotes

de pacotes

b. Origem Comutador de pacotes

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? c. Quanto tempo demorará para movimentar o arquivo do hospedeiro de origem até o hospedeiro de destino quando é usada segmentação de mensagem? Compare este resultado com sua resposta no item ‘a’ e comente. d. Além de reduzir o atraso, quais são as razões para usar a segmentação de mensagem? e. Discuta as desvantagens da segmentação de mensagem. P32. Experimente o applet “Message Segmentation” apresentado no site deste livro. Os atrasos no applet correspondem aos atrasos obtidos no problema anterior? Como os atrasos de propagação no enlace afetam o atraso total fim a fim na comutação de pacotes (com segmentação de mensagem) e na comutação de mensagens? P33. Considere o envio de um arquivo grande de *F* bits do hospedeiro A para o hospedeiro B. Há dois enlaces (e dois comutadores) entre A e B, e os enlaces não estão congestionados (isto é, não há atrasos de fila). O hospedeiro A fragmenta o arquivo em segmentos de *S* bits cada e adiciona 80 bits de cabeçalho a cada segmento, formando pacotes de *L* =80 + *S* bits. Cada enlace tem uma taxa de transmissão de *R* bits/s. Qual é o valor de *S* que minimiza o atraso para levar o arquivo de A para B? Desconsidere o atraso de propagação. P34. O Skype oferece um serviço que lhe permite fazer uma ligação telefônica de um PC para um telefone comum. Isso significa que a chamada de voz precisa passar pela Internet e por uma rede telefônica. Discuta como isso poderia ser feito.

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 de- talhes de sua operação, fazendo que eles executem determinadas ações e observando tais ações e suas consequên- cias. 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

Destino

Pacote

Comutador

Destino de pacotes