ROTEAMENTO

SOLUÇÕES
EDUCACIONAIS
INTEGRADAS

Roteamento móvel

Leandro Salenave Gonçalves

OBJETIVOS DE APRENDIZAGEM

- Descrever o roteamento para dispositivos móveis.
- Apresentar casos de roteamento em redes *ad hoc*.
- Explicar a técnica de *tunneling* no roteamento móvel.

Introdução

Para estudarmos roteamento móvel, é fundamental compreendermos que os roteadores são equipamentos tecnológicos que ligam rede de dados. Um exemplo da mobilidade que trataremos neste capítulo e que está ligado a equipamentos que não precisam estar conectados fisicamente por cabos para compartilhar a comunicação são os telefones móveis (também conhecidos como *smartphones*), que possuem tecnologia específica para poder fazer chamadas telefônicas a partir da conexão do aparelho a uma antena. As constantes evoluções e os estudos na área da mobilidade possibilitam o acréscimo de serviços aos *smartphones*, como, por exemplo, o acesso à internet.

Os *smartphones* não estão sozinhos na busca pelo acesso à mobilidade dos roteadores: dificilmente um *notebook* de uma residência fica ligado à rede por meio de um cabo; impressoras que usam a tecnologia *wireless* estão cada vez mais comuns; e os aparelhos de televisão já são capazes de acessar conteúdos da rede. Assim, é correto afirmar que, como toda conexão de dados, os roteamentos móveis precisam estabelecer protocolos e camadas necessários para padronizar o modo como os diferentes fabricantes e operadoras vão operar seus transportes de dados. Sobre a abrangência das camadas desse tipo de rede, Forouzan e Mosharraf (2013, p. 471) afirmam que "[...] a tecnologia sem fio abrange [...] tanto a camada de enlace, quanto a camada física da pilha de protocolos TCP/IP". Em

outras palavras, a mesma complexidade estrutural da rede física é perceptível na rede móvel, acrescida da preocupação com a segurança frente a tantas disponibilidades de serviços.

Neste capítulo, você poderá, além de entender o processo operacional dos roteamentos móveis, estudar dois conceitos distintos e complementares de rede. Um deles diz respeito às chamadas redes *ad hoc*, que se caracterizam por ligações temporariamente estabelecidas entre vários computadores e dispositivos. O outro conceito é o de tunelamento, que se refere à técnica de encapsular um protocolo dentro de outro, permitindo, por exemplo, enviar pacotes com segurança na internet.

Roteamento para dispositivos móveis

No que diz respeito ao uso de dispositivos móveis, hoje em dia os usuários finais desejam estar conectados a todo momento e em qualquer lugar. Nesse sentido, esses *hosts* móveis "[...] criam uma nova compilação: antes de rotear um pacote para um *host* móvel, primeiramente a rede precisa localizá-lo" (TANENBAUM, 2003, p. 289, tradução nossa).

Ainda sob esse entendimento acerca da disponibilidade, coexistem estruturalmente diferentes nomenclaturas que atendem ao roteamento móvel quanto à sua abrangência, entre as quais estão a LAN, a MAN e a WAN. Como nosso foco é a mobilidade, a relação que se estabelece é de conexões sem fio, o que na literatura pode ser encontrado como WLAN, WMAN e WWAN.

Uma vez que conhecer o destino é fundamental para entregar os pacotes de dados em uma rede, ao tratar de *hosts* móveis, o grande problema é saber onde eles estão. Conforme descreve Tanembaum (2003, p. 289, tradução nossa), "O objetivo do roteamento em sistemas móveis que estejam usando os seus endereços locais é fazer os pacotes alcançarem esses *hosts* de forma eficiente, onde quer que eles possam estar".

Na prática, as duas formas mais difundidas de conexão de dados em rede por dispositivos móveis são mediante os pacotes de dados de uma operadora de telefonia celular (3G, 4G, etc.) e pelo sinal Wi-Fi de uma rede. A Figura 1 demonstra um esquema de rede em que dispositivos móveis acessam os dados da rede a partir de um ponto de acesso Wi-Fi.

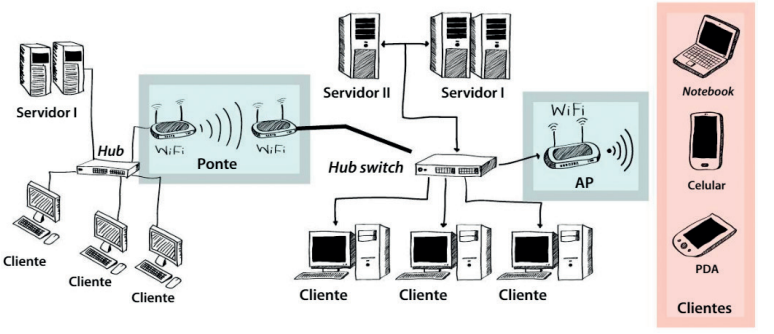

Figura 1. Uso do Wi-Fi como ponte e ponto de acesso.
Fonte: Adaptada de Ohmega1982/Shutterstock.com ([201-] *apud* LUMMERTZ, 2019, p. 74).

A outra forma de se estar conectado é por meio dos pacotes de dados fornecidos por uma operadora de telefonia celular. Segundo Tanembaum (2003, p. 128), a tecnologia que atende a esse sistema apresenta uma evolução tecnológica de transmissão: da **voz analógica** para a **voz digital**, chegando à **voz digital mais dados**.

O fato é que, para cada nova implementação tecnológica — que possibilita não apenas melhorias na voz digital, mas também uma crescente demanda pelo consumo de dados —, é necessário haver tecnologia compatível nos aparelhos celulares e nas antenas de transmissão. E tudo isso deve atender às regulamentações da agência reguladora do país, que, no caso do Brasil, é a ANATEL.

As diferentes tecnologias foram batizadas com o número da sua geração seguido da letra "G" (p. ex., 2G e 3G). Sobre o uso das antenas e a implementação do 4G, Forouzan e Mosharraf (2013, p. 514) afirmam:

> Usando esse sistema de antenas em conjunto com multiplexação especial, o 4G permite que fluxos independentes sejam transmitidos simultaneamente a partir de todas as antenas, aumentando muitas vezes a taxa de transferência de dados.

Também são exemplos de acesso móvel aos roteadores dispositivos ligados a aparelhos que antes precisavam da intervenção humana para operar. São condicionadores de ar, máquinas de lavar roupa, portões eletrônicos, cortinas, intervenções na condução de um veículo, operações fabris de uma empresa, etc. Essas conexões móveis que utilizam a rede como meio de

ligação recebem o nome de Internet das Coisas, que hoje são uma realidade em constante evolução.

Saiba mais

Internet das Coisas (IoT, do inglês *Internet of Things*) é uma rede de objetos físicos dotados de tecnologia embarcada capaz de receber e transmitir dados. Trata-se de aparelhos com capacidade computacional que são utilizados no cotidiano das pessoas e que se conectam à internet.

Porém, o esquema de rede apresentado na Figura 1 promove o acesso a dados não pelas antenas das operadoras, e sim pelo padrão IEE 802.11, comumente chamado "Wi-Fi". Mesmo sendo, desde a sua concepção, muito mais moderno que as redes cabeadas, esse tipo de estrutura passou por vários ajustes para atender a critérios de velocidade, custos de implementação e compatibilidade entre dispositivos. Assim, quando você verificar que uma rede possui padrões 802.11b, 802.11g ou 802.11n, saiba que se trata de variações sobre um mesmo tipo de padrão.

O zelo pelo encaminhamento dos roteadores garante a capacidade de explorar o melhor resultado possível de uma rede. No entanto, se os demais equipamentos ligados à rede não estiverem dentro dos padrões mais atuais, toda a rede vai baixar o padrão para atender ao equipamento mais antigo. No atendimento ao Wi-Fi, é utilizado o protocolo CSMA/CA (do inglês *Carrier Sense Multiple Access with Collision Avoidance*), que, na prática, permite a utilização dos modos de infraestrutura e *ad hoc*.

A propagação do sinal pode ser prejudicada por alguns empecilhos, como, por exemplo, os diversos tipos de materiais de construção e outros equipamentos eletrônicos. Por isso, não é qualquer lugar da casa ou do escritório que pode acomodar o equipamento. Além da suscetibilidade à interferência, a segurança da rede sem fio é grande fonte de preocupação, uma vez que os pacotes de dados trafegam livres pelo ar, e, desse modo, é possível que seu conteúdo seja revelado por outros membros que não o destino.

Considerando o modo estrutura, os dispositivos conectados precisam de um acesso do AP para fazer parte da rede. É comum que essa associação ocorra mediante um processo de autenticação, normalmente associado ao uso de senha ou por um filtro definindo o MAC daqueles que têm permissão para acesso à rede.

Desde a sua concepção, as redes móveis ganharam uma identificação programável para facilitar a localização do roteador por meio de um nome. Esse nome da rede é conhecido pela sigla SSID (do inglês *service set identifier*).

Vale registrar que, buscando aumentar a segurança, alguns profissionais de rede ocultam o SSID. Uma vez localizada a rede a que o dispositivo pretende se conectar, a liberação de uso acontece mediante a liberação do número de série do dispositivo, o MAC, ou mediante uma senha de acesso. Visando à coleta de dados pessoais, algumas redes liberam a conexão de um dispositivo ao seu roteador por meio de SSIDs sem senha; porém, ao se acessar a rede, o seu uso é condicionado a um questionário a ser respondido ou à satisfação de uma determinada condição, como, por exemplo, o compartilhamento da localização pessoal em uma rede social.

Para finalizarmos esta seção, vamos retomar o seu início, quando falamos sobre roteamento a partir de um celular. Se partirmos dos pressupostos de que todos os dispositivos que forem se conectando são passíveis de autenticação, que a rede é identificada por um SSID e que todos estão ligados a partir do próprio celular, é possível afirmar que essa conexão é um exemplo de ponto de acesso Wi-Fi.

Roteamento em redes *ad hoc*

Uma vez que já definimos que a grande diferença entre as conexões de estrutura e a *ad hoc* está na inexistência de um ponto central de ligação, é possível afirmar que, metodologicamente, a *ad hoc* é uma conexão ponto a ponto que liga diretamente dispositivos para que possam transacionar pacotes de dados.

O roteamento dessas redes ligadas diretamente ponto a ponto é chamado MANETs (do inglês *mobile ad hoc networks*). Nesse modelo, todos os nós fazem papel de roteadores, e as transmissões são realizadas na forma de *broadcast*, em que o enlace está ligado à potência de transmissão. Outra característica dos MANETs é a possibilidade de que um serviço prestado por um nó não esteja acessível no próximo dispositivo, visto que há variáveis quanto aos recursos tecnológicos de cada ponto. Na Figura 2, é representada uma comunicação entre os nós de uma rede MANET.

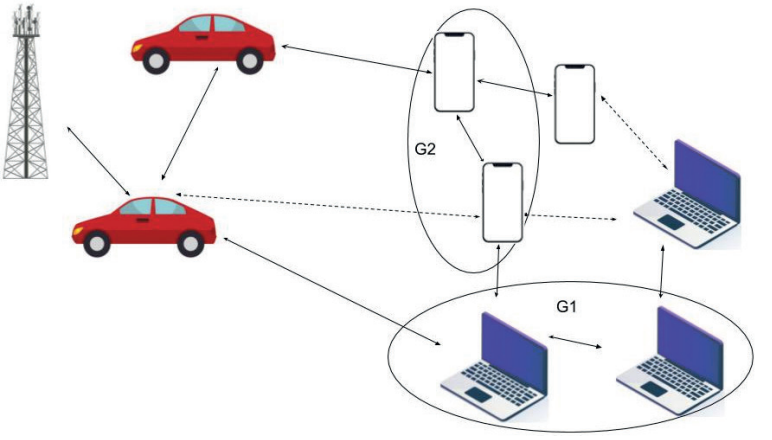

Figura 2. Roteamento em redes móveis *ad hoc*.

Como se observa na Figura 2, mesmo se tratando de uma conexão ponto a ponto, é possível estabelecer grupos (simbolizados pelos círculos G1 e G2), e as ligações podem ter conexões consideradas de enlace bom (sinalizadas pelas linhas contínuas) ou de enlace ruim (sinalizadas pelas linhas pontilhadas). A classificação dos enlaces está relacionada a muitas variáveis. Mesmo sendo MANETs como os demais nós, ao se tratar de conexões em veículos, protocolos específicos são somados ao MANET, atribuindo-se a eles o nome VANETs (do inglês *vehicular ad hoc networks*).

A fim de atender às características do *ad hoc*, protocolos foram criados para definir os padrões de comunicação. Podemos classificar os protocolos *ad hoc* em basicamente dois grupos: **proativos** e **reativos**. O *ad hoc* proativo está em constante estado de descoberta e manutenção de rotas, mesmo não havendo uma imediata necessidade de sua utilização. O *ad hoc* reativo, por sua vez, realiza a busca das rotas a um determinado destino somente quando é necessário comunicar-se com ele. Também chamado "roteamento sob demanda", o protocolo reativo executa a descoberta de novos nós apenas se existir uma solicitação por parte do nó originador da conexão.

Mesmo que seja um padrão econômico quanto ao tráfego na rede, o tempo entre a solicitação e o atendimento (conhecido na literatura como "latência") é consideravelmente maior no protocolo *ad hoc* reativo, se comparado ao proativo. Isso porque, para atender à solicitação, pode ainda não haver rotas para o destino. Por outro lado, esse padrão compensa a latência com alta

disponibilidade, podendo atender a limitados, mas constantes espectros de comunicação. Para atender ao *ad hoc* reativo, dois protocolos podem ser tomados como referência: o AODV e o DSR.

O AODV é um protocolo de roteamento *ad hoc* sob demanda em um vetor de distância "[...] destinado ao uso por nós móveis em uma rede *ad hoc*. Ele oferece adaptação rápida às condições de *link* dinâmico, baixo processamento e sobrecarga de memória, baixa utilização da rede e determina *unicast* rotas para destinos dentro da rede *ad hoc*" (RFC 3561, 2003, p. 1, tradução nossa).

No protocolo DSR (*Dynamic Source Routing*), cada nó armazena um *cache* de roteamento. Como define o RFC 4728 (2007), trata-se de um protocolo de roteamento projetado especificamente para uso sem fio. "O DSR permite que a rede seja completamente auto-organizada e autoconfigurável, sem a necessidade de qualquer infraestrutura ou administração de rede existente" (RFC 4728, 2007, p. 1, tradução nossa).

Assim, é correto afirmar que a diferença entre DSR e AODV é que, no primeiro, cada nó possui uma tabela de roteamento de salto, armazenando no seu *cache* todos os possíveis caminhos, ao passo que o AODV guarda em sua tabela apenas o nó máximo de uma entrada para cada destino. O gráfico apresentado na Figura 3 ajuda a identificar a quantidade de taxa de transferência necessária entre os diferentes protocolos. Embora o gráfico também apresente o OLSR, neste momento ele não faz parte do nosso estudo.

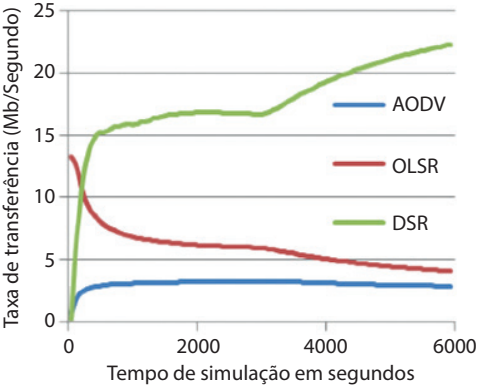

Figura 3. Comparação entre protocolos *ad hoc*.
Fonte: Adaptado de Elshaikh, Kamel e Awang (2009).

Conforme Figura 3, o protocolo AODV ocupa muito menos taxa de transferência que o DSR. Porém, saliente-se que essa constatação não descreve

a superioridade de um protocolo sobre o outro; o que ela descreve é a sua aplicabilidade. No DSR, os resultados são melhores quando há menor mobilidade e poucos nós. Já o AODV tem melhores resultados quando há vários nós e alta mobilidade.

Tunneling no roteamento móvel

Assim como em muitos protocolos, os aplicáveis a roteamentos móveis também fazem uso do tunelamento. Segundo Andrew Tanenbaum (2003), a necessidade de tunelamento de pacotes deriva da necessidade de um *host* móvel enviar pacotes roteados até a LAN local do *host*, o que é demonstrado na etapa 1 da Figura 4.

> Depois de obter o pacote encapsulado, o agente externo remove o pacote original do campo de carga útil e o envia ao *host* móvel como um quadro de enlace de dados. Em segundo lugar, o agente local diz ao transmissor que dali em diante ele deverá enviar pacotes ao *host* móvel encapsulando-os no campo de carga útil de pacotes explicitamente endereçados ao agente externo, em vez de enviá-los ao endereço local do *host* móvel (etapa 3) (TANENBAUM, 2003, p. 290, tradução nossa).

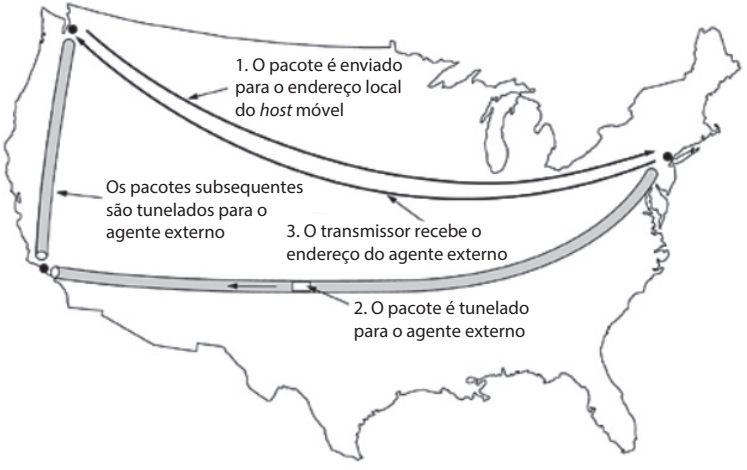

Figura 4. Fases de um tunelamento.
Fonte: Adaptada de Tanenbaum (2003).

As diferenças entre tunelamento Ip-em-Ip, tunelamento Ip-em-TCP e criptografia em carga útil são definidas por Douglas Comer (2016). O autor afirma que a criptografia possibilita as transformações "[...] dos dados úteis, mas deixa o cabeçalho intacto"; assim, "[...] quem interceptar os dados será capaz de aprender os endereços de origem e destino, bem como os números das portas" (COMER, 2016, p. 462). Quando a opção é por túneis Ip-em-Ip, conteúdo e cabeçalho são criptografados, ou seja, no tunelamento Ip-em-Ip, "[...] todos os campos do datagrama original são criptografados, incluindo o cabeçalho original" (COMER, 2016, p. 462). Por fim, no tunelamento Ip-em-TCP, as "[...] partes estabelecem uma conexão TCP e depois usam-na para enviar datagramas criptografados" (COMER, 2016, p. 463).

Manter esse nível de segurança cobra um preço da rede, o qual certamente está ligado ao desempenho. Entre as principais implicações, estão as apresentadas a seguir.

- **Latência:** ocorre porque o tempo entre envio e chegada está além dos processos de tunelamento. Uma vez que usam a rede roteada como meio, eles estão passíveis dos atrasos naturais desse processo.
- **Taxa de transferência:** ocorre porque está limitada às velocidades da rede (no caso, da internet). Esse problema de desempenho fica mais evidente em sistemas de alta disponibilidade projetados para rodar nas LANs.
- **Sobrecarga e fragmentação:** ocorrem porque, para encapsular e extrair os conteúdos tunelados nos datagramas, um conteúdo extra é acrescentado no datagrama. Considerando-se as diferentes velocidades e a disponibilidade de redes e sabendo-se que os datagramas precisam ser fracionados para transmissão, pode acontecer de algumas frações chegarem antes que outras, precisando aguardar a entrega de todas para restaurar o datagrama inteiro.

Não se pode falar sobre tunelamento sem citar as redes privadas virtuais (VPNs, do inglês *virtual private networks*). Esse tipo de infraestrutura usa redes públicas, como a internet, como meio de conexão entre dois dispositivos. A partir desse momento, a VPN inicia o processo de túnel, pois é encapsulado dentro dessa conexão um protocolo que garante a privacidade, ou seja, garante que apenas origem e destino tenham conhecimento do pacote como um todo, incluindo os dados e seu cabeçalho.

As VPNs são uma maneira de atender às necessidades de conexões seguras a custos aceitáveis, uma vez que a internet possui custos menores que os

das redes privativas. A Figura 5 ilustra a substituição de uma rede privativa pela VPN sobre a internet.

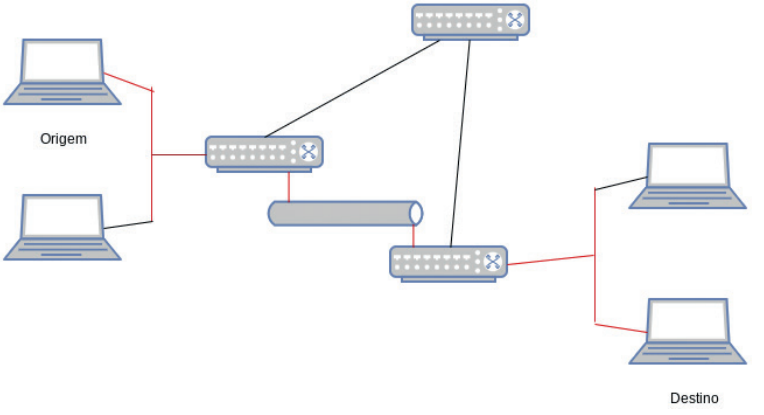

Figura 5. Rotas entre origem e destino, com e sem uso de tunelamento de VPN.

Como demonstrado na Figura 5, a comunicação entre origem e destino pode ocorrer por diferentes caminhos. Seguindo as linhas em vermelho, é possível identificar que um túnel faz a ligação entre o roteador mais próximo da origem e o mais próximo do destino. Isso simboliza que, nessa fase do tunelamento, os pacotes que trafegam possuem um processo de criptografia, dificultando a leitura do conteúdo por qualquer um que não seja o destino específico.

Para exemplificar a função do tunelamento, Tanenbaum (2003, p. 329, tradução nossa) lança mão da seguinte analogia:

> Imagine uma pessoa dirigindo seu carro de Paris a Londres. Na França, o carro trafega em baixa velocidade, usando sua própria energia; no entanto, ao chegar ao Canal da Mancha, ele é colocado em um trem de alta velocidade e é transportado para a Inglaterra pelo Eurotúnel (não é permitido o tráfego de automóveis nesse túnel). Na realidade, o carro está sendo transportado como uma carga [...]. Na outra extremidade, o carro passa a transitar nas estradas inglesas e continua a trafegar em velocidade baixa, com sua própria energia. Em uma rede externa, o *tunneling* de pacotes funciona da mesma forma.

Nessa analogia, o carro representa o pacote de dados, e o transporte de trem representa a camada que roda sob o tunelamento. Em síntese, a VPN é uma conexão encriptada na qual os pacotes de dados trafegam na internet em geral entre os computadores ou dispositivos móveis. Uma vez que a sua

conexão é criptografada, ninguém que interage com o túnel VPN é capaz de "ler" as comunicações.

Fique atento

É possível configurar uma conexão VPN a partir do próprio celular. Em celulares Android, basta seguir os passos apresentados a seguir para ativar as configurações.

1) Em "Menu", toque no botão "Configurações".
2) Toque no botão "Conexões sem fio e redes" e, depois, em "Mais".
3) Selecione qual tipo de protocolo VPN usar — a) PPTP; b) L2TP; c) L2TP/Ipsec PSK; d) L2TP/Ipsec CRT.
4) É possível que seja solicitado um certificado, o qual pode ser baixado ou instalado por meio do cartão microSD do Android. Caso isso aconteça, acesse "Configurações/Segurança" e marque a caixinha que diz "Usar credenciais confiáveis".
5) É necessário dar um nome à conexão.

Referências

COMER, D. *Redes de Computadores*. Porto Alegre: Bookman, 2016.

ELSHAIKH, M.; KAMEL, N.; AWANG, A. High throughput routing algorithm metric for OLSR routing protocol in Wireless Mesh Networks. *In*: International Colloquium on Signal Processing & Its Applications, 5., 2009, Kuala Lumpur. *Proceedings* [...]. Kuala Lumpur: [*s. l.*], 2009. p. 445–448. Disponível em: https://www.researchgate.net/publication/224503146_High_throughput_routing_algorithm_metric_for_OLSR_routing_protocol_in_Wireless_Mesh_Networks. Acesso em: 17 nov. 2020.

FOROUZAN, B. A.; MOSHARRAF, F. *Redes de computadores*: uma abordagem *top-down*. Porto Alegre: AMGH, 2013.

LUMMERTZ, R. S. *Cabeamento estruturado*. Porto Alegre: Sagah, 2019.

RFC_3561 - Roteamento Ad hoc On-Demand Distance Vector (AODV). *IETF Tools*, jul. 2003. Disponível em: https://tools.ietf.org/html/rfc3561. Acesso em: 17 nov. 2020.

RFC_4728 - O protocolo de roteamento de fonte dinâmica (DSR) para redes ad hoc móveis para IPv4, *IETF Tools*, feb. 2003. Disponível em: https://tools.ietf.org/html/rfc4728. Acesso em: 17 nov. 2020.

TANENBAUM, A. S. *Computer Network*. New Jersey: Prentice Hall, 2003.

Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Conteúdo:

SAGAH
SOLUÇÕES EDUCACIONAIS INTEGRADAS