errôneas. As empresas também precisam tomar medidas especiais para assegurar alto nível de qualidade de dados. Isso inclui usar padrões de dados válidos para toda a empresa, bancos de dados projetados para minimizar a inconsistência e a redundância, auditorias de qualidade de dados e software de limpeza e padronização de dados.

Palavras-chave

Administração de dados, 162
Análise preditiva, 159
Atributos, 145
Auditoria de qualidade de dados, 163
Banco de dados, 144
Banco de dados relacional, 145
Campo, 145
Campo-chave, 145
Chave estrangeira, 146
Chave primária, 145
Data cleansing, 164
Data mart, 155
Data mining, 159
Data warehouse, 154
DBMS orientado a objeto, 153
Diagrama entidade/relacionamento, 147
Dicionário de dados, 152
Entidade, 145
Gestão de banco de dados, 162
Integridade referencial, 149
Inteligência empresarial (BI), 155
Linguagem de manipulação de dados, 152
Linguagem estruturada de consulta (SQL), 152
Mineração de textos, 160
Mineração na Web, 160
Normalização, 148
Política de informação, 162
Processamento analítico on-line (OLAP), 158
Registros, 145
Servidor de banco de dados, 161
Sistema de gestão de banco de dados (DBMS), 149
Tuplas, 145

Perguntas de revisão

1. Como um banco de dados relacional organiza os dados e como ele difere de um banco de dados orientado a objeto?

- Defina e explique os conceitos de entidades, atributos e campos-chave.
- Defina banco de dados relacional e explique como ele organiza e armazena as informações.
- Explique o papel dos diagramas entidade/relacionamento e da normalização no projeto do banco de dados.
- Defina banco de dados orientado a objeto e explique como ele difere de um banco de dados relacional orientado a objeto.

2. Quais os princípios de um sistema de gestão de banco de dados?

- Defina sistema de gestão de banco de dados (SGBD), descreva como ele funciona e explique os benefícios que proporciona.
- Explique a diferença entre a visão lógica e a visão física dos dados.
- Defina e descreva as três operações de um sistema de gestão de banco de dados relacional.
- Nomeie e descreva os três principais recursos de um DBMS.

3. Quais as principais ferramentas e tecnologias para acessar informações em bancos de dados e aprimorar o desempenho empresarial e a tomada de decisão?

- Descreva o que é data warehouse e explique como ele funciona.
- Defina inteligência empresarial e como ela se relaciona com a tecnologia de banco de dados.
- Descreva os recursos do processamento analítico on-line (OLAP).
- Defina data mining, descreva os tipos de informação obtidos a partir do data mining e explique em que ele difere do OLAP.
- Explique como a mineração de textos e a mineração na Web diferem do data mining.
- Explique como os usuários podem acessar informações dos bancos de dados internos de uma empresa via Web.

4. Quais são os papéis da política de informação e da administração de dados na gestão de dados?

- Defina política de informação e administração de dados e explique como elas ajudam as empresas a organizar seus dados.

5. Por que a garantia de qualidade é tão importante para a empresa?

- Liste e descreva os problemas de qualidade de dados mais comuns.
- Liste e descreva as ferramentas e técnicas mais importantes para garantir a qualidade dos dados.

Para discutir

1. Ninguém precisa de um software de gestão de banco de dados para criar um ambiente de banco de dados. Discuta.

2. Em que medida os usuários finais devem estar envolvidos na seleção de um sistema de gestão de banco de dados e no projeto do banco de dados?

Colaboração e trabalho em equipe

Forme um grupo de três ou quatro colegas. Escolham um banco de dados on-line para explorar — o AOL Music ou o Internet Movie Database (IMDB), por exemplo. Explorem esses sites para ver quais informações oferecem. Depois, enumere as entidades e os atributos que precisam controlar em seus bancos de dados. Façam um diagrama do relacionamento entre as entidades que o grupo identificou. Se possível, use o Google Sites para postar links para outras páginas da Web, anúncios para a equipe, trabalhos; para trocar ideias e trabalhar colaborativamente em documentos do projeto. Tente usar o Google Docs para desenvolver uma apresentação de suas descobertas para sua turma.

Resolvendo problemas organizacionais

Problemas com o banco de dados sobre terroristas

Depois das consequências dos ataques de 11 de setembro, críticos e defensores dos sistemas de informação utilizados pela comunidade de inteligência norte-americana se uniram para ajudar a analisar o que saiu errado e como prevenir futuros incidentes terroristas. O Centro de Triagem de Terroristas do FBI (Terrorist Screening Center), ou TST, foi criado para organizar e padronizar informações sobre terroristas suspeitos de diferentes agências do governo em uma lista única com vistas a melhorar a comunicação entre as agências. Foi criado um banco de dados de terroristas suspeitos denominado lista de observação de terroristas. Diversas agências vinham mantendo listas próprias e essas agências não dispunham de um processo consistente para compartilhar informações relevantes.

Os registros no banco de dados do TST contêm dados sensíveis, mas não classificados, sobre a identidade de terroristas, como nome e data de nascimento, que podem ser compartilhados com outras agências de triagem. Informações sigilosas sobre as pessoas na lista de observação são mantidas em outros bancos de dados pertencentes a agências de segurança e inteligência. Os registros da lista de observação vêm de duas fontes: Centro Nacional Antiterrorismo e o FBI. Gerenciado pelo Escritório do Diretor Nacional de Inteligência, o Centro Nacional Antiterrorismo fornece informações de identificação de indivíduos com ligações ao terrorismo internacional. O FBI também fornece essas informações, mas em relação ao terrorismo nacional.

Essas agências coletam e mantêm informações sobre terroristas e designam indivíduos para inclusão na lista de observação consolidada do TST. Elas devem seguir procedimentos rígidos estabelecidos pelo diretor de cada agência e aprovados pelo procurador-geral dos Estados Unidos. A equipe do TST deve revisar cada registro submetido antes de ser incluso no banco de dados. Um indivíduo permanecerá na lista de observação até que o respectivo departamento ou agência que indicou seu nome para a lista determine que a pessoa deve ser retirada dela e excluída do banco de dados.

O banco de dados com a lista de observação TST é atualizado diariamente com novos nomes, modificações nos registros existentes e exclusões. Desde sua criação, a lista agrupa 400 mil pessoas, registradas sob 1,1 milhão de nomes e apelidos, e continua crescendo a uma taxa de 200 mil registros a cada ano. As informações na lista são distribuídas para uma ampla gama de sistemas de agências do governo para uso nos esforços em deter ou detectar os movimentos de terroristas conhecidos ou suspeitos.

Dentre as agências que recebem as informações estão FBI, CIA, Agência de Segurança Nacional, Agência de Segurança em Transportes, Departamento de Segurança Interna, Proteção Alfandegária e de Fronteiras, Serviço Secreto, Serviço Militar e a Casa Branca. As companhias aéreas utilizam os dados fornecidos pelo sistema do TSA (Agência de Segurança em Transportes) em suas listas de interdição e permissão para embarque em voos para pré-triagem dos passageiros, enquanto o sistema de Proteção Alfandegária e de Fronteiras usa os dados da lista de observação para ajudar a identificar aqueles que entram nos Estados Unidos. O sistema do Departamento de Estado faz triagem dos indivíduos que solicitam visto de entrada no país e os residentes que requisitam passaportes, enquanto as agências locais de estado e segurança recorrem ao sistema do FBI para ajudar em prisões, detenções e outras atividades judiciais criminais. Cada uma dessas agências recebe o subconjunto de dados da lista de observação que pertence à sua missão específica.

Sempre que um indivíduo faz uma reserva aérea, chega a uma porta de entrada para os Estados Unidos, solicita um visto norte-americano ou é parado pela polícia estadual ou local em território desse país, a agência de triagem de fronteira ou a companhia aérea realiza uma pesquisa sobre o indivíduo com base no nome nos registros do banco de dados de terroristas. Quando o sistema com-

putadorizado de comparação de nomes gera um acerto (uma equivalência potencial entre nomes) com relação a um registro da lista de observação, a companhia aérea ou agência revisa a possível equivalência. As equivalências claramente positivas ou as exatas mas inconclusivas (incertas ou difíceis de serem verificadas) são encaminhadas aos centros de inteligência ou operações da agência de triagem adequada para inspeção mais detalhada. O TST, por sua vez, verifica seu banco de dados e outras fontes, incluindo bancos de dados sigilosos mantidos pelo Centro Nacional Antiterrorismo e pelo FBI, para confirmar se o indivíduo é uma equivalência positiva, negativa ou inconclusiva com o registro da lista de observação. O TST cria um relatório diário incluindo todas as equivalências positivas e o distribui para inúmeras agências federais.

Embora a unificação de várias listas de terroristas tenha sido um passo positivo no combate ao terrorismo, o projeto foi lento e meticuloso, demandando a integração de pelo menos 12 bancos de dados diferentes. Dois anos depois do processo de integração, 10 a 12 bancos de dados foram processados. Os dois bancos de dados restantes (sistema de identificação biométrica da imigração e das fronteiras, e o sistema integrado de identificação de digitais do FBI) são bancos de dados biométricos. Ainda há trabalho a ser feito na otimização da utilidade da lista de observação de terroristas.

Relatórios do Escritório de Contabilidade do Governo e do Escritório do Inspetor-Geral norte-americanos garantem que a lista contém imprecisões e que as políticas departamentais do governo para indicação e remoção da lista não são uniformes. Houve ainda um protesto público motivado pelo tamanho da lista e por incidentes amplamente difundidos de pessoas que obviamente não eram terroristas e descobriram seu nome na lista.

Informações sobre o procedimento para inclusão na lista devem, necessariamente, ser cuidadosamente protegidas para que a lista seja eficiente contra terroristas. Por outro lado, às pessoas inocentes afetadas, a impossibilidade de saber como foram parar na lista é irritante. Os critérios específicos para inclusão na lista não são de conhecimento público. Sabemos, entretanto, que as agências do governo preenchem suas listas realizando grandes varreduras nas informações coletadas sobre viajantes, utilizando diversas ortografias erradas ou variações dos nomes dos possíveis terroristas. Isso costuma causar a inclusão de pessoas que não deveriam estar na lista de observação, conhecidas como 'falsos positivos'. Resulta também na listagem múltipla de algumas pessoas sob ortografias diferentes de seu nome.

Embora esses critérios de seleção possam ser eficientes para controle do maior número possível de terroristas potenciais, também levam a um número muito maior de entradas erradas na lista do que se o processo de inclusão fosse mais refinado. Exemplos famosos de 'falsos positivos' incluem Daniel Brown, fuzileiro naval norte-americano parado no aeroporto para triagem adicional após oito meses no Iraque; o falecido senador Ted Kennedy, detido repetidas vezes porque seu nome lembrava o apelido utilizado por um terrorista suspeito; e John Anderson, que, apesar da pouca idade (seis anos), foi detido em um aeroporto para investigação. Como Kennedy, Anderson deve ter sido incluído porque seu nome é igual, ou é semelhante, ao de um possível terrorista.

Esses incidentes chamam a atenção para a qualidade e a precisão dos dados na lista de observação consolidada do TST. Em junho de 2005, um relatório do Escritório do Inspetor-Geral do Departamento de Justiça encontrou contagens inconsistentes de registros, registros duplicados e incompletos ou oriundos de fontes imprecisas. Embora o TST tenha aprimorado várias vezes seus esforços de identificação e correção de registros incompletos ou imprecisos da lista de observação, o inspetor-geral observou, em setembro de 2007, que a gestão da lista ainda apresentava algumas fraquezas.

Se pudessem escolher entre uma lista que controla todos os terroristas potenciais ao custo de incluir alguns inocentes e uma lista que não controla todos os terroristas porque evita a inclusão de inocentes, muitos escolheriam a primeira opção, apesar dos incômodos. Contudo, para que os esforços valham a pena aos que já foram incluídos na lista equivocadamente, não existe processo de reparação simples e rápido de remoção de nomes.

O número de solicitações de exclusão da lista de observação continua a crescer, totalizando mais de 24 mil (cerca de 2 mil por mês) e com percentual de resolução de somente 54 por cento. Em 2008, o tempo médio de processamento de uma solicitação era de 40 dias, não rápido o suficiente para dar conta do número de pedidos de exclusão recebidos. Como resultado, viajantes íntegros que inexplicavelmente se descobrem na lista não dispõem de uma maneira fácil de terem o nome excluído dela.

Em fevereiro de 2007, o Departamento de Segurança Interna criou o seu Programa de Solicitação de Correção para Viajantes (*TRIP – traveler redress inquiry program*) afim de ajudar os que foram erroneamente incluídos na lista de observação a terem o nome excluído e, assim, evitar triagens e questionamentos adicionais. A mãe de John Anderson disse que, apesar de seus esforços, não conseguiu retirar o nome do filho da lista. O senador Kennedy contou que somente conseguiu excluir seu nome da lista após relatar o caso pessoalmente a Tom Ridge, diretor do Departamento de Segurança Interna.

Oficiais de segurança dizem que erros como os que causaram a inclusão de Anderson e Kennedy na lista de impossibilitados de voar e na lista de observação consolidada ocorrem devido à equivalência entre dados imperfeitos nos sistemas das companhias aéreas. Muitas dessas empresas não incluem sexo, nome do meio ou data de nascimento em seus registros de reserva, o que aumenta a probabilidade de falsas equivalências.

Uma maneira de aprimorar a triagem e ajudar a reduzir o número de pessoas erroneamente marcadas para investigação adicional seria utilizar um sistema mais sofisticado que envolvesse um maior número de dados pessoais sobre os indivíduos na lista. O TST está desenvolvendo tal sistema, denominado 'Voo Seguro' (em inglês, *Secure Flight*), mas ele é continuamente atrasado por preocupações com privacidade relacionadas a sensibilidade e segurança dos dados coletados. Outros programas de sobrevivência e listas de observação semelhantes, como as tentativas da Agência Nacional de Segurança de obter

informações sobre terroristas suspeitos, receberam críticas por possíveis violações de privacidade.

Além disso, a lista de observação atraiu críticas devido a seu potencial para promoção de determinação de perfis e discriminação racial. Alguns alegam que foram incluídos em virtude de sua raça ou descendência étnica, como David Fathi, advogado da União Americana pelas Liberdades Civis, de descendência iraniana, e Asif Iqbal, cidadão norte-americano de descendência paquistanesa com o mesmo nome de um preso de Guantânamo. Críticos verdadeiros da política internacional norte-americana, como autoridades eleitas e professores universitários, também se descobriram na lista.

Um relatório divulgado no início de maio de 2009, por Glenn A. Fine, inspetor-geral do Departamento de Justiça, informa que o FBI manteve erroneamente quase 24 mil pessoas em sua própria lista de observação que fornece dados para a lista de terroristas com base em dados desatualizados ou irrelevantes. Ao examinar cerca de 69 mil reclamações com relação à lista do FBI, o relatório descobriu que 35 por cento das pessoas continuavam na lista apesar das justificativas inadequadas. Ainda mais preocupante, a lista não continha o nome das pessoas que deveriam ter sido listadas devido a ligações terroristas. Os oficiais do FBI dizem que a agência realizou melhorias, incluindo melhor treinamento, processamento mais rápido de reclamações e exigência de revisão de precisão e completude das indicações à lista por parte dos supervisores dos escritórios regionais.

Quanto mais cedo essas melhorias forem feitas, melhor. No início de 2008, foi revelado que 20 terroristas conhecidos não haviam sido incluídos corretamente na lista de observação. (Não se sabe se esses indivíduos conseguiram entrar nos Estados Unidos.) Em junho de 2009, o TST anunciou que pelo menos seis homens suspeitos de crimes de ameaça à segurança nacional ou por eles processados ainda mantinham suas licenças federais de aviação, inclusive um libanês condenado a 27 anos de prisão pela corte escocesa devido ao atentado ao voo 103 da Pan Am.

Fontes: Eric Lichtblau, "Justice Dept. Finds Flaws in F.B.I. Terror List". *The New York Times*, 7 maio 2009; Spencer S. Hsu, "GAO Cites Gun Sales to Those on Watch List". *The Washington Post*, 23 jun. 2009; Matthew L. Wald, "6 Considered Threats Kept Licenses for Aviation". *The New York Times*, 26 jun. 2009; Bob Egelko, "Watch-list Name Confusion Causes Hardship". *San Francisco Chronicle*, 20 mar. 2008; Siobhan Gorman, "NSA's Domestic Spying Grows as Agency Sweeps Up Data". *The Wall Street Journal*, 10 mar. 2008; Ellen Nakashima, "Reports Cite Lack of Uniform Policy for Terrorist Watch List". *The Washington Post*, 18 mar. 2008; Scott McCartney, "When Your Name is Mud at the Airport". *The Wall Street Journal*, 29 jan. 2008; Audrey Hudson, "Airport Watch List Now Reviewed Often". *The Washington Times*, 11 abr. 2008; Mimi Hall, "Terror Watch List Swells to More Than 755,000". *USA Today*, 23 out. 2007; e "Justice Department Report Tells of Flaws in Terrorist Watch List". CNN.com, 7 set. 2007.

Questões

1. Quais conceitos deste capítulo aparecem neste caso?
2. Por que foi criada lista de terroristas? Quais os benefícios dela?
3. Descreva algumas das fraquezas da lista de observação. Quais fatores humanos, organizacionais e tecnológicos são responsáveis por essas fraquezas?
4. Se você fosse responsável por gerenciar o banco de dados do Centro de Triagem de Terroristas, que medidas tomaria para corrigir algumas de suas fraquezas?
5. Você acredita que a lista de terroristas representa uma ameaça significativa à privacidade dos indivíduos ou aos direitos constitucionais? Justifique.

Referências bibliográficas

CAPPIELLO, Cinzia; FRANCALANCI, Chiara; PERNICI, Barbara. "Time-Related Factors of Data Quality in Multichannel Information Systems". *Journal of Management Information Systems*, v. 20, n. 3, inverno 2004.

CHEN, Andrew N. K.; GOES, Paulo B.; MARSDEN, James R. "A Query-Driven Approach to the Design and Management of Flexible Database Systems". *Journal of Management Information Systems*, v. 19, n. 3, inverno 2002-3.

CLIFFORD, James; CROKER, Albert; TUZHILIN, Alex. "On Data Representation and Use in a Temporal Relational DBMS". *Information Systems Research 7*, n. 3, set. 1996.

ECKERSON, Wayne W. "Data Quality and the Bottom Line". *The Data Warehousing Institute*, 2002.

FAYYAD, Usama; RAMAKRISHNAN, Ramasamy; SRIKANT, Ramakrisnan. "Evolving Data Mining into Solutions for Insights". *Communications of the ACM 45*, n. 8, ago. 2002.

FOSHAY, Neil; MUKHERJEE, Avinandan; TAYLOR, Andrew. "Does Data Warehouse End-User Metadata Add Value?". *Communications of the ACM 50*, n. 11, nov. 2007.

GARTNER Inc. "'Dirty Data' is a Business Problem, not an IT Problem, Says Gartner". Sydney, Austrália, 2 mar. 2007.

HENSCHEN, Doug. "The Data Warehouse Revised". *Information Week*, 26 maio 2008.

HOFFER, Jeffrey A.; PRESCOTT, Mary; TOPPI, Heikki. *Modern Database Management*. 9 ed. Upper Saddle River, NJ: Prentice-Hall, 2009.

KIM, Yong Jin; KISHORE, Rajiv; SANDERS, G. Lawrence. "From DQ to EQ: Understanding Data Quality in the Context of E-Business Systems". *Communications of the ACM 48*, n. 10, out. 2005.

KLAU, Rick. "Data Quality and CRM", Line56.com, accesso em 4 mar. 2003.

KROENKE, David M.; AUER, David. *Database Processing 11e*. Upper Saddle River, NJ: Prentice-Hall, 2010.

LEE, Yang W.; STRONG, Diane M. "Knowing-Why about Data Processes and Data Quality". *Journal of Management Information Systems*, v. 20, n. 3, inverno 2004.

LOVEMAN, Gary. "Diamonds in the Datamine". *Harvard Business Review*, maio 2003.

McKNIGHT, William. "Seven Sources of Poor Data Quality". *Information Management*, abr. 2009.

PIERCE, Elizabeth M. "Assessing Data Quality with Control Matrices". *Communications of the ACM 47*, n. 2, fev. 2004.

REDMAN, Thomas. *Data Driven: Profiting from Your Most Important Business Asset*. Boston: Harvard Business Press, 2008.

SCANLON, Robert J. "A New Route to Performance Management". *Baseline Magazine*, jan./fev. 2009.

WEIER, Mary Hayes. "In Depth: Business Intelligence". *Information Week*, 14 abr. 2008.

Capítulo

6

Telecomunicações, Internet e tecnologia sem fio

OBJETIVOS DE ESTUDO

Ao concluir este capítulo, você será capaz de responder às seguintes perguntas:

1. Quais os principais componentes das redes de telecomunicações e quais as principais tecnologias de rede?
2. Quais os principais meios de transmissão e tipos de rede?
3. Como a Internet e a tecnologia de Internet funcionam e como facilitam a comunicação e o comércio eletrônico?
4. Quais as principais tecnologias e padrões para redes, comunicação e acesso à Internet sem fio?
5. Por que a identificação por radiofrequência (RFID) e as redes de sensores sem fio são tão importantes para as empresas?

PLANO DO CAPÍTULO

Caso de abertura: Aeroporto Internacional de Los Angeles decola com nova tecnologia de redes

Telecomunicações e redes no mundo empresarial de hoje

Redes de comunicação

A Internet global

A revolução sem fio

Projetos práticos em SIG

Resolvendo problemas organizacionais — Google *versus* Microsoft: o confronto dos gigantes da tecnologia

AEROPORTO INTERNACIONAL DE LOS ANGELES DECOLA COM NOVA TECNOLOGIA DE REDES

Atualmente, o que é necessário para ser um aeroporto internacional moderno? O Los Angeles World Airport (LAWA) está tentando responder a essa pergunta. O LAWA é um departamento da Cidade de Los Angeles, Califórnia, que é dono e opera os aeroportos internacionais de Los Angeles e de LA/Ontário; o Aeroporto Van Nuys; o Aeroporto Regional LA/Palmdale. As instalações físicas desses aeroportos e a infraestrutura de TI estavam desatualizadas. A nova geração de aeronaves gigantescas, com asas enormes, não passava na maioria dos portões dos aeroportos do LAWA. Além disso, o departamento precisava de maior poder computacional e de mais recursos de rede para tornar suas operações mais eficientes e convenientes aos viajantes.

Para recuperar sua posição entre os aeroportos internacionais de primeira linha, no final de 2006 o LAWA começou a atualizar tanto as instalações físicas quanto a infraestrutura de TI do Terminal Tom Bradley, pertencente ao Aeroporto Internacional de Los Angeles (LAX). Os projetos estarão concluídos em 2013. O terminal terá seu tamanho quase duplicado, e todo o aeroporto contará com uma nova rede local Ethernet (LAN). A rede do LAX está conectada às redes dos outros aeroportos do LAWA.

A gerência do LAWA deseja disponibilizar sua rede para as 70 companhias aéreas que usam seus aeroportos para que gerem receita adicional e cubram os custos. As companhias aéreas serão cobradas por essas tecnologias conforme o uso que fizerem. As grandes organizações possivelmente continuarão a utilizar suas próprias linhas e redes de telecomunicação, mas muitas companhias pequenas irão optar por utilizar a rede do LAWA para evitar os gastos com aquisição e manutenção de sua própria tecnologia.

Cada vez mais, o LAWA recorre à tecnologia para quase tudo, e a rede sem fio é crucial. A rede sem fio irá se expandir por todos os aeroportos. Pagando uma taxa, os passageiros poderão acessar a Internet de qualquer área pública, desde o meio-fio até o bico da aeronave. Quando os aviões chegarem aos portões, as conexões sem fio podem ser utilizadas para encomendar peças e transmitir instruções ao pessoal de manutenção. Dispositivos móveis sem fio são utilizados no monitoramento e na verificação de bagagens. Dispositivos sem fio denominados COWs (*common use on wheels* — uso comum sobre rodas) podem ser levados até os passageiros que esperam em longas filas para ajudá-los a obter uma passagem ou realizar o check-in. Os COWs conectam-se aos sistemas de uso comum do aeroporto e possuem uma tela para exibição de informações sobre voos. A flexibilidade oferecida pela tecnologia sem fio viabilizou a reorganização das atividades de trabalho de modo a aumentar a eficiência e a assistência ao cliente.

Em maio de 2009, o LAWA lançou um novo site de intranet para seus cerca de 4 mil empregados. A intranet disponibiliza as últimas notícias sobre aeroportos e negócios aéreos, além de salas de bate-papo, blogs e wikis para compartilhamento de conhecimento e experiências. A maioria dos funcionários do LAWA tem acesso à intranet a partir de seus computadores desktop. Aqueles sem um computador desse tipo receberam recentemente uma versão para PDA do site. O LAWA está cogitando a possibilidade de abrir algumas partes de sua intranet para órgãos e intendentes municipais, e talvez grupos comunitários locais que possam se beneficiar com as informações disponibilizadas.

Fontes: Eileen Feretic, "The Future of Flight". *Baseline*, jun. 2009; "CIO Profiles: Dom Nessi: Deputy Executive Director and CIO, Los Angeles World Airports". *Information Week*, 4 maio 2009; e www.airport-la.com, acessado em 12 jul. 2009.

A história do LAWA ilustra alguns dos principais novos recursos e oportunidades oferecidos pela tecnologia de redes atual. O LAWA montou uma poderosa rede local para conectar dispositivos e aeronaves dentro de seus aeroportos, além de uma rede sem fio de suporte a dispositivos sem fio e com acesso à Internet. Essas tecnologias melhoraram os serviços oferecidos aos clientes e aumentaram a eficiência tanto dos aeroportos quanto das aeronaves.

A figura de abertura do caso nos chama a atenção para pontos importantes levantados pelo caso e pelo capítulo. O LAWA precisava competir com outros aeroportos como destino internacional ou ponto de parada para muitas companhias aéreas. Se não atualizasse sua infraestrutura de TI para algo mais moderno, perderia negócios com o número cada vez maior de voos internacionais utilizando aeronaves gigantescas. Sua imagem seria denegrida.

A gerência decidiu expandir os aeroportos e implantar uma nova tecnologia de redes, incluindo uma poderosa rede local, redes sem fio, dispositivos sem fio para check-in e acesso à Internet e uma nova intranet. Essas melhorias tornaram o uso do local mais fácil tanto para os passageiros quanto para as companhias aéreas, economizando tempo e custos operacionais. O LAWA precisou reformular seus processos de bilhetagem e check-in, dentre outros, para tirar proveito da nova tecnologia.

Telecomunicações e redes no mundo empresarial de hoje

Se você é funcionário ou administrador de uma empresa, não consegue fazer praticamente nada sem redes. Você precisa comunicar-se rapidamente com clientes, fornecedores e funcionários. Até 1990, sua comunicação corporativa poderia ser feita pelos sistemas postal ou telefônico por voz ou fax. Hoje, porém, você e seus funcionários usam computadores e e-mail, a Internet, celulares e computadores portáteis conectados a redes sem fio para esse propósito. Atualmente, falar em fazer negócios significa falar em redes e Internet.

Tendências em redes e comunicações

No passado, as empresas usavam dois tipos de redes fundamentalmente diferentes: redes telefônicas e de computadores. Historicamente, as redes telefônicas lidavam com a comunicação por voz, e as redes de computadores se ocupavam do tráfego de dados. As redes telefônicas foram construídas por companhias telefônicas ao longo do século XX usando tecnologias de transmissão de voz (hardware e software); em todo o mundo; essas empresas quase sempre operavam como monopólios regulamentados. As redes de computadores, por sua vez, foram originalmente construídas por empresas de computadores que procuravam transmitir dados entre computadores localizados em lugares diferentes.

Graças à contínua desregulamentação das telecomunicações e à inovação das tecnologias de informação, as redes de computadores e telefones foram pouco a pouco se fundindo em uma única rede digital, que usa os mesmos equipamentos e padrões da Internet. Embora essa transformação ainda não esteja completa, a tendência geral é de convergência entre as redes de computadores e telefones. Empresas de telecomunicações como a AT&T e a Verizon hoje oferecem transmissão de dados, acesso à Internet, serviço telefônico sem fio e programas de televisão, além de serviço de voz. Empresas de comunicação a cabo como a Cablevision, a Comcast e a Net hoje disponibilizam serviços de voz e acesso à Internet. As redes de computadores expandiram-se a ponto de incluir a telefonia por Internet e alguns serviços de vídeo. E, cada vez mais, todas essas comunicações de dados, vídeo e voz utilizam tecnologia de Internet.

Tanto as redes de comunicação de dados quanto as de voz também vêm se tornando mais poderosas (rápidas), portáteis (menores e móveis) e baratas. Por exemplo, em 2000, a velocidade de conexão à Internet típica era de 56 quilobits por segundo, enquanto hoje mais de 60 por cento dos usuários de Internet nos Estados Unidos contam com conexões de **banda larga** de alta velocidade, proporcionadas por companhias telefônicas e de TV a cabo, que

rodam de 1 milhão a 15 milhões de bits por segundo. O custo por quilobit de comunicação caiu exponencialmente, de 25 centavos de dólar em 2000 para menos de 1 centavo de dólar atualmente.

Cada vez mais, a comunicação de dados e voz, assim como o acesso à Internet, ocorre sobre plataformas sem fio de banda larga, como celulares, dispositivos digitais de mão e PCs em rede sem fio. Em poucos anos, mais da metade dos usuários de Internet nos Estados Unidos utilizarão smartphones e netbooks/tablets portáteis para acesso à rede. Em 2009, 73 milhões de norte-americanos acessaram a Internet através de dispositivos móveis e espera-se que esse número dobre em 2013 (eMarketer, 2009).

O que é uma rede de computadores?

Se precisar conectar os computadores de dois ou mais funcionários no mesmo escritório, você necessitará de uma rede de computadores. Mas o que é exatamente uma rede? Na sua forma mais simples, uma rede consiste em dois ou mais computadores conectados. A Figura 6.1 ilustra os principais componentes de hardware, software e transmissão usados em uma rede simples: um computador cliente e um computador servidor dedicado, interfaces de rede, um meio de conexão, software de sistema operacional de rede, um hub (ou concentrador) ou um switch (ou comutador).

Cada computador na rede contém um dispositivo de interface de rede chamado **cartão de interface de rede (NIC — *network interface card*)**. Hoje em dia, a maioria dos computadores pessoais traz esse cartão embutido na placa-mãe. O meio de conexão para interligar os componentes de rede pode ser um fio telefônico, um cabo coaxial ou sinais de rádio, no caso de celulares e redes locais sem fio (Wi-Fi).

O **sistema operacional de rede (NOS — *networking operating system*)** encaminha e administra comunicações e coordena os recursos de rede. Esse sistema pode residir em todos os computadores da rede ou em um único servidor designado para todas as aplicações. Dentro de uma rede, um computador servidor é um computador que realiza importantes funções de rede para computadores clientes, tais como mostrar páginas da Web, armazenar os dados e o sistema operacional de rede (e, assim, controlar a rede). Softwares de servi-

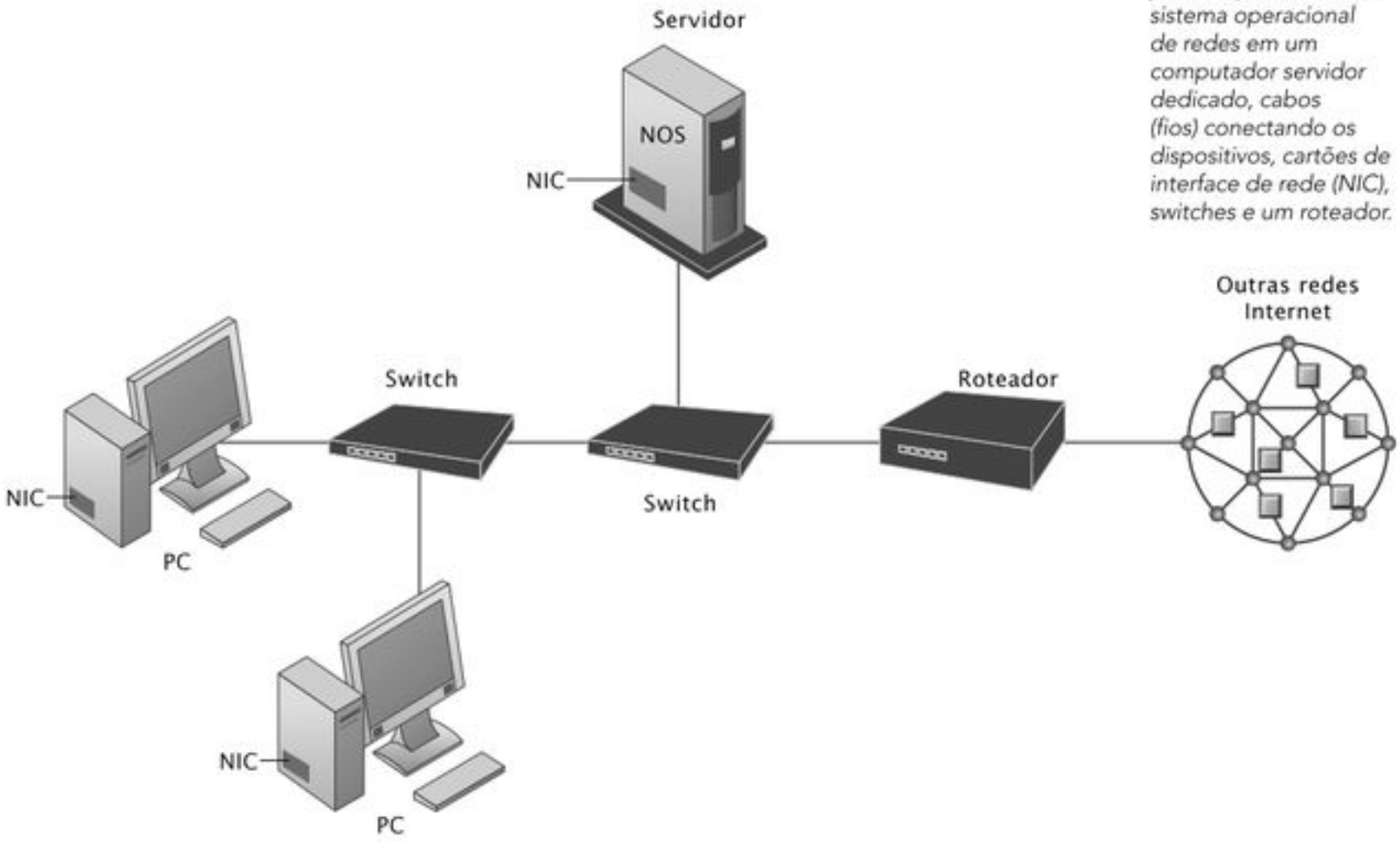


Figura 6.1

Componentes de uma rede de computadores simples

Ilustramos aqui uma rede de computadores muito simples, composta por computadores, um sistema operacional de redes em um computador servidor dedicado, cabos (fios) conectando os dispositivos, cartões de interface de rede (NIC), switches e um roteador.

dor — como Microsoft Windows Server, Linux e Novell Open Enterprise Server — são os sistemas operacionais de redes mais amplamente utilizados.

A maioria das redes também conta com um switch ou um hub que atua como ponto de conexão entre os computadores. Os **hubs** são dispositivos muito simples que conectam os componentes de rede, enviando um pacote de dados para todos os outros dispositivos conectados. O **switch** é mais inteligente que um hub, pois pode filtrar e repassar dados para um destinatário específico.

Para se comunicar com outra rede, tal como a Internet, a rede costuma usar um dispositivo chamado roteador. Um **roteador** é um processador de comunicações especial usado para encaminhar pacotes de dados através de diferentes redes, assegurando que a mensagem enviada chegue ao endereço correto.

Redes em grandes empresas

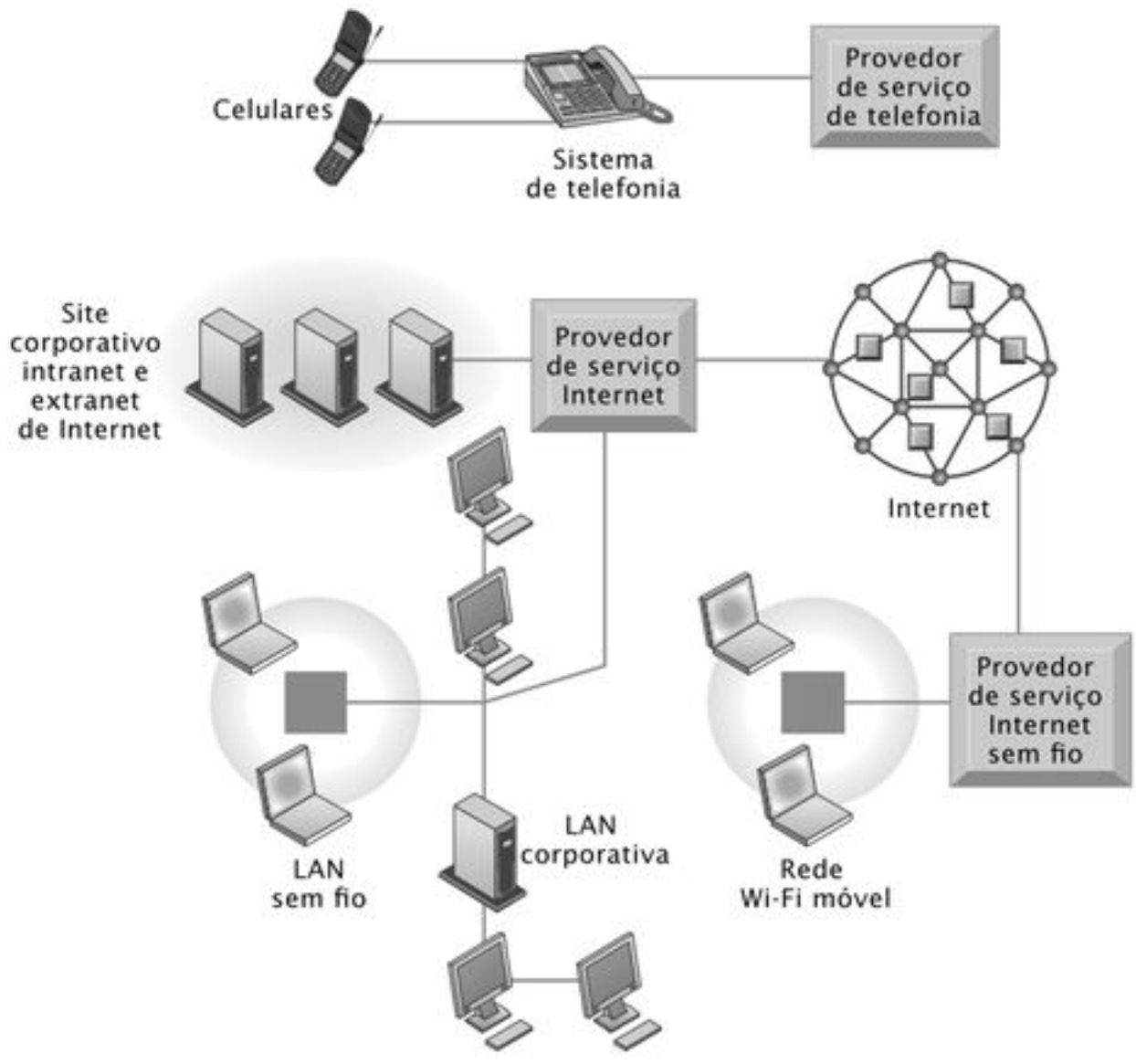
A rede que acabamos de descrever pode ser adequada a uma pequena empresa. Mas como ficam as grandes corporações, com inúmeras filiais e milhares de funcionários? À medida que uma empresa cresce, vai aglutinando centenas de pequenas redes locais (LANs), que podem ser unidas facilmente em uma infraestrutura de rede corporativa. A infraestrutura de rede para uma grande organização consiste em um grande número de pequenas redes locais conectadas a outras redes locais e a redes corporativas que abrangem toda a empresa. Uma série de servidores potentes é utilizada para comportar um site corporativo, uma intranet corporativa e às vezes uma extranet. Alguns desses servidores podem também estar conectados a outros computadores de grande porte, a fim de atender aos sistemas de *back-end*.

A Figura 6.2 oferece um exemplo dessas redes corporativas de maior escala e complexidade. No exemplo, você pode ver que a infraestrutura de rede corporativa comporta uma força de vendas móvel que usa celulares; funcionários fora da empresa mas conectados ao site corporativo, ou redes corporativas internas que usam redes locais sem fio móveis (Wi-Fi); e um sistema de videoconferência que os gerentes podem usar ao redor do mundo. Além dessas redes de computadores, toda a organização de uma empresa normalmente

Figura 6.2

Infraestrutura de rede corporativa

É, atualmente, um conjunto de muitas redes diferentes: desde a rede de telefonia comutada pública até a Internet e as redes locais corporativas que conectam grupos de trabalho, departamentos ou escritórios.



inclui uma rede separada de telefonia, que lida com a maior parte dos dados de voz. Muitas empresas estão abandonando suas redes telefônicas tradicionais e usando telefones por Internet (VoIP), que rodam na rede de dados preexistente (esses sistemas serão descritos mais adiante).

Como é possível perceber na figura, essa infraestrutura usa uma ampla variedade de tecnologias, desde redes de dados corporativas e serviço de telefonia tradicional até serviço de Internet, Internet sem fio e celulares sem fio. Um dos principais problemas que as empresas enfrentam atualmente é como integrar todos esses canais e redes de comunicação diferentes em um sistema coerente, que permita o fluxo de informação de uma parte da empresa a outra e de um sistema a outro. À medida que as redes de comunicação se tornam digitais e baseadas em tecnologia de Internet, passa a ser mais fácil integrá-las.

Principais tecnologias de rede digital

As redes digitais contemporâneas e a Internet se baseiam em três principais tecnologias: computação cliente/servidor, uso de comutação de pacotes e desenvolvimento de padrões de comunicação amplamente usados (o mais importante deles é o *Transmission Control Protocol/Internet Protocol* [TCP/IP]) para conectar redes e computadores diferentes.

Computação cliente/servidor

No Capítulo 5, apresentamos a **computação cliente/servidor**, na qual computadores clientes são conectados a uma rede com um ou mais computadores servidores. A computação cliente/servidor é um modelo de computação distribuída em que uma parcela do poder de processamento fica dentro de pequenos e baratos computadores clientes, sob controle do usuário, e literalmente reside em computadores de mesa, laptops e dispositivos de mão. Esses poderosos clientes estão conectados uns aos outros por meio de uma rede controlada por um computador servidor de rede. O servidor estabelece as regras de comunicação para a rede e fornece a cada cliente um endereço, de maneira que os outros possam localizá-lo na rede.

A computação cliente/servidor vem substituindo em grande medida a computação centralizada em mainframes, na qual praticamente todo o processamento ocorre em um grande computador mainframe central. A computação cliente/servidor levou a informática a departamentos, grupos de trabalho, chão de fábrica e outras partes da empresa que não poderiam ser atendidas por uma arquitetura centralizada. A Internet é o maior exemplo de computação cliente/servidor.

Comutação de pacotes

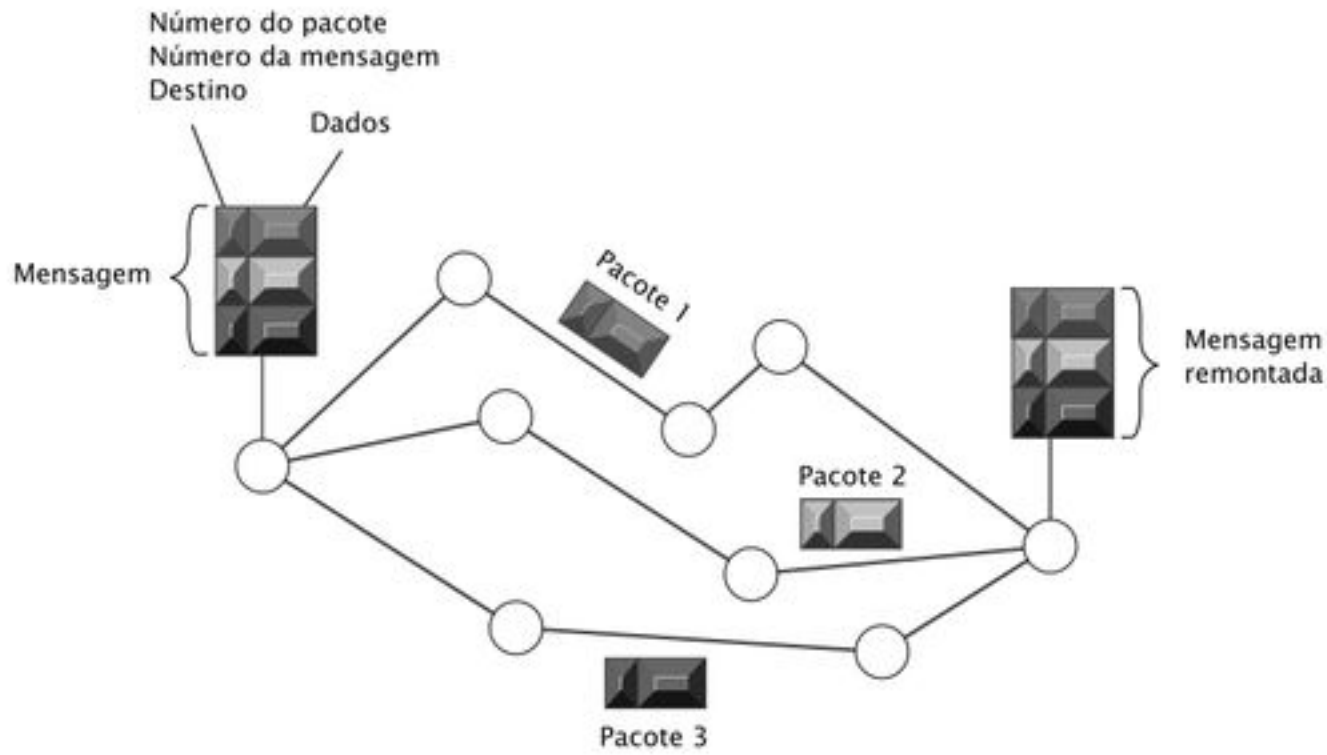
A **comutação de pacotes** é um método que consiste em fragmentar mensagens digitais em pequenos pacotes, enviar esses pacotes por vias de comunicação diferentes à medida que eles são disponibilizados e, depois, remontá-los quando chegarem ao seu destino (veja a Figura 6.3). Antes do desenvolvimento da comutação de pacotes, as redes de computadores usavam circuitos telefônicos arrendados e dedicados à comunicação com outros computadores distantes. Em redes comutadas por circuito, como o sistema de telefonia, um circuito completo ponto a ponto é montado e, então, a comunicação pode seguir em frente. Essas onerosas técnicas de comutação por circuito desperdiçavam a capacidade de comunicação disponível, pois o circuito era mantido independentemente de sua utilização.

A comutação de pacotes torna o uso da capacidade de comunicação da rede muito mais eficiente. Em redes comutadas por pacote, as mensagens são fragmentadas em pequenos feixes de dados de tamanho fixo chamados 'pacotes'. O tamanho dos pacotes varia muito, dependendo do padrão de comunicação em uso. Os pacotes incluem informações para dirigi-los ao endereço correto e verificar erros de transmissão com os dados. Os pacotes são transmitidos via vários canais de comunicação utilizando roteadores, cada um trafegando independentemente pela rede. Pacotes de dados originários de uma fonte podem ser roteados por trajetos diferentes da rede antes de serem remontados como a mensagem original ao chegarem ao seu destino.

Figura 6.3

Redes de comutação de pacotes

Os dados são agrupados em pequenos pacotes, transmitidos de modo independente via vários canais de comunicação e remontados no destino final.



TCP/IP e conectividade

Em uma rede de telecomunicações típica, diversos componentes de hardware e software precisam trabalhar juntos para transmitir informações. Para se comunicar, os diferentes componentes da rede simplesmente aderem a um conjunto comum de regras chamado protocolo. **Protocolo** é um conjunto de regras e procedimentos que comanda a transmissão de informações entre dois pontos de uma rede.

No passado, a existência de muitos protocolos proprietários e incompatíveis muitas vezes forçava as empresas a adquirir equipamentos de comunicação e informática de um único fornecedor. Hoje, porém, as redes corporativas cada vez mais utilizam um padrão único, universal e comum chamado **Transmission Control Protocol/Internet Protocol (TCP/IP)**. O TCP/IP foi desenvolvido no início da década de 1970 como ferramenta da Agência de Pesquisas Avançadas do Departamento de Defesa dos Estados Unidos (DARPA) para ajudar cientistas a transmitir dados entre computadores de diferentes tipos e a longas distâncias.

O TCP/IP usa um conjunto de protocolos. Os principais são o TCP e o IP. *TCP* significa *Transmission Control Protocol* (TCP), o qual lida com o movimento de dados entre os computadores. O TCP estabelece uma conexão entre os computadores, sequencia a transferência de pacotes e reconhece os pacotes enviados. *IP* significa *Internet Protocol* (IP), responsável pela entrega dos pacotes e inclui a desmontagem e a remontagem dos pacotes durante a transmissão. A Figura 6.4 ilustra o modelo de referência, com quatro camadas, do Departamento de Defesa para o TCP/IP.

1. *Camada de aplicação*: a camada de aplicação permite aos programas aplicativos clientes acessar as outras camadas, e define os protocolos utilizados para intercambiar dados. Um desses protocolos de aplicação é o Hypertext Transfer Protocol (HTTP), usado para transferir arquivos de páginas Web.
2. *Camada de transporte*: a camada de transporte é responsável por fornecer à camada de aplicação serviços de empacotamento e comunicação. Essa camada inclui o TCP e outros protocolos.
3. *Camada de Internet*: a camada de Internet é responsável por endereçar, rotear e empacotar pacotes de dados chamados datagramas IP. O Internet Protocol é um dos protocolos usados nessa camada.
4. *Camada de interface de rede*: situada na base do modelo de referência, a camada de interface de rede é responsável por receber os pacotes de quaisquer meios de rede físicos e colocá-los nesses mesmos meios.

Dois computadores usando TCP/IP podem comunicar-se, mesmo que estejam baseados em plataformas de hardware e software diferentes. Dados enviados de um computador para

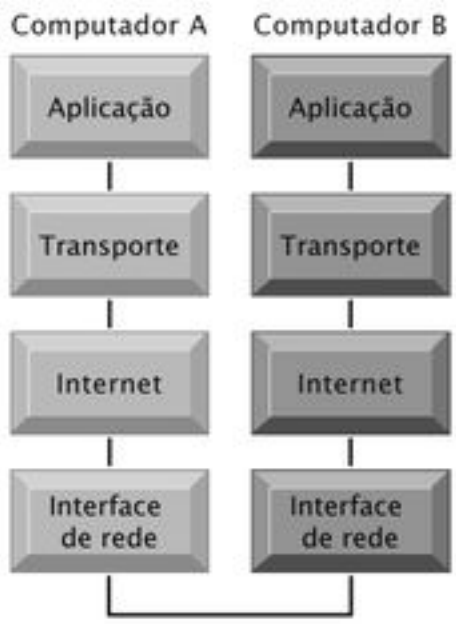


Figura 6.4

Modelo de referência do Transmission Control Protocol/Internet Protocol (TCP/IP)

A figura ilustra as quatro camadas do modelo de referência TCP/IP para comunicações.

outro seguem para baixo e atravessam todas as quatro camadas, começando pela camada de aplicação do computador remetente e passando pela camada de interface de rede. Após os dados alcançarem o computador hospedeiro receptor, eles viajam para cima pelas camadas e são remontados em um formato que o computador receptor possa usar. Se este encontrar um pacote danificado, solicitará ao computador remetente que o retransmita. Esse processo será revertido quando o computador receptor emitir uma resposta.

Redes de comunicação

Vamos olhar mais de perto as diversas tecnologias e arranjos de rede disponíveis para as empresas.

Sinais: digital *versus* analógico

Existem duas maneiras de enviar uma mensagem em uma rede: utilizando um sinal analógico ou um digital. Um *sinal analógico* é representado por uma onda contínua que passa por um meio de comunicação e tem sido utilizado para transmissões de voz. Os dispositivos analógicos mais comuns são o aparelho telefônico, o alto-falante do computador ou o fone de ouvido do iPod — todos eles criam ondas analógicas que podem ser captadas pelos ouvidos.

Um *sinal digital* é uma onda de forma discreta, não contínua. Transmite dados codificados em dois estados discretos: bits 1 e bits 0, representados como pulsos elétricos ativos e inativos. Como os computadores se comunicam por sinais digitais, se alguém quiser usar o sistema telefônico analógico para enviar dados digitais, precisará de um dispositivo chamado **modem** para converter sinais digitais no formato analógico (veja a Figura 6.5). *Modem* é a abreviatura de modulação/demodulação. Modems a cabo conectam seu computador à Internet utilizando uma rede a cabo. Modems DSL conectam seu computador à Internet por meio de rede telefônica de uma empresa de telefonia. Modems sem fio executam a mesma função que um modem tradicional, conectando seu computador a uma rede sem fio que pode ser a de seu celular ou uma rede Wi-Fi. Sem os modems, os computadores não poderiam se comunicar uns com os outros através de redes analógicas (que incluem os sistemas telefônicos e as redes a cabo).

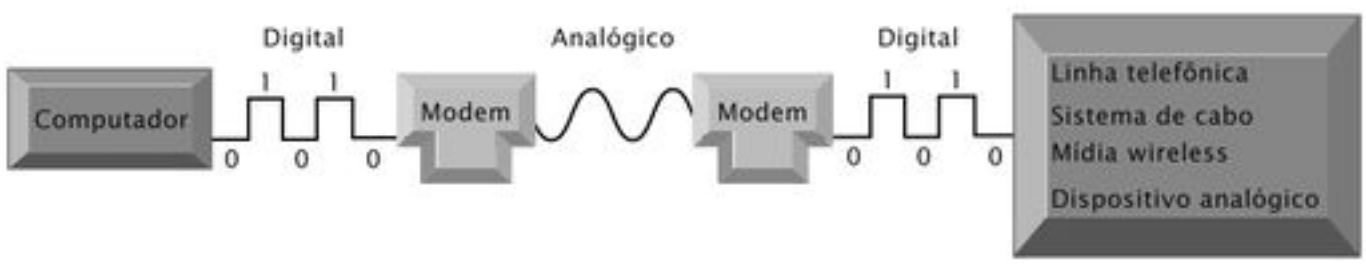


Figura 6.5

Funções do modem

Modem é um dispositivo que converte os sinais digitais de um computador para a forma analógica, de modo que possam ser transmitidos por linhas telefônicas analógicas. Também é utilizado para reconverter sinais analógicos em digitais, para serem recebidos por um computador.

Tipos de rede

Existem muitos tipos de rede e várias maneiras de classificá-los. Podemos, por exemplo, analisar as redes em termos de seu alcance geográfico (ver Tabela 6.1).

Redes locais

Se trabalha em uma empresa que utiliza redes, provavelmente está conectado a outros funcionários e grupos por meio de redes locais. Uma **rede local (LAN — *local-area network*)** é projetada para conectar computadores pessoais e outros dispositivos digitais em um raio de 500 metros. Normalmente, as LANs conectam alguns computadores em um escritório pequeno, todos os computadores de um edifício ou todos os computadores em muitos edifícios próximos. As LANs interconectadas dentro de vários edifícios ou em determinada área geográfica, como um *campus* universitário ou uma base militar, criam uma **rede de *campus* (CAN — *campus-area network*)**. As LANs podem estar ligadas a redes remotas de longa distância (WANs, descritas adiante nesta seção) e outras redes ao redor do mundo por meio da Internet.

Reveja a Figura 6.1, que poderia servir como modelo para uma pequena LAN a ser usada em um escritório. Um dos computadores é um servidor de arquivos de rede dedicado, que dá aos usuários acesso aos recursos computacionais compartilhados da rede, entre os quais programas de software e arquivos de dados. O servidor determina quem tem acesso a quê e em qual sequência. O roteador conecta a LAN a outras redes, que podem ser a Internet ou outra rede corporativa, de maneira que a LAN possa trocar informações com redes externas a ela. Os sistemas operacionais de LAN mais comuns são Windows, Linux e Novell. Em todos eles, o protocolo de rede padrão é o TCP/IP.

Ethernet é o padrão de LAN dominante na rede física. Ele especifica o meio físico que transportará os sinais entre os computadores, as regras de controle de acesso e uma estrutura padronizada, ou um conjunto de bits usados para transportar os dados através do sistema. Originalmente, o Ethernet comportava uma taxa de transferência de dados de 10 megabits por segundo. Versões mais recentes, como o Fast Ethernet e o Gigabit Ethernet, comportam taxas de transmissão de dados de 100 megabits por segundo e 1 gigabit por segundo, respectivamente, e são utilizadas em backbones de rede.

A LAN ilustrada na Figura 6.1 usa uma arquitetura cliente/servidor, em que o sistema operacional de rede reside primordialmente em um único servidor de arquivos, e o servidor provê a maior parte do controle e dos recursos da rede. Alternativamente, as LANs podem usar uma arquitetura ***peer-to-peer* (ponto a ponto)**. Uma rede *peer-to-peer* trata todos os processadores da mesma maneira e é utilizada, sobretudo, em pequenas redes, com no máximo dez usuários. Os vários computadores da rede podem intercambiar dados por acesso direto, assim como compartilhar dispositivos periféricos, sem ter de passar por um servidor independente.

Em LANs equipadas com os sistemas operacionais da família Windows Server, a arquitetura *peer-to-peer* é denominada *modelo de rede de grupo de trabalho*, um modelo em que um pequeno grupo de computadores pode compartilhar recursos, como arquivos, pastas e impressoras, pela rede, sem a necessidade de um servidor dedicado. O *modelo de rede de domínio* do Windows, em contrapartida, usa um servidor dedicado para gerenciar os computadores da rede.

Tabela 6.1 Tipos de rede

Tipo	Áreas
Rede local (LAN)	Até 500 metros; um escritório ou andar de edifício
Rede de *campus* (CAN)	Até 1 quilômetro; um *campus* de faculdade ou as instalações de uma empresa
Rede metropolitana (MAN)	Uma cidade ou área metropolitana
Rede remota (WAN)	Área transcontinental ou global

LANs maiores têm muitos clientes e inúmeros servidores, com servidores independentes para serviços específicos, tais como armazenamento e gestão de arquivos e bancos de dados (servidores de arquivos ou servidores de bancos de dados), gestão de impressoras (servidores de impressoras), armazenamento e gestão de e-mail (servidores de e-mail) ou armazenamento e gestão de páginas da Web (servidores da Web).

As LANs às vezes são descritas segundo o modo pelo qual os componentes estão conectados, ou segundo sua **topologia**. As três topologias de LAN mais comuns são estrela, barramento e anel (veja a Figura 6.6).

Na **topologia em estrela**, todos os dispositivos da rede estão conectados a um único hub. A Figura 6.6 ilustra uma **rede em estrela** simples, na qual todos os componentes de rede estão conectados a um único hub. Todo o tráfego da rede flui através desse hub. Na *rede em estrela estendida*, hubs ou camadas múltiplas estão organizados em uma hierarquia.

Na **topologia em barramento**, uma estação transmite sinais que viajam em ambas as direções ao longo de um único segmento de transmissão. Todos os sinais são transmitidos em ambas as direções para toda a rede. Todas as máquinas da rede recebem os mesmos sinais, e o software instalado nas máquinas clientes permite que cada uma 'escute' as mensagens endereçadas especificamente a ela. **Redes em barramento** são a topologia Ethernet mais comum.

A **topologia em anel** conecta os componentes de rede em um círculo fechado. As mensagens passam de um computador para outro em uma única direção ao longo do círculo, e apenas uma estação de cada vez pode transmitir dados. **Redes em anel** são utilizadas majoritariamente em LANs mais antigas, que usam o software de rede Token Ring.

Redes remotas e metropolitanas

Redes remotas (WANs — *wide-area networks*) abrangem grandes distâncias geográficas — regiões, estados, continentes ou até o planeta. A WAN mais potente e universal é a Internet. Os computadores conectam-se a uma WAN através de redes públicas, como o sistema telefônico, sistemas de cabo privados ou através de linhas e satélites alugados. Uma **rede metropolitana (MAN — *metropolitan-area network*)** é uma rede que abrange uma área metropolitana, normalmente uma cidade e seus arredores. Seu alcance geográfico fica entre o de uma WAN e o de uma LAN.

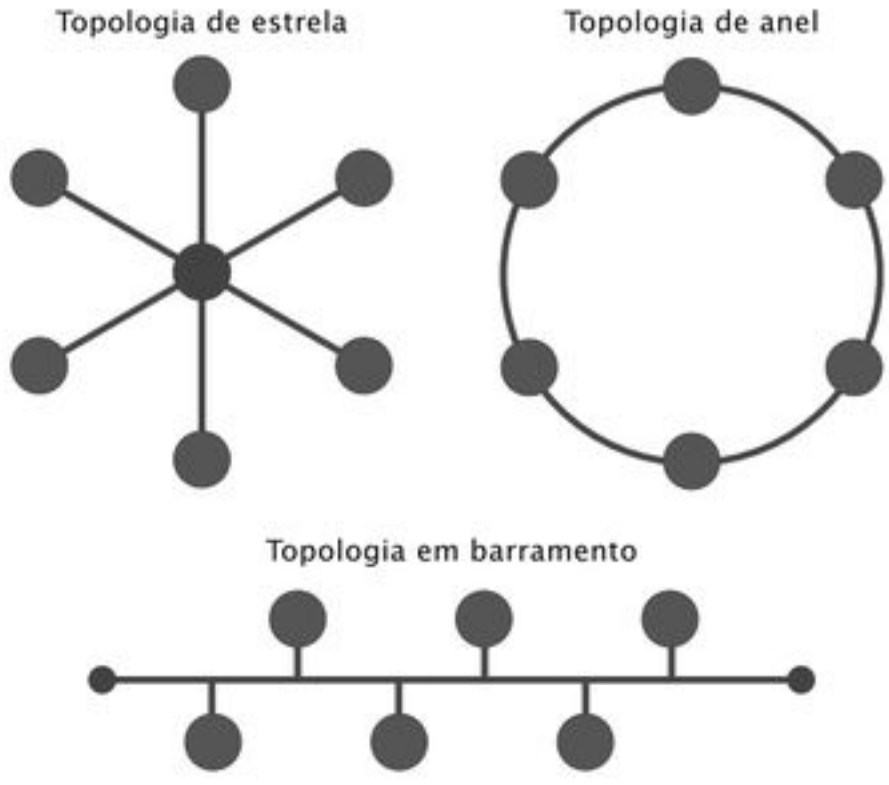


Figura 6.6

Topologias de rede

As três topologias de rede básica são estrela, anel e barramento.

Meios de transmissão física

As redes usam diferentes tipos de meios de transmissão física, incluindo par trançado, cabo coaxial, fibra óptica e meios de transmissão sem fio. Cada um deles tem suas vantagens e limitações. Cada meio também permite ampla gama de velocidades, conforme a configuração de hardware e software utilizada.

Par trançado

O **par trançado** é um meio de transmissão mais antigo que consiste em fios de cobre trançados aos pares. Grande parte dos sistemas telefônicos dos edifícios baseia-se em pares trançados, instalados para processar comunicação analógica, mas que também podem ser usados para comunicações digitais. Embora seja um meio de transmissão física antigo, os pares trançados atualmente instalados em redes locais, como o CAT5, podem alcançar velocidades de até 1 Gbps. Recomenda-se que o cabeamento utilizado nesse tipo de tecnologia fique limitado a uma extensão máxima de 100 metros.

Cabo coaxial

O **cabo coaxial**, semelhante ao utilizado para televisão a cabo, consiste em um fio de cobre isolado e de grande espessura, que pode transmitir um volume de dados maior do que o par trançado. O cabo coaxial foi utilizado nas primeiras redes locais e ainda é usado para longas extensões (mais de 100 metros) em grandes edifícios. Este cabo atinge velocidades superiores a 1 Gbps.

Fibras e redes ópticas

Cabos de fibra óptica são filamentos de fibra óptica transparente, cada um com a espessura de um fio de cabelo, reunidos em cabos. Os dados são transformados em pulsos de luz, que são enviados pelo cabo por um dispositivo a laser, a uma taxa que varia de 500 quilobits a vários trilhões de bits por segundo em ambientes experimentais. O cabo de fibra óptica é consideravelmente mais veloz, mais leve e mais durável do que os meios com fios metálicos, sendo mais adequado a sistemas que exigem transferência de grandes volumes de dados. Por outro lado, é mais difícil trabalhar com cabos de fibra óptica, pois são mais caros e exigem uma instalação mais complexa.

Até há pouco tempo, os cabos de fibra óptica eram usados primeiramente para o backbone de redes de alta velocidade, que gerenciam o tráfego principal. Atualmente, empresas de telefonia celular, como a Verizon, estão começando a instalar linhas de fibra óptica em residências para oferta de novos tipos de serviços, como o serviço de Internet FiOS, da Verizon, que oferece velocidades de download de até 50 Mbps.

Meios de transmissão sem fio

A transmissão sem fio baseia-se em sinais de rádio de frequência variada. Existem três tipos de redes sem fio utilizadas por computadores: micro-ondas, celular e sem fio. Sistemas de **micro-ondas**, tanto terrestres quanto espaciais, transmitem sinais de rádio de alta frequência pela atmosfera e são amplamente utilizados para comunicação ponto a ponto de alto volume e longa distância. Os sinais de micro-ondas seguem uma linha reta e não acompanham a curvatura da Terra; portanto, os sistemas terrestres de transmissão de longa distância requerem estações de retransmissão posicionadas a intervalos de 40 a 50 quilômetros. A transmissão de longa distância também é possível rebatendo-se os sinais de micro-ondas a partir de satélites equipados para servir como estações de retransmissão de sinais de micro-ondas.

Os satélites utilizam transmissão por micro-ondas e são comumente utilizados para comunicações entre grandes empresas dispersas geograficamente, as quais seria difícil interligar por meios cabeados ou por micro-ondas terrestres, e também para serviços de Internet residenciais, em especial nas áreas rurais. Por exemplo, a BP p.l.c. utiliza satélites para transferência, em tempo real, de dados de exploração de campos petrolíferos coletados em pesquisas no fundo do oceano. Navios de exploração transferem esses dados por satélites geossíncronos a centrais de computação nos Estados Unidos para utilização dos

pesquisadores em Houston, Tulsa, e na área suburbana de Chicago. A Figura 6.7 mostra como o sistema funciona. Os satélites também são utilizados em televisões domésticas e serviços de Internet. Nos Estados Unidos, os principais provedores de Internet via satélite (Dish Network e DirectTV) possuem cerca de 30 milhões de assinantes, e aproximadamente 17 por cento de todas as famílias norte-americanas acessam a Internet utilizando serviços via satélite (eMarketer, 2009).

Os sistemas celulares também utilizam ondas de rádio e uma variedade de protocolos diferentes para se comunicar com antenas (torres) localizadas em áreas próximas, denominadas *células*. Comunicações transmitidas através de um **telefone celular** são transmitidas à célula local pelo celular e em seguida passadas de uma antena a outra — de uma célula a outra — até chegar a seu destino final.

As redes sem fio estão substituindo as cabeadas tradicionais em muitas aplicações, além de criar novas aplicações, serviços e modelos de negócio. Na Seção 6.4, temos uma descrição detalhada das aplicações e dos padrões tecnológicos que estão conduzindo essa 'revolução sem fio'.

Velocidade de transmissão

A quantidade de informações que pode ser transmitida por qualquer canal de telecomunicações é medida em bits por segundo (bps). É necessária uma mudança de sinal, ou ciclo, para transmitir um ou vários bits por segundo; portanto, a capacidade de transmissão de cada tipo de meio de telecomunicação depende de sua frequência. O número de ciclos por segundo que pode ser enviado é medido em **hertz** — um hertz equivale a um ciclo do meio de comunicação.

A faixa de frequências que pode ser acondicionada em determinado canal de comunicação chama-se **largura de banda**. A largura de banda é a diferença entre as frequências mais baixa e mais alta que podem ser acondicionadas em um único canal. Quanto maior a faixa de frequências, maior a largura de banda e a capacidade de transmissão do meio. A Tabela 6.2 compara a velocidade de transmissão dos principais tipos de meio.

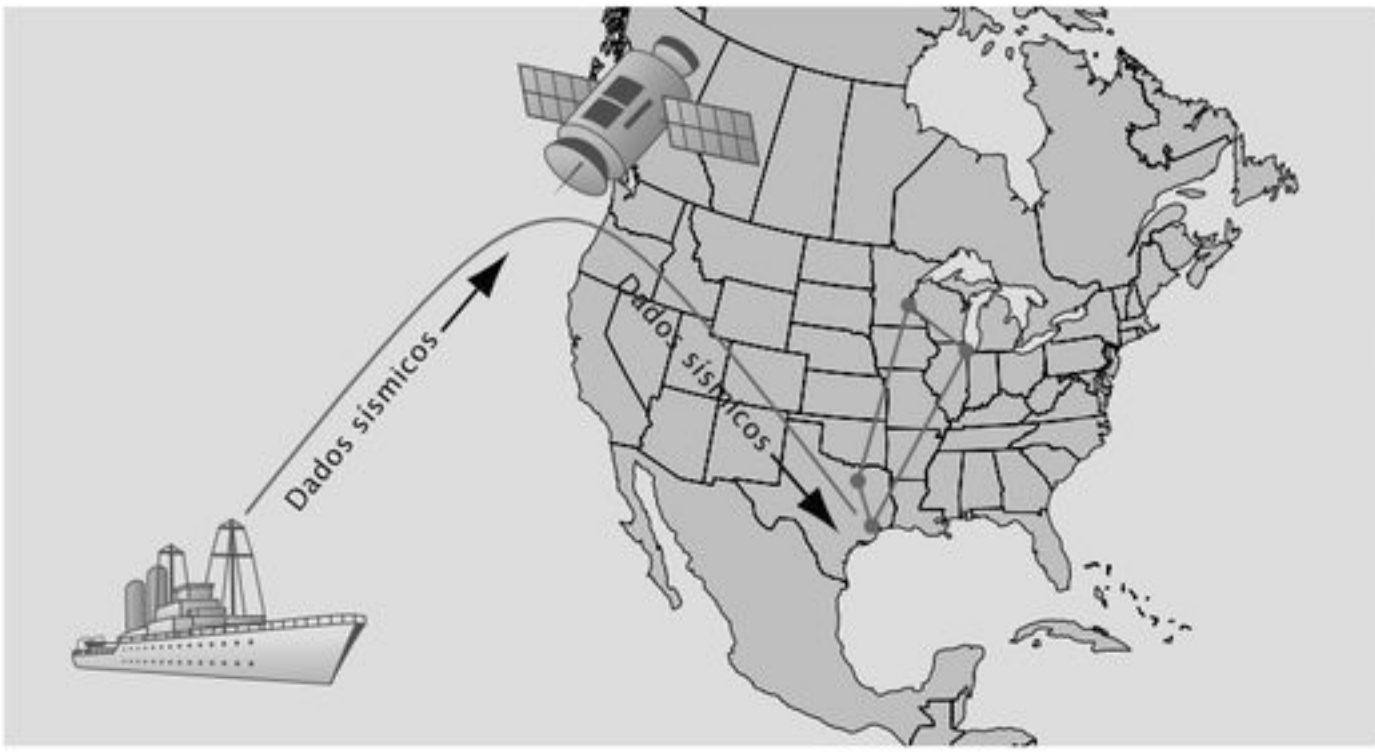


Figura 6.7

Sistema de transmissão por satélite da BP

Satélites ajudam a BP a transferir dados sísmicos entre navios de exploração petrolífera e centros de pesquisa nos Estados Unidos.

Tabela 6.2 **Velocidades típicas dos meios de transmissão de telecomunicação**

Meio	Velocidade
Par trançado (não blindado)	Até 100 Mbps
Micro-ondas	Até 600 + Mbps
Satélite	Até 600 + Mbps
Cabo coaxial	Até 1 Gbps
Cabo de fibra óptica	Até 6 + Tbps

Mbps = megabits por segundo
Gbps = gigabits por segundo
Tbps = terabits por segundo

A Internet global

Todos nós a usamos, e muitos de nós acreditamos que não poderíamos viver sem ela. A Internet se tornou de fato uma ferramenta profissional e pessoal indispensável. Mas o que é exatamente a Internet? Como funciona e o que a tecnologia de Internet tem a oferecer às empresas? Vamos analisar os atributos mais importantes para as empresas.

O que é Internet?

A Internet se tornou o sistema de comunicação público mais abrangente e, hoje, rivaliza com o sistema telefônico global em alcance e amplitude. É também o maior exemplo de redes interconectadas e computação cliente/servidor no mundo, conectando centenas de milhares de redes individuais em todo o planeta. Essa gigantesca rede começou no início da década de 1970 como uma rede do Departamento de Defesa dos Estados Unidos para conectar cientistas e professores universitários ao redor do mundo.

A maioria das residências conecta-se à Internet por meio de um provedor de serviços de Internet, ao qual paga uma assinatura. Um **provedor de serviços de Internet** (**ISP** — ***Internet service provider***) é uma organização comercial com conexão permanente com a rede que vende conexões temporárias a assinantes. Net, Telefonica e AT&T são ISPs. As pessoas também podem conectar-se à Internet por meio de suas empresas, universidades ou centros de pesquisa com domínios próprios.

Existe uma série de provedores de serviços de Internet. A conexão através de uma linha telefônica tradicional e um modem, a uma velocidade de 56,6 quilobits por segundo (Kbps), costumava ser a forma mais comum de conexão ao redor do mundo, mas está sendo rapidamente substituída por conexões banda larga. Conexões via linha digital de assinante (DSL), cabo e satélite e linhas T oferecem esses serviços de banda larga.

As tecnologias de **linha digital de assinante (DSL)** também operam por linhas telefônicas preexistentes, transportando voz, dados e vídeo, mas com capacidade de transmissão que variam de 385 Kbps a 9 megabits por segundo. Proporcionadas por fornecedores de televisão a cabo, as **conexões de Internet a cabo** usam linhas coaxiais a cabo digitais para prover acesso de alta velocidade à Internet a empresas e residências. Podem proporcionar acesso à Internet a mais de 10 megabits por segundo. Nas áreas nas quais os serviços DSL e a cabo não estão disponíveis, é possível acessar a Internet via satélite, embora algumas conexões via Internet apresentem velocidades de *upload* inferiores às dos serviços de banda larga.

T1 e T3 são padrões de telefonia internacionais para comunicações digitais. São linhas concedidas dedicadas ideais para empresas e agências governamentais com requisitos de nível de serviço garantido. As **linhas T1** oferecem uma taxa de transmissão garantida de 1,54 megabit por segundo, enquanto as linhas T3 garantem uma taxa de 45 megabits por segundo.

Arquitetura e endereçamento da Internet

A Internet está baseada no pacote de protocolo de rede TCP/IP descrito anteriormente neste capítulo. Todos os computadores na Internet recebem um único **endereço IP (Internet Protocol)**, que é atualmente o número de 32 bits representado por quatro séries de números que vão de 0 a 255 e são separados por pontos. O endereço de www.microsoft.com, por exemplo, é 207.46.250.119.

Quando um usuário envia uma mensagem a outro usuário da Internet, a mensagem é decomposta em pacotes por meio do protocolo TCP. Cada pacote contém seu endereço de destino. Os pacotes são então enviados do cliente para o servidor de rede e, de lá, para quantos servidores forem necessários até chegar ao computador específico com um endereço conhecido. No endereço de destino, os pacotes são remontados de modo a formar a mensagem original.

O sistema de nomes de domínio

Seria absurdamente difícil para os usuários da Internet lembrar sequências de 12 números, por isso um **Sistema de Nomes de Domínio (*Domain Name System* — DNS)** converte os endereços IP em nomes de domínio. **Nome de domínio** é o termo que corresponde, em nosso idioma, ao endereço IP de 32 bits exclusivo de cada computador conectado à Internet. Os servidores DNS mantêm o banco de dados com os endereços IP mapeados para os seus nomes de domínio correspondentes. Para acessar um computador na Internet, os usuários precisam apenas especificar seu nome de domínio.

O DNS tem uma estrutura hierárquica (veja a Figura 6.8). No topo da hierarquia DNS está o domínio-raiz. Os domínios dos dois níveis seguintes são denominados domínios de primeiro nível e de segundo nível.

Domínios de primeiro nível são nomes com dois ou três caracteres com os quais você está familiarizado por navegar na Web — por exemplo, .com, .edu, .gov, e os diversos códigos de país, tais como .ca para Canadá ou .it para Itália. Domínios de segundo nível possuem duas partes, designando o nome de primeiro nível e o nome de segundo nível — tais como buy.com, nyu.edu ou amazon.ca. Um nome de hospedeiro na base da hierarquia designa um computador específico, seja na Internet ou em uma rede privada.

As extensões de domínio mais comuns disponíveis hoje e oficialmente legalizadas são as que aparecem na lista a seguir. Países também têm nomes de domínio tais como .uk, .au e .fr (Reino Unido, Austrália e França, respectivamente). Estão incluídos na lista dois

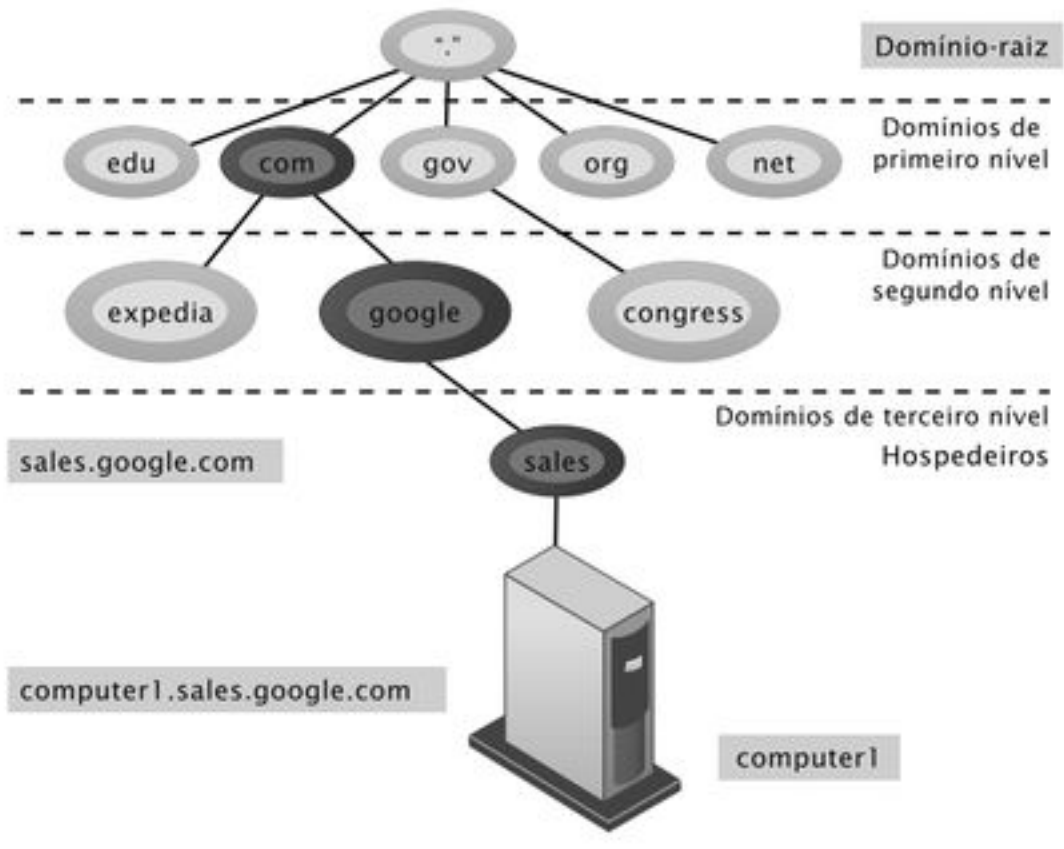


Figura 6.8

O Sistema de Nome de Domínio

O Sistema de Nome de Domínio é um sistema hierárquico com um domínio-raiz, domínios de primeiro nível, domínios de segundo nível e computadores hospedeiros no terceiro nível.

domínios de primeiro nível recentemente aprovados, .biz e .info. No futuro, essa lista se expandirá para incluir muitos outros tipos de organizações e setores.

.com	Empresas/organizações comerciais
.edu	Instituições educacionais
.gov	Órgãos públicos
.mil	Órgãos militares
.net	Computadores em rede
.org	Fundações e organizações sem fins lucrativos
.biz	Empresas
.info	Provedores de informação

Governança e arquitetura da Internet

O tráfego de dados da Internet navega através de redes backbone transcontinentais de alta velocidade, que geralmente operam na faixa de 45 megabits por segundo a 2,5 gigabits por segundo (veja Figura 6.9). Essas linhas-tronco em geral pertencem a companhias telefônicas de longa distância (chamadas *provedores de serviço de rede*) ou a governos nacionais. Nos Estados Unidos, as linhas de conexão local pertencem a companhias telefônicas regionais e de televisão a cabo, e conectam à Internet assinantes residenciais e corporativos. As redes regionais alugam acesso a ISPs, empresas privadas e instituições governamentais.

Cada empresa paga por suas próprias redes e seus próprios serviços locais de Internet, sendo uma parte paga aos proprietários das linhas-tronco de longa distância. Usuários individuais pagam ISPs para utilização de seus serviços e normalmente pagam uma taxa de assinatura que não varia em função do uso que fazem da Internet. Existe um debate que discute se essa organização deve continuar ou se os usuários que fazem uso mais intenso da Internet baixando grandes arquivos de vídeo e música devem pagar mais pela quantidade que consomem. A Seção Interativa sobre organizações explora esse assunto ao examinar os prós e contras da neutralidade de rede.

Ninguém é 'dono' da Internet e ela não tem uma administração formal. No entanto, políticas de Internet universais são estabelecidas por uma série de organizações profissionais e órgãos governamentais, como o Internet Architecture Board (IAB), que ajuda a definir a estrutura geral da Internet; o Internet Corporation for Assigned Names and Numbers (ICANN), que atribui endereços de IP; e o World Wide Web Consortium (W3C), que estabelece a *hypertext markup language* (HTML) e outros padrões de programação para a Web.

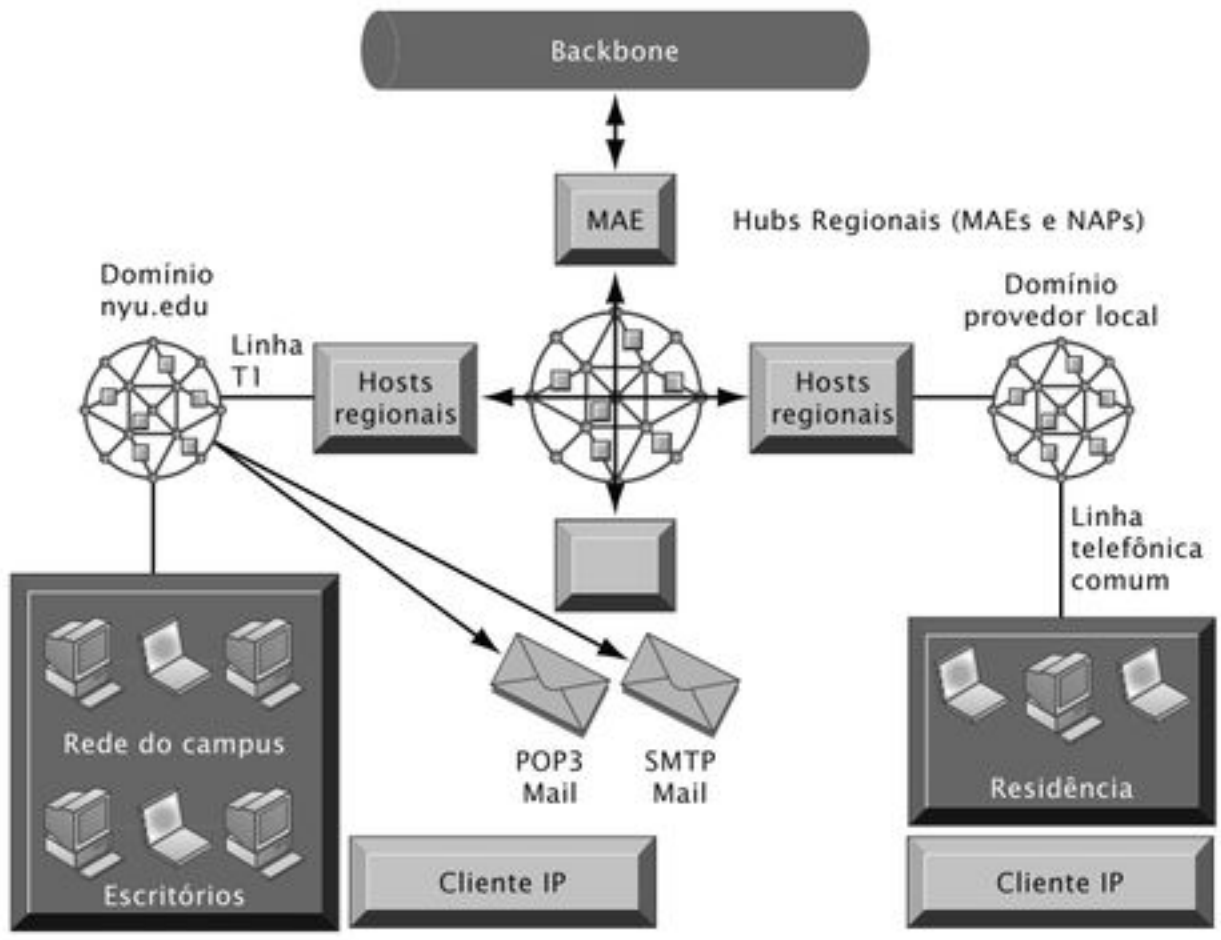


Figura 6.9

Arquitetura de rede da Internet

O backbone da Internet conecta-se a redes regionais, as quais, por sua vez, dão acesso a provedores de serviços de Internet, grandes empresas e instituições públicas. Os pontos de acesso a redes (NAPs — network access point) e as Internet exchanges (troca de Internet) metropolitanas (MAEs — metropolitan-area exchanges) são hubs em que o backbone intercepta redes regionais e locais e os proprietários do backbone se conectam uns com os outros.

SEÇÃO INTERATIVA: ORGANIZAÇÕES A neutralidade da rede deve continuar?

Que tipo de usuário de Internet você é? Você usa a rede para operações de e-mail e pesquisa de números telefônicos? Ou passa o dia inteiro on-line, assistindo a vídeos no YouTube, baixando arquivos de música ou se entretendo com jogos para múltiplos jogadores? Se você é do segundo tipo, está consumindo grande parte da largura de banda e centenas de milhões de pessoas como você podem começar a tornar a Internet mais lenta. Em 2007, o YouTube consumiu o equivalente ao consumo de toda a Web em 2000. Esse é um dos argumentos sustentados atualmente para cobrança de usuários com base no volume da capacidade de transmissão que utilizam.

Segundo um relatório de novembro de 2007, uma empresa de pesquisa projetou que a demanda pelo uso da Internet pode ultrapassar a capacidade da rede em 2011.

Se isso acontecer, a Internet pode não sofrer uma parada súbita, mas os usuários se depariam com velocidades lentas de download e baixo desempenho de sites como YouTube, Facebook e outros serviços pesados. (O uso intenso de iPhones nas áreas urbanas de Nova York e São Francisco já afetou os serviços da rede sem fio da AT&T.)

Outros pesquisadores acreditam que, à medida que o tráfego digital na Internet aumenta, mesmo a uma taxa de 50 por cento ao ano, a tecnologia para gestão de todo esse tráfego avança em ritmo igualmente acelerado.

Além dessas questões técnicas, o debate sobre a medição do uso da Internet concentra-se na questão da neutralidade de rede, que é a ideia de que os provedores de serviços de Internet devem permitir o acesso igualitário a conteúdo e aplicações, independente da fonte ou natureza do conteúdo. Atualmente, a Internet é realmente neutra: todo seu tráfego é tratado igualmente com base na filosofia 'primeiro a chegar, primeiro a ser atendido' dos proprietários de backbones. A Internet é neutra porque foi construída sobre linhas telefônicas, sujeitas a leis de 'acesso universal'. Essas leis exigem que as empresas telefônicas tratem todas as chamadas e todos os clientes da mesma maneira. Elas não podem oferecer benefícios extras aos clientes dispostos a pagar taxas mais altas por chamadas mais rápidas ou de melhor qualidade, modelo conhecido como serviço por camadas.

No entanto, as empresas de telecomunicações a cabo querem poder cobrar preços diferenciados com base na largura de banda consumida por conteúdo distribuído pela Internet. Em junho de 2008, a Time Warner Cable começou a testar a cobrança mensurada por seu serviço de acesso à Internet na cidade de Beaumont, Texas. No programa piloto, a empresa cobrava um dólar extra por mês para cada gigabyte recebido ou enviado além do limite de banda do plano contratado. A Time Warner Cable relatou que cinco por cento de seus clientes utilizavam metade da capacidade de suas linhas locais sem pagar nada mais do que os clientes com baixo uso, e que a cobrança mensurada foi a maneira 'mais justa' de financiar os investimentos necessários em sua infraestrutura de rede.

Essa não é a forma tradicional de funcionamento da Internet e contradiz as metas da neutralidade de rede. Defensores da neutralidade estão pressionando o Congresso norte-americano para que se regule o setor, exigindo que os provedores de rede se privem desses tipos de práticas. A estranha aliança dos defensores da neutralidade de rede inclui MoveOn.org, União Cristã, Associação Norte-americana de Bibliotecas, todos os grandes grupos consumidores, muitos blogueiros e pequenas empresas, além de algumas grandes empresas de Internet — como Google e Amazon.

Os provedores de serviços apontam o aumento da pirataria de material com direitos autorais pela Internet. Comcast, o segundo maior provedor de serviços de Internet nos Estados Unidos, relatou que o compartilhamento ilegal de arquivos protegidos por direitos autorais estava consumindo 50 por cento de sua capacidade de rede. Em determinado momento, Comcast diminuiu a velocidade de transmissão de arquivos de BitTorrent, amplamente usados para pirataria e compartilhamento ilegal de material protegido, inclusive vídeos. A Comcast recebeu críticas duras pela gestão de pacotes BitTorrent, e a Comissão Federal de Comunicações definiu que a empresa deveria parar de interromper o tráfego ponto a ponto em nome da gestão de rede. A Comcast abriu um processo contra a Comissão, questionando sua autoridade para impor a neutralidade de rede.

Defensores da neutralidade de rede argumentam que o risco de censura aumenta quando os operadores de rede seletivamente bloqueiam ou diminuem a velocidade de acesso a determinados conteúdos. Já existem muitos exemplos de provedores de Internet restringindo o acesso a materiais sensíveis (como o comentário anti-Bush no vídeo de um show da banda Pearl Jam, um programa de mensagens instantâneas do grupo pró-escolha NARAL, ou o acesso a competidores como Vonage). O governo paquistanês bloqueou o acesso a sites anti-islamismo e a todo o conteúdo do YouTube em resposta a materias que julgavam difamadores ao Islã.

Defensores da neutralidade de rede também argumentam que uma Internet neutra encoraja a todos a inovar sem a permissão das empresas de cabo e telefonia ou outras autoridades, e essa nova igualdade de condições para todos já deu origem a inúmeras novas organizações. A permissão do fluxo de informação irrestrito torna-se essencial para os mercados livres e para a democracia à medida que o comércio e a sociedade estão cada vez mais migrando para o mundo virtual.

Os proprietários de redes acreditam que as regulamentações propostas pelos defensores da neutralidade de rede travarão a competitividade norte-americana com a repressão da inovação e causarão prejuízos aos clientes que irão se beneficiar das práticas de rede 'discriminatórias'. Nos Estados Unidos, os serviços de Internet ficam atrás de muitas outras nações em termos

de velocidade, custo e qualidade dos serviços, o que dá credibilidade aos argumentos dos provedores.

Defensores da neutralidade de rede reagem dizendo que os provedores norte-americanos têm muito poder devido à falta de opção por serviços. Sem competição suficiente, possuem maior liberdade para definir preços e políticas, e os clientes não podem procurar refúgio em outras alternativas. Os provedores podem fazer distinção em favor de seu próprio conteúdo. Mesmo os usuários de banda larga em grandes áreas metropolitanas não dispõem de muitas opções de serviços. Se existissem mais opções de acesso à Internet, a neutralidade de rede não seria um assunto tão urgente. Clientes insatisfeitos poderiam simplesmente trocar para provedores que fazem cumprir a neutralidade de rede e permitem acesso ilimitado à Internet.

Em 21 de setembro de 2009, a Comissão Federal de Comunicações dos Estados Unidos anunciou sua intenção de formalizar um conjunto de regras para apoio à neutralidade de rede com base em princípios defendidos pela Comissão desde agosto de 2005. Essas regras dão aos clientes o direito de acesso a conteúdos, aplicações e serviços de Internet de sua escolha, e garantem o uso de dispositivos para conexão à rede. As regras também apoiam a competição entre provedores de redes, aplicações e serviços e conteúdo de Internet. Duas novas regras impediriam que os provedores fizessem distinção entre conteúdo particular e garantiriam a transparência de suas práticas de gestão de rede. Pela primeira vez, todas essas regras seriam aplicadas às empresas sem fio.

Fontes: Fawn Johnson e Amy Schatz, "FCC Chairman Proposes 'Net Neutrality' Rules". *The Wall Street Journal*, 21 set. 2009; Grant Gross, "FCC Chairman Calls for Formal Net Neutrality Rules". *IDG News Service*, 21 set. 2009; Joanie Wexler, "Net Neutrality: Can We Find Common Ground?. *Network World*, 1º abr. 2009; Andy Dornan, "Is Your Network Neutral?. *Information Week*, 18 maio. 2008; Steve Lohr, "Video Road Hogs Stir Fear of Internet Traffic Jam". *The New York Times*, 13 mar. 2008; e Peter Burrows, "The FCC, Comcast, and Net Neutrality". *Business Week*, 26 fev. 2008.

PERGUNTAS SOBRE O ESTUDO DE CASO

1. O que é a neutralidade de rede? Por que a Internet praticou a neutralidade de rede até o momento?
2. Quem é a favor da neutralidade de rede? Quem é contra? Por quê?
3. Qual seria o impacto sobre os usuários individuais, as empresas e o governo se os provedores de Internet aderissem ao modelo de serviço por camadas?
4. Você é a favor de uma legislação que garanta a neutralidade de rede? Justifique.

Essas organizações influenciam órgãos governamentais, os principais proprietários de rede, ISPs, corporações e desenvolvedores de software — e de fato o fazem — com o objetivo de manter a Internet operando da maneira mais eficiente possível. Além desses organismos profissionais, a Internet também precisa conformar-se às leis soberanas dos Estados-nações na qual opera, assim como à infraestrutura técnica existente nesses locais. Embora nos primeiros anos da Internet e da Web houvesse pouca interferência dos poderes Executivo ou Legislativo, essa situação está mudando à medida que a Internet assume papel cada vez maior na distribuição de informação e conhecimento — e passa a incluir conteúdos que alguns consideram discutíveis.

A Internet do futuro: IPv6 e Internet2

A Internet não foi originalmente projetada para lidar com a transmissão de gigantescas quantidades de dados e um número de usuários em crescimento explosivo. Como muitas empresas e órgãos públicos receberam grandes lotes com milhões de endereços IP para acomodar suas atuais e futuras forças de trabalho, e como o número de pessoas com acesso à Internet aumentou, até 2012 ou 2013 o mundo vai ficar sem endereços IP disponíveis dentro da convenção de endereçamentos atual. Está em desenvolvimento uma nova versão do esquema de endereçamento IP chamada *Internet Protocol versão 6* ***(IPv6)***, que contém endereços de 128 bits (2 elevado à potência 128), ou mais de 1 quatrilhão de endereços exclusivos possíveis.

A **Internet2** e a Next-Generation Internet (NGI) são consórcios que representam 200 universidades, empresas e órgãos públicos nos Estados Unidos que estão desenvolvendo redes backbone de alta performance, com bandas largas variando de 2,5 gigabits por segundo a 9,6 gigabits por segundo. Os grupos de pesquisa da Internet2 estão desenvolvendo e implantando: novas tecnologias para práticas de roteamento mais eficientes; diferentes níveis de serviço, dependendo do tipo e da importância dos dados em transmissão; e aplicações avançadas para computação distribuída, laboratórios virtuais, bibliotecas digi-

tais, aprendizagem distribuída e teleimersão. Essas redes não substituem a Internet pública, mas representam a oportunidade de testar tecnologia de ponta que, mais tarde, pode migrar para atingir o público em geral.

Tecnologia e serviços de Internet

A Internet é baseada na tecnologia cliente/servidor. Indivíduos que utilizam a Internet controlam o que fazem por meio de aplicativos clientes, como o software de navegação Web. Todos os dados, entre eles as mensagens de e-mail e as páginas da Web, são armazenados em servidores. Um cliente utiliza a Internet para requisitar informações de um servidor da Web particular localizado em um computador distante, e este servidor envia a informação requisitada de volta ao cliente via Internet. Os capítulos 4 e 5 descrevem como os servidores da Web trabalham com servidores de aplicativo e de banco de dados para acessar informações em aplicativos de sistemas de informação internos em uma organização e em seus bancos de dados correlatos. As plataformas clientes atuais incluem não somente PCs, mas celulares, dispositivos de mão e outros equipamentos de informação.

Serviços de Internet

Um computador cliente conectado à Internet tem acesso a uma variedade de serviços, como e-mail, grupos eletrônicos de discussão (Usenet e LISTSERVs), bate-papo e mensagens instantâneas, **Telnet**, **File Transfer Protocol (FTP)** e a World Wide Web. A Tabela 6.3 descreve brevemente esses serviços.

Cada serviço de Internet é implantado por um ou mais programas de software. Todos os serviços podem rodar em um único computador servidor; diferentes serviços também podem ser alocados a máquinas diferentes. A Figura 6.10 mostra um dos modos possíveis de organização desses serviços em uma arquitetura cliente/servidor multinível.

O **e-mail** permite que mensagens sejam trocadas entre computadores, com recursos para direcionar mensagens a vários destinatários, repassar mensagens e anexar documentos de texto ou arquivos de multimídia às mensagens. Embora algumas organizações operem seus próprios sistemas internos de correspondência eletrônica, grande parte dos e-mails atualmente é enviada pela Internet. Os custos com e-mails são muito inferiores aos equivalentes para entrega por voz, correio ou serviço de entrega, o que transforma a Internet em um meio de comunicação barato e rápido. A maioria das mensagens de e-mail chega a qualquer parte do mundo em questão de segundos.

Em aproximadamente 90 por cento dos ambientes de trabalho norte-americanos os funcionários se comunicam interativamente usando ferramentas de **bate-papo** ou mensagens instantâneas. O bate-papo permite que duas ou mais pessoas conectadas simultaneamente à Internet mantenham conversações interativas, ao vivo. Os sistemas de bate-papo suportam conversas por voz e vídeo, bem como as conversas escritas. Muitas empresas de varejo on-line oferecem serviços de bate-papo em seus sites para atrair visitantes, incentivar novas compras regulares e aprimorar o serviço de atendimento.

Tabela 6.3 **Os serviços de Internet mais importantes**

Recurso	Funções suportadas
e-mail	Mensagem pessoa a pessoa; compartilhamento de documentos
Bate-papo e mensagens instantâneas	Conversações interativas
Newsgroups	Grupos de discussão em painéis eletrônicos de avisos
Telnet	Fazer logon em um sistema de computador e trabalhar em outro
FTP	Transferir arquivos de um computador para outro
World Wide Web	Extrair, formatar e apresentar informações (incluindo texto, áudio, elementos gráficos e vídeo) usando links de hipertexto

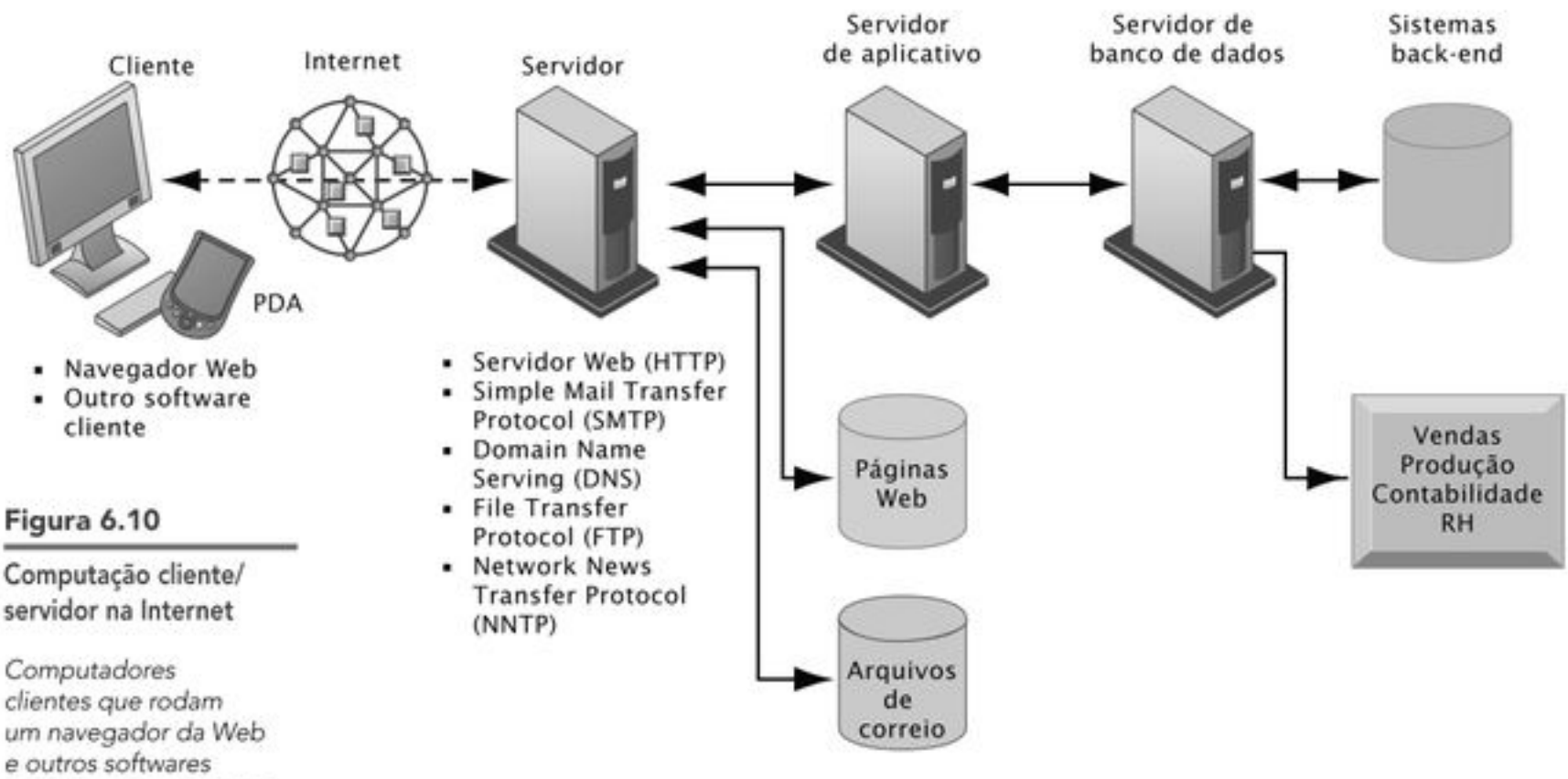


Figura 6.10

Computação cliente/servidor na Internet

Computadores clientes que rodam um navegador da Web e outros softwares podem acessar serviços disponíveis em servidores via Internet. Esses serviços podem rodar todos em um único servidor ou em múltiplos servidores especializados.

A **mensagem instantânea** é um tipo de serviço de bate-papo que permite aos participantes criar seus próprios canais de bate-papo. O sistema de mensagem instantânea alerta o usuário sempre que alguém de sua lista particular está on-line, de modo que possa iniciar uma conversação com aquela pessoa em particular. Há diversos sistemas concorrentes de mensagem instantânea, dentre eles Yahoo! Messenger, Google Talk e Windows Live Messenger. Preocupadas com segurança, algumas empresas estão desenvolvendo sistemas proprietários de mensagem instantânea, a partir de ferramentas como o Lotus Sametime.

Newsgroups são grupos mundiais de discussão, nos quais as pessoas compartilham informações e ideias sobre um tópico definido, como radiologia ou bandas de rock. A discussão ocorre em grandes 'painéis eletrônicos' nos quais qualquer um pode inserir mensagens para que outras pessoas leiam. Existem milhares de grupos que discutem praticamente qualquer tópico.

O uso de e-mail, mensagens instantâneas e da Internet por parte dos funcionários supostamente incrementaria sua produtividade, mas a Seção Interativa sobre pessoas, a seguir, mostra que isso nem sempre é verdade. Atualmente, muitas empresas acreditam que precisam monitorar as atividades de Web e e-mail dos funcionários. Mas será que isso é ético? Embora existam algumas boas razões empresariais para o monitoramento, o que isso representa em termos da privacidade do funcionário?

Voz sobre IP

A Internet também se tornou uma plataforma popular para transmissão de voz e networking corporativo. A tecnologia de **voz sobre IP (VoIP – *voice over IP*)** transmite informações de voz sob formato digital, por meio da comutação de pacotes, evitando assim a tarifa cobrada pelas redes de telefonia locais ou de longa distância (veja a Figura 6.11). Chamadas telefônicas que normalmente seriam transmitidas por redes telefônicas públicas passam a transitar pela rede corporativa, baseada no Protocolo de Internet, ou pela Internet pública. Chamadas telefônicas IP podem ser feitas e recebidas por um computador de mesa equipado com microfone e alto-falantes ou caixas de som, ou por um telefone habilitado.

Empresas como provedores de serviços de telecomunicações (tais como a Verizon) e corporações de transmissões a cabo (como a Time Warner e a Cablevision) oferecem serviço de VoIP. O Skype oferece VoIP grátis em todo o mundo por meio de uma rede *peer-to-peer*, e a Google possui seu próprio serviço gratuito de VoIP.

Embora um sistema telefônico IP exija uma série de investimentos iniciais, o VoIP pode reduzir os custos de gestão de rede e de comunicação de 20 a 30 por cento. Essa tecnologia permite, por exemplo, que a Virgin Entertainment Group economize 700 mil dólares por

SEÇÃO INTERATIVA: PESSOAS — Monitorando empregados na rede: falta de ética ou boa prática profissional?

Ao explodir o uso da Internet pelo mundo, explodiu também o uso do e-mail e da Web para questões pessoais no local de trabalho. Diversos problemas gerenciais surgiram. Primeiro, verificar e-mails, responder mensagens instantâneas ou dar uma olhadela em um pequeno vídeo do YouTube ou MySpace cria uma série contínua de interrupções que desvia a atenção do empregado das tarefas. Segundo a Basex, uma empresa de pesquisa da cidade de Nova York, essas distrações chegam a tomar 28 por cento de um dia médio de trabalho nos Estados Unidos e resultam em 650 bilhões de dólares de perda de produtividade por ano!

Segundo, esses intervalos não estão necessariamente relacionados ao trabalho. Um número de estudos conclui que pelo menos 25 por cento do tempo on-line do empregado é gasto com navegação não relacionada ao trabalho, e cerca de 90 por cento dos empregados enviam e recebem e-mails pessoais no trabalho.

Muitas empresas começaram a monitorar o uso que seus empregados fazem de e-mail, blogs e da Internet, algumas vezes sem que eles soubessem. Uma recente pesquisa da American Management Association (AMA) realizada em 304 empresas norte-americanas de todos os portes descobriu que 66 por cento delas monitoram as mensagens de e-mails e as conexões da Web de seus empregados. Embora as empresas possuam o direito legal de monitorar essas atividades enquanto os funcionários estão no trabalho, essa atitude representa falta de ética ou simplesmente um bom negócio?

Gerentes preocupam-se com a perda de tempo e a diminuição da produtividade quando os empregados focam-se em questões pessoais em vez de profissionais. Tempo em excesso gasto em assuntos pessoais, seja na Internet ou não, pode significar perda de receita ou clientes superfaturados. Alguns empregados podem estar cobrando dos clientes o tempo que passam lidando com questões particulares on-line ou resolvendo outros assuntos, o que gera cobrança excessiva aos clientes.

Se o tráfego pessoal nas redes da empresa for muito alto, pode acabar obstruindo a rede de forma que negócios legítimos não possam ser executados. Schemmer Associates, uma firma de arquitetura em Omaha, Nebraska, e o Hospital Potomac, em Woodridge, Virgínia, descobriram que seus recursos computacionais estavam limitados devido à falta de largura de banda causada pelo uso que empregados faziam da conexão com a Internet para assistir e baixar arquivos de vídeo.

Quando os empregados acessam e-mail ou a Internet nas instalações do empregador ou com seus equipamentos, qualquer coisa que façam, incluindo atos ilegais, carrega o nome da empresa, que pode ser rastreada e acusada. Gerentes de muitas empresas se preocupam com a possibilidade de que material racista, de sexo explícito ou potencialmente ofensivo acessado ou rastreado por seus empregados resulte em publicidade adversa e mesmo em processos para a empresa. Mesmo que se descubra que a empresa não é responsável, responder a processos pode lhe custar dezenas de milhares de dólares.

As empresas também temem o vazamento de informações confidenciais e segredos de negócios através de e-mails ou blogs. Em recente pesquisa realizada pela American Management Association em conjunto com o Instituto ePolicy, descobriu-se que 14 por cento dos empregados entrevistados admitiram ter enviado e-mails confidenciais ou potencialmente embaraçosos para pessoas que não pertenciam à empresa.

As empresas norte-americanas têm o direito legal de monitorar o que os empregados estão fazendo com o equipamento da empresa durante o horário de trabalho. A questão é se a vigilância eletrônica é uma ferramenta apropriada para a manutenção de um ambiente de trabalho eficiente e positivo. Algumas empresas tentaram proibir todas as atividades pessoais das redes corporativas. Outras bloqueiam o acesso do empregado a sites específicos ou sites sociais, ou limitam o tempo de acesso pessoal à Web.

A Enterprise Rent-A-Car, por exemplo, bloqueia o acesso dos empregados a determinados sites e monitora as postagens on-line dos colaboradores sobre a empresa. A Ajax Boiler, em Santa Ana, Califórnia, usa software da SpectorSoft Corporation que registra todos os sites da Web visitados pelos empregados, o tempo gasto em cada site e todos os e-mails enviados. A Flushing Financial Corporation instalou um software que impede que os empregados enviem e-mails a determinados endereços e inspeciona os anexos de e-mails em busca de informações sensíveis. A Schemmer Associates usa o OpenDNS para categorizar e filtrar conteúdo da Web e bloquear vídeos indesejados.

Algumas empresas demitiram empregados que passaram dos limites. Um terço das empresas pesquisadas pelo estudo da AMA demitiu empregados devido ao mau uso da Web no trabalho. Dentre os gerentes que demitiram por esse motivo, 64 por cento o fizeram porque os e-mails dos empregados continham linguagem inapropriada ou ofensiva, e mais de 25 por cento demitiram empregados por conta do uso excessivo de e-mails.

Nenhuma solução está livre de problemas, mas muitos consultores acreditam que as empresas deveriam estabelecer políticas de uso de e-mails e Internet. As políticas devem explicitar as regras fundamentais que definem, por cargo ou nível, sob quais circunstâncias os empregados podem usar as instalações da empresa para acesso a e-mail, blog ou sites. As políticas também devem informar aos empregados se essas atividades são monitoradas e explicar a razão para tal.

Agora, a IBM possui 'diretrizes de computação social' que englobam as atividades de empregados em sites como Facebook e Twitter. As diretrizes recomendam que os empregados não revelem sua identidade, lembram que os mesmos são pessoalmente responsáveis pelo que publicam e solicitam que sejam evitadas

discussões sobre tópicos controversos não relacionados ao papel que desempenham na IBM.

As regras devem ser criadas para necessidades de negócios e culturas específicas. Embora algumas empresas possam impedir que todos os empregados visitem sites com conteúdo de sexo explícito, funcionários de empresas jurídicas ou hospitais podem solicitar acesso a esses sites. Firmas de investimento precisarão permitir que muitos de seus empregados acessem outros sites de investimento. Uma empresa que dependa largamente de compartilhamento de informações, inovação e independência poderia muito bem achar que o monitoramento traz mais problemas do que soluções.

Fontes: Michelle Conline e Douglas MacMillan, "Web 2.0: Managing Corporate Reputations". *Business Week*, 20 maio. 2009; Dana Mattioli, "Leaks Grow in a World of Blogs". *The Wall Street Journal*, 20 jul. 2009; James Wong, "Drafting Trouble-Free Social Media Policies". Law.com, 15 jun. 2009; Nancy Gohring, "Over 50 Percent of Companies Fire Workers for E-Mail, Net Abuse". *InfoWorld*, 28 fev. 2008; Bobby White, "The New Workplace Rules: No Video-Watching". *The Wall Street Journal*, 4 mar. 2008; e Maggie Jackson, "May We Have Your Attention, Please?". *Business Week*, 23 jun. 2008.

PERGUNTAS SOBRE O ESTUDO DE CASO

1. Os gerentes devem monitorar o uso que os empregados fazem da Internet e de e-mails? Justifique.
2. Descreva uma política eficiente de uso de e-mails e Internet para uma empresa.
3. Os gerentes deveriam informar aos empregados que seu comportamento na Web está sendo monitorado ou deveriam manter segredo? Justifique.

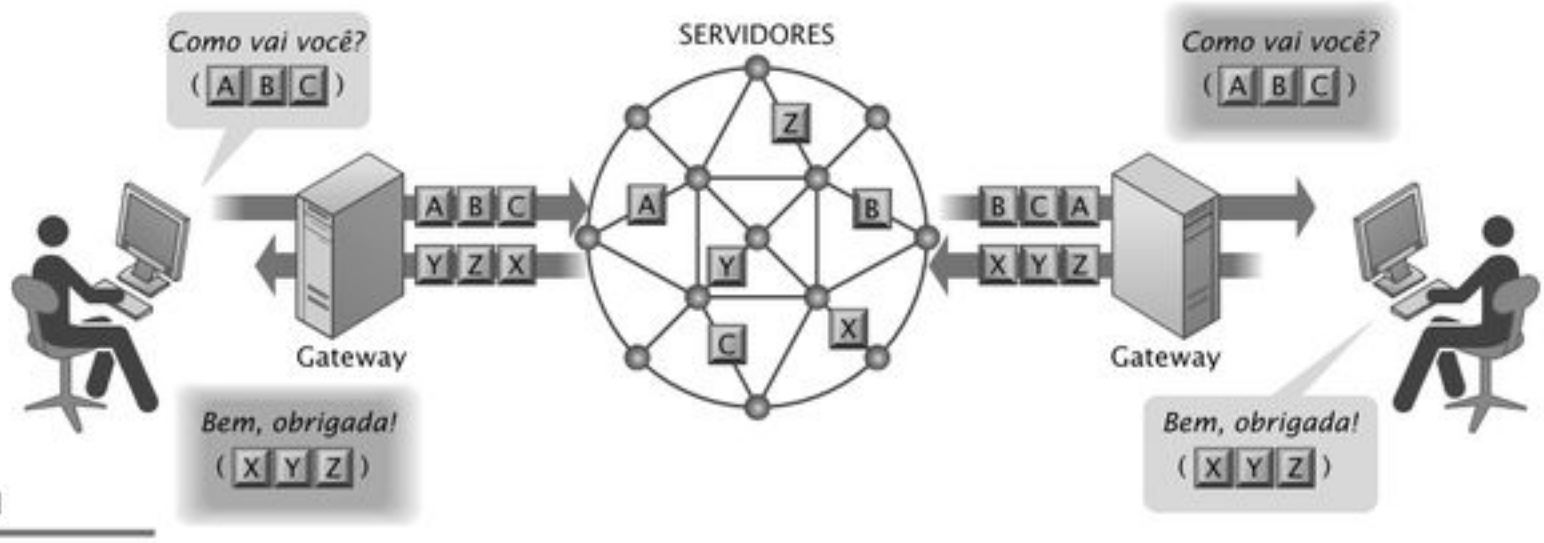


Figura 6.11

Funcionamento da telefonia IP

Uma chamada telefônica IP digitaliza e fragmenta uma mensagem de voz em pacotes de dados que podem transitar por diferentes rotas antes de serem remontados em seu destino final. Um servidor que está mais próximo do destino da chamada, denominado gateway, organiza os pacotes na ordem correta e os direciona ao número de telefone do recebedor ou do endereço IP do computador de destino.

ano em chamadas de longa distância. Além de diminuir os custos das chamadas de longa distância e eliminar as tarifas mensais das linhas privadas, uma rede IP oferece uma infraestrutura única para voz e dados, o que proporciona serviços tanto de telecomunicações quanto de informática. As empresas não precisam mais manter redes separadas, nem providenciar suporte e pessoal para cada tipo de rede.

Outra vantagem do VoIP é a flexibilidade. Diferentemente da rede telefônica tradicional, ele permite acrescentar ou mudar de lugar aparelhos telefônicos em diferentes escritórios, sem que seja preciso refazer o cabeamento ou reconfigurar a rede. Com o VoIP, uma chamada de conferência pode ser feita com uma simples operação de clicar e arrastar na tela do computador, selecionando o nome dos participantes. Por fim, o correio de voz e o e-mail podem ser combinados no mesmo diretório.

Comunicações unificadas

No passado, cada uma das redes de uma empresa para dados cabeados e sem fio, comunicações por voz e videoconferência operava de forma independente e tinha de ser separadamente gerenciada pelo departamento de sistemas de informação. Hoje em dia, entretanto, as empresas conseguem fundir modos díspares de comunicação em um serviço único universalmente acessível utilizando a tecnologia de comunicação unificada. As **comunicações unificadas** integram canais distintos para comunicação por voz, comunicação de dados,

mensagens instantâneas, e-mails e conferência eletrônica em uma experiência única na qual o usuário pode perfeitamente alternar entre modos diferentes de comunicação. A tecnologia de presença mostra se uma pessoa está disponível para receber uma chamada. As empresas precisarão avaliar como o fluxo de trabalho e os processos de negócios serão alterados por essa tecnologia de modo a ajustar seu valor.

A CenterPoint Properties, imobiliária de uma importante área industrial de Chicago, recorreu à tecnologia de comunicação unificada para criar sites colaborativos para cada uma de suas agências. Cada site oferece um ponto de acesso único a dados estruturados e não estruturados. A tecnologia de presença integrada permite que os integrantes das equipes enviem e-mail e mensagens instantâneas, e realizem chamadas e videoconferências com um único clique.

Rede virtual privada

Imagine que você tenha um grupo de marketing encarregado do desenvolvimento de novos produtos e serviços para sua empresa, com membros espalhados por todo o país. O ideal seria que pudessem mandar e-mails uns aos outros e se comunicar com o escritório central, sem nenhuma chance de intrusos interceptarem as comunicações. No passado, uma solução para esse problema seria trabalhar com grandes empresas de redes privadas que oferecessem redes dedicadas, privadas e seguras aos clientes. Mas essa solução era muito cara. Uma solução mais barata é criar uma rede privada virtual dentro da Internet pública.

Uma **rede virtual privada (VPN — *virtual private network*)** é uma rede privada, criptografada e segura, configurada dentro de uma rede pública para tirar proveito das economias de escala e da infraestrutura de gestão das grandes redes, tais como a Internet (veja a Figura 6.12). A VPN oferece à sua empresa comunicações criptografadas e seguras, a um custo muito mais baixo que o dos mesmos recursos oferecidos pelos provedores tradicionais, que usam redes privadas para proporcionar comunicações seguras. As VPNs também oferecem infraestrutura de rede para que sejam combinadas redes de dados e voz.

Vários protocolos são utilizados para proteger os dados transmitidos pela Internet pública, inclusive o Protocolo de Tunneling (tunelamento) Ponto a Ponto (PPTP). Por um processo denominado *tunelamento*, pacotes de dados são criptografados e acondicionados dentro de pacotes IP. Adicionando esse 'invólucro' ao redor da mensagem de rede para ocultar seu conteúdo, as organizações podem criar uma conexão privada que trafega pela Internet pública.

A World Wide Web

Você provavelmente já utilizou a Internet para baixar música, pesquisar informações para um trabalho ou ler notícias. A World Wide Web (a Web) é o mais conhecido serviço de Internet. Trata-se de um sistema com padrões universalmente aceitos para armazenar,

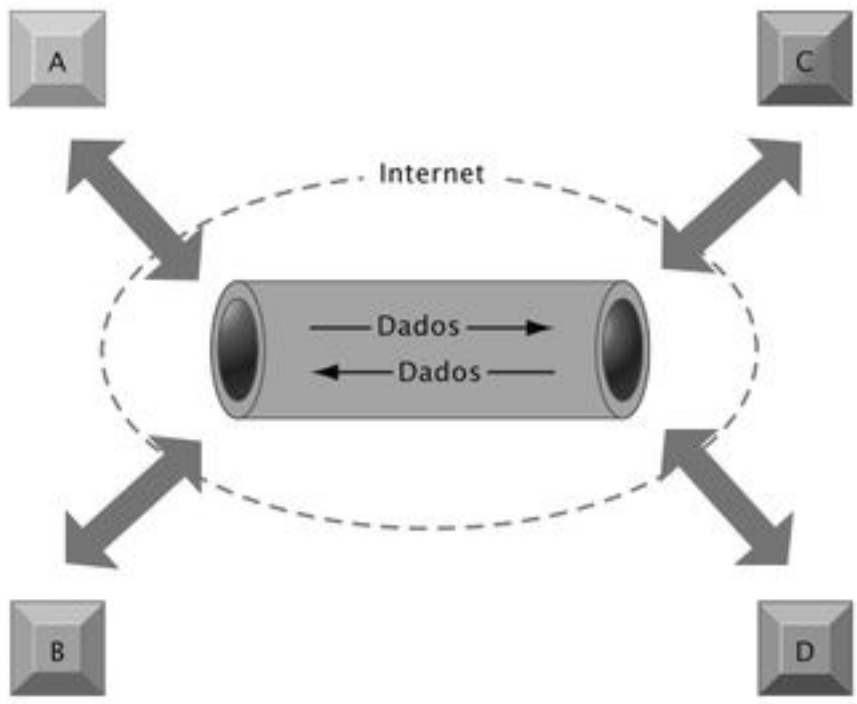


Figura 6.12

Uma rede privada virtual que usa a Internet

Esta VPN é uma rede privada de computadores unidos por uma conexão 'tunelada' segura, que transita pela Internet. Ela protege os dados transmitidos pela Internet pública, codificando-os e acondicionando-os dentro do Protocolo de Internet (IP). Adicionando esse 'invólucro' ao redor da mensagem de rede para ocultar seu conteúdo, as organizações podem criar uma conexão privada que trafega pela Internet pública.

recuperar, formatar e apresentar informações utilizando uma arquitetura cliente/servidor. Páginas da Web são formatadas por meio de hipertexto, com links embutidos que vinculam os documentos uns aos outros, assim como vinculam páginas a outros objetos, como som, vídeo ou arquivos de animação. Quando clica em um elemento gráfico e um videoclipe começa a ser exibido, isso significa que você clicou em um hyperlink. Um **site** típico é uma coleção de páginas conectadas a uma página principal.

Hipertexto

As páginas da Web são baseadas em linguagem-padrão de hipertexto chamada HTML (*hypertext markup language*), que formata documentos e reúne links dinâmicos para outros documentos e imagens armazenados no mesmo computador ou em computadores remotos (veja o Capítulo 4). Essas páginas são acessíveis via Internet porque o software de navegador da Web que opera em seu computador pode requisitar as páginas armazenadas em um servidor hospedeiro de Internet por meio do **protocolo de transferência de hipertexto (HTTP — *hypertext transfer protocol*)**, o padrão de comunicações utilizado para transferir páginas na Web. Por exemplo, quando você digita um endereço da Web em seu navegador, como www.sec.gov, seu navegador envia uma requisição HTTP ao servidor sec.gov, requisitando a home page de sec.gov.

HTTP é o primeiro conjunto de letras no início de qualquer endereço da Web; é seguido pelo nome de domínio, que especifica o computador servidor da organização que armazena o documento. A maioria das empresas tem um nome do domínio igual ou muito parecido com o seu nome corporativo oficial. O caminho do diretório e o nome do documento são as duas outras informações dentro do endereço de Web que ajudam o navegador a localizar a página requisitada. Como um todo, o endereço é denominado **localizador uniforme de recursos (URL — *uniform resource locator*)**. Quando digitado em um navegador, um URL diz ao software exatamente onde procurar a informação. Na URL *http://www.megacorp.com/content/features/082602.html*, por exemplo, *http* representa o protocolo usado para exibir páginas da Web; *www.megacorp.com* é o nome de domínio; *content/features* é o caminho do diretório que identifica onde a página está armazenada dentro do servidor do domínio; e *082602.html* é o nome do documento e do formato no qual ele se encontra (trata-se de uma página HTML).

Servidores da Web

Um servidor da Web é um software que localiza e administra páginas da Web armazenadas. Ele localiza as páginas solicitadas por um usuário no computador onde estão armazenadas e as envia ao computador dessa pessoa. Servidores de aplicativo normalmente rodam em computadores dedicados, embora, em pequenas organizações, possam residir todos em um único aparelho.

Atualmente, o servidor da Web mais comum é o Apache HTTP Server, que domina 46 por cento do mercado. O Apache é um produto de código aberto e gratuito que pode ser baixado da Web. O Internet Information Services, da Microsoft, é o segundo servidor mais comum, com participação de mercado de 22 por cento.

Procurando informações na Web

Ninguém sabe exatamente quantas páginas existem na rede. A Web visível é a parte que as máquinas de busca visitam e sobre as quais as informações são registradas. Por exemplo, o Google visitou cerca de 50 bilhões de páginas em 2008, embora admita publicamente indexar mais de 25 bilhões. Mas existe uma 'Web oculta' (também conhecida como 'Web profunda') que contém aproximadamente 800 bilhões de páginas adicionais, muitas delas proprietárias (tais como as páginas do *The Wall Street Journal* on-line, que não podem ser visitadas sem um código de acesso) ou armazenadas em bancos de dados corporativos protegidos.

Máquinas de busca Obviamente, com tantas páginas da Web, encontrar instantaneamente páginas específicas que possam ajudar você ou a sua empresa é um grande desafio. A questão é: como encontrar aquelas duas ou três páginas que realmente deseja e necessita entre os bilhões de homepages indexados? As **máquinas de busca** tentam resolver o problema de achar informações úteis na Web de maneira quase instantânea e são, ao que tudo

indica, o 'killer app' (abreviatura de 'aplicativo matador') da era da Internet. As máquinas de busca atuais conseguem pesquisar arquivos HTML, de aplicativos Microsoft Office, arquivos PDF e aqueles de áudio, vídeo e imagem. Existem centenas de máquinas de busca diferentes no mundo, mas a ampla maioria dos resultados de busca é fornecida pelos três principais provedores: Google, Yahoo! e Microsoft (que lançou recentemente sua máquina de busca chamada Bing).

As máquinas de busca da Web surgiram no início da década de 1990 como programas de software relativamente simples que vagavam pela nascente da rede, visitando páginas e reunindo informações sobre o conteúdo de cada. As primeiras máquinas de busca eram simplesmente índices de palavras-chave oriundas de todas as páginas que visitavam. Elas contavam o número de vezes que uma palavra aparecia nessas páginas e armazenavam essa informação em um índice, fornecendo ao usuário listas de páginas que podiam não ser relevantes à sua pesquisa.

Em 1994, David Filo e Jerry Yang, alunos de ciência da computação da Universidade Stanford, criaram uma lista selecionada à mão de suas páginas da Web favoritas e a denominaram 'Yet Another Hierarchical Officious Oracle' (algo como 'Mais um Oráculo Hierárquico Invasivo'), ou Yahoo!. O Yahoo! nunca foi uma máquina de busca propriamente dita, mas uma seleção editada de sites organizados por categorias que os editores consideram úteis. Depois, o Yahoo! desenvolveu seus próprios recursos de máquina de busca.

Em 1998, Larry Page e Sergey Brin, dois outros alunos de ciências da computação de Stanford, lançaram a primeira versão do Google. Essa máquina de busca era diferente: não apenas indexava as palavras de cada página da Web, como montava um *ranking* desses resultados de busca com base na relevância de cada página. Page patenteou a ideia de um sistema de *ranking* de páginas (PageRank System), que, em essência, mede a popularidade de uma página da Web calculando quais outros sites fazem link para aquela página. A contribuição de Brin foi criar um programa *crawler* da Web exclusivo, que indexava não apenas palavras-chave em uma página, mas combinações de palavras (tais como autores e os títulos de seus artigos). Essas duas ideias tornaram-se a base para a máquina de busca Google. A Figura 6.13 ilustra como o Google funciona.

Os sites para localização de informações tornaram-se tão populares e fáceis de usar que servem também como grandes portais para a Internet (veja o Capítulo 9). Úteis, ninguém esperava que as máquinas de busca fossem grandes máquinas de fazer dinheiro. Atualmente, entretanto, são a base para uma crescente forma de marketing e propaganda denominada **marketing de máquina de busca**. Quando os usuários inserem um termo de busca no Google, no Bing, no Yahoo! ou em qualquer outro site que utilize os serviços dessas máquinas de busca, recebem dois tipos de listas: os links patrocinados, que levam ao site dos anunciantes que pagaram para ser listados (normalmente no topo da página de resultados de busca), e os resultados de busca 'orgânicos', ou não patrocinados. Além disso, os anunciantes podem comprar pequenas caixas de texto no lado direito da página de resultados de busca. Atualmente, os anúncios pagos ou patrocinados são a forma de publicidade na Internet de crescimento mais rápido; são também novas poderosas ferramentas de marketing que combinam, com precisão e no momento exato, os interesses do consumidor e as mensagens publicitárias. O marketing de máquina de busca imprime valor ao processo de pesquisa. Em 2009, esse tipo de marketing gerou 12,2 bilhões de dólares em receita, metade de todos os anúncios on-line. Noventa e oito por cento da receita anual de 22 bilhões de dólares do Google vem do marketing de máquina de busca (eMarketer, 2009).

Como o marketing de máquina de busca é eficaz, as empresas estão começando a otimizar seus sites da Web para reconhecimento por máquinas de busca. Quanto mais bem otimizada for a página, mais alta será sua classificação nas listagens de resultados das máquinas de busca. A **otimização de máquinas de busca (SEO — *search engine optimization*)** é o processo de melhoria de qualidade e volume do tráfego na Web para um site através do emprego de uma série de técnicas que ajudam a alcançar melhor classificação nas principais máquinas de busca quando determinadas palavras e expressões são digitadas no campo de pesquisa. Uma técnica é garantir que as palavras utilizadas na descrição do site combinem

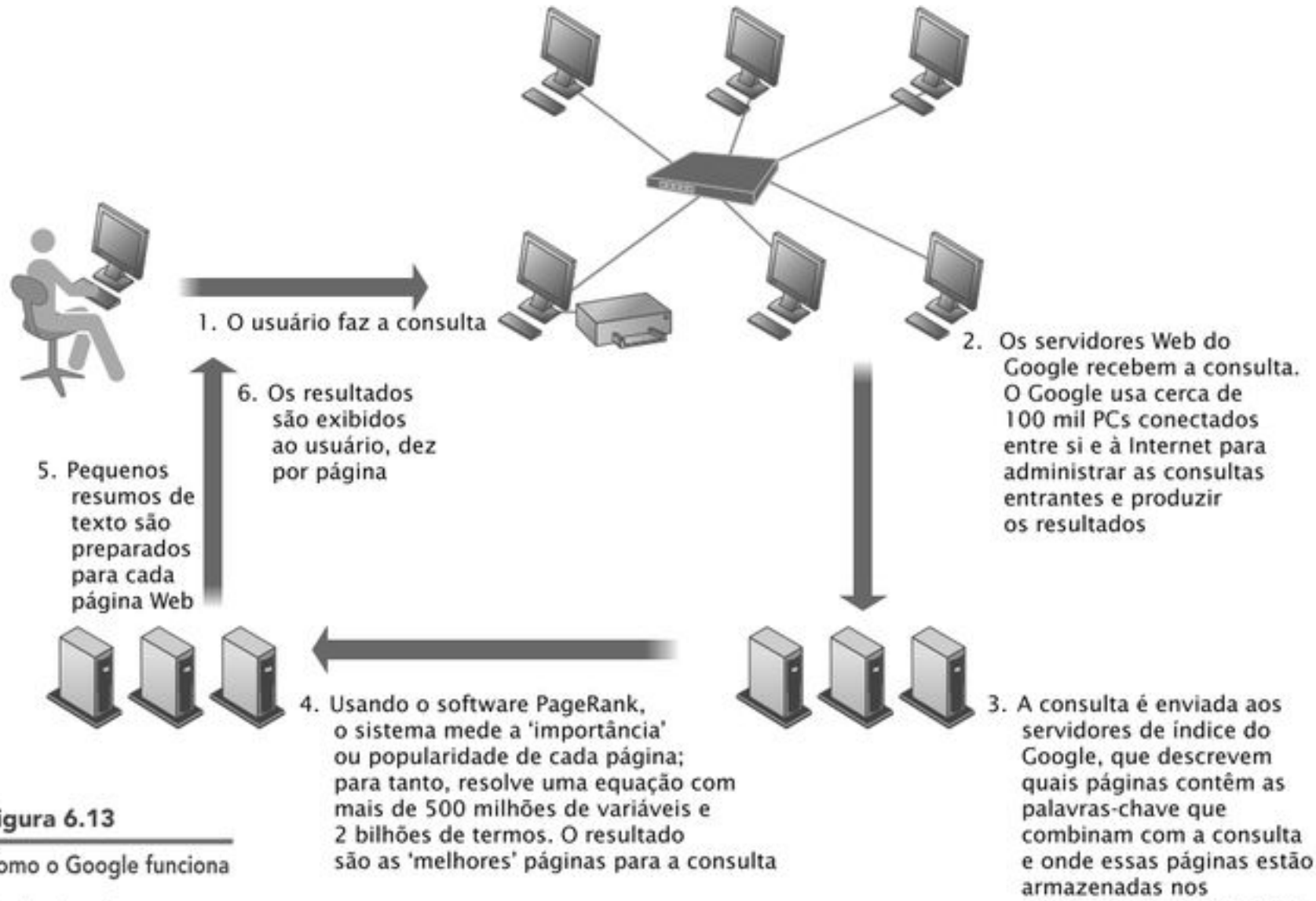


Figura 6.13

Como o Google funciona

A máquina de busca Google está continuamente vasculhando a Web, indexando o conteúdo de cada página, calculando sua popularidade e armazenando as páginas, de maneira que possa responder rapidamente às solicitações do usuário relativas a determinada página. Todo o processo leva cerca de meio segundo.

com aquelas que possivelmente serão usadas nas buscas pelos clientes potenciais. O seu site está mais propenso a estar entre os resultados no topo da lista se utilizar 'iluminação' no lugar de 'lâmpadas' caso a maioria dos clientes potenciais estejam procurando por 'iluminação'. Também é vantajoso ligar seu site ao maior número possível de outros sites, pois as máquinas de busca avaliam essas ligações para determinar a popularidade de uma página da Web e como ela está ligada a outros conteúdos na rede. A premissa é que, quanto mais links existirem em um site, mais útil esse site deve ser.

Em 2008, cerca de 100 milhões de pessoas por dia nos Estados Unidos utilizaram uma máquina de busca, produzindo mais de 17 bilhões de consultas por mês. Existem centenas de máquinas de busca, mas as três principais — Google, Yahoo! e Bing — são responsáveis por 90 por cento de todas as buscas (Figura 6.14).

Embora as máquinas de busca tenham sido originalmente criadas para pesquisa de textos em documentos, a explosão de vídeos e imagens on-line criou uma demanda por máquinas de busca que pudessem rapidamente encontrar vídeos específicos. As palavras 'dança', 'amor', 'música' e 'garota' são todas excessivamente populares nos títulos de vídeo do

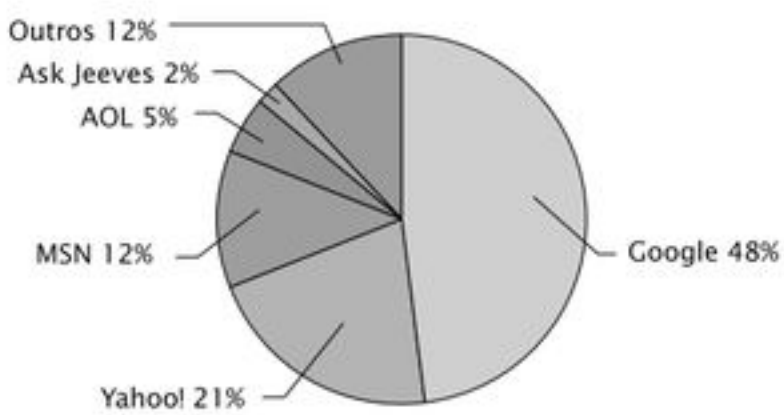


Figura 6.14

Principais máquinas de busca nos Estados Unidos

Google é a máquina de busca mais popular na Web, responsável por 70 por cento de todas as pesquisas realizadas.

YouTube, e a busca por essas palavras-chave produz uma enxurrada de resultados mesmo quando o conteúdo do vídeo não estiver relacionado ao termo pesquisado. Pesquisar vídeos é um desafio, pois os computadores não são tão bons e rápidos no reconhecimento de imagens digitais. Algumas máquinas de busca começaram a indexar roteiros de filmes para que seja possível pesquisar pelo diálogo para encontrar um filme. Uma das máquinas de busca de vídeo mais populares é a Blinkx.com, que armazena 18 milhões de horas de vídeo e emprega um grande grupo de classificadores humanos que compara o conteúdo dos vídeos enviados ao site com seus títulos.

Robôs de compras e agentes inteligentes O Capítulo 11 descreve os recursos dos agentes de software com inteligência embutida, que podem reunir ou filtrar informações e realizar outras tarefas para auxiliar os usuários. Munidos de agentes inteligentes, os **robôs de compra** pesquisam a Internet em busca de informações de compras. Robôs como o MySimon ou o Google Product Search podem ajudar as pessoas interessadas em fazer uma compra a filtrar e recuperar informações sobre produtos de seu interesse, avaliar produtos concorrentes de acordo com critérios estabelecidos pelo usuário e negociar as condições de entrega e o preço com os vendedores. Muitos desses agentes de compras pesquisam a Web em busca de preços e disponibilidade de produtos especificados pelo usuário e devolvem uma lista de sites que vendem o item com informações de preço e um link de compra.

Web 2.0

Os sites atuais não contêm somente conteúdo estático — eles permitem que as pessoas colaborem, compartilhem informações e criem novos serviços e conteúdos on-line. O termo '**Web 2.0**' refere-se a essa segunda geração de serviços interativos da Web. Se você possui fotos compartilhadas pela Internet no Flickr ou em outro site de fotos, posta um vídeo no YouTube, cria um blog, usa a Wikipedia ou inclui um *widget* em sua página do Facebook, certamente utiliza alguns recursos desses serviços da Web 2.0.

A Web 2.0 possui quatro características que a definem: interatividade, controle do usuário em tempo real, participação social (compartilhamento) e conteúdo criado pelo usuário. As tecnologias e os serviços por trás desses recursos incluem computação em nuvem, *mashups* e *widgets*, blogs, RSS, wikis e redes sociais.

Mashups e *widgets*, apresentados no Capítulo 4, são serviços de software que permitem que usuários e desenvolvedores de sistemas misturem e combinem conteúdo ou componentes de software para criar algo inteiramente novo. Por exemplo, o Flickr — site para armazenamento e compartilhamento de fotos do Yahoo! — combina fotos e outras informações sobre as imagens fornecidas pelos usuários com ferramentas para torná-las utilizáveis em outros ambientes de programação.

Essas aplicações de software rodam no próprio site, não no desktop. Com a Web 2.0, a Web deixa de ser simplesmente uma coleção de sites navegáveis para transformar-se em uma fonte de dados e serviços que podem ser combinados para criar as aplicações de que o usuário precisa. Ferramentas e serviços da Web 2.0 têm abastecido a criação de redes sociais e outras comunidades on-line nas quais as pessoas podem interagir umas com as outras da maneira que quiserem.

Um **blog**, termo popular para Weblog, é um site pessoal com uma série de postagens cronológicas (da mais nova para a mais velha) escritas por seu autor e links a páginas relacionadas. O blog pode incluir uma *blogroll* (uma coleção de links para outros blogs) e *trackbacks* (uma listagem de postagens em outros blogs que fazem referência a uma postagem no blog em questão). A maioria dos blogs permite que os leitores façam comentários sobre as postagens realizadas. Os blogs podem ser hospedados tanto em um site terceirizado — como Blogger.com, LiveJournal.com, TypePad.com e Xanga.com — ou os blogueiros podem baixar software como o Movable Type ou o Wordpress para criar um blog que é hospedado pelo provedor de Internet do usuário.

As páginas dos blogs costumam ser variações de modelos oferecidos pelo serviço ou software de blog. Por isso, milhões de pessoas sem qualquer tipo de habilidade com HTML podem publicar suas próprias páginas e compartilhar conteúdo com outras pessoas. A totalidade de sites relacionados a blogs costuma ser chamada de **blogosfera**. Embora os blogs

tenham se tornado ferramentas populares de publicação pessoal, eles também têm usos empresariais (ver capítulos 9 e 10).

Se você é um ávido leitor de blogs, pode usar RSS para manter-se atualizado sobre seus blogs favoritos sem que precise verificar constantemente as atualizações. O **RSS**, abreviatura de *Rich Site Summary*, ou *Really Simple Syndication*, agrupa conteúdos de sites de modo que possam ser utilizados em outros ambientes. A tecnologia de RSS extrai conteúdos específicos de sites e os transmite automaticamente para o computador dos usuários, onde podem ser armazenados para visualização futura.

Para receber uma informação via RSS, é preciso instalar um software agregador ou leitor de notícias que pode ser baixado da Web. (O Microsoft Internet Explorer inclui recursos de leitura de RSS.) Outra alternativa é criar uma conta em um site agregador na Web. Você informa ao agregador para coletar todas as atualizações de determinada página, ou lista de páginas, ou para coletar informações sobre determinado assunto através da realização de pesquisas na Web em intervalos específicos. Uma vez que tenha se tornado assinante, recebe automaticamente novos conteúdos à medida que eles são postados nos locais especificados.

Uma série de empresas usa RSS internamente para distribuir informações corporativas atualizadas. A Wells Fargo utiliza RSS para distribuir notícias, que os empregados podem customizar para visualizar as notícias empresariais de maior relevância a suas atividades. As fontes RSS (RSS *feeds*) são tão populares que os editores on-line estão desenvolvendo meios de apresentar anúncios com seu conteúdo.

Os blogs permitem que os visitantes adicionem comentários ao conteúdo original, mas não deixam que eles alterem o material originalmente postado. **Wikis**, em contrapartida, são sites colaborativos nos quais os visitantes podem incluir, excluir ou modificar o conteúdo do site, inclusive o trabalho de autores prévios. O termo 'wiki' vem da palavra havaiana para 'rápido'.

O software de wiki normalmente oferece modelos que definem *layouts* e elementos comuns a todas as páginas, exibem código de programa editável pelo usuário e transforma o conteúdo em uma página baseada em HTML para exibição em navegador. Alguns programas de wikis permitem somente a formatação básica de textos, enquanto outras ferramentas permitem o uso de tabelas, imagens e até elementos interativos, como pesquisas e jogos. A maioria das wikis oferece recursos para monitoração do trabalho de outros usuários e correção de erros.

Como as wikis facilitam o compartilhamento de informações, elas têm muitos usos empresariais. Os representantes de vendas da Motorola, por exemplo, usam wikis para compartilhar informações sobre vendas. Em vez de desenvolver uma abordagem de vendas para cada cliente, os representantes reutilizam as informações postadas na wiki.

O Centro Nacional de Segurança Virtual do Departamento de Segurança Interna dos Estados Unidos lançou uma wiki para facilitar a colaboração entre as agências federais no que diz respeito à segurança virtual. O Centro e outras agências utilizam a wiki para compartilhamento de informações em tempo real sobre ameaças, ataques e respostas e como um repositório de informações técnicas e padrões.

Redes sociais As redes sociais permitem que os usuários criem comunidades de amigos e colegas profissionais. Os membros costumam criar um perfil, uma página da Web na qual publicam fotos, vídeos, arquivos MP3 e texto, e então compartilham esses perfis com outros membros que identificam como amigos ou contatos. Sites de rede social são altamente interativos, oferecem ao usuário controle em tempo real e baseiam-se em conteúdo por ele gerado, além de serem largamente baseados na participação social e no compartilhamento de conteúdos e opiniões. Os principais sites de redes sociais são Facebook, MySpace (cada um com mais de 100 milhões de membros) e LinkedIn (para contatos profissionais).

Para muitos, os sites de redes sociais são o exemplo de aplicação da Web 2.0, aqueles que irão mudar radicalmente a forma como as pessoas utilizam seu tempo on-line, como se comunicam e com quem; os empresários mantêm contato com clientes, fornecedores e empregados; os anunciantes alcançam seus clientes potenciais. Os grandes sites de redes sociais também estão se transformando em plataformas de desenvolvimento de aplicações

nas quais os membros podem criar e vender aplicações para outros membros da comunidade. Só o Facebook teve mais de 1 milhão de desenvolvedores que criaram mais de 350 mil aplicativos para jogos, compartilhamento de vídeos e comunicação com amigos e familiares. Falaremos mais sobre aplicações empresariais das redes sociais nos capítulos 9 e 10, mas você também pode encontrar discussões sobre esse tema em vários outros capítulos do texto.

Web 3.0: a Web do futuro

Todos os dias, cerca de 100 milhões de norte-americanos informam 500 milhões de termos para pesquisa nas máquinas de busca. Quantas dessas consultas retornam resultados úteis (ou seja, uma resposta útil dentre os três primeiros resultados listados)? Comprovadamente, menos da metade. Google, Yahoo!, Microsoft e Amazon estão tentando aumentar as chances de as pessoas obterem respostas úteis com as pesquisas realizadas. Entretanto, com mais de 50 bilhões de páginas indexadas, os meios disponíveis para que se encontre a informação que verdadeiramente se busca são um tanto primitivos, baseados nas palavras utilizadas nas páginas e na popularidade relativa do site dentre as pessoas que utilizam os mesmos termos para pesquisa. Em outras palavras, é totalmente arbitrário.

O futuro da Web envolve, em grande parte, o desenvolvimento de técnicas que tornem a busca nos 50 bilhões de páginas mais produtiva e significativa para as pessoas comuns. A Web 1.0 resolveu o problema da obtenção do acesso à informação. A Web 2.0 solucionou o problema do compartilhamento de informações com outras pessoas e a questão da construção de novas experiências. A **Web 3.0** é a promessa de um futuro no qual todas essas informações digitais, todos esses contatos, podem ser entrelaçados em uma única experiência significativa.

Algumas vezes, essa Web é chamada de **Web Semântica**. O termo 'semântica' refere-se ao significado. A maioria do conteúdo atual da Web é projetada para ser lida por humanos e exibida por computadores; não para que programas de computador a analisem e manipulem. As máquinas de busca conseguem descobrir quando determinado termo ou palavra-chave aparece em um documento da Web, mas não conseguem realmente compreender seu significado ou como ele se relaciona a outras informações na página. É possível atestar esse fato no Google com duas pesquisas. Primeiro, digite 'Paris Hilton'. Em seguida, digite 'Hilton em Paris'. Como o Google não entende português, não faz ideia de que, na segunda pesquisa, você está interessado no Hotel Hilton em Paris. Como não consegue entender o significado das páginas que indexou, a máquina de busca retorna as páginas mais populares para as consultas nas quais 'Hilton' e 'Paris' apareçam nas páginas.

Descrita pela primeira vez em 2001, em um artigo da *Scientific American*, a Web Semântica é um esforço colaborativo liderado pelo Consórcio World Wide Web para incluir uma camada de significado acima da Web existente de modo a reduzir o volume de envolvimento humano na pesquisa e no processamento de informações na Web (Berners-Lee *et al*., 2001).

As visões sobre o futuro da Web variam, mas geralmente se concentram em maneiras de tornar a Web mais 'inteligente', com a facilitação da compreensão da informação pela máquina, promovendo uma experiência mais intuitiva e eficiente ao usuário. Digamos, por exemplo, que você deseja organizar uma festa com os colegas de tênis na sexta-feira, depois do trabalho, em um restaurante local. Um dos problemas é que você já havia marcado de ir ao cinema com outro amigo. No ambiente da Web Semântica 3.0, você conseguiria coordenar essa mudança de planos para os compromissos com os colegas de tênis e o cinema com o amigo, e fazer uma reserva no restaurante simplesmente com um conjunto de comandos informados por texto ou voz através de seu *smartphone*. Atualmente, este recurso é inconcebível.

Os trabalhos para transformação da Web em uma experiência mais inteligente seguem a passos lentos, em grande parte porque é difícil fazer com que máquinas, inclusive programas, sejam realmente inteligentes como humanos. Mas existem outras visões sobre o futuro da Web. Alguns vislumbram uma Web 3-D na qual é possível andar através de páginas em ambientes tridimensionais. Outros apontam para a ideia de uma Web disseminada que controla tudo — desde as luzes de seu quarto até o espelho retrovisor de seu carro —, sem falar na gestão de seus compromissos.

Outras tendências complementares que levam ao futuro da Web 3.0 incluem o uso mais difundido da computação em nuvem e do modelo de negócios de software como serviço, a difusão da conexão entre as plataformas móveis e os dispositivos de acesso à Internet, e a transformação da Internet de uma rede dividida em aplicações e conteúdos isolados em um conjunto mais integral e interoperável. Essas visões mais modestas do futuro da Web 3.0 têm mais chances de se materializar no curto prazo.

A revolução sem fio

Você usa seu celular para tirar e enviar fotos, encaminhar mensagens de texto ou baixar clipes de música? Leva seu laptop à classe ou à biblioteca para acessar a Internet? Se respondeu sim, faz parte da revolução sem fio! Celulares, laptops e pequenos dispositivos de mão se metamorfosearam em plataformas de computação portáteis que permitem realizar algumas das tarefas de computação que costumava fazer no seu PC.

A comunicação sem fio ajuda as empresas a entrar em contato com clientes, fornecedores e funcionários mais facilmente, além de proporcionar arranjos de organização do trabalho mais flexíveis. A tecnologia sem fio também cria novos produtos, serviços e canais de vendas, conforme discutiremos no Capítulo 9.

Se precisar de comunicação móvel e poder computacional ou acesso remoto a sistemas corporativos, você pode trabalhar com uma série de dispositivos sem fio, como telefones celulares, ***smartphones*** e computadores pessoais com conexão sem fio. Apresentamos os *smartphones* nas discussões sobre a plataforma digital móvel, nos capítulos 1 e 4. Além da transmissão de voz, eles apresentam recursos para e-mail, mensagens, acesso sem fio à Internet, fotografia digital e gestão de informações pessoais. Os recursos do iPhone e do BlackBerry ilustram o quanto os celulares evoluíram, transformando-se em pequenos computadores portáteis.

Sistemas celulares

O serviço celular digital utiliza muitos padrões concorrentes e incompatíveis. Na Europa e em grande parte do mundo, exceto nos Estados Unidos, o padrão é o Global System for Mobile Communication (GSM). O grande trunfo do GSM é sua capacidade de roaming internacional. Nos Estados Unidos, entre os sistemas de celular GSM existentes estão o T-Mobile e o AT&T Wireless.

Nos Estados Unidos, o padrão dominante é o Code Division Multiple Access (CDMA), usado por Verizon e Sprint. O CDMA foi desenvolvido pelos militares durante a Segunda Guerra Mundial. Ele transmite em várias frequências, ocupa o espectro inteiro e distribui os usuários aleatoriamente por uma série de frequências ao longo do tempo. De maneira geral, o CDMA é mais barato de implantar, mais eficaz no uso do espectro e oferece transmissão de voz e de dados de qualidade superior à do GSM.

As gerações mais antigas de celulares foram projetadas primeiramente para transmissões por voz e eram limitadas de dados em forma de mensagens de texto. Os operadoras sem fio agora oferecem redes celulares mais poderosas, denominadas redes de terceira geração (**redes 3G**), com velocidade de transmissão que vai de 144 quilobits por segundo para usuários móveis — digamos, dentro de um carro — até mais de 2 megabits por segundo para usuários estacionários. Essa capacidade de transmissão é suficiente para vídeos, recursos gráficos e outras mídias sofisticadas, além de voz, o que torna as redes 3G adequadas para o acesso à Internet de banda larga sem fio, bem como para transmissões ininterruptas de dados. Muitos dos aparelhos celulares disponíveis atualmente estão preparados para uso da rede 3G, inclusive a nova versão do iPhone da Apple.

As redes 3G são amplamente utilizadas no Japão, Coreia do Sul, Taiwan, Hong Kong, Cingapura e em partes do norte da Europa. Em regiões dos Estados Unidos sem a cobertura das redes 3G, as operadoras de celular atualizaram suas redes para suporte à transmissão de alta velocidade. Nesse meio-tempo, as redes 2,5G oferecem transmissões de dados que vão de 60 a 354 quilobits por segundo, permitindo que os celulares sejam utilizados para acesso

à Internet, download de músicas e outros serviços de banda larga. A rede EDGE, da AT&T, utilizada pela primeira geração de iPhones é um exemplo. PCs equipados com uma placa especial podem utilizar esses serviços de banda larga dos celulares a qualquer instante e em qualquer lugar onde exista conexão sem fio com a Internet.

A próxima evolução em comunicação sem fio, denominada **rede 4G**, é totalmente comutada por pacotes e capaz de oferecer velocidades que vão de 1 megabit por segundo a 1 gigabit por segundo, com qualidade superior e alta segurança. Voz, dados e vídeo de alta qualidade estarão disponíveis aos usuários em qualquer lugar. A expansão comercial das redes 4G acontecerá nos próximos anos. As empresas de telecomunicações como Sprint, Verizon e NTT DoCoMo já começaram a desenvolver sistemas 4G.

Acesso à Internet e redes de computação sem fio

Se você tem um laptop, talvez possa usá-lo para acessar a Internet enquanto caminha de área em área na sua casa, ou de mesa em mesa na biblioteca da universidade. Uma gama de tecnologias vem surgindo para proporcionar acesso sem fio de alta velocidade à Internet a partir de PCs e outros dispositivos de mão sem fio, ou mesmo de celulares. Esses novos serviços de alta velocidade têm levado o acesso à Internet a inúmeros lugares que não são cobertos pelos serviços de Internet cabeados tradicionais.

Bluetooth

Bluetooth é o nome popular do padrão de rede sem fio 802.15, utilizado para criar pequenas **redes pessoais (PANs — *Personal-Area Network*)**. Ele conecta até oito dispositivos em um raio de dez metros usando comunicação baseada em rádio de baixa potência, e pode transmitir até 722 quilobits por segundo na faixa de 2,4 GHz.

Telefones sem fio, pagers, computadores, impressoras e dispositivos de computação que usam o Bluetooth se comunicam uns com os outros e até mesmo operam uns aos outros sem a intervenção direta do usuário (veja a Figura 6.15). Por exemplo, uma pessoa pode selecionar um número de telefone em um PDA sem fio e automaticamente ativar uma chamada no celular digital, ou essa pessoa pode instruir o notebook a enviar um documento a uma

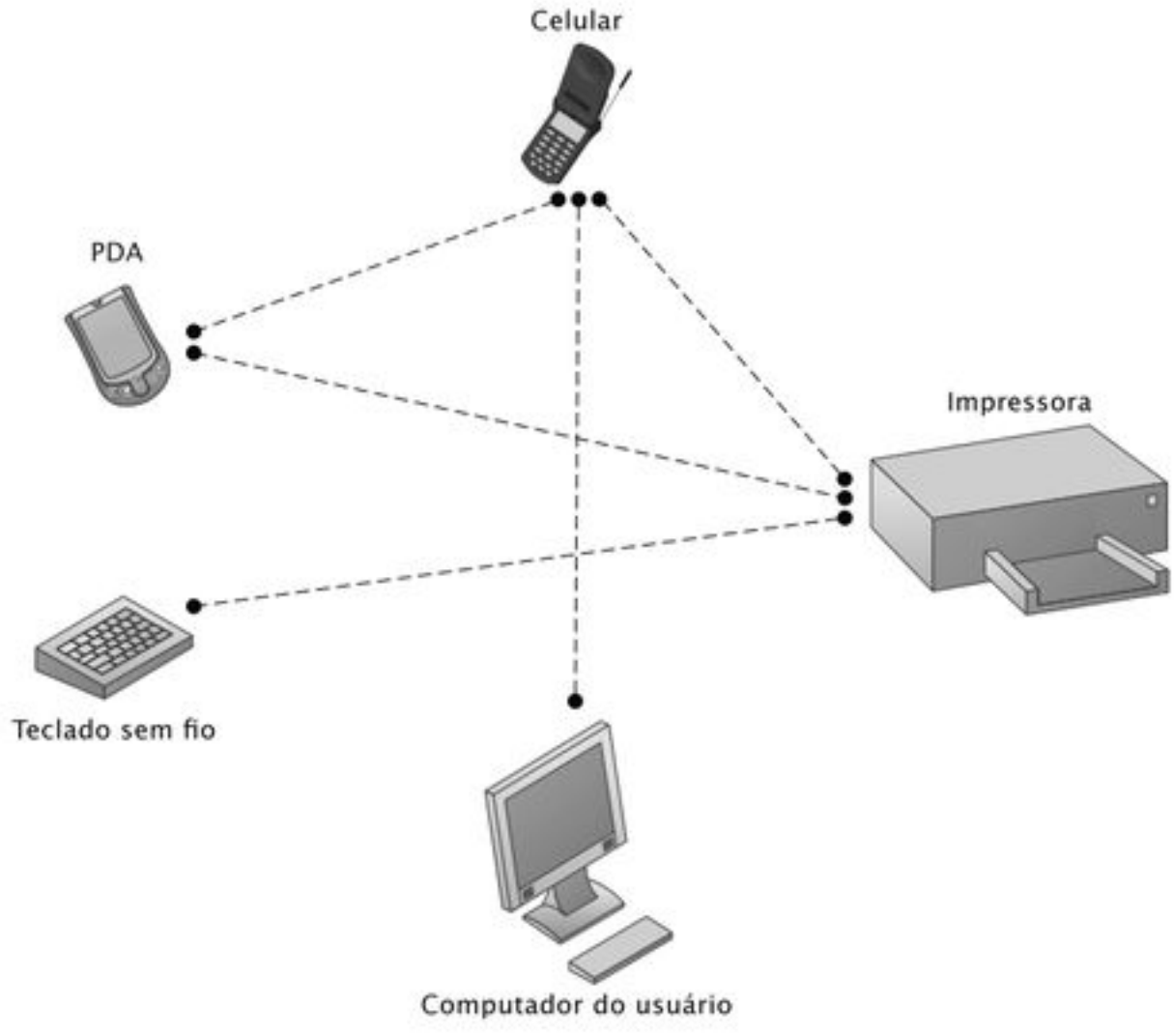


Figura 6.15

Rede Bluetooth (PAN)

O Bluetooth permite que uma variedade de dispositivos, incluindo celulares, PDAs, mouses e teclados sem fio, PCs e impressoras interaja entre si sem a necessidade de fios, dentro de uma área de dez metros. Além das conexões mostradas aqui, o Bluetooth pode ser usado para colocar em rede dispositivos similares, permitindo que sejam enviados dados de um PC a outro, por exemplo.

impressora sem usar fios. O Bluetooth consome pouca energia e é adequado para dispositivos que funcionam com bateria, como computadores de mão, celulares ou PDAs.

Embora caia como uma luva para o trabalho em redes pessoais, o Bluetooth também pode ser usado em grandes corporações. Os motoristas da FedEx, por exemplo, usam Bluetooth para transmitir dados das vendas coletados com seus computadores PDA PowerPad para transmissores celulares, que repassam os dados aos computadores da empresa. Os motoristas não precisam mais perder tempo conectando fisicamente seus PDAs aos transmissores; além disso, o Bluetooth trouxe uma economia de 20 milhões de dólares para a FedEx.

Wi-Fi

O conjunto de padrões IEEE para LANs sem fio é a família 802.11, também conhecida como **Wi-Fi** (abreviatura de *Wireless Fidelity*, ou Fidelidade sem Fio). Existem três padrões nessa família: o 802.11a, o 802.11b e o 802.11g. O 802.11n é um padrão emergente que pretende aumentar a velocidade e capacidade das redes sem fio.

O padrão 802.11a pode transmitir até 54 megabits por segundo na faixa de frequência de 5 GHz — banda não licenciada — e cobre uma distância efetiva de 10 a 30 metros. O padrão 802.11b pode transmitir até 11 megabits por segundo na faixa de 2,4 GHz — banda não licenciada — e cobre uma distância efetiva de 30 a 50 metros, embora essa distância possa ser ampliada em ambientes externos utilizando-se antenas instaladas em torres. O padrão 802.11g pode transmitir até 54 megabits por segundo na faixa de 2,4 GHz. Uma vez finalizado, o padrão 802.11n transmitirá a uma velocidade acima de 600 megabits por segundo.

O padrão 802.11b foi o mais largamente utilizado para a criação de LANs sem fio e acesso à Internet sem fio. No entanto, o 802.11g está se tornando cada vez mais utilizado para esses fins, e já são disponibilizados sistemas capazes de lidar com o padrão 802.11n.

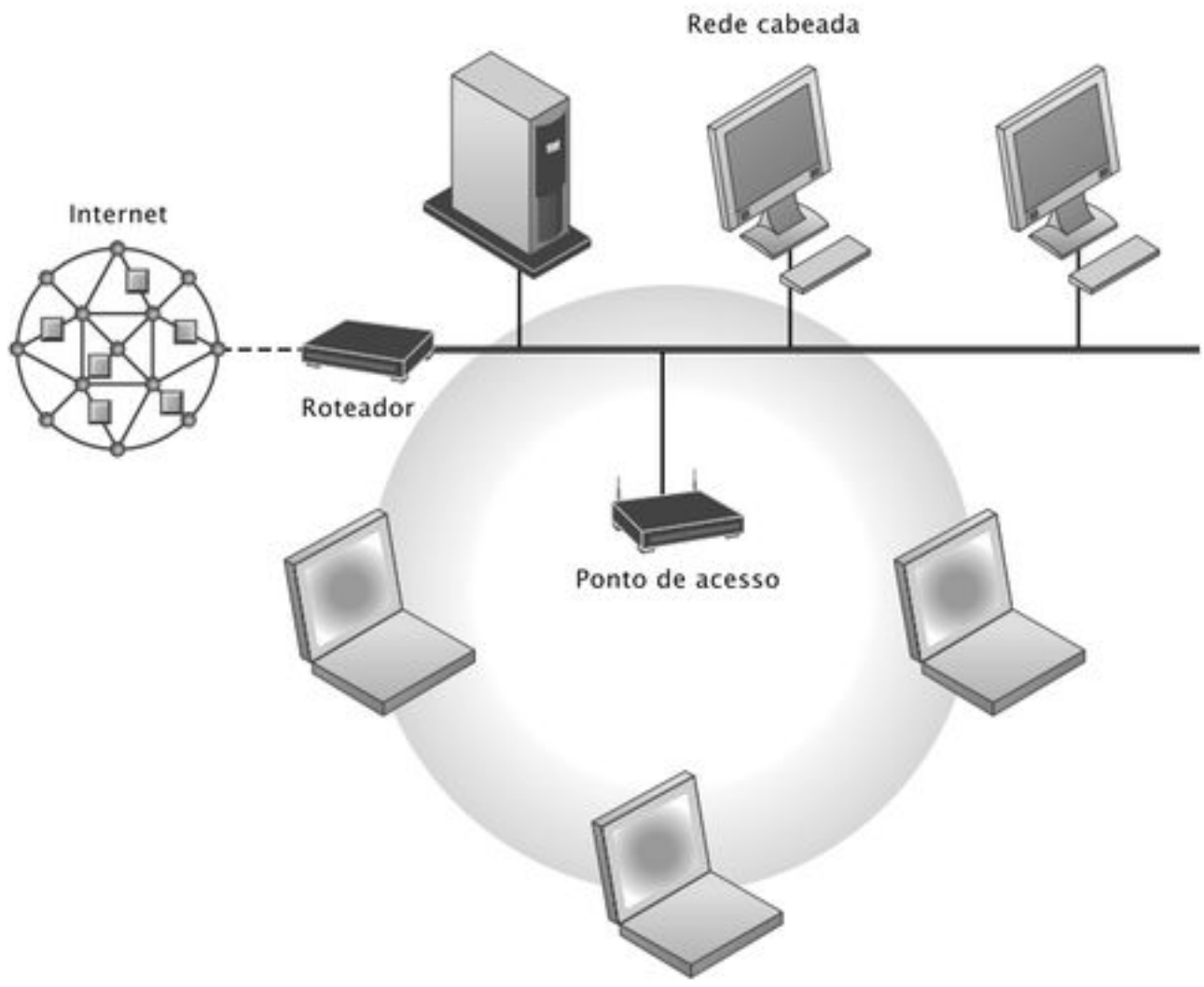
Na maioria das comunicações Wi-Fi, os dispositivos sem fio se comunicam com uma LAN cabeada por meio de pontos de acesso. Ponto de acesso é uma caixa composta por um transmissor/receptor de rádio e por antenas conectadas a uma rede cabeada, um roteador ou hub.

A Figura 6.16 ilustra uma LAN sem fio 802.11 que opera em um modo de infraestrutura e conecta um pequeno número de dispositivos portáteis à LAN cabeada maior. Em sua maioria, os dispositivos portáteis são máquinas clientes. Os servidores que as estações

Figura 6.16

Uma LAN sem fio 802.11

Laptops equipados com cartões de interface de rede conectam-se a uma LAN cabeada por meio do ponto de acesso. O ponto de acesso usa ondas de rádio para transmitir sinais da rede cabeada aos adaptadores clientes, onde esses sinais são convertidos em dados que os dispositivos portáteis possam entender. O adaptador cliente transmite, então, os dados do dispositivo portátil de volta para o ponto de acesso, que os repassa à rede cabeada.



clientes portáteis precisam utilizar estão na rede cabeada. O ponto de acesso controla as estações sem fio, atuando como uma ponte entre a LAN cabeada principal e a sem fio. (Uma ponte conecta duas LANs baseadas em tecnologias diferentes.) O ponto de acesso também controla as estações sem fio.

Laptops mais recentes vêm equipados com chips aptos a receber sinais de Wi-Fi. Os modelos mais antigos podem precisar de uma placa de rede sem fio.

Wi-Fi e acesso à Internet sem fio

O padrão 802.11 também oferece acesso sem fio à Internet por meio de uma conexão de banda larga. Nesse caso, um ponto de acesso se liga a uma conexão Internet, que pode vir de uma linha de TV a cabo ou de um serviço telefônico DSL. Os computadores dentro do alcance de um ponto de acesso poderiam utilizá-lo para conexão sem fio à Internet.

Empresas de todos os portes estão usando redes Wi-Fi para oferecer acesso à Internet e LANs sem fio de baixo custo. Hotspots de Wi-Fi se disseminam em hotéis, salas de espera de aeroportos, bibliotecas e *campi* universitários, proporcionando acesso móvel à Internet. O Dartmouth College é um dos muitos *campi* onde os alunos atualmente podem usar Wi-Fi para pesquisa, estudo e entretenimento.

Hotspots normalmente consistem em um ou mais pontos de acesso posicionados no teto, no muro ou em outro ponto estratégico de um lugar público para proporcionar a máxima cobertura sem fio em uma área específica. Os usuários dentro do alcance de um hotspot podem acessar a Internet a partir de seus laptops, handhelds ou telefones celulares que são Wi-Fi, como o iPhone da Apple. Alguns hotspots são gratuitos ou não exigem softwares adicionais para serem usados; outros podem exigir ativação e a abertura de uma conta de usuário, mediante o fornecimento de um número de cartão de crédito.

Apesar disso tudo, a tecnologia Wi-Fi apresenta muitos desafios. Até este momento, os usuários não podem passar livremente de um hotspot para outro, se esses usarem diferentes serviços de rede Wi-Fi. A menos que o serviço seja gratuito, os usuários teriam de se logar em contas diferentes para cada serviço, cada uma com suas próprias tarifas.

Uma das principais desvantagens das redes sem fio é sua fraqueza nos recursos de segurança, que faz com que elas se tornem vulneráveis a invasores. O Capítulo 8 fornece maiores detalhes sobre as questões de segurança em redes sem fio.

Outra desvantagem das redes Wi-Fi é a suscetibilidade à interferência de sistemas próximos que operem no mesmo espectro, como telefones sem fio, fornos de micro-ondas e outras LANs sem fio. Redes sem fio baseadas na especificação 802.11n resolvem esse problema, pois usam várias antenas sem fio em conjunto para transmitir e receber dados, além de tecnologia denominada *MIMO* (de *Multiple Input Multiple Output*, ou múltipla saída, múltipla entrada) para coordenar os vários sinais de rádio simultâneos.

WiMax

Nos Estados Unidos e em todo o mundo, um número surpreendentemente grande de regiões não tem acesso à conectividade de banda larga, fixa ou Wi-Fi. Como o alcance dos sistemas Wi-Fi não passa de 90 metros da estação base, é difícil para comunidades rurais que não contam com serviço a cabo ou DSL conseguir acesso sem fio à Internet.

Para lidar com esses problemas, o IEEE desenvolveu uma nova família de padrões conhecida como WiMax. O **WiMax**, abreviatura de *Worldwide Interoperability for Microwave Access*, ou Interoperabilidade Mundial para Acesso por Micro-ondas, é o termo popular para o Padrão IEEE 802.16, conhecido como a 'Interface Aérea para Sistemas Fixos de Acesso sem Fio de Banda Larga'. O WiMax tem uma cobertura de acesso sem fio que chega a quase 50 quilômetros, bem mais do que os 90 metros do Wi-Fi e os 9 metros do Bluetooth, e uma taxa de transferência de dados de até 75 megabits por segundo. A especificação 802.16 também exibe sólidos atributos de segurança e qualidade de serviço para transmissão de voz e vídeo.

As antenas WiMax são potentes o bastante para transmitir conexões de Internet de alta velocidade a antenas instaladas no telhado de residências e empresas a quilômetros de distância. Celulares e computadores equipados com recursos de WiMax estão começando a

aparecer no mercado. A Clearwire, que pertence à Sprint Nextel, utiliza tecnologia WiMax como base das redes 4G que está implantando nos Estados Unidos. Os planos da Clearwire eram de oferecer esse serviço a 120 milhões de pessoas até o final de 2010. Entretanto, o futuro do WiMax é incerto porque a Verizon Wireless e os provedores sem fio estão baseando suas redes 4G em uma tecnologia concorrente chamada Long-Term Evolution (LTE).

Redes de sensores sem fio e RFID

As tecnologias móveis estão criando novas maneiras de trabalhar e produzir melhor em todos os departamentos de uma empresa. Além dos sistemas sem fio que acabamos de descrever, os sistemas de identificação por radiofrequência (RFID) e as redes de sensores sem fio estão causando impacto.

Identificação por radiofrequência (RFID)

Os sistemas de **identificação por radiofrequência (RFID — *radio frequency identification*)** representam uma poderosa tecnologia para rastrear a movimentação de mercadorias ao longo da cadeia de suprimentos. Os sistemas RFID usam minúsculas etiquetas com microchips embutidos com dados sobre um item e sua localização para transmitir sinais de rádio a curta distância para leitores RFID. Os leitores RFID repassam, então, os dados por rede a um computador que os processa. Diferentemente dos códigos de barra, as etiquetas RFID não precisam estar na linha de visão da leitora para serem reconhecidas.

A etiqueta RFID é eletronicamente programada com informações capazes de identificar um item de maneira exclusiva, além de outros dados sobre o item, como localização, onde e quando foi fabricado ou seu estágio durante a produção. Embutido na etiqueta está um chip que armazena esses dados. O restante da etiqueta é uma antena que transmite os dados para o leitor.

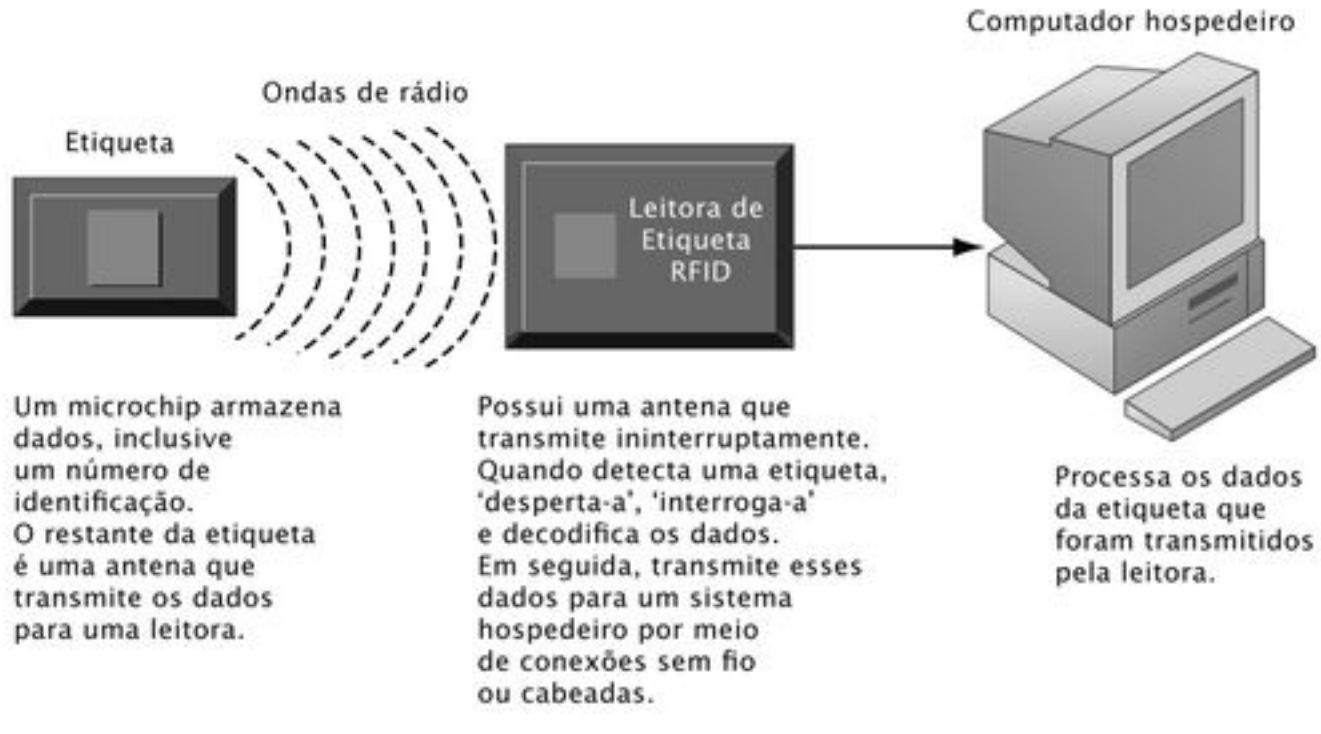
A unidade leitora consiste em uma antena e um transmissor de rádio com função de decodificação, anexados a um dispositivo de mão ou estacionário. A leitora emite ondas de rádio em um raio que vai de 2,5 centímetros até 30 metros, dependendo de sua potência de saída, da frequência de rádio empregada e das condições do ambiente circundante. Quando uma etiqueta RFID entra no raio do leitor, essa etiqueta é ativada e começa a enviar dados. O leitor captura tais dados, decodifica-os e envia-os de volta por uma rede sem fio ou cabeada até um computador hospedeiro, para posterior processamento (veja a Figura 6.17). Tanto as antenas quanto as etiquetas RFID podem ter vários formatos e tamanhos.

As etiquetas RFID ativas são alimentadas por bateria interna e costumam permitir que os dados sejam regravados e modificados. As etiquetas ativas podem transmitir para centenas de metros, mas podem custar muitos dólares e encarecer as etiquetas. Sistemas automatizados de cobrança de pedágio como o E-ZPass, de Nova York, utilizam etiquetas RFID ativas.

Figura 6.17

Como o RFID funciona

O RFID usa transmissores de rádio de baixa potência para ler dados armazenados em uma etiqueta a distâncias que variam de 2,5 centímetros a 30 metros. A leitora captura os dados da etiqueta e os envia por rede a um computador hospedeiro, onde serão processados.



Etiquetas RFID passivas não possuem fonte própria de energia e obtêm seu poder operacional da energia por radiofrequência transmitida pelo leitor RFID. São menores, mais leves e mais baratas do que as etiquetas ativas, mas alcançam somente alguns metros.

Na gestão da cadeia de suprimento e no controle de estoques, os sistemas RFID capturam e gerenciam informações mais detalhadas sobre itens em armazéns ou na produção do que os sistemas de código de barras. Se um grande número de itens for expedido de uma vez, os sistemas RFID rastreiam cada palete, lote ou até mesmo itens unitários do carregamento. Essa tecnologia pode ajudar as empresas como o Walmart a aprimorar as operações de recebimento e armazenamento através da melhoria da habilidade de 'enxergar' exatamente o estoque dos armazéns ou das prateleiras das lojas de varejo.

O Walmart, nos Estados Unidos, instalou leitores de RFID nas plataformas de recebimento das lojas para registrar a chegada de paletes e caixas de produtos enviados com etiquetas RFID. O leitor lê a etiqueta uma segunda vez à medida que as caixas são levadas das áreas de armazenamento para o andar de vendas. Um software combina os dados de venda do PDV do Walmart com os dados RFID relacionados ao número de caixas levadas para o andar de vendas. O programa determina os itens que logo estarão esgotados e gera automaticamente uma lista de produtos a serem trazidos do armazém para reabastecer as prateleiras das lojas antes que se esvaziem. Essa informação ajuda o Walmart a reduzir os itens com estoque zerado, aumenta as vendas e reduz os custos.

O custo das etiquetas RFID costumava ser muito alto para que se fizesse amplo uso delas, mas agora uma etiqueta passiva custa menos do que 10 centavos de dólar nos Estados Unidos. À medida que o preço cai, a tecnologia RFID começa a ter um custo compensador para algumas aplicações.

Além de instalar leitoras RFID e sistemas de etiquetagem, as empresas talvez precisem fazer upgrade em seu hardware e software para processar as gigantescas quantidades de dados produzidos pelos sistemas RFID — transações que podem totalizar dezenas ou centenas de terabytes.

Um software é utilizado para filtrar e agregar os dados RFID e evitar que sobrecarreguem as redes da empresa e os aplicativos de sistema. Com frequência, os aplicativos precisam ser reprojetados para aceitar os grandes volumes de dados gerados pelo RFID e compartilhar esses dados com outros aplicativos. Os principais fornecedores de software integrado, incluindo SAP e Oracle-PeopleSoft, já oferecem versões prontas para RFID de seus aplicativos de gestão da cadeia de suprimentos.

Redes de sensores sem fio

Se sua empresa quisesse tecnologia de última geração para monitorar a segurança de edifícios ou detectar substâncias perigosas, poderia lançar mão de uma rede de sensores sem fio. **Redes de sensores sem fio (WSNs — *wireless sensor networks*)** são redes de dispositivos sem fio interconectados e introduzidos no ambiente físico para fornecer medições de vários pontos em grandes espaços. Elas se baseiam em dispositivos com sensores e antenas de radiofrequência, armazenamento e processamento embutidos. Esses dispositivos se unem por uma rede interconectada que direciona os dados capturados por eles para um computador que fará a análise.

Essas redes possuem desde centenas até milhares de nós. Como os dispositivos sensores sem fio ficam anos instalados, sem manutenção ou interferência humana, precisam ter consumo de energia baixíssimo e baterias capazes de resistir longos períodos — por anos, na verdade.

A Figura 6.18 ilustra um tipo de rede de sensores sem fio, com dados oriundos dos nodos individuais fluindo pela rede em direção de um servidor com maior poder de processamento. O servidor atua como uma porta (*gateway*) para uma rede baseada em tecnologia Internet.

As redes de sensores sem fio são muito úteis em áreas como monitoramento de mudanças ambientais; monitoramento de tráfego ou atividade militar; proteção de propriedade; operação e gestão eficiente de máquinas e veículos; estabelecimento de perímetros de segurança; monitoramento da gestão da cadeia de suprimento; e detecção de materiais radioativos, biológicos ou químicos.

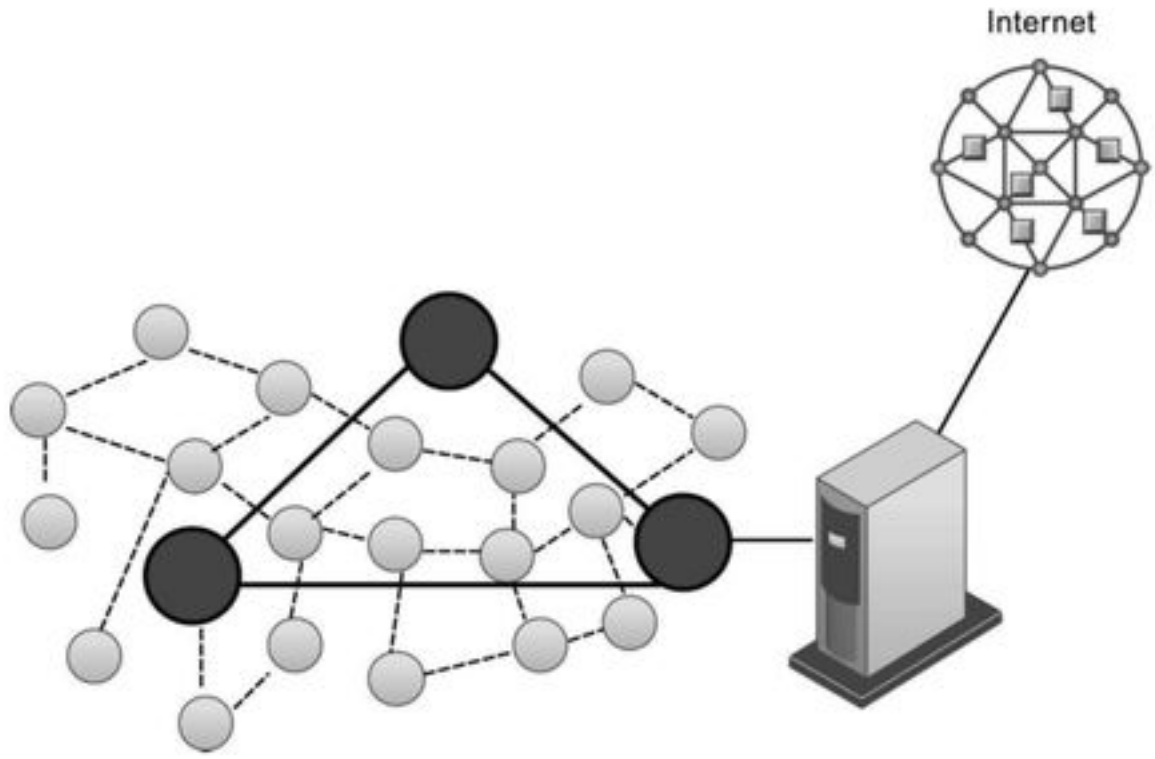


Figura 6.18

Uma rede de sensores sem fio

Os pequenos círculos representam os nós de nível mais baixo, enquanto os círculos maiores representam os nós do topo. Os nós de nível mais baixo repassam os dados uns para os outros ou para os nós de nível mais alto, que transmitem os dados mais rapidamente e aumentam o desempenho da rede.

Projetos práticos em SIG

Os projetos nesta seção oferecem experiência prática na avaliação e seleção de tecnologia de comunicação, utilizando software de planilha eletrônica para aprimorar a seleção de serviços de telecomunicação e usando máquinas de busca da Internet para pesquisas empresariais.

Problemas de decisões gerenciais

1. Sua empresa fornece tijolos de cerâmica para Home Depot, Lowe's, e outras lojas de artigos para o lar. Solicitaram que começasse a utilizar etiquetas de identificação por radiofrequência em cada caixa de tijolos despachada para ajudar os clientes a melhorar a gestão de seus produtos e o de outros fornecedores em seu armazém. Use a Web para identificar o custo de componentes de hardware, software e redes para um sistema RFID. Quais fatores devem ser considerados? Quais as principais decisões a serem tomadas na decisão sobre a adoção dessa tecnologia?
2. A BestMed Medical Supplies Corporation vende produtos e equipamentos médicos e cirúrgicos de mais de 700 fornecedores distintos para hospitais, clínicas médicas e consultórios. A empresa emprega 500 pessoas em sete localidades diferentes em estados do oeste e do meio-oeste, e conta com gerentes de contas, representantes para atendimento e suporte aos clientes, além do pessoal de armazém. Os empregados se comunicam através de serviços tradicionais de telefone por voz, e-mail, mensagens instantâneas e telefones celulares. A gerência deseja saber se a empresa deve adotar um sistema unificado de comunicação. Quais as principais decisões a serem tomadas na decisão sobre a adoção dessa tecnologia? Use a Web, se necessário, para descobrir mais a respeito de comunicações unificadas e seu custo.

Aperfeiçoando a tomada de decisão: usando software de planilha eletrônica para avaliar serviços sem fio

Habilidades de software: fórmulas de planilhas, formatação

Habilidades organizacionais: análise de serviços e custos de telecomunicações

Neste projeto, você vai utilizar a Web para pesquisar serviços sem fio alternativos e utilizará software de planilha eletrônica para calcular os custos dos serviços sem fio para uma força de vendas.

Você gostaria de equipar sua força de vendas, formada por 35 pessoas e baseada em Cincinnati, Ohio, com celulares capazes de transmitir voz, enviar mensagens de texto e tirar e enviar fotos. Use a Web para selecionar um provedor de serviços sem fio que ofereça

serviços nos Estados Unidos, assim como bons serviços em sua região. Examine as características dos aparelhos celulares que cada fornecedor oferece. Suponha que cada um dos 35 vendedores gaste 3 horas por dia durante o expediente (das 8 às 18 horas) em comunicação de voz móvel, envie 30 mensagens de texto por dia e 5 fotos por semana. Use seu software de planilha para determinar o serviço sem fio e o aparelho que oferecem o melhor preço por usuário durante um período de dois anos. Para os propósitos deste exercício, não precisa considerar os descontos corporativos.

Alcançando excelência operacional: usando máquinas de busca na Web para pesquisa empresarial

Habilidades de software: fórmulas de planilhas eletrônicas, formatação
Habilidades empresariais: análise de serviços e custos de telecomunicações

Este projeto ajudará a desenvolver sua habilidade para usar máquinas de busca na Web na pesquisa empresarial.

Você deseja saber mais a respeito do etanol como combustível alternativo para veículos motorizados. Use as máquinas de busca a seguir para obter essas informações: Yahoo!, Google e Bing. Se quiser, experimente também outros sistemas. Compare o volume e a qualidade da informação que encontra com cada ferramenta de busca. Qual é mais fácil de usar? Qual produziu os melhores resultados para sua pesquisa? Por quê?

Resumo

1. **Quais os principais componentes das redes de telecomunicações e as principais tecnologias de rede?** Uma rede simples consiste em dois ou mais computadores conectados. Os componentes de rede básicos incluem computadores, interfaces de rede, um meio de conexão, um software de sistema operacional de rede e um hub ou switch. Em uma grande empresa, a infraestrutura de rede depende de infraestruturas públicas e privadas que comportem o movimento de informações através de diversas plataformas tecnológicas. Isso inclui o sistema telefônico tradicional, a comunicação celular móvel, redes locais sem fio, sistemas de videoconferência, um site corporativo, intranets, extranets e uma gama de redes remotas e locais, inclusive a Internet.

As redes contemporâneas foram moldadas pelo surgimento da computação cliente/servidor, pelo uso da comutação de pacotes e pela adoção do *Transmission Control Protocol/Internet Protocol* (TCP/IP) como padrão universal de comunicações para conectar diferentes redes e computadores, inclusive a Internet. Os protocolos oferecem um conjunto de regras comuns que permitem a comunicação entre diversos componentes em uma rede de telecomunicações.

2. **Quais os principais meios de transmissão e tipos de rede?** Os principais meios de transmissão física são os fios telefônicos de cobre trançado, os cabos de cobre coaxiais, os cabos de fibra óptica e a transmissão sem fio. Embora seja relativamente lento, o par trançado permite que as empresas usem o cabeamento dos sistemas telefônicos preexistente para a comunicação digital. Os cabos coaxiais e de fibra óptica são usados para transmissões de alto volume, mas sua instalação é cara. Micro-ondas e satélites são usados para comunicação sem fio a longas distâncias. Redes locais (LANs) conectam PCs e outros dispositivos digitais em um raio de 500 metros; hoje, são utilizadas para muitas tarefas computacionais corporativas. Os componentes de rede podem ser conectados em topologia de estrela, de anel ou em barramento. Redes remotas (WANs) abrangem grandes distâncias geográficas, que vão de muitos quilômetros até o alcance global; trata-se de redes privadas administradas de maneira independente. Redes metropolitanas (MANs) abrangem uma única área urbana.

As tecnologias de linha digital de assinante (DSL), as conexões de Internet a cabo e as linhas T1 costumam ser usadas para conexões da Internet de alta capacidade.

As conexões de Internet a cabo oferecem acesso de alta velocidade à Web ou a intranets corporativas a velocidades de até 10 megabits por segundo. Uma linha T1 comporta uma taxa de transmissão de dados de 1,544 megabit por segundo.

3. **Como a Internet e a tecnologia de Internet funcionam e como facilitam a comunicação e o comércio eletrônico?** A Internet é uma rede de redes mundial que utiliza o modelo de computação cliente/servidor e um modelo de referência de rede TCP/IP. Cada computador na Internet recebe um endereço IP exclusivo. O Sistema de Nome de Domínio (DNS) converte endereços IP em nomes de domínio, de maneira que os usuários apenas precisam especificar o domínio para acessar um computador na Internet, em vez de digitar seu endereço IP numérico. Políticas de Internet internacionais são estabelecidas por institutos e organismos públicos, tais como o Internet Architecture Board e o World Wide Web Consortium.

Entre os principais serviços de Internet estão e-mail,

newsgroup, bate-papo, mensagens instantâneas, Telnet, FTP e a World Wide Web. As páginas da Web baseiam-se na HTML (*hypertext markup language*) e podem exibir texto, elementos gráficos, vídeo e áudio. Diretórios de sites, máquinas de busca e tecnologia RSS ajudam os usuários a localizar as informações de que precisam na Web. RSS, blogs, redes sociais e wikis são recursos da Web 2.0
As empresas também estão começando a economizar usando a tecnologia VoIP para transmissão de voz, e utilizando redes privadas virtuais (VPNs) como alternativa de baixo custo às WANs privadas.

4. Quais as principais tecnologias e padrões para redes, comunicação e acesso à Internet sem fio? Redes celulares estão evoluindo para redes de alta velocidade, com ampla largura de banda e baseadas na comutação de pacotes. As redes de banda larga 3G são capazes de transmitir dados a velocidades que vão de 144 quilobits por segundo a mais de 2 megabits por segundo. As redes 4G estão começando a ser lançadas e alcançam velocidades de transmissão que podem chegar a 1 gigabit por segundo.
Entre os principais padrões de celular estão o Code Division Multiple Access (CDMA), usado majoritariamente nos Estados Unidos, e o Global System for Mobile Communication (GSM), padrão na Europa e em grande parte do mundo.
Entre os padrões para redes de computadores sem fio estão o Bluetooth (802.15) para pequenas redes pessoais (PANs), o Wi-Fi (802.11) para redes locais (LANs) e o WiMax (802.16) para redes metropolitanas (MANs).

5. Por que a identificação por radiofrequência e as redes de sensores sem fio são tão importantes para as empresas? Os sistemas de identificação por radiofrequência (RFID) representam uma potente tecnologia para controle da movimentação de produtos através da utilização de pequenas etiquetas com dados embutidos sobre um item e sua localização. As leitoras RFID leem os sinais de rádio transmitidos por essas etiquetas e transmitem, então, os dados por rede a um computador encarregado de processá-los. As redes de sensores sem fio (WSNs) são redes de dispositivos sem fio, com alguma capacidade de transmissão por rádio e processamento, interconectados e incorporados no ambiente físico, cujo objetivo é fornecer medições de vários pontos em grandes espaços.

Palavras-chave

Banda larga, 174
Bate-papo, 189
Blog, 197
Blogosfera, 197
Bluetooth, 201
Cabo coaxial, 182
Cabos de fibra óptica, 182
Cartão de interface de rede (NIC), 175
Comunicações unificadas, 192
Comutação de pacotes, 177
Conexões de Internet a cabo, 184
E-mail, 189
Endereço IP (Internet Protocol), 185
File Transfer Protocol (FTP), 189
Hertz, 183
Hotspots, 203
Hubs, 176
Identificação por radiofrequência (RFID), 204
Internet2, 188
Largura de banda, 183
Linha digital de assinante (DSL), 184
Linhas T1, 184
Localizador uniforme de recursos (*uniform resource locator* — URL), 194
Máquinas de busca, 194
Marketing de máquina de busca, 195
Mensagem instantânea, 190
Micro-ondas, 182
Modem, 179
Nome de domínio, 185
Otimização de máquinas de busca (*search engine optimization* — SEO), 195
Par trançado, 182
Peer-to-peer (ponto a ponto), 180
Protocolo, 178
Protocolo de transferência de hipertexto (HTTP), 194
Provedor de serviços de Internet (ISP), 184
Rede 4G, 201
Rede em estrela, 181
Rede local (*local-area network* — LAN), 180
Rede metropolitana (metropolitan-area network — MAN), 181
Rede virtual privada (VPN), 193
Redes de sensores sem fio (WSNs), 205
Redes 3G, 200
Redes em anel, 181
Redes em barramento, 181
Redes pessoais (personal-area networks — PANs), 201
Redes remotas (*wide-area networks* — WANs), 181
Redes sociais, 198
Robôs de compras, 197
Roteador, 176
RSS, 198
Sistema de Nomes de Domínio (DNS), 185
Sistema operacional de rede (NOS), 175
Site, 194
Smartphones, 200
Switch, 176
Telefone celular, 183
Telnet, 189
Topologia, 181
Transmission Control Protocol Internet Protocol (TCP/IP), 178
Voz sobre IP (VoIP), 190
Web 2.0, 197
Web 3.0, 199
Web Semântica, 199
Wi-Fi, 202
Wikis, 198
WiMax, 203

Questões

1. Quais os principais componentes das redes de telecomunicações e das principais tecnologias de rede?

- Descreva as características de uma rede simples e da infraestrutura de rede de uma grande empresa.
- Nomeie e descreva as principais tecnologias e tendências que moldaram os sistemas de telecomunicação contemporâneos.

2. Quais os principais meios de transmissão e os principais tipos de rede?

- Nomeie os diferentes meios de transmissão física e compare-os em termos de velocidade e custo.
- Defina rede local (LAN), descreva seus componentes e as funções de cada um.
- Nomeie e descreva as principais topologias de rede.

3. Como funcionam a Internet e a tecnologia da Internet? Como elas suportam a comunicação e o comércio eletrônico?

- Defina Internet, descreva como ela trabalha e explique como ela agrega valor para as empresas.
- Explique como funcionam os sistemas de nome de domínio e de endereçamento IP.
- Defina e descreva VoIP e redes virtuais privadas, e explique como eles agregam valor para as empresas.
- Liste e descreva as diferentes maneiras de localizar informações na Web.
- Compare a Web 2.0 e a Web 3.0.

4. Quais os principais padrões e tecnologias para redes sem fio, comunicações e acesso à Internet?

- Compare Bluetooth, Wi-Fi, WiMax e redes 3G.
- Descreva os recursos de cada um deles e os tipos de aplicação ao qual cada um deles se adapta melhor.

5. Por que a tecnologia RFID e as redes de sensores sem fio são valiosas para os negócios?

- Defina RFID, explique como essa tecnologia funciona e explique como ela agrega valor às empresas.
- Defina redes de sensores sem fio, explique como funcionam e descreva os tipos de aplicação que as utilizam.

Para discutir

1. Foi dito que nos próximos anos os *smartphones* irão se tornar o dispositivo portátil mais importante que teremos. Discuta as implicações dessa afirmação.

2. Todas as grandes empresas varejistas e industriais deveriam migrar para o RFID? Por quê?

Colaboração e trabalho em equipe

Avaliando smartphones

Forme um grupo de três ou quatro colegas. Compare os recursos do iPhone, da Apple, com *smartphones* de outros fornecedores com recursos similares. Sua análise deve considerar o custo de aquisição de cada dispositivo, as redes sem fio nas quais cada dispositivo pode operar, planos de serviços e custo dos aparelhos, além dos serviços disponíveis para cada dispositivo. Você deve considerar também outros recursos de cada aparelho, inclusive a possibilidade de integração com aplicações existentes. Que aparelho escolhe? Que critérios utilizaria para guiar sua escolha? Se possível, use o Google Sites para postar links para outras páginas da Web, anúncios para a equipe, trabalhos; para trocarem ideias e trabalharem colaborativamente em documentos do projeto. Tente usar o Google Docs para desenvolver uma apresentação de suas descobertas para sua turma.

Resolvendo problemas organizacionais

Google *versus* Microsoft: O confronto dos gigantes da tecnologia

Google e Microsoft, duas das mais importantes empresas de tecnologia surgidas nas últimas décadas, estão equilibradas na luta pela dominação do ambiente de trabalho e da Internet. A batalha já está adiantada. A Google dominou a Internet, enquanto a Microsoft dominou o desktop. Ambas, entretanto, estão cada vez mais em busca de crescimento na área de domínio da outra. A competição entre as empresas está se tornando acirrada.

Diferenças nas estratégias e nos modelos de negócios das duas empresas ilustram por que esse conflito irá definir nosso futuro tecnológico. A Google começou como uma empresa de pesquisa dentre muitas, mas a eficiência de seu algoritmo de PageRank e dos serviços de propaganda on-line, juntamente à sua habilidade para atrair as melhores e mais brilhantes mentes do setor, lançaram a Google para a projeção global. A ampla infraestrutura da empresa

permite que ofereçam as velocidades de pesquisa mais rápidas e uma variedade de produtos baseados na Web. A Google acredita que as aplicações on-line serão um de seus próximos grandes negócios à medida que amadurecem seus negócios de pesquisa e pesquisa-propaganda.

A Microsoft alcançou sua gigantesca estatura com a força de seu sistema operacional Windows e de seu pacote Office de aplicativos de produtividade, utilizados por mais de 500 milhões de pessoas ao redor do mundo. Algumas vezes difamada por suas práticas anticompetitivas, a empresa e seus produtos são produtos para empresas e consumidores em busca de melhorias na produtividade de suas tarefas computacionais.

Hoje em dia, as duas empresas possuem visões de futuro muito diferentes, influenciadas pelo desenvolvimento contínuo da Internet e pela crescente disponibilidade de conexões Internet banda larga. A Google acredita que a maturação da Internet irá permitir que um número cada vez maior de tarefas seja executado pela Web, em computadores localizados em centros de dados remotos, e não nos desktops ou em computadores que pertençam às empresas. Essa ideia é conhecida como computação em nuvem, e é essencial para que o modelo de negócios da Google siga adiante. A Microsoft, por sua vez, construiu seu sucesso em torno do modelo da computação desktop. A meta da Microsoft é abraçar a Internet enquanto convence os clientes a manter o desktop como ponto central das tarefas computacionais.

Com a variedade de produtos baseados na Internet e ferramentas de pesquisa on-line, propaganda on-line, mapeamento digital, colaboração on-line, gerenciamento de fotos digitais, transmissão digital de rádio, blogs, redes sociais e visualização de vídeos on-line, a Google foi pioneira na computação em nuvem. A empresa está apostando na ideia de que a computação baseada na Internet irá acabar com a computação desktop como a principal maneira como as pessoas usam o computador. Usuários empregariam diversos dispositivos de conectividade para acessar aplicações de servidores remotos armazenados em centros de dados, em oposição ao trabalho local na máquina.

Uma vantagem do modelo de computação em nuvem é que os usuários não estariam atrelados a uma máquina particular para acesso a informações ou realização de seu trabalho. Outra é que a Google seria responsável pela maior parte da manutenção dos centros de dados que abrigam essas aplicações. As desvantagens do modelo, entretanto, são as exigências de uma conexão com a Internet para uso das aplicações, bem como as preocupações com a segurança em torno do fato de a Google gerenciar as informações. A empresa está apostando na onipresença da Internet e na disponibilidade das conexões banda larga e sem fio para compensar essas desvantagens.

A Microsoft já possui diversas vantagens significativas para continuar sendo relevante mesmo se a computação em nuvem se tornar tão boa quanto a Google anuncia. A empresa conta com um conjunto de aplicativos consagrados e populares com os quais muitos consumidores e empresas se sentem confortáveis. Quando a Microsoft lança um produto, os usuários dos produtos Office e Windows podem ter certeza de que saberão como utilizá-lo e que ele funcionará em seu sistema.

Ainda assim, a computação em nuvem representa uma ameaça para o principal modelo de negócios da Microsoft, que gira em torno do desktop como centro para quase todas as tarefas computacionais. Se, em vez de comprarem software da Microsoft, os consumidores puderem adquirir acesso às aplicações armazenadas em servidores remotos por um custo bastante inferior, o desktop deixa de ocupar a posição central. No passado, a Microsoft usava a popularidade de seu sistema operacional Windows (presente em 95 por cento dos PCs mundiais) e do Office para destruir os produtos concorrentes, como Netscape Navigator, Lotus 1-2-3 e WordPerfect. As ofertas da Google, entretanto, são baseadas na Web e, portanto, não são dependentes do Windows ou do Office. A Google acredita que a grande maioria das tarefas computacionais, em torno de 90 por cento, podem ser realizadas na nuvem. A Microsoft se opõe a essa afirmativa, alegando que ela é excessivamente exagerada.

Está claro que a Microsoft deseja reforçar sua presença na Internet caso a Google esteja correta. No início de 2008, ela tentou comprar a Yahoo! por 45 bilhões de dólares e não conseguiu. A Microsoft desejava não só fortalecer sua presença na Internet, mas também acabar com a ameaça de um acordo publicitário entre Google e Yahoo!. Em junho de 2008, essas chances diminuíram ainda mais por conta de um acordo entre Google e Yahoo! sob o qual a Yahoo! terceirizou uma parte de sua propaganda para a Google; que planejou distribuir alguns de seus anúncios junto de algumas das áreas menos rentáveis de pesquisa da Yahoo!, pois a tecnologia Google é muito mais sofisticada e gera maior receita por pesquisa do que qualquer outro concorrente. A Microsoft tentou novamente em julho de 2009, quando fechou um acordo com a Yahoo! no qual a empresa passa a utilizar a máquina de busca Bing.

As novas metas da Microsoft são 'inovar na pesquisa, ganhar em painéis de anúncios, reinventar experiências com portais e mídias sociais'. Embora a Microsoft enfrente desafios consideráveis na busca por esses objetivos, ela já progrediu. Em maio de 2009, a Microsoft lançou o Bing, uma nova máquina de busca na Internet que recebeu críticas bastante favoráveis pela qualidade de seus resultados, seus recursos e seu projeto. A popularidade do Bing ainda está atrás da de Yahoo! e Google, mas está atraindo muitos usuários. A Microsoft espera que a ferramenta ajude a empresa a se fortalecer no mercado de propaganda associada à pesquisa — principal mercado da Google.

Enquanto isso, a Google está desenvolvendo um novo sistema operacional baseado em seu navegador Web Chrome. O sistema operacional Google Chrome tem o objetivo inicial de ser utilizado nos computadores netbook de baixo custo (ver Capítulo 4), mas conseguirá gerenciar um PC completo. O sistema operacional é rápido, leve e capaz de conectar um usuário à Web em poucos segundos, e irá promover a visão de computação baseada na Web da Google.

A peça central dos esforços da Google para invadir o terreno da Microsoft é sua suíte Google Apps, uma série de aplicações baseadas na Web que incluem Gmail, mensagens instantâneas, calendário, aplicações de processamento de textos, apresentação e planilhas (Google Docs), e ferramentas para criação colaborativa de sites. Essas aplicações são versões mais simples dos aplicativos Microsoft

Office; a Google está oferecendo versões básicas delas gratuitamente, e edições 'Premier' por uma fração do preço da Microsoft. A assinatura da edição 'Premier' da Google Apps custa 50 dólares por ano/pessoa, enquanto a compra da versão para uma pessoa do Microsoft Office custa 500 dólares.

A Google acredita que a maioria dos usuários do Office não precisa dos recursos avançados do Word, do Excel e de outros aplicativos do pacote, e tem muito a ganhar com a migração para a Google Apps. Pequenas empresas, por exemplo, podem preferir versões mais simples e mais baratas de aplicativos para edição de textos, planilhas e apresentações eletrônicas porque não precisam dos recursos avançados do Microsoft Office. A Microsoft discorda, alegando que o Office é resultado de muitos anos e dólares de pesquisa em torno do que os consumidores desejam, e que esses consumidores estão muito satisfeitos com os produtos da empresa. Muitas outras empresas concordam, dizendo que estão relutantes em se afastar do Office porque o pacote é uma 'escolha segura'. Essas empresas estão sempre preocupadas com o fato de seus dados não estarem armazenados localmente e de que podem existir violações de leis como a Sarbanes-Oxley, que exige que as empresas mantenham e relatem seus dados ao governo sempre que solicitado.

A Microsoft está reagindo com a oferta de mais recursos de software e serviços baseados na Web para fortalecer sua presença on-line. Isso inclui a SharePoint, uma plataforma baseada na Web para colaboração e gerenciamento de documentos (ver Capítulo 2) e o Microsoft Office Live, que oferece serviços baseados na Web para e-mails, gerenciamento de projetos e organização de informações, além de complementos on-line para o Office.

Em setembro de 2009, a Microsoft apresentou sua versão Web da nova suíte Office 2010, a Office Web Apps, que inclui Word — para processamento de textos; Excel — para planilhas eletrônicas; Power Point — para apresentações; e OneNote — para coleta e compartilhamento de informações. Uma versão gratuita do Office Web, que inclui anúncios, está disponível aos usuários através do serviço on-line do Microsoft Windows Live. Outras versões estarão disponíveis para empresas mediante o pagamento de uma taxa. Usuários do Office Web Apps que possuam a versão desktop do Office conseguirão alternar entre as duas ferramentas sem problemas.

A Microsoft espera que versões tão leves e baseadas na Web de seus produtos irão diminuir a concorrência com o Google Docs e outras opções populares sem diminuir a lucratividade de seus produtos que ainda funcionam em PCs desktop ou servidores corporativos. O sistema operacional Microsoft Windows 7 possui uma versão que roda bem nos pequenos netbooks.

A batalha entre a Google e a Microsoft não está sendo travada somente na área de ferramentas de produtividade de escritório, navegadores Web e sistemas operacionais. Essas duas empresas estão trocando golpes em diversos outros campos, incluindo mapas na Web, vídeo on-line, software para telefones celulares e ferramentas on-line de registros de saúde. A Salesforce.com (veja o estudo de caso no final do Capítulo 4) representa o lado de outro conflito entre os dois gigantes. A Microsoft tentou entrar no modelo de software como serviço (SaaS) popularizado pela Salesforce.com, oferecendo um produto CRM competitivo por uma fração do preço. A Google seguiu um caminho contrário, criando uma parceria com a Salesforce para integração de sua aplicação CRM à ferramenta Google Apps e criação de um novo canal de vendas para comercializar a Google Apps para empresas que já adotaram o software CRM da Salesforce.

Ambas as empresas estão tentando se abrir como plataformas para desenvolvedores. A Google já lançou, inclusive, sua Google App Engine, que permite que programadores externos desenvolvam e lancem suas próprias aplicações por um custo mínimo. Em uma medida que representou uma mudança brusca em relação a sua antiga política, a Microsoft anunciou que revelaria muitos detalhes essenciais de seu software que costumavam ser mantidos em segredo. Os programadores terão menos dificuldades na construção de serviços que funcionem com os programas Microsoft. Os segredos da empresa lhe ajudaram a controlar o mercado, pois fazia com que outras empresas tivessem de utilizar o Windows no lugar de desenvolverem alternativas, mas se eles não puderem fazer o mesmo com a Google Apps, é melhor tentar outra abordagem para atrair desenvolvedores.

O tempo dirá se a Microsoft conseguirá ou não se defender dos desafios da Google a sua dominância no setor tecnológico. Muitas outras empresas promissoras foram vítimas da mudança de paradigma — como a dos mainframes para os computadores pessoais; a da impressão tradicional para a distribuição pela Internet; e, se a Google conseguir, dos computadores pessoais para a computação em nuvem.

Fontes: Jessica E. Vascellaro, "Google Strives to Help Online Software Catch Up". *The Wall Street Journal*, 15 jul. 2009; Neil McAllister, "Sneak Peek: Microsoft Office Web Apps". *InfoWorld*, 18 set. 2009; Miguel Helft, "Bing Delivers Credibility to Microsoft". *The New York Times*, 14 jul. 2009 e "Google's Free Phone Manager Could Threaten a Variety of Services". *The New York Times*, 12 mar. 2009; Jessica Hodgson, "Microsoft to Offer Office over Web as It Responds to Google Threat". *The Wall Street Journal*, 14 jul. 2009; Miguel Helft e Ashlee Vance, "Google Ploans a PC Operating System". *The New York Times*, 8 jul. 2009; Clint Boulton, "Microsoft Marks the Spot". *eWeek*, 5 maio 2008; Andy Kessler, "The War for the Web". *The Wall Street Journal*, 6 maio 2008; John Pallatto e Clint Boulton, "An On-Demand Partnership" e Clint Boulton, "Google Apps Go to School". *eWeek*, 21 abr. 2008; Miguel Helft, "Google and Salesforce Join to Fight Microsoft". *The New York Times*, 14 abr. 2008; e Robert A. Guth, Ben Worthen, e Charles Forelle, "Microsoft to Allow Software Secrets on Internet". *The Wall Street Journal*, 22 fev. 2008.

Perguntas sobre o estudo de caso

1. Defina e compare as estratégias de negócios e os modelos de negócios da Google e da Microsoft.
2. A Internet tirou o PC do centro das atenções? Justifique.

3. Por que a Microsoft tentou comprar a Yahoo!? Como isso afeta seu modelo de negócios? Você acha que é uma boa medida?
4. Qual a importância da Google Apps para o sucesso futuro da Google?
5. Você usaria a Google Apps em vez dos aplicativos do Microsoft Office para realizar suas tarefas computacionais? Justifique.
6. Que empresa e qual modelo de negócios você acredita que vai vencer essa guerra épica? Justifique.

Referências bibliográficas

BORLAND, John. "A Smarter Web". *Technology Review*, mar./abr. 2007.

BROOKS, Jason. "WiMax Back on the Map". *eWeek*, 7 abr. 2008.

CHOPRA, Sunil; SODHI, Manmohan S. "In Search of RFID's Sweet Spot". *The Wall Street Journal*, 3 mar. 2007.

DEKLEVA, Sasha; SHIM, J. P.; VARSHNEY, Upkar; KNOERZER, Geoffrey. "Evolution and Emerging Issues in Mobile Wireless Networks". *Communications of the ACM*, 50, n. 6, junho 2007.

FISH, Lynn A.; FORREST, Wayne C. "A Worldwide Look at RFID". *Supply Chain Management Review*, 1º abr. 2007.

GINEVAN, Sean. "Will WiMax Go the Distance?". *Information Week*, 17 mar. 2008.

GREENEMEIER, Larry. "RFID Tags Are on the Menu". *Information Week*, 5 fev. 2007.

HELFT, Miguel. "Google Makes a Case That It Isn't So Big". *The New York Times*, 29 jun. 2009.

HOOVER, J. Nicholas. "Enterprise 2.0". *Information Week*, 26 fev. 2007.

HOUSEL, Tom; SKOPEC, Eric. *Global Telecommunication Revolution: The Business Perspective*. New York: McGraw-Hill, 2001.

JESDANUN, Anick. "Researchers Explore Scrapping Internet". *Associated Press*, 13 abr. 2007.

KOCAS, Cenk. "Evolution of Prices in Electronic Markets under Diffusion of Price-Comparison Shopping". *Journal of Management Information Systems*, 19, n. 3, inverno 2002-2003.

LAGER, Marshall. "The Second Coming of 2.0". *Customer Relationship Management*, jun. 2008.

McCAFFERTY, Dennis. "All for One-Platform". *Baseline*, maio 2009.

McGEE, Marianne Kolbasuk. "Track This". *Information Week*, 11 fev. 2008.

NICOPOLITIDIS, Petros; PAPADEMITRIOU, Georgios; OBAIDAT, Mohammad S.; POMPORTSIS, Adreas S. "The Economics of Wireless Networks". *Communications of the ACM* 47, n. 4, abr. 2004.

PANKO, Raymond. *Business Data Networks and Telecommunications 7e*. Upper Saddle River, NJ: Prentice-Hall, 2009.

PAPAZOGLOU, Mike P. "Agent-Oriented Technology in Support of E-Business". *Communications of the ACM*, 44, n. 4, abr. 2001.

POTTIE, G. J.; KAISER, W.J. "Wireless Integrated Network Sensors". *Communications of the ACM*, 43, n. 5, maio 2000.

TALBOT, David. "The Internet Is Broken". *Technology Review*, dez. 2005/jan. 2006.

VARSHNEY, Upkar; SNOW, Andy; McGIVERN, Matt; HOWARD, Christi. "Voice Over IP". *Communications of the ACM*, 45, n. 1, jan. 2002.

VASCELLARO, Jessica E. "Coming Soon to a Phone Near You". *The Wall Street Journal*, 31 mar. 2008.

WEISER, Mark. "What Ever Happened to the Next-Generation Internet?". *Communications of the ACM*, 44, n. 9, set. 2001.

WINGFIELD, Nick; VRANICA, Suzanne. "Microsoft's 'Bing' to Take on Google". *The Wall Street Journal*, 12 mai. 2009.

XIAO, Bo; BENBASAT, Izak. "E-Commerce Product Recommendation Agents: Use, Characteristics, and Impact". *MIS Quarterly*, 31, n. 1, mar. 2007.

Capítulo

7

Segurança em sistemas de informação

OBJETIVOS DE ESTUDO

Ao concluir este capítulo, você será capaz de responder às seguintes perguntas:

1. Por que sistemas de informação estão vulneráveis a destruição, erros e uso indevido?
2. Qual o valor empresarial da segurança e do controle?
3. Quais os componentes de uma estrutura organizacional para segurança e controle?
4. Quais são as mais importantes tecnologias e ferramentas disponíveis para salvaguardar recursos de informação?

PLANO DO CAPÍTULO

Caso de abertura: *Boston Celtics marca pontos importantes contra* spyware

Vulnerabilidade dos sistemas e uso indevido

Valor empresarial da segurança e do controle

Como estabelecer uma estrutura para segurança e controle

Tecnologias e ferramentas para garantir a segurança dos recursos de informação

Projetos práticos em SIG

Estudo de caso: resolvendo problemas organizacionais — *Estamos prontos para uma guerra virtual?*

BOSTON CELTICS MARCA PONTOS IMPORTANTES CONTRA SPYWARE

Enquanto o Boston Celtics lutava por um ponto na final de alguns anos atrás, outra batalha acirrada era travada por seus sistemas de informação. Jay Wessel, vice-presidente de tecnologia do time de basquete, tentava marcar pontos contra os *spywares* de computador. Wessel e sua equipe de TI gerenciavam cerca de cem laptops distribuídos para técnicos e caça-talentos e para os funcionários de vendas, marketing e finanças, e essas máquinas estavam sendo inundadas de *malware* (software malicioso).

Como qualquer franquia de esporte, o Celtics está na estrada a maior parte do tempo durante a temporada de jogos. Técnicos, recrutadores e outros integrantes da equipe estão em jogos externos 40 vezes ou mais em cada temporada, utilizando o computador portátil para rever jogos e atualizar o status dos jogadores. Eles se conectam continuamente à Internet e à rede interna do Celtics a partir de aeroportos, hotéis e outros locais públicos. Segundo Wessel, "as conexões de Internet dos hotéis são foco da atividade de *spyware*". As pessoas retornavam à sede do time, em Boston, com os laptops infectados na estrada e contaminavam a rede. Além disso, o *spyware* estava afetando a acessibilidade e o desempenho do banco de dados proprietário de estatísticas do Celtics, criado no Microsoft SQL Server e utilizado pelos técnicos para preparar o time para os jogos. Wessel e sua equipe estavam sobrecarregados e investindo muito tempo tentando livrar as máquinas e a rede das contaminações.

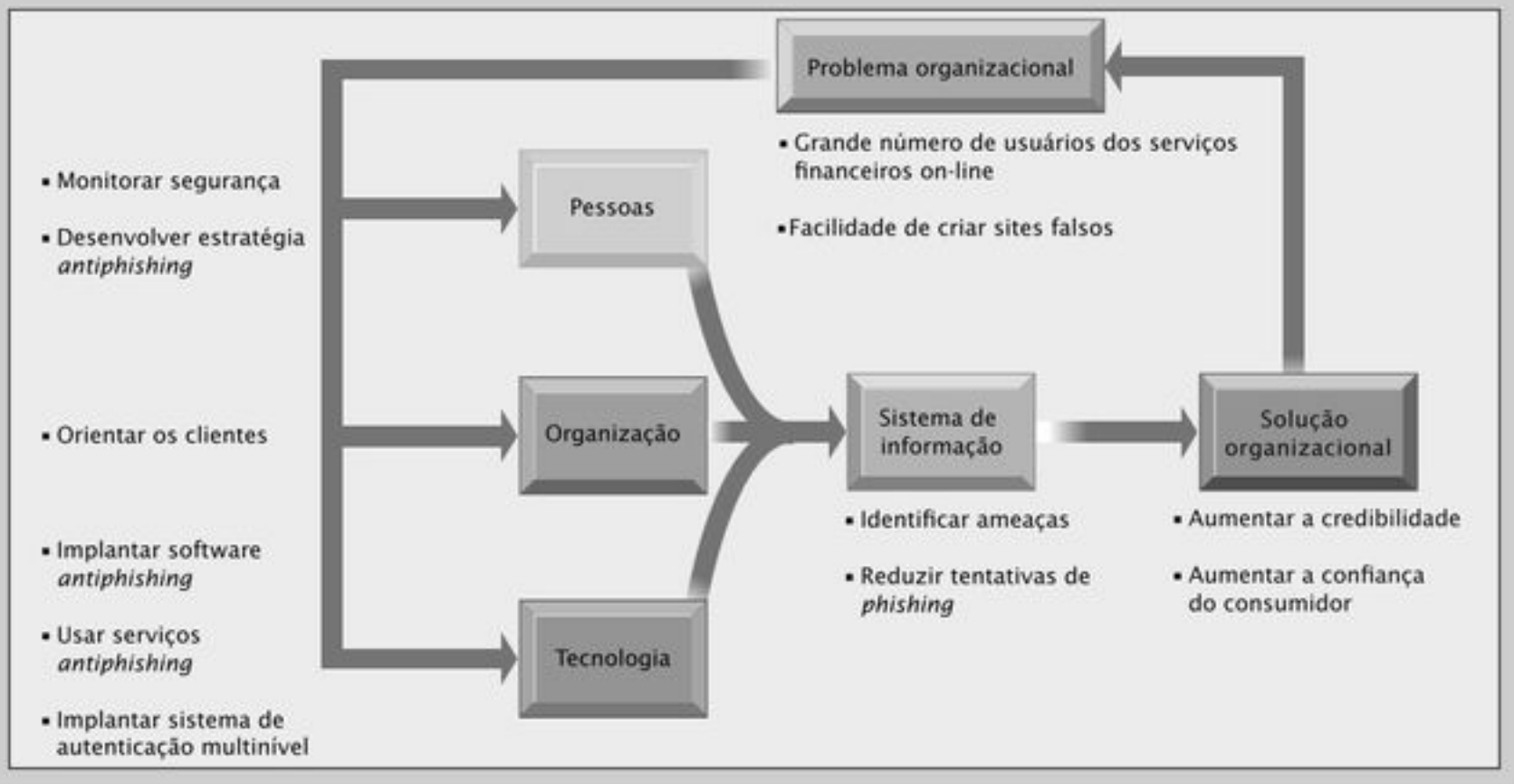
Durante um jogo da final, uma corrente de *spyware* invadiu os laptops por meio de uma conexão ruim de Internet em um hotel em Indiana. Foi quando Wessel decidiu tomar medidas mais agressivas contra *spywares*. Suas opções eram limitadas porque sua equipe era pequena e a empresa não dispunha de muitos recursos para tratar a segurança. A solução de software de segurança utilizada pelo Celtics (Aladdin eSafe Security Gateway e Webroot Spy Sweeper) era muito pesada. A única maneira de o Celtics executar a suíte de edição de vídeo utilizada para avaliar novos jogadores era remover esses produtos.

Como solução, Wessel decidiu recorrer ao aplicativo de segurança Mi5 Networks' Webgate. A ferramenta se posiciona entre o *firewall* e a rede do Celtics, impede que o *spyware* entre na rede e evita que as máquinas já infectadas se conectem a ela. O Webgate também impede que as máquinas infectadas por *spyware* retransmitam dados para a fonte que as infectou.

As máquinas infectadas ficam em quarentena e são limpas pela equipe de Wessel. O Webgate oferece uma tela de resumo executivo para que Wessel verifique a lista de máquinas infectadas, a atividade interna da botnet, ataques remotos e tentativas de *spyware* de se comunicar sorrateiramente com seus autores. Para complementar o Webgate, o Celtics usa o Surfcontrol (atualmente parte do Websense) que filtra atividades de e-mail e navegação na Web; o software antivírus Trend Micro; a tecnologia SonicWALL para detecção de invasão; e o Aladdin eSafe para detecção adicional de *malware*.

A rede do Celtics está livre de *spyware* desde que instalou o Webgate e essas outras ferramentas. O desempenho dos laptops, diminuído pelo software malicioso, aumentou; a rede corporativa funciona de modo muito mais veloz, e o número de chamadas para o suporte do Celtics diminuiu. Wessel observa, entretanto, que o sistema de segurança não funcionaria sem a educação dos usuários. Os empregados devem assinar uma política de uso aceitável que define o que é permitido fazer em suas máquinas, e são explicitamente desencorajados a visitar sites que possam transmitir mais *malware* para a rede do Celtics.

Fontes: Mi5 Networks, "Boston Celtics Shut Out Spyware with Mi5 Webgate Appliance", www.mi5networks.com, acessado em 19 set. 2009; Doug Bartholomew, "The Boston Celtics' New Malware Point Guard". *Baseline Magazine*, jan. 2008; e Bill Brenner, "Boston Celtics Face Off Against Spyware". SearchSecurity.com, acessado em 23 jun. 2008.



Os problemas que o *spyware* criou para o Boston Celtics ilustram algumas das razões pelas quais as empresas precisam prestar especial atenção à segurança dos sistemas de informação. O *spyware* malicioso que infectou os laptops de técnicos e empregados quando eles estavam viajando comprometeram o desempenho dos sistemas internos da empresa, dificultando para os empregados obter as informações de que precisavam para realizar suas tarefas.

A figura de abertura de caso nos chama a atenção para pontos importantes levantados pelo caso e pelo capítulo. Os técnicos do Boston Celtics e outros integrantes da equipe precisam usar seus laptops para se conectar aos sistemas internos da empresa enquanto viajam com o time. A conexão a redes públicas sem fio de hotéis e aeroportos expôs os computadores a softwares maliciosos, que os laptops acabaram por transmitir aos sistemas corporativos. A empresa estava gastando muito tempo e dinheiro livrando seus sistemas de *malware*. A gerência decidiu investir em uma nova tecnologia de segurança para fornecer camadas adicionais de proteção. Também revisou procedimentos de segurança que exigiam que os laptops infectados permanecessem em quarentena para não infectar os sistemas corporativos. A solução escolhida manteve o sistema do Celtics livre de *spyware* e aumentou o desempenho do sistema.

Vulnerabilidade dos sistemas e uso indevido

Você pode imaginar o que aconteceria se tentasse se conectar à Internet sem um firewall ou software antivírus? Em segundos o seu computador seria danificado, e talvez levasse dias para reabilitá-lo. Se seu computador fosse usado para administrar sua empresa, talvez você não conseguisse atender os clientes nem fazer pedidos aos fornecedores enquanto ele estivesse fora do ar. É possível que precisasse contratar — a preço de ouro — especialistas em sistemas para fazê-lo funcionar outra vez. E no fim descobrisse que, nesse meio-tempo, seu sistema de computador foi dominado por invasores que roubaram ou destruíram dados valiosos, incluindo arquivos confidenciais de pagamento de clientes. Se grande quantidade de dados tivesse sido destruída ou divulgada, sua empresa talvez nunca mais conseguisse se recuperar!

Em resumo, se você opera uma empresa hoje, precisa ter a segurança e o controle como prioridades. O termo **segurança** abarca as políticas, os procedimentos e as medidas técnicas usados para impedir acesso não autorizado, alteração, roubo ou danos físicos a sistemas de informação. Os **controles**, por sua vez, consistem em todos os métodos, as políticas e os procedimentos organizacionais que garantem a segurança dos ativos da organização, a precisão e a confiabilidade de seus registros contábeis e a adesão operacional aos padrões administrativos.

Por que os sistemas são vulneráveis

Quando grandes quantidades de dados são armazenadas sob formato eletrônico, ficam vulneráveis a muito mais tipos de ameaças do que quando estão em formato manual. Sistemas de informação em diferentes localidades podem ser interconectados por meio de redes de telecomunicação. Logo, o potencial para acesso não autorizado, uso indevido ou fraude não fica limitado a um único lugar, mas pode ocorrer em qualquer ponto de acesso à rede. A Figura 7.1 ilustra as ameaças mais comuns contra sistemas de informação contemporâneos. Elas podem originar-se de fatores técnicos, organizacionais e ambientais, agravados por decisões administrativas equivocadas. No ambiente de computação cliente/servidor multicamadas ilustrado aqui, existem vulnerabilidades em cada camada e nas comunicações entre as camadas. Os usuários da camada cliente podem causar danos ao introduzir erros ou ao acessar sistemas sem autorização. É possível acessar os dados enquanto vagam pela rede, roubar dados valiosos durante a transmissão ou alterar mensagens sem autorização. A radiação também pode interromper a rede em vários pontos. Intrusos podem deflagrar ataques de recusa de serviço ou inserir softwares mal-intencionados para interromper a operação de

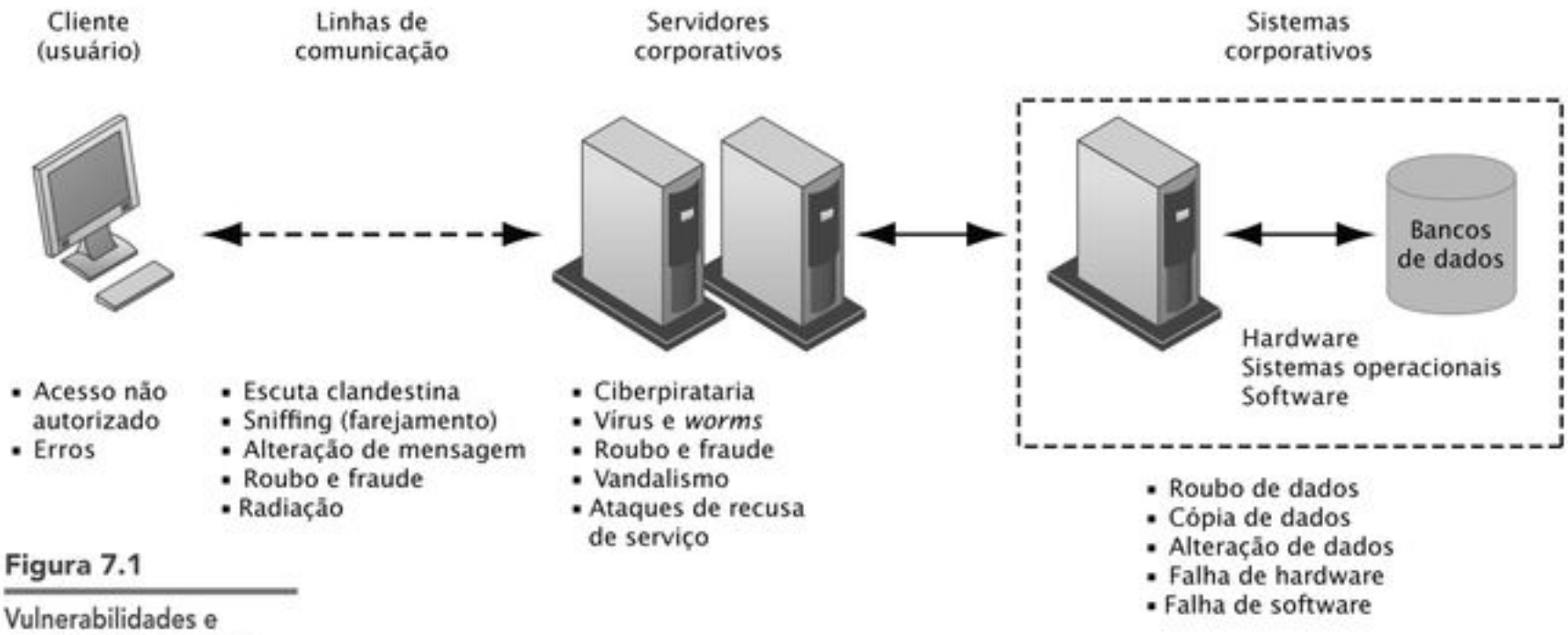


Figura 7.1

Vulnerabilidades e desafios de segurança contemporâneos

Normalmente, a arquitetura de uma aplicação baseada na Web inclui um cliente, um servidor e sistemas de informação corporativos conectados a bancos de dados. Cada um desses componentes apresenta vulnerabilidades e desafios de segurança. Enchentes, incêndios, quedas de energia e outros problemas técnicos podem causar interrupções em qualquer ponto da rede.

sites. Aqueles capazes de penetrar nos sistemas corporativos podem destruir ou alterar os dados armazenados em bancos de dados ou em arquivos.

Quando o hardware quebra, não está configurado apropriadamente ou é danificado por uso impróprio ou atividades criminosas, os sistemas não funcionam como deveriam. Já as causas de falha em softwares são erros de programação, instalação inadequada ou alterações não autorizadas. Além disso, quedas de energia, enchentes, incêndios ou outros desastres naturais podem prejudicar sistemas de computador.

As parcerias com outras empresas, no âmbito nacional ou internacional, aumentam a vulnerabilidade do sistema, pois informações valiosas podem residir em redes e computadores fora do controle da organização. Sem uma boa estrutura, dados valiosos podem ser perdidos, destruídos ou cair em mãos erradas, revelando importantes segredos comerciais ou informações que violem a privacidade pessoal.

O uso crescente de dispositivos portáteis para computação empresarial ajuda a piorar esse cenário. A portabilidade faz com que seja fácil roubar ou perder telefones celulares e *smartphones*, e suas redes estão vulneráveis a acesso por intrusos. *Smartphones* utilizados por executivos podem conter dados sensíveis como números de vendas, nomes de clientes, telefones e endereços de e-mail. Invasores podem acessar redes corporativas internas através desses dispositivos. Downloads não autorizados podem introduzir software malicioso.

Vulnerabilidades da Internet

Grandes redes públicas, incluindo a Internet, são mais vulneráveis porque estão abertas a praticamente qualquer um; quando sofrem abusos, as proporções do impacto podem ser imensas. Quando a Internet se torna parte da rede corporativa, os sistemas de informação da organização podem ficar vulneráveis a ações de estranhos.

Computadores permanentemente conectados à Internet via modem a cabo ou linha DSL estão mais sujeitos à invasão por estranhos, já que usam um endereço de Internet fixo, tornando-se, portanto, mais fáceis de identificar. (No serviço de discagem, para cada sessão é determinado um endereço de Internet temporário.) Um endereço de Internet fixo cria um alvo permanente para hackers.

Caso não utilizem uma rede privada segura, os serviços de telefonia baseados na tecnologia de Internet (Capítulo 6) podem ser mais vulneráveis que a rede de voz comutada. A maior parte do tráfego de voz sobre IP (VoIP) na Internet pública não está criptografada, de maneira que qualquer pessoa com uma rede possa ouvir as conversas. Hackers podem interceptar diálogos para obter dados de cartão de crédito e outras informações pessoais confidenciais, ou podem até mesmo interromper o serviço de voz entupindo os servidores que o comportam com tráfego falso.

A vulnerabilidade também aumentou com o uso disseminado de e-mail, mensagens instantâneas e programas ponto a ponto (P2P). O e-mail pode conter anexos que servem como trampolim para softwares mal-intencionados ou acesso não autorizado a sistemas corporativos internos. Os funcionários podem usar mensagens de e-mail para transmitir segredos de negócio, dados financeiros ou informações confidenciais dos clientes a destinatários não autorizados. Os aplicativos de mensagem instantânea mais comuns não usam uma camada segura para mensagens de texto, por isso podem ser interceptados e lidos por estranhos durante a transmissão pela Internet pública. O recurso de mensagens instantâneas pela Internet pode, em alguns casos, ser usado como passagem secreta para uma rede até então segura. Compartilhar arquivos através de redes P2P, como as utilizadas no compartilhamento de músicas ilegais, também pode transmitir software malicioso ou expor a estranhos as informações de computadores individuais ou corporativos.

Desafios da segurança sem fio

É seguro se conectar a redes sem fio em aeroportos, bibliotecas ou outros locais públicos? Depende do quão alerta você está. Mesmo a rede sem fio de sua casa está vulnerável, pois é fácil fazer a varredura das redes sem fio que utilizam tecnologias a rádio. Tanto o Bluetooth quanto o Wi-Fi são suscetíveis a escutas. Embora o alcance das redes Wi-Fi seja de apenas algumas dezenas de metros, ele pode ser estendido a 400 metros por meio de antenas externas. As redes locais (LANs) que usam o padrão 802.11 podem ser facilmente penetradas por estranhos munidos de laptops, cartões sem fio, antenas externas e softwares piratas gratuitos. Os hackers podem usar essas ferramentas para detectar redes desprotegidas, monitorar o tráfego da rede e, em alguns casos, obter acesso à Internet ou a redes corporativas.

A tecnologia de transmissão Wi-Fi foi projetada para que as estações se encontrassem e ouvissem umas às outras com facilidade. Os *identificadores de conjunto de serviços (Service Set Identifiers — SSID)* que identificam os pontos de acesso em uma rede Wi-Fi são transmitidos várias vezes e podem ser captados muito facilmente por programas *sniffers* (farejadores) intrusos (veja a Figura 7.2). Em muitos lugares, as redes sem fio não contam com proteções básicas contra o **war driving**, ação em que um espião dirige um carro entre edifícios ou estaciona do lado de fora e tenta interceptar o tráfego por redes sem fio.

Um hacker pode usar uma ferramenta de análise de 802.11 para identificar o SSID. (Windows XP, Vista e Windows 7 têm recursos para detectar o SSID usado na rede e automaticamente configurar o NIC de rádio dentro do dispositivo do usuário.) Um intruso que tenha se associado ao ponto de acesso usando o SSID correto pode acessar outros recursos na rede e utilizar o sistema operacional Windows para identificar outros usuários conectados à rede e, inclusive, clicar nos dispositivos de outros usuários, localizar arquivos de documentos e mesmo abrir ou copiar esses arquivos.

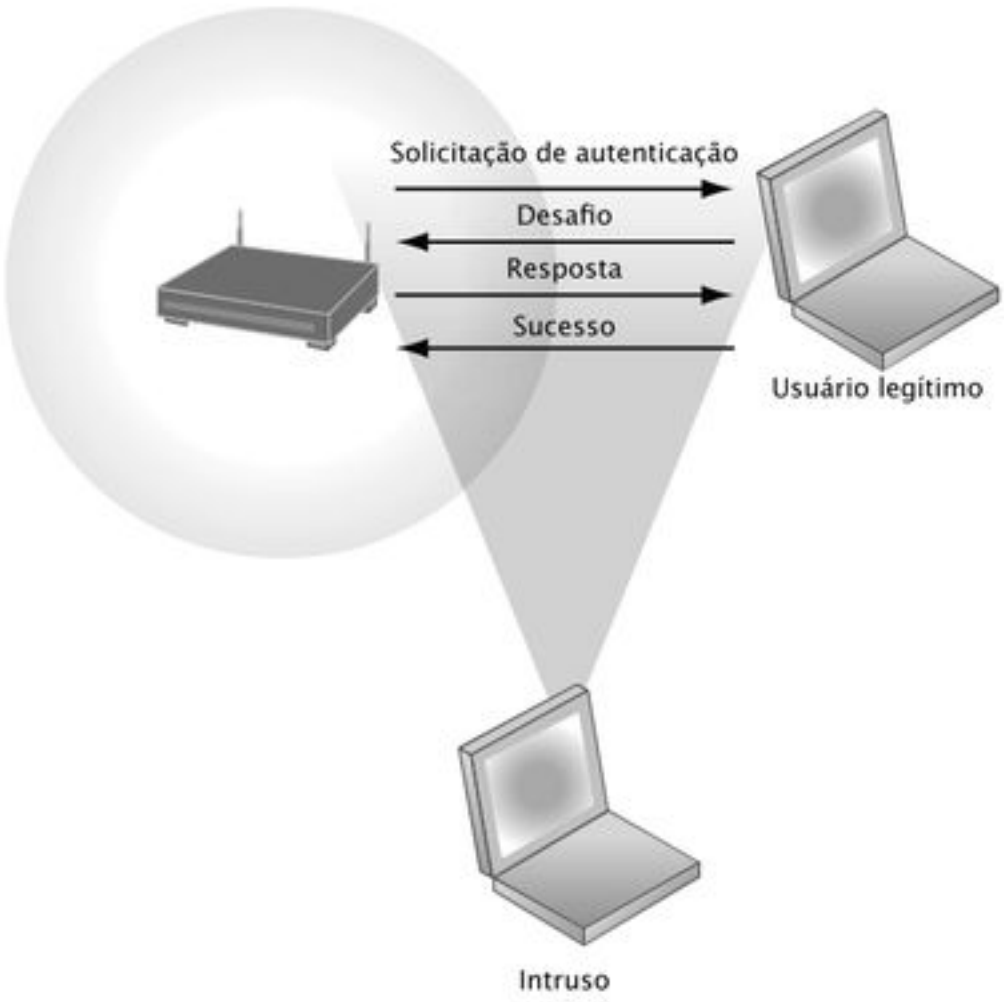
Os invasores também podem usar as informações que colheram sobre endereços IP e SSIDs para estabelecer pontos de acesso ilícitos em um canal de rádio diferente, em lugares físicos próximos aos usuários; assim, forçam o NIC de rádio do usuário a se associar ao ponto de acesso ilícito. Uma vez tendo ocorrido essa associação, os hackers podem capturar nomes e senhas de usuários acima de qualquer suspeita.

O padrão de segurança inicial desenvolvido para Wi-Fi, denominado *Wired Equivalent Privacy (WEP),* não é muito eficiente. O WEP vem embutido em todos os produtos de padrão 802.11, mas seu uso é opcional. Os usuários precisam ativá-lo e muitos se esquecem de fazê-lo, deixando muitos pontos de acesso desprotegidos. A especificação WEP básica exige que um ponto de acesso e todos os seus usuários compartilhem a mesma senha criptografada de 40 bits, facilmente decodificada por hackers a partir de uma pequena quantidade de tráfego. Sistemas de autenticação e criptografia mais robustos já estão disponíveis, mas é interesse dos usuários instalá-los.

Figura 7.2

Desafios de segurança em ambientes Wi-Fi

Muitas redes Wi-Fi podem ser facilmente invadidas por intrusos. Eles usam programas sniffers *para obter um endereço e, assim, acessar sem autorização os recursos da rede.*



Software mal-intencionado: vírus, *worms*, cavalos de Troia e *spywares*

Programas de software mal-intencionados são designados ***malware*** e incluem uma variedade de ameaças, tais como vírus de computador, *worms* e cavalos de Troia. **Vírus de computador** é um programa de software espúrio que se anexa a outros programas de software ou arquivos de dados a fim de ser executado, geralmente sem conhecimento nem permissão do usuário. A maioria dos vírus de computador transporta uma 'carga'. A carga pode ser relativamente benigna, como instruções para exibir uma mensagem ou imagem, ou pode ser altamente destrutiva — destruir programas ou dados, entupir a memória do computador, reformatar o disco rígido ou fazer com que programas funcionem de maneira imprópria. Normalmente, os vírus passam de computador para computador quando se executa determinada ação, como enviar um e-mail com anexo ou copiar um arquivo infectado.

Os ataques mais recentes vêm de ***worms***, programas de computador independentes que copiam a si mesmos de um computador para outro por meio de uma rede. (Diferentemente dos vírus, eles podem funcionar sozinhos, sem se anexar a outros arquivos de programa, e dependem menos do comportamento humano para se disseminar. Isso explica por que os *worms* se espalham muito mais rapidamente que os vírus.) Os *worms* destroem dados e programas, assim como prejudicam e até interrompem o funcionamento de redes de computadores.

Worms e vírus são muitas vezes disseminados pela Internet a partir de arquivos de software baixados de arquivos anexados a transmissões de e-mail, de e-mails danificados ou de mensagens instantâneas. Os vírus também invadem sistemas de informação computadorizados a partir de discos ou máquinas 'infectados'. Os *worms* transmitidos por e-mail são os mais problemáticos.

Existem mais de 200 vírus e *worms* para contaminação de dispositivos móveis, como Cabir, Commwarrior e Frontal.A. Este último, por exemplo, instala um arquivo corrompido que causa falhas no telefone e impede que o usuário reinicie o dispositivo. Os vírus para dispositivos móveis podem representar grandes ameaças para a computação empresarial, pois existem muitos dispositivos móveis atualmente conectados aos sistemas de informação corporativos.

Aplicações da Web 2.0 — como blogs, wikis e redes sociais como Facebook e MySpace — surgiram como um novo caminho para *malware* e *spyware*. Essas aplicações permitem que os usuários publiquem código de software como parte do conteúdo permitido, e esse código pode ser automaticamente executado quando a página é visualizada. Em agosto de 2008, por exemplo, hackers maliciosos atacaram usuários ingênuos do Facebook através de postagens no mural, utilizado pelos integrantes para deixar mensagens uns para os outros. Assumindo a identidade de amigos dos usuários, os hackers postaram mensagens incentivando o clique em um link para um vídeo que os transportava a uma página perigosa da Web onde recebiam a instrução de baixar a nova versão do Flash player, da Adobe, para visualizar o vídeo. Se os usuários autorizassem o download, o site instalava um cavalo de Troia chamado Troj/Dloadr-BPL que trazia outros programas ao PC. Em julho de 2009, hackers exploraram as vulnerabilidades do popular serviço TwitPic, do Twitter. Roubaram os dados de conexão ao site de Britney Spears e enviaram mensagens a seus seguidores dizendo que a cantora havia morrido (Acohido, 2009; Perez, 2008).

A Tabela 7.1 descreve as características de alguns dos *worms* e vírus mais prejudiciais já existentes.

Ao longo da última década, *worms* e vírus causaram bilhões de dólares de prejuízo às redes corporativas, sistemas de e-mail e dados. Segundo a pesquisa *State of the Net 2009*, da *Consumer Reports*, os consumidores norte-americanos perderam 7,5 bilhões de dólares por conta de *malware* e varreduras on-line, e a maioria dessas perdas foi causada por *malware* (*Consumer Reports*, 2009).

Cavalo de Troia é um software que parece benigno, mas depois faz algo diferente do esperado. O cavalo de Troia em si não é um vírus, porque não se replica, mas é muitas vezes uma porta para que vírus ou outros códigos mal-intencionados entrem no sistema do computador. O termo refere-se ao gigantesco cavalo de madeira usado pelos gregos durante a Guerra de Troia para enganar os troianos, que abriram para eles os portões de sua cidade fortificada. Uma vez dentro dos muros da cidade, os soldados gregos escondidos no cavalo revelaram-se e tomaram o local.

Outro exemplo de cavalo de Troia dos tempos modernos é o Pushdo Trojan, que usa um link para um cartão eletrônico como chamariz em um e-mail para enganar usuários do Windows e fazê-los iniciar um programa executável. Uma vez que é executado, ele finge ser um servidor Web Apache e tenta distribuir programas *malware* executáveis para as máquinas Windows infectadas.

No momento, **ataques por SQL injection** são as maiores ameaças do tipo *malware*. Ataques por SQL injection tiram proveito das vulnerabilidades nas aplicações da Web codificadas com deficiência para introduzir código de programa malicioso nos sistemas e redes corporativos. Essas vulnerabilidades ocorrem quando uma aplicação da Web falha na autenticação ou filtro dos dados digitados por um usuário em uma página — o que pode acontecer quando se encomenda algo on-line. O atacante usa o erro de validação de dados de entrada para enviar uma consulta SQL perigosa ao banco de dados, plantar código malicioso ou acessar outros sistemas na rede. Grandes aplicações da Web possuem centenas de locais para entrada de dados de usuários, cada uma criando uma oportunidade para um ataque por SQL injection.

Acredita-se que um grande número de aplicações da Web está vulnerável a ataques por SQL injection, e existem ferramentas disponíveis para que os hackers verifiquem essas vulnerabilidades. Essas ferramentas conseguem localizar um campo de entrada de dados em um formulário da rede, inserir dados nesse campo e verificar a resposta para ver se está vulnerável a um ataque por SQL injection.

Alguns tipos de ***spyware*** (software espião) também atuam como softwares mal-intencionados. Esses programinhas instalam-se nos computadores para monitorar a atividade do internauta e usar as informações para fins de marketing. Milhares de tipos de *spyware* já foram documentados.

Muitos usuários acham *spyware* irritante e alguns críticos se preocupam com as violações à privacidade dos usuários de computador. Algumas formas de *spyware*, porém, são

Tabela 7.1 **Exemplos de códigos mal-intencionados**

Nome	Tipo	Descrição
Conficker (também conhecido como Downadup, Downup)	Worm	Detectado pela primeira vez em novembro de 2008. Usa falhas do Windows para controlar máquinas e conectá-las a um computador virtual que pode ser comandado remotamente. Possui mais de 5 milhões de computadores ao redor do mundo sob seu controle. Difícil de exterminar.
Storm	Worm/Cavalo de Troia	Identificado pela primeira vez em 2007. Espalha-se por spam com um falso anexo. Infectou mais de 10 milhões de computadores, fazendo com que eles se juntassem à sua rede zumbi de computadores ligados à atividade criminal.
Sasser.ftp	Worm	Apareceu pela primeira vez em maio de 2004. Espalhou-se pela Internet através do ataque a IPs aleatórios. Faz com que os computadores travem e reiniciem continuamente e os leva a procurar mais vítimas. Infectou milhões de computadores ao redor do mundo, afetando as operações de check-in da British Airways, das estações da guarda costeira britânica, de hospitais em Hong Kong, das agências de correio de Taiwan e do Westpac Bank da Austrália. Sasser e suas variações causaram um dano estimado entre 14,8 e 18,6 bilhões de dólares ao redor do mundo.
Mydoom.A	Worm	Apareceu pela primeira vez em 26 de janeiro de 2004. Espalha-se como anexo de e-mail. Envia mensagens para coletados de máquinas infectadas, falsificando o endereço do remetente. No seu auge, este worm diminuiu o desempenho da Internet global em dez por cento e o tempo de download de páginas da Web em até 50 por cento. Foi programado para parar depois de 12 de fevereiro de 2004.
Sobig.F	Worm	Identificado pela primeira vez em 19 de agosto de 2003. Espalha-se por meio de anexos de e-mail e envia montantes massivos de mensagens com informações falsas sobre o remetente. Foi desativado em 10 de setembro de 2003, depois de danificar mais de 1 milhão de PCs e causar um dano estimado entre 5 e 10 bilhões de dólares.
ILOVEYOU	Vírus	Detectado pela primeira vez em 3 de maio de 2000. Vírus de script escrito em Visual Basic e transmitido como um anexo em e-mails com o assunto ILOVEYOU. Sobrescreve música, imagens e outros arquivos com uma cópia sua. Causou um dano estimado entre 10 e 15 bilhões de dólares.
Melissa	Macro vírus/ Worm	Apareceu pela primeira vez em março de 1999. Script de macro do Word enviado para infectar arquivos do Word para as 50 primeiras entradas do livro de endereços do Microsoft Outlook. Infectou de 15 a 29 por cento de todos os PCs, causando um prejuízo entre 300 e 600 milhões de dólares.

muito mais perversas. Os ***key loggers*** (literalmente, registradores de tecla) registram cada tecla pressionada em um computador para roubar números seriais de softwares, deflagrar ataques na Internet, obter acesso a contas de e-mail, descobrir senhas para sistemas de computador protegidos ou coletar informações pessoais como números de cartão de crédito. Outros programas espiões alteram as homepages do navegador da Web, redirecionam pedidos de busca ou entopem a memória do computador a ponto de diminuir sua velocidade.

Hackers e cibervandalismo

Hacker é um indivíduo que pretende obter acesso não autorizado a um sistema de computador. Dentro da comunidade hacking, o termo ***cracker*** normalmente é usado para designar o *hacker* com intenções criminosas, embora na imprensa em geral os termos *hacker* e *cracker* sejam usados indiscriminadamente. *Hackers* e *crackers* obtêm acesso não autorizado após encontrar fragilidades nas medidas de segurança empregadas pelos sites e sistemas de computador, muitas vezes tirando proveito das várias características da Internet que a tornam um sistema aberto e fácil de usar.

As atividades dos *hackers* deixaram de ser meras invasões de sistemas e se expandiram, a ponto de incluir roubo de mercadorias e informações, danos em sistemas e **cibervandalismo**, isto é, a interrupção, a alteração da aparência ou até mesmo a destruição de um site ou sistema de informação corporativo. Por exemplo, cibervândalos transformaram muitos grupos de sites do MySpace dedicados a interesses como produção doméstica de cerveja ou bem-estar animal em muros virtuais repletos de fotografias e comentários ofensivos.

Spoofing e sniffing

Na tentativa de ocultar sua verdadeira identidade, os *hackers* muitas vezes se disfarçam usando endereços de e-mail falsos ou fingindo ser outra pessoa. O ***spoofing*** (disfarce) também pode envolver o redirecionamento de um link para um endereço diferente do desejado, estando o site espúrio 'disfarçado' como o destino pretendido. Links formulados para levar a determinado site podem ser reescritos para enviar os usuários a um site totalmente diferente, conforme o interesse do *hacker*. Por exemplo, se os *hackers* redirecionam os clientes para um site falso parecidíssimo com o verdadeiro, podem então receber e processar pedidos, literalmente roubando o negócio ou pegando informações confidenciais do cliente. Mais detalhes sobre outras formas de *spoofing* são fornecidos na explanação sobre crimes de informática.

Sniffer (farejador) é um tipo de programa espião que monitora as informações transmitidas por uma rede. Quando usados de maneira legítima, os *sniffers* podem ajudar a identificar pontos frágeis ou atividades criminosas na rede; mas quando usados para fins ilícitos, podem ser danosos e muito difíceis de detectar. Os *sniffers* permitem que os *hackers* roubem informações de qualquer parte da rede, inclusive mensagens de e-mail, arquivos da empresa e relatórios confidenciais.

Ataques de recusa de serviço

No **ataque de recusa de serviço (ataque DoS — *denial of service*)**, *hackers* lotam um servidor de rede ou servidor da Web com centenas de falsas comunicações ou requisições de informação, a fim de inutilizar a rede. A rede recebe tantas consultas que não consegue lidar com elas e, assim, fica indisponível para solicitações de serviço legítimas. Um **ataque distribuído de recusa de serviço (ataque DDoS — *distributed denial of service*)** usa inúmeros computadores para inundar e sobrecarregar a rede a partir de diferentes pontos. Durante os protestos na eleição iraniana de 2009, por exemplo, ativistas estrangeiros apoiadores de oposição fizeram ataques DDoS ao governo do Irã. O site oficial do governante do país (ahmedinejad.ir) ficou inacessível em diversas ocasiões.

Embora não destruam informações nem acessem áreas restritas dos sistemas de informação da empresa, os ataques DoS muitas vezes tiram um site do ar, impedindo que usuários legítimos o acessem. Para sites de e-commerce muito procurados, esses ataques custam caro. Enquanto o site está fora do ar, os clientes não podem realizar compras. As pequenas e médias empresas estão especialmente vulneráveis, pois suas redes tendem a ser menos protegidas do que as redes das grandes empresas.

Os responsáveis por ataques de recusa de serviços geralmente usam milhares de PCs 'zumbis' infectados por softwares mal-intencionados sem o conhecimento dos proprietários e, depois, organizados em uma **botnet** (algo como 'rede de robôs'). Os *hackers* criam as botnets infectando os computadores alheios com um *malware* robô, que abre uma 'passagem secreta' por meio da qual o atacante pode dar instruções. O computador infectado

torna-se, então, um escravo, ou zumbi, servindo a um computador mestre que pertence a outra pessoa. Quando o *hacker* já infectou computadores em número suficiente, pode usar os recursos conjuntos da botnet para deflagrar ataques distribuídos de recusa de serviço, campanhas de *phishing* ou de e-mails 'spam' não solicitados.

O estudo de caso no final do capítulo descreve ondas múltiplas de ataques distribuídos de recusa de serviço direcionados a um conjunto de sites de agências governamentais e outras empresas da Coreia do Sul e dos Estados Unidos realizados em julho de 2009. O responsável pelo ataque utilizou uma botnet que assumiu o controle de 65 mil computadores e conseguiu tirar esses sites do ar por vários dias. A maioria dos robôs vinha da China e da Coreia do Norte. Ataques via botnet originários da Rússia foram responsáveis por tirar do ar os sites do governo estoniano, em abril de 2007, e do governo georgiano, em julho de 2008.

Crimes de informática

A maioria das atividades de *hacking* é composta por atos criminosos, e a vulnerabilidade dos sistemas que acabamos de descrever faz deles alvos para outros tipos de crimes de informática. Em julho de 2009, por exemplo, agentes federais norte-americanos prenderam Sergey Aleynikov, programador de computadores da firma de investimentos bancários Goldman Sachs, por roubar software proprietário utilizado na realização de negócios rápidos e lucrativos no mercado financeiro. O software trouxe muitos milhões de dólares em lucros anuais para a Goldman e, nas mãos erradas, poderia ter sido utilizado para manipular o mercado financeiro de modo desleal. O Departamento de Justiça dos Estados Unidos define **crimes de informática** como "quaisquer violações da legislação criminal que envolvam conhecimento de tecnologia da informática em sua perpetração, investigação ou instauração de processo". O computador pode ser alvo de um crime ou instrumento de um crime. A Tabela 7.2 dá exemplos dessas duas categorias de crimes de informática.

Ninguém sabe a magnitude do problema dos crimes de informática — quantos sistemas são invadidos, quantas pessoas estão envolvidas nessa prática ou o prejuízo econômico total.

Tabela 7.2 **Exemplos de crime de informática**

Computadores como alvos de crime
Violar a confidencialidade de dados computadorizados protegidos
Acessar um sistema de computador sem autorização
Acessar intencionalmente um computador protegido para cometer fraude
Acessar intencionalmente um computador protegido e infligir-lhe danos, de maneira negligente ou deliberada
Transmitir intencionalmente um programa, código de programa ou comando que deliberadamente cause danos a um computador protegido
Ameaçar causar danos a um computador protegido
Computadores como instrumentos de crime
Roubo de segredos comerciais
Cópia não autorizada de software ou de material com propriedade intelectual registrada, como artigos, livros, músicas e vídeos
Esquemas para defraudação
Usar e-mail para ameaças ou assédio
Tentar intencionalmente interceptar comunicações eletrônicas
Acessar ilegalmente comunicações eletrônicas armazenadas, inclusive e-mail e caixa postal de voz
Possuir material de pedofilia armazenado em um computador ou transmiti-lo eletronicamente

De acordo com uma pesquisa realizada em 522 empresas sobre segurança e crimes de informática, conduzida pelo CSI em 2008, a perda anual dos participantes ocasionada por crimes de informática e ataques à segurança estava próxima de 500 mil dólares (Richardson, 2008). Muitas empresas relutam em registrar esse tipo de crime, ou porque pode haver funcionários envolvidos, ou porque a organização teme que, ao tornar pública a sua vulnerabilidade, isso manche sua reputação. Os tipos de crime de informática mais danosos do ponto de vista financeiro são os ataques DoS, a introdução de vírus, o roubo de serviços e a interrupção de sistemas de computador.

Roubo de identidade

Com o crescimento do comércio eletrônico e da Internet, o roubo de identidade tem se tornado especialmente perturbador. **Roubo de identidade** é um crime em que um impostor obtém informações pessoais importantes, como número de identificação da Previdência Social, número da carteira de motorista ou número do cartão de crédito para se fazer passar por outra pessoa. As informações podem ser usadas para obter crédito, mercadorias ou serviços em nome da vítima, ou para dar ao ladrão falsas credenciais. De acordo com a Javelin Strategy & Research, 4,7 por cento dos norte-americanos foram vítimas de roubo de identidade em 2008 e sofreram perdas que totalizaram 48 bilhões de dólares (Javelin, 2009).

O roubo de identidade floresceu na Internet, com arquivos de cartão de crédito como um dos alvos principais dos *hackers* de sites. Além disso, os sites de e-commerce são fontes fabulosas de informações pessoais dos clientes — nome, endereço e número telefônico. Munidos dessas informações, os criminosos podem assumir novas identidades e estabelecer linhas de crédito para seus próprios fins.

Uma prática cada vez mais popular é uma forma de *spoofing* chamada ***phishing***, já descrita no caso de abertura deste capítulo. O *phishing* envolve montar sites falsos ou enviar mensagens de e-mail parecidas com as enviadas por empresas legítimas, a fim de pedir aos usuários dados pessoais confidenciais. As mensagens de e-mail instruem o destinatário a atualizar ou confirmar cadastros, fornecendo números da Previdência Social, informações bancárias ou de cartões de crédito e outras informações confidenciais, respondendo ao próprio e-mail, ou inserindo os dados no site falso. Dentre as principais empresas atacadas por esse método estão Ebay, PayPal, Amazon, Walmart e uma variedade de bancos.

Novas técnicas de *phishing* denominadas *evil twins* e *pharming* são ainda mais difíceis de detectar. Os ***evil twins*** (gêmeos do mal) são redes sem fio que fingem oferecer conexões Wi-Fi confiáveis à Internet, tais como aquelas encontradas em saguões de aeroportos, hotéis ou cafeterias. Com a rede falsa, que parece idêntica a uma rede pública legítima, os fraudadores tentam capturar senhas ou números de cartão de crédito dos incautos usuários que se conectam a ela.

O ***pharming***, por sua vez, redireciona os usuários a uma página da Web falsa, mesmo quando a pessoa digita o endereço correto da página da Web no seu navegador. Isso é possível porque os praticantes do *pharming* conseguem acessar as informações sobre endereços que os provedores de serviços de Internet armazenam para acelerar a navegação; caso esses ISPs usem softwares com brechas de segurança em seus servidores da Web, os fraudadores conseguem 'hackear' e alterar esses endereços.

A Seção Interativa sobre organizações descreve o maior caso de roubo de identidade registrado até hoje, no qual *hackers* invadiram sistemas corporativos de empresas como TJX Corporation, Hannaford Brothers, 7-Eleven e outros varejistas importantes e roubaram mais de 130 milhões de números de cartões de crédito e débito. Ao ler esse caso, preste atenção às questões humanas, organizacionais e tecnológicas levantadas pelo problema e avalie se essas empresas implantaram soluções eficientes.

O Congresso norte-americano reagiu à ameaça dos crimes de informática em 1986, com a *Lei de Uso Indevido e Fraude de Informática*. Essa lei torna ilegal o acesso a um sistema de computador sem autorização. A maior parte dos estados norte-americanos possui leis similares, e os países europeus dispõem de legislação no mesmo sentido. O Congresso norte-americano também aprovou, em 1996, a *Lei Nacional de Proteção à Infraestrutura de Informação*,

SEÇÃO INTERATIVA: ORGANIZAÇÕES — O pior roubo de dados da história

Em 17 de agosto de 2009, o jovem de 28 anos Alberto Gonzalez, de Miami, foi acusado pelo maior crime de invasão e roubo de identidade da história dos Estados Unidos, juntamente de dois cúmplices russos. Promotores públicos federais alegaram que os três premeditaram um esquema global para roubar mais de 130 milhões de números de cartões de crédito e débito entre os anos de 2006 e 2008 invadindo os sistemas computacionais de empresas, entre elas a cadeia de supermercados Hannaford Bros., 7-Eleven e Heartland Payment Systems, uma administradora de cartões de crédito.

O grupo utilizou uma rede de computadores em Nova Jersey, Califórnia, Illinois, Letônia, Holanda e Ucrânia para infiltrar os sistemas computadorizados das empresas-alvo utilizando técnicas sofisticadas para evitar a detecção por software antivírus. Eles plantaram programas nas redes dessas empresas que lhes permitiam roubar mais dados no futuro, além de programas do tipo *sniffer* para capturar dados de cartões enquanto eram transmitidos entre os sistemas computacionais. Uma quantidade não especificada de números de cartões de crédito e débito roubados foi vendida on-line e usada para realizar compras não autorizadas e retiradas bancárias.

Gonzalez e seu grupo também foram responsáveis por outros grandes roubos de dados. Em 18 de setembro de 2009, Gonzalez foi acusado em 19 casos de atividades criminais e fraude com cartão de crédito contra Barnes & Noble, OfficeMax, Boston Market e Sports Authority. O jovem também foi responsabilizado pelo roubo de 40 milhões de números de cartões de crédito e débito da TJX Cos., matriz da T.J. Maxx.

Os roubos de dados nas lojas Hannaford, Heartland e 7-Eleven realizaram ataques por *injection* (SQL), definidos anteriormente neste capítulo. Ataques desse tipo são bem compreendidos e há anos os especialistas em segurança alertaram os varejistas sobre eles. Ainda assim, muitas empresas ainda usam versões antigas do software gerenciador de banco de dados SQL Server, da Microsoft, que permite que *hackers* assumam o controle do banco de dados por meio de *injection*.

Gonzalez e seus comparsas começaram a realizar ataques por *injection* por volta de agosto de 2007. Antes disso, eles invadiam sistemas corporativos explorando fragilidades da segurança da rede sem fio. Os ladrões dirigiam ao redor dos prédios e varriam as redes sem fio dos varejistas em busca de vulnerabilidades. Em seguida, instalavam *sniffers* que se conectavam às redes de processamento de cartões de crédito, interceptando números de cartões de crédito e débito e números pessoais de identificação.

Em julho de 2005, essas técnicas permitiram que o grupo extraísse mais de 40 milhões de números de cartões de crédito e débito da TJX. A equipe de Gonzalez identificou uma rede vulnerável em uma loja de departamentos da Marshalls, em Miami, e utilizou-a para instalar *sniffers* nos computadores da matriz da cadeia, a TJX. O grupo então conseguiu acessar o banco de dados central da empresa, que armazenava transações dos consumidores de lojas como T.J. Maxx, Marshalls, HomeGoods e A.J. Wright nos Estados Unidos e em Porto Rico, e das lojas HomeSense, no Canadá.

A TJX ainda utilizava o antigo sistema de criptografia WEP (*wired equivalent privacy*), relativamente fácil de ser quebrado por *hackers*. Outras empresas já tinham mudado para o padrão WPA (*wi-fi protected access*), mais seguro e com criptografia mais complexa; mas, na época, a TJX ainda não havia feito a troca. Mais tarde, um auditor descobriu que a empresa também havia negligenciado a instalação de *firewalls* e criptografia de dados na maioria dos computadores que utilizavam rede sem fio, além de não instalar adequadamente outra camada de software de segurança que havia adquirido. Em um processo da Comissão de Valores Mobiliários, a TJX admitiu ter transmitido dados de cartões de crédito aos bancos sem criptografia, violando as instruções da própria empresa. A TJX também retinha em seus sistemas os dados dos proprietários dos cartões por muito mais tempo do que o estipulado pelas regras do setor para armazenamento de tais informações.

Em março de 2008, a gerência da TJX concordou em fortalecer a segurança dos sistemas de informação da empresa. Ela também concordou em receber auditores terceirizados para rever medidas de segurança a cada dois anos durante os próximos 20 anos. A empresa já gastou mais de 200 milhões de dólares para tratar seu roubo de dados, incluindo acordos legais. A Forrester Research estima que os gastos da TJX com o roubo de dados podem ultrapassar 1 bilhão de dólares ao longo dos próximos cinco anos, incluindo custos com consultores, atualizações de segurança, honorários de advogados e marketing adicional para reaver clientes.

A Hannaford Bros. também já começou a implantar medidas adicionais de segurança. A empresa atualizou seus *firewalls*, instalou um sistema de segurança e um serviço de detecção ininterruptos da IBM, e também começou a criptografar o tráfego que flui pela rede privada entre os registros de suas lojas e sua administradora de cartões de crédito. (As instruções dos padrões de segurança de dados do setor de administradoras de cartões existentes, que se aplicam também a todas as empresas administradoras de cartões de crédito, exigem somente que sejam criptografados os dados transmitidos em redes públicas.)

Fontes: Jaikumar Vijayan, "SQL Injection Attacks Led to Hartland, Hannaford Breaches". *Chief Security Officer*, 19 ago. 2009; Dan Kaplan, "After Breach, Hannaford Details IT Security Remodel". *SC Magazine*, 23 abr. 2009; Brad Stone, "3 Indicted in Theft of 130 Million Card Numbers". *The New York Times*, 18 ago. 2009 e "11 Charged in Theft of 41 Million Card Numbers". *The New York Times*, 6 ago. 2008; Siobhan Gorman, "Arrest in Epic Cyber Swindle". *The Wall Street Journal*, 19 ago. 2009; Andrew Conry-Murray, Dan Berthiaume, "Data Breaches Cause Concern". *eWeek*, 7 abr. 2008; e "T.J. Maxx Probe Reveals Data Brach Worse Than Originally Thought". *Information Week*, 21 fev. 2007.

PERGUNTAS SOBRE O ESTUDO DE CASO

1. Liste e descreva as fragilidades do controle de segurança da Hannaford Bros. e das empresas TJX.
2. Que fatores humanos, organizacionais e tecnológicos contribuíram para esses problemas?
3. Qual foi o impacto empresarial das perdas de dados da TJX e da Hannaford sobre essas empresas e seus consumidores?
4. As soluções adotadas pela TJX e pela Hannaford foram eficientes? Justifique.
5. Nesse caso, quem deveria ser culpado pelas perdas causadas pelo uso fraudulento de cartões de crédito? TJX e Hannaford? Os bancos distribuidores dos cartões de crédito? Os consumidores? Justifique.
6. Que soluções sugeriria para evitar os problemas?

transformando a distribuição de vírus e ataques de *hackers* contra sites em crimes federais. Outras leis norte-americanas, como as que dispõem sobre escuta clandestina, fraude por meio eletrônico, espionagem financeira, privacidade das comunicações eletrônicas, assédio e ameaças por e-mail e pornografia infantil, cobrem crimes de informática envolvendo interceptação de comunicação eletrônica, uso de comunicação eletrônica para defraudação, roubo de segredos comerciais, acesso ilegal a comunicações eletrônicas armazenadas, uso de e-mail para ameaças e assédio e transmissão ou posse de pornografia infantil.

Alguns atos danosos cometidos com computadores não são necessariamente ilegais, mas ainda assim podem ser considerados antiéticos. O **uso indevido do computador** é a prática de atos que envolvem o computador e nem sempre são ilegais, mas são vistos como antiéticos. Um tipo de uso indevido amplamente disseminado é o **spam**, pelo qual organizações ou indivíduos enviam milhares e até mesmo centenas de milhares de e-mails e mensagens eletrônicas não solicitadas, perturbando a vida de pessoas e empresas.

Fraude do clique

Quando você clica em um anúncio exibido por uma máquina de busca, o anunciante normalmente paga uma taxa por cada clique, que supostamente fará com que clientes potenciais sejam direcionados a seus produtos. A **fraude do clique** ocorre quando um indivíduo ou programa de computador clica fraudulentamente em um anúncio on-line sem qualquer intenção de descobrir mais sobre o anunciante ou realizar uma compra. A fraude do clique tornou-se um problema sério no Google e em outros sites que oferecem propaganda paga por clique.

Algumas empresas contratam empresas terceirizadas (em geral de países de baixa renda) para clicar fraudulentamente em anúncios dos concorrentes a fim de enfraquecê-los através do aumento dos custos de marketing. A fraude do clique também pode ser deflagrada por programas de computador que realizam o clique, normalmente utilizando botnet para esse fim. Máquinas de busca como as do Google tentam monitorar a fraude do clique, mas relutam em falar sobre seus esforços para lidar com o problema.

Ameaças globais: ciberterrorismo e guerra cibernética

As atividades cibercriminais que descrevemos — distribuição de *malware*, ataques de recusa de serviço e golpes por *phishing* — não têm fronteiras. A Sophos, empresa de segurança de computadores, relatou que 37 por cento do *malware* que identificou em 2008 tinha origem nos Estados Unidos, enquanto 28 por cento vinha da China, e 9 por cento partia da Rússia (Sophos, 2009). A natureza global da Internet permite que cibercriminosos atuem — e causem danos — em qualquer parte do mundo.

Existe uma crescente preocupação de que as vulnerabilidades da Internet e de outras redes poderiam ser exploradas por terroristas, serviços de inteligência estrangeiros ou outros grupos para criar perturbações e prejuízos disseminados. Alguns ciberataques podem visar o software que controla redes de energia elétrica, sistemas de controle de tráfego aéreo ou redes de grandes bancos e instituições financeiras. Acredita-se que pelo menos 20 países estejam desenvolvendo recursos de ataque e defesa para uma verdadeira guerra cibernética. O estudo de caso no final do capítulo discute esse problema com riqueza de detalhes.

Ameaças internas: funcionários

Quando pensamos em ameaças à segurança de uma empresa, tendemos a pensar em algo que se origina fora da organização. Na verdade, os próprios funcionários representam problemas sérios de segurança. Eles têm acesso a informações privilegiadas e, na presença de procedimentos de segurança internos frouxos, muitas vezes podem perambular por todos os sistemas da organização sem deixar vestígios.

Pesquisas concluíram que a falta de conhecimento dos usuários é a maior causa isolada de falhas na segurança de redes. Muitos funcionários esquecem a senha para acessar o sistema de computadores, ou permitem que colegas a utilizem, o que compromete o sistema todo. Intrusos mal-intencionados em busca de acesso ao sistema podem enganar os funcionários fingindo ser membros legítimos da empresa; assim, conseguem fazer com que revelem sua senha. Essa prática é denominada **engenharia social**.

Os funcionários — tanto usuários finais quanto especialistas em sistemas de informação — também são uma grande fonte de erros introduzidos nos sistemas de informação. Os funcionários podem introduzir erros inserindo dados incorretos, ou deixando de seguir as regras para o processamento de dados e o uso do equipamento. Especialistas em sistemas de informação também geram erros de software ao projetar e desenvolver novos softwares, ou ao fazer a manutenção dos programas existentes.

Vulnerabilidade do software

Erros de software também representam uma constante ameaça aos sistemas de informação, causando perdas indizíveis na produtividade. A crescente complexidade e o constante aumento de tamanho dos programas, juntamente das demandas por distribuições programadas no mercado, contribuíram para um aumento nas falhas de software ou vulnerabilidades. Um erro de programação no Departamento de Habitação da Cidade de Nova York, por exemplo, foi responsável pelo cálculo errôneo do aluguel de centenas de famílias assistidas entre setembro de 2008 e maio de 2009. As famílias afetadas teriam de pagar cerca de 183 dólares a mais pelo aluguel e foram ameaçadas de despejo por não pagar todo o valor (Fernandez, 2009).

Um problema sério com o software é a presença de ***bugs*** escondidos ou defeitos no código do programa. Estudos demonstraram que é quase impossível eliminar todos os *bugs* dos grandes programas. A principal fonte de erros é a complexidade do código de tomada de decisões. Um programa relativamente pequeno de algumas centenas de linhas irá conter dezenas de decisões que levarão a centenas ou mesmo milhares de caminhos diferentes. Programas importantes dentro da maioria de empresas costumam ser muito maiores, com dezenas de milhares ou mesmo milhões de linhas de código, cada uma com um número ainda maior de alternativas e caminhos se comparados aos programas menores.

A taxa zero de defeitos não pode ser alcançada nos grandes programas. O teste completo simplesmente não é possível. Milhares de anos seriam necessários para testar completamente os programas que contêm milhares de alternativas e milhões de caminhos. Mesmo com teste rigoroso, somente seria possível saber se determinado programa é confiável após um longo tempo de uso operacional.

Os softwares comerciais muitas vezes contêm falhas que geram não apenas problemas de desempenho, mas também vulnerabilidades de segurança que abrem as redes a invasores. Anualmente, as empresas de segurança identificam cerca de 5 mil vulnerabilidades de software na Internet e em programas para PC. Em 2008, por exemplo, a Symantec identificou 47 vulnerabilidades no Microsoft Internet Explorer, 99 nos navegadores Mozilla e 40 no Safari, da Apple. Algumas dessas vulnerabilidades são críticas (Symantec, 2009).

Para corrigir as falhas de software identificadas, os fornecedores criam softwares denominados ***patches*** (remendos) que consertam as falhas sem prejudicar o funcionamento do programa. Exemplo disso é o Vista Service Pack 2 (SP2), lançado em abril de 2009, que inclui algumas melhorias na segurança contra diversos *hackers* e *malware*. Cabe aos usuários do software localizar a vulnerabilidade, testar e aplicar todos os *patches*. Esse processo denomina-se *gestão de patch*.

Como a infraestrutura de TI de uma empresa normalmente possui uma infinidade de aplicativos empresariais, instalações de sistemas operacionais e outros serviços de sistema, a manutenção de *patches* em todos os dispositivos e serviços usados pela empresa pode ser um procedimento dispendioso e demorado. Além disso, os *malwares* são criados tão rapidamente que as empresas têm muito pouco tempo para agir, entre o momento em que uma vulnerabilidade e um *patch* são anunciados e o momento em que o software mal-intencionado aparece para explorar aquela vulnerabilidade.

Valor empresarial da segurança e do controle

Como a segurança não está diretamente relacionada à receita de vendas, muitas empresas relutam em gastar muito com ela. No entanto, a proteção dos sistemas de informação é tão crucial para o funcionamento da empresa que merece um olhar mais atento.

As empresas têm ativos de informação valiosíssimos a proteger. Sistemas muitas vezes abrigam informações confidenciais sobre impostos, ativos financeiros, registros médicos e desempenho profissional das pessoas. Eles também podem conter informações sobre operações corporativas, incluindo segredos de negócio, planos de desenvolvimento de novos produtos e estratégias de marketing. Sistemas governamentais podem armazenar informações sobre armamentos, operações de inteligência e alvos militares. Esses ativos de informação têm um valor incalculável, e a repercussão pode ser devastadora se forem perdidos, destruídos ou colocados em mãos erradas. Segundo estudo recente, se uma grande empresa tem sua segurança comprometida, em dois dias a partir da falha ela perde aproximadamente 2,1 por cento de seu valor de mercado, o que se traduz em uma perda média de 1,65 bilhão de dólares no mercado de ações a cada incidente (Cavusoglu, Mishra e Raghunathan, 2004).

Controle e segurança inadequados também podem criar sérios riscos legais. As empresas precisam proteger não apenas seus próprios ativos de informação, mas também os de clientes, funcionários e parceiros de negócios. Caso não consigam fazê-lo, podem ter de gastar muito em um litígio por exposição ou roubo de dados. Uma organização pode ser responsabilizada pelo risco e pelo dano desnecessários gerados caso não tenha tomado as medidas preventivas apropriadas para evitar a perda de informações confidenciais, corrupção de dados ou violação de privacidade. A BJ's Wholesale Club, por exemplo, foi processada pela Comissão Federal de Comércio por permitir que *hackers* acessassem seus sistemas e roubassem dados relacionados a cartões de crédito e débito para compras fraudulentas. Os bancos que cobraram os cartões com os dados roubados exigiram 13 bilhões de dólares da BJ's para compensá-los pelo reembolso pago aos proprietários dos cartões pelas compras fraudulentas. Uma sólida estrutura de controle e segurança que proteja os ativos de informação da empresa pode, portanto, gerar um alto retorno sobre o investimento. Segurança e controle fortes também aumentam a produtividade do empregado e diminuem os custos operacionais.

Requisitos legais e regulatórios para a gestão de registros eletrônicos

Nos últimos tempos, regulamentações do governo norte-americano forçam as empresas a levar a segurança e o controle mais a sério, pois exigem a proteção dos dados contra uso indevido, exposição e acesso não autorizado. Com isso, as empresas enfrentam novas obrigações legais no que diz respeito à retenção de documentos e à gestão de registros eletrônicos, bem como à proteção da privacidade.

Se você trabalhar no setor de saúde, nos Estados Unidos, sua empresa deverá obedecer à **Lei Americana de Responsabilidade e Portabilidade dos Seguros-Saúde (HIPAA)**, de 1996. Essa lei estabelece regras e procedimentos quanto à privacidade e à segurança médicas para simplificar a administração da saúde e automatizar a transferência de dados entre prestadores de serviço de saúde, beneficiários e operadores de planos de saúde. Para tanto, os membros do setor precisam reter informações dos pacientes por seis anos e garantir a confidencialidade desses registros. A lei especifica padrões de segurança, privacidade e